09:00-09:30  **Registration**
09:30-09:40  **Welcome & Opening**
09:40-10:30  **Session 1: Keynote Speech**
            Cyber Space - are we getting too close to the edge? - Prof Basie von Solms
10:30-11:30  **Session 2: User-centred Cyber**
            (a) Big Brother, Big Brother, Let Me In
                Frans Frederik Blauw
            (b) Brainjacking: Risks of Neurological Implants
                Laurie Pycroft
            (c) Engagement 2.0 - Views of Biobank Participants Regarding Dynamic Consent
                Harriet Teare
11:30-11:45  **Coffee break**
11:45-12:15 **Session 3: Lightning Talks**
            (a) Network Security in Oxford University's Networks
                Freddie Barr-Smith
                Laurin B Weissinger
            (c) Investigating the Impact of Gender Differences on Cyber Security Skills
                Paula Fiddi
12:15-12:45  **Session 4: Funding 101**
            How to Prepare a Good Grant Funding Application - Nathan Davies
12:45-13:45  **Lunch**
13:45-14:45 **Session 5: Organisational Security**
            (a) Investigating the Design and Usefulness of Sonification for Network Monitoring
                Louise Axon
            (b) Protecting Cybersecurity Machine Learning
                Wai Sze Leung
            (c) A Secure Mobile Operating System Model
                Jaco Du Toit
14:45-15:15 **Session 6: Lightning Talks**
            (a) On the Qui Vive: Exploring Differences Between States in Cyber Security Readiness
                Max Smeets
            (b) Security through Obstinance
                Arianna Schuler Scott
            (c) A Stage Structured Hybrid Model for Disease Dynamics Modelling
                Soumya Banerjee
15:15-15:30  **Coffee Break**
15:30-16:30 **Session 7: Security Risks & Controls**
            (a) Are we managing the risk of sharing Cyber Situational Awareness? A UK Public Sector Case Study
                Michael Davies and Menisha Patel
            (b) Mapping the Coverage of Security controls in Cyber Insurance Proposal Forms
                Daniel Woods, Ioannis Agrafiotis and Jason Nurse
            (c) Costs and benefits of greater cooperation between the E.U. and U.S. in cybersecurity
                Benjamin Dean
16:30-16:40  **Judges' Deliberation**
16:40-17:00  **Wrap-up & Awards Presentation**

*The Committee:* Katherine Fletcher, Mariam Nouh, Jason R.C. Nurse, Elizabeth Phillips, Meredydd Williams, Kristopher Wilson & Adam Zibak
Big Brother, Big Brother, Let Me In

Frans Frederik Blauw
Academy of Computer Science and Software Engineering, University of Johannesburg
fblauw@uj.ac.za

Keywords: authentication; context-aware; big brother

In a world plagued by passwords, users face a constant onslaught of login screens. Humiliated by having to click on the “Forgot Password” link, users everywhere are crying out for salvation. [1] Where is the biometric authentication that had been promised? [2] How will you know when I am still here? Who will set us free?

Well, there is always Big Brother, or rather, context-aware systems. [3]

This research investigates the combined use of traditional authentication context-awareness systems.

The aim of this research is to attempt to prove that continuous authentication can alleviate the problems and difficulties of active authentication, giving users a peace of mind to continue with their daily burdens. By continually verifying the identity of the user behind a computing device, the trustworthiness of the identity of the user can be improved.

The objective is to develop a model that is to act as a “central point” between all related context-aware systems. It aims to use existing data from different context aware providers, and create a central point for authorisation. As an authorisation point, it can verify the authenticity of a user to any other system requesting it.

The aim is to not only simplify the implementation of active authentication, but to integrate different ways of authentication to create a process of seamless and continuous authentication.

Brainjacking: Risks of Neurological Implants

Laurie Pycroft
University of Oxford
laurie.pycroft@nds.ox.ac.uk

Keywords: permissions; medical; neurological; cyber; security

The internet of things provides ever-increasing security challenges, with few areas being more concerning and complex than medical device security. Previous work has demonstrated flaws in external drug pumps, home monitoring systems, and even implantable cardiac devices and insulin pumps.

In this talk I outline novel risks associated with neurological implants. Taking a biomedical approach, I identify potential attacks that a cyber criminal could undertake with unauthorised access to a patient’s implant, focusing on deep brain stimulation systems, which are among the most common variety of neurological implant in use today. These include simple attacks such as denial of treatment via premature battery draining or accessing confidential patient information, up to manipulation of stimulation parameters to induce extremely damaging effects, some of which result in challenging ethical and legal implications.

Although these risks are all currently very speculative, I discuss the importance of device manufacturers investing in cyber-security mechanisms, and the challenges facing them in implementing robust security protections.
Engagement 2.0 - Views of Biobank Participants Regarding Dynamic Consent

Harriet Teare
HeLEX Centre, Department of Population Health, University of Oxford
harriet.teare@dph.ox.ac.uk

Keywords: Dynamic Consent, web 2.0, biobank, engagement, qualitative study

Web 2.0 technologies have enabled new methods of engagement, moving from static mono-directional sources of information to interactive user-led experiences. Use of web 2.0 technologies for engagement is gaining momentum within the health sector however this is still in its infancy in biobanking research. We conducted a series of focus groups with biobank participants to gauge their views on a web 2.0 Dynamic Consent interface. The findings from this study suggest that participants would welcome more interactive engagement with biobanks, and the opportunity to hear more about how their data and samples are being used in research.

