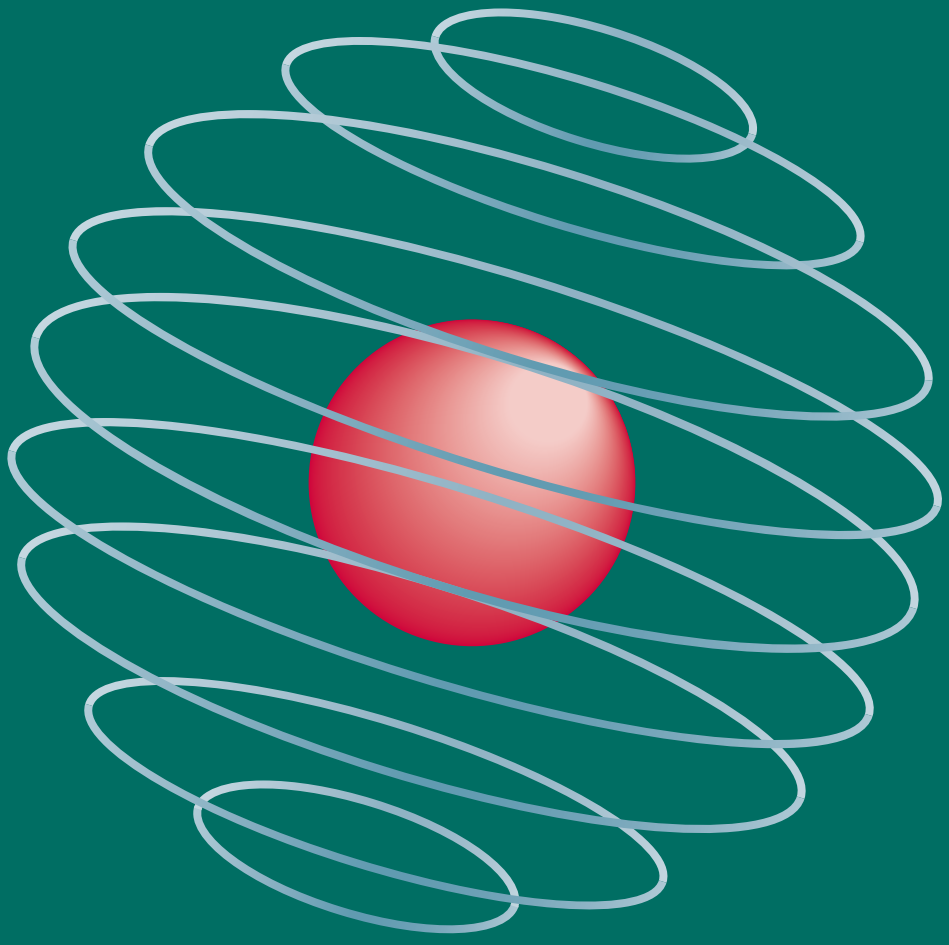
2020 YEARBOOK



UNIVERSITY OF OXFORD

CENTRE *for* DOCTORAL TRAINING *in* CYBER SECURITY

UKRI Engineering and Physical Sciences Research Council

Contents

All details correct as of August 2020

Director's Welcome

It's no exaggeration to say that this has been a year like no other – even if it's already a cliché. As University buildings closed in mid-March in response to the developing pandemic, members of the CDT were scattered. Some faced 'lockdown' in Oxford, whether in college rooms or private accommodation; others decamped to home countries or other places; one or two were even trapped in unexpected places. We have tried to capture something of the spirit of that period in some special articles for the yearbook.

Such a sudden dislocation has been quite disruptive for many. Whether through anxiety and health fears for themselves or loved ones; whether through having to work in constrained circumstances away from the office, library or lab; or whether through having to put experimental work on hold completely: many have seen their work substantially slowed or changed.

Of course, in common with the rest of the world, CDT members have found and sometimes enjoyed new ways of working. Lots of academic conferences moved online this year – and that made them accessible to a much wider audience than could ordinarily attend. We were able to arrange and deliver several online courses – one with a lecturer from the US East Coast who might have found it hard to spend a week in Oxford but could readily join us through electronic means. Our seminar programme has continued, as has our weekly Friday afternoon cyber café catch-up, moved from the Robert Hooke Building to Microsoft Teams (bring your own coffee!).

So, despite the disruptions, lots of excellent work has carried on this year. Students have submitted theses (the University at last allowed online submission, from the start of this academic year!) and defended them in virtual viva exams (academic gowns and sub fusc optional but encouraged). Papers have been published, career plans made, and countless contributions to the improvement of global cyber security have been produced.

We're rapidly approaching the point now where there are more alumni outside the CDT than we have currently-enrolled students, and news of some of those graduates is included here. These are the ones going out to change the world for the better – and by whom we will measure the impact of the CDT for many years to come.

Andrew Martin
Professor of Systems Security
Director, CDT in Cyber Security

Co-Director's Perspective

It has become a truism: cybersecurity is an interdisciplinary problem. No single academic profession can frame the problem uniformly. Stronger data encryption, for example, will not solve the question of why politically motivated hacking occurs in the first place. And yet one cannot deny that humans and machines have separate essences; understanding human behaviour is not the same as mastering computer programming. Interdisciplinarity, therefore, does not mean unidisciplinarity. Each discipline must recognise its own strengths and limits. Therein lies the central challenge of cyber studies: how to merge the knowledge and insights of distinct disciplines while preserving their core intellectual identities.

The CDT has embraced the educational aspect of that challenge. In the last seven years we developed a general curriculum that covers the broad gamut of cyber issues from diverse perspectives, ranging from secure systems architecture to data privacy ethics to the geopolitics of interstate hacking. Our approach is based on the recognition that cybersecurity challenges political, social, even philosophical understandings rather than merely technical ones. It applies even after students have departed to host departments across the University, where they deepen their studies within a defined discipline. The Centre provides continued opportunities to cross disciplinary divides via elective modules, research seminars, field excursions, and social events. To apply a metaphor borrowed from politics, the CDT represents a miniature "Congress of Disciplines" that respects the priorities, strengths, and limits of its member delegations. Although our model requires that students embed themselves within a disciplinary constituency, they are never far from the debates of the central chamber.

The model has worked well. Students who delve into the complex workings of machines gain a valuable understanding of how political and social forces shape their development and use. Those who focus on human affairs acquire a sense of rapidly changing technological realities. What emerges is a cohort of individuals equipped with specialised knowledge in defined fields and broad insights across them. This combination of perspectives prepares them to address problems of security that by their very nature transcend familiar jurisdictions of learning. And so our students have gone on to successful careers in academia, government, and private industry, much to the benefit of organizations that continue to grapple with increasingly sophisticated technological threats.

Not all truisms become truths. To proclaim (as many observers do) that cybersecurity is an interdisciplinary endeavour is not to make it so automatically. The natural inclination of academic disciplines is to dig chasms, not erect bridges, between fields of study. Opening up the interdisciplinary arena therefore requires a concerted institutional effort. Sometimes this effort entails integrating cyber studies into disciplines – such as political science or geography – that did not previously recognise it as relevant. In this way, the CDT has managed to fill at least some seats in a Congress that still features too many empty benches.

Lucas Kello
Associate Professor of International Relations
Co-Director, CDT in Cyber Security

Submitted Theses

OLUSOLA AKINROLABU

Supervisors: Andrew Martin, Department of Computer Science and Steve New, Saïd Business School

Cyber supply chain risks in cloud computing – the effect of transparency on the risk assessment of SaaS applications

While the cloud model has many economic and functional advantages, the increased external interactions of cloud applications have expanded the complexity of its architectures and reshaped its supply chain. Due to the variety of parties involved in cloud service delivery and the high degree of supplier autonomy, assessing cloud risks has become a challenge. Also, the widespread application of traditional frameworks to cloud risk assessment has several shortcomings, including the subjectivity of risk evaluation and inability to measure cyber risk in complex systems.

Recognising that recent work on cloud risk assessment has focussed on cloud consumer risks, we sought to address the cloud service provider (CSP) risk assessment challenge. This research began with an in-depth assessment of the literature in cloud risk assessment and supply chain transparency. We conducted surveys and semi-structured interviews to validate the transparency gap and establish its link with qualitative risk assessment methods. The results of the studies substantiated the need for more rigour in cloud risk assessments and provided evidence on how this can be improved with supply chain transparency.

To address this gap, we proposed the Cyber Supply Chain Cloud Risk Assessment (CSCCRA) model; a quantitative and supply chain-inclusive model targeted at Software-as-a-Service (SaaS) CSPs. The model is made up of three main components, two of which are novel inclusions to cloud risk assessment, i.e. supply chain mapping and supplier security assessment. The CSCCRA model reflects the systems thinking approach, enabling CSPs to visualise information flow through the supply chain, assess supplier security posture, document assumptions regarding the risk factors, and appraise security controls.

In evaluating the CSCCRA model, a three-step approach was adopted. First, the de¬veloped model was evaluated by the author and members of the academic community to ensure that it met our initial criteria. Second, the model was face-validated by cloud and risk experts within the industry. Third, we conducted three real-world case studies, using the model to assess the risks of SaaS providers. The result of these evaluations confirmed the usefulness and applicability of the model for assessing cloud provider risks. Also, the case study results and subsequent development of the CSCCRA web application showed that a structured and systematic application of the proposed model within a SaaS organi¬sation was capable of yielding objective and defensible results. The model demonstrated its utility by assisting stakeholders to quantify cloud risks, while also promoting cost-effective risk mitigation and optimal risk prioritisation.

Overall, these results advance knowledge both for research and in practice, taking us one step further into improving cloud risk assessment.

Bio

Olusola graduated with a BSc. (Honours) in Computer Science from Babcock University, Nigeria and also holds a Master's degree in Mobile and High-Speed Telecommunications Networks from Oxford Brookes University.

His industry experience spans over 16 years, where he has worked in both network and security-related roles. He has been involved in the design, implementation and support of global networks at this time. He currently holds various industry certifications including CISSP-ISSAP, CISA, CCSP, GSEC, TOGAF, GSNA, and CNSE. Following the completion of his DPhil, Olusola now works as a Security Architect within the Financial Industry.

His DPhil thesis explored the effect of supply chain transparency on the objectivity of cloud risk assessment. Through the application of a systems thinking approach to the problem area, the research showed that the application of a quantitative, structured, transparent and supply chain-inclusive model to cloud risk assessment could yield meaningful risk values and support proactive risk mitigation.

Publications

Can improved transparency reduce supply chain risks in cloud computing? Akinrolabu, O. and New, S. Operations and Supply Chain Management Journal, 10(3), pp.130-140, 2017.

Cyber supply chain risks in cloud computing–bridging the risk assessment gap. Akinrolabu, O., New, S. and Martin, A. Open Journal of Cloud Computing (OJCC), 5(1), pp 1-19, 2017.

The challenge of detecting sophisticated attacks: Insights from SOC Analysts. Akinrolabu, O., Agrafiotis, I. and Erola, A. 1st International Workshop on Cyber Threat Intelligence Management (CyberTIM 2018), 2018.

CSCCRA: A Novel Quantitative Risk Assessment Model for Cloud Service Providers. Akinrolabu, O., New, S. and Martin, A. 15th European, Mediterranean, and Middle Eastern Conference on Information Systems (EMCIS2018), (pp. 177-184). Springer, 2018.

Cloud Service Supplier Assessment: A Delphi Study. Akinrolabu, O., New, S. and Martin, A. In Proceedings of the 8th International Conference on Innovative Computing Technology (INTECH 2018), 2018.

Assessing the security risks of multicloud SaaS Applications: A Real-world case study. Akinrolabu, O., New, S. and Martin, A. In Proceedings of the 6th IEEE International Conference on Cyber Security and Cloud Computing

(CSCloud 2019), 2019.
Cyber risk assessment in cloud provider environments: Current models and future needs. Akinrolabu, O., Nurse, J., Martin, A., New, S. Computers & Security Journal, Volume 87, pp. 1-18, 2019.
CSCCRA: A Novel Quantitative Risk Assessment Model for Cloud Service Providers. Akinrolabu, O., New, S., Martin, A. Computers Journal, Volume 8, Issue 3, pp. 1-17, 2019.
Mini-Project: Can improved transparency reduce supply chain risks in cloud computing?
Mini-Project: Towards optimising the detection of sophisticated attacks in Security Operation Centres (SOCs).

BUSHRA ALAHMADI

Supervisor: Ivan Martinovic,
Department of Computer Science

Malware Detection in Security Operation Centres

Malware has evolved from viruses attacking single victims to more sophisticated malware with disruptive purposes. For example, WannaCry ransomware attacks led to hundreds of disruption to NHS care in 2017. Although organizations might have invested in security technologies, their susceptibility to WannaCry hints that the problem goes beyond technology. Security Operations Centres (SOCs) are the first-line of defence in an organisation, providing 24/7 monitoring, detection, and response to security attacks. This thesis aims to explore the challenges in malware detection in Security Operation Centres (SOCs) providing recommendations for possible technological solutions.

We first start by investigating the workflow SOC practitioners follow. Through semi-structured interviews, we recognise the analysts' role in the SOC and their interactions with the technological solutions for malware monitoring, detection, investigation and response. Our results highlight the overwhelming reliance on analysts throughout the SOC operations, which might benefit from automation. We elicit the analysts analytical thinking when making decisions, identifying the influential factors that might impact their decision making.

Moreover, we investigate security practitioners' perspectives of the security monitoring tools deployed in SOCs and their perception of the high false-positive rates. By identifying the weaknesses and strengths in current SOC tools and challenges in deploying network-monitoring tools, we derive recommendations for future SOC tools development.

Understanding the type of malware is an essential step in determining the best response. Sometimes getting access to the infected host is not possible and analysts refer to the network traffic for analysis. Hence, we propose a system that classifies network flow sequences to a malware family. The proposed system is privacy-preserving and effective in classifying a binary to a malware family based on its network traffic, not requiring access to the malware binary itself.

Behavioural malware detection approaches are found to be the most reliable by analysts. We propose a behaviour-based malware detection system that improves over state-of-the-art by detecting new or unseen malware. The system uses behavioural high-level network features preserving the privacy of the monitored hosts. Using this system, malware's network activities are captured and modelled as a Markov Chain. Due to the modeling of general bot network behavior by the Markov Chains, the system can detect new malware that has not been seen before making it robust against malware evolution.

The novelty of this research is to provide a systematic study on SOCs processes, people, and technology; providing researchers with an understanding of the challenges and opportunities within; bridging that knowledge gap and thereby setting a better foundation for future research in the field.

Bio

I have completed my PhD at the Centre for Doctoral Training in Cyber Security, University of Oxford, under the supervision of Professor Ivan Martinovic on Malware Detection in Security Operation Centres (SOCs). Before starting my PhD, I received an MSc degree with distinction in Computer Science and Engineering with a concentration on Network and Information Assurance from Santa Clara University, USA. My research on malware and SOCs has led me to develop an understanding of future research directions of ML/AI in SOCs. I am also investigating the application of Software Defined Networking (SDN) for the active monitoring and detection of malware. I received the Computer Antivirus Research Organisation (CARO) award and Google Anita Borg scholarship in 2016 and Anne McLaren Award of Excellence from Kellogg College in 2017. I was also the president of Oxford Women in Computer Science Society (OxWoCS) and founder of inspireHer - an initiative to encourage girls to code. I also organised workshops at the Annual Hay Festival in the United Kingdom to teach children to code using robotics. I frequently engage with industry through public speaking, recently giving a webinar on Explainability in AI for Google (2020), and a talk at Google Cloud Next 2019 on using ML to detect malicious activities. I am currently an Assistant professor at King Saud University in Saudi Arabia, working part-time as a cybersecurity consultant.

Publications

AlAhmadi, B.A. and Martinovic, I., 2018, May. MalClassifier: Malware family classification using network flow sequence behaviour. In 2018 APWG Symposium on Electronic Crime Research (eCrime) (pp. 1-13). IEEE.
Alahmadi, B.A., Mariconti, E., Spolaor, R., Stringhini, G. and Martinovic, I., BOTection: Bot Detection by Building Markov Chain Models of Bots Network Behavior, AsiaCCS'20
Axon, L. Alahmadi B.A., Nurse J.RC , Goldsmith M., Creese S, Sonification in security operations centres: what do security practitioners think? (Workshop on Usable Security (USEC) at the Network and Distributed System Security (NDSS) Symposium 2018)---Best Paper Award
Axon, L. Alahmadi B.A., Nurse J.RC , Goldsmith M., Creese S, Data Presentation in Security Operations Centres: Exploring the Potential for Sonification to Enhance Existing Practice, Journal of Cybersecurity 2020
Alahmadi, B.A., Legg P.A, Nurse J.RC , Using Internet Activity Profiling for Insider-threat Detection. 12th Special Session on Security in Information Systems - WOSIS 2015

EMAN ALASHWALI

Supervisor: Andrew Martin,
Department of Computer Science

Negotiation Transparency and Consistency in Configurable Protocols: An Empirical Investigation

Configurability (also known as agility), is a protocol design framework that allows protocols to support multiple values for parameters such as the protocol version and ciphersuite. At the beginning of a new protocol session, both communicating parties, e.g. client and server, negotiate these parameters to reach a mutual agreement on optimal values for these parameters, which will be used for the rest of the session. The parameters negotiation phase is critical as it defines the security guarantees that the protocol can provide in a particular session. Hence, it has been an attractive target for downgrade attacks. While the literature has looked at the authenticity and integrity of parameters negotiation in configurable protocols to prevent downgrade attacks under the man-in-the-middle attacker model, negotiation transparency and consistency under other attacker models have been largely overlooked.

Are there unexplored attacker models that can result in a downgrade? Can a semi-trusted server discriminate against its clients without being detected? Can two clients' requests to the same server receive inconsistent security guarantees? Can we achieve a better balance between security and backward compatibility?

In this thesis we aim to answer these unexplored interrelated questions, with a focus on the TLS protocol as one of the most important and widely used configurable protocols. To this end, we first introduce a taxonomy of downgrade attacks in the TLS protocol and application protocols using TLS. Second, we define three types of negotiation models based on a new notion we introduce, which we call the "negotiation power". Third, we introduce a novel attacker model which we call the "discriminatory" model. Fourth, through a measurement-based case study on the Forward Secrecy property and the TLS protocol, we find that there are indeed servers that select non-Forward Secrecy, nevertheless they support it, proving that, in the same vein, discrimination downgrade attacks can go unnoticed. Fifth, through two measurement-based case studies in TLS and HTTPS, we quantify inconsistencies in HTTPS and TLS responses to requests that differ in subtle variables that are not expected to affect the received security guarantees. Namely, we quantify inconsistent servers' responses to requests with versus without the "www." prefix, and to requests from different geographic locations. Finally, we examine the concept of "prior knowledge" to reduce the downgrade attacks' surface.

The results of this thesis introduce transparency and consistency as needed properties in configurable protocols, and show that they are not perfectly achieved in widely used protocols today such as TLS and HTTPS.

Bio

Eman holds MSc. in Information Security from University College London (UCL), UK, and BSc. in Computer Science from King Abdulaziz University (KAU), Saudi Arabia. She works as a Lecturer at KAU. Her research interests are in the theory and practice of network security protocols. In her spare time, Eman enjoys reading, drawing, and photography.

Publications:

Alashwali, E. S., Szalachowski, P. & Martin, A. (2020), Exploring HTTPS Security Inconsistencies: A Cross-Regional Perspective, Computers & Security, 97(101975).

Alashwali, E. S., Szalachowski, P. & Martin, A. (2019b), Towards Forward Secure Internet Traffic, in Proceedings of Security and Privacy in Communication Networks (SecureComm), pp. 341–364.

Alashwali, E. S., Szalachowski, P. & Martin, A. (2019a), Does "www." Mean Better Transport Layer Security?, in Proceedings of Conference on Availability, Reliability and Security (ARES), pp. 23:1–23:7.

Alashwali, E. S. & Rasmussen, K. (2018b), What's in a Downgrade? A Taxonomy of Downgrade Attacks in the TLS Protocol and Application Protocols Using TLS, in Proceedings of Security and Privacy in Communication Networks (SecureComm), pp. 468–487.

Alashwali, E. S. & Rasmussen, K. (2018a), On the Feasibility of Fine-Grained TLS Security Configurations in Web Browsers Based on the Requested Domain Name, in Proceedings of Security and Privacy in Communication Networks (SecureComm), pp. 213–228.

Alashwali, E. S. & Szalachowski, P. (2018), DSTC: DNS-based Strict TLS Configurations, in Proceedings of Risks and Security of Internet and Systems (CRiSIS), pp. 93–109.

RICHARD BAKER

Supervisor: Ivan Martinovic,
Department of Computer Science

Exploiting the Physical in Cyber-Physical Systems

This thesis argues that cyber-physical systems are, by their very nature, at risk from physical-layer attacks as well as cyber attacks. The proliferation of cheap and easy-to-use sensing and actuation technologies has drastically lowered the bar for attackers to conduct physical-layer attacks, even with only limited resources. As our reliance upon cyber-physical systems grows, so too does the impact of attacks.

It is argued that the same easy accessibility of technology that equips attackers, also enables the use of physical-layer security techniques in developing defences. A series of work is presented, exploring the practical use of physical phenomena to secure real-world cyber-physical systems.

Timing constraints are used for the verification of aircraft location claims, to inhibit spoofing. This demonstrates a straightforward application of physical-layer techniques, enhanced with mobility, to drastically limit an attacker's capabilities.

Wireless propagation measurements are used to determine the presence of a drone and track it during a privacy-invasion attack; where traffic itself does not provide sufficient insight. The successful results highlight the potential for using even simple, ubiquitous metrics to gain detailed insight into the physical world.

Leaked electromagnetic signals are then used to detect a class of malicious network; exploiting the wireless propagation mode to achieve better performance and more convenient deployment characteristics than are possible with the original signal. This demonstrates the scope for incorporating unconventional physical effects to improve a security design.

The combined results are drawn on to argue that the use of physical-layer features is practical in real systems, even those that were not originally designed with due consideration for their tacit physical dependencies.

An eavesdropping attack is also presented against a state-of-the-art electric-vehicle charging system. This attack builds upon the electromagnetic leakage used defensively earlier, which is exacerbated by design choices made in the charging system. The eavesdropping attack is shown to be widely effective against real deployments, with results that suggest various active attacks would also be effective.

Observations from the attack are used to argue that as well as being practical, it is also necessary to incorporate physical-layer features in security design, as even emerging modern systems with detailed security models are vulnerable to critical physical-layer attacks.

Bio

Richard is a lifelong computer scientist, having first broken the family computer aged four – long before his MEng at Imperial College London. Since then he has held various technical jobs within finance, insurance and public health; both in the UK and abroad. His broad technical interests include the use of side-channels both for attackers and defenders, the latter where there are sorely underused, the incorporation of physical properties into security and monitoring systems, the economisation of cybercrime, qualifying the impact of security risks and where security common-sense comes from, if anywhere. He is a member of the Systems Security Lab, with a software-defined radio speciality. He is also a proud member of Oxford's 0x002147 CTF team and a founding member of the Competitive Computer Security Society.

Conferences

Baker, R. and Martinovic, I., 2019. Losing the Car Keys: Wireless PHY-Layer Insecurity in EV Charging. To appear USENIX Security 2019.

Baker, R. and Martinovic, I., 2018. EMPower : Detecting Malicious Power Line Networks from EM Emissions. IFIP-Sec 2018.

Birnbach, S., Baker, R. and Martinovic, I., 2017. Wi-Fly?: Detecting Privacy Invasion Attacks by Consumer Drones. NDSS 2017.

Workshops

Baker, R. and Martinovic, I., 2016, October. Secure Location Verification with a Mobile Receiver. In Proceedings of the 2nd ACM Workshop on Cyber-Physical Systems Security and Privacy (pp. 35-46). ACM.

Outreach

Baker, R. 2018, April. UAV-ing a laugh?!. Oxford CompSoc Talk.

Baker, R. 2016, May. The Drones Club: Consumer UAVs, their (ab)uses and some countermeasures. 'Research Uncovered' Talk.

MARY BISPHAM

Supervisors: Michael Goldsmith and Ioannis Agrafiotis
Department of Computer Science

The Security of Human-Computer Interaction by Speech

This thesis investigates the security issues associated with human-computer interaction by speech, focussing on the context of voice-controlled digital assistants. The security of human-computer interaction by speech has become increasingly important as use of voice control has become more widespread. The research questions addressed in the thesis are whether the speech interface presents particular vulnerabilities that are not relevant to other types of interfaces, and, if so, what these vulnerabilities are and how attacks exploiting them can be defended. Based on a critical review of prior work, it is argued that the speech interface does represent a new attack surface with specific security vulnerabilities that have not as yet been comprehensively studied. These vulnerabilities arise both in relation to the inherently open nature of the speech interface, as well in relation to unintended functionality in the technologies implemented in voice-controlled systems to imitate human speech and language processing.

The thesis makes three main contributions towards closing the gaps in knowledge on the security of human-computer interaction by speech identified in the review of prior work. The first contribution of the thesis is a novel taxonomy of the types of attacks that might be executed via a speech interface, representing a systemisation of knowledge in this area. The second contribution of the thesis is experimental work demonstrating new types of attacks via the speech interface that are foreshadowed in prior work, but have not been validated in practice. The experimental work develops systematic methodologies for executing attacks that hide malicious voice commands in nonsensical word sounds and in apparently unrelated utterances. The methodologies applied in these experiments involve testing both machine and human responses to such input to assess the potential for exploiting differences in machine and human perceptions to execute covert attacks. The third contribution of the thesis is proposals for the development of new defence mechanisms to counter attacks via the speech interface for which no effective defence mechanisms are currently available. These proposals include feasibility tests on the application of two existing technologies for security purposes in voice-controlled systems. The proposals for new defence mechanisms are grounded in a novel attack

and defence modelling approach for analysing the security of human-computer interaction by speech that enables conceptualisation of the security of the speech interface in an inclusive framework, and facilitates a review of currently available defence mechanisms.

Bio

Mary holds a first degree in Latin, and also holds several Master degrees, including an MA in Copyright Law and an MSc in Bioinformatics. Prior to joining the CDT Mary worked for some years in intellectual property administration. .

Publications:

A taxonomy of attacks via the speech interface Mary K Bispham, Ioannis Agrafiotis and Michael Goldsmith. In Proceedings of CYBER 2018 : The Third International Conference on Cyber–Technologies and Cyber–Systems. ThinkMind Digital Library for the Third International Conference on Cyber–Technologies and Cyber–Systems (CYBER 2018). 2018.

Nonsense Attacks on Google Assistant and Missense Attacks on Amazon Alexa Mary K Bispham, Ioannis Agrafiotis and Michael Goldsmith In Proceedings of ICISSP 2019. Pages 75–87. 2019.

Attack and Defence Modelling for Attacks via the Speech Interface Mary K Bispham, Ioannis Agrafiotis and Michael Goldsmith In Proceedings of ICISSP 2019. Pages 519–527. 2019.

Mini-Project: Linguistic Features of Impersonation in Online Discourse

Mini-Project: Security Vulnerabilities in Speech Recognition Systems

ALEXANDER DARER

Supervisors: Andrew Martin, Department of Computer Science and Joss Wright, Oxford Internet Institute

Monitoring Internet Censorship; Linguistic Connectivity within the Webgraph

Monitoring Internet Censorship remains a complex research task. Censors around the world employ sophisticated measures to enforce policies of censorship, and there are often repercussions for those who access sensitive material within an area under a censorship regime. For these reasons, we as researchers must be careful about how we test and measure censorship within certain countries. One cannot ethically monitor for filtered content if it puts another individual or group at risk of harm.

A major area within censorship research is building and maintaining URL filter lists for different countries. Alex's work is building this capability by developing automated methods for discovering and monitoring blocked URLs that don't rely on human interaction or local knowledge of censored regions. An important part of this research is performing measurements on infrastructure rather than using volunteers to determine if certain content is filtered.

Publications:

Alexander Darer, Farnan, Oliver and Joss Wright. "FilteredWeb: A Framework for the Automated Search-Based Discovery of Blocked URLs." Proceedings of the 2017 Network Traffic Measurement and Analysis Conference (TMA). TMA, 2017.

Farnan, Oliver, Alexander Darer, and Joss Wright. "Poisoning the Well: Exploring the Great Firewall's Poisoned DNS Responses." Proceedings of the 2016 ACM on Workshop on Privacy in the Electronic Society. ACM, 2016.

Joss Wright, Alexander Darer and Oliver Farnan. "Filterprints: Identifying Localised Usage Anomalies in Censorship Circumvention Tools."

RICHARD EVERETT

Supervisors: Stephen Roberts and Michael Osborne, Department of Engineering Science

General learning algorithms for multi-agent environments

Richard completed his DPhil with the machine learning research group lead by Stephen Roberts. After graduating from UCL with a Masters degree in Computer Science, he moved to Oxford to start applying machine learning to complex multi-agent problems. His work focuses on using game theory and agent-based modelling to study how agents do, and should, interact in the real-world. In the past, he has applied his research to advertising, finance, and cybersecurity, and has also worked with the airline Emirates.

Publications

A. Cobb, R. Everett, A. Markham, S. Roberts. "Identifying Sources and Sinks in the Presence of Multiple Agents with Gaussian Process Vector Calculus" Proceedings of the 24th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. ACM, 2018.

R. Everett, S. Roberts. "Learning Against Non-Stationary Agents with Opponent Modeling and Deep Reinforcement Learning" AAAI Spring Symposium Series on Learning, Inference, and Control of Multi-Agent Systems, 2018.

R. Everett. "Opponent Modelling of Non-Stationary Agents with Deep Reinforcement Learning" NIPS Workshop on Learning in the Presence of Strategic Behavior, 2017.

D. Hendricks, A. Cobb, R. Everett, S. Roberts. "Inferring Agent Objectives at Different Scales of a Complex Adaptive System" NIPS Workshop on Learning in the Presence of Strategic Behavior, 2017.

R. Everett, J. Nurse, and A. Erola. "The anatomy of online deception: what makes automated text convincing?." Proceedings of the 31st Annual ACM Symposium on Applied Computing. ACM, 2016.

A Distributed Cyber Analytics System for Streaming Anomaly Detection

ILIAS GIECHASKIEL

Supervisor: Kasper Rasmussen
Department of Computer Science

Leaky hardware: modeling and exploiting imperfections in embedded devices

Embedded systems are found in many safety- and security-critical applications, and bring aspects of the physical world to the digital one and vice versa. However, imperfections in this hardware bridge can break the integrity of sensor inputs into an embedded device, causing it to act upon the wrong data. For instance, malicious electromagnetic transmissions can trick systems into inducing defibrillation shocks and raising the temperature of infant incubators, both with potentially severe health consequences.

Unfortunately, such attacks which alter sensor outputs without changing the property being measured itself have so far only been studied in an ad-hoc manner. In my thesis, I address this shortcoming in two ways. First, I create a taxonomy of these "out-of-band" signal injection attacks and defenses. Second, I propose a framework that quantifies security in their context through a system model, mathematical definitions, and an algorithm that can compare the "security level" of off-the-shelf systems.

In my thesis, I also investigate Field-Programmable Gate Arrays (FPGAs), which are available on public cloud infrastructures, and are also integrated in many consumer end-products, such as smartphones and laptops. As FPGAs are often used in sensitive applications, including genome processing, cryptography, and financial modeling, it is necessary to ensure that they can maintain the secrecy of the data that they process.

However, the confidentiality of FPGA data can be broken, as I demonstrate through three new sources of information leakage due to hardware imperfections. The first source exists between "long wires" within seven families of Xilinx FPGAs. I explain how to exploit long-wire leakage for covert- and side-channel attacks, both locally, and on two commercial FPGA clouds through novel ring oscillators structures that bypass currently-deployed countermeasures.

The second source of leakage operates even when different FPGA users are isolated to distinct dies of the same chip. These unintended interactions demonstrate that current FPGA architectures are not well-suited for multi-tenancy, despite the physical isolation of user logic. Finally, I show that assigning dedicated FPGAs to different users is still not enough to prevent cross-FPGA communication: shared Power Supply Units (PSUs) leak information between physically distinct FPGA, CPU, and GPU boards, which can be detected via means of a novel receiver design and classification metric.

Overall, in my thesis, I highlight that the underlying electrical properties of embedded devices often fall short of protecting the integrity and the confidentiality of the data that they process, and allow remote attackers to spoof sensor measurements or infer cryptographic keys and other types of data.

Bio

Ilias submitted and defended his DPhil thesis in 2019. He was a Clarendon and Cyber Security Scholar at Kellogg College, where he was also funded by the EPSRC and the Oxford CDT in Cyber Security. His dissertation, "Leaky Hardware: Modeling and Exploiting Imperfections in Embedded Devices" focused on embedded systems security, primarily as it relates to Analog-to-Digital Converters (ADCs) and Field-Programmable Gate Arrays (FPGAs). During his final DPhil year, Ilias was a Visiting Assistant in Research at Yale University. Prior to that, he studied Mathematics at Princeton University and Advanced Computer Science at the University of Cambridge.

Ilias also co-founded the Competitive Computer Society and was the captain and co-founder of Oxford's security Capture-the-Flag (CTF) team Ox002147, frequently participating in CTF contests individually and with Ox002147. During his undergraduate and graduate studies, Ilias interned in the Data License team at Bloomberg, the Windows Security team at Microsoft, the Product Abuse team at Dropbox, the Embedded Systems team at Microsoft Research, and the Hardware/FPGA team at Jump Trading. He is currently a Hardware Research Engineer at Jump Trading, and continues to do research on FPGA security in his spare time.

Peer-Reviewed Publications

I. Giechaskiel, K. B. Rasmussen, and J. Szefer. "C^{3}APSULe: Cross-FPGA Covert-Channel Attacks through Power Supply Unit Leakage". In 41st IEEE Symposium on Security and Privacy (S&P), 2020. DOI: 10.1109/SP40000.2020.00070.

S. Tian, W. Xiong, I. Giechaskiel, K. B. Rasmussen, and J. Szefer. "Fingerprinting Cloud FPGA Infrastructures". In 28th ACM/SIGDA International Symposium on Field-Programmable Gate Arrays (FPGA), 2020. DOI: 10.1145/3373087.3375322.

I. Giechaskiel and K. B. Rasmussen. "Taxonomy and Challenges of Out-of-Band Signal Injection Attacks and Defenses". IEEE Communications Surveys & Tutorials (COMST), vol. 22, no. 1, pp. 645–670, March 2020. DOI: 10.1109/COMST.2019.2952858.

I. Giechaskiel, K. B. Rasmussen, and J. Szefer. "Reading Between the Dies: Cross-SLR Covert Channels on Multi-Tenant Cloud FPGAs". In 37th IEEE International Conference on Computer Design (ICCD), 2019. DOI: 10.1109/ICCD46524.2019.00010.

I. Giechaskiel, Y. Zhang, and K. B. Rasmussen. "A Framework for Evaluating Security in the Presence of Signal Injection Attacks". In 24th European Symposium on Research in Computer Security (ESORICS), 2019. DOI: 10.1007/978-3-030-29959-0_25. **Best Paper Award**.

I. Giechaskiel, K. B. Rasmussen, and J. Szefer. "Measuring Long Wire Leakage with Ring Oscillators in Cloud FPGAs". In 29th International Conference on Field-Programmable Logic & Applications (FPL), 2019. DOI: 10.1109/FPL.2019.00017.

I. Giechaskiel, K. Eguro, and K. B. Rasmussen. "Leakier Wires: Exploiting FPGA Long Wires for Covert- and Side-Channel Attacks". ACM Transactions on Reconfigurable Technology and Systems (TRETS), vol. 12, no. 3, pp. 11:1–11:29, September 2019. DOI: 10.1145/3322483

I. Giechaskiel, K. B. Rasmussen, and K. Eguro. "Leaky Wires: Information Leakage and Covert Communication Between FPGA Long Wires". In

13th ACM Asia Conference on Computer and Communications Security (ASIACCS), 2018. DOI: 10.1145/3196494.3196518.

I. Giechaskiel, C. Cremers, and K. B. Rasmussen. "When the "Crypto" in Cryptocurrencies

Breaks: Bitcoin Security Under Broken Primitives". IEEE Security & Privacy, vol. 16, no. 4, pp. 46–56, July/August 2018. DOI: 10.1109/MSP.2018.3111253.

I. Giechaskiel, C. Cremers, and K. B. Rasmussen. "On Bitcoin Security in the Presence of Broken Cryptographic Primitives". In 21st European Symposium on Research in Computer

Security (ESORICS), 2016. DOI: 10.1007/978-3-319-45741-3_11.

I. Giechaskiel, G. Panagopoulos, and E. Yoneki. "PDTL: Parallel and Distributed Triangle Listing for Massive Graphs". In 44th International Conference on Parallel Processing (ICPP), 2015. DOI: 10.1109/ICPP.2015.46.

DENNIS JACKSON

Supervisor: Andrew Simpson,
Department of Computer Science

Improving Automated Protocol Verification: Real World Cryptography

The design and analysis of new cryptographic protocols is a challenging endeavour. It requires considerable expertise, significant manual effort and a long delay between design and an accepted proof of security. However, the use of automated tools to formally verify protocols has matured in recent years. Originally limited to simple protocols, automated tools can now be used to analyse complex real world protocols such as TLS, 5G and Signal. Unlike traditional approaches, these tools can be used by non-experts, require comparatively little effort and offer results in a matter of days rather than months.

However, the symbolic model used by these tools has been criticised for its abstract model of cryptographic primitives, which has an unclear relationship with real world cryptographic behaviour. Further, there are cryptographic primitives which cannot be represented in the symbolic model. This motivates several natural research questions.
How well do contemporary symbolic models of cryptographic primitives match real world behaviour? Where symbolic models fall short, can we improve them? Can we extend symbolic models to capture more cryptographic primitives? In this thesis, we set out to address these questions for two commonly used cryptographic primitives: digital signatures and Diffie Hellman groups.

We first consider digital signatures. We uncover a startling mismatch between the cryptographic definition and the symbolic model, which we investigate and repair. Consequentially, we discover a number of new attacks on real world protocols. We also document a number of prior verifications which missed these attacks due to their traditional symbolic model of digital signatures.
Next we explore Diffie Hellman groups. Unlike digital signatures, symbolic Diffie Hellman models have evolved considerably over the past two decades and we review this progress. We discuss two key shortcomings. Firstly that these models only describe prime order groups, despite the prevalence of non-prime order groups in practice. We develop new symbolic models to remedy this and show their effectiveness on real world protocols. The second shortcoming is that these models cannot describe protocols which make use of the full field structure of Diffie Hellman exponents. We develop a new system of constraint solving rules, based on previous work, which can be used to analyse this class of protocols.

Finally, we conclude by looking back at the common themes across our work. We argue that automated analysis using symbolic methods is remarkably effective for finding real world attacks and suggest some promising lines of future work.

Bio

I studied Mathematics at the University of Warwick, graduating with a Masters in 2015. I then joined the Cybersecurity CDT at Oxford and started my DPhil studies with Prof Cas Cremers of the Information Security Group. My research focused on the formal verification of security protocols and models of cryptographic primitives.

After my DPhil thesis was accepted in February 2020, I joined the Information Security Group at ETH Zurich as a PostDoc, led by Prof David Basin. As well as carrying on my research in formal verification, I took part in the design and analysis of the DP3T Contact Tracing protocol, now adopted by Google, Apple and in widespread deployment. I also joined the Tor Project as a Core Contributor, helping to improve performance and network health.

