CYBER SECURITY OXFORD

Early-careers Researchers Symposium

September 30, 2015
Tony Hoare Room – Robert Hooke Building, University of Oxford

Programme

9:30 - 10:00	Registration
10:00	Welcome
10:05 - 10:45	Session 1: Security and the Social *Chair: Laurin Weissinger* Collaboration of Threat Intelligence Analysts – Jan Ahrend Cybersecurity and Philosophy: New problems and concepts – David Mellor
10:45 - 11:30	Discussion: Cybersecurity: Hype or Real Threat? *Chair: Graham Fairclough* Panel: Jassim Happa and Emma Osborn
11:30 -11:45	Coffee break
11:45 - 12:30	Session 2: Hardware and Software *Chair: Bushra AlAhmadi* AppScanner: Automatic Fingerprinting and Identification of Smartphone Apps from Encrypted Network Traffic – Vincent Taylor Security and Software Verification – TBC Looks Like Eve: Exposing Insider Threats Using Eye Movement Biometrics – Simon Eberz
12:30 - 13:30	Lunch
13:30 - 14:15	Session 3: Law, Politics and Policy *Chair: Jamie Collier* Cyber-security as Risk Management: A Political Perspective – James Shires The Evolution of Computer Misuse Legislation – Kristopher Wilson
14:15 - 14:45	Coffee break
14:45 - 15:45	Session 4: Comfort Zones and Jurisdictions *Chair: Ioannis Agrafiotis* Direct-to-consumer genetic testing T&CS – Andelka Phillips Diffusing (Cyber) Security Atmospheres: Implantable Medical Devices – Andrew Dwyer Ungoverned spaces: learning from the age of privateering – Florian Egloff
15:45 - 16:15	Wrap up and prizes

Contact: katherine.fletcher@cs.ox.ac.uk

UNIVERSITY OF OXFORD

ocado TECHNOLOGY

Abstracts

Collaboration of Threat Intelligence Analysts

Jan-Marten Ahrend
Computer Science Department,
University of Oxford
ahrend@cs.ox.ac.uk

Keywords: *Cyber Threat Intelligence, Collaboration, Ethnography, Computer Supported Cooperative Work (CSCW)*

The ability to be alerted in advance about cyber threats and to contain any damage has taken on great interest in academia and industry and is evolving into an important field. While CSCW research has witnessed a shift from understanding individual to collaborative work in the last few decades, empirical materials on practitioners' actual collaboration practices and the coordination of their activities to 'do cyber threat intelligence' through technology is still relatively lacking.

Given these limitations, the research question addressed by this study can be framed as: *How do cyber threat intelligence analysts collaborate and coordinate their activities to produce threat intelligence?* A series of semi-structured interviews (N=5) and user diary studies were conducted at three cyber threat intelligence service providers. In this session, we present some of the formal and informal ways through which analysts collaborate and coordinate their work to produce threat intelligence reports for their clients. In addition to the empirical investigations of these practices, we consider the implications for design for supportive technologies. Some of the gained insights have been operationalised in a prototype and will be evaluated in the future to iterate on the gained understandings and the developed requirements.

Cybersecurity and philosophy: New problems and concepts

David Mellor
CDT Cyber Security / Department of Computer Science
University of Oxford
david.mellor@cs.ox.ac.uk

***Keywords**: cybersecurity; continental philosophy; social and critical theory*

My work seeks to turn cybersecurity into specifically philosophical problems, by asking: What is cyber? What is security? What is cybersecurity?

I then look to address these problematics through constructing a set of related-yet-distinct concepts, with the aim of confronting the extensive realities of cyber - far beyond system-defence - within the very political and ethical nature of being.

Here, I will provide a brief overview of my project and show how I go about using various materials to build these concepts, which I have called: *network aesthetics*, *science fictions*, *utopias*, and *cyberfutures*.

This work is clearly situated within the tradition of continental or European philosophy, and I will briefly explain what this means as a technique of thought and as a distinctive methodological approach.

By way of example, I will talk about the metaphor and materiality of networks - the core, conjoined aspects of cyber - using Thomas Pynchon's *The Crying of Lot 49* and China Miéville's *The City & The City* to discuss the fears and emergences of the network imaginary.

I will then look at the work of artist Simon Stålenhag, specifically *Vagrant - The Crow*, in order to illustrate the necessity of interrogating our potential cyberfutures, showing how we are haunted by futures that never arrived and terrorized by futures we still believe possible.