We propose that by adopting web 2.0 tools for Dynamic Consent, we can move towards an ‘Engagement 2.0’ model whereby research participants have the opportunity for more interactive engagement with medical research, setting up a two-way communication channel between participants and researchers, for the benefit of both.

Network Security in Oxford University's Networks

Freddie Barr-Smith  
Department of Computer Science, Computing Services, University of Oxford  
freddie.barr-smith@it.ox.ac.uk

Keywords: cybersecurity; networks; systems

There is an organisational and strategic implementation of information security and governance policy that must be followed throughout the university, though especially by the computing services. Organisationally the teams most concerned with the security of Oxford’s networks are OxCert, (Oxford’s Cybersecurity Response Team), NetDev (Network Development), NetOps (Network Operations) and SysDev (Systems Development). The most common security tasks used are mail queue clears for users that have been compromised (this is noticed through triggers after log analysis) and VPN traces for users sharing copyrighted material, identified by external copyright holders [1]. OxCert also conduct log analysis in order to detect malicious network activity and spamming in progress. There is protection in the network architecture design involving implementation of firewalls and access control, aided by regular patching.

In addition to this email is encrypted using transport layer security [2] and SPF records, this was not implemented for security however but to ensure that external mail carriers will accept our SMTP traffic [3]. There is authentication and logging of users connected to each network by MAC and IP addresses in addition to user IP. This is also required for university computer operators to provide an audit trail. This is also in combination with the provision of physical security by restricted access to data centres and other buildings.

Good cyber-security regulation is applicable in practice: when policies are not lived by practitioners but only superficially followed, security goals are weakened. This paper argues that currently, there is a tension between regulation and practice overall, even though some subfields are more affected than others. This paper is based on expert interviews with IT-Security experts in different positions, from system architects in big corporations to self-employed security consultants. Even though there is some variation, it is puzzling to see that across the board, practitioners seem detached from cyber-regulation.

While regulation should provide a constructive baseline, experts emphasise that implementing regulation in daily security work remains tricky and work-intensive, yet without much practical impact. Experts criticise, amongst other things, the abstractness of many directives, their often superficial requirements, and their focus on compliance rather than a working overall security concept and structure: practitioners need clear guidelines, regulative flexibility, and realistic rules. National and international regulation and standards must support them in building secure systems according to the organisation and situation in question rather than prescribing procedures without empirical consideration. Such more practically-focussed Cyber Strategies would increase considerably the readiness of organisations worldwide. Thus, regulators should take a different approach to encourage security.
Investigating the Impact of Gender Differences on Cyber Security Skills

Paula Fiddi
Department of Computer Science, University of Oxford
paula.fiddi@cs.ox.ac.uk

Keywords: Security; Human factors; Cyber security skills; Security professional; Gender and diversity

The growing concern of gender related differences and diversity in the Computing/ICT sector workforce cuts across industry and academia. This is due to societal boundaries, cultural perspectives and psychological barriers caused by the perception of the engineering, science and technology fields seen as a "male domain". Women in security are bound by this dominant cultural perception of the masculinity of the security industry [1]. Security (information, systems or cyber) is an area of that requires both technical and socio-technical studies because it is human-oriented. Secure systems are designed and built by humans, to serve human users and carry out human-oriented processes [3]. Furthermore, cyber crimes and security breaches know no boundaries and become issues to everyone at the slightest point of vulnerability. Hence, the demand for a diverse pool of security professionals to protect companies and individuals from these perceived threats [2].

This preliminary empirical study aims to explore the differences in approach, attitude, and practices between male and female computer security practitioners. Are there any differences in the cyber security skills of male and female security practitioners? If there are, what are they and how do they impact the cyber security profession or workforce? The study hopes to identify differences in cyber security skills as well as difficulties faced by male and female security professionals in their day-to-day activities within their working environments.

Findings of this study seek to provide the ICT community with an understanding of this impact and identify the potential benefit of a more diverse workforce. As diversity in the cyber security workforce will provide a variety of perspectives to security incidents and possible threats as well as offer organisations with different views on risk management, security products and services.