Internships

Privacy, Networking & Security Research Internship with Mozilla. Mountain View, Summer 2019.

Publications

A Spectral Analysis of Noise: A Comprehensive, Automated, Formal Analysis of Diffie-Hellman Protocols. Guillaume Girol, Lucca Hirschi, Ralf Sasse, Dennis Jackson, Cas Cremers, David Basin. At USENIX Security Symposium 2020 (USENIX Security 20)

Seems Legit: Automated Analysis of Subtle Attacks on Protocols that use Signatures. Dennis Jackson, Katriel Cohn-Gordon, Cas Cremers, Ralf Sasse. At ACM Conference on Computer and Communications Security 2019 (CCS 2019)

Prime, Order Please! Revisiting Small Subgroup and Invalid Curve Attacks on Protocols using Diffie-Hellman. Cas Cremers, Dennis Jackson. Distinguished Paper at IEEE Computer Security Foundations Symposium 2019 (CSF 2019)

Eprints:

The Provable Security of Ed25519: Theory and Practice. Jacqueline Brendel, Cas Cremers, Dennis Jackson, Mang Zhao. IACR Eprint 2020/823

Decentralized Privacy-Preserving Proximity Tracing (DP3T). Carmela Troncoso, Mathias Payer, Jean-Pierre Hubaux, Marcel Salathé, James Larus, Edouard Bugnion, Wouter Lueks, Theresa Stadler, Apostolos Pyrgelis, Daniele Antonioli, Ludovic Barman, Sylvain Chatel, Kenneth Paterson, Srdjan Čapkun, David Basin, Jan Beutel, Dennis Jackson, Marc Roeschlin, Patrick Leu, Bart Preneel, Nigel Smart, Aysajan Abidin, Seda Gürses, Michael Veale, Cas Cremers, Michael Backes, Nils Ole Tippenhauer, Reuben Binns, Ciro Cattuto, Alain Barrat, Dario Fiore, Manuel Barbosa, Rui Oliveira, José Pereira. ArXiv:2005.12273

MARIAM NOUH

Supervisors: Michael Goldsmith,
Sadie Creese and Jason Nurse
Department of Computer Science

On Combating Online Radicalisation: A Framework for Cybercrime Investigations

The complexity of cybercrimes is constantly increasing with advanced tools, attack vectors, and Modus Operandi adopted by offenders every day. Criminals have easy access to advanced technical abilities that they need to carry their attacks, using what is called crime-as-a-service, from the dark web and online black markets. Similarly, the nature of cybercrimes has generated multitudes of data introduced by the "cyber" aspect of these crimes, which makes the process of identifying evidence similar to searching for a needle in a haystack. To aid law enforcement to better detect, analyse, and understand the threat landscape posed by cyber-criminals, research into the area of cybercrime intelligence has flourished. Law enforcement faces numerous challenges when policing cybercrimes. The methods and processes they use when dealing with traditional crimes do not necessarily apply in the cyber world. Additionally, criminals are usually technologically aware and one step ahead of the police. Furthermore, current tools created to support law enforcement to better police cybercrimes more often conflict with how they are used to operate, and are too complex, thus making them difficult to adopt. In this thesis, we aim to design and develop a cybercrime intelligence framework for law enforcement that provides decision support to detect and analyse the behaviour of cyber-criminals. To do so, we need to better understand the cybercriminal ecosystem, as well as understand the current capabilities of law enforcement agencies, and the challenges they face when policing cybercrimes. We achieve this through semi-structured interviews conducted with professionals and law enforcement agents investigating cybercrimes. From there, we define a framework to aid them in addressing some of the challenges they face. Moreover, the cybercrime landscape varies considerably in regard to the type of crime and what they target. Some crimes target computers and systems while others target the human. As there has been considerable research focusing on analysing cybercrimes that target
systems such as (Malware, Hacking, DDOS), the focus on the crimes that target the human (e.g., cyber-bullying, online radicalisation) has recently become more evident. In this research, we focus on the area of online radicalisation and utilize our framework to better understand the properties of the radical propaganda and develop methods to defend against its spread. We focus on the ISIS group aiming to identify measures to automatically detect radical content and activities in social
media. We identify several signals, including textual, psychological and behavioural, that together allow for the identification of radical messages, using methods such as natural language processing, social network analysis, and machine learning. Our findings can be utilised as signals for detecting online radicalisation activities by law enforcement and social media platforms to help keep the online world safer.

Bio

Mariam received her MSc. degree in Information Systems Security from Concordia University, Canada, where she researched methods for automatic integration of security concepts into software design models. She holds BSc. degree in Information Technology from King Saud University, Saudi Arabia. She has completed her DPhil in Cyber Security as part of the Computer Science department focusing on developing a framework for cybercrime investigations and designing methods to combat online radicalization.

Before joining Oxford, Mariam worked as a security analyst in the banking sector conducting security compliance reviews, risk assessment, and penetration testing. She then developed interest in research and joined King Abdulaziz City for Science and Technology, the national research labs of Saudi Arabia, as a research associate working on multiple research projects in collaboration with MIT University.

Mariam's research interest spans multiple areas including cybercrimes, social network analysis, natural language processing, and machine learning. During her time at Oxford, she has been an active member of the Oxford Women in Computer Science Society (OxWoCS) aiming to promote and support women in STEM. In her down time, Mariam enjoys participating in CTF competitions, playing squash, and doing street photography.

Academic Publications and Posters

M. Nouh and J. R. C. Nurse, "Identifying Key-Players in Online Activist Groups on the Facebook Social Network," 2015 IEEE International Conference on Data Mining Workshop (ICDMW), Atlantic City, NJ, 2015, pp. 969-978. doi: 10.1109/ICDMW.2015.88

M. Nouh, J. R. C. Nurse and M. Goldsmith, "Towards Designing a Multipurpose Cybercrime Intelligence Framework," 2016 European Intelligence and Security Informatics Conference (EISIC), Uppsala, 2016, pp. 60-67. doi: 10.1109/EISIC.2016.018

M. Nouh, J. R. C. Nurse and M. Goldsmith. "POSTER: Detection of Online Radical Content Using Multimodal Approach", 2017 IEEE European Symposium on Security and Privacy (EuroSP2017), Paris, 2017.

M. Nouh, J. R. C. Nurse and M. Goldsmith, "CCINT: The Cyber-Crime INTelligence Framework for Detecting Online Radical Content, Grace Hopper Celebration Conference (GHC), Orlando, USA. October 2017. (3rd prize award, ACM Student Research Competition)

M. Nouh, J. R. C. Nurse and M. Goldsmith, Applying Machine Learning to Detect Evidence of Online Radical Behavior. Artificial Intelligence at Oxford conference (AI @Oxford), 2018. (Poster)

M. Nouh, J. R. C. Nurse, and M. Goldsmith. Understanding the Radical Mind: Identifying Signals to Detect Extremist Content on Twitter. IEEE International Conference on Intelligence and Security Informatics (ISI), July 2019

M. Nouh, J. R. C. Nurse, Helena Webb, and M. Goldsmith, Cybercrime Investigators are Users Too! Understanding the Socio-Technical Challenges Faced by Law Enforcement. Workshop on Usable Security and Privacy (USEC) Internet Society, San Diego, California, Feb 24, 2019. ISBN 1-891562-57-6 https://dx.doi.org/10.14722/usec.2019.23032

Invited Talks

Identifying influential users in activist groups on Facebook. Social Networking in cyberspace (SNIC) conference, 2015.

Understanding the Radical Mind Using Linguistic and Psychological properties. Behavioral and Social Sciences in Security (BASS), 2018

Identifying Signals to Detect Radicalism on Twitter. Vox-Pol Conference on Violent Extremism, Terrorism, and the Internet: Present and Future Trends, 2018.

Understanding Cybercrime for Better Policing: Regional and Global Challenges, at Chatham House The Royal Institute for International Affairs, London, UK, 2019

Panel discussion on Cyber Security and Emerging Online threats, Manchester, UK, 2019

KRISTOPHER WILSON

Supervisor: Rebecca Williams, Faculty of Law

What's Wrong with the CMA? Computer Misuse and the Criminal Law

The introduction of any new criminal law is accompanied by a series of justifications. The CMA was justified by the Law Commission based on five considerations: fair labelling and deterrence; that it would serve a supplementary role to existing offences by criminalising conduct on their periphery; that the ultimate harm of malicious uses of computers was the access to, and impairment of, computer operations and this fell outside the experience of the criminal law; that 'hacking' served a criminogenic function; and that other jurisdictions had enacted similar provisions.

Since the introduction of the CMA, the operation of computing and network technologies has continued to evolve. As such, this thesis aims systematically to revisit the justifications set out to support the creation of the computer specific offences contained in the Act. It will argue that these justifications no longer support the CMA, if indeed they ever did so. The evolution of computing technology, well beyond that contemplated by lawmakers at the time, means the problems computers presented to the criminal law are better served by reconsidering the structure and operation of general offences, rather than creating new specific offences. The notion of 'computer crime' as being a subject for the substantive criminal law has, in most cases, turned out to be illusory.

Bio

Kris currently works as a Lecturer in the Faculty of Law at the University of Technology Sydney, teaching a number of core and elective subjects and researching the criminalisation of data access and the protection of Indigenous Knowledges in a digital context. Prior to completing his DPhil in the CDT, he graduated with a Bachelor of Laws (Honours) at Flinders University in Adelaide, South Australia, before undertaking a Master of Laws at the University of New South Wales in Sydney, specialising in Media and Technology Law. He has also worked at the University of Reading, teaching LLM modules on Internet Law, Data Protection and Privacy Law, and Intellectual Property Law.

Publications

Kristopher Wilson, 'As Brexit dominates news, Investigatory Powers Bill sneaks in under the radar', The Conversation, 1 July 2016 https://theconversation.com/as-brexit-dominates-news-investigatory-powers-bill-sneaks-in-under-the-radar-61780.

Kristopher Wilson, 'The Computer Misuse Act 1990 (UK) and Responding to the Evolving Cybercrime Threat Landscape', CDT Working Paper 2015.

Kristopher Wilson, 'Virtual Private Networks and 'Geo-Blocked' Works: Service Users as Unwitting Cyber Criminals', CDT Working Paper 2015.

Kristopher Wilson, 'Future Proof Your Legal Career: The Future of Legal Practice' at South Australian Legal Services Commission Conference 29 June 2018

Kristopher Wilson and Ellen van Neervan, 'Data Nullius' in Allison Whittaker (ed) Blak Letter Law (Forthcoming)

Kristopher Wilson, 'Article 7(2) of the 1995 UNIDROIT Convention' in Ana Vrdoljak et al. Oxford Commentaries on International Heritage Law (Oxford University Press) (Forthcoming)

Kristopher Wilson, 'Computer-Related Crime' in David Caruso et al South Australian Criminal Law and Procedure (3rd edition, Lexis Nexis) (Forthcoming)

Approaching Data Protection by Design in Connected Communal Spaces

A Case for Contextualised Participatory Design

Martin Kraemer, CDT16

There is a gap between person-centred data protection legislation and practices, and communal implications of internet-connected technology. Modern communal spaces – such as our homes – typically involve heterogeneous groupings of individuals with dynamic social structures, unattributed responsibilities, and varying levels of skill. Designing systems for use in these spaces requires taking into account communal factors, however data protection for communal spaces is not deeply understood. Studies to disentangle this complex problem space lie at the heart of my doctoral work. In this short article, I make the case for *Contextualised Participatory Design* which appears promising in accounting for heterogeneous social groups and their dynamics, complementing individual perspectives on data protection.

Introduction

Over the past 30 years, internet-connected technology has fundamentally changed the way we conduct our lives. Where, why, and how people make use of the internet has had long lasting impact: internet cafes emerged and disappeared; people started working from home and other places; and the newest wave of internet-connected smart home devices brings increasingly sophisticated and unobtrusive technology to our homes. Today, we use internet-connected technology ubiquitously: we are connected anywhere and everywhere we go, often without realising it. The resulting context collapses have been discussed at great length in the literature: portability of devices and ad hoc sharing of information between locations means that traditional physical, social, and institutional boundaries are blurred as people carry devices to different spaces.

Data Protection by Design is increasingly recognised by law- and policy makers.

Concerns of data protection are almost omnipresent in studies of internet-connected technology use, and legislators have taken on the challenge of regulating the collection and use of data. The focus of our work lies within the EU, whose General Data Protection Regulation (GDPR) is said to have had impact on technology globally [16]. The EU adapted existing privacy-by-design guidelines as data protection principles to codify rules for data collection and processing [4]. The GDPR requires

that these principles are to be followed from the outset, by design and by default. They detail rules for data processing and use, and they highlight the importance of appropriate security measures.

The spirit of the GDPR is to protect individuals' right to privacy and, by implication, society as a whole ; however, it is unclear how its rather abstract data protection principles can be observed for the broad variety of connected communal spaces such as cafes or smart homes. For example, different skills, interests, and preferences in using internet-connected technology can cause friction; a security camera might capture several people at the same time, while only one of them set up and explicitly consented to its use.

Research on privacy beyond the individual in communal spaces is nascent.

In the academic literature, issues of data protection have been researched in context of informational or data privacy. Because privacy is "inherently socio-technical and situated", we need to use methods that "explore people and situations" in spaces "where the 'right' definition of privacy might not be known at the outset" [24]. Existing privacy theories highlight the importance of context for privacy and its interactional and interpersonal character [1,11,21]. Most empirical work assumes perspectives of individuals or of specific user groups [25,26], while few contributions have explicitly considered aspects of connected and communal privacy [2,23]. However,

to apply data protection by design successfully to connected communal spaces a better understanding of how individuals and communities manage their privacy, both individually and as a diverse group, is required.

The literature on informational privacy reveals several different notions of privacy beyond the individual. Each being different in scope, they demonstrate the complexities of the problem space, emphasising the entanglement of privacy with social and cultural considerations. Between them, these contributions consider common goals, shared data (or shared inferred information), shared access to devices and accounts, a shared sense of community across online and offline spheres, physical proximity with other people, and feelings of responsibility for others.

However, the *use of technology in shared communal spaces* such as our homes has altered the way we conduct our lives. In these socially, physically, and temporally diverse settings, technology use is embedded in interpersonal relationships, follows perceived norms, roles, and hierarchies, and is continuously negotiated [6,8,9]. In the home, networks and devices are often shared between household members and used collectively. In contrast to 'third spaces', members of the household expect to share access to and distribute responsibilities for networks and devices, considering personal characteristics (attitude, aptitude, competence, and skill) when navigating individual and shared use of devices [5,10,14].

It is unclear how to comply by design with requirements of laws and regulations.

Data protection by design has mostly been approached by emerging practice and research in privacy engineering. The field has a strong policy and engineering focus, aiming to translate regulatory guidelines and requirements into engineering practice [13,54]. For example, [22] identified three different approaches including architecture, policy, and interaction; [7] proposed design strategies; and [15] linked engineering best practices with privacy impact assessment and privacy enhancing technologies to make privacy-by-design goals verifiable and measurable. These approaches have been criticised for their 'check-list' character [12], and chosen design perspectives were said to be narrow in their understanding of privacy as individual control over data [24].

Within the domain of informational privacy research, [24] argued for the application of design orientations such as Value Sensitive (e.g. [17]) and Participatory Design (e.g [18]). Communal aspects in particular have been considered by participatory design (PD) approaches (e.g. in workplace, in design environment, or in workshops) [19]. [26] employed participatory design to explore privacy perceptions and designs of smart home owners [25] and bystanders [26]. They suggest shifting the focus toward cooperative mechanisms and bystander-centric mechanisms to equally consider both perspectives by design, and they highlight the importance of considering privacy seeking behaviours, varying expectations, and contextual variations in understanding and contrasting privacy perceptions [26]. This illustrates how these orientations help to explore situations in which a clear definition of privacy might not be known from the outset.

To summarise, approaching data protection by design and by default in connected communal spaces needs to take into consideration: (1) the important impact of the use of connected technology in shared and communal spaces beyond the individual; (2) the complex and interrelated nature of data protection in such spaces, in that individual perspectives overlap with each other and a group perspective emerges; (3) context when designing for data protection in the form of social and cultural facets but also physical features of the environment in which a technology is used; and (4) shortcomings of existing approaches, in that methods from the related field of privacy engineering are not fit for this purpose.

A case for Contextualised Participatory Design

We propose contextual participatory design (PD) to address these challenges. Our proposal follows calls from previous contributions bridging the gap between privacy and design [20,24] and the successful application of participatory design (PD) working with specific user groups [25,26] and communities [3]. Known as the "third space in HCI" [19], PD reinforces the role of end users as stakeholders in the design process and can be instrumental in understanding their values and expertise [19,24]. Thereby, PD invites interpretation by users and focuses more on collectivism than individualism, with a heterogeneity of perspectives becoming the norm [19].

PD allows the interpersonal character of data protection in shared spaces to take centre stage in investigations, allowing participant designers to more fully exploring its contextual nature. Exploring data protection "through the eyes of stakeholders" [24] in this way allows us to investigate how stakeholders make sense of data protection in connected and shared spaces. A PD approach, then, appears promising for three reasons: (1) the lack of a clear approach definition of data

protection in shared connected spaces; (2) PD allows the interpersonal character of data protection in shared spaces to take centre stage; and (3), thereby, PD is well suited to explore its contextuality.

A popular PD approach in the literature is the Future Workshop format. Stakeholders join researchers in *critiquing* the present, *envisioning* the future, and *implementing*—moving from the present to the future [19]. We suggest to adapt this format as follows:

Critiquing the present – introduce the problem space in three steps: (1) task participants to explore shared spaces as context for the design exercise, i.e. the home and a coffee shop; (2) introduce participants to design challenges of data protection that are familiar to them and useful in discussing data protection goals, e.g. retaining control over data; and (3) provide guiding questions to jointly reflect on what data protection could mean in such spaces.

Envisioning the future – posit a relatable design challenge, e.g. focused on a common activity so that the design activity can be facilitated through shared experiences. Assist with sketching and clarify technical questions where required, but leave it to the group to fill the design space given to them. Conclude the session with a presentation and short discussion of the design solution.

Implementing – help participants with drawing more specific sketches of contextual use and mockups of the devices and interfaces so as to fully capture their ideas and understanding. If desired, prototype some of their ideas later and involve some of the initial participants in user testing.

This approach is well suited to approach data protection by design and by default in connected communal spaces for three main reasons: (1) it shifts focus to improving a familiar task/problem in (2) considering a familiar environment (e.g. home or a cafe) while (3) exploring a somewhat familiar design space (data protection). Based on our initial applications of this approach, the use of existing design techniques and artefacts appears promising in introducing stakeholders to a problem space without requiring them to be "conversationally familiar" from the outset. We believe a structured contextual exploration can benefits explorations of privacy: Firstly, in a multi-cultural society such as ours, a contextual exploration of data protection can foreground socio-cultural aspects; and secondly, the approach allows our participants to become familiar with each others' lived experiences.

Contributing towards reusable and relatable insights

Ultimately, we hope the described approach can help with much needed innovation towards achieving data protection by design internet-connected technologies. The design session becomes a melting pot for the needs and desires of privacy researchers, information technology experts, user experience designers, and user groups. What might result from these sessions – and our initial efforts would encourage everyone to pursue this stream of research – is the development of a common vocabulary. This vocabulary and insights on its usefulness are much needed to advance existing design techniques and artefacts so as to account for contextual aspects that matter to users and enable designers to more holistically consider data protection in communal spaces by design.

Acknowledgements

Ideas for large parts of this article stem from long discussions and joint research efforts with my supervisor Ivan Flechais and my fellow DPhil students Norbert Nthala, Paula Fiddi, and William Seymour.

References

1. I Altman. 1975. The environment and social behavior: privacy, personal space, territory, crowding. Brooks/Cole Pub. Co., Monterey, Calif. Retrieved from https://books.google.co.uk/books?id=GLBPAAAAMAAJ

2. Alison Burrows, David Coyle, and Rachael Gooberman-Hill. 2018. Privacy, boundaries and smart homes for health: An ethnographic study. Health & Place 50, May 2017: 112–118. https://doi.org/10.1016/j.healthplace.2018.01.006

3. Chhaya Chouhan, Christy M. LaPerriere, Zaina Aljallad, Jess Kropczynski, Heather Lipford, and Pamela J. Wisniewski. 2019. Co-designing for community oversight: Helping people make privacy and security decisions together. Proc. ACM Hum.-Comput. Interact. 3, CSCW. https://doi.org/10.1145/3359248

4. Council of the European Union. 2016. General Data Protection Regulation. OJ L 119. Retrieved from http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf

5. Andy Crabtree, Richard Mortier, Tom Rodden, and Peter Tolmie. 2012. Unremarkable networking: the home network as a part of everyday life. Proceedings of the Designing Interactive Systems Conference. ACM.: 554–563. https://doi.org/10.1145/2317956.2318039

6. Andy Crabtree, Peter Tolmie, and Will Knight. 2017. Repacking 'Privacy' for a Networked World. Computer Supported Cooperative Work: CSCW: An International Journal 26, 4-6: 453–488. https://doi.org/10.1007/s10606-017-9276-y

7. George Danezis, Josep Domingo-Ferrer, Marit Hansen, Jaap-Henk Hoepman, Daniel Le Metayer, Rodica Tirtea, and Stefan Schiffner. 2015. Privacy and data protection by design - from policy to engineering.

8. Paul Dourish and Genevieve Bell. 2011. Rethinking privacy. In Divining a digital future: Mess and mythology in ubiquitous computing. The MIT Press, Cambridge, Mass., 137–160. https://doi.org/10.7551/mitpress/9780262015554.003.0069

9. Paul Dourish. 2006. Re-Space-ing Place : " Place " and " Space " Ten Years On. In Proceedings of the 2006 20th anniversary conference on computer supported cooperative work - cscw '06, 299——308.

10. Radhika Garg and Christopher Moreno. 2019. Understanding Motivators , Constraints , and Practices of Sharing Internet of Things. Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies 3, 2: 1–21. https://doi.org/10.1145/3328915

11. Erving Goffman. 1975. The presentation of self in everyday life. Life as theater: 173. https://doi.org/10.2307/258197

12. Seda Gürses and Jose M. Del Alamo. 2016. Privacy Engineering: Shaping an Emerging Field of Research and Practice. IEEE Security and Privacy 14, 2: 40–46. https://doi.org/10.1109/MSP.2016.37

13. Seda Gürses, Carmela Gradiant Troncoso, and Claudia Diaz. 2015. Engineering privacy by design reloaded. Amsterdam Privacy Conference: 1–21. Retrieved from https://iapp.org/resources/article/engineering-privacy-by-design-reloaded/

14. Martin J Kraemer, Ivan Flechais, and Helena Webb. 2019. Exploring communal technology use in the home. In Proceedings of the halfway to the future symposium 2019 (HTTF 2019). https://doi.org/10.1145/3363384.3363389

15. Inga Kroener and David Wright. 2014. A Strategy for Operationalizing Privacy by Design. The Information Society 30, 5: 355–365. Retrieved from http://www.tandfonline.com/doi/abs/10.1080/01972243.2014.944730

16. He Li, Lu Yu, and Wu He. 2019. The Impact of GDPR on Global Technology Development. Journal of Global Information Technology Management 22, 1: 1–6. https://doi.org/10.1080/1097198X.2019.1569186

17. Ewa Luger, Lachlan Urquhart, Tom Rodden, and Michael Golembewski. 2015. Playing the legal card: Using ideation cards to raise data protection issues within the design process. ACM Press, New York, NY, USA. https://doi.org/10.1145/2702123.2702142

18. D. J. Mir, Y. Shvartzshnaider, and M. Latonero. 2018. It takes a village: A community based participatory framework for privacy design. In 2018 ieee european symposium on security and privacy workshops (euros pw), 112–115. https://doi.org/10.1109/EuroSPW.2018.00022

19. M.J. Muller. 2003. Participatory design: The third space in HCI. Human-Computer Interaction Handbook 4235, January 2002: 1051–1068. https://doi.org/10.1145/153571.255960

20. Deirdre K Mulligan and Jennifer King. 2011. Bridging the gap between privacy and design. U. Pa. J. Const. L. 14: 989–1034.

21. Helen Nissenbaum. 2009. Privacy in context: Technology, policy, and the integrity of social life. Stanford University Press.

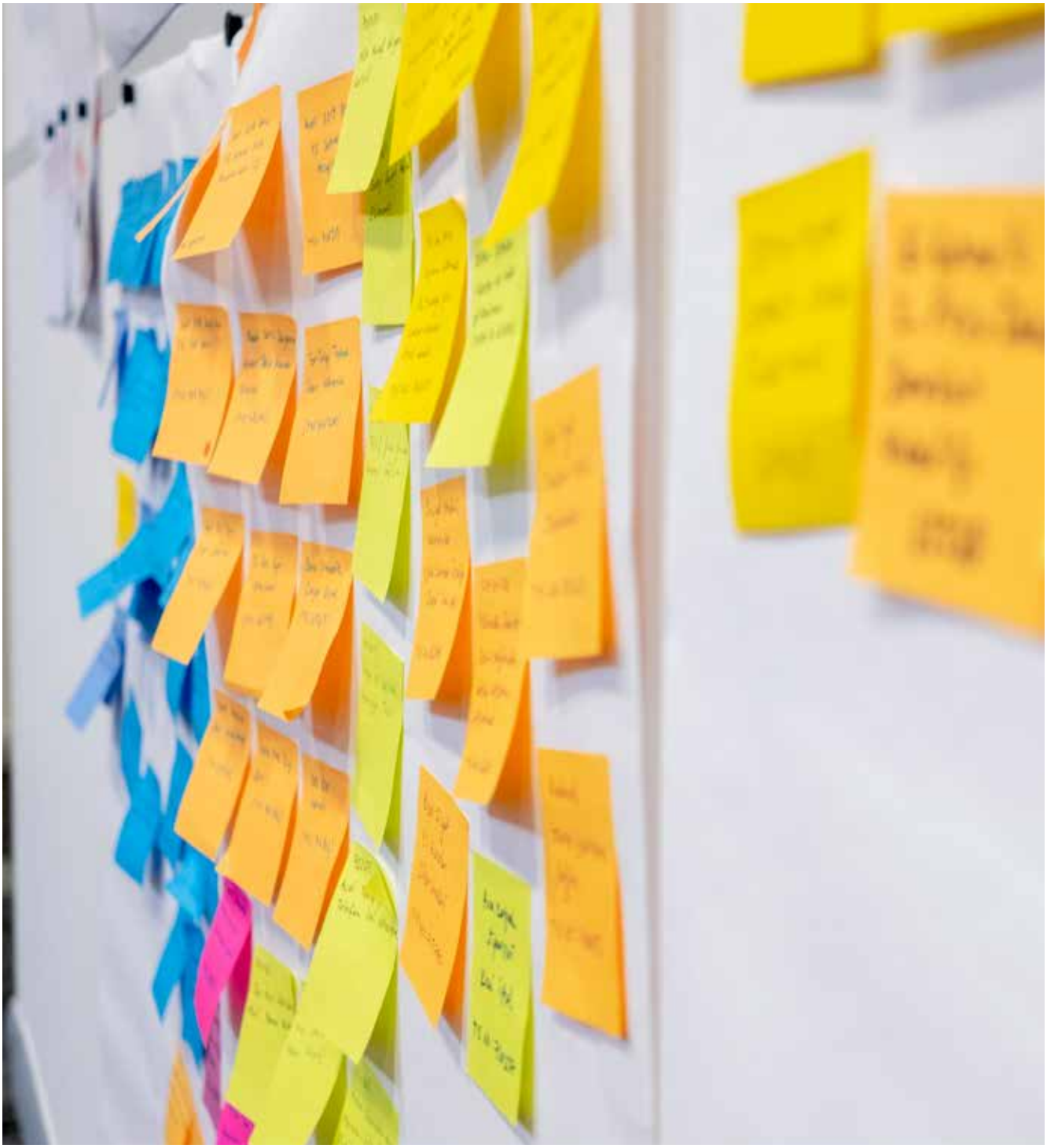
22. Sarah Spiekermann and Lorrie Faith Cranor. 2009. Engineering Privacy. IEEE Transactions on Software Engineering 35, 1: 67–82. https://doi.org/10.1109/TSE.2008.88

23. Peter Tolmie and Andy Crabtree. 2018. The practical politics of sharing personal data. Personal and Ubiquitous Computing 22, 2: 293–315. https://doi.org/10.1007/s00779-017-1071-8

24. Richmond Y. Wong and Deirdre K. Mulligan. 2019. Bringing design to the privacy table: Broadening "design" in "privacy by design" through the lens of hci. In Proceedings of the 2019 chi conference on human factors in computing systems (CHI '19). https://doi.org/10.1145/3290605.3300492

25. Yaxing Yao, Justin Reed Basdeo, Smirity Kaushik, and Yang Wang. 2019. Defending My Castle: A Co-Design Study of Privacy Mechanisms for Smart Homes. Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems: 1–12. https://doi.org/https://doi.org/10.1145/3290605.3300428

26. Yaxing Yao, Justin Reed Basdeo, Oriana Rosata Mcdonough, and Yang Wang. 2019. Privacy perceptions and designs of bystanders in smart homes. Proc. ACM Hum.-Comput. Interact. 3, CSCW. https://doi.org/10.1145/3359161



"Ada & Grace & Jane & me" [1]

Eman Alashwali, CDT15 and Klaudia Krawiecka, CDT17

With a generous sponsorship from our CDT, we had the pleasure to attend the first "High-Tech Women in Science and Technology: From Cybersecurity to Artificial Intelligence" event, organised by the CYSEC Cybersecurity, TU Darmstadt, Germany. It was the longest event we have ever attended: from 8 a.m. to 7 p.m, packed with a great line of talks, panel discussions, and networking.

Interestingly, the event was in memory of Jane Fawcett (1921-2016), and it took place on March 4 (her date of birth), 2020. Jane is a British code breaker, who worked at Bletchley Park during World War II. She recently became known for her role in deciphering a message that led to the sinking of a German warship, hence to a victory in the battle. While she did significant work at that time, she never spoke about it until the 90s. The event organisers state the following touching message:

"We want to encourage women in tech to show off their work and talk about their successes in order to motivate young women to do the same".

The event contained a long line of interesting talks by distinguished female speakers from all over the world. The topics varied between technical covering hardware and software security, personal experiences, and motivational talks, from both academia and industry.

For example, Najwa Aaraj from the Technology Innovation Institute in the United Arab Emirates (UAE) talked about "IoT security challenges: embedded encryption and machine learning technologies". One of the challenges they tackle is integrating lightweight cryptography in the Internet of Things (IoT) SW and HW co-design. Another research area that Najwa talked about is employing machine learning techniques in anomaly detection in IoT devices. Then, Ileana Buhan from Riscure talked about "Learning when to stop: in life & when training deep networks". Ileana took us through a trip in time of cryptanalysis techniques from 1941 to 2020, imagining that Jane would carry out her cryptanalysis, and think of what are to tools she needs and the challenges she will face throughout the time. She shared with us some state of the art techniques in side-channel analysis using deep neural networks, and some of the challenges they face in, and how to combat them.

During this event, we attended two panel discussions. The first one was led by Dr. Juliane Kramer from TU Darmstadt and assembled five female students from various research institutions in Europe. The students shared their experiences and talked about challenges in pursuing their degrees. Moreover, the panelists discussed their motivations and rationales behind choosing an academic career instead of following an industrial path. They highlighted the importance of understanding underlying technology in reasoning about security controls and engineering standards. The panel members also discussed the diversity of their research environments, indicating that there is still room for improvement. During the second panel discussion, the cybersecurity professionals discussed risks and opportunities arising from emerging technologies such as AI, neuromorphic systems, IoT, post-quantum security, and 5G. This session was moderated by Prof. Ahmad-Reza Sadeghi. The panel members discussed the possibility of using machine learning for security as well as adversarial characteristics of this technology. However, the main discussion revolved around AI technology and its different aspects. The panelists conversed if this technology is overestimated and misunderstood, or it can become our salvation. They also talked about its accountability. The opinions were divided, however, the panel members concluded that AI is a powerful tool that can, in the future, enable and facilitate technological development.

[Left to right]: Eman, Klaudia, and Professor Ahmad-Reza Sadeghi from TU Darmstadt

The interested reader can find most of the talks video recordings at the "CYSEC Darmstadt" Youtube channel under the "High-Tech Women 2020" videos. Additionally, presentation slides are available at: https://htw.trust-sysec.com

The event allowed us to discuss our career paths, challenges, and experiences with fellow female researchers in cybersecurity. While the event was inspiring and successful, as one of the panelists said, we hope to witness the day where such events (that are designed to support women in science and technology) are no longer needed!

[1]Title credit goes to the event organisers at TU Darmstadt.

[Above] Jane Fawcett. © nytimes.com

"We want to encourage women in tech to show off their work and talk about their successes in order to motivate young women to do the same"

Oxford's CDT in Cybersecurity from a student's perspective

Marcel Stolz, CDT16

When I came to Oxford, my background was mostly in Computer Science. True, I had done an unconventional minor degree in Musicology alongside my Computer Science studies back in Switzerland, but the main focus of my undergraduate and master's degree had been on technical projects in the domain of network interface programming. I anticipated that my research activities at the CDT in Cybersecurity would be mainly of technological nature.

During the first year at the CDT, my perspective on cybersecurity was massively broadened thanks to our weekly modules from different disciplines of cybersecurity research. I developed a fascination for the interconnectedness of technological problems with questions related to international affairs, ethics, and society in general. I came to understand that while my knowledge and interest in technological computer science was valuable, it would be even more interesting to connect the insights I had as a "tech person" with the questions arising in other disciplines. I was able to experiment with such a cross-disciplinary approach in my two mini projects and decided that I found it to be fascinating. Retrospectively, I have to admit that starting a DPhil in an area that I do not hold an undergraduate degree in might have been more venturesome than I first anticipated: I had to learn a whole new vocabulary, different research methods and become accustomed with the research world of other disciplines (e.g. where to publish, what to publish, and that conferences in other subjects were very different from conferences in computer science). While it took some time to identify the knowledge I needed to acquire, I received a lot of support from my peers at the CDT and my supervisors. The academic environment I have experienced is very supportive to unconventional approaches that might be labelled as "somewhat bonkers" by some, but I would describe as driving innovation in research. I believe that this openness to new ideas is one of the reasons why Oxford is the world's leading university.

While other disciplines have fairly established methodological standards and a clear canon and consensus-building mechanism, for example through high ranking conferences or journals, cybersecurity has only quite recently begun to emerge across several disciplines. Even more recent is the understanding that problems in cybersecurity can no longer be approached within the silo of a single discipline: the second half of the 20th century has brought forward a high level of innovation in what we would usually refer to as information security, IT security, or technical cybersecurity. With the mass of connected devices available at the beginning of the 21st century, academics (and also others) have come to the understanding that cybersecurity is no longer just a technical problem, and that law, police, users, and our societies, political and democratic processes are deeply affected. Thus, not only the discipline of computer science is affected, but also that of law, political science, social science, criminology, psychology, etc. Yet, as is common in academia, often the first approach to a new problem is to examine it with the tools we are already familiar with; the conventional research approach of each individual discipline. While I believe that each discipline requires a foundation, canon, and methods for establishing a theoretical consensus, I am strongly convinced that we need to look beyond our conventional horizons in order to inspire good research – particularly in cybersecurity. And I think that Oxford's CDT provides an ideal environment to assist with this: first, we enjoy a high amount of freedom in our research while having access to a network of fantastic and successful researchers. They enable us to remain on the edge of their world-reading research activities. Numerously I have been lucky enough to receive "that one pointer" I needed from someone in our CDT network in order to come up with a great idea. The continuous activities of our CDT – the student symposium, "Deep Dives", visiting researchers, Friday seminars, etc. – strongly help in continuously extending this network. I also appreciate the possibility to engage in elective modules provided by the CDT every year. Sometimes these module are connected directly with my research, or with methods I would like to use, while other times I pick a module that is from a different area of cybersecurity that I would like to learn more about. While it is nice to follow one's interest, it is often also the case that this engagement with something that is not directly connected to my research yields ideas that further inspire my DPhil research. And I also stay up-to-date with developments in cybersecurity that might later become relevant to my research activities, even if they are not directly impacting my research area at the moment.

All of these activities help to gain a better understanding, to improve personal research and communication skills, and to stay on top of current cybersecurity research – we get both the breadth and depth we require for outstanding research.

Even though my time at Oxford has often taken slightly different turns than anticipated – and some of them felt very difficult to start with – I am convinced that our time here is highly valuable, both in terms of developing cybersecurity proficiency and in my development as a human being. I have not found any other place that could awaken a similar amount of fascination as Oxford when it comes to research and interdisciplinarity – and I think at this point I should thank everyone involved in the CDT for making it such a great place for us students.

A Frightening but Virtuous Cycle: Responsible Disclosure in Practice

James Pavur, CDT17

Science is a collaborative effort of thousands iterating on each other's discoveries to better understand the world. A core tenant of academic freedom is thus the right to publish and disseminate findings widely. A discovery made but unshared cannot advance knowledge.

One of the more unique aspects of cyber-security research is that such discoveries can threaten the security of real-world systems. While many disciplines have codified ethical processes for ensuring that the pursuit of knowledge does not cause unintentional harm, only a few must grapple with the possibility that this knowledge itself could be harmful.

In cyber-security, we grapple with the possible dual-use nature of our research through a process of "responsible disclosure." A key contrast with other potentially dual-use disciplines is that cyber-security vulnerability discoveries are made in engineered systems. While it is not possible to alter the laws of chemistry to prevent a newly discovered compound from being used in chemical weapons, it is absolutely possible to alter a software system to prevent a newly discovered exploit from being used in cyber-attacks. Responsible disclosure is about prioritizing information sharing with those who are best positioned to make such changes.

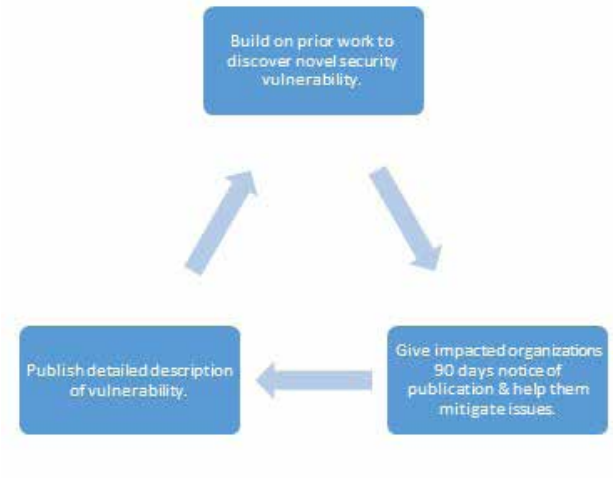


Figure I The Vulnerability Disclosure Cycle

The general process for responsible disclosure is straightforward. When a vulnerability is discovered, we notify organizations with direct exposure – generally the manufacturers of a vulnerable system. They are given exclusive knowledge of this vulnerability for some period (standard practice is around 90 days) to assess and mitigate the risks. After this, the vulnerability is disclosed publicly, often in the form of peer-reviewed publication.

This phased information sharing approach strikes a careful balance between the potential harms of bad actors abusing our findings and the benefits of the wider academic and engineering community building on them. Further, it dissuades the mistaken assumption that a vulnerability known to academics would not be discoverable by criminals and other attackers. By stating clearly that a vulnerability will become public knowledge, we can encourage industry to consider the risks of the vulnerability itself, rather than the probability that it will be re-discovered. Once published, other researchers can learn from the vulnerability and consider how novel variants may apply to other systems. This creates a virtuous cycle whereby the academic process aligns with commercial pressures to secure systems quickly and safely.