My argument is that conceptual investigations such as this are a vital aspect of framing and confronting the broadest realities of cyber and its securities.

AppScanner: Automatic Fingerprinting and Identification of Smartphone Apps from Encrypted Network Traffic

Vincent F. Taylor
Department of Computer Science,
University of Oxford
vincent.taylor@cs.ox.ac.uk

Keywords: *android; smartphone apps; device fingerprinting; privacy leakage; machine learning*

Smartphone usage continues to grow at an explosive pace as devices become more powerful, versatile, and affordable. Gartner reports that smartphone sales exceeded one billion devices in 2014, an increase of 28.4% over 2013. Of the mobile handsets sold in 2014, more than two-thirds were smartphones [1]. This vast smartphone usage has attracted the attention of adversaries, network administrators, investigators, and marketing agencies, who could benefit from insight into the apps running on a smartphone or network. Indeed, the list of apps installed on a smartphone can be used to: identify vulnerable apps that may be exploited; determine the use of sensitive apps on a victim's device; assist with network planning and traffic management; and aid consumer market research. To this end, we have developed a methodology for smartphone app fingerprinting, implemented in a system called AppScanner, which fingerprints and identifies smartphone apps from their network traffic only. AppScanner only relies on the 'shape' or other characteristic features of the network traffic and does not leverage packet payload information. For this reason, AppScanner will even identify apps that only send encrypted network traffic.

Fingerprints for apps are automatically built by running them on a physical device or in an emulator and using tools to simulate user input. In this way, various UI screens in an app are explored in a highly-scalable way, while at the same time collecting all the resulting network traffic coming from the apps. Various pre-processing strategies are applied to these network traces to remove noise from the data and other imperfections that come about from other artefacts of wireless networks. Feature generation is done on the remaining 'cleaned-up' traffic to obtain the feature vectors that are used directly to train our machine learning algorithms. Various trade-offs in feature generation strategy are explored for each of the machine learning approaches that are implemented.

We built and deployed AppScanner and carried out a comprehensive set of experiments to assess its performance. We built and tested it using 110 of the most popular apps in the Google Play Store. The machine learning models were built in as little as two seconds or as much as two hours or more depending on the particular classification strategy that was employed. Additionally, the resulting models were as small as one megabyte or as large as 350 megabytes. Without post-processing on the output of AppScanner, our best classification strategy achieved 89.5%, 85.9%, and 86.9% for precision, recall, and overall accuracy. Using a novel post-processing strategy which helped AppScanner to be more conservative in its predictions, we achieved in excess of 99% for precision, recall, and accuracy, while being able to classify more than three-quarters of the unlabelled input.

[1] Gartner. (2015, March) Gartner says smartphone sales surpassed one billion units in 2014. [Online]. Available: http://www.gartner.com/newsroom/id/2996817

Looks Like Eve: Exposing Insider Threats Using Eye Movement Biometrics

Simon Eberz
Department of Computer Science
University of Oxford
Simon.eberz@cs.ox.ac.uk

***Keywords**: biometrics, authentication, insider threats*

Passwords are arguably the mechanism most commonly used to secure access to computer systems. Besides their widespread use they suffer from a number of problems, including bad memorability and weak passwords being chosen by many users. In order to mitigate this issue we propose a novel biometric based on distinctive eye movement patterns. A system based on this biometric could serve as a second line of defense after a password is broken, and also quickly detect an intruder taking control of an unlocked workstation. Leveraging insights from related medical and neuroscientific work we design a set of 20 distinctive biometric features. These features are based on characteristics of different eye movements, including fixations, saccades and microsaccades. In order to validate their effectiveness we perform a study consisting of 30 volunteers recruited from the general public while using tasks that reflect the unique requirements of our insider threat model. In order to determine the time stability of our features we repeat the experiment twice within two weeks. The results indicate that we can reliably authenticate users over the entire period. While our data is collected using a sophisticated eye tracking device we show that our approach is feasible even with cheap hardware available to consumers today. We discuss the advantages and limitations of our approach in detail and give practical insights on the use of this biometric in a real-world environment.