Investigating the Design and Usefulness of Sonification for Network Monitoring

Louise Axon
Department of Computer Science, University of Oxford
louise.axon@cs.ox.ac.uk

Keywords: Network Monitoring; Sonification; Anomaly Detection; Network Security

We present a research agenda and methodology for investigating the design and usefulness of sonification – the representation through sound – of network data for network security monitoring. In Security Operations Centres (SOCs), computer networks are generally monitored by security analysts using a combination of anomaly-detection techniques, Intrusion Detection Systems (IDS) and data presented in visual and text-based forms. In the last two decades significant progress has been made in developing novel sonification systems to further support network-monitoring tasks. A range of systems has been proposed in which sonified network data is presented for incorporation into the network-monitoring process; however many of these have not been sufficiently validated and there is a lack of uptake in SOCs. We present the state-of-the-art in sonification design for network security monitoring tasks, and propose a research agenda comprising investigation of optimal design aesthetics, formalisation of the network data and attack representation requirements, and investigation of the usefulness of sonification through comprehensive user testing with security analysts. We detail a methodology for addressing this research agenda in three parts: user testing of intuitive data-sound mappings; construction of a formalised approach to network data representation through sonification; and quantitative and qualitative user testing of sonification systems.
Protecting Cybersecurity Machine Learning

Wai Sze Leung
Academy of Computer Science and Software Engineering, University of Johannesburg
wsleung@uj.ac.za

Keywords: machine learning; Internet of Things; detection

The gap between attacker and security expert is growing ever wider thanks to the ongoing popularity of the Internet of Things (IoT), resulting in all manner of devices becoming connected. Such a trend has not only increased the number of potential weaknesses in the form of poorly secured devices, but created additional sources of data that may need to be processed and reviewed by security personnel [1]. Such problems are exacerbated by numerous factors that include a glaring shortage of trained security professionals needed to monitor systems, the potential violation of users’ privacies when reviewing data, and wasting limited resources when pursuing false alarms [2].

Machine Learning (ML) is often used as a means of automating the process to support security professionals [3-4]. However, since ML requires that it has access to existing data in order to “learn” to identify future incidences, attackers persistent in their attacks (easily accomplished since attacks can be automated) can therefore “corrupt” this learning process, weakening the ML approach. The manner in which ML is deployed in a diverse environment such as the Internet of Things will therefore require better oversight [1, 5] to ensure that the various sources of security data does not undo its correct learning practices. The research aims to examine how artificial intelligence techniques can make sense of the various sources of security data within the IoT environment, and to identify the trustworthy sources, in order to protect the ML process.

A Secure Mobile Operating System Model

Jaco Du Toit
Academy of Computer Science and Software Engineering, University of Johannesburg
jacodt@uj.ac.za

Keywords: mobile; operating system; cyber security

Many users are using multiple devices for both work and personal use. Many of these devices include mobile devices. The challenge that companies and users face is that data often needs to be exchanged between these various devices. To make the problem more complex, data can either be classified as either personal or business. Cloud storage has been used in most cases to transfer data between the various computing devices of an employee. This transfer of data using cloud storage is arguably not the most secure method for transferring data.

We propose a model where a person only use one device. The device does not have any screen or keyboard attached. The device connects to user input/output devices like screens, touch screens, televisions, monitors, projectors or keyboards wireless. This allows a user to carry the device with him and interact with the device using various form factor screens and keyboards. This eliminates the need for multiple devices.

Because the device is purposely built for both personal and business use, the architecture of the operating system has two very important properties.

The first property is the secure container property. This property ensures owner controlled access to applications and data. The property enforces encryption at rest which provides assurance to various data owners that a device owner cannot access the data without specific permissions and control.

The second property is the mutual authentication property. This property ensures that any peripheral communicating with the device must be mutually authenticated. The authentication level happens per secure container. This assures data owners that only approved peripherals can access the data and applications contained in a secure container.
On the Qui Vive: Exploring Differences Between States in Cyber Security Readiness

Max Smeets
Department of Politics and International Relations, University of Oxford
Max.Smeets@politics.ox.ac.uk

Keywords: cyberspace, cyber security readiness, cyber policy, C3 Dataset

Over the last two decades, national and international security communities have established new policies, partnerships, laws and institutions to effectively prevent and respond to significant cyber incidents. There however remain significant differences across countries when it comes to the readiness against (potential) cyber-attacks. Whereas some countries - such as the United States (US), the United Kingdom (UK), and Estonia - are considered to be ahead of the curve, other countries are lacking behind in coordinating new initiatives in response to the cyber threat.

Although the variation in cyber policy response between countries has often been described, it remains largely unexplained. The purpose of this article is to explain the variation in cyber readiness between countries.

A new dataset was developed, the Country Cyber Capability (C3) dataset, that aggregates earlier datasets and operationalizes additional variables on countries’ cyber capability to offer a quantitative analysis, assessing the substantive effects. This study unsurprisingly finds that a country’s economic size clearly matters for its preparedness or availability to act against cyber-attacks. I also find that a country’s dependency on the internet positively affect its level of cyber readiness. However, against the predictions of the rational choice model, it is shown that states which suffer from more cyber-attacks are not significantly more likely to be well-prepared for cyber-attacks. There seems to be an alarming disconnect between the actual cyber threat landscape and the governments’ cyber operations.
Security through Obstinacy

Arianna Schuler Scott
Centre for Doctoral Training in Cyber Security, University of Oxford
arianna.schulerscott@linacre.ox.ac.uk

Keywords: privacy through obscurity; heuristic processing; systematic processing; privacy awareness

Privacy through obscurity. Security through obscurity is the hope that system vulnerabilities remain undiscovered. Privacy through obscurity is the idea that unless you’re a celebrity or person of interest, information is gathered but no one will ever look at it [1].

Heuristic and