In practice, vulnerability disclosure can be quite a bit more complex. My own first experience with security research is a good parable to this effect. As a high school student, I uncovered a vulnerability in my school's computer system which allowed unrestricted access to sensitive information about students and faculty as well as some other information systems (e.g. security cameras). I shot an email off to an academic advisor detailing the vulnerability. A few weeks later, I found myself seated before a disciplinary tribunal and was briefly suspended for violating the schools' technology use policy.

The important lesson I learned is that vulnerability reports are not always well-received and security research is often a diplomatic exercise as much as it is a technical one. The perfect synergistic cycle of security research, vulnerability patching and academic publication is a highly idealized case while reality can be considerably messier.

For example, we recently published a paper on protocol vulnerabilities in a particular class of satellite communications systems. The vast majority of companies we contacted about the vulnerability were receptive to our responsible disclosure efforts, thanking us for the information and arranging calls to get our ideas or discuss possible mitigations. However, one company responded by threatening legal action if we published, suggesting that our research was somehow criminal in nature. With careful and deliberate communications, we eventually reached a degree of mutual understanding with the company and published the paper without incident. However, this experience demonstrates that even the same exact research and same exact disclosure letter can be perceived in radically different ways and that this reception is often beyond the control of researchers.

Why take such a risk? After all, there are plenty of unsolved cybersecurity questions which are not only safer but also often more publishable than the simple discovery of vulnerabilities. Engineering secure systems, designing

efficient cryptographic protocols, or improving the usability of existing techniques are all valuable contributions which elegantly sidestep the risks and tensions of vulnerability disclosure. Indeed, such topics can often feel more productive in that they propose solutions and promise comparatively generalizable findings.

One key advantage of vulnerability research is the direct link that the responsible disclosure norm facilitates between researchers and industry. The annals of even top-tier cybersecurity conferences are littered with well-conceptualized scientific studies which are briefly noticed within academic circles before vanishing into oblivion. The process of responsible disclosure hedges against this risk, ensuring that research, at a minimum, is directly considered by those who it most directly impacts. This provides a route to facilitate meaningful change beyond academia. When coupled with more traditional computer science, a symbiosis emerges whereby disclosures can contextualize academic solutions, creating connections and building a case for real-world implementation of academic security systems.

In sum, the norms of responsible disclosure create an ecosystem in which vital vulnerability research can be conducted within a reputable and ethical ecosystem. By taking on the risks of discovering and communicating vulnerabilities to potentially hostile audiences, we can better bridge the divide between security academia and industry. The ultimate result is academic research which more directly addresses real-world needs and deeper appreciation in industry for the academic approach to knowledge generation.

The Inaugural ACE Winter School

Anjuli R. K. Shere, CDT18

From 13-16 January 2020, eleven of our CDT researchers at various stages of our DPhils embarked on a residential multidisciplinary cyber security programme at the University of Newcastle. The 'Academic Centres of Excellence' (ACE) group of research centres are 19 UK universities endorsed by the National Cyber Security Centre (NCSC) and recognised by the Department for Digital, Culture, Media and Sport, as well as the Engineering and Physical Sciences Research Council and GCHQ. This inaugural 'ACE Winter School' hosted over one hundred doctoral students from the ACE group who study cyber security. The organisers hoped that "by engaging with each other and experts from academia, industry and government, research students will develop innovative ideas from the intersection of their research projects", a goal that was certainly accomplished. On a personal note, it was wonderful to meet other doctoral students in-person after having followed their thoughts and publications online, and I am sure that many collaborative efforts will spin out from the week we all spent together in Newcastle. The week's agenda was brimming with lectures and workshops on all manner of real-world current and anticipatory issues, based on the NCSC's Cyber Security Body of Knowledge (CyBOK). Through careful curation, the Winter School's organisers managed to make all the lectures accessible to doctoral students from a wide variety of backgrounds, so that we could at least understand the key points of each talk, from technical analyses of avionic data links to psychology-based discussions on the exploitation of human vulnerabilities. They achieved this by inviting lecturers to travel from a multitude of places to stand before us and talk about their different studies, like jigsaw pieces that look totally different but slot together to reveal a picture - cyber security - that spoke to all of us.

Of course, a second core feature of our time spent in Newcastle was networking; we were able to meet and further question the academics who gave the talks, as well as gathering in hotel lobbies and bars after-hours to get to know the other students who had travelled from all over the country to discuss our shared desire to investigate and improve cyber security issues. One pub that saw hordes of us descend in the evenings to discuss our doctoral experiences and completely unrelated interests was The Duke of Wellington High Bridge, which had the dubious honour of being situated opposite the conference's recommended hotel.

Our first talk of the week was given by Professor Madeline Carr (UCL), entitled 'Cybersecurity beyond Technology: The Human Dimensions'. She highlighted the significance of events such as this, which introduce socio-technical elements of cyber security to a field that was previously seen as exclusionary to non-computer-scientists. In particular, Professor Carr impressed upon us the need to recognise that technology develops in the context of human power, so that we could understand the importance of both challenging preconceptions and facilitating clear communication between stakeholders in order to ensure that our work raises standards and has a positive impact. This theme carried through the rest of the trip, with Professor Adam Joinson (University of Bath) arguing that cyber security experts must push for a shift from a compliance-based model of cyber security to persuasive technology, as most organisations currently employ punitive sanctions for poor security behaviour, thereby framing workers as "weak links" rather than engaging them as part of a defence strategy. This was particularly interesting in light of a talk given the next day by Professor Lynne Coventry

(Northumbria University), about exploitable human vulnerabilities. Given my own professional experiences, I was excited to see the conference open with such nuanced representation of benefits and challenges associated with the human side of security.

Then, the topics shifted to a different kind of problem-solving: Professor Shujun Li (University of Kent) raised some of the challenges of user authentication, reminding us that it is not just policy that must be adapted but also the technological side of security, including a possible end to the prevalence of vulnerability-ridden passwords. Professor Gianluca Strighini (Boston University) walked us through the cybercriminal malware ecosystems, from vectors to countermeasures. Dr. Shishir Nagaraja (University of Strathclyde) added to the cybercrime conversation, covering threat modelling and detection of Command and Control infrastructures. Regarding how these threats might be thwarted, Dr. George Theodorakopoulos (Cardiff University) gave us an interesting statistical perspective on privacy-preserving data processing, including how data protection can be established at various stages of data production, processing and storage. Something I particularly enjoyed about these talks was the way that they encompassed technical, legal and policy issues, so that we came away with a more holistic understanding of cyber security's multifaceted nature.

Escalating discussions around the scale and intensity of the potential threats were talks by our own Professor Ivan Martinovic, who explained his group's research into the safety and security balance needed for Aviation/ Transportation Communication networks, and Dr. Tariq Elahi (University of Edinburgh), whose insights into defence against mass surveillance and censorship enlightened us as to how issues in the cyber-realm fit within the big picture of global politics and human life. Also on the subject of interference in democracy, Professor Steve Schneider (University of Surrey) gave us a compelling argument for secure electronic voting, highlighting the pros and cons, and elucidating the encryption/decryption processes. Similarly, Professor Eerke Boiten (De Montfort University) discussed the utility and feasibility of cyber intelligence sharing. This kind of practical consideration is particularly fascinating when juxtaposed with the talk by Professor Chris Hankin (Imperial College) on security-critical nodes in critical infrastructure systems. These talks were especially interesting to me as they helped to contextualise more technical aspects of cyber security.

Oxford's Professor Marina Jirotka spoke of responsible innovation and the dilemma of too little or too much control. Dr. Jose M. Such (KCL) elaborated on the topic of security, privacy and trust in AI-enabled systems, explaining that AI security and privacy requires interpretable, accessible transparency. Professor Thomas Gross (University of Newcastle) reminded us of the importance of the role of evidence-based methods in cyber security research, giving us clear, helpful guidance as to how we can effectively make individual studies rigorous enough to add to the knowledge and methods of our field. To me, these talks were instrumental in reasserting the significance of research methods, rather than allowing us to slip into a more laissez-faire "the ends justify the means" attitude.

Speaking of efficacy, Professor Awais Rashid (University of Bristol) clarified why software keeps being produced with vulnerabilities, despite significant recent technological and academic advances. Professor Sanjay Rawat's (University of Bristol) discussion of evolutionary fuzzing techniques detailed the way in which the software testing technique grew into its current form. This talk was especially interesting as it followed Professor Thomas Pasquier's (University of Bristol) lecture on provenance-based intrusion detection, which described how records of information flows between kernel objects, such as files, could be captured and analysed to design intrusion detection systems. I was happy to realise that the CDT's intensive first year schedule had prepared me well to critically follow even these talks, which were more computer science heavy.

Unfortunately, most of the workshops (with the exception of Lucas Kello's Cyber Crisis Simulation which, for CDT-ers, was also an assessment in our first year) were marked as only accessible to the more computer-science-focused conference delegates. Although this ruled out participation for a number of participants, unlike the more accessible talks, those who did participate from CDT particularly mentioned that the workshops about Ethical Hacking for Industrial Control Systems, Introduction to Programmable Networks for Security, and How to Securely Use Cryptography were all useful experiences.

In addition to the series of enthralling talks, participants were able to display our research posters, giving us the opportunity to reflect on and admire some of the work being undertaken by our peers to make the future more secure. There was also a conference-wide activity that involved working in groups of students from various universities to create something that promoted the positive aspects of cyber security to the general public. All the wonderful entries left us feeling uplifted and empowered, and three of our CDT members were part of teams that got special mentions by the judges! George Chalhoub's team won first place, with a demonstration of their song "Creds, Access, Dos and Don'ts" - to the tune (and with the accompanying movements) of "Heads, Shoulders, Knees and Toes"! Mark Quinlan's team were runner-ups with their skit "Fleabay", and Hayyu Imanda's team were commended for their innovative cyber security-themed haikus.

Months later, I remain grateful to have had the chance to listen to a constellation of speakers whose work is a shining reminder of the impact that our own research could have on global cyber security, in a myriad of ways. Cheesy though it sounds, the bonds forged by mutual doctoral stress and a shared desire to contribute to the field with our doctoral studies have also given me a number of friends from across the country whose dedication and work inspires my own research. I plan to sign up for the next ACE Winter School, wherever it is, and I would thoroughly recommend the experience to any CDT members who were unable to attend in 2020.

The CDT in Numbers

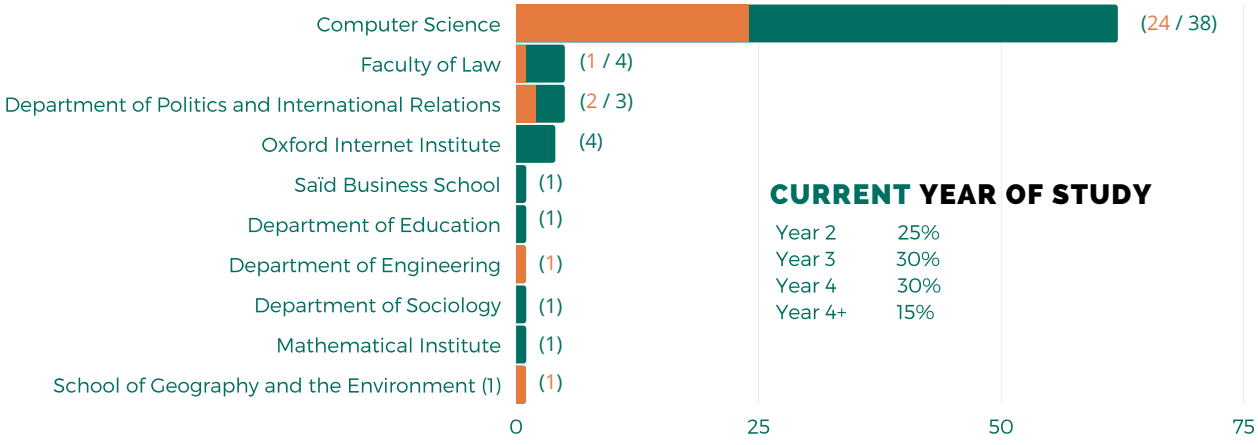
SUMMER 2020

CURRENT STUDENT PROGRESS

The CDT currently has 52 students 'in-flight' with a further 29 having completed and submitted their theses before September 2020. Based on expected submission deadlines the balance between 'in-flight' and completed students will reverse in April 2021. Our Alumni News section highlights the positive impact this growing community of former students is having on the academic environment, their communities and industry as a whole.

CURRENT AND COMPLETED STUDENT HOST DEPARTMENTS

The CDT continues to work with a diverse group of departments, bringing new perspectives to existing fields and expertise in tackling new challenges. We currently have students hosted by eight departments across the university in both technical and non technical disciplines.



CURRENT YEAR OF STUDY

Year 2	25%
Year 3	30%
Year 4	30%
Year 4+	15%

50%

of graduates are now working in academic roles within leading institutions around the globe.

39%

of graduates have secured roles in industry in a range of organisations, including the consultancy, FinTech and charitable sectors.

11%

of graduates are working within government roles helping communities in which they serve.

1.5

Average number of journal papers published this year, per student.

46.4

Average number of journals read this year, per student.

STUDENT LOCATIONS WHILE WORKING FROM HOME

6.1

Average number of MS Teams students report being enrolled in since working from home.

71

Average number of total MS Teams meetings, per student, since working from home.

OUR RECENT ALUMNI ROLES INCLUDE:

- Research Associate in Systems Security, University of Oxford. (Air-to-ground communications systems and protocols in use for aviation)
- Lecturer, Faculty of Law at the University of Technology Sydney (UTS), New South Wales
- Strategic Cyber Threat Intelligence Analyst, Digital Shadows
- Research Scientist, Facebook
- Hardware Research Engineer, Jump Trading

CDT13 to 15 Bios

Ranjbar Balisane

Supervisor: Andrew Martin, Department of Computer Science

Ranjbar has a First Class B.Sc. (Hons) in Ethical Hacking & Network Security and M.Sc. with Distinction in Forensic Computing. Prior to joining the CDT in Cyber Security at Oxford, he worked as an eCampus project manager for Soran University, Kurdistan, initiating the first large scale eCampus in Iraq, working in collaboration with LS Cables (LG). He has experience in vulnerability discovery, penetration testing, programming, networking, and protocol design.

DPhil Thesis: Engineering Secure, Usable, and Privacy Preserving Identity Management System using Trusted Computing.

Researching systematic approach to enhancing authentication privacy and security using trusted computing.

While a lot of research is focused on enhancing a particular method of authentication such as enhancing hashing algorithms, or ways which fingerprint templates are stored, or finding new and more secure ways to authenticate a user. This research focuses on the underlying architecture using the advances made in technology to provider better privacy protection, security and more usable security.

Publications

R A. Balisane and A. Martin (2016). Trusted Execution Environment-Based Authentication Gauge (TEEBAG). In Proceeding of the New Security Paradigms Workshop (NSPW), Colorado, USA, 2016. ACM.

Atamli-Reineh, R. Borgaonkar, R. A. Balisane, G. Petracca, and A. Martin (2016). Analysis of Trusted Execution Environment usage in Samsung KNOX. In Proceedings of the Workshop on System Software for Trusted Execution (SysTex), Trento, Italy, 2016.

Mini-Project; OpenSky – Towards Secure Next Generation Air Traffic Communication Protocols

Mini-Project: Trusted Computing versus Identity

Aaron Ceross

Supervisor: Andrew Simpson, Department of Computer Science

Aaron has a background in law and prior to joining the CDT, he worked as a researcher in data protection, privacy, and surveillance at the University of Groningen in the Netherlands as well as the University of Malta. Aaron recently completed the MSc in Computer Science from the University of Bristol in order to expand his technical abilities as well as be able to engage in more multidisciplinary research.

DPhil Thesis: Metrics and models for privacy engineering.

This research proposes to investigate how privacy risks can be more effectively articulated to information system designers. The goal is to be able to establish a link between a systems-level risk analysis and regulatory outcomes. This entails the following questions: (i) what are the challenges faced by information system designers with regards to privacy, as both a broad concept and multilevel values? (ii) what information needs to be made available in order for these challenges to be overcome? (iii) is this information drive measurably effective privacy practices for systems design? This research seeks to match the causes of regulatory liability to specific system design implementation, focusing on being able to accurately link normative regulatory values to a system's operational metrics. This results in measures which may inform organisations of the risks to personal data. One of the means by which empirical data may be gathered for privacy failures within information systems is from events such as data breaches, and other events recorded by authorities. These data may be used as ground truth from which to develop objective, generalisable metrics for privacy risk. This thus provides a more quantitative measures for privacy risk analysis, which hitherto has been largely qualitative, subjective measures. This would therefore better inform the information systems engineering process.

Publications

"Examining data protection enforcement actions through qualitative interviews and data exploration" at the 37th annual conference of the British and Irish Legal, Education and Technology Association (April 2017), and will be published in the International Review of Law, Computers and Technology.

"The use of data protection enforcement actions as a data source for privacy economics" at the 3rd International Workshop on Technical and Legal Aspects of Data Privacy and Security (September 2017), to be published in the SAFECOMP 2017 Workshop Proceedings in Lecture Notes in Computer Science

Mini-Project: Understanding threats to anonymisation: Gap-analysis and research directions

Mini-Project: Exploring Liabilities and Remedies for Data Breach

Jacqueline Eggenschwiler

Supervisor: Rebecca Williams, Faculty of Law

Jacqueline Eggenschwiler is a doctoral researcher at the University of Oxford's Centre for Doctoral Training in Cyber Security. Her research looks at the contributions of non-state actors to global cybersecurity norm formation processes and corresponding governance implications. Jacqueline holds degrees in International Affairs and Governance, International Management, and Human Rights from the University of St. Gallen and the London School of Economics and Political Science.

DPhil Thesis: Non-State Actors and Norms of Responsible Behaviour in Cyberspace

This thesis examines the roles and contributions of non-state actors to global cybersecurity norm formation processes. Specifically, it analyses how, in which capacities, and how effectively non-state protagonists engage in norm cultivation endeavours by surveying nine exploratory case studies, grouped into three clusters, i.e. (a) civil society and academia, (b) corporate actors, and (c) expert communities.

Triangulating different qualitative means and methods of data collection and analysis, this thesis suggests that non-state actors have come to exert discernible politico-legal influence over discussions about norms of responsible behaviour for the virtual realm.

The results of this inquiry go to show that non-state actors have to be taken seriously as key contributors to global cybersecurity steering efforts, and that their activities have important implications for global accountability and legitimacy structures. Their normative undertakings also have significant consequences for how authority is shared between governmental and non-governmental entities.

Publications:

Eggenschwiler, J. (2017), 'Accountability Challenges Confronting Cyberspace', Internet Policy Review, Vol. 6 No. 3, pp. 1–11.

Eggenschwiler, J. (2018), 'A Typology of Cybersecurity Governance Models', St Antony's International Review, Vol. 13 No. 2, pp. 64–78.

Eggenschwiler, J. (2019a), International Cybersecurity Norm Development: The Roles of States Post-2017, Brussels, available at: https://perma.cc/7PR4-C72T.

Eggenschwiler, J. (2019b), 'An Incident-Based Conceptualization of Cybersecurity Governance', in Ellis, R. and Mohan, V.K. (Eds.), Rewired: Cybersecurity Governance, John

Wiley & Sons, Hoboken, NJ.

Eggenschwiler, J., Agrafiotis, I. and Nurse, J.R. (2016), 'Insider Threat Response and Recovery Strategies in Financial Services Firms', Computer Fraud & Security, Vol. 2016 No. 11, pp. 12–19.

Eggenschwiler, J. and Silomon, J. (2018), 'Challenges and Opportunities in Cyber Weapon Norm Construction', Computer Fraud & Security, Vol. 2018 No. 12, pp. 11–18.

Other:

2017 EuroSSIG Fellow (https://eurossig.eu/eurossig/),

NextGen@ICANN 58, Copenhagen

Graham Fairclough

Supervisors: Victoria Nash, Oxford Internet Institute and Robert Johnson, Faculty of History

Prior to coming up to Oxford Graham served in the British Army, reaching the rank of Colonel. Operational tours included Northern Ireland, Belize, The Balkans, Iraq and Cyprus serving in intelligence and counter-intelligence roles. Senior appointments include a tour in the United Kingdom's Permanent Joint Headquarters (PJHQ), responsible for the delivery of operational intelligence architecture and capability globally, including Iraq and Afghanisatan, during the period 2007-2010, and between 2010-2013, he was the first Chief of Staff to the UK's Chief of Defence intelligence, within the Ministry of Defence. He has served on several occassions with the Government Communications Headquarters (GCHQ) and worked closely with other elements of the United Kingdom's intelligence community and its international partners.

Graham is a graduate of the United Kingdom's Staff College where he gained a MA in Defence Studies from Kings College, London and also holds a MSc in Knowledgement Management Systems from Cranfield University. He participates in NATO's Urbanisation Programme, the 5 Eyes' Contested Urban Environment (CUE) experiement and contributes to the development of United Kingdom military doctrine through a number of work streams where he advises on information manoeuvre and the challenge of operating in a future information led environment. Graham is an associate reseacher with the Changing Character of War Programme at the University of Oxford, working on the impact of the cyber environment on warfare, how cyber security challenges are understood by senior decision makers, and the role of strategic partnerships in delivering national cyber security strategy.

DPhil Thesis: The Emergence of Offensive Cyber in National Cyber Security Strategy: From the Secret State to the Public Space – A United Kingdom Perspective.

Achieving a safe and secure cyber environment is an issue of national security for states. The consequences of not attaining this objective are significant: the denial of critical infrastructure, financial cost, loss of intellectual property, the compromise of personal security and reputational damage. For the United Kingdom, cyber security is considered to be a Tier 1 security concern. United Kingdom government statements concerning the challenges faced in delivering a secure cyber environment indicate a recognition that its current approach to delivering cyber security is no longer valid: 'Getting cyber security right requires new thinking'. A changing threat landscape has led to the acknowledgment of the role and necessity of offensive cyber capability in achieving cyber security, 'We will defend ourselves, but we will also take the fight to you'. This emphasis on the offensive, represents a major shift in the strategic underpinnings on which the United Kingdom's national cyber security strategy has historically been founded. Placing, alongside the existing pillars of a strong defence and a high level of resilience, a third pillar of a strong offence. The requirement exists to understand the nature of this strategic change in policy and its impact on how the United Kingdom implements its national cyber security strategy to meet the challenge of the competitive cyber environment.

Publications

The Mouse, the Tank and Hybrid War: Understanding the Battlespace. G Fairclough. Presented at ICMSS 2016 Conference, Istanbul, Turkey.

A Model to Facilitate Discussions about Cyber Attacks. J Happa, G Fairclough, M Goldsmith and S Creese. Presented at CYCON 2015 and to be published in forthcoming Ethics and Politics for Cyber Warfare.

"Rolling ODD DICE: Operations in Future Urban Warfare". G J Fairclough. Presented at ISSS – ISAC 2015 Conference, Springfield, MA, USA. Published in NATO Urbanisation Experiment 2030. ACT, NATO.

The Truth is Out There – Intelligence in the Cyber Age

The United Kingdom and Japanese Approaches to Cyber Security: Themes for Global Cyber Security Capacity Building in the Future

John Galea

Supervisor: Daniel Kroening, Department of Computer Science

John Galea completed his B.Sc. undergraduate degree in Computer Science and Artificial Intelligence at the University of Malta. He continued his studies and was awarded a Master's degree in Computer Science in 2015.

John is currently reading for a DPhil in Cyber Security at the Department of Computer Science, University of Oxford, under the supervision of Prof Daniel Kroening. His interests revolve around binary analysis, vulnerability discovery and dynamic binary instrumentation (DBI). Some of his research builds upon the DBI engine DynamoRIO, an open-source project which he actively contributes to and helps maintain.

DPhil Thesis: Optimizing Generic Taint Analysis on Binary Applicationss

Dynamic Taint Analysis is a pivotal technique in software security. Typical use-cases include malware analysis, vulnerability discovery and attack detection. However, its runtime overhead is known to severely limit its practical adoption. This performance problem is exacerbated if the taint analysis conducted is generic, as the implementation of the taint engine cannot be optimized for a particular policy. Therefore, during the course of my DPhil, I explore methods to enhance the performance of generic taint analysis on x86 binary applications (without the availability of source-code). These optimizations range from vectorizing taint propagation to dynamically generating fast paths in a just-in-time fashion.

Publications

Mini-Project: The Verser protocol: Verifying Services of IoT Devices Based on Their Capabilities

Mini-Project: ROPEX: Towards the Circumvention of Data Execution Prevention via Automatic Exploit Generation

The Taint Rabbit: Optimizing Generic Taint Analysis with Dynamic Fast Path Generation

John Galea and Daniel Kroening, AsiaCCS 2020

William Osborn

Supervisor: Andrew Martin, Department of Computer Science

After graduating high school in Albuquerque, New Mexico, William joined the U.S. Military where he served as a paratrooper in Afghanistan with the 82nd Airborne Division, in support of the NATO-led International Security Assistance Force. Following his military service he received a Bachelors of Science from Penn State University in Security and Risk Analysis, focusing on Intelligence Analysis and Modelling. William then received a Masters Degree from Duke University focusing in Information Science and Information Studies. William is currently conducting research at the Saïd Business School, focusing on offensive cyber security measures as well as Corporate Cyber crime and Harm Analysis. He plans to work with corporate partners in developing offensive cyber security strategies and help them structure their physical security measures.

DPhil Thesis: Offensive Cyber Strategies for Medium to Large Corporations

He is interested in looking at the current and seemingly weak cyber security infrastructure of corporations. He will be looking at past cases of cyber incidents, fraud and attacks, response times as well as autopsies of the attacks. Given the data, he hopes to develop a new non-static strategy that evolves with the needs of corporations based off of their specific needs.

Publications

Harvard Business Review: https://hbr.org/2016/10/companies-should-understand-where-cybercrime-thrives

Mini-Project: How does geopolitical relevance and foreign investment impact a small island nation's cyber security strategy?

Mini-Project: The Ecosystem of Cybercrime: A Comparison of cybercrime in Brazil and Russia

Michal Piskozub

Supervisor: Ivan Martinovic, Department of Computer Science

Michal has been interested in Computer Science (and technology related topics) since his childhood friend introduced him to it at the age of 7. He continued this passion by doing BSc in Computer Science at King's College London and MSc in Computer Science at the University of Oxford. In the Cyber Security CDT in Oxford he completed two projects titled: On The Way To Adaptive Honeypots, and Dynamic Re-Planning For Cyber-Physical Situational Awareness. His DPhil project is titled Network Traffic Analysis For Malware Detection. Topics he is interested in include network security, malware analysis and data visualisation.

DPhil Thesis: Network Traffic Analysis For Malware Detection

Due to the fact that malware detection by analysing an executable is challenging and ineffective on a large scale, this project approaches the problem from a different perspective. Almost all modern malicious programs connect back to their authors to either ask for commands or send data from an infected computer. This is accomplished by using the Internet and more precisely by using computers' networking capabilities.

The aim of this project is to detect malware based on network traffic data. All network connections use packets as fundamental units that carry data. On the lowest level malware that communicates back to its origin creates and sends packets which constitute part of the behaviour of malware. The objective of this project is to perform a behavioural analysis of malicious programs by analysing network interactions.

While there are a number of papers that propose methods to detect malware based on their network behaviour, they concentrate on doing so manually and work with small datasets. The project will explore ways of automatic creation of features that are associated with known and new malware activities and will create a platform that will allow to work with datasets on the scale of big data.

Publications

Michal Piskozub, Riccardo Spolaor, and Ivan Martinovic. 2019. MalAlert: Detecting Malware in Large-Scale Network Traffic Using Statistical Features. SIGMETRICS Perform. Eval. Rev. 46, 3.

Michal Piskozub, Riccardo Spolaor, Mauro Conti, and Ivan Martinovic. 2019. On the Resilience of Network-based Moving Target Defense Techniques Against Host Profiling Attacks. In Proceedings of the 6th ACM Workshop on Moving Target Defense (MTD '19).

Mini-Project: On the Way to Adaptive Honeypots

Mini-Project: Dynamic Re-Planning For Cyber-Physical Situational Awareness

Tina Wu

Supervisor: Andrew Martin, Department of Computer Science

Tina completed her MSc in Forensic Computing and Security at the University of Derby. She then joined Airbus Group as a Research Engineer focusing on research in cyber security and forensics in industrial control systems. Her research interests are in Forensics and monitoring of industrial control systems with a focus on live memory forensics, novel attack detection methods, malware analysis, side channel attacks and the Internet of Things (IoT). Now she is a DPhil student at Oxford's CDT in Cyber Security, her research focuses on developing and improving the digital forensic process in the IoT.

DPhil Thesis: IoT Digital Forensics and Security

In Tina's DPhil project she is working to improve the digital forensic procedures required to carry out investigations in the IoT environment. The first part of the digital forensic investigation process involves identifying the number and the type of devices on the network, with the number of IoT devices being connected to networks, increasing, an investigator may miss hidden devices. Exploring practical methods to automatically fingerprint IoT devices on the network will speed up the identification process in an investigation.

Beside the technical challenges in IoT forensics, Tina has explored non-technical challenges such as; definitions, experience and capability in the analysis of IoT data/devices and current/future challenges. Tina has also been exploring using Bluetooth Low Energy (BLE) to extract evidential data from IoT consumer medical devices.

Publications

Wu, Tina and Jason R. C. Nurse. "Exploring The Use Of PLC Debugging Tools For Digital Forensic Investigations On SCADA Systems." JDFSL 10 (2015): 79-96.

Wu, T. and Martin, A., 2018,"'Bluetooth Low Energy used for Memory Acquisition from Smart Health Care Devices". Accepted at The 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications / / 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), New York, NY, 2018, pp. 1256-1261.

Adam Zibak

Supervisor: Andrew Simpson, Department of Computer Science

After obtaining his bachelor's degree in Computer Science, Adam completed the MSc in IT Law and Management from King's College London (Distinction) where he gained a grounding in the areas of Law which are most relevant to Information Technology as well as an understanding of business management techniques used within industry. Prior to joining the CDT, Adam worked as an open-source intelligence researcher and Arabic linguist for the International Centre for Security Analysis at King's College London.

Adam's primary research interest is cyber threat intelligence sharing, with an emphasis on evaluating the efficacy of current threat sharing initiatives and systems. Adam is the President of the Oxford University Strategic Studies Group (OUSSG). During his tenure, the Group paid special attention to Cyber Security topics, which included inviting high-profile field experts such as the Technical Director of NCSC, the former Director of GCHQ and NATO's Assistant Secretary General for Emerging Security Challenges.

DPhil Thesis: A Holistic Framework for Evaluating the Efficacy of Cyber Security Information Sharing Efforts

Cyber security information sharing is increasingly regarded as a crucial element in improving national and organisational cyber security posture. Growing efforts in the public and private sectors to foster cyber security information sharing have resulted in today's complex constellation of sharing centres, organisations, platforms and tools in various industries and government agencies, but have brought inconsistent observed improvement in security outcomes. A growing body of evidence from the academic and grey literature suggests that focus is shifting from creating interoperable sharing solutions to generating value. However, despite the growing interest and the proliferation of sharing efforts, the literature on the ability to fairly and accurately measure the value of these efforts remains limited.

In this research proposal we lay out the motivation for an empirical study that explores several aspects of information sharing in order to develop evaluation metrics and frameworks. A qualitative-dominated methodological approach will be utilised to develop more nuanced insights into the stakeholders' attitudes and understandings. The contribution will be in threefold: developing a taxonomy for cyber security information sharing as well as design goals; assessing the needs and determining the requirements for an information sharing evaluation framework; and assembling a suite of evaluation metrics within a holistic evaluation framework.

Publications

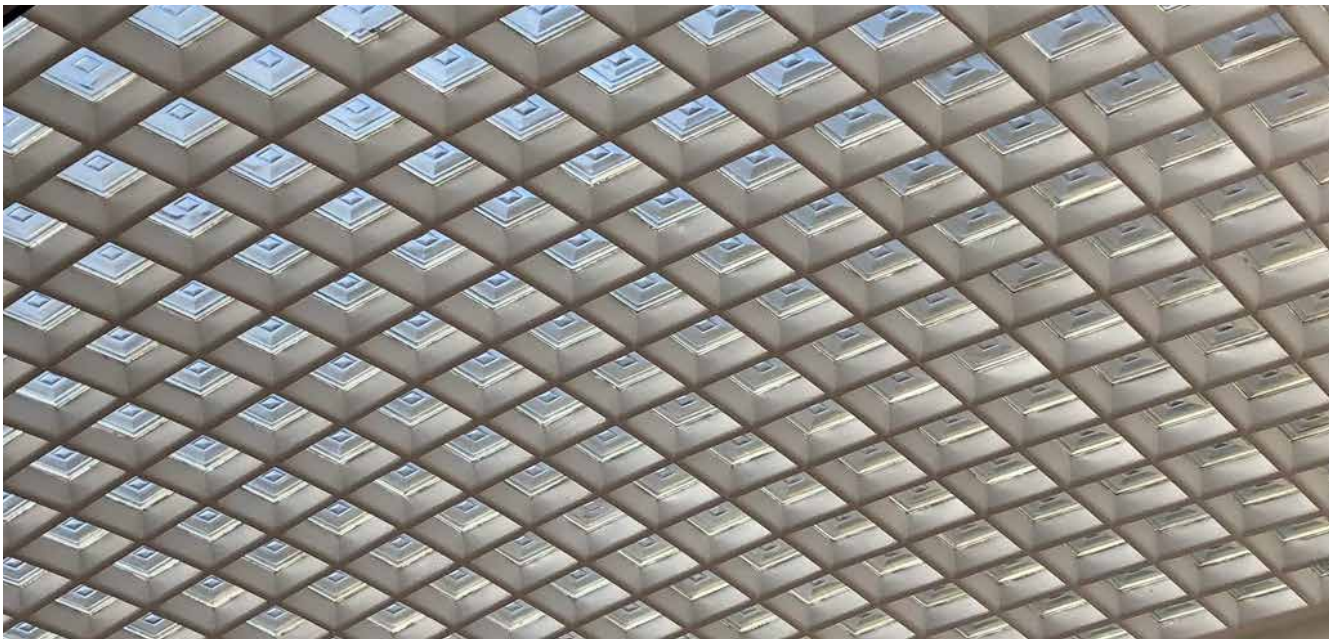
Adam Zibak and Andrew Simpson. 2018. Can We Evaluate the Effectiveness of Cyber Security Information Sharing Efforts?. In Proceedings of the 2018 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (CyberSA 18). IEEE.

Adam Zibak and Andrew Simpson. 2019. Towards Better Understanding of Cyber Security Information Sharing. In Proceedings of the 2019 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (CyberSA 19). IEEE.

Adam Zibak and Andrew Simpson. 2019. Cyber Threat Information Sharing: Perceived Benefits and Barriers. In Proceedings of The 14th International Conference on Availability, Reliability and Security (ARES 2019). ACM.

Mini-Project: When You Lose, Do Not Lose the Lesson: A Case Study on The Sony Pictures Entertainment 2014 Data Breach

Mini-Project: Conceptual Pipelines for the Access-data Centric Approach to Open Source Intelligence (in collaboration with Horus Security Consultancy)



CDT16 Bios

Angeliki Aktypi

Supervisor: Kasper Rasmussen, Department of Computer Science

Angeliki holds a Diploma (M.Eng. equivalent) in Electrical and Computer Engineering from the Democritus University of Thrace (Greece, 2014). She received her M.Sc. in Communications & Computer Security jointly delivered by Telecom ParisTech and Eurecom (France, 2014), as a 'VRIka!' Scholar of the French Embassy in Greece. She was enrolled at the Centre for Doctoral Training in Cyber Security, at the University of Oxford in 2016 as a Linacre College student member, funded by the EPSRC. After completing her training year, she joined the Department of Computer Science, under the supervision of Prof. Kasper Rasmussen. During her studies, she has pursued internships at British Telecom (the U.K., 2014), at Thales (France, 2016) and at ICS-FORTH (Greece, 2020), all focused on security research topics. Her DPhil thesis focuses on the design of secure and decentralised protocols for the communication of entities in the IoT domain and is partially supported by a Russel Group Studentship by British Telecom.

DPhil Thesis: Discovery of and Access to Resources between Entities within IoT Systems

The rapid increase in the use of connected devices (e.g., wearables, smart locks) and cloud applications (e.g., collaboration platforms, big data tools) established trends for a fully programmed and distance manageable lifestyle and shifted the character of the society to be open and network-oriented. The proliferation on connectivity combined with the increase in cyber-crime and the terrorism expansion in cyber space have created an urgent need to rapidly advance our security countermeasures and re-think of traditional approaches. Recognising this need, this DPhil thesis is going to explore and propose the deployment of security infrastructures in connected environments, many times referred to as the Internet of Things. In particular, the objective is to develop secure and resilient to attacks protocols that enable effective discovery and access to resources between entities within IoT systems. Entities include devices (such as sensors, actuators, embedded systems), but also include software-only virtual entities (such as virtual service instances in a cloud or fog computing context).

Publications

SeCaS: Secure Capability Sharing Framework for IoT Devices in a Structured P2P Network, Angeliki Aktypi, Kubra Kalkan and Kasper B. Rasmussen, In 10th ACM Conference on Data and Application Security and Privacy (CODASPY '20). Pages 271–282. ACM. March, 2020.

Unwinding Ariadne's Identity Thread: Privacy Risks with Fitness Trackers and Online Social Networks, Angeliki Aktypi, Jason R.C. Nurse and Michael Goldsmith, In 1st International Workshop on Multimedia Privacy and Security in conjunction with the 24th ACM Conference on Computer and Communication Security (CCS'17). ACM. October, 2017.

John Gallacher

Supervisor: Joss Wright, Oxford Internet Institute

John is a DPhil student within the University of Oxford's Cyber Security Centre for Doctoral Training. His research focuses on investigating the causes of online polarisation, ranging from aggressive intergroup contact, the spread of extremist material and hostile interference from foreign states. He is based within the Oxford Internet Institute and the Department for Experimental Psychology under the supervision of Dr Joss Wright, Dr Jonathan Bright and Dr Marc Heerdink.

John's work combines analytic methods drawn from computer science (machine learning, natural language processing and network science) with insights from experimental psychology and open source information from social media in order to measure how groups interact online, and how this relates to real world events.

He holds a BA in Experimental Psychology from the University of Oxford, and worked previously as a security consultant.

DPhil Thesis: The Security Implications of Online Intergroup Contact

This project will use a range of well-established psychology analysis techniques combined with novel analytical methods (machine learning, network analysis, text analysis, and others) to investigate the effects of online intergroup contact in natural settings, discover what conditions are necessary for positive outcomes, and test whether these conditions are being met by groups that have the potential to become security threats to society across the globe. I first aim to investigate the effect of intergroup interaction online between opposing political groups, and how this effects the extent of physical violence when these groups interact in the real world. Following this, I will investigate how the anonymity provided by internet applications affects groups dynamics, both within and between groups, before moving to investigate the effects of echo-chambering within the broader internet echo system and how this can be manipulated. Finally, I propose an experimental study of the effects of exposure to digital information and propaganda on implicit group associations in a range of individuals.

The application of established psychological methods to address these emerging online questions is highly novel and has real potential to shed light on a range of currently poorly understood phenomena.