The politics of knowledge: how cyber-security risks are constructed

James Shires
Department of Politics and International Relations
University of Oxford
james.shires@chch.ox.ac.uk

***Keywords**: international relations, constructivism, risk*

Constructivism in social science holds that many aspects of the world are not simply brute fact. It is commonly understood that categories like gender, class, and race are not pre-given, but are the result of contingent interactions between humans, involving both language and behaviour: in other words, these categories are 'socially constructed' [1]. International Relations constructivism applies this insight to entities such as the international financial system, the global order of states, and national identities, among others. The purpose of 'problematising' facts we ordinarily take for granted is to talk about relations of power behind the production of those facts: who benefits from the structure of these entities, and who is disadvantaged, sidelined, or denied recognition.

This presentation uses constructivism to analyse a body of knowledge I term 'negative forecasts', which includes both threats and risks. Negative forecasts have a specific *grammar*, including three elements: a subject (the entity for which negative consequences are predicted), an object (the ultimate source of the threat), and a vector (the means by which the negative event occurs). Any subdivision of negative forecasts is based, implicitly or explicitly, on these elements. For example, to examine 'cyber-security risks' is to select some negative forecasts explicitly based on their vector.

The three elements of negative forecasts not only enable the categorisation of threats and risks, but also point to how their construction might be analysed. The construction of subjects and objects (e.g. the subject 'US national security') is a massive affair, relying on a wide variety of sources including historical events, popular media, and political and legal actions. In contrast, the construction of the vector is performed by a relatively small group of experts (in this case, cyber-security professionals). Importantly, expertise cannot simply (and circularly) be defined in terms of knowledge of the facts: rather, it is a set of social cues, habits and practices that binds together cyber-security professionals, and separates them from non-experts. These practices include ways of reasoning and thinking that connect the occurrence of specific events, described in a certain way, to specific negative forecasts. I call this the cyber-security 'logic of risk'.

The key moment in constructing cyber-security risks is the transition from the expert logic of risk to the that of non-experts, including policymakers. Previous work on experts in International relations, often in the form of 'epistemic communities' [2], suggests that expert knowledge can be simply transferred, along with normative commitments, to policymakers. This presentation argues that the non-expert understanding of risk is instead a result of a struggle between different expert groups to obtain power *through* the assertion of their version of the risk, enabling others (such as policymakers or financial backers) to play a more active role in the process. One must therefore understand the practices (including social and technical norms, areas of competition and professional disagreements) of cyber-security professionals in order to understand how cyber-security risks are constructed.

[1] For a review and critique of the term, see I. Hacking, “The Social Construction of What?”, 2000, Harvard University Press
[2] The original article on epistemic communities, which began an extensive debate, is P.M. Haas, “Epistemic Communities and International Policy Coordination”, in International Organization, 46(1) 1992, pp.1-35

The Evolution of Computer Misuse Legislation: Evaluating Utility and Understanding Prosecutorial Trends

Kristopher Wilson
CDT Cyber Security / Faculty of Law
University of Oxford
kristopher.wilson@cybersecurity.ox.ac.uk

***Keywords**: Criminal Law; Computer Misuse Act; unauthorised access and use; prosecution trends*

The increased development and use of digital technology is creating a number of complex challenges across many aspects of law. While underlying common law principles in some circumstances have, over time, translated relatively well to the use of digital technology through analogy, for example the tort of defamation [1], other areas have received explicit legislative attention in direct response to perceived challenges. In criminal law, this is particularly the case with the design and implementation of the UK's first piece of computer specific legislation, the *Computer Misuse Act 1990* (the 'CMA'). But the development of technology and its resulting use is not static and any legislative intervention must be constantly re-evaluated and assessed against the underlying changes in function, capacity and use of the technology sought to be targeted.

Effective evaluation of the adaptability of computer specific criminal legislation cannot be undertaken without first understanding the socio-political and legal landscape that impacted the conceptualisation of the legal framework that legislation sets out. Essential to this is the consideration of factors that influenced the decision of lawmakers to legislatively intervene in the operation of existing criminal law offences [2]. Further, while the provisions within the CMA appear *prima facie* flexible enough to cover the broad scope of malicious activity that can be undertaken in the computing context, it is necessary to note that the underlying philosophical and jurisprudential justifications for the CMA's framework remain based on computers and networks as they operated in the late 1980's. While the legislation has been amended since, such amendments have involved neither a critical engagement with, nor a substantive reassessment of, its broader conceptual framework, rather such amendments have been confined within its pre-existing bounds [3].