Publications

Gallacher, J.D., & Heerdink, M., (2019) Measuring the effect of hostile information operations: a case study of Russian Internet Research Agency interference in online conversations Defence Strategic Communications, 6, 155-198

Gallacher, J.D., Heerdink, M. & Hewstone, M., (2018) Online engagement between opposing extremist political groups predicts physical violence of offline encounters Under Review – Nature Human Behaviour

Gallacher, J.D., & Fredheim, R., (2018) Division aboard, cohesion at home: How the Russian troll factory works to divide societies overseas whilst spreading pro-regime messages to domestic audiences. Responding to Cognitive Security Challenges, Chapter 5, NATO Strategic Communications Centre of Excellence

Fredheim, R., & Gallacher, J.D., (2018) Robotrolling 3/2018. NATO Strategic Communications Centre of Excellence

Gallacher, J.D., Barash, V., Howard, P.N., & Kelly, J,. (2017) Junk News on Military Affairs and National Security: Social Media Disinformation Campaigns Against US Military Personnel and Veterans. Data Memo 2017.9. Oxford, UK: Project on Computational Propaganda

Gallacher, J.D., (2019) Automated Detection of Terrorist and Extremist Content. Extreme Digital Speech: Contexts, Responses, and Solutions. VoxPol Network of Excellence for Research in Violent Online Political Extremism (In press)

Mini-Project 1: Information Warfare and Computational Propaganda

Mini-Project 2: Violent Political Extremism and Intergroup Contact Online

Munir Geden

Supervisor: Kasper Rasmussen, Department of Computer Science

Before steering into a research-based career, Munir worked for more than five years as a software engineer in financial IT industry, after receiving his BSc in Computer Engineering followed by MSc in Engineering and Technology Management from Bogazici University (Istanbul).

He came to the UK for pursuing another master's degree in Software Systems Engineering at UCL with a research and security focus which brought him to Oxford to gain a better understanding of cyber-security by employing an interdisciplinary perspective.

In addition to previous interest in malware analysis via both static and dynamic techniques, he is currently working on the detection of runtime attacks exploiting memory bugs in a remote context.

DPhil Thesis: Remote Attestation of Runtime Behaviours

Most remote attestation techniques ensure only the load-time integrity of applications by applying checksum functions on static code regions. However, these static techniques cannot catch runtime attacks (e.g., code-reuse, non-control data attacks) that operate on dynamic memory regions such as stack or heap areas. To take the runtime attestation a step forward, I am working on an attestation scheme that checks the compliance of dynamic properties collected at runtime with the static features extracted from the code in advance.

Publications

"Ngram and Signature Based Malware Detection in Android Platform", Master's thesis supervised by Dr. Jens Krinke, UCL

Geden, M. and Happa, J., 2018, October. "Classification of Malware Families Based on Runtime Behaviour". In 11th International Symposium on Cyberspace Safety and Security (pp. 33-48). Springer, Cham.

Geden, M. and Rasmussen, K., 2019, August. "Hardware-assisted Remote Runtime Attestation for Critical Embedded Systems. In 2019 17th Annual Conference on Privacy, Security, and Trust (PST), IEEE.

Faisal Hameed

Supervisors: Sadie Creese, Michael Goldsmith and Ioannis Agrafiotis, Department of Computer Science

A seasoned cybersecurity professional with a track record of (15 years +) experience spanning various engineering, consulting and management CISO entities. Working in diverse environments from promising start-ups to international organizations (The World Bank Group, ExxonMobil, E&Y, HP, Unilever, UK Gov) to. B.Sc in CS, M.Sc in Information Security and Assurance from the States.

Faisal's research interests are in national and international security capacity building and maturity models.

DPhil Thesis: Formalising an outline around risk assessments for national critical infrastructures.

Most remote attestation techniques ensure only the load-time integrity of applications by applying checksum functions on static code regions. However, these static techniques cannot catch runtime attacks (e.g., code-reuse, non-control data attacks) that operate on dynamic memory regions such as stack or heap areas. To take the runtime attestation a step forward, I am working on an attestation scheme that checks the compliance of dynamic properties collected at runtime with the static features extracted from the code in advance.

Publications

Mini-Project: Disrupting Trust in CyberCriminal Marketplace

In publication: What Really Works: Analysing Trends and Success Factors in International Cybersecurity Capacity Building Initiatives

Manuel Hepfer

Supervisors: Thomas Powell and Thomas Lawrence, Saïd Business School

Manuel Hepfer is a doctoral student at Oxford University, studying in the Said Business School under the supervision of Professors Thomas C. Powell and Thomas B. Lawrence. His research focuses on the resilience of organizations in the empirical context of cybersecurity.

Manuel's academic background combines the areas of computer science and business administration. After graduating from Reutlingen University (Germany) top of his class with a bachelor's degree in Business Informatics in 2015, he pursued his education at the London School of Economics, where he graduated in 2016 with Distinction in Management, Information Systems, and Digital Innovation.

After gaining experience during practical placements in management consultancies (PricewaterhouseCoopers, Audi Consulting) and large corporations (Porsche Financial Services, Robert Bosch GmbH), Manuel started his Doctoral degree at Oxford University. Manuel provides tutorials to undergraduate students and students on Diploma programs that are part of Saïd Business School's executive education. He also works regularly as a teaching assistant, currently for the MBA course on Big Data.

During his studies, Manuel has been actively involved in extracurricular activities, for example as a student ambassador during his time at the London School of Economics, and as an active player and committee member in the Oxford University Volleyball Club. Manuel is also a founder and director of OxSecure, a not-for-profit consultancy that provides pro-bono cybersecurity advice to charities, social enterprises, and other not-for-profit organizations.

DPhil Thesis: Organisational Resilience: The Case of Cybersecurity

Manuel is interested in the resilience of organizations facing adversity. Despite decades of research, key elements of organizational resilience remain poorly understood. The purpose of Manuel's research is to advance the study of organizational resilience.

Manuel works on three research projects.The first research project reviews and integrates literature on organizational resilience published in leading business and management journals. The second research project is an empirical study that explores the cognitive foundations of organizational resilience in the context of cybersecurity, comparing how three global organizations have responded differently to the same cyberattack. The third research project enhances our practical understanding of organizational resilience by showing how executives can improve their organizational resilience to cyberattacks and capture strategic opportunities before and after a cyberattack occurs.

Publications

Hepfer, M., Powell, T.C., "How to Make Cybersecurity a Strategic Asset." MIT Sloan management review (2020).

Monica Kaminska

Supervisor: Lucas Kello, Department of Politics and International Relations

Monica studied International Relations at LSE for her bachelor's degree and, during this time, undertook internships at the Foreign and Commonwealth Office and in the business intelligence sector. She then moved to Cambridge to pursue an MPhil in Geographical Research. After graduating she worked in the financial sector, advising private equity funds and strategy consultancies. Given her background in the social sciences, she is particularly interested in the impact of cyber threats on international security. During her first year at the CDT, Monica undertook a mini-project at the Oxford Internet Institute where she co-authored two research memos on computational propaganda and social media activity during the 2017 UK General Election. She also presented the research at the Global Legislative Openness Conference in Kiev, Ukraine and the International Bar Association Conference in Sydney, Australia.

DPhil Thesis: Restrained responses: explaining the puzzle of lack of meaningful and proportionate punishment for major offensive cyber operations.

States struggle to punish cyber actions that are highly damaging to national interests yet fail to meet the threshold of armed attack. The "risk society" perspective in international relations theory raises questions about whether deterrence via punishment is the rationally effective recourse in such situations. Western policymakers have used risk management to evaluate the emerging security environment and security risks of the cyber domain – including

the properties of complex adaptive systems, the ease of proliferation, and collateral damage – leading to policies that seem to privilege responses other than punishment. Risk management involves reducing likelihoods of scenarios to a level deemed tolerable or as low as can reasonably be achieved; thus it often neglects punishment considerations. This thesis analyses and explains this Western policy attitude. It argues that the prevailing risk management framework underlies the failure to apply proportionate punishment and potentially more effective deterrent responses to cyberattacks.

Publications

Gallacher, J. D., Kaminska, M., Kollanyi, B., & Howard, P. N. (2017) Junk News and Bots during the 2017 UK General Election: What Are UK Voters Sharing Over Twitter? Data Memo 2017.5. Oxford, UK: Project on Computational Propaganda

http://comprop.oii.ox.ac.uk/2017/05/31/junk-news-and-bots-during-the-2017-uk-general-election/

Kaminska, M., Gallacher, J.D., Kollanyi, B., Yasseri, T., & Howard, P. N. (2017). Social Media and News Sources during the 2017 UK General Election. Data Memo 2017.6 Oxford, UK: Project on Computational Propaganda

http://comprop.oii.ox.ac.uk/2017/06/06/social-media-and-news-sources-during-the-2017-uk-general-election

Gallacher, J. D., & Kaminska, M., (2017) Facebook needs to be more open about its effect on democracy. The Guardian

https://www.theguardian.com/commentisfree/2017/jun/12/general-election-social-media-facebook-twitter?CMP=soc_3156

Collier, J., & Kaminska, M., (2017) Bashing Facebook is not the answer to curbing Russian influence operations. Council on Foreign Relations.https://www.cfr.org/blog/bashing-facebook-not-answer-curbing-russian-influence-operations

Mini-Project: Computational Propaganda and the 2017 UK General Election

Mini-Project: Why is retaliation against offensive Russian cyber actions generally so difficult? A comparison of past responses from Estonia, Germany and the US.

Martin Kraemer

Supervisor: Ivan Flechais,
Department of Computer Science

Martin is a 4th year DPhil student at the Department of Computer Science working on privacy in smart homes with Ivan Flechais and Helena Webb. He is particularly interested in improving privacy by design through a deep understanding of communal and digital privacy practices of using 'smart' (internet-connected) devices.

Before coming to Oxford, Martin graduated with an MSc in Computer Science (distinction) from The University of Edinburgh, has previously worked as consultant with SAP and holds a BSc in Business Information Systems from Duale Hochschule Badenwurttemberg (Mannheim).

DPhil Thesis: Empowering Users' Privacy Practices in Smart Homes

The increase in data collection in our homes is fuelled by the emergence of internet-connected devices. These devices are designed to transfer, process, and disseminate data which becomes a pivotal part of the relationship between technology providers and households. However, reactions to events revealing manufacturers' practices and attitudes show a misalignment of expectations. Ultimately damaging the relationship, these issues are often referred to in the context of privacy.

Previous empirical privacy research has been carried out in other technological contexts or from risk management, system, and network perspectives in the home. Most of these studies were limited to temporary accounts of individuals. In the home, traditionally considered as one of the most private spaces, technology overlaps established social structure and related practices. Technology becomes communal, to some extent used by the community of the household rather than a single individual.

This thesis disentangles communal privacy practices in smart homes in three steps: an initial mixed method exploration of communal smart home technology use; a longitudinal, ethnographic study of communal privacy practices with 5 households; and the development of design artefacts for smart homes to share our insights but also as a tool for future design practice.

Publications

Flechais, I., Krämer, M., & Seymour, W. Responsibility and privacy: Caring for a dependent in a digital age. This paper was presented at the CHI 2020 Networked Privacy Workshop: Privacy and Power: Acknowledging the Importance of Privacy Research and Design for Vulnerable Populations, 26 April 2020 (Virtual workshop).

William Seymour, Martin J. Kraemer, Reuben Binns, and Max Van Kleek. 2020. Informing the Design of Privacy-Empowering Tools for the Connected Home. In Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (CHI '20). Association for Computing Machinery, New York, NY, USA, 1–14.

Martin J. Kraemer, Ulrik Lyngs, Helena Webb, and Ivan Flechais. 2020. Further Exploring Communal Technology Use in Smart Homes: Social Expectations. In Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems (CHI EA '20). Association for Computing Machinery, New York, NY, USA, 1–7.

Martin J Kraemer, Ivan Flechais, and Helena Webb. 2019. Exploring Communal Technology Use in the Home. In Proceedings of the Halfway to the Future Symposium 2019 (HTTF 2019). Association for Computing Machinery, New York, NY, USA, Article 5, 1–8.

Kraemer, M.J., Seymour, W., Binns, R., Van Kleek, M., & Flechais, I. (2019). Informing the future of data protection in smart homes. Presented at the CHI'19 Workshop on New Directions for the IoT: Automate, Share, Build, and Care.

MJ Kraemer. Preserving Privacy in Smart Homes: A Socio-Cultural Approach. Proceedings of Conference Extended Abstracts on Human Factors in Computing Systems (CHI), ACM, 2018

MJ Kraemer, I Flechais. Researching Privacy in Smart Homes: A Roadmap of Future Directions and Research Methods. Living in the Internet of Things: Cybersecurity of the IoT Conference, IET, 2018.

MJ Kraemer, J Happa, S Creese. Exploring the Relationship between Residual Risk

Awareness and Cyber Security Posture - A qualitative study on the state of cyber security in large enterprises. Technical Paper. 2018.

Krämer, Aspinall, Wolters. POSTER: Weighing in eHealth Security - A Security and Privacy Study of Smart Scales. Proceedings of the 23rd ACM SIGSAC Conference on Computer and Communications Security, ACM, 2016

Andikan Otung

Supervisor: Andrew Martin, Department of Computer Science

Andikan studied Electronic & Electrical Engineering (MEng) at UCL, where he graduated on the Dean's list. After graduation, Andikan began a career in telecommunications, working in London as a Sales Engineer for Ciena - a multibillion dollar networking-infrastructure vendor. As well as (officially) becoming an inventor, Andikan developed an increasing interest in Security, through his work on the government side of sales operations.

As the more perceptive of readers may have already gathered, Andikan is both technically and commercially minded. His interests reflect this and include: IoT Security, Trusted Computing, DDoS, Cryptography, Multi-factor (including location-based) Authentication as well as commercial strategies enabling the fast creation and adoption of new technologies.

Arianna Schuler Scott

Supervisors: Sadie Creese, Michael Goldsmith and Helena Webb, Department of Computer Science and Harriet Tear, Centre for Health, Law and Emerging Technologies

Arianna is a DPhil student working within the Cyber Analytics Group under Professor Sadie Creese, supervised by Professor Michael Goldsmith. Her work on dynamic consent and data protection compliance is co-supervised by Dr Helena Webb, whose focus lies with Human Centred Interaction in the Department of Computer Science, and Dr Harriet Teare, Research Leader at RAND Europe.

Arianna's work draws together data-protection, privacy and consent to answer whether consent mechanisms can be put to use as a way to protect privacy. This is because Arianna believes that users should find saying "maybe" (or even "no") to online data-use should be as easy as saying "yes". There are two parts to Arianna's work - guidelines for how choice can be presented to users, and communication strategies enabling these choices to be informed. This "choice architecture" is designed for informed consent processes that exist over time, and must allow people to change their minds.

DPhil Thesis: Dynamic Consent: a mechanism for privacy control?

Telling people how their data has been (or will be) used is more likely to engender engagement and build trust than overloading them with information they do not understand. This applies to consent because "informed" consent has slowly become "inundated" consent where people are expected to make decisions based on an overwhelming amount of information. Informed consent was initially developed to prevent physical harm, but the harms caused by data-abuse, such as profiling and surveillance are less tangible. As research moves online, the problems around consent remain, but the environment is unfamiliar territory for many researchers.

A dynamic form of consent has been proposed for online research environments. This "dynamic consent" lets people change their mind about taking part, provides feedback on the project, and shows further opportunities for engagement. Arianna is evaluating dynamic consent by interviewing researchers and participants involved in a project that uses it. Drawing from participant and researcher consultations, Arianna is developing practical guidelines for implementing dynamic consent that focus on two components. The first is that participants must be allowed to shape their research involvement by choosing how they want their personal data to be used. The second is that researchers must report project development and results, providing information on opportunities for further participation.

Publications

Schuler Scott, A., Goldsmith, M., Teare, H., Webb, H. & Creese, S., 2019. Why We Trust Dynamic Consent to Deliver on Privacy. In Trust Management XIII: 13th IFIP WG 11.11 International Conference (IFIPTM) Proceedings, vol. 563, p. 28. Springer Nature.

Schuler Scott, A., Goldsmith, M. and Teare, H., 2018. Wider Research Applications of Dynamic Consent. In IFIP International Summer School on Privacy and Identity Management Proceedings, pp. 114-120. Springer, Cham.

Schuler Scott, A., Goldsmith, M., Teare, H., Creese, S. and Kaye, J., 2018. Dynamic Consent in Cybersecurity for Health. In Int'l Conf. Health Informatics and Medical Systems (HIMS'18). CSREA Press.

Talks

2020) "RE: I've been forced to sign this and I am not happy", a 20-minute talk addressing the recent upheaval in European data-handling and its impact on privacy awareness.

(2020) "Protecting ourselves online: Why we shouldn't take cookies from strangers", a 20-minute public engagement exercise focusing on data use and institutional responsibility.

(2020) "Designing responsible, participatory research", a 15-minute talk to CDT students about designing and implementing research methods.

(2019) Developed, coordinated and ran "Cybersecurity in Context" at the CDT, a module designed to teach technical skills and explore causes and responses to cybersecurity events. Topics covered: forensics, binary exploitation, web attacks and a cyber crisis simulation.

Impact

(2020) Protecting User Data as a Software Developer, Computer Science Department, UNIQ Summer School. 2 hours, online, 30 sixth-form students.

(2019) Cybersecurity in Context, Centre for Doctoral Training in Cyber Security. 4 days, in-person, 13 PhD students.

(2018) Cyber Crisis Simulator, Centre for Doctoral Training in Cyber Security. 2 days, in-person, 13 first-year PhD students.

William Seymour

Supervisor: Max van Kleek, Department of Computer Science

William's research focuses on ethical human-computer interaction in the smart home. With a background in computer science, he frequently designs and develops prototypes for use in research experiments. His work also includes the use of speculative and fictional design to probe beyond the edges of what is possible with today's technology.

DPhil Thesis: Informing the Design of Privacy-Empowering Tools for the Connected Home

The home is an essential private space in people's lives, providing safety and isolation from the outside world. After decades of existence in popular imagination, the notion of a 'smart home' as a domestic space enriched with connected digital devices is gradually becoming a reality. The connected home of science fiction was one that promised a new way of living, allowing people to pursue more efficient, safer, and fulfilled lives, built on the assumption that this new technology would respect existing social conventions around privacy, autonomy, and the social order of the home. But this is still far from being realised, with devices routinely collecting data on people and activities within the home, often ignorant of the relationships and power dynamics that exist between cohabitants.

The primary goal of my thesis is therefore to inform the design of privacy-empowering tools for the smart and connected homes. To this end, my research will inform a design philosophy for devices that addresses the current major ethical concerns with them, and is flexible enough to adapt to new technologies and concerns as they arise. This begins with an understanding of what smartness is perceived to be from the perspective of end users, and the associated ethical concerns generated by smartness. Focussing on privacy specifically, I explored the design space for privacy-empowering technologies in the home through the deployment of a technology probe. Over six weeks the probe showed how people can be supported in forming and acting on privacy preferences, effectively retrofitting good behaviour onto existing devices. Finally, I use insights from the philosophical literature on respect to create design guidelines for future smart devices. These guidelines are explored through the creation of a variety of fictional and speculative design artefacts.

Publications

Informing the Design of Privacy-Empowering Tools for the Connected Home. W. Seymour, M. J. Kraemer, R. Binns, and M. Van Kleek. Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems.

Strangers in the Room: Unpacking Perceptions of 'Smartness' and Related Ethical Concerns in the Home. W. Seymour, R. Binns, Petr Slovak, M. Van Kleek, and N. Shadbolt. Proceedings of the 2020 ACM Conference on Designing Interactive Systems.

Does Siri Have a Soul? Exploring Voice Assistants Through Shinto Design Fictions. W. Seymour, and M. Van Kleek. Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems (alt.CHI).

Privacy Therapy with Aretha: What if your firewall could talk? W. Seymour. Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems (Graduate winner, SIGCHI Student Research Competition)

Marcel Stolz

Supervisors: Michael Goldsmith, Department of Computer Science and Lucas Kello, Department of Politics and International Relations

Marcel first became aware of security and defence matters during his military service in the Swiss army, serving as an officer (first lieutenant) in the electronic operations unit. During Marcel's Bachelor's and Master's studies at the University of Bern, he gained insights into political work as member of the university's TUX party, discussing topics such as privacy. Marcel subsequently worked with Swisscom, Switzerland's national phone operator, in the Big Data Mobility Insights Squad.

Marcel's current interest lies in combining his technical knowledge with his interests in politics and history. He explores aspects of state, net and platform neutrality, how it can be implemented in cyberspace, and what capabilities a neutral nation should build up in cyberspace. Furthermore, he collaborates on projects with FIIA on European strategic autonomy (including the current 5G & Huawei discussion) and a cybersecurity capacity assessment of Switzerland with the Global Cyber Security Capacity Centre at the Oxford Martin School.

DPhil Thesis: Neutrality in Cyberspace

Publications

Conference Paper Publication: On Neutrality and Cyber Defence. ECCWS 2019

Current project: Technical Aspects of the 5G debate (currently being prepared as a collaborative publication with FIIA)

Mini-Project: Neutrality and Cyber Defence

Mini-Project: Assessing Risks from Wearable IoT Devices in a Military Context (currently being prepared for publication in a Journal)

Oleh Stupak

Supervisors: Greg Taylor, Oxford Internet Institute and Aleksei Parakhonyak, Department of Economics

Oleh holds MSc in Economics from Paris 1 Pantheon-Sorbonne (France) and BSc, MA degrees in International Economics from Taras Shevchenko National University of Kyiv (Ukraine). Alongside with academia, he obtained more than six years of experience in private sector. Three of which, Oleh held a CEO position in the self-founded company "thelamp". The company was a projection of his curiosity to the innovative technologies. It provided a full range of IT services and specialised on the tailoring of unique software solution for commercial and governmental purposes.

His MSc thesis in Paris 1 was devoted to the research on DDoS (distributed denial-of-service) attack risk for industries. The model developed during that period is capable of calculating the enterprises' chance of being the subject of DDoS attack considering 25 economic and technical parameters.

Oleh is convinced that the future stands in interdisciplinary approaches and cooperation among schools. His desire for knowledge and world outlook brought him to Oxford's CDT in Cyber Security. Currently, Oleh focuses on the emerging cyber security threats for enterprises. His broad area of interests includes: enterprises behaviour and unfair competition in the information environment, cyber security risks.

DPhil Thesis: The Economics of Industrial Cyber Espionage

Publications

Mini-Project: Unfair Competition in the information environment. Industrial information leakage

Mini-Project: Unfair Competition in the information environment. The DDoS attack

Jack Sturgess

Supervisor: Ivan Martinovic, Department of Computer Science

Jack graduated from the University of Surrey with a BSc (Hons) in Mathematics and an MSc (Dist.) in Information Security. He worked as a software engineer at Accenture for 1 year and at IBM for 5 years; he also co-founded a video games company, while at IBM, that released two titles on PlayStation Network and one on Steam. An avid traveler, Jack volunteered as a conservationist in Arizona and California after his first degree, camping and working in the middle of nowhere while enjoying fantastic landscapes! His interests also include programming, board-gaming, hiking, and number theory.

Jack's research interests include authentication, biometrics, steganography, and the Internet-of-Things. Being part of the CDT has

proven to be an excellent way to study the interweave of these subjects and to understand their implications across other disciplines.

DPhil Thesis: Wearable Authentication Using Inertial Sensors

Publications

Sturgess, J., & Martinovic, I., "VisAuth: Authentication over a Visual Channel using an Embedded Image", Cryptology and Network Security (CANS) 2017

Sturgess, J., Nurse, J. R. C., & Zhao, J., "A Capability-oriented Approach to Assessing Privacy Risk in Smart Home Ecosystems", PETRAS 2018

Olivia Sturrock

Supervisor: Andrew Martin, Department of Computer Science

With a background in Economics, Olivia first studied computer science at Liverpool University graduating with a MSC in Advanced Computer Science and Internet Economics. Her dissertation for this, in ontological meaning negotiation between agents, led to key interests of multi-agent systems, agent negotiations and how these subjects can be applied to cybersecurity.

MPhil Project: Smart Cities: Security Implications of Smart Critical Infrastructure

Looking at how the development of Smart Cities and the related technology could affect the security of the city.

Publications

Mini-Project: The Changing Security Needs for Distributed Energy Generation in the UK

Valentin Weber

Supervisors: Lucas Kello, Department of Politics and International Relations and Joss Wright, Oxford Internet Institute

Valentin is a Research Affiliate with the Centre for Technology and Global Affairs, University of Oxford. Previously, he was an Open Technology Fund Senior Fellow in Information Controls at the Berkman Klein Center for Internet & Society, Harvard University. Valentin is interested in how the cyber domain is changing conflicts and state strategies. His current research focuses on the role of information controls in state strategies.

DPhil Thesis:The diffusion of cyber norms: technospheres, sovereignty, and power

My thesis studies the proliferation of the internet sovereignty and internet freedom norms. It researches the United States, China, and Russia, which are the main norm promoting countries in cyberspace.

Publications

"Making Sense of Technological Spheres of Influence." Strategic Update. LSE IDEAS. April 2020.

"The Sinicization of Russia's Cyber Sovereignty Model." Net Politics - Council on Foreign Relations. 1 April 2020.

"Studying Information Control Diffusion: An Agenda for Further Research." Open Technology Fund. February 2020.

"Understanding the Global Ramifications of China's Information Controls Model." in Artificial Intelligence, China, Russia, and the Global Order: Technological, Political, Global, and Creative Perspectives. Air University Press. October 2019.

"The Worldwide Web of Chinese and Russian Information Controls." Working Paper. Centre for Technology and Global Affairs. September 2019.

"The Worldwide Web of Chinese and Russian Information Controls." Report. Open Technology Fund. September 2019.

"中国和俄罗斯信息 控制的全球网." Report. Open Technology Fund. September 2019.

"Всемирная паутина российского и китайского контроля за информацией." Report. Open Technology Fund. September 2019.

"Future of Global Competition and Conflict Virtual Think Tank Report." NSI. September 2019.

Vasilis Ververis, Marios Isaakidis, Valentin Weber, and Benjamin Fabian. "Shedding Light on Mobile App Store Censorship." In Proceedings of the 27th Conference on User Modelling, Adaptation and Personalization Adjunct. June 2019. Larnaca, Cyprus. ACM, New York, NY.

Valentin Weber and Vasilis Ververis. "Measuring Censorship on Mobile App Stores." OxPol. 3 May 2019.

"Finding a European Response to Huawei's 5G Ambitions." Norwegian Institute of International Affairs. March 2019.

"A Bold Proposal for Fighting Censorship: Increase the Collateral Damage." Net Politics - Council on Foreign Relations. 31 January 2019.

"Understanding the Global Ramifications of China's Information Controls Model." in AI, China, Russia, and the Global Order: Technological, Political, Global, and Creative Perspectives. White Paper for the Joint Chiefs of Staff. January 2019.

"Linking Cyber Strategy with Grand Strategy: The Case of the United States." Journal of Cyber Policy. 2018.

"States and Their Proxies in Cyber Operations." Lawfare. 15 May 2018.

"The Rise of China's Security-Industrial Complex." Net Politics - Council on Foreign Relations. 17 July 2018.

"Why China's Internet Censorship Model Will Prevail Over Russia's." Net Politics - Council on Foreign Relations. 12 December 2017.

Oxford University Competitive Computer Security Society

Sebastian Köhler, CDT18

Last November, the Oxford University Competitive Computer Security Society elected a new committee. We want to thank the previous committee for their excellent work that lead to the continuous success of this society. The new committee is composed of Sebastian Köhler as President, Marine Eviette as Secretary, Yashovardhan Sharma as Treasurer, George Chalhoub as IT-Officer/ Webmaster, Freddie Barr-Smith as Outreach Officer and Anjuli Shere as Recruitment Officer.

In Michaelmas, we started to run a new format of weekly sessions with topics ranging from Cryptography to AntiVirus Evasion. Instead of just solving traditional Capture-the-Flag challenges, we split the courses in a theoretical and a practical part. The theory of the first half was directly applicable to the practical exercises in the second half. The main reason for changing the format was to make it easier for students that haven't gained any previous experience in solving CTF challenges to join and participate.

While traditional Capture-the-Flag challenges are a lot of fun, they are often not realistic. We also wanted to give the students the opportunity to work on more realistic scenarios and challenges as we see them in the real world. Therefore, we created a team on HackTheBox, an online platform for penetration testing that offers access to a large network of vulnerable computers. The goal is to earn points by exploiting these vulnerabilities, gaining access to the computer and finding the flag.
Unfortunately, the pandemic didn't allow us to continue our weekly meetings and to participate in in-person events. Nevertheless, we still take part in online competitions. For example, some members of the society participated in the qualifiers of this year's Space Security Challenge "Hack-a-Sat", organised by the United States Air Force. In contrast to traditional Capture-the-Flag challenges, the event offered a wide variety of problems directly related to astronomy, astrophysics, astrometry and satellite communication systems. The challenges ranged from reverse engineering parts of a real-time operating system (RTOS), that often runs on satellites, to solving complex orbital mechanics calculations. Even though the team was not able to qualify for the final held at this years DEF CON, the team placed 39th out of 1600 participating teams.

We are currently working hard on future events with a series of different topics, including but not limited to hardware hacking and wireless protocol security. We want to take this opportunity to thank the Centre for Doctoral Training in Cyber Security for their continuous support! We are looking forward to an exciting time ahead. In the meantime - stay healthy and keep hacking!

Remote Covert-Channel Attacks on Field-Programmable Gate Arrays

Ilias Giechaskiel, CDT14

1 Introduction

Field-Programmable Gate Arrays, or FPGAs, are integrated circuit (IC) chips which are composed of primitives called lookup tables (LUTs); memory elements, such as flip-flops (FFs); and routing wires that connect these blocks together. Unlike other ICs, however, the physical connections within FPGAs are reconfigurable. This means that the lookup tables can be programmed to represent different logic functions, such as `AND`, `NOT`, or `XOR`, and chained together in different ways. These logic gates form Boolean circuits, which can represent pure functions, whose outputs depend only on their inputs (*combinational logic*). By introducing memory elements, the circuit can keep track of past state, allowing for the design of *sequential logic* and finite state machines.

Figure 1 shows a picture of an Artix 7 FPGA chip mounted on a Nexys 4 DDR board. Although the FPGA chip may look like any other chip, the circuits that can be implemented on it are surprisingly powerful: it is possible to create entire general-purpose CPUs on FPGAs, all while designing other parts of the FPGA logic to perform specialized tasks simultaneously. This flexibility and parallelization can produce high-bandwidth, low-latency circuits that are used, among other things, in genomic sequencing, cryptography, financial modeling, post-decay particle detection, and the replacement of network cards and Solid-State Drive (SSD) controllers. FPGAs have thus not only permeated distributed systems and critical infrastructure, but they are also often integrated in consumer electronics, such as smartphones and laptops. It is therefore necessary to ensure that their computations are performed in a trustworthy manner.

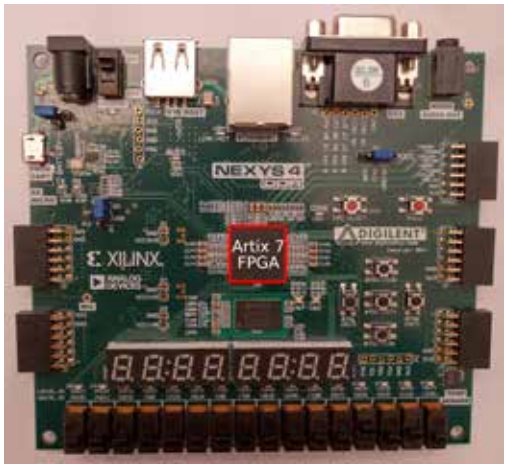


Figure 1: An Artix 7 FPGA chip on a Nexys4 DDR board. Lookup tables, flip-flops, and long wires are some of the resources in the FPGA chip, outlined in red.

Many types of attacks on FPGAs are possible. Some focus on reverse engineering the code that is running on the FPGA chips. Others assume that the adversary has physical access to the hardware, and can manipulate voltage and temperature conditions, for instance to cause faults in calculations or bias the randomness generated for cryptographic operations. However, another class of remote attacks has recently surfaced, and targets multi-tenant FPGAs, where two or more users share parts of the reconfigurable fabric.

Although multi-tenant setups are not common at present, several proposals for virtualizing the underlying hardware have become popular, in part due to the growing size of the FPGA resources, and the emergence of cloud FPGA platforms, such as F1 instances on Amazon Web Services. These types of deployments prevent direct physical access to the underlying FPGA hardware. Remote covert-channel attacks on multi-tenant FPGAs formed the majority of my DPhil thesis, during which I introduced three novel communication mechanisms:

1. I first showed that certain types of routing resources within the FPGA chip, called *long wires*, leak information about their state in a way which can be measured fully on-chip.
2. I then demonstrated that isolating users to different physical dies (*super logic regions*, or *SLRs*) of the same FPGA chip is insufficient to prevent covert-channel attacks.
3. I finally introduced a new class of attacks between dedicated, single-tenant FPGA designs on commercial off-the-shelf boards.

In this article, I summarize the key insights behind these three contributions and discuss their implications for shared FPGA infrastructures, along with possible countermeasures.

2 Ring Oscillators

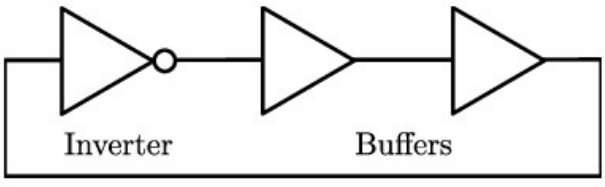


Figure 2: A Ring Oscillator (RO) with one inverter and two buffer stages.

The central primitive that makes remote attacks possible is a *Ring Oscillator*, or *RO*, which consists of an odd number of `NOT` gates (implemented using LUTs), chained together in a ring formation. In other words, the output

of the last gate is fed back as the input to the first gate, as shown in Figure 2. ROs form a loop whose output at any stage oscillates between 1 and 0 (true and false). The frequency of oscillation depends on the number of stages in the RO, the delay between the stages, as well as Process, Voltage, and Temperature (PVT) variations in the environmental conditions and the manufacturing process. The sensitivity of ROs to these variations makes them ideal for temperature and voltage monitors. At the same time, the dynamic switching activity of ROs can cause voltage drops within the FPGA, also making them suitable for covert-channel transmitters.

3 Long-Wire Leakage

FPGAs organize their logic resources including lookup tables and flip flops in a grid-like format within the chip, with different types of communication wires connecting elements between the various locations of the device. These wires have different orientations and lengths, and include *vertical long wires*, which can efficiently connect resources that are far apart and share the same *x* coordinate.

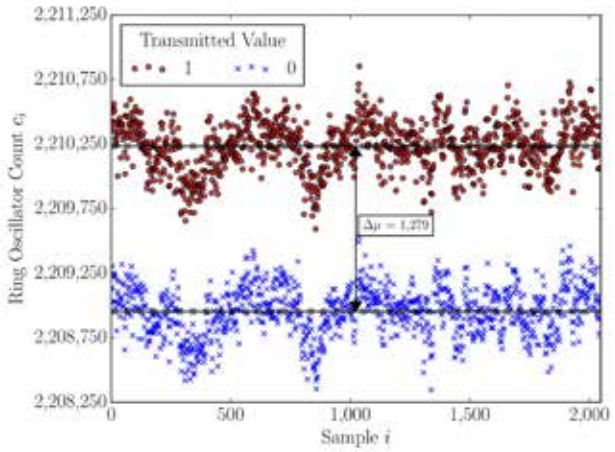


Figure 3: Ring oscillator counts when the victim long wires are carrying a 0 (blue crosses) are smaller than when they are carrying a 1 (red circles): the adversary can distinguish between the two possible states of the victim circuit using a simple threshold.

Vertical long wires, it seems, have unintended electrical properties that their shorter counterparts do not: if a long wire carries a logic 1, the delays of nearby long wires are slightly shorter than when it carries a logic 0. This difference in delay allows adversarial circuits sharing the same reconfigurable FPGA fabric to covertly communicate, even when they are not directly connected. Alternatively, it allows an attacker to eavesdrop on an unsuspecting victim circuit, and recover information such as key bits carried on the long wires. Figure 3 shows an example of the long-wire leakage, demonstrating that an adversary can use a ring oscillator to distinguish between the logic state of a nearby victim circuit using long wires: when the victim long wires are carrying a logic 1, the RO counts are higher than when the long wires are carrying a logic 0.

The long-wire leakage phenomenon is present in seven families of Xilinx FPGAs, spanning high-end devices from 2006 to ones introduced a decade later on public FPGA cloud infrastructures. Moreover, it persists even in the presence of other activity on the device, allowing an adversary to create a high-bandwidth covert channel (6kbps with 99.9% accuracy) between unconnected circuits. As a result, *potentially-adversarial logic needs to be physically isolated from other logic instantiated on the FPGA*. As the next section explains, isolation unfortunately is not enough.

4 Cross-Die Communications

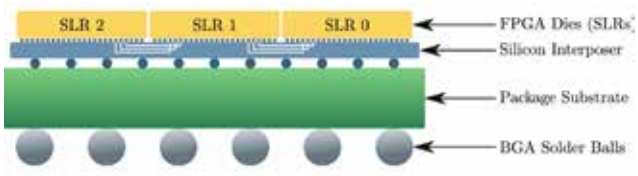


Figure 4: High-end FPGA chips are composed of multiple Super Logic Regions (SLRs), which are separate dies, connected and powered through the silicon interposer. Figure adapted from Xilinx User Guide UG872.

High-end FPGAs are made up of separate physical dies, called Super Logic Regions (SLRs), as shown in Figure 4. SLRs provide a natural way of partitioning different users to physically-isolated regions, but is such a partitioning mechanism enough to prevent cross-user information leakage in multi-tenant FPGAs? As it turns out, it is not: a user who enables many ring oscillators at once can cause a voltage drop that is measurable across the chip. This fact can be used to create a channel that has an even higher bandwidth than the long-wire one, reaching 4.6Mbps with 97.6% accuracy.

Deploying this covert channel on commercial cloud FPGAs requires overcoming some hurdles, as cloud providers detect and prohibit ring oscillators. However, replacing one of the LUT buffer stages with a flip-flop or a latch can hide the ring oscillator, and bypass such countermeasures.

In summary, cross-SLR information leakage can be exploited even on the cloud, and suggests that *current device architectures are unsuitable for multi-tenant cloud occupancy*. To put it differently, single-tenant setups are necessary for security. Are they sufficient, though? The title of the next section perhaps spoils the answer: even dedicated FPGA boards can be vulnerable to information leakage through their power supply!

5 Cross-FPGA Channels

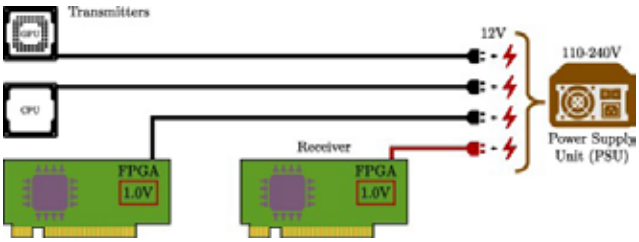


Figure 5: FPGA-to-FPGA, CPU-to-FPGA, and GPU-to-FPGA leakage in co-located environments. The devices are powered through the same PSU, but do not share any logic, and are physically unmodified.

Even if FPGA boards are allocated on a per-user basis, they still have to share some common infrastructure, including

their Power Supply Unit (PSU). And if one FPGA contains many ring oscillators, the dynamic activity of these ROs can cause a small (yet significant) voltage drop that is visible even at the power supply level. So, creating a transmitter is easy. But how can these voltage drops be detected by an entirely different FPGA sharing the same PSU?

Normally, the voltage regulator of the receiver FPGA would filter out these fluctuations. However, the receiver FPGA can strain its own voltage regulator by toggling *stressor* ring oscillators on and off. This allows the receiver FPGA to detect fluctuations caused by external activity not only of a transmitting FPGA, but also of CPUs and GPUs powered by the same PSU (Figure 5). In other words, *cross-board FPGA-to-FPGA, CPU-to-FPGA, and GPU-to-FPGA covert channels are possible*, with accuracies of up to 100% in some cases. So what can be done?

6 Discussion

Remote attacks on FPGAs are dangerous precisely because they do not require access to the physical hardware: the sources of information leakage described above are not only present in unmodified, off-the-shelf hardware, but also do not require accounting for noisy environments, i.e., they are measurable without having to precisely control the voltage or temperature of the FPGA. Moreover, they do not make use of system monitors or other privileged primitives that would normally be inaccessible to user logic in cloud and other setups.

This makes providing countermeasures against these types of attacks a challenging feat. When it comes to information leakage of static signals on long wires, physical separation is required, taxing though it may be for dense designs. However, physical isolation cannot prevent sources of information leakage due to dynamic activity—even when the activity is on an entirely different FPGA board!

Instead of addressing the underlying vulnerabilities directly, one may instead try to make them harder to exploit by preventing transmissions from taking place, or receiver circuits from being instantiated—at the cost of legitimate uses of ring oscillators in Physical Unclonable Functions (PUFs), True Random Number Generators (TRNGs), and temperature sensors, for example. Even then, the latch- and flip-flop-based ring oscillators mentioned above show that it is possible to create alternative designs circumventing such countermeasures. Moreover, circuits other than ROs can potentially be used as transmitters, provided they also create heavy dynamic switching activity. For example, programmable interconnect points or Digital Signal Processing blocks can also cause voltage drops that are suitable for covert- or side-channel attacks, all while providing seemingly innocuous functionality.

Overall, even though defenses can attempt to hide the useful signal for the attacker under the noise floor, to fundamentally prevent the various sources of FPGA information leakage from occurring, *hardware-level changes are necessary*. Within FPGAs, a more thorough analysis of how to prevent long-wire leakage from occurring in future FPGA architectures is needed. In addition, independent voltage regulation circuits between different SLRs could enable secure multi-tenant deployments with strong physical isolation guarantees. Finally, improving the voltage regulators on the FPGA boards and better-isolating different outputs of the external power supply would make single-tenant cross-FPGA attacks harder.

7 Conclusion

Although a relatively new area of research, remote covert- and side-channel attacks on FPGAs are becoming increasingly relevant. This is not only because they require few resources that can often be hidden behind dual-use functionality, but also because sensitive applications are finding their way onto public cloud infrastructures.

With the move towards multi-die chips and shrinking node sizes, the multi-tenant threat model is becoming more accepted by the security and FPGA communities, and may soon become a practicable reality. As years may pass before the required changes to the hardware layer can be implemented, it is imperative for academics and manufacturers to come together to pinpoint the root causes of vulnerabilities that currently remain elusive without access to details on the proprietary FPGA chip designs.

References

[1] Ilias Giechaskiel, Kasper Bonne Rasmussen, and Jakub Szefer. "C^{3}APSULe: Cross-FPGA Covert-Channel Attacks through Power Supply Unit Leakage". In: 41st IEEE Symposium on Security and Privacy (S&P). 2020.

[2] Ilias Giechaskiel, Ken Eguro, and Kasper Bonne Rasmussen. "Leakier Wires: Exploiting FPGA Long Wires for Covert and Side Channel Attacks". In: ACM Transactions on Recon gurable Technology and Systems (TRETS) 12.3 (Sept. 2019), pp. 11:1--11:29.

[3] Ilias Giechaskiel, Kasper Bonne Rasmussen, and Jakub Szefer. "Measuring Long Wire Leakage with Ring Oscillators in Cloud FPGAs". In: 29th International Conference on Field-Programmable Logic & Applications (FPL). 2019.

[4] Ilias Giechaskiel, Kasper Bonne Rasmussen, and Jakub Szefer. "Reading Between the Dies: Cross-SLR Covert Channels on Multi-Tenant Cloud FPGAs". In: 37th IEEE International Conference on Computer Design (ICCD). 2019.

[5] Ilias Giechaskiel, Kasper Bonne Rasmussen, and Ken Eguro. "Leaky Wires: Information Leakage and Covert Communication Between FPGA Long Wires". In: 13th ACM Asia Conference on Computer and Communications Security (ASIACCS). 2018.

Hunted during a DPhil

Anjuli R.K. Shere, CDT18

For many people, the COVID-19 pandemic was their first experience of months of confinement in a single building. Although this global crisis is certainly new to me, my last few summers have been spent in near-isolation with a team of roughly 15 'Hunters', sitting in a sunless bunker where we absorb, analyse and predict the lives of complete strangers, almost 24/7. Among our many targets have been the father of the UK Prime Minister, a Member of Parliament, and a Lord Mayor - as well as a slew of television celebrities.

These so-called 'fugitives' voluntarily go on the run from our simulated state powers for up to a month and, if they can evade capture until the final day, win a share of £100,000 for themselves or - in the case of Celebrity Hunted - for the charity Stand Up To Cancer. Our 'Hunter' team represents law enforcement and intelligence agencies, and is composed of experts in myriad areas of security, including open-source intelligence, military and policing operations, private and corporate investigations, and ethical hackers (employees of NCC Group). While the finished Grierson Award-winning and BAFTA-nominated show falls into the category of 'Constructed Reality', the highly time-pressured cross-disciplinary work done by our team to apprehend the fugitives is certainly real. My role is that of an intelligence analyst, with a focus on profiling the lives and characters of our targets so that we can track them down before their month on the run is up.

The team thrives because of its diverse (and sometimes conflicting) perspectives and, during our limited down-time, everyone shares their skills, passions and aspirational work stories - from social engineering one's way onto a nuclear submarine to using open-source investigative skills to find missing people. While I remain in awe of all the Hunters, it took less than one series for me to be inspired by the tales told and talents exhibited by the NCC 'Cyber Team' and to inspire my own next career steps, including applying for a DPhil with CDT.

In fact, continuing with Hunted during my first year of the CDT influenced my mini-projects, which evolved into my current DPhil research. I was prompted to conduct my first mini-project, which assessed how new data protection legislation and public awareness of state surveillance have affected open-source investigations in the UK, when I recognised that a few of the tools previously used by the Hunters had lost some of their functionality following the implementation of the 2018 UK Data Protection Act. My second mini-project, which became the pilot study for my thesis research, focused on whether journalists accurately perceive and effectively protect themselves against threats from novel internet-connected devices. This was inspired by the flipside of that recognition because, even without the complete arsenal of tools that we were used to having at our disposal, the Hunters' "powers of the state" still far exceeded the defensive capabilities of any of our

adversaries. I realised that, despite the fugitives' mental and physical preparation and constant hypervigilance while on the run, the asymmetry between our skills, resources, and imagination was immense. If this is the case for people who chose to pit themselves against the state for a pre-established period of time, I wondered how anyone could be expected to protect themselves against similar forces indefinitely.

This disparity is particularly visible and troubling regarding news organisations and journalists, who are increasingly under threat of surveillance, censorship and intimidation from a variety of vectors and highly capable actors. It is my belief that the free press is a critical pillar of democracy, with accessible and transparent journalism of all forms key to educating the electorate and ensuring just and representative government. Throughout my life, I have associated journalists with superheroes, such as Clark Kent and Peter Parker. One of my first human heroes was Roberto Saviano, an investigative journalist whose exposé attributed crimes to more members of the Camorra mafia than had ever previously been documented, putting many of them behind bars although it led to threats on his life. The ongoing attempt to silence Saviano as a message to others who might consider standing against powerful criminal entities against which the state has proven ineffective is one example of the ramifications on an individual human rights level, societally, and in terms of international relations and security, of attacks on journalism. The potential to engage in the kind of in-depth investigation for which Saviano is known was one of my primary motivations for becoming a Hunter.

A 2014 study by Google researchers Huntley and Marquis-Boire showed that 21 of the top 25 news organisations in the world had been the targets of "likely state-sponsored attacks". The advent of 'Internet of Things' (IoT) devices (new networked technologies that are constantly collecting user and bystander data) dramatically expands the attack surface of both journalists and their sources. These mass-produced devices that are intended to prioritise convenience rather than security are often also designed to subtly blend into an existing environmental aesthetic. The Hunters in our Cyber Team regularly invent new feats of wizardry and have demonstrated how the prevalence of such devices could facilitate remote reconnaissance of a target's home or work address, including allowing us to build a profile of a fugitive's daily routine and identity by piecing together footage from "cat cams", logs from domestic devices like boilers, and clips retained by voice assistants. These unconnected bits of information coalesce, first into a pattern of life and then into actionable intelligence. Given the ubiquity of exciting new IoT devices, a target's data emissions are becoming less of a digital footprint than a fingerprint: specific to each individual.

Our goal on Hunted is never to cause psychological or physical harm to our fugitives, simply to capture them, so we only gather the information necessary to do so. We also strictly abide by data protection laws, as we are not actually acting on behalf of the state and so cannot claim "legitimate interest" for collection of any data beyond that covered by fugitives' consent. Still, the Hunted Team has amply illustrated that the IoT brings with it the potential to enact cyber-attacks that could discredit or otherwise undermine individuals, e.g. news sources, through highly targeted cyber-physical and psychological attacks. Hunted has also alerted me to the existence of numerous unexplored anticipatory attack models that could threaten media companies, e.g. supply chain attacks that exploit insecure technological infrastructure of the entire industry such as communications equipment, hacks of internet-connected security systems and other remote-access devices, like smart light bulbs that could be used to both exfiltrate user data and to induce epileptic fits in individual journalists and sources.

Considering the probability of both surveillance of and aggression against members of the free press, it seems important to anticipate and record these kinds of unusual IoT threat models that may not be used against a high percentage of journalists globally but are certainly likely to be mobilised against individuals with particular influence or insight. As such, my DPhil thesis research aims to create a framework for mitigations of IoT threats to the free press, through the curation of taxonomies of both IoT devices and their associated virtual, physical and legal threat models. Luckily, this topic enables me to continue my tenure on Hunted. In fact, filming the programme gives me the unique opportunity to be surrounded by investigators and penetration testers from around the world, who can regale me with ideas for innovative (and terrifyingly intrusive) ways in which the IoT can be manipulated - and for countering these threats. I call this "threat intelligence sharing", instead of an attempt to be rewarded for excellent storytelling with free drinks, once we emerge from the darkness of our Hunter headquarters.

If Hunted has taught me anything, it is that it is no longer enough for fugitives to ditch their smartphones. One thing is certain: The Internet of Things would be Kryptonite for Clark Kent's privacy. Today, it is no longer Superman who has X-ray vision (useful for scanning cupboards for lurking internet-connected recording devices), but the state who can see right through you.

The certification of cyber security degrees: a tool to mitigate the cyber security skills shortage?

Tommaso de Zan, CDT17

The lack of professionals with cyber security knowledge and skills, the so-called cyber security skills shortage (CSSS), is a risk for both economic development and national security, which has forced countries to find solutions to increase the cyber security workforce pipeline. Among other policies, some countries have introduced the certification of cyber security degrees as a mean to increase both the quantity and the quality of cyber security graduates entering the labour market. This article, which summarizes a research report I authored for the European Union Network and Information Security Agency (ENISA),[1] analyzes why the certification of cyber security degrees might be a good (partial) solution to the CSSS problem and how four countries – Australia, France, the United Kingdom and the United States – have set procedures and standards to certify their national cyber security degrees.

The cyber security skills shortage and the issue of the "right" cyber security knowledge and skills

The cyber security skills shortage (CSSS) is the lack of qualified cyber security professionals in the labour market, which is usually characterised by unfilled or hard-to-fill vacancies and raises in the wages of professionals with in-demand skills and knowledge (McGuinness, Pouliakas, & Redmond, 2018).

There are various indicators suggesting that cyber security is one of the most constrained sectors in the labour market. Figures based on the US market shows that in 2019 (Burningglass, 2019):

- security job postings had increased by 94% since 2013, while information technology (IT) vacancies had increased by only 30%;
- cyber security jobs accounted for 13% of all IT jobs, but their salaries commanded a 16 % premium over other IT ones;
- cyber security vacancies also took 20% longer to fill than those in other IT occupations;
- the ratio of currently employed cyber security professionals to vacancies had not changed since 2015-16, being stable at 2.3, whereas by comparison there were 5.8 employed workers for any other job in the economy.

Although results should be interpreted with caution,[2] industry research also unanimously concludes that a CSSS is well established. For example, the 2019 cyber security workforce study by the International Information System Security Certification Consortium estimated the current global shortage to be around 4.07 million professionals and that the workforce would need to grow by 145 % to meet labour market demand ((ISC)², 2019).

The cyber security skill shortage is a multidimensional policy issue that is compounded by several factors. Among these, employers lament that is hard for them to recognise the skills that potential cyber security candidates have, or to find them at all. A quick review of the literature suggests that many issues regarding cyber security education could be mitigated by imposing standards for the knowledge and skills that cyber security students should acquire and thus rearrange cyber security educational and training pathways (Conklin, Cline, & Roosa, 2014; European Cyber Security Organisation, 2018; Gagliardi, Hankin, Gal-Ezer, McGettrick, & Meitern, 2016; Vishik & Heisel, 2015). When stakeholders stress the need to teach more cyber security in computer science degrees, underline the poor alignment between education and labour market demands, propose multidisciplinary expertise and encourage educators to promote more hands-on education, they are suggesting to provide clarity on the "right" cyber security knowledge and skills that students should be equipped with once they graduate with a degree in cyber security

.

Redefining curricula and educational paths is one of the major challenges regarding the cyber security skill shortage. In fact, major stakeholders in the debate do not necessarily agree on what the right cyber security knowledge and skills really are, as it is expressed by differences in the various cyber security knowledge and skills frameworks currently available (Chartered Institute of Information Security, 2019; Joint Task Force on Cyber security Education, 2017; Newhouse, Keith, Scribner, & Witte, 2017; Rashid et al., 2018). One way to address this challenge is for the relevant stakeholders — most

1 The research report can be accessed here: https://www.enisa.europa.eu/publications/the-status-of-cyber-security-education-in-the-european-union.

2 Industry research employing surveys falls short of providing strong scientific results on the incidence of the CSSS. These surveys are beleaguered by serious methodological issues to such an extent that caution should be exercised when using these data to design public policies. Issues include non-randomisation of the population surveyed, poor choice of indicators and doubtful quantification of the shortage at the international level. However, this research is useful insofar as it underlines a policy issue that has been underinvestigated and needs careful consideration from both researchers and policymakers

importantly academia, governments and employers — to sit around a table and discuss the basic knowledge and skills that students should develop when they undertake a computing degree with a focus on cyber security .

Cyber security degree certification around the world

Australia, France, the United Kingdom and the United States are among the countries to have set procedures and standards to certify their cyber security degrees. There are currently 387 degrees that are certified by national authorities of these four states.[3] These states established certification for cyber security degrees mainly:

- to have more graduates with skills readily deployable by the industry;
- to help employers understand skills and knowledge that students have developed in their academic careers;
- to assist students in making more informed decisions about their degree choices.

When authorities award certification, they attest that a degree meets the standards and criteria that a group of national experts considers necessary for a cyber security educational program. With the exception of Australia, where the process is supervised by the Department of Education, these certifications are generally overseen by states' main cyber security national institutions, namely the Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) in France, the Department of Homeland Security (DHS) and the National Security Agency (NSA) in the United States, and the National Cyber Security Center (NCSC) in the United Kingdom.

The expected ultimate impact of the certification of cyber security degrees is to reduce the CSSS and mitigate national vulnerabilities through the promotion of cyber security education, research and awareness.

Although processes and criteria differ among these 4 countries,[4] they also have several commonalities:

- Not surprisingly, certification is awarded to degrees that provide an adequate amount of taught courses and activities that are specific to cyber security. This is done to differentiate courses that are in cyber security (or computer science degrees with a clear focus on cyber security) from IT courses that could claim to provide some sort of cyber security education but not enough to form well-rounded cyber security graduates.

- Certification is typically awarded to those institutions that can show in great detail how cyber security education is provided. For example, national authorities often inquire about the structure of the curriculum and if more practical training is included. Moreover, a number of certification processes ask directly about the kind of examinations students undergo, including for example how students do their dissertations, what courses take place to increase students' academic skills, how much time students spend on hands-on activities and if students are encouraged to attend cyber security competitions. Finally, academic institutions often have to declare whether or not the degree prepares students for a professional certification.

- A lot of importance is placed on the quality of the faculty, meaning that national authorities request biographies and curricula vitae of lecturers. Academic institutions are often asked to clarify the nature of the cyber security research that faculty is engaged in and if at least part of the faculty has an industry background.

- Degrees that have a broader interdisciplinary focus have more chance of being certified. For example, topics that are not solely technical are strongly encouraged, such as legal courses on data protection. Sometimes, even degrees that are not purely technical but have a predominant organisational component can receive certification, although generally speaking the emphasis is on teaching foundational engineering and computer science knowledge. In sum, cyber security should be taught in a multidisciplinary manner and students should be exposed to a variety of policy, social, legal and ethical aspects.

- National authorities place importance on external outreach activities and collaboration opportunities that degrees have in place. From various education-to-labour market initiatives, such as workplace training, business mentoring or internships and traineeships, to more academic forms of collaborations with similar institutions, states seem to sponsor those degrees that enhance and enrich a vigorous national cyber security ecosystem.

- Finally, governments are interested in knowing about academic and employment outcomes. Most notably, they seek to know how many students enroll each year, how many graduates a course produces and possibly the types of jobs alumni end up securing after obtaining the degree.

3 As of December 2019.

4 For a detailed description of national criteria and processes, see the ENISA publication from pg. 16 – 22.

Conclusions

When academia, employers and governments come together to determine what educational and training experiences would be appropriate for cyber security, they recognise the importance of achieving conceptual clarity on what it means to equip students with the right cyber security knowledge and skills. Clarifying this will help mitigate one of the many factors that compounds the CSSS.

This is also useful because it better defines roles and responsibilities in developing the skills and knowledge of the national cyber security workforce. This is especially true because employers should recognise that higher education institutions are not necessarily meant to provide graduates with the specific skills for a particular job; rather, they are intended to give students the knowledge, skills and methods that will equip them to constantly engage with an evolving threat scenario. As pointed out by Malan et al. (2018), cyber security should be seen as a very technical subject requiring many years of experience. Therefore, even students who obtain degrees that are highly relevant will need to develop their knowledge and skills further once they leave the educational system, which implies that they must be provided with the right opportunities for training by the employers themselves.
However, determining what the right skills are is only a portion of a much wider problem that is worsened by several other factors. This report concentrated on only one of the main causes attributed to the CSSS. Although cyber security degree certification could be a step in the right direction, it cannot be considered the only solution. In fact, some countries have articulated cyber security education and skills strategies in which policies such as certification are only one of several instruments, which include for instance cyber security courses at high school level, national cyber security competitions and various types of financial aid.

Moreover, scholars studying the intersection of education with the labour market have long warned about the need to go beyond initiatives that target only the supply side of the equation (Mayhew & Keep, 2014). There is plentiful evidence suggesting that the CSSS is affected by problems that are generated on the demand side of the equation as well, namely when employers ask for several years of professional experience and professional certification or are unwilling to invest in human capital by providing training opportunities. Incorporating policies to tackle issues that arise on the demand side of the labour market, including deployment and 'skill utilisation', are likely to be as, or perhaps even more, beneficial (Buchanan, Finegold, Mayhew, & Warhurst, 2017). In this context, it would be particularly promising to find solutions easing the transition from the education system into the labour market and giving an active and systematic role to employers in developing the cyber security workforce.

Taking this into account, certification of cyber security degrees might be an important turning point in a comprehensive cyber security workforce development strategy. This is because it could clarify what knowledge and skills the education system is supposed to instil and, consequently, what sort of training and further learning opportunities employers should provide when students enter the workforce, recognizing the fact that each stakeholder has a role in the formation and development of skills of the national cyber security workforce.

References

ISC)2. (2019). Strategies for Building and Growing Strong Cyber security Teams - (ISC)2 Cyber security Workforce Study 2019. Retrieved from https://www.isc2.org/-/media/ISC2/Research/2019-Cyber security -Workforce-Study/ISC2-Cyber security -Workforce-Study-2019.ashx?la=en&hash=D087F6468B4991E0BEFFC017BC1ADF59CD5A2EF7

Buchanan, J., Finegold, D., Mayhew, K., & Warhurst, C. (2017). Introduction: Skills and Training: Multiple Targets, Shifting Terrain. In J. Buchanan, D. Finegold, K. Mayhew, & C. Warhurst (Eds.), The Oxford Handbook of Skills and Training (Vol. 1). https://doi.org/10.1093/oxfordhb/9780199655366.013.33

Burningglass. (2019). Recruiting Watchers for the Virtual Walls: The State of Cyber security Hiring. Retrieved from https://www.burning-glass.com/wp-content/uploads/recruiting_watchers_cyber security _hiring.pdf

Chartered Institute of Information Security. (2019). Skills Framework - Version 2.4. Retrieved from https://www.ciisec.org/CIISEC/Resources/Capability_Methodology/Skills_Framework/CIISEC/Resources/Skills_Framework.aspx?hkey=8976fc14-4ce7-46c3-8751-ce18d16fecf0

Conklin, W. A., Cline, R. E., & Roosa, T. (2014). Re-engineering Cyber security Education in the US: An Analysis of the Critical Factors. 2014 47th Hawaii International Conference on System Sciences, 2006–2014. https://doi.org/10.1109/HICSS.2014.254

European Cyber Security Organisation. (2018). Gaps in European Cyber Education and Professional Training.

Gagliardi, F., Hankin, C., Gal-Ezer, J., McGettrick, A., & Meitern, M. (2016). Advancing Cyber security Research and Education in Europe - Major Drivers of Growth in the Digital Landscape. Europe Policy Committee Association for Computing Machinery.

Joint Task Force on Cyber security Education. (2017). Cyber security Curricula 2017 - Curriculum Guidelines for Post-Secondary Degree Programs in Cyber security . Retrieved from https://europe.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf

Malan, J., Lale-Demoz, E., & Rampton, J. (2018). Identifying the Role of Further and Higher Education in Cyber Security Skills Development. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/767425/The_role_of_FE_and_HE_in_cyber_security_skills_development.pdf

Mayhew, K., & Keep, E. (2014). Industrial strategy and the future of skills policy: The high road to sustainable growth. Retrieved from https://www.cipd.co.uk/Images/industrial-strategy-and-the-future-of-skills-policy_2014_tcm18-10247.pdf

McGuinness, S., Pouliakas, K., & Redmond, P. (2018). Skills Mismatch: Concepts, Measurement and Policy Approaches. Journal of Economic Surveys, 32(4), 985–1015. https://doi.org/10.1111/joes.12254

Newhouse, W., Keith, S., Scribner, B., & Witte, G. (2017). National Initiative for Cyber security Education (NICE) Cyber security Workforce Framework. Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf

Rashid, A., Danezis, G., Chivers, H., Lupu, E., Martin, A., Lewis, M., & Peersman, C. (2018). Scoping the Cyber Security Body of Knowledge. IEEE Security & Privacy, 16(3), 96–102. https://doi.org/10.1109/MSP.2018.2701150

Vishik, C., & Heisel, M. (2015). Cyber security Education snapshot for workforce development in the EU. Retrieved from https://resilience.enisa.europa.eu/nis-platform/shared-documents/wg3-documents/cyber security -education-snapshot-for-workforce-development-in-the-eu/at_download/file

Best Paper Award at SecureComm 2019

Eman Alashwali, CDT15

Eman Alashwali, a final year DPhil student has led a paper that won the "Best Paper Award" out of 149 original submissions in the 15th International Conference in Security and Privacy of Communication Networks (SecureComm19), held at Orlando, the US. The paper entitled "Towards Forward Secure Internet Traffic" is co-authored with Prof. Andrew Martin and Prof. Pawel Szalachowski from Singapore University of Technology and Design.

The paper introduces a novel adversarial model which they called the "discriminatory" adversarial model. The paper identifies the lack of transparency in the negotiation of sensitive parameters such as the protocol version and ciphersuite in some configurable protocols such as the TLS protocol that is used to secure Internet communication. The paper includes a case study on the Forward Secrecy property in the TLS protocol, which exemplifies the applicability of the discriminatory model. Finally, the paper provides some proposals towards Forward Secure Internet traffic through the "Best Effort" approach. The paper can be found in: https://arxiv.org/pdf/1907.00231.pdf

Oxford team wins Cyber 9/12 London competition

Manuel Hepfer (CDT16), Alexis Ciambotti (MPhil Politics), Yashovardhan Sharma (CDT18) and Matthew Rogers (CDT18)

Cyber 9/12 is a cyber policy competition for students across the globe, who compete to develop national security policy recommendations which tackle a fictional cyber-incident. Students from Oxford have taken part in the competition before but this is the first year the Oxford team has done so well. Our 'CyberSeals' team reached the finals, and then won the competition!

Team member Matthew Rogers writes, 'We were given a 40-page intelligence brief from multiple sources and month to write a situation assessment and decision brief, giving a 10-minute oral presentation to UK government experts who acted as judges. For the semi-finals we had to do the same, but this time a 20 page intelligence brief in just 13 hours from 5pm to 9am. In the competition finals we were given 20 minutes alone in a room with a 10-page intelligence brief, and then promptly presented a 10-minute brief, with a 15-minute Q&A on stage to all attendees. Through this competition we evaluate the threats different actions propose to the UK government, technological responses, and the multi-national, inter-agency, and government/industry connections that must be considered when responding to cyber attacks. This is especially when the attribution is unclear and situation only continues to escalate.'

Klaudia Krawiecka nominated at the 2020 Vice Chancellor's Diversity Awards

Klaudia Krawiecka has been recognised as part of this year's Vice Chancellor's Awards for her efforts in increasing women's representation and embracing diversity across the field of Computer Science. The VCs awards showcase the exceptional efforts of members of the university who have inspired others, demonstrated leadership and made a difference to equality and diversity in the University's working, learning and social environment.

Klaudia has been a pivotal part of the Oxford Women in Computer Science Society (OxWoCS) holding roles from Outreach Officer to President. During her term, she promoted diversity at flagship events such as Oxford Hack, encouraging women's societies to submit teams and providing an inclusive a welcoming atmosphere for all participants. Other activities include programming workshops for schoolgirls in years 7 to 9 helping to inspire future computer scientists too.
Further information on the awards can be found at https://www.ox.ac.uk/about/oxford-people/vice-chancellors-diversity-award

CDT17 Bios

Thomas Burton

Supervisor: Kasper Rasmussen, Department of Computer Science

Thomas studied an MComp in Computer Science (with Security and Resilience) for four years at Newcastle University. His current areas of interest include secure localisation, misusing localisation schemes for attacks, and mesh networking.

At Newcastle he studied a range of topics from system security and information security and trust to high integrity software development and the challenge of developing highly dependable systems. His third and fourth year dissertation projects covered the security related topics of biometric security and authentication, and cryptographic, specifically zero-knowledge proofs. He has also spent several summers working with a health sciences and bioinformatics group. With them he has worked on a range of projects ranging from website development to algorithm development. During this work, he experienced working with people from a range of academic departments and fields.

DPhil Thesis: Secure Urban Audio Localisation

I am looking at the use of smartphones for urban search and rescue. Specifically I am working on secure protocols for using audio to locate smartphone devices to assist in an urban disaster environment. This type of localisation has a number of potential challenges to overcome as a result of limited low level hardware access, the scale over which the protocols are being used, and how easily an attacker can interfere as the cost of mounting at attack is low. Attackers also have several key advantages, such as, being able to transfer information at the speed of light using normal radio communication which is much faster than the sound used for the localisation.

Selina Yoon Cho

Supervisors: Ivan Flechais, Department of Computer Science and Jonathan Lusthaus, Department of Sociology.

Selina is interested in understanding how the Internet facilitates online crime and deviance. The methodologies in her past and present research include Natural Language Processing techniques, mainly topic modelling and sentiment analysis, and qualitative interviews. Selina holds an MSc (Distinction) in Information Security and a BA in Economics. Her 2015 Masters dissertation examined the concept of security through obscurity through its design applications in communication protocols and steganography.

Curious to explore the applications of data analytics in threat discovery, Selina interned in the Product Management team at Cloudflare overseeing enterprise-level DDoS traffic monitoring, and collaborated with WWF to build an NLP model that detects emerging threats against World Heritage Sites. She also worked as a Research Assistant at the Oxford Internet Institute providing technical support for privacy tools, and as a Security Administrator at KEPCO KPS, a South Korean plant engineering company, assisting with network monitoring and troubleshooting.

Outside research, Selina was the President of the Oxford Fintech and Legaltech Society, where she hosted interdisciplinary seminars related to the UK startup scene in financial and legal technology. She remains as the webmaster of the site to date.

DPhil Thesis: Self-governing communities in online game cheating

Online game cheating is a multi-million dollar industry, growing evermore robust against the anti-cheat measures put in place by the developers. Despite its prevalence, there is a lack of understanding in how the cheat resources are managed outside the official gaming scene.

This thesis is an exploratory research into cheating communities to understand how they operate and govern themselves. We design our studies based on the framework of self-governance, and analyse differing levels of trust and compliance that exist among users. We use a mixed-methods approach for data collection combining web scraping and interviews with the community members. The findings will be used for forming new theories in the field of Human Centred Computing, understanding resource management in fringe communities, and identifying deviant behaviours in end-user designed systems.

Publications

S. Y. Cho, J. Happa and S. Creese, "Capturing Tacit Knowledge in Security Operation Centers," in IEEE Access, vol. 8, pp. 42021-42041, 2020, doi: 10.1109/ACCESS.2020.2976076.

S. Y. Cho and J. Wright, "Into the Dark: A Case Study of Banned Darknet Drug Forums," in Lecture Notes in Computer Science, Cham: Springer International Publishing, 2019, pp. 109–127, doi: 10.1007/978-3-030-34971-4_8.

Tommaso De Zan

Supervisors: Ewart Keep and Liam Gearon, Department of Education; Andrew Martin, Department of Computer Science.

Tommaso is a DPhil student in Cyber Security at the University of Oxford, where he analyzes policies aimed at reducing the cyber security skills shortage. In particular, he investigates whether cyber security competitions affect students' interest in a cyber security career and how.

In the context of his research, he conducted a six month-traineeship at the European Union Network and Information Security Agency (ENISA) in Athens and continues to collaborate with ENISA on topics related to skills development in the EU. Moreover, he was a visiting student at the Center for International Security at the Hertie School in Berlin.

He is also a Research Associate with the Centre for Technology and Global Affairs (DPIR, Oxford University), a member of the Global Forum on Cyber Expertise, and a steering committee member of the Cyber Youth Initiative (Royal United Services Institute).

Prior to his DPhil, he was an Associate Fellow at the European Union Institute for Security Studies and a Researcher at the International Affairs Institute (IAI). Before joining IAI, he interned at the International Peace Research Institute in Geneva.

He holds a Master's degree in International Relations from the University of Bologna and he was an exchange student at the Josef Korbel School of International Studies and Université catholique de Louvain.

DPhil Thesis: Do competitions affect students' interest in cyber security career? The cyber security skills shortage and public policy interventions

Employers have been lamenting for several years the lack of cyber security professionals in the labour market, the so-called cyber security skills shortage. The shortfall of information security workers means that our data, networks and systems are less secure, which might undermine economic development and national security. Governments have scrambled to redress this trend and have designed and implemented policies to increase the pipeline of cyber security professionals. Among these policies, cyber security competitions have sprouted and received the support of governments and industry alike. Nonetheless, it is generally unknown whether skills shortage policies such as cyber security competitions work and how. This dissertation project investigates the outcomes of these competitions, especially whether they affect students' career interest in cyber security.

Publications:

De Zan T., Giacomello G., Martino L. (forthcoming), "Italy", Routledge Handbook of Global Cybersecurity, edited by Manjikian M. and Romaniuk S. N., Routledge, New York;

De Zan T. (2020), "Future Research on the Cyber Security Skills Shortage", in Cyber-Security Education: Principles and Policies, edited by Austin G., Routledge, New York, https://bit.ly/2UMquJ6;

De Zan T. and Di Franco F. (2020), "EU Cyber Security Skills Development: The Certification of Cyber Security Degrees and ENISA's Cyber Security Higher Education Map," European Union Network and Information Security Agency, https://bit.ly/3dTS7Yc;

De Zan T. (2020), "The shortfall of cyber security competencies in Italy" (Italian), Agenda, Enciclopedia Treccani, Roma, http://bit.ly/2U2jOqb;

De Zan T. (2019), "The Italian Cyber Security Skills Shortage in the International Context", Global Cyber Security Center, Rome, https://bit.ly/2OG9flg;

De Zan T. (2019), "Much Ado About the Cyber Skills Shortage", Net Politics, Digital and Cyberspace Policy Program, Council on Foreign Relations, New York, https://on.cfr.org/2tHwSTx;

De Zan T. (2019), "Mind the Gap: the Cyber Security Skills Shortage and Public Policy Interventions", Global Cyber Security Center, Rome, https://bit.ly/2tpedvs;

Seb Farquhar

Supervisor: Yarin Gal, Department of Computer Science

Seb is interested in cyber security within machine learning and artificial intelligence. This includes technical work on robust deep learning systems that are able to recognize and safely handle unexpected or adversarial inputs as well as privacy-preserving machine learning and policy questions related to the safe adoption of AI systems. Before beginning this DPhil, Seb worked at the Future of Humanity Institute at the University of Oxford, was Director of the Global Priorities Project, a think tank focusing on global catastrophic risk management, and worked for McKinsey & Co. as a consultant focusing on public sector clients. He has a Master's degree in Physics and Philosophy from the University of Oxford.

DPhil Thesis: Foundations for secure deep learning

In this research project I explore foundations for safe and secure deep learning including:

-Systems capable of detecting anomalies/out-of-distribution behaviour using Bayesian deep learning methods and ensembles.

-Differentially private deep learning systems for learning over extended periods of time or across related simultaneous contexts with managed privacy leakage.

-Deep learning architectures optimized for secure multi-party computation.

Jack K

Faculty of Law.

Jack's background is in public international law. His research focuses on how existing frameworks of international law apply to cyber operations.

Klaudia Krawiecka

Supervisor: Ivan Martinovic, Department of Computer Science

Klaudia is a doctoral student at the Centre for Doctoral Training in Cyber Security at the University of Oxford and the recipient of (ISC)² Women's Cyber Security and Google Women Techmakers scholarships. She graduated from the NordSecMob programme in 2017, obtaining a Master's degree in Security and Mobile Computing from two universities: Aalto University and Norwegian University of Science and Technology. Her adventure with computer science began in primary school. She continued to develop her passion during high school and in college. During the second year of her Bachelor's studies, she took an internship in the ICT security office where she was introduced to computer forensics and cyber security fields; in addition, she had a great opportunity to conduct training for police officers on NFC technology and the risks arising from its use. She also worked as a Research Assistant at Aalto University in Secure Systems Group. Her research project, which developed into her Master's dissertation, resulted in the development of SafeKeeper, an open-source system that secures users' passwords on the web. This project received three prestigious awards from the Finnish Information Security Association, the Finnish Computer Science Society, and Aalto University.
Her doctoral research focuses on identifying and tackling security challenges in the Internet of Things (IoT) environments. Considering the existing limitations of such environments, she works on improving access control and authentication systems by leveraging the heterogeneity of IoT devices.

Until 2019 she was a President of the Oxford Women in Computer Science Society (OxWoCS). Apart from leading and coordinating technical workshops and hackathons, her responsibilities included organizing events to promote Computer Science among female students.

DPhil Thesis: Authenticating Internet of Things (IoT) devices using out-of-band channels

The amount of Internet of Things (IoT) devices available on the market increases significantly every year. Many such devices are integral parts of smart buildings, which are equipped with modern systems and technologies designed to increase the safety and comfort of their users. Many devices are not equipped with displays or do not allow users to verify their operation. Out-of-band channels such as visual channels (e.g. Augmented Reality) may provide a novel way of authenticating various sensors and give the users an appropriate feedback. The research focuses on designing, implementing, examining and assessing different out-of-band authentication channels and to determine which ones provide stronger security guarantees and fulfil usability, deployability and performance requirements.

Dennis Malliouris

Supervisor: Andrew Simpson, Department of Computer Science

Dennis started the DPhil in Cyber Security programme in 2017. He has an MRes in Management (Distinction) for which he studied at London Business School and University College London. He was awarded the SoM Full Scholarship for the duration of his studies. Priorly, he graduated first in his class with an MSc in Management & Finance from UCL. Dennis also obtained a BA in Management (first-class), has a certificate in financial valuation from Oxford's Saïd Business School (OCVP), and is a qualified management accountant (IHK). Dennis worked on multidisciplinary in-house consultancy projects at Siemens in Germany and the UK, at a technology-driven hedge fund, and in financial research & valuation.

His research at the CDT explores financial, strategic, and organisational implications of cyber security for firms. Specifically, his research projects analyse underlying and consequential costs of security breaches and information security investments. Dennis grew up multilingually and speaks English, German, Greek, and French. He represents Oxford University in regional and national competitions, and New College on university-level, in multiple sports. He gratefully acknowledges CDT/EPSRC funding, New College's 1379 Society Old Members Scholarship, and New College's Sporting and Cultural Award.

DPhil Thesis: Finance & Cyber Security: Uncovering Underlying and Consequential Costs of Cyber Security Breaches

Publications:

D.D. Malliouris & A.C. Simpson (2019). The stock market impact of information security investments: the case of security standards. In: The 2019 Workshop on the Economics of Information Security (WEIS 2019).

D.D. Malliouris & A. Simpson (2020). Underlying and consequential costs of cyber security breaches: changes in systematic risk. In: The 2020 Workshop on the Economics of Information Security (WEIS 2020).

D.D. Malliouris, A.T. Vermorken, M.A.M. Vermorken (2020). Aggregate insider trading and future market returns in the United States, Europe, and Asia. International Journal of Finance & Economics (in press).

Romy Minko

Supervisors: Artur Ekert and Christophe Petit, Maths Institute

Romy's background is primarily in Mathematics, although she also holds a BSc in Chemistry from the University of Melbourne. Romy first became interested in cryptography while at secondary school in Australia and subsequently went on to complete the MSc in the Mathematics of Cryptography and Communications at Royal Holloway, graduating with Distinction. Her research interests lie in post-quantum cryptography and quantum computation; she is currently focussed on supersingular isogeny-based cryptosystems and has previously conducted research in blind quantum computing. Romy is also a 2018 Policy Fellow with the Department of Prime Minister and Cabinet of Australia, where she experienced drafting cybersecurity policy at a government level.

DPhil Thesis: Post-quantum cryptography using multivariate polynomial systems

Multivariate public-key cryptography (MPKC) is one of the four most common branches of post-quantum cryptography, describing cryptosystems based on solving systems of multivariate polynomials. An important step in the cryptanalysis of MPKC system is finding a Gröbner basis for the system. My research focusses on adapting generic Gröbner Basis algorithms to families of multivariate polynomial systems with specific structures. I am currently looking at multivariate linearised polynomials, which have not been studied in great detail.