Further, these conceptions of computer operation have led lawmakers to continue to frame offences around the interdependent definitions of 'unauthorised' and 'access'. The definitions within the CMA have been structured as to be as broad as possible so as to remain 'technology neutral'. The result has been a lack of adequate exploration of interconnection with other pre-existing non-computer specific offences, for which there is considerable overlap [4]. There has also been limited, if any, consideration that the broad nature of the drafting of the offences may inhibit their practical utility, with more targeted and specific offences from other areas of criminal law better encapsulating the conduct of an accused person and that conduct being prosecuted accordingly. Indeed, a substantial proportion of prosecutions under the CMA could have been prosecuted under non-computer specific criminal laws [5]. This raises questions as to the suitability of the 'unauthorised access' model to describing and tackling the problem of computer crime/misuse in its broadest context. Remaining unanswered is the fundament question facing criminal law jurisprudence: what quality is it precisely, if anything, that makes computers, electronic devices, and data different?

[1] See, eg, Matthew Collins, *The Law of Defamation and the Internet* (Oxford University Press, 2nd ed, 2005).

[2] Stefan Fafinski, 'Access Denied: Computer Misuse in an Era of Technological Change' (2006) 70 *Journal of Criminal Law* 424,

[3] See Criminal Justice and Public Order Act 1994, the Criminal Justice (Terrorism and Conspiracy) Act 1998, the Police and Justice Act 2006, and the Serious Crimes Act 2015.

[4] Johnathon Clough, *Principles of Cybercrime*, (Cambridge University Press, Cambridge, 2010).

[5] See, eg, André Bywater, 'Cybercrime & Security Update: Prosecutors confirm 702 hacking cases charged' *Cordery Legal Compliance* (24 November 2014) <http://www.corderycompliance.com/cybercrime-security-update-prosecutors-confirm-702-hacking-cases-charged/> accessed 24 June 2015.

Direct-to-consumer genetic testing T&CS

Andelka M. Phillips
Faculty of Law,
University of Oxford
andelka.phillips@law.ox.ac.uk

***Keywords**: direct-to-consumer genetic testing; clickwrap contracts; genetic information; consumer rights; privacy; security*

This talk will provide a brief introduction to direct-to-consumer genetic testing (DTCGT) and the wrap contracts used by companies offering these services. My doctoral thesis examines the use of online wrap contracts and the protection of consumers' rights in their genetic information in the context of DTCGT. A major component of my doctoral thesis consists of a review of DTCGT companies' Terms of Use, Terms of Service, Privacy Policies, and Disclaimers of Liability. In order to do this, I compiled a list of 230 companies currently operating in this field.

At present, DTCGT occupies a regulatory grey area, as it does not fit neatly into existing legal categories and the use of wrap contracts in this context can be viewed as a form of private legislation. This allows the industry to self-regulate, but this regulation is heavily biased in favour of companies and at present there is an imbalance in the protection of the respective parties' rights. The primary focus of my current research has been on those companies offering health-related testing services, but in the future I hope to explore issues raised by other categories of testing. Approximately 102 companies offer some form of health-related testing, with half of these based in the USA. I have examined the contracts of 71 companies providing DTC for health purposes and this talk will introduce you to some of the terms likely to be included in these contracts and the issues raised by the use of these contracts and the lack of specific legal regulation of the industry.

Diffusing (Cyber) Security Atmospheres: Implantable Medical Devices

Andrew Dwyer
Centre for Doctoral Training in Cyber Security,
University of Oxford
andrew.dwyer@mansfield.ox.ac.uk

Keywords: *Geography, biosensors, medicine, borders, safety, security by default*

This paper looks at the social implications in the design of implantable medical devices (IMDs) and cyber security. This brings together geographical understandings of the world, using the concepts of atmospheres and critical densities as a way to explore the intricate dynamic between cyber security, a biosensor and cancer tumours. This paper provides an overview of IMD security literature and offers an insight into how designers and projects develop medical devices, building on the limited knowledge on biosensors. Cyber security is considered para-site to processes beyond and including the medical environment and allows for a new way to understand the interplay it has with multiple different spaces and technologies. Through the particular physical properties and knowledge of the project I worked with, I propose that security by default is questioned as an appropriate method to decrease cyber security risk and whether a more nuanced approach is required.