Additionally I am exploring applications of the HHL quantum algorithm for solving systems of multivariate polynomials, in particular Boolean systems.

James Pavur

Supervisor: Ivan Martinovic, Department of Computer Science

James hails from Atlanta, Georgia (USA) and holds a BSFS in Science, Technology, and International Affairs from Georgetown University in Washington, DC. He is at Oxford on a Rhodes Scholarship (Georgia and Wolfson, 17). His thesis revolves around the security and privacy aspects of satellites and space-based systems with his most recent research focusing on satellite telecommunications and broadband services.

He has dabbled in cybersecurity through a variety of professional experiences – including functioning as the principle cyber decision maker at a 500 employee non-profit (Students of Georgetown Incorporated). His internship experiences include working as a Reverse Engineer for Embedded Systems at Booz Allen Hamilton, auditing building control and SCADA systems as a contractor for the US General Services Administration, and investigating computer crimes with the US Postal Service's Office of the Inspector General. He has also contributed to telecommunications and privacy policy research through Georgetown's Software and Security Engineering Research Center.

His language of choice is python, although (with generous use of Google) he is also proficient in C/C++, JavaScript, C#, PHP, and Visual Basic.He enjoys hackathons and CTF competitions, collecting (and sometimes consuming) tea, flying kites, and pretending he knows how to play squash.

DPhil Thesis: On Space Cyber-Security

This project focuses on cyber-security concerns for satellite systems. On going experimental research includes the investigation of privacy and security properties for modern satellite broadband connections over the Digital Video Broadcasting for Satellite (DVB-S) protocol, and the integrity and authenticity of space situational awareness data for flight control and orbit determination. The project also considers the strategic and political effects of Cyber-ASAT (Anti-Satellite Weapon) capabilities.
Longer term, the thesis will focus on providing core security principles and best practices to enable the secure operation of critical space missions. These principles will be derived from experimental research and strategic analysis.

Publications:

James Pavur, Daniel Moser, Vincent Lenders, and Ivan Martinovic. 2019. Secrets in the Sky: On Privacy and Infrastructure Security in DVB-S Satellite Broadband. In WiSec '19: Conference on Security and Privacy in Wireless and Mobile Networks, May 15– 17, 2019, Miami, FL, USA. ACM, New York, NY, USA. https://doi.org/10.1145/3317549.3323418

James Pavur and Ivan Martinovic. 2019. The Cyber-ASAT: On the Impact of Cyber Weapons in Outer Space. In 2019 11th International Conference on Cyber Conflict - Silent Battle, May 28-31, 2019, Tallinn, Estonia. NATO CCD COE Publications, Tallinn, Estonia.

James Pavur. 2018. Cyber Security and AI (Seminar). Rhodes Artificial Intelligence Laboratory - Speaker Series. November 07, 2018, Oxford, United Kingdom.

J. Pavur, D. Moser, M. Strohmeier, V. Lenders and I. Martinovic, "A Tale of Sea and Sky: On the Security of Maritime VSAT Communications," in 2020 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, US, 2020 pp. 1384-1400.

J. Pavur and C. Knerr, "GDPArrrrr: Using Privacy Laws to Steal Identities." In BlackHat USA '19. Las Vegas, NV, 2019.

J. Pavur, "Whispers Among the Stars: A Practical Look at Perpetrating (and Preventing) Satellite Eavesdropping Attacks," Conference Briefing In BlackHat USA '20. Las Vegas, NV, 2020.

J. Pavur, "Whispers Among the Stars: A Practical Look at Perpetrating (and Preventing) Satellite Eavesdropping Attacks," Conference Briefing In DEFCON 28. Las Vegas, NV, 2020.

J. Pavur, "Trust and Truth in Space Situational Awareness," Conference Briefing in DEFCON 28 Aerospace Village. Las Vegas, NV, 2020.

Mark Quinlan

Supervisor: Andrew Simpson, Department of Computer Science

Mark Quinlan has gained a mixture of industry experience and academic knowledge prior to starting a DPhil in Cyber Security, his industry experience including BAE Systems where he worked within the cyber field in both commercial and government projects.

His consultancy business designed and built manufacturing resource planning systems, as well as systems security strategy consultancy for companies ranging from British racing teams to Japanese Tier One suppliers.

Mark lives with his partner, and when not pursuing his academic passions he enjoys restoring classic cars, driving karts and said cars, hiking, non-fiction, and enjoying good food and company. Once upon a time Mark was a Dutchman, but has lived in the UK since 2004.

DPhil Thesis: Cyber Continuum; towards a security engineering framework incorporating legacy systems

Mark is looking into privacy and security of Internet of Things devices, and

their wider infrastructural landscape. Current work includes a privacy and security analysis of connected cars through the examination of the data-gathering systems of a production vehicle, to ascertain some of the privacy-related threats to which such systems give rise.

Future work: With the lifecycle of an average car being approximately nine years, a connected car has a longer lifespan than the typical IoT device. In addition, it is significantly more likely to be re-sold over its lifetime. When looking at embedded devices across the IoT spectrum, more and more devices are falling outside traditional consumer devices such as speakers and home security, increasingly being used within city infrastructure, and in private and commercial transportation such as cars, the need for security management over longer lifecycles becomes more apparent.

The high-level research objectives are as follows;

1 What is the current state of the literature on the management of legacy embedded systems, and their associated infrastructure?
2 What is the current state of manufacturers providing security updates to their products?
3 What would a theoretical framework incorporating the long-term management of legacy IoT devices look like?

Lonie Sebagh

Supervisors: Jonathan Lusthaus and Federico Varese, Department of Sociology

Lonie is researching the disruption of online criminal trade by various stakeholders from law enforcement to private industry and trading platforms, combining sociology, criminology, and economics perspectives. Her thesis involves three different research methods: 1) laboratory experiments aiming to measure traders' behaviours and responses to operations aimed at eroding trust on online criminal marketplaces, 2) content analysis of reports, news articles, and Blog posts of organisations in different sectors in order to evaluate the way they communicate about the disruption of online criminal trade, and 3) interviews with experts in different sectors to discuss their role in the disruption landscape. The use of mixed methods will allow for the formulation of theory and recommendations about the disruption of online criminal trade by different stakeholders.

Prior to joining the CDT Lonie was a student in Business and Management at the Universities of St Andrews and Edinburgh. Her interest in Cyber Security stems from her work experience in the IT Security department of a private bank in Geneva in 2014, which inspired her to make the transition from Business to Information Technology through a PG Diploma (Distinction) with an emphasis on Computer Security and Critical software engineering.
In her spare time Lonie can be found in her College where she works as a Junior Dean, providing welfare support to fellow postgraduate students.

DPhil Thesis: The disruption of the online criminal trade of drugs and wildlife – beyond law enforcement

This thesis explores the actors and activities involved in the disruption of the online criminal trade of drugs and wildlife, both on the Dark and Surface web. Although much research has been conducted about law enforcement operations such as criminal platform takedowns and administrator and vendor arrests, little is known about who other than law enforcement is involved in these operations, what activities they perform, and what skills and support they bring to this endeavour. This research contributes to the fields of sociology and cyber criminology by providing a better understanding of the various other players involved in the disruption of online criminal drug and wildlife trade, from government to academia, private organisations, non-profits, trading platforms, and cybercriminals themselves. Recommendations are then provided for each of these entities about the future disruption of this crime type.

Presentations:

L. Sebagh, J. Lusthaus, E. Gallo, F. Varese, 2020. Cooperation and distrust in cybercriminal markets - an experimental study of marketplace disruption. In: 2020 Extra Legal Governance Seminar series (ExLegi), May 8, Oxford, England.

L. Sebagh, J. Lusthaus, E. Gallo, F. Varese, 2019. Responses to Slander and Sybil Disruption Operations in Online Criminal Marketplaces - a Laboratory Experiment. In: 2019 European Economic Science Association (ESA) Meeting, September 5-8, Dijon, France.

Sean Sirur

Supervisors: Kasper Rasmussen, Department of Computer Science, Tim Muller, University of Nottingham

Initially interested in the distinct fields of mathematics and psychology, Sean was naturally drawn to computer science once introduced to its formal insights into reasoning, decision-making and communication. Attending the UoEdinburgh for a Bsc (Hons) in Computer Science and Physics, They specialized in security and formal methods, particularly formal languages and verification. Their dissertation focused on translating a formalism for communicating processes into an mathematically-formalized program. Statistical physics was their secondary focus.

While these mathematical interests both shape and apply to the methodology of their thesis, Sean's interests in psychology and welfare motivated the topic. Interested in privacy, Sean undertook a short research project interviewing SMES and multinationals about GDPR-compliance and their use of advice from various sectors. Sean's main focus is now on trust and reputation, however.

Sean also loves teaching. They currently work as a TA for both the Software Engineering Masters program and the Computer Science Dept, having worked in similar roles at Edinburgh. Their other interests include literature, art and music and they appear to be on fairly good terms with nature and the outside world.

DPhil Thesis: The Effects of Information Lag on Decision-Making in Trust Networks

Cooperative decision-making agents in many systems will spread information amongst themselves. When said information consists of evidence or beliefs about the pros and cons of interacting with some entity, the agents can be said to be making "trust" decisions about that entity and the knowledge sharing would then be an instance of "reputation". Examples include ratings systems (eBay, Trustpilot) or social media (Facebook, Twitter). Information propagation may suffer from delays, however. While much work has gone into constructing low-latency systems, very little research exists on the exploitation of this lag once present (dubbed "reputation lag attacks" or "RLAs").

There are no theoretical frameworks for such attacks. This thesis proposes to apply network theory (the mathematical study of networks) to formalize such environments. Spreading on networks, an active area of mathematical research, is a highly intuitive manner of capturing this sharing phenomenon and so may give new insights into the attack. Initial research consisted of building a preliminary formalism for RLAs and then provably demonstrating their existence. Future research includes investigating how attackers can improve their strategies; investigations into possible real-world instances of RLAs; and finding mitigations to RLAs.

Publications

Sirur, S., & Muller, T. (2019). The Reputation Lag Attack. In Proceedings of the 13th IFIP WG 11.11 International Conference on Trust Management July 17 - July 19, 2019, Copenhagen, Denmark

Sirur, S., Nurse, J.R. and Webb, H., 2018, October. Are We There Yet?: Understanding the Challenges Faced in Complying with the General Data Protection Regulation (GDPR). In Proceedings of the 2nd International Workshop on Multimedia Privacy and Security (pp. 88-95). ACM

Eva Stanková

Supervisor: Justine Pila, Faculty of Law

Eva is reading for a DPhil in Cyber Security at the University of Oxford within the CDT 2017 cohort. Her DPhil thesis is devoted to the legal implications of computational creativity of artificial intelligence-driven systems deployed in cyber defence. She looks at whether objects generated by those systems can be protected by patents or copyright under currently applicable law. Her thesis will also include policy recommendations focusing on promoting innovation and information sharing in the field of cyber security. In her mini-projects she focused on evolution of data protection regulation in Europe and legal implications of AI-driven creativity in cyber security.

After her graduation from the Law Faculty of Charles University in Prague Eva practiced law in Prague-based law firms as an Associate in corporate, IP/IT, media and telecommunication legal teams. In 2015, her interest in intellectual property law and competition law brought her to the Munich Intellectual Property Law Centre (MIPLC). Eva also dealt with policy coordination in internal market at the Secretariat General of the European Commission in Brussels.

DPhil Thesis: AI-Driven Defence Systems and the Limits of Copyright and Patent Law

This research deals with computational creativity in the context of the current state of the art artificial intelligence algorithms deployed in network defence. It features a legal assessment of whether objects generated by AI-driven systems qualify for copyright and patent protection under the current legal regimes in Europe and in the United Kingdom. In order to examine the eligibility for the legal protection, a human creativity requirement will be analysed, and it will be determined how it is applied to computer-generated objects. This project will conclude with recommendations towards such a legal regime for AI-generated objects which would be ideal for incentivising innovation in the field of cyber security.

Publications:

September 2019 From Creativity Requirements Towards Creativity Tests – a presentation given at the European Policy for Intellectual Property 14th Annual Conference at the ETH, Zurich

Conference talks:

January 2020 AI-generated inventions and creativity tests in patent law - an invited speaker at the European IP Institutes Network Innovation Society (EIPIN-Innovation Society) conference in Maastricht

Henry Turner

Supervisor: Ivan Martinovic, Department of computer Science

Henry comes from Colchester, Essex and holds a MEng from Imperial College London in Computing. His thesis examines security aspects of biometric systems, with a particular focus on voice processing systems and their resilience to realistic attacks, as well as developing ways to better protect users of these systems.

During his time at Imperial College London he completed his thesis on security schemes in body sensor networks and facilitating secure communication in embedded medical devices. He has interned as a software engineer at Intel Security (McAfee) working on corporate network monitoring products. Prior to this he also ran a small enterprise publishing iPhone and Android applications during his teenage years, distributing more than 250,000 copies of his applications during the project's lifespan.

DPhil Thesis: Improving the Security of Voice Interface Systems

Voice interfaces have become common on modern devices, and increasingly support complex interactivity, as well as authentication mechanisms to provide personalised (and sensitive) functionality to users.

We focus on such voice interfaces, and in particular improving their performance in adversarial situations. We do this through the testing of attacks against such systems and through the development of tools to analyse security properties. In turn these allow us to identify flaws and weaknesses in voice systems.

We then design improved voice interface systems to combat weaknesses and flaws we identify, to improve their overall security properties.

In addition to work on voice interface systems, we intend to try and translate some of our attacks and tooling to other biometric systems, to see if they suffer from similar weaknesses and can be improved in similar ways.

Publications:

Turner, H., Lovisotto, G. and Martinovic, I. Attacking Speaker Recognition Systems with Phoneme Morphing, European Symposium on Research in Computer Security 2019, 23-27 September 2019, Luxembourg

Innovation Inaction or In Action? The Role of UX in the Security and Privacy Design of Smart Home Cameras

George Chalhoub, CDT18, and Prof. Ivan Flechais

Smart home devices offer great utility and functionality. However, the rise in the adoption of those devices is accompanied with new security and privacy threats. The need for user-centered security and privacy design is important, given that inhabitants are demographically-diverse and have different abilities. Prior work has explored different usable security and privacy solutions for smart homes; however, the applicability of user experience principles to security and privacy design is under-explored.

In a joint work with researchers from University College London and Michigan State University, CDT18 student George Chalhoub explores how design teams factor UX into the security and privacy design of smart cameras. The study which was published in SOUPS2020 shows that UX was seen as helpful in fostering innovation in the design of privacy solutions. However, UX was not used or considered in the design of security solutions because of an explicit need for established, tried-and-tested security solutions.

Methodology

We conducted semi-structured interviews with 20 employees of three smart home companies in the United Kingdom, focusing on understanding their design processes and practices. We aimed to investigate the design, development, and implementation of three security camera products that had been in production for years. Our study aimed to address the following research question:

How do product design teams factor UX into the security and privacy design of smart home cameras?

After designing our initial interview questions, we conducted a small-scale pilot study with four designers of smart home devices at the third Annual Secure Internet of Things Security Conference in November 2019 in Reading. We used the findings to identify potential problems (e.g., adverse events, time, cost) in advance prior to conducting the full-scale study. Four researchers in total analyzed the interview data using Grounded Theory. The researchers met and discussed the differences and generated a codebook consisting of 155 initial codes.

Results

All product design teams used an agile methodology to drive the development process of their smart home cameras. We found that the practice of adopting 'tried-and-tested' security inhibits innovation in security design. In addition, the perception of security being only a technical problem, for which there are 'best practice' technical solutions, limits the consideration of social aspects of

security. In particular, it creates a gap between UX factors and the security design process (e.g., UX designers having no sight of any security requirements).

Despite the gaps that we found in security design, our results show companies innovate in the privacy design space (e.g., creating a novel geographic-based privacy feature). Our data shows that UX stakeholders in design teams elicited and handled privacy requirements. The practice of incorporating UX design principles to respect the privacy of their users (e.g., giving users control, intrusiveness, and avoiding creepiness) seems to encourage innovation in the privacy space. Moreover, we found that companies are motivated in preserving the trust-relationship and nurturing trust with their customers, as privacy or security failures (e.g., intrusive or vulnerable products) would undermine that relationship. Finally, regulation such as GDPR legally requires design teams to consider data protection by design in the requirements.

Implications

Despite recognizing the importance of security in the design process, our results show an inherent contradiction between tried-and-tested and innovative. Wanting innovative security is in conflict with the practice of favouring tried-and-tested security solutions or procuring

security solutions from reputable vendors. Furthermore, all design teams used agile methodologies which typically do not explicitly deal with security issues. Agile teams treated security as a technical problem with technical solutions, and not an area requiring innovation.

Conclusion

Our results show that tried-and-tested solutions were highly demanded in companies which prefer reliability and assurance (e.g., reusing existing good security practices). Those practices were shown to hinder innovation, however, we believe more research is needed to explore the relationship between UX, innovation, and security. In particular, a key issue is to uncover what aspects of a security design can be safely innovated, and how UX can be used to design more appropriate and effective user experiences in security.

In addition, there are notable effects that follow from the growing number of regulations and laws coming into force (e.g., GDPR) that traverse the design phase. Our participants reported that GDPR guidelines touched on facets of product design but often failed to translate into specific requirements which caused disparities in the design process. While GDPR requires practitioners to factor security and privacy into the design process, it can bring more confusion to the design table. More work needs to look into new techniques and tools that address how data protection regulations and practices can factor the application of UX design principles.

Ethics

This study was approved by The Central University Research Ethics Committee (CUREC/CS_C1A_19_049).

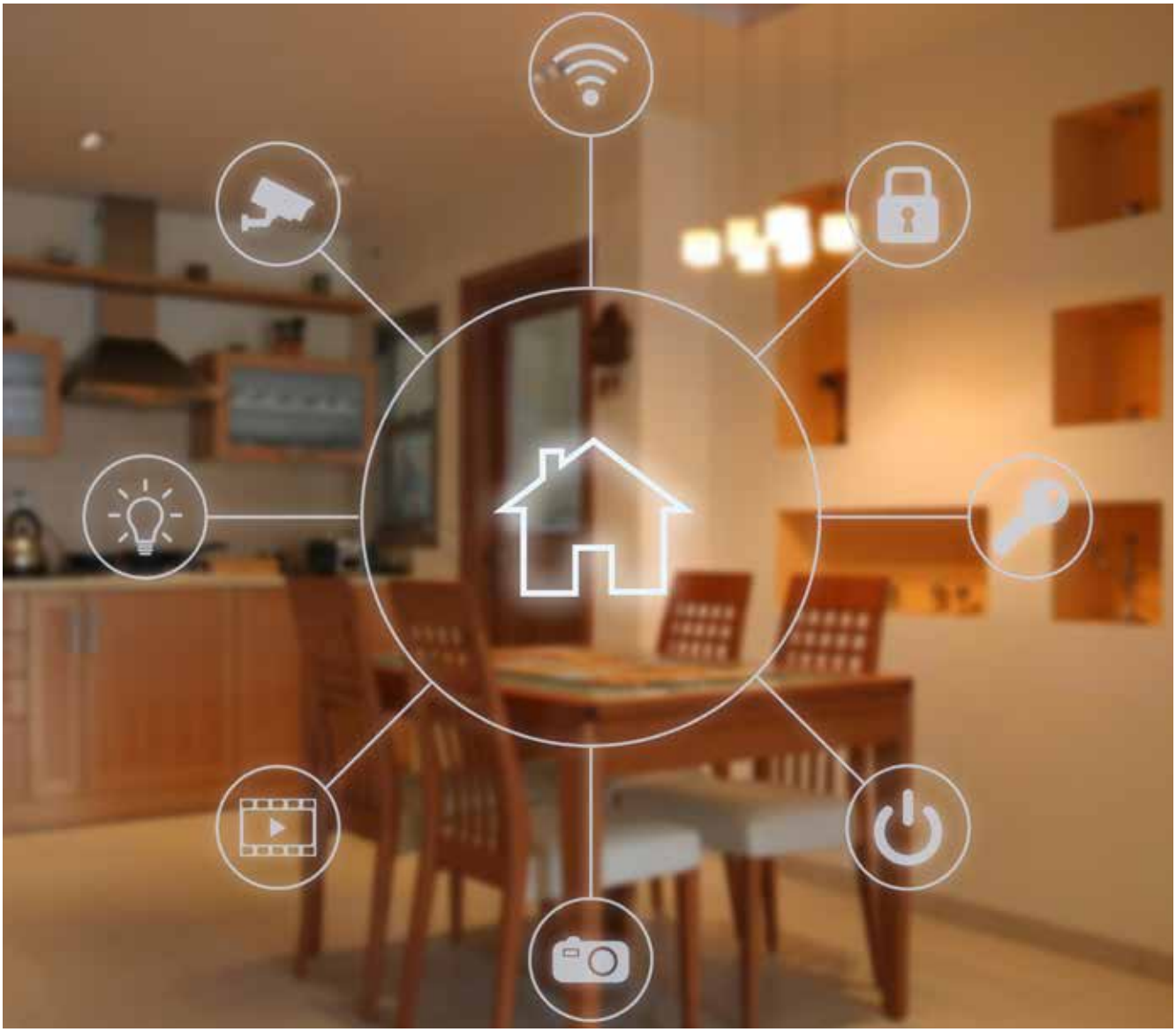
Acknowledgements

This study was supported by the 2018-2019 Information Commissioner's Office's (ICO) Grants Programme.

Publications arising from work

George Chalhoub, Ivan Flechais, Norbert Nthala, Ruba Abu–Salma and Elie Tom. Factoring User Experience into the Security and Privacy Design of Smart Home Devices: A Case Study. In Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems (CHI EA 2020). ACM. April, 2020.

George Chalhoub, Ivan Flechais, Norbert Nthala, and Ruba Abu-Salma. Innovation Inaction or In Action? The Role of User Experience in the Security and Privacy Design of Smart Home Cameras. In the 16th Symposium on Usable Privacy and Security (SOUPS 2020). USENIX Association. August, 2020.



2020 - University of Oxford Chess Cuppers

Jack Jackson, CDT18 and Anirudh Ekambaranathan, CDT18

There are many parallels to be drawn between the game of chess and the study of cybersecurity. As a practitioner of either art, you must anticipate the actions of others, whilst operating within a landscape in which every move matters. Often within cybersecurity, as in chess, losing isn't the same as failing. You can execute a seemingly perfect plan, but all it takes is a single slip to allow your opponent the opportunity to execute a move which devastates your defences. It is only natural then that the CDT boasts a number of chess enthusiasts within its ranks.

At the start of the 2019-20 academic year, two academics from the 2018 CDT cohort, Anirudh Ekambaranathan and Jack Jackson, commenced battle on the chess board for the right to represent Linacre College at the 2020 University of Oxford, Chess Cuppers. Both emerged victorious, with Anirudh taking his place at second board for the college, and Jack third.

Although Linacre college remains one of the smallest of its kind at the University, their four person team fought relentlessly, making it to the semi-finals of the tournament. Unfortunately, it was there that they were thwarted by Jesus college, who fielded the best chess player at the University at the time.

Whilst it can sometimes prove difficult to participate in extracurricular activities whilst reading for a DPhil, the CDT supports its students in doing so. In fact, it was a department approved grant which facilitated the purchasing of equipment to help both Anirudh and Jack in applying their knowledge to the chess board.

Whether it is extending upon the bodies of literature within their respective research domains, or demonstrating their strategic and tactical superiority over their opponents in friendly competition; the CDT is proud of its students' successes, and supports them in achieving their goals whatever they may be.

Quantum Cryptanalysis of Post-Quantum Cryptography Workshop

Romy Minko, CDT17

"[Post-quantum cryptosystems] are designed to resist the known quantum attacks, but can other quantum algorithmic tools be applied in novel ways to break the algorithms using the proposed parameters? Can new quantum algorithms break them?"
Simon's Institute for the Theory of Computing, https://simons.berkeley.edu/

In late February, I attended the Quantum Cryptanalysis of Post-Quantum Cryptography Workshop, run by the Simons Institute for the Theory of Computing, hosted by UC Berkeley. Due to some fortuitous scheduling, the Workshop coincided with the end of a series of workshops in lattice-based cryptography and the start of a series in quantum algorithms. Experts from both fields gathered to share insights into the potentiality and development of quantum attacks on cryptosystems. Pursuant to the primary goal of the Simons Institute, the workshop served to highlight opportunities for collaborative research.

The schedule was filled with talks from experts on both sides of the divide, covering all five main families of post-quantum cryptography. In lattice based cryptography, we were given an overview of state-of-the-art quantum cryptanalysis and connections between underlying hard mathematical problems, as well as progress made in algebraic techniques for lattice reduction. A number isogeny-based cryptography talks centred on the complexity of attacks against CSIDH, a relatively new system proposed to NIST for standardisation. We saw two different arguments discounting the viability of Chen et al.'s quantum attack against multivariate cryptosystems, one of which was the beginning of a larger body of work on condition numbers (results which are eagerly awaited). Finally, the open problems in hash- and code- based cryptography were explained and a representative from Microsoft gave us a crash course in Q#, an open-source language for developing quantum algorithms, and its use for quantum cryptanalysis.

A central theme of discussion between sessions was the nature of cryptanalysis research and the question of presenting failures in a positive light. Cryptanalysis research often involves many failed attempts at breaking a given cryptosystem, which can feel like a waste of time and resources. Rather than being a mere exercise in protecting academic egos, the discussion emphasised the benefits of publicising so-called failures, particularly for researchers new to the field. CFail, an annual conference celebrating abandoned approaches, was hailed as a perfect example, and further suggestions were made of starting a more regular newsletter of a similar nature. Towards the end of the workshop, we saw this mentality in action: Antoine Joux presented his work on Drinfield Modules, with the conclusion that they should not be used for isogeny-based cryptography. While failures in research is by no means unique to cryptanalysis, I am glad to be in a field that consciously attempts to champion every aspect of the research experience.

Attending this workshop was a wonderful opportunity to meet some huge names in cryptography, for which I am grateful to the CDT's Supplementary Research Fund. Watch this space for some results in quantum algorithms!

Interdisciplinarity in cyber security – a personal perspective

Mary Bispham, CDT15

Being a member of the CDT over the last few years has enabled me not only to pursue an original research project, but also to develop practical cyber security skills that have set me on a potential new career path. I came to the CDT with a mixed bag of professional experience and academic qualifications, the latter of which notably did not include a degree in Computer Science. In addition to academic training in different aspects of cyber security, the CDT also offered me the opportunity to engage with the practical aspects of cyber security through participation in Capture the Flag competitions as a member of the Competitive Computer Security Society, founded by fellow members of the CDT. Subsequently I was able to build on this experience in completing a six-month industry internship in penetration testing, and am now well-positioned to seek full-time employment in the penetration testing industry after completion of my doctorate. Whilst the core purpose of the CDT is clearly academic rather than vocational, the CDT's interdisciplinary environment provided me with an opportunity to make a change in career direction that would not otherwise have been possible, alongside the opportunity to conduct academic research.

My personal experience of the value of interdisciplinarity in cyber security is perhaps reflective of the wider development of cyber security as an academic field. There has been an increasing recognition that ensuring the security of computer systems requires not only technical expertise, but also input from other areas such as the social sciences, law and the humanities. Security guru Bruce Schneier has recently made the complementary suggestion that the role of the white-hat or 'public-interest' hacker might be expanded beyond a purely technical remit to address broader societal vulnerabilities. Schneier suggests that the skillset applied by benevolent hackers to identify unintended functionality in computer systems, so as to pre-empt its exploitation by malicious actors in specific technical scenarios such as SQL injection or buffer overflow attacks, might be adapted to identify potential for unintended consequences in social systems, such as legislative loopholes, deficiencies in electoral processes or vulnerabilities in human psychology. With this suggestion the concept of interdisciplinarity in cyber security may have come full circle, from the application of non-technical perspectives to the security of computer systems, to the application of a computer security mindset to the security of non-technical systems.

https://www.schneier.com/news/archives/2020/02/rsac_how_to_hack_soc.html

Project on Operational Cyber Security for the Industrial Internet of Things

Louise Axon (CDT14), Marcel Stolz (CDT16), Arianna Schuler Scott (CDT16), Katherine Fletcher, and Sadie Creese, Department of Computer Science

Between May 2019 – June 2020, a group of academics, students and staff involved with the CDT explored the upcoming operational security challenges in the Industrial Internet of Things (IIoT). The project was sponsored by the Lloyd's Register Foundation and led by Professor Sadie Creese, Robert Hannigan (Chairman, BlueVoyant, and Director of GCHQ 2014-17) and Ali El Kaafarani (CEO, PQShield), managed by Katherine Fletcher and researched by Arianna Schuler Scott and Marcel Stolz (current CDT DPhil students) and Louise Axon (a post-doctoral researcher and CDT alumna). The project has culminated in a Lloyd's Register Foundation Foresight Review, and will be made publicly available on the LR Foundation website (https://www.lrfoundation.org.uk/en/foresight/).

IoT-enabled industrial control systems (ICS) are becoming a significant proportion of our current and future critical infrastructures, with high uptake in areas such as energy, transport, buildings and physical infrastructure, and manufacturing facilities. The scale of Industrial IoT (IIoT) devices, networks and data, and interconnectedness of systems across organisations and industries, are growing rapidly. Industry and society are developing a critical reliance on IIoT systems and their "smart" functionality, and the consequences of failure can be high in these environments. It is essential that we understand how to deliver secure and resilient infrastructures.

The IIoT (alongside other emerging technologies such as Artificial Intelligence and Quantum Computing) will

exacerbate cyber security challenges that already exist, and will create new challenges of its own. The scale of devices and communications, volumes of data, and interconnectedness of organisations all make effective cyber security (and risk management) difficult. Moreover, new shared risks are introduced to systems (including risks to physical safety), contributing to an increased potential for severe and systemic cyber-harm. There is a need to analyse and evaluate the upcoming cyber security challenges for industry, and the actions that need to be prioritised in order to address these challenges.

Through several workshops we identified and considered the key risks that are emerging as the IIoT scales up, and explored whether the current operational change in cyber security will be sufficient to meet the likely demands of a future IIoT. The workshops were held in Singapore (October 2019), at Worcester College, Oxford (January 2020), and in San Francisco (February 2020) and attended by a range of experts from industry, academia, government and standards bodies.

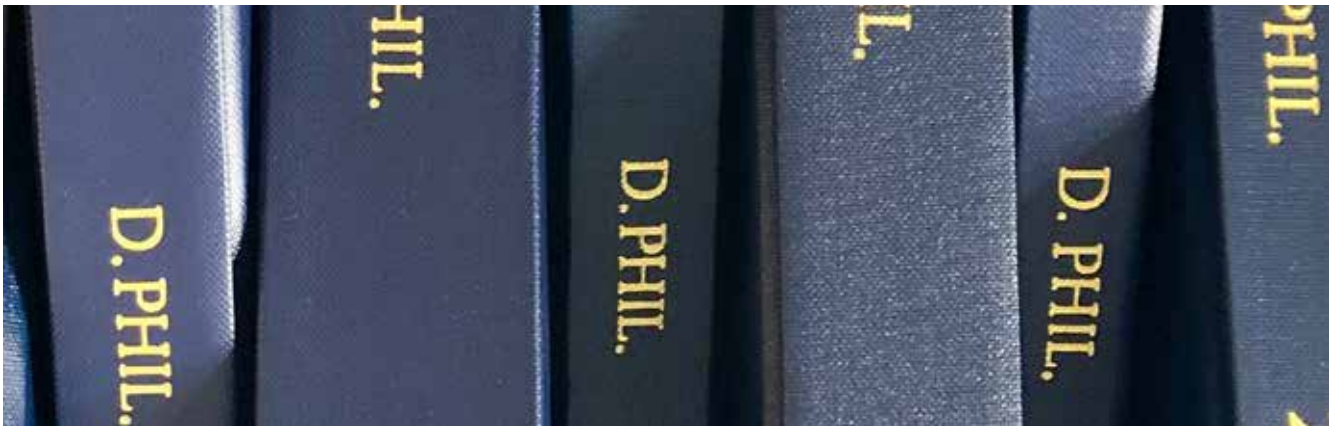
During the workshops, rich discussions were held around the risks that are emerging as a result of the adoption of the IIoT across multiple sectors, the extent to which existing and developing operational cyber security capabilities are sufficient to address these risks, where capability gaps exist that will not be closed through the current pace of change in operational cyber security (e.g., because capabilities do not scale, are not interoperable, are not technically feasible, do not exist yet, or are not tested), and the actions that need to be prioritised in order to address gaps. The workshops were also a great opportunity to make new contacts, travel to new places and see some sights!

A number of interesting findings emerged. It is clear that critical classes of risk control will be severely challenged by the IIoT, and will need evolved or new approaches in order to translate effectively. A key example is the inventory of devices: current approaches will likely struggle to cope with the scale-up, dynamism and complexity of the IIoT. It is not always clear which devices are "in" or "out" of a network, due to physical movement of devices, shared ownership models, and the ways software-defined networks can pop in and out of existence as needed: inventory snapshots are likely to go out of date almost as soon as they are made. This is particularly important since risk controls are interdependent: many other classes of risk control (e.g., monitoring, incident response and data protection) depend on having an accurate inventory of devices, so would also be impacted by this failure (i.e., the problem is more complicated than simply considering how individual classes of control will measure up in the IIoT).

Another example of a capability gap is recovery from a security incident: as manual fall-back becomes infeasible for large and complicated systems-of-systems, the approach to recovery will need to change (e.g., become more automated), because manual recovery processes will be too slow. The training of personnel will need to evolve as increasing numbers of organisations become newly reliant on the IIoT, and there are widening gaps in skills and awareness, and also conflicts between the decision-making of security and safety cultures within organisations. There are also challenges to actually researching and testing the vulnerabilities of, and security solutions for, many IIoT environments: in cases where the integrity and availability of systems is safety-critical, testing in the live environment is impractical and potentially dangerous. Live environments cannot just be pulled offline for a weekend of pen-testing. One of the report's key recommendations is the establishment of simulation facilities, to enable the community to conduct research into how to secure the IIoT in a consequence-free environment.

There was also rich discussion around how the increasing interconnectedness and interdependence of IIoT organisations is creating the potential for shared and systemic risk, creating challenges for assuring the trustworthiness of supply chains and third-party services, and creating complex challenges for deciding the primary liability and responsibility for security. This in turn creates new challenges for regulation and insurance, as we seek to promote improved security practice.

Based on our findings we made a number of recommendations for action: practical next steps that organisations using the IIoT can take, and areas that require further research and investigation. We hope to contribute to exploring solutions in some of these areas in the future!



Lessons learned: three ways to make your outreach successful

Arianna Schuler Scott (CDT16)

Whether we have a background in education, industry, the civil service or the private sector, all CDT applicants have had to put their communication skills to good use. As Professor Martin mentions in the foreword to this yearbook, the academic shift to online working has brought positive change: access to expertise and a much wider audience. Such a move has meant we have also had to rethink our research methods (in-person interviews are now calls), communication (conferences have gone virtual), and what "outreach" looks like. Being funded by the Engineering and Physical Sciences Research Council (EPSRC) means that my stipend is owed to the UK taxpayer. I design my research to receive input from members of the public, report findings in a way that is as clear as possible, and I commit to outreach work. At this CDT, we are at the bleeding-edge of academic contribution; we cover secure systems, verification and assurance, organisational risk, law and criminology, national security and international relations, and human aspects of Cyber Security. We have a duty to uphold our end of the social contract between academia and society because without public support, research would be very much harder to do. Part of this duty is to prioritise outreach where we can, and make our findings accessible. In some cases, these findings need to be accessible to policy-makers. In others, our role is simply to educate. In this article I will talk about a workshop I ran as part of a summer school for prospective students. I hope to encourage others to do the same – outreach is often seen as a barrier to good research (I have heard it described as time ill-spent!), but with clear parameters and good management it can be just as educational for both parties.

The UNIQ summer school opens up Oxford to the best and brightest 16-17 year olds for whom the university may not have traditionally been an option. Although it is usually a residential endeavour, the year of 2020 saw the summer school move online during lockdown. I took this opportunity to design and run a workshop that introduced 35 eager sixth formers to my research area: data protection. All was in hand, so I thought, as I have followed my academic focus through thick and thin over the past four years. I was reminded however, that to meaningfully engage in any project, you have to be all-in. I found that truly rewarding outreach teaches both sides something new, and requires blood (courage), sweat (constant vigilance) and tears (collaboration). My first encounter with UNIQ was last year, when I assisted with a colleague's workshop. The students were highly motivated and wanted to engage with the subject matter. The differing levels of Computer Science know-how echoed my own experience of the CDT, where as a cohort we needed to develop common understandings. When the opportunity arose to run a UNIQ session, I didn't hesitate to take it.

My time at the CDT had equipped me in every way possible, but there really is no substitute for hands-on experience. One of my personal mantras has always been that luck is simply "preparation meeting opportunity". I cannot remember where this comes from, but in this instance my mantra held. Experience is a hard taskmistress however, and there was plenty to learn. I came up against time, organisation and personal constraints despite an excellent grounding from the CDT in terms of project management, people management, and practical teaching experience. I have captured these challenges and my eventual solutions in the hope that this is the push that anyone reading this, who is also interested in outreach and public engagement, needs. From the CDT, I learned that you can teach well in lockdown. Adam is an expert in risk-modelling, with decades of industry experience. He employed a "flipped learning" approach in his online threat modelling elective. This meant he provided assignments ahead of time and spent class-time on discussion. Our classes were reflective – he asked us to summarise our takeaways and what had piqued our interest to tailor how he delivered the next session. Classes were discussion-heavy so there was no way we could avoid taking part, and every assignment we submitted received public feedback so that everyone benefited from lessons learned. From this class I learned that to be effective, an online class requires a substantial shift in culture. One does not simply take in-class methods and translate them directly, because online learning requires learner validation – check-ins. This is a shift in ethos as much as it is a shift in methods.

My research focuses on how data can be protected in different ways, and how those protections are built by interdisciplinary software development teams. My expertise and focus meant that everything about this project was going to work. 100%. My research focuses on communication – and I am a communicator, so what could go wrong? I put an outline together and submitted my proposal. I would draw on two things: my time organising hackathons in universities across the US and UK, and my previous CDT teaching experience that got cohorts forming groups, storming ahead, and performing to the best of their abilities.

Lesson 1: try not to rest on your laurels.

I did not know that trying to get students "forming groups, storming ahead, and performing to the best of their abilities" online requires a communication protocol. Without this, chaos reigns. Although everyone would be talking at the same time, no one would be communicating. The UNIQ liaison's email was kind, but their message was clear: the plan wasn't going to work. I had worked with 13 DPhil students face-to-face, and interacting with 30+ teenagers online was going to be entirely different. My tasks had many moving parts, and safeguarding concerns

meant that breakout groups would need supervision. My team could not accommodate this; my resources were limited. I had been confident in my initial plan and it took a long time to rethink how to communicate when the only way I could interact with students was via a chat function.

Lesson 2: there is no need to reinvent the wheel.

There is a significant body of literature on how to educate online – this is not a new field, and yet I had insisted on inventing my own teaching methods. Hours into the second iteration of this workshop I put pride aside and my postgraduate training kicked in: I threw my hands into the air and did some research. My original proposal consisted of a series of seven videos, each five minutes long. The group task that I assigned the students was to be completed over the hour-long lunch break they had scheduled. I had unwittingly put pressure on myself to create a series of seven videos, and in assigning work over a break I was planning to apply pressure to my students. It will be no surprise to you reader, I am sure, that asking students to work over designated free time is a no-no. Instilling unhealthy work habits early-on is frowned upon as a method, in the educator community. So I followed paths that others had walked before me: I shortened down to a series of five videos, each running between two and three minutes. I also enacted a strict "no working over lunch" policy. For the students, that is.

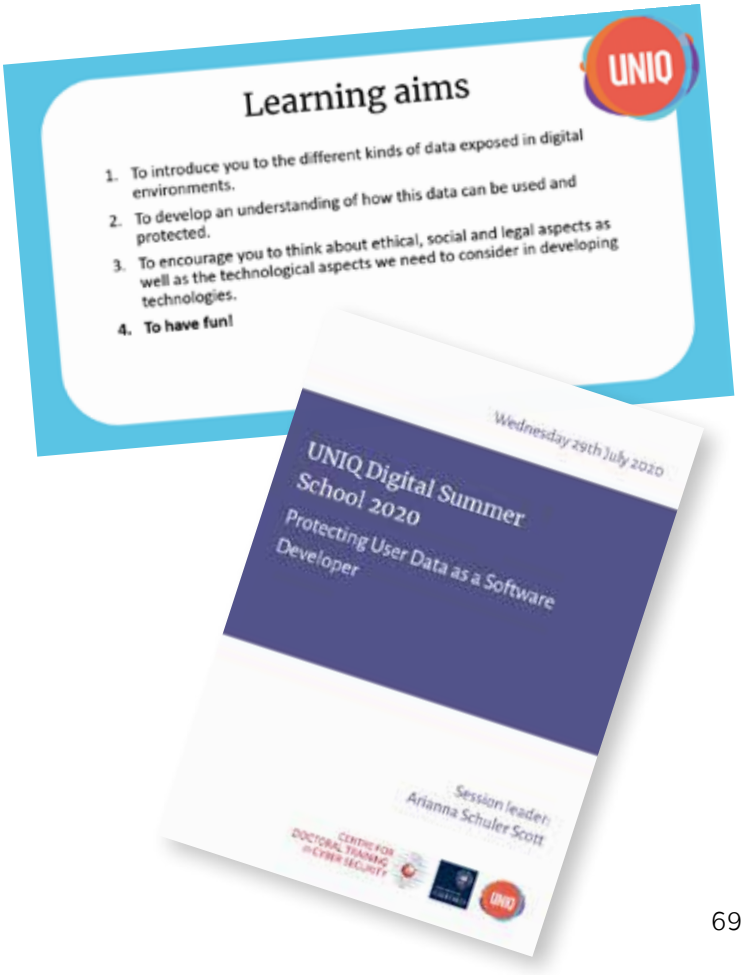
Lesson 3: use the people around you.

My frustration at investing significant time and energy into an outline that kept missing the point peaked at Proposal 2.0. I decided to ask my UNIQ liaison, colleagues and fellow educators a simple question – "what do you think"? The first rule of public engagement is to know your audience. It has been some time since I was 17 years old, so I needed help. My contact at UNIQ told me about similar sessions, and what had worked for similar, non-UNIQ online sessions. A CDT colleague reminded me that the cohort of students would have mixed backgrounds, suggesting I work from first principles. My teaching contact gave me some pointers, and told me that things were looking good. The more (targeted) input I asked for, the better my session was shaping up to be. As a subject matter expert I had not thought about my role as a facilitator (rather than dictator), learning requirements, and most importantly I had lost sight of how good things were looking.

I amended the workshop, recorded my videos and created a step-by-step student guide. Even if I had been hit by a bus the day before, this workshop would still run. I wrote my learning objectives and course aims down and shared those with my students. I told them what I wanted them to do, and why I wanted them to do it. I was honest about my own limitations and asked students to give themselves (and their classmates) space. On the day I ran into all sorts of problems, but their impact was negligible because I had set out my expectations for what I wanted my students to do. I made sure that I was providing regular feedback in the form of assessment feedback and simply reassuring my learners that they were doing well, signposting them to what was coming next. I finished off the session with a live Q&A. This was difficult to run, with one-way video and a chat function, but rather than show my frustration I emphasised how students *could* feedback and invited them to take part.

All in all, "Protecting User Data as a Software Developer" was one success in a week of many, and the feedback has been encouraging. Students have said "it was very interactive" and they "enjoyed the session". One student expanded by saying that they "loved the last lesson... (about security) since I got to work in a smaller group, so we all got the opportunity to say what was on our minds". I also received feedback from my colleagues - "you really nailed the interactivity, which is so important with pre-university students especially, and which academics tend to find it hard to do as it's very different from their usual modes of large group teaching". I am proud of this work, and I must acknowledge that it does not exist in a vacuum, only coming about through collaboration and working my contacts. It is a point of pride for me that "Importantly I think you got people interacting with each other and... [doing this] really well virtually, not an easy task!" and it is a testament to my time as part of the CDT otherwise I would not have been as well equipped to do the job.

My finishing point is that outreach work does not have to be difficult, but it must have purpose. This kind of work is incredibly rewarding and does not need to be done for free, neither should it act as a barrier to good research. More DPhil work could make use of (and benefit from) outreach promoting public awareness and understanding. Cybersecurity is as essential to the public interest as it ever was, and we exercise extraordinary privilege as researchers to put our creativity and knowledge to use in disseminating relevant information in a useful way.



CDT18 Bios

Freddie Barr-Smith

Supervisor: Ivan Martinovic, Department of Computer Science

Freddie holds a BSc in Computer Science and Business Management (First) and an MSc in Software and Systems Security (Distinction). He also has held positions in infrastructure and security in multiple sectors.

He also holds several security certifications including Offensive Security Certified Professional (OSCP), CREST Practitioner Security Analyst (CPSA) and CREST Registered Penetration Tester (CRT).

His research mainly is concerned with malware and the techniques cybercriminals use to counter and evade antivirus and other analysis systems. The objectives of his research being to illustrate and enumerate the various evasion techniques that are used by malware to evade manual and automated analysis. The formation of this research consists of analysis at scale of data and development of proof of concepts of these techniques. This research area also touches upon cybercrime and forensics.

DPhil Thesis: Volatile Anti-Forensic Techniques

The aims of this research are broadly to illustrate and enumerate the various evasion techniques that are used by malware to evade manual and automated analysis by analysts and automated systems. There are various ways to confound forensic analysis. Initially was focused on removing evidence from logs and hard drives. Has moved towards evasion of memory and dynamic analysis.
These evasion techniques include recognition of malign techniques which have evolved and become exponentially more complex as the arms race of malware development continues.

Analysis of these will include analysis at scale of existing and newly created malware, analysing large datasets from various threat intelligence providers. Additionally there will be creation of proof of concepts that demonstrate innovative techniques within this area and analysis of other malware activity at scale.

Furthermore, this research may involve discovery of flaws within antivirus software or other analysis software used to detect and analyse malware or cyber criminal activity. To an extent this flaw discovery can be identified as vulnerability research, with the aim of strengthening the tools used to analyse and protect against malware.
This research will strengthen skills in malware analysis, vulnerability analysis and penetration testing, skills necessary to forge a career in cybersecurity and skills of which there is currently a shortage.

This subfield has a constant flow of novel data and has the combined innovation of cybercriminals, a variety of nation state groups and academia contributing to it's rapid development. Therefore analysing this data will contain a large amount of novelty. Additionally contributing new techniques in this vein.

This research will involve active collaboration with a number of private sector companies. Additionally as results of this research may come in the form of detected vulnerabilities within existing antivirus detection and analysis systems, these will help strengthen these systems within both the private and public sector.

This collaboration between academia and private sector is especially important as many of the systems in use by the private sector are only under robust analysis by state actors. Due to this it is important to codify into the academic body of knowledge, the tools and techniques which may only be known or in use by criminal and state actors.

Publications:

Mini-Project: Living Off The Land: Systematic Review of Use of Living-Off-The-Land Technique by Malware

Mini-Project: Onion Optical Illusions: Imitation of Onion Services

Freddie Barr–Smith and Joss Wright "Phishing With a Darknet: Imitation of Onion Services" In 2020 APWG Symposium on Electronic Crime Research (eCrime). 2020.

George Chalhoub

Supervisor: Ivan Flechais,
Department of Computer Science

George holds a BS in Computer Science from the Department of Computer Science and Mathematics of the Lebanese American University. He obtained his MSc in Computer Science from the school of Electronics and Computer Science at the University of Southampton, in collaboration with Lloyd's Register. He previously worked as a Cyber Security Analyst and is currently an Expert Contributor at Oxford Analytica. His doctoral research is supported by the Information Commissioner's Office and explores the application of user experience (UX) principles in the security and privacy design of smart homes.

DPhil Thesis: The UX of Things: Exploring UX Principles to Inform the Design of Security and Privacy in the Smart Home

Smart homes are under attack. Threats can harm both the security of these homes and the privacy of their inhabitants. As a result, in addition to delivering pleasing and aesthetic experiences, smart devices need to protect households from vulnerabilities and attacks. Further, the need for user-centered security and privacy design is particularly important for such an environment, given that inhabitants are demographically-diverse (e.g., age, gender, educational level) and have different skills and (dis)abilities.

Prior work has explored different usable security and privacy solutions for smart homes; however, the applicability of UX principles to security and privacy design is under-explored. This research project aims to address the on-going challenge of security and privacy in the smart home through the lens of UX design. The objective of this thesis is two-fold. Firstly, to investigate how UX factors and principles affect smart home users and the product design process. Secondly, to inform product design through the development of an empirically-tested data-driven framework for UX design of security and privacy in smart home products.

In the first step, we aim to explore the relationship between UX, security, and privacy in smart homes from user and designer perspectives: through (i) conducting a qualitative interview study with smart home users (n=20) and (ii) analyzing data from a longitudinal study of smart home device adoption and use in households (n=6); and, we plan to explore the role of UX in the design of security and privacy in smart homes through qualitative semi-structured interviews with smart home designers through two rounds of interviews (n=20, n=20).

In the second step, using our exploratory results, we aim to build an empirically-tested data-driven descriptive framework for UX design of security and privacy in the smart home products. To evaluate the applicability of our framework, we are running participatory design workshops with a diverse group of smart home stakeholders. Finally, using our framework, we will extract thematic recommendations supporting security and privacy design practice in smart home products.

By bringing UX design to the smart home security and privacy table, we believe that this project will have a significant impact on academia, industry, and government organizations. Our framework will inform the product design process of security and privacy in this emerging technological area while contributing to scholarly practice.

Publications:

George Chalhoub. The UX of Things: Exploring UX Principles to Inform Security and Privacy Design in the Smart Home. In Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems (CHI EA 2020). ACM. April, 2020.

George Chalhoub, Ivan Flechais, Norbert Nthala, Ruba Abu-Salma and Elie Tom. Factoring User Experience into the Security and Privacy Design of Smart Home Devices: A Case Study. In Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems (CHI EA 2020). ACM. April, 2020.

George Chalhoub and Ivan Flechais. "Alexa, are you spying on me?": Exploring the Effect of User Experience on the Security and Privacy of Smart Speaker Users. In 22nd International Conference on Human-Computer Interaction (HCII 2020). Springer. July, 2020.

George Chalhoub, Ivan Flechais, Norbert Nthala, and Ruba Abu-Salma. Innovation Inaction or In Action? The Role of User Experience in the Security and Privacy Design of Smart Home Cameras. In the 16th Symposium on Usable Privacy and Security (SOUPS 2020). USENIX Association. August, 2020.

Anirudh Ekambaranathan

Supervisors: Max Van Kleek and Jun Zhao, Department of Computer Science

Anirudh holds an MSc in Computer Science and Education from Twente University in the Netherlands. His research focuses on applied machine learning in the context of cyber security. Currently he is researching anomaly based intrusion detection systems. His previous research projects focused on Wi-Fi tracking and stylometric linkability in darknet markets. Before joining the CDT he worked as a part-time math teacher in secondary school and had his own cyber security startup.

DPhil Thesis: Understanding Design Features of Family Apps and Design Choices made by Family App Developers

Children have established a significant presence online through mobile devices, leading to an increase in the number of apps designed for children. Mobile apps can provide educational value for children across the globe, giving developers the opportunity to make positive contribution. However, data monetisation remains the main source of income for developers in this space. Targeted ads or game promotions become the norms in the freemium apps, including those used by children. Children not only find them annoying and a waste of time, but also are often nudged to make choices that reduce their personal privacy and leave them more vulnerable to data tracking.

New initiatives are set up to improve children's data protection and online safety. For example, the ICO in the UK is setting up children-specific regulations, and the Federal Trade Commission in the US is calling responses to a review of the Children's Online Privacy Protection Act (also known as COPPA). However, to create proper regulations and incentivise developers to adopt age appropriate design guidelines, we need to understand (1) why responsible design choices are difficult for developers, (2) a better understanding of harms design features in children's apps may cause, and (3) tools for practitioners to effectively assess age appropriateness of children's apps.

Publications:

Mini-Project: Because we cannot control third-party adverts": Understanding Design Choices Made by Family App Developers

Mini-Project: GAN Based Anomaly Detection Using Protocol Conditioning and Feature Corruption

Marine Eviette

Supervisor: Andrew Simpson, Department of Computer Science

Marine is a Radcliffe scholar with interests in Privacy and Cryptography- having undertaken prior research in Post Quantum Cryptography, Cryptanalysis of Historical Ciphers and Online Privacy. Besides this, she previously completed a Masters thesis which sought to help prevent the propagation of Cyber Attacks by utilizing a ZKP verified Distributed Ledger Technology. Her current research interests, however, are strongly rooted in the area of Privacy; where she is choosing to pursue a DPhil project that focuses on exploring how access control models can help to prevent metadata exploitation in the era of big data, in order to aid in protecting users' privacy.

DPhil Thesis: Mitigating the Proliferation and Exploitation of metadata through introduction of Access Control

The implicit nature of consent regarding metadata currently enables companies to extort users' privacy and uncover, otherwise hidden, identity elements, which jeopardises users' sense of control. We find that the scale of metadata has led to online browsing habits shaping an extremely detailed trail of online activities via the passive digital footprints that are unknowingly left behind. Such digital footprints that are being accumulated by means of dataveillance have led to inferences on identity elements that dramatically expose user identity, whilst rendering these users powerless in the managing of their personal privacy.

By modelling privacy as an access control problem, we seek to combat inference-driven identity exposure that threatens user privacy. We aim to achieve this through clearly defined policies that target the aggregation of metadata and the consequent inferences. However, at present, there is no one unifying method to privacy and identity management as it relates to this problem. Therefore, whilst it may indeed prove fruitful to reason about access to data objects as a method of protecting individuals' privacy; without further consideration, we are set to be hindered by the unfavourable state of the internet today, as users currently have no control over their own data and consequently cannot control access to it.

The case for ownership becomes increasingly complex when we consider the analysis done on data aggregates; here, companies are analysing user

generated data, in order to identify patterns and make inferences. These subsequent processes generate a further set of data, which is often as valuable as the original data, yet this analysis information is automatically owned by the company performing the analysis.

In our work, we hope to reason about data collection and access control from the perspective of users which is decidedly a very challenging task, as users do not typically control access to their collated data. Coincidentally, there have been a number of projects that have begun to investigate methods for users to regain ownership, and consequent control, of their data, through the introduction of decentralised architectures that can be implemented atop of the current internet.

Our research project aims to leverage the solutions to these and similar privacy problems, in order to present preliminary ideas of access control modelling as it pertains to metadata and identity management. In line with this, we investigated numerous approaches to similar problems, whereupon we decided to follow a similar route to researchers' design of a framework for secure data collection through the extension of the Category-Based Access Control metamodel.

By utilising Category-Based Access Control we hope to be able to build upon the foundations of access control, so as to reason about this complex privacy problem. Our proposed research is of significant value as there is a pressing need for more transparency amongst sharing and management of metadata online.

Publications/ Conferences:

Dec 2020: Towards models for the Mitigation of Metadata Exploitation

15th IFIP Summer School on Privacy and Identity Management – IFIPSC2020

Co-author: Andrew Simpson

Jun 2019: Cybersecurity and Intimate Partner Violence

Connected Life Conference 2019

Co-authors: Julia Slupska, Romy Minko, Zhi Tan and Fatima Zahra

Martin Georgiev

Supervisor: Ivan Martinovic, Department of Computer Science

Martin holds a BEng degree from the University of Edinburgh which incorporated an exchange year at University of California, Irvine (UCI). During his stay abroad, he developed an interest in cyber security and published a joint paper with the SPROUT (Security and Privacy Research OUTfit) group at ESORICS. He has various internship experiences ranging from detecting compromised accounts at Facebook to developing innovative systems for the banking industry at Royal Bank of Canada. At Oxford, Martin is interested in authentication using behavioral biometrics. More specifically, he is looking into models for continuous mobile authentication based on touch patterns, their practical applications and privacy concerns stemming from their use.

DPhil Thesis: Behavioural Biometrics for Authentication

The research project aims at investigating the feasibility of using various behavioral biometrics in authentication scenarios. This field of study focuses on establishing uniquely identifying patterns in human activity such as keystroke, mouse and touchscreen dynamics as well as voice, gait and cognitive behaviour. This is typically a non-invasive method for authentication as it does not require users to learn how to operate a particular system or remember unique passcodes and phrases. Furthermore, there are no active steps required for authentication but rather it is a seamless integration with the regular operation of the system. Often authentication systems based on behavioural biometrics can be used as a multifactor safeguard in conjunction with other more traditional cybersecurity measures. Despite being a somewhat well research area with some apparently successful projects currently there are few successful commercial systems employing the technology. The goal of the research is to design, develop and test novel systems for authentication based on behavioural biometrics and close the gap between promising research and practical applications. For instance, developing a continuous authentication model based on phone usage patterns such as touchscreen gestures and gyroscope micro movements in space. Another aspect of the project focuses on identifying problems in past research in the area and some of the reasons it tends to be unsuitable for practical use. For example, the reported sample sizes in some of the studies might not be large enough to accurately represent the population using such systems. Finally, there are unique privacy challenges stemming from the use of highly accurate authentication systems based on behavioural biometrics. One way to maliciously employ this technology is to create unique fingerprints for users which can then be exploited for tracking behaviour and identity throughout multiple non-connected systems. It also might be possible to reveal personal information about users through their behaviour patterns. Gender, age and cultural groups could exert specific traits which might be detectable by the technology described above.

Publications:

Mini-Project: Adversarial noise injection into digital images through electromagnetic interference

Mini-Project: Towards continuous touch-based mobile authentication using neural networks

CDT18 Bios continued

Hayyu Imanda

Supervisor: Kasper Rasmussen, Department of Computer Science

Inda is a Jardine Scholar at Exeter College. She grew up in Jakarta, Indonesia before moving to the UK to take her BSc in Mathematics from the University of Edinburgh. She then completed her MSc in Mathematics and Foundations of Computer Science at Oxford, where she focused on post-quantum cryptography, with a dissertation on the security of supersingular isogeny key exchange.
After briefly working as a software developer, she went home to Jakarta and took an internship at a consultancy before starting the CDT. In her first year, she co-organised the CDT in Cyber Security conference with Royal Holloway.
She is a 2x full Blue in lawn tennis and the incoming president for the Oxford University Lawn Tennis Club. She feels most at home out in the ocean scuba diving, and deeply cares about wildlife conservation; when possible, she spends time away from Oxford travelling across her diverse home country. You might also find her stranded abroad during a pandemic!

DPhil Thesis: Modelling an Adversary with Privileged Access

Traditional adversary models in cryptography primarily assumes a network adversary with no access to endpoints. We now know that this is far from sufficient. Adversaries with a higher capability, with continuous authorized access to endpoints for example, benefit from the lack of sufficient security design against them. My research aims to model an adversary with a high level of control over the network, as well as access to privileged information. In particular, I am looking at cases where there exists an asymmetric power dynamic between the adversary and the victim; for example, government whistleblowers, intimate partner violence, and those under targeted surveillance. Due to the power imbalance between the victim and the adversary, previous mitigations to endpoint compromise -- for example, key rotation, wouldn't suffice. New security goals have to be defined, and we design cryptographic mitigations which satisfy those goals.

Publications:

Mini-Project: Mass Surveillance and Isogeny-Based Cryptography: An Introduction

Mini-Project: Location Privacy in Conservation

Jack Jackson

Supervisor: Max Van Kleek, Department of Computer Science

Jack is currently a DPhil Researcher at the University of Oxford, where he resides within the Centre for Doctoral Training in Cyber Security. Jack has previously held roles as a Chief Technology Officer, Principal Technology Consultant, Research Scientist, Cryptographer, and Cognitive Engineer; across a number of Europe's most prolific Startups. For his work, Jack has been honoured with a number of accolades, including a Europe-wide entrepreneurship award. He has also acted as both a keynote and guest speaker at several prolific conferences, including the International Workshop on the Future Perspective of Decentralized Applications, held in conjunction with the 24th International European Conference on Parallel and Distributed Computing - where he also sat as a Program Committee member.

Before joining Oxford, Jack made a name for himself within both the Startup and Blockchain communities across Europe. This stemmed from his researching into privacy-enabling blockchain technologies, where he explored the application of advanced cryptographic mechanisms, such as: homomorphic encryption, differential privacy and secure multiparty computation - to distributed ledger ecosystems. In recognition for his efforts, Jack was invited to act as an Associate Editor at Frontiers Open Access Journal, where he curated his own section on the Fourth Industrial Revolution. In this role, Jack leads a team of seasoned academics, consisting of established professors and postdoctoral researchers.

Whilst at Oxford, Jack has been invited to act as an Expert Consultant on Blockchain Technologies by United Nations (UN) entities. As of 2019, Jack has committed to conducting research into a number of areas, including: cyber insurance, social engineering, and the development and application of deep fake technologies. To these ends, he is utilising his rich and diverse background, which branches across a broad array of areas within: insurance, artificial intelligence, cryptography and distributed ledger technologies.

DPhil Thesis: Deep Phishing

While advances in security and software engineering processes have greatly increased the robustness and resilience of software to cyber attacks, comparable advances in cyber security resilience have not been made at the human level. This shortcoming can be effectively observed across a spectrum of successful human-centric cyber crime campaigns, such as: social engineering, phishing and psychological operations (PsyOps). Recent developments in the field of artificial intelligence (AI) and increased data collation capabilities facilitated by methods drawn from social engineering, threaten to increase the effectiveness of these attacks. Providing adversaries with the extended capability of scaling their capacity to both act and sound human, underpinned by the information necessary to inform attempted mimicry. Two such advancements include the introduction of deep fake technologies, which have enabled the hijacking of trusted personas at will, by means of impersonation; and the development of open-source intelligence (OSINT) tools, capable of mining publicly accessible information, such as that on social media sites. Understanding the threats these technologies pose in the context of cyber security, especially in the context of enabling targeted social engineering, remains an under-researched area. To these ends, we plan to evaluate existing attack frameworks across each of the aforementioned criminal domains, identifying key aspects which may be automated or enhanced through the assumption of AI. In particular, we aim to explore potential capability extensions within targeted spear phishing campaigns, enabled by the introduction of deep fake technologies into the kill chain; in what we refer to as a Deep Phishing attack. Deep Phishing can best be defined as the AI-facilitated impersonation of an individual, for the purpose of extracting information from a target with which they have sufficient social proximity.

The primary intended outcomes of our research are threefold. First, we aim to extrapolate future attack models given the observable advances in deep fake generation capabilities, and how that might impact more traditional social engineering attack models. Second, we plan to gain an understanding of the identified emerging threats, through the prototyping of software capable of performing the proposed attacks. Finally, we intend to explore potential mitigation strategies, including improving target resilience through automated, AI-based red-teaming against individuals. Beyond this, we wish to analyse how accessible information on an individual (via sources such as social media and data leaks) can be indicative of one's exposure to attack, through data correlation; with the goal of informing future personal information publishing decisions, and next generation user authentication protocols. To these ends, we hope to understand whether fundamental knowledge gaps across users could be addressed using intelligent tutoring (ITS) approaches to personalise and tailor representations with detail appropriate to the user's understanding.

Publications:

Mini-Project: Deep Phishing

Mini-Project: Creating a Pre-Competitive Dataset for Cyber Risk

Talks:

Social Engineering: HSBC Cybersecurity Awareness Week 2019

Deep Fake Technology, CDT Showcase 2019

Deep Phishing: Social Engineering, Redefined as part of Commonwealth Members of Parliament briefing day "Research, Risk and Resilience: Cyber Security and Public Policy", 2020

Sebastian Köhler

Supervisor: Ivan Martinovic, Department of Computer Science

Sebastian is a doctoral researcher in the Centre for Doctoral Training in Cyber Security at the University of Oxford. As part of the Systems Security Lab (SSL), run by Professor Ivan Martinovic, he researches the security of the physical layer of a variety of large and complex systems, such as vision-based intelligent and automotive systems.

He started to specialise on Cyber Security during his undergraduate studies in Computer Science at the University of Applied Sciences Würzburg-Schweinfurt, Germany. Due to his interests in the security of modern cars, he completed his bachelor's degree with a dissertation at the research and development centre of the Dr. Ing. h.c. F. Porsche AG. Before his doctorate, he received a master's degree in Computing & Security and got awarded the prize for the best overall performance on the MSc in Computing & Security for the academic year 2017/18 from King's College London.

In his spare time, Sebastian enjoys improving his knowledge and skills by attending Capture the Flag challenges, hackathons and conferences. As the president of the Competitive Computer Security Society, Sebastian shares his passion for security-related topics by organising and hosting different events, such as workshops, CTFs and talks. Recently, he has been selected to serve as a Shadow Programm Committee member for IEEE Security & Privacy 2020, one of the most prestigious security conferences.

DPhil Thesis: Exploiting Physical Phenomena to Enhance the Security of Cyber-Physical Systems

Large and complex cyber-physical systems, such as autonomous vehicles and industrial control systems, are increasingly relying on the input of a wide variety of sensors. For instance, self-driving cars often use Light Detection and Ranging (LiDAR) in combination with cameras to perceive their environment. In general, a sensor measures a physical quantity such as light, heat and sound. With the ongoing integration of sensors into the decision-making process of cyber-physical systems, the integrity of the measurements is becoming a cornerstone of the correct behavior of the system. However, a sensor cannot validate the authenticity of the measured quantity. An adversary could tamper the measurement by injecting malicious electromagnetic signals into the sensor to spoof a physical stimulus.

In addition, the secure interconnection of those systems to exchange information, such as the sensor measurements, is becoming more and more crucial. A recent example is the communication between an electric vehicle and a charging station. During the charging session, the vehicle measures the State of Charge (SoC) and the battery temperature and reports them to the charging station, which in turn regulates the maximum current. This enables a gentler and faster charging process. This communication has to be secure to ensure that an adversary cannot tamper the communication and spoof the sensor measurements. However, recent research has shown that attacks on the physical layer using electromagnetic waves can bypass security mechanisms on higher layers.

This research project is twofold. On the one hand, we demonstrate signal injection attacks on the physical layer against critical components of cyber-physical systems to impair their correct functioning. For example, we analyse how an adversary can interfere with the charging communication of electric vehicles using electromagnetic waves to interrupt the charging process or even cause irreversible damage. On the other hand, we evaluate defense mechanisms to protect against such attacks. More precisely, we investigate how physical phenomena associated with signal injection attacks in the wireless domain can be facilitated for attack detection and prevention.

Publications:

Mini-Project: Using Structured Demand Manipulation Attacks to Disrupt the Power Grid

Mini-Project: Interrupting the CCS Charging Communication using Radio Frequency Interference

Arthur Laudrain

Supervisor: Lucas Kello, Department of Politics and International Relations

Arthur P.B. Laudrain (@APB_Laudrain) is a Rotary Global Scholar for Peace and a doctoral researcher in cybersecurity at Wolfson College. His interests relate to decision-making, coercion through cyber means and assessing states' military capabilities in cyberspace. He has collaborated with the French Strategic Research Institute (IRSEM, Paris) and is consulting for the International Institute for Strategic Studies (IISS, London). His writing was featured on BBC Science Focus, Lawfare, The Military Balance+ and The Journal of Political Science Education. Arthur previously attended King's College London and Leiden Law School.

DPhil Thesis: Hacks, Leaks and Statecraft: Determinants of Foreign Policy Response to Electoral Interference

Most states consider state-sponsored cyberattacks, including influence and electoral interference operations, to be a critical threat to their national security. Yet, we have little understanding of how states react to these threats when they materialise. In three recent cases of electoral interference (DNC leaks, Macron leaks, Brexit referendum), the response of the respective states brings questions, in particular as to their timing, their domain of action and the resources committed. Why did the United States, France and the United Kingdom either fail to respond or responded lightly to foreign interference in their democratic processes? With this research project, I suggest that by investigating key players and group dynamics during the foreign decision-making *process*, I may be able to contribute to the explanation of restraint as a foreign policy *outcome*. To do this, I leverage the rich theoretical framework of Foreign Policy Analysis.

Writings and Publications

Trey Herr, Arthur P. B. Laudrain & Max Smeets, "Mapping the Known Unknowns of Cybersecurity Education: A Review of Syllabi on Cyber Conflict and Security", Journal of Political Science Education, 28 Feb 2020.

Arthur P. B. Laudrain, "5G and the Huawei controversy: is it about more than just security?", BBC Science Focus, 21 Mar 2020.

"France's 'strategic autonomy' takes to space", International Institute for Strategic Studies (London), 14 Aug 2019.

"France's New Offensive Cyber Doctrine", Lawfare (Washington DC), 26 Feb 2019.

Conferences

"The State, its Institutions and Processes: Applying Decision-Making Models to French Cyber Security and Defence", Bridging the Gap Workshop, Columbia SIPA (NYC), 11 – 12 Nov 2019.

"The Paris Call for Peace and Security in Cyberspace: A Year Later", Global Governance of AI and Cyber Security Panel, Bonn International Security Forum, 1 – 3 Oct 2019.

"Military Cyber Operations: Comparative Approach of France and the UK", National Research Agency Cyber Studies Seminar, Université de Bordeaux, 6 Jun 2019.

Matthew Rogers

Supervisor: Kasper Rasmussen
Department of Computer Science

Matthew is a 2018 Rhodes Scholar with a degree in software engineering from Auburn University. His experience includes work with Dynetics, an engineering firm, doing malware analysis and reverse engineering APT malware. Additionally he has spent time at the Defense Digital Service, bolstering their cyber capabilities. He has spoken at several conferences on malware analysis and cyber security education. His research focuses on creating cheap intrusion detection systems for serial data bus networks, primarily J1939. From this he hopes to build out mission assurance research for critical transportation and military system.

DPhil Thesis: Securing J1939 Systems through Minimal System Modifications

Since the early 2000s millions of industrial systems have taken their existing Controller Area Network (CAN) Bus infrastructure and added a software standard, J1939, to simplify communication between the different electronic control units (ECUs) controlling the vehicle. The standard was initially designed for ground vehicles, but is now common place across agriculture and forestry equipment, military vehicles, marine vessels, power generators, and much more. While this is useful for industrial systems, the underlying infrastructure is still CAN, a serial data data bus protocol with no authentication, or effective security mechanisms. For the last decade academia and enthusiasts continually showed hacking an automobile is possible with access to the CAN Bus, even going as far as remotely gaining access. The J1939 standard only simplifies the hacking process by removing the need for reverse engineering the proprietary CAN messages of consumer automobiles. Not only does this simplify hacking single vehicles, it makes attacks agnostic to installed ECUs, enabling non-targeted attacks across fleets of heterogeneous vehicles.

We propose using the J1939 standard for defensive purposes. Instead of relying purely on header and timing data we can analyze the data field, making sense of the 8 bytes of data previously left untouched for practicality's sake. We begin this research with 2 premises: we can only add a single device to the J1939 Bus without modifying any existing ECUs, and we cannot have any false positives. Modifying every installed ECU is expensive, and discourages future firmware upgrades, effectively discouraging security. False positives generally risk alert fatigue, causing true positives to go unnoticed. The safety critical systems typically found running J1939 are too valuable for any level of false positives to be acceptable. To test for false positives we run our IDS against real truck data.

For this research we built a state-based rules framework which compares arbitrary J1939 data fields, adjusted to their real values. In doing so we created over 40,000 rules, 10,000 of which require some level of training to maintain system knowledge across system reboots. With these rules we are able to detect an attacker transmitting fixed-rate messages (e.g., every 100ms) across the bus if a legitimate ECU is already transmitting it. We apply this same timing based security guarantee to non-fixed-rate messages by ensuring the conditions for that message, such as a diagnostic trouble code message, being sent are met. These conditions come from fixed-rate messages, and so provide the same security guarantee. Additionally we ensure the attacker is unable to prevent an existing ECU from speaking short of physically removing it from the CAN Bus, an action that requires far more advanced physical access than traditionally seen in automotive hacking. This work falls within the EPSRC engineering research area, and was done in collaboration with Shift5 Inc. Future work will being the areas of Incident Response using the J1939 standard, using side-channel mechanisms for defensive purposes, and using a hueristics approach on the J1939 data field.

Talks:

Speaker at the Association of Old Crows 55th Symposium panel on "Preparing EMS Superiority" : "Electronic Sheepdogs : Providing the Hacker's Mindset to Everyone"

Publications:

Mini-Project: Incident Response and Prevention Recovery in J1939

Mini-Project: A State-Based Rules Framework for Serial Data Bus Networks

Yashovardhan Sharma

Supervisor: Ivan Martinovic, Department of Computer Science

Yashovardhan has been fiddling with computers ever since he was a toddler. A penchant for testing the limits of what was possible given a computer system made him naturally inclined towards computer security.

He completed his MPhil in Advanced Computer Science from the University of Cambridge and his BTech (Honours) in Computer Science and Engineering from IIIT-Delhi. Having worked on projects ranging from Healthcare to Artificial Intelligence to Human Computer Interaction, his focus recently has been on the area of Privacy and Security, with an emphasis on Cryptography. During his sojourn at Oxford he hopes to design and build trusted systems that leak minimal information and are reasonably resistant to compromise.

The interdisciplinary and collaborative nature of the CDT is a key reason for Yashovardhan to have come to the "other place". Born and raised in India, he is also known for his ability to enjoy non-spicy food.

DPhil Thesis: Analysing the Safety of Collision Avoidance Protocols in Aviation

Collision avoidance protocols for autonomous and semi-autonomous vehicles form the backbone of a safe and reliable global transportation system. In the case of aviation, the Traffic Alert and Collision Avoidance System (TCAS) is responsible for ensuring the safety of aircraft and reducing the chances of mid-air collisions. However the safety and efficacy of TCAS is yet to be analysed from a security perspective- especially given the current and ever-increasing levels of air-traffic with regard to a protocol conceived nearly two decades ago.

This research project aims to model and analyse the constraints specified by TCAS that are required for safe operation. The goal is to determine whether TCAS still meets its operational goals with regard to collision avoidance, and further investigate whether it is vulnerable to malicious attack. The novelty of our research methodology is that we use real-world data (aircraft transponder messages) for our analysis of TCAS's safety, rather than relying on simulations or statistical testing. This allows us to glean accurate and up-to-date information regarding the usage of TCAS around the world. Based on our results, we are then in a unique position to understand the potential risks posed by TCAS, the consequences posed by them, and most importantly - possible methods of remedying them.

Publications:

Mini-Project: Analysing the Safety of Collision Avoidance Protocols in Aviation

Mini-Project: Exploring the Impact of Availability in Secure Enclaves

Anjuli R. K. Shere

Supervisors: Andrew Martin, Department of Computer Science and Jason Nurse, University of Kent

Anjuli (@AnjuliRKShere) is an analyst, writer, and researcher, with experience of journalistic and security-related investigations. While attending 'Particle Summer School' at CERN, she was inspired by the scientific progress created by global collaboration. She has since studied a BA (Hons) in Politics and International Relations at the University of Nottingham, and spent a year gaining a Certificate in Social Sciences and Humanities at Sciences Po, Paris.

Alongside her master's degree in Science and International Security in the Department of War Studies at King's College London, Anjuli began reporting on current affairs for the New Statesman. She specialised in strategic security threats posed by emerging technological concerns, and wrote her dissertation on the extent to which machine learning could protect the NHS from cyber-attacks. Her professional endeavours also include working as the conference and research analyst for the Association for International Broadcasting.

During the first year of her doctorate in Cyber Security at the University of Oxford, Anjuli co-organised and emceed the CDT conference on Cyber Espionage and returned to her work as an intelligence analyst on Channel 4's award-winning fugitive simulation, 'Hunted'. She also conducted cross-disciplinary research projects within the faculties of Law and Computer Science, covering open-source intelligence, data protection legislation, state surveillance and emerging technologies.
Currently, Anjuli's thesis research aims to create a framework for mitigations of Internet of Things threats to the free press, for transcontinental news organisations to integrate into their cyber security strategies. Her case study countries are the UK, USA, Australia and Taiwan.

DPhil Thesis: How can physical, legal and virtual threats from novel Internet of Things devices affect press freedom in the UK, USA, Australia and Taiwan, and how might these threats be mitigated?

The existence and maintenance of a free press can be used as a barometer for the state of a democratic society, as public access to factual information about powerful people and organisations is key to an educated electorate. Therefore, attempts to curtail transparent, accessible and free journalism can be seen as threats to a branch of the critical national infrastructure of a democracy, and thus to the democratic state itself. This has potential implications on an individual human rights level and in terms of international relations and security.

My DPhil research aims to comprehensively investigate and document what journalists and media organisations are doing, procedurally and technologically, to protect themselves against innovative and well-resourced attackers. I would compare this with the recommendations of experts from a variety of backgrounds, including academic, governmental and non-governmental. The objective is determining the extent to which the current protections (and the systems by which these are chosen and updated) are effective against contemporary and anticipated threat models - particularly emerging technological and legal threats – and how these protections might be improved for my chosen case studies and for news organisations in democracies more broadly.