Ungoverned spaces: learning from the age of privateering [1]

Florian Egloff
Centre for Doctoral Training in Cyber Security
University of Oxford
florian.egloff@pmb.ox.ac.uk

***Keywords**: international relations, non-state actors, state-sponsorship, intelligence*

The current understanding of state and non-state actors in cybersecurity literature does not adequately capture the relationship between them. While non-state actors are often mentioned in the literature, they are in fact embedded in a thicker fabric of relations between states than has so far been portrayed. Policymakers have occasionally tried to conceptualise these relations by resorting to the analogy to privateering [2]. Whilst some scholars have pointed to the merit of the analogy, no in-depth research has been undertaken to assess how the analogy might be used to inform the modern cybersecurity challenge [3].

The presentation addresses this gap in the literature. It considers the analogy's potential for a reappraisal of the multitude of actors present in cybersecurity. The interaction between state and non-state actors bears resemblances to actors seen in a previous time in history and such resemblances aid to elicit the security dynamics introduced by cyberspace. The use of the concepts of the privateer, mercantile company, and the pirate enables a recasting of relationships to the state that is unavailable in today's public/private and foreign/domestic divides. The breaking up of the state/non-state divide into a more continuous set of relationships allows for a richer understanding of cybersecurity.

The presentation uses the critical potential of the analogical research design to disrupt the current thinking and introduces concepts that can capture some elements of change. In doing so, the research on the interaction between state, semi-state, and nonstate actors will demonstrate that the International Relations discipline brings a unique insight to the analysis of cyber(in)security – one that can illuminate the political roots of some of the challenges that other disciplines, like computer science, have struggled with. The result is a more detailed understanding of the interaction between states and non-state actors in cybersecurity and its implications for International Relations.

[1] This presentation draws on and refines concepts originally introduced in a working paper for the Oxford University Cyber Studies Programme: Florian Egloff, "Cybersecurity and the Age of Privateering: A Historical Analogy," Cyber Studies Working Papers, no. 1 (2015), bit.ly/cyberprivateer.

[2] See e.g. Aaviskoo, Jaak. "Cyber Defense – the Unnoticed Third World War." Ministry of Defence. http://www.kaitseministeerium.ee/en/news/defence-minister-jaak-aaviksoo-cyber-defense-unnoticed-third-world-war.

[3] Existing scholarship on the lessons of privateering for cybersecurity faces some shortcomings: It is underdeveloped, focuses too much on warfare, or centres on privateering as a policy option rather than assessing its potential for the re-examination of the state/non-state distinction. See J. Laprise, "Cyber-Warfare Seen through a Mariner's Spyglass," *Technology and Society Magazine, IEEE* 25, no. 3 (2006); Noa Shachtman and P. W. Singer, "The Wrong War: The Insistence on Applying Cold War Metaphors to Cybersecurity Is Misplaced and Counterproductive," Brookings, http://www.brookings.edu/research/articles/2011/08/15-cybersecurity-singer-shachtman; Thomas Dullien, "Piracy, Privateering ... And the Creation of a New Navy," in *SOURCE Dublin*(Dublin2013); B. Nathaniel Garrett, "Taming the Wild Wild Web: Twenty-First Century Prize Law and Privateers as a Solution to Combating Cyber-Attacks," *University of Cincinnati Law Review* 81, no. 2 (2013); Peter W. Singer and Allan Friedman, *Cybersecurity and Cyberwar : What Everyone Needs to Know*(New York, NY: Oxford University Press, 2014).

Short bio (bit.ly/florianegloff)

Florian Egloff is a Clarendon Scholar and DPhil Candidate in Cyber Security at Oxford’s Centre for Doctoral Training in Cyber Security, supervised by Dr. Lucas Kello. He focuses on the implications of cyber enabled national and transnational non-state actors to international security. He is interested in politics, intelligence, and the role of non-state actors in cyber security.

Florian has a professional background working for the Swiss Federal Department of Foreign Affairs and banking. He completed his undergraduate studies in Law and International Affairs at the University of St. Gallen and holds a Masters of International Relations from the Graduate Institute of International and Development Studies (IHEID, Geneva). He has been a visiting student at SciencesPo Paris and at the Jackson Institute for Global Affairs at Yale University.

Florian provides input into the Oxford Martin School Global Cyber Security Capacity Building Centre's working group on cyber policy and cyber defence and contributes to the Cyber Studies Programme at the Department of Politics and International Relations.