Publications:

Jun 2020: Selected to present "Now You [Don't] See Me: How have the GDPR and a changing public awareness of the UK surveillance state impacted OSINT investigations?" (my Mini-Project 1 findings) at the Surveillance and Society conference in Rotterdam (postponed due to COVID-19)

Jun 2020: "Reading the investigators their rights: A review of literature on the General Data Protection Regulation and open-source intelligence gathering and analysis" (my Mini-Project 1 literature review) is to be published in the SCR peer-reviewed publication affiliated with New College/University of Oxford, The New Collection, http://mcr.new.ox.ac.uk/journal/

May 2020: "Securing a Free Press inside a Networked Panopticon: The case of the Internet of Things" (my Mini-Project 2 report) was published at The 5th European Workshop on Usable Security (EuroUSEC 2020), https://eusec20.cs.uchicago.edu/eusec20-Shere.pdf

Jan 2020: "Growth of privately held data increases risk of espionage" (co-written with Neil Ashdown) for Jane's Intelligence Review, https://www.janes.com/images/assets/638/94638/Growth_of_privately_held_data_increases_risk_of_espionage.pdf

Nov 2019: "AIB November Meeting Report," in AIB Media Freedom Initiative Briefing and Update for Members, https://aib.org.uk/Media-Freedom/AIB-Media-Freedom-Initiative-report-191119.pdf

Oct 2019: "5th Annual Inter-CDT Conference: Cyber Espionage Report," in University of Oxford CDT in Cyber Security Yearbook 2019, https://www.cybersecurity.ox.ac.uk/site-resources/uploads/2020/02/2019-yearbook_web.pdf

May 2019: Centres for Doctoral Training in Cyber Security: University of Oxford & Royal Holloway Cyber Espionage Conference Report: 2nd-3rd May 2019, https://pure.royalholloway.ac.uk/portal/files/33922755/Cyber_Espionage_Conference_Report_.pdf

Dec 2018: "ASAP90 Conference 27th-28th September 2018 Report" for the Association for International Broadcasting, https://aib.org.uk/asap90-conference-27th-28th-september-2018/

Sep 2018: ASAP90 Conference Guidebook & Radio Taiwan International corporate social responsibility pledge, https://asap90.rti.org.tw/wp-content/uploads/2018/09/CONFERNCE-WITH-NOTES-20SEPT2018-0926.pdf

New Statesman (profile: https://www.newstatesman.com/writers/321610)

Julia Slupska

Supervisors: Gina Neff, Mariarosaria Taddeo, Joss Wright, Oxford Internet Institute and Max Van Kleek, Department of Computer Science

Julia Slupska (@jayslups) is a doctoral student at the Centre for Doctoral Training in Cybersecurity and the Oxford Internet Institute. Her research focuses on how cybersecurity concepts and practices can address technologically-mediated abuse. She is also exploring how feminist theories and methodology—such as participatory action research and the ethics of care—can improve cybersecurity. Previously, she completed the MSc in Social Science of the Internet on the role of metaphors in international cybersecurity policy. Before joining the OII, Julia worked on an LSE Law project on comparative regional integration and coordinated a course on Economics in Foreign Policy for the Foreign and Commonwealth Office. She also works as a freelance photographer.

DPhil Thesis: Design Justice in Security Architectures

Feminist theorists have long argued that gendered security problems, such as domestic abuse, are "individualized" and taken out of the public and political domain (Tickner 2004; Walby et al 2014).

Unfortunately, the emerging field of cybersecurity risks recreating these dynamics by omitting or dismissing gendered technologically-facilitated abuse (or "tech abuse") such as stalking, surveillance, and image-based abuse (or "revenge porn") from the threat models that shape where researchers investigate challenges to security (Slupska 2019).

The project is based on the following research questions/objectives:
RQ1: How can cybersecurity practices better serve the targets of tech abuse?
RQ2: How can feminist theory and praxis improve cybersecurity research and practice?

On the basis of these two research questions, I plan to develop a feminist approach to cybersecurity which draws on feminist critiques of security studies (Enloe 1989; Cohn 1987; Tickner 2004), feminist technoscience (Wajcman 2007) and the emerging 'design justice' model for technology design (Constanza-Chock 2018). I will start by conducting a set of empirical studies, which will form the basis of a normative political theory for cybersecurity. These empirical studies may include:

- co-designing an "abusability" test for smart devices or image sharing platforms with survivors, tech abuse experts, and conventional cybersecurity experts
- follow-up interviews with co-design workshop participants to explore contrasting understandings of security and strategies for approaching tech abuse
- interviews with product managers exploring how abusability could become incorporated into industry practice
- participatory action research in the form of feminist digital security trainings

This project will use innovative co-design methodologies which have only rarely been applied to cybersecurity. Following feminist approaches to knowledge creation and the emerging 'design justice' model for technology design (Constanza-Chock 2018), people's individual experiences and individual positionality may help to expand how cybersecurity researchers do the work of threat modelling and usable security design. Rather than dictating what threats citizens should be worrying about, this project will develop a model for eliciting and listening to citizens' concerns to expand the scope of threat modelling in cybersecurity. This process will also create pathways for citizens to engage in shaping future research directions for cybersecurity: ones that are grounded in the lived experience of those who are traditionally excluded from discussions of cyber- or information security.
Inspired by Marwick and Boyd's (2018) call for projects that discuss more diverse conceptualizations of "the user" or the subject, I will use collaborative, participatory, and creative practices to address cybersecurity challenges in the UKRI-funded "Reconfigure" citizen science research project. Participatory security design avoids the assumption that security of the individual will follow from technical security and ensures that actors who may ordinarily be marginalized have their perspectives taken into account (Heath et al. 2018). It incorporates 'situated' knowledge and practices (Haraway 1988) so that information security can be studied in a grounded way.

Publications:

J. Slupska and L. Tanczer. (forthcoming) "Intimate Partner Violence (IPV) Threat Modeling: Tech Abuse as Cybersecurity Challenge in the Internet of Things (IoT)." In Technology-Facilitated Violence and Abuse – International Perspectives and Experiences. Emerald Publishing.

J. Slupska. "Safe at Home: Towards a Feminist Critique of Cybersecurity", St. Anthony's International Review, Summer Issue (2019), no. 15: Whose Security is Cybersecurity? Authority, Responsibility and Power in Cyberspace. Available at SSRN.

J. Slupska. "War, Health and Ecosystem: Generative Metaphors in Cybersecurity Governance." Philosophy and Technology (2020). https://doi.org/10.1007/s13347-020-00397-5."

J. Slupska, R. Minko, Z. Tan, F. Zahra and M. Eviette. "Cybersecurity and Intimate Partner Violence"

Map the System Research Competition, published in Yearbook of the Centre for Doctoral Training in Cybersecurity (2019).

D. Chalmers and J. Slupska. "The Regional Remaking of Trade and Investment Law." European Journal of International Law, Volume 30, Issue 1, (2019), https://doi.org/10.1093/ejil/chz004.

N. Maroun and J. Slupska. "International LGBT Leaders Take the Stage" Public Diplomacy Magazine (2014).

Public Engagements:

"Safe at Home: Towards a Feminist Critique of Cybersecurity", 2020 International Studies Association, cancelled due to COVID-19 global pandemic

"Reconfigure: Feminist Action Research in Cybersecurity" 2020 Human-Computer Interaction (CHI) Direct Action Workshop, cancelled due to COVID-19 global pandemic

"War, Health, & Ecosystem: Generative Metaphors in International Cybersecurity Policy" (05 November 2019), Hague Conference on Cyber Norms 2019 – Best Paper Award.

"'We're All Happily Married Here!': Intimate Partner Violence as a Cybersecurity Issue" (03 October 2019), Royal Holloway Information Security Group Seminars

"Designing IoT Security for Intimate Threats," (21 May 2019), London IoT Meetup Group

"Towards a Feminist Critique of Smart Home Security Analysis" (9 March 2019), Oxbridge Women in Computer Science Conference

Claudine Tinsman

Supervisors: Max Van Kleek, Department of Computer Science and Rebecca Williams, Faculty of Law

Claudine has a BA in Political Science from UC San Diego. During her time in California, she worked in San Diego city government and at a large immigration law firm. She holds a Master of Law (MLaw) in Legal Issues, Crime and Security of Information Technologies from the University of Lausanne. Her master's thesis examined the potential implications of treating intelligent agents as legally liable actors.

Her DPhil research aims to design effective and customisable subjective harm mitigation implementations that enable users to safeguard and promote their mental wellbeing.

She currently serves as assistant to the papers chairs for the ACM Human Factors in Computing Systems Conference 2021 (CHI2021).

DPhil Thesis: Curating Contact and Conduct in Online Spaces

Many people spend a significant amount of their daily lives communicating with one another online. Children and teenagers are significantly more likely than adults to engage socially online, enabling them to communicate with anyone, anywhere from a very young age. These users may be unaware that they are harming others by their words and actions online, while those exposed to such antisocial behaviour online may feel unable to remove themselves from situations detrimental to their mental wellbeing.

Research in psychology and the social sciences has shown that negative experiences with online contact can have deleterious effects on users' mental health and may in turn encourage certain types of antisocial behaviours.

While all users can and should be concerned about who they engage with online, this project focuses on groups of users who are likely to have specific concerns about exposure to online content and contact, such as parental figures, teenagers, and children. This project has the potential to both help users who exhibit antisocial conduct to engage in more prosocial behaviour, and to prevent others from being subjected to harmful behaviours.

At its core, this research seeks to develop tools that afford users greater control over the contact they experience in online spaces. It combines research from psychology, learning sciences, linguistics, and computer science in order to explore automated solutions that can identify specific threats within the context of online interactions in real time. Specifically, pattern analysis of word use in conversations will be used to assess whether a user's online conversation displays antisocial characteristics. These methods will be combined with machine learning to create tools that can be deployed as conversations unfold.

The ultimate purpose of this research is to provide two complimentary measures to make online communication safer: On the one hand, it will produce tools that provide real-time educational interventions to individuals whose conversations display traits of specific types of conduct, such as cyberbullying. On the other, it will provide users seeking to protect themselves and those under their care (e.g. parents and children) with a notification system when conversations escalate to levels that the users deem undesirable.

Talks:

Presented DPhil research to approximately 40 Commonwealth MPs attending a conference on cyber security at the Oxford Martin School.

"Social Engineering Attacks", Cyber Security Awareness Week, HSBC (20/05/2019).

Appeared on the Big Questions Podcast (Oxford Sparks): Appeared as a guest on the show to explain cyber security concepts to a non-specialist public audience (27/03/2019).

Publications:

Mini-Project: Defining Personal Data under the GDPR: Challenges for Organisational Cyber Threat Intelligence Sharing

Mini-Project: A Universal Security Rating System for Mobile Apps: Preventing Today's Fraud From Becoming Tomorrow's Nightmare

Fatima Zahrah

Supervisor: Michael Goldsmith and Jason Nurse, Department of Computer Science

Fatima received a BSc (Hons) degree in Computer Science from the University of Bradford. Fatima's research interests focus around online hate and investigates how online platforms are strategically used by cyber criminals and hate groups. Her work combines insights drawn from social sciences and uses methods from computer science, including natural language processing, machine learning and social media analysis.

DPhil Thesis: Investigating the Cross-platform Behaviours of Online Hate Groups

Online hate thrives globally through self-organized, scalable clusters that interconnect to form robust networks spread across multiple social media platforms, countries and languages. Despite efforts from law enforcement agencies and platform developers to

remove or limit such content, online hate ideologies and extremist narratives are still being linked to several crimes around the world. The networks formed by hate groups have proven to be remarkably resilient and have increasingly shown to migrate across various platforms and networks, maintaining and oftentimes expanding their connections in the process. Previous research in online hate has generally focussed around one particular platform, even though there is sufficient evidence showing that hate groups often strategize the usage of different online platforms in order to circumvent current monitoring efforts. This research will aim to bridge this gap by investigating how online hate groups make use of multiple platforms to propagate criminal and extremist content. More specifically, it will involve a cross-platform-analysis of the behaviours of such hate groups in order to better understand and detect networks of organised hate. This project will be conducted with particular consideration of the following research questions:

RQ1: How can the current online hate research landscape be advanced by considering through exploring several online platforms?

RQ2: How do hate groups adapt their behaviour on different platforms?

RQ3: How is information transferred and shared by hate groups across platforms?

RQ4:How can we model online hate detection and analysis across various platforms?
Through this, the research aims to determine how multiple online platforms are strategically used by hate organisations, and produce more efficient hate detection and analysis methods. The findings from this will then be used to aid the development of a web interface as a tool for law enforcement agencies to detect, analyse and help remove criminal hate.

Publications:

Forthcoming:

Zahrah, F., Nurse, J.R.C. and Goldsmith, M., September 2020. #ISIS vs #ActionCountersTerrorism: A Computational Analysis of Extremist and Counter-extremist Twitter Narratives. To be presented at the 2nd Workshop on Attackers and Cyber-Crime Operations, co-located with IEEE EuroS&P 2020.

Presentations:

Slupska, Julia, Romy Minko, Zhi Tan, Fatima Zahra and Marine Eviette. "Cybersecurity and Intimate Partner Violence" (2019) Map the System Research Competition. Also presented at Connected Life Conference 2019.

Community Response to COVID-19

The impact of the sudden lockdown across the UK on the 23rd March was felt by the CDT community in a variety of ways; on research, with the loss of time or focus, access to academic resources or disruption to long held fieldwork plans. Impacts too have been felt on a personal level with concerns and caring responsibilities for family and friends; some being called for national service and others stranded many miles from home relying on the kindness of strangers.

Over the lockdown, the community has experienced both positive and negative changes to everyday life. Some have discovered new hobbies, others taking on volunteer work, creating COVID related apps or simply running errands for more vulnerable members of the community. For some, this has been a very difficult time and for all, it has been a moment for reflection.

We have captured a few comments from our students during this period and share with their permission below:

"I have recently started volunteering for an OxfordHub project, providing online tutoring to primary school children needing support during this lockdown period."

"I have skyped more often with friends at home or abroad (we did not previously have the time)"

"Lockdown has affected me in both positive and negative ways. While parts of my research can be conducted from home without access to specific people or resources, which I realise is not the case for everyone, other parts have slowed down as people are less responsive to emails or less available to participate in interviews, for instance. The lockdown has also allowed me to re-focus on my research as many distractions were suddenly taken away and to make consistent progress in these unexpected circumstances."

"I have been looking after family during the lockdown"

"The lockdown has made me realise that I do not actually go or meet with friends much, so my routine has not changed during the pandemic. I would like to change that when the lockdown is over and focus on enjoying the outside world more."

"I've taken a photography course, a shark conservation course, and learned how to play bridge. I was even featured on a video by the Lawn Tennis Association (LTA) for my tennis at home tricks! I'll make sure to get in touch with my long lost friends more often than only when a pandemic happens. My lessons learnt: always have travel & medical insurance, and asking for help is not a sign of weakness."

"The lockdown has only partially affected me: instead of working at the library I work from home! Instead of going swimming, I discovered cycling, which can be quite fun."

"I was surrounded by nothing but kindness when I was completely dependent on others - strangers, even. It reminds me of how much good there is in the world."

During this socially distanced time, the Peer Support Network was launched, staffed by trained volunteers each accredited by Mental Health England as Mental Health First Aiders, making themselves available to answer questions and support colleagues during the difficult months of 2020.

For those funded by the UKRI's Engineering and Physical Sciences Research Council, additional funding extensions for up to six months have been provided for students at any stage of their DPhil, who have been impacted by COVID-19 in a direct or indirect way.

101 days, 6 flights, and an 18 hour bus ride home

Hayyu Imanda, CDT18

Every person has had a unique experience brought by the pandemic, with the surfacing of challenges surfacing none of us could have imagined at the start of the year. This is my personal story.

In mid-March, I left Heathrow Airport with some of my teammates from the Oxford University Lawn Tennis Club. This year's Blues tour was planned for 10 days in Cape Town, which included friendly matches with universities and local clubs, and of course, some sightseeing. Our excitement dropped when we arrived in our transit airport, as we read that the South African president has just declared a national state of disaster, and a travel ban for nationals from high risk countries (including the UK) to be introduced in 2 days' time, with visas from those countries cancelled with immediate effect.

Within the very short transit period, with minutes to spare on final boarding call, we decided that we turn around and neglect the tour altogether. However, at the time, given how recent the president's address was, there were no official documents about the new regulations, and the airline did not allow us to reschedule our tickets. We were each forced to buy a new ticket, which, for students, was quite a considerable amount. After consulting with an airline staff, the following idea was introduced: given my unique visa status compared to the rest of my British teammates, if they make the regulations official during the 8-hour flight duration which would result in my refusal of entry at the border, I would be sent back by the airline at no additional cost. With a split-second decision, I hugged my friends goodbye – the last I would give anyone for months - and I boarded the plane to Cape Town, by myself.

On my arrival into Cape Town, the border officer welcomed me into South Africa with the widest, friendliest smile. As I picked up my luggage, I asked myself, "now what?"

I decided to take this opportunity to explore Cape Town, socially distanced. This is a part of the world that is entirely new to me; I witnessed the appalling remnants of apartheid, an easy thing for many travellers to pretend to not see. I drove to the south-westernmost point of the continent, hiked a couple of mountains, and smiled at the African wildlife including giraffes, penguins (yes, penguins! In Africa!), whales - there was also a cameo of multiple seals in one Cyber Café. Among what might sound like an incredible time spent in Cape Town, none of those could still not cloud my anxieties. The fact was the following: I was by myself, in a foreign country with no-one I know, in the middle of a pandemic.

When I received the email about the cancellation of my return flight, I immediately booked another ticket, with another airline, to my home country. On the date of the flight, my Airbnb host described the airport she just visited as "chaos"; I ensured her that I've checked in online the day before, and the flight is still confirmed. I naively smiled, returned the rental car, and walked my suitcase with confidence into the departure lounge. I still had a calm smile as I read on the departure board that my flight was delayed by 6 hours. "I'm sure they'll just connect me on the next flight from the transit airport, it's the airline's responsibility to bring me home," I said to my mum.

After phoning the airline call centre – with hours of waiting time – I was not allowed to board as the airline

was grounding all of their planes in two days, and the connecting flight I would have missed was the last one to Indonesia, while the connections to London were full. I stayed at the airport to try and find any other flight that would leave that day, to either of my two homes. A couple of hours after, all possibilities of flying out of the country on the day evaporated – my tears started, and I was left with no other option. I pride myself on being well-organised and meticulous, however on that day, I was in a position I have never found myself in. At 8:30pm, in desperation, I messaged the Consul for Consular Affairs at the Indonesian Consulate in Cape Town (who I contacted on arrival) via their WhatsApp hotline and she informed me the news that South Africa will enter a national lockdown in 3 days' time. Hotels were not happy about my travel history, and I had nowhere to go. I asked to stay at her couch for the night, so I can try again the next day.

We met in the Indonesian Consulate, where I was picked up and driven to the consulate guest house, where I stayed the night. In the morning, I was picked up to find another plane ticket (the third!) – with the ticketing office in town shut, we went to the airport, with no success: no seats are available for the rest of the week. I booked another flight for the week after, given that there was no indication that the lockdown would not allow flights out of the country. I was then driven to the residence of the Consul General to Indonesia in Cape Town. They had a room for me ready, and the consul general informed me that I can stay there until I am able to leave.

Only when I arrived in the residence that they asked me about administrative items; they knew nothing of me apart from me being a student on a tourist visa. In fact, the only thing they cared about was that I was of Indonesian citizen, and they reiterated that it is their constitutional duty to put me under their protection. In his words: "this residence belongs to the country, and not mine personally. Here, you are a guest of Indonesia, but so am I – you have every right to be here."

I cannot describe the shift in the spectrum of emotions I felt the day that the consulate helped me. I went from being in a state full of anxiety to feeling calm and completely safe, all with appreciation to the consulate.

During my stay, I had access to all the facilities of the residence and shared many delightful, gripping conversations with the consul general and his wife during mealtimes. I became aware of the challenges diplomats had to face in response to the evolving nature of the pandemic, and the difficult, quick decisions they had to make. Seafarers were flown on a Japanese repatriation flight, and with coordination with the Japanese government, they were allowed to disembark in Japan to fly on a commercial airline home. Unfortunately, one seafarer lost his life at sea, and due to the restrictions on international flights, had to be buried in a Muslim cemetery in Cape Town without the physical presence of family members. Other stranded travellers had to stay indefinitely with their family members.

The consul for consular affairs continuously kept me up to date with the changing regulations and in particular, kept asking me how I was doing – a simple, powerful question to ask during a period of uncertainty. I never felt alone, and I had my complete trust with the consulate to assist me.

Though there were repatriation flights organised by the UK High Commission to South Africa, I was not allowed

to book a ticket, as I was not a British citizen or a direct dependant of one.

It was never clear when the South African government would allow commercial airlines again, as the original 3-week lockdown ('Level 5') was extended to 5 weeks, only to be followed by a tiered system where international flights will only be allowed on 'Level 1'. When a repatriation flight was organised by the Indonesian Embassy to South Africa in Pretoria and the Consulate in Cape Town, coordinating with the South African government and South African Airways, I leapt at the only chance of getting out of the country.

I said goodbye to those I shared the past 6 weeks with, feeling conflicted - sad to leave what felt like my family in Cape Town, but very happy to be reunited with mine at home. They thanked me for being a part of their family for a couple of weeks, even though I was the one who was completely dependent on them. I couldn't do anything but thank them, and I'm not sure I'll ever be able to repay their kindness.

On Tuesday, May 5th 2020, 9 Indonesians took an 18-hour road journey from the consulate in Cape Town to the Indonesian Embassy in Pretoria, which included police escort past the lockdown curfew and a unique chance to see South African sceneries outside of Cape Town. When I met other stranded Indonesians in Pretoria, they all had their own unique stories: seafarers at the end of their sails, workers having finished their employment, and travellers waiting for refunds of dozens of millions of Rupiahs (i.e. thousands of pounds) from airline companies as they desperately bought multiple tickets trying to get home. One lady had to say goodbye to her South African husband for an indefinite amount of time, as his residency had expired – he had to wait until South Africa opens its borders, and for Indonesia to allow non-resident foreigners.

After a plethora of paperwork in the embassy, we were escorted by the South Africa national travel police to OR Tambo International Airport in Johannesburg. 27 Indonesians flew the 10-hour flight from Johannesburg to Denpasar, the first ever of such route. On arrival in Bali, we were greeted by the military and the ministry of health as we got screened and antibody tested before flying to Jakarta the next day. The flight flew back to Johannesburg carrying stranded South Africans from Jakarta and Bali, and they all, including the crew who were volunteers, would be quarantined at a government's facility for two weeks.

On landing in Soekarno Hatta, I shed a few tears of relief. It was finally over. I completed my 14-day self-isolation in my family home thankfully with no issues, spending Eid with my family, and flying back to Oxford two months later.

What was supposed to be a 10-day trip in Cape Town turned into 3.5 months away in two different countries with many new experiences, lessons learned, and lifelong friendships. I was completely dependent on others, yet I received nothing but kindness and warmth. I am eternally grateful for Indonesian Ministry of Foreign Affairs for taking care of their citizens abroad, especially with the challenging landscape resulting from the pandemic. With no less importance, what helped was also the virtual support that I've received from many parties: the CDT - in particular, David – for always having the time to pick up the phone whenever I needed advice; my supervisor Kasper Rasmussen, who has been more supportive than I could ever have hoped; The Jardine Foundation, Exeter College, and the Oxford University Sports Federation, for checking on me continuously and providing financial assistance. Though this story might not sound like one, it was an entirely positive experience. There is an incredible amount of kindness in this world.

Pand-Veillance: Covid-19 is a Catalyst for Mass Surveillance, and a Wake-Up Call for Privacy & Transparency

Arthur Laudrain, CDT18

Abstract

What are the effects of Covid19 on mass-surveillance practices? What are the risks to our democratic societies in particular? How can we balance between safeguarding our civil liberties, and protecting the well-being of the Nation in such extraordinary times?

The Covid-19 pandemic is acting as a catalyst for mass-surveillance, leading governments to adopt exceptional surveillance measures. The danger, in both democratic societies and others, is that they are not rolled back once the emergency is over. The opportunity is to better define the balance between individual liberties and the common interest. To achieve such balance, we argue CT systems should adopt a decentralized privacy-preserving model, with user consent and transparency at its core. But privacy by design is not enough; it must be backed up by strong legal safeguards. These measures will ultimately reduce misinformation and the risk of chilling effect on citizens exercising their fundamental rights.

We observe that governments deploy three categories of surveillance technology to address three distinct -and legitimate- public health purposes. Looking into specific surveillance programmes already established, we find CT and QE raise numerous privacy issues. We then address them with an overview of potential technical and legal solutions. We rely on a manual media survey, leverage public policy trackers and the theories and concepts of surveillance studies within an inductive approach.

Argument & Implications

The Covid-19 pandemic is acting as a catalyst for mass-surveillance. Two legitimate public health priorities in particular, contact tracing (CT) and quarantine enforcement (QE), are leading governments all around the world to adopt exceptional surveillance measures, sometimes repurposing tools designed for counterterrorism or dissent control. Exceptional circumstances are political windows of opportunity for deploying new surveillance tools and practices, as we observed in the aftermath of 9/11. The danger, in both democratic societies and others, is that they are not rolled back once the emergency is over. The opportunity is to better define the balance between individual liberties and the common interest.

A catalyst in three steps

The Covid-19 pandemic, as other disrupting events in the past, produces what we can best describe as a catalyst, consisting of three stages: trigger, deployment and persistence. Each step is well-known of political scientists, especially surveillance studies scholars.

The trigger: How exceptional circumstances facilitate exceptional measures

There is nothing new in arguing that exceptional circumstances facilitate the initiation of similarly exceptional laws and regulations. Wars, major terror attacks and other events that stand out by the extent of their violence create a political opening. This is also known as "rallying round the flag" (Hetherington & Nelson, 2003; Murray, 2017). This political window of opportunity -also referred to as surge- can lead to mission creep, as we witnessed in the aftermath of 9/11, with the extension of intelligence agencies' powers and jurisdictions (Deflem & McDonough, 2015, p. 11; Wood et al., 2003, p. 11). The window of opportunity is not exclusive to surveillance and extends to most kinds of political power. In Hungary, Viktor Orbán used the pandemic to suspend Parliament and is to rule exclusively by decree, without time limits (Bottoni, 2020).

Deployment: Repurposing or importing counter-terror and dissent control tools

In the past few weeks, we have been observing a trend of governments repurposing or importing mass-surveillance tools to tackle the many public health challenges Covid-19 brings. In authoritarian regimes mostly -but not only-, surveillance apparatus that were originally developed for countering terrorism or domestic dissent are being reconfigured towards digital process tracing and quarantine enforcement. In some cases, they combine CCTV footage, GPS and phone tracking, as well as bank cards usage. This merging of data is not new, yet it necessitates very strong containment measures against abuse and to avoid potential chilling effects on fundamental rights (Laudrain, 2019). Within the jurisdiction of the European Court of Human Rights for instance, using non-anonymized data mandates the introduction of both technical and legal safeguards, notably in terms of the scope of the collection, the timeframe of retention and limitation of its purpose. But these are no ordinary times, and all human rights regimes hold provisions for temporary emergency measures, within necessity, appropriateness and proportionality (Olbrechts,

2020). While it is still unclear how much governments will choose to tilt the balance towards safeguarding the common good to the detriment of individual freedoms, some have already announced plans to derogate from human rights regimes (Makszimov, 2020).

Persistence: The risk of normalization and long-term curtailing of human rights

In effective democratic regimes with strong human rights standards, exceptional measures are rolled back once the situation that warranted them disappears. This is, however, rarely the case in other regimes. China, for instance, possesses a long experience of "using major events, including the 2008 Beijing Olympics and the 2010 World Expo in Shanghai, to introduce new monitoring tools that outlast their original purpose" (Mozur et al., 2020). The concept was coined in the late 70s as function creep and used extensively to study the spreading of civilian technology towards intelligence and military purposes (Winner, 1978).

Even functioning democracies can suffer from such phenomenon. Terror attacks are regularly "used to normalize oppressive surveillance measures, perhaps making them seem more palatable or even necessary" (French & Monahan, 2020) and install them for good in the society's security landscape. In the context of pandemic surveillance, the risk of persistence also arises out of an increased dependence of healthcare systems and governments more widely on major tech companies, from the Silicon Valley or elsewhere. Once these public-private partnerships and infrastructures are established (or enhanced), they could be translated back into the realms of counter-terrorism and dissent.

Implications from the perspectives of public policy, research and activism

Digital contact tracing must rely on a Decentralized Privacy-Preserving Proximity (DP3T) model. It fulfills its public health purpose without infringing on people's privacy. The decentralized nature of the system would provide reassurance in terms of data repurposing and persistence. That said, devil hides in details, and the strength of privacy safeguards by design will depend on their case-by-case implementations. For instance the UK app, even if it is expected to rely on a privacy-preserving system developed by Apple and Google, might still allow for the de-anonymization of users (Pegg & Lewis,

Privacy by design, while necessary, is insufficient. It must be backed up by a commitment to transparency and by legal safeguards.

2020). That is why privacy by design, while necessary, is insufficient. It must be backed up by a commitment to transparency -by making the source code public- and by legal safeguards. Such safeguards must particularly address the risk of surveillance persistence. They should implement clear exit strategies that include sunset clauses on the data collected and the infrastructure built. This set of measures will ultimately reduce misinformation and the risk of chilling effect on citizens exercising their fundamental rights (Laudrain, 2019).

In the meantime, what should scholars, journalists, activists or policy-makers do? First, we should closely monitor surveillance measures taken by governments. There are already initiatives by NGOs and scholars to that effect, and we should leverage them. Second, we should ensure that emergency measures are fully rolled back once the health situation does not warrant it anymore. We should particularly monitor territories with low human rights standards and weak legal safeguards. Lastly, but most critically, we should pay attention to how technology is being further integrated into existing surveillance schemes, as much in democratic regimes as in others.

On a more positive note, the technology and partnerships that are being developed during this crisis are not only a potential threat. They are opportunities, too. It is the ideal time to think about how we can implement privacy by design further into our digital infrastructures and our digital lives. It is also a good time to collectively think about how much we value privacy as a human right, and whether our laws and institutions are up to these expectations. As with all crises, the window of opportunity goes both ways.

People, permits and COVID-19: trust, data-tracing and privacy in the Kurdistan region

Arianna Schuler Scott (CDT16) and Ranjbar Balisane (CDT13)

Ranjbar Balisane's research has focused on identity management and trusted hardware. Here, he talks to Arianna Schuler Scott about his role as part of the Kurdistan region's response to COVID-19 and the cybersecurity principles that drive his work.

"It was a panic point... [which meant] everyone was panicking and more likely to listen", Ranj describes his elevation from temporary advisor to project lead. By showing decision-makers what technology could make possible, he was hired on the spot to build a tool reconciling individual and national interests.

The region of Kurdistan imposed a hard curfew as COVID-19 reared its ugly head; to go out you needed a permit, and queueing for a permit would put you in close proximity with other people. To design and implement a national data-tracing application would mean collecting personal data, tracking GPS coordinates and establishing fair permit allocations. A system such as this one must be built on sound principles, but in time trade-offs have to be considered.

Ranj has sound advice for navigating the crisis of a global pandemic, where the situation could quickly become political. "Work in your zone – I am a very practical person and there are boundaries and limitations you will hit so figure out what those are. In software engineering there are more features than politics". His development ethos focused on keeping privacy at the forefront of development (storing data for a matter of weeks rather than years), distributing permits to those who needed them, and designing such a system to be easily used.

While political situations may provide and help refine the scope of a project, responsibility for how software is used lies with the technology leads. "Whoever is in charge of the project will set limits – data-storage, for example. If my settings are 30 days, someone on another project might use a different figure". Security is important throughout the development process as there are constant risk trade-offs that have to be made. Good principles have to be non-negotiable.

"This is all about privacy... I wanted user choice and a fair system", says Ranj. "It was really important that we learned lessons from Australia, Singapore, Korea etc., adapting what others had done to the dynamics of my situation". In the past 10 years the world has been ravaged by vicious outbreaks of cholera, swine flu and ebola, among many others. Strategies to prevent such diseases from spreading are needed, and the role of technology is becoming more and more central. The way we develop these technologies however, has to have security at its heart.

Ranj and his team met their deadline – the app was finished. Law enforcement agents were trained in its use and the Kurdistan region prepared for another wave of COVID-19. But, almost as quickly as it clamped down, curfew was lifted and the app was put on pause.

As of early August, the Kurdistan region has counted around 17,500 confirmed cases of COVID-19 far fewer than the UK's 311,000. Data plays a larger role than ever before in shedding light on complex challenges. We must protect it and use it responsibly. Ranj's work is just one example of the CDT's impact on the wider world, and shows the importance of cybersecurity professionals at every level who can combine technical expertise with organisational (and national) priorities: "I kept asking myself, how could I best protect people's privacy in such a situation... there is limited time to play, and there was no way I could ignore the ethical considerations".

Life after the CDT

Kristopher Wilson, CDT14

I submitted my DPhil in mid-2019 after a great four (and a bit!) years in the CDT and Faculty of Law. I spent my final year of the DPhil back in South Australia as I had secured a short-term appointment in the Law School at Flinders University. There I had the opportunity to build new technology focused subjects in the online Juris Doctor programme: topics in criminal law, intellectual property law, and jurisprudence. My experience at Oxford and in the CDT programme allowed me to embed cross-disciplinary concerns and understandings into these core courses to great results.

When my time at Flinders came to an end, I secured my current (and a permanent) position as a lecturer in the Faculty of Law at the University of Technology Sydney (UTS) in New South Wales. As part of my position at UTS I became a founding member of our new Centre for Cybersecurity and Privacy – a cross-disciplinary centre co-located with the School of Computer Science. I am currently working with a small team of legal researchers on Australian specific legal projects: most recently on consumer protection issues with respect to IoT devices. I am also working on a small project identifying the 'gaps' in the Australian criminal law with respect to surveillance device offences vis-à-vis the short-term and holiday rental market, and another considering the legal implications arising from the development of schemes to purchase and trade shares in real estate on blockchain-based platforms. Beyond this, I am also building and contributing to a number of projects that consider the development of data protection principles with respect to Aboriginal Australian traditional knowledges, and the development of legal technology support for cultural heritage protection.

Teaching at UTS has been a personal highlight: I've supervised a number of technology-focused honours theses, most recently including one on the use of lethal autonomous weapons under international humanitarian law, and another exploring the regulation of simulated gambling in video games (a topic of potential regulation emerging around the world, including this year in the UK through recommendations from the House of Lords). I am currently also supervising two PhD students – a very strange feeling! This past year I also had the opportunity to co-convene the 2020 Allens Neota UTS Law Tech Challenge for Social Justice where we link groups of students with community legal centres and other legal settings to develop and build apps that focus on improving key community access to justice initiatives.

It's been a busy time since leaving Oxford, but the skills I developed at the CDT are being put to good use! I'm looking forward to coming back for a visit soon!


POWER
Cloud
85%
70%
100%
50%
30%
MONEY
Diagram
Loading
STOP
SKILLS
IDEA

Alumni News

Daniel Woods (CDT15) was awarded a Marie Curie Fellowship to investigate an approach to quantifying cyber risk using insurance prices. The project will be conducted primarily from Innsbruck in the Austrian Alps. Willis Towers Watson (a CDT board member) supported the application as a project partner.

Andrew Dwyer (CDT14) has secured a 3-year Addison Wheeler Research Fellowship at Durham University researching 'AI' and 'offensive cyber'. The Fellowship begins in October 2020.

Emma Osborn (CDT13) is partnering with IASME Consortium on a number of research projects developing industry standards. Further industry collaborators are welcome on these projects to reflect the different perspectives across the industry, please contact emma@ocsrc.co.uk for further information.

Katriel Cohn-Gordon (CDT-13) is lead author on "DELF: Safeguarding deletion correctness in Online Social Networks" released by Facebook Engineering, the full paper can be found at: https://engineering.fb.com/security/delf/

Meredydd Williams (CDT14) was awarded with 'Engineer/Consultant of the Year at Roke's 2019 annual awards, in addition to taking on the new role of Senior Consultant in Roke's Information Assurance & Human Science area alongside serving as Innovation Lead and Bid Manager for Roke's Consultancy department. During the past year Meredydd has delivered security guest lectures at Southampton University and University of Kent.

David Mellor (CDT13) In addition to his full time role as Senior Lecturer in Social Policy (International Affairs) at the University of South Wales, is currently writing a book titled 'Robots and Everyday Life' due to be published next year with Routledge. This is a sociological and philosophical investigation about the forecast integration of intelligent machines into society. It deals with issues of ethics and morality, agency and power, and sets out urgent questions about future social and ecological conditions that might be afforded by an 'automatic society'.

The Alumni network is continuing to expand – please see **www.cybersecurity.ox.ac.uk/alumni** for further details

The CDT Team

Andrew Martin – CDT Director

Professor of Systems Security, Department of Computer Science

An Oxford graduate, Andrew worked as a Software Engineer at Praxis in Bath, where he first encountered some of the challenges of information security and secure systems engineering in the late 1980s. After a DPhil back in Oxford, he escaped to the other side of the world to be a Research Fellow at the Software Verification Research Centre in the University of Queensland. Eventually the excellent weather and relaxed way of life got the better of him, and so he returned to the UK, and entered his current post in 1999.

The core of his research interest here has been in the security in distributed systems. Mostly of late that's been explored through looking at applications of hardware-based security controls – often described as Trusted Computing technologies - particularly as applied to cloud, mobile, and embedded applications (now known as the Internet of Things). His research group has been looking for the architectural elements and design patterns necessary to make trusted clouds and secure IoT a reality. These ideas have the potential to transform how we think about distributed systems and the security of the information they process.

Michael Goldsmith – CDT Co-Director

Senior Research Fellow, Associate Professor, Department of Computer Science

Michael Goldsmith is a Senior Research Fellow at the Department of Computer Science and Worcester College, Oxford. With a background in Formal Methods and Concurrency Theory, Goldsmith was one of the pioneers of automated cryptoprotocol analysis. His research work has investigated a range of Technology Strategy Board and industrial or government-funded projects ranging from highly mathematical semantic models to multidisciplinary research at the social-technical interface. He is an Associate Director of the Cyber Security Centre, Co-Director of the newly launched Centre for Doctoral Training in Cybersecurity and is active in the IAAC Academic Liaison Panel.

Lucas Kello – CDT Co-Director

Associate Professor of International Relations, Director of the Centre for Technology and Global Affairs, Department of Politics and International Relations

Lucas serves as Director of the Centre for Technology and Global Affairs, a major research initiative exploring the impact of modern technology on international relations, government, and society. His recent publications include The Virtual Weapon and International Order (Yale University Press), "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft" in International Security, and "Security" in The Oxford Companion to International Relations (Oxford University Press).

Joss Wright – CDT Co-Director

Senior Research Fellow, Oxford Internet Institute

Joss Wright is Senior Research Fellow at the Oxford Internet Institute, where his research focuses on the analysis of information controls and their global development, and on the design and applications of privacy enhancing technologies.

Joss' work focuses on interdisciplinary approaches to the measurement and analysis of technologies that exert, subvert, or resist control over information. He has a particular interest in bridging the gaps between technically-focused analyses of security and privacy technologies, and their broader social and political implications.

In addition to his work on internet censorship, Joss also co-directs the Oxford Martin School's Programme on the Illegal Wildlife Trade, in which he researches the trade in illegal and unsustainable wildlife products online.

Katherine Fletcher – CDT Industry Liaison Officer

Katherine is the Coordinator of Cyber Security Oxford, the University-wide network of cyber security researchers and practitioners. Her role in the CDT is to help connect students to the wider community of Oxford researchers, and to support matchmaking for research projects with industry or other external partners. Katherine has over 10 years' experience as a Project / Programme manager largely based in Oxford, specialising in large-scale, multidisciplinary research projects spanning academia and industry. Recent experience includes managing research projects in biomedical/computer science (linking pharma industry and academia), open-source software development projects (academic data management) and cyber security (multiple business sectors and academia).

Katherine received a BA in International Relations from William Jewell College (Liberty, Missouri, USA; 2001), and an MA in Global Political Economy from the University of Sussex (2004).

David Hobbs – CDT Centre Administrator

David joined the CDT in September 2013, just before the first cohort of students arrived. He is responsible for the day to day administration of the programme and acts as a first point of contact on course students and our alumni network. David has over 12 years of experience within Higher Education in several UK universities. Prior to moving to Oxford, David studied and worked at the University of York for a number of years.

Centre for Doctoral Training in Cyber Security
Dept of Computer Science
Wolfson Building
Parks Road
Oxford
OX1 3QD

cdt@cybersecurity.ox.ac.uk
01865 610644

UNIVERSITY OF OXFORD

CENTRE *for* DOCTORAL TRAINING *in* CYBER SECURITY

UKRI Engineering and Physical Sciences Research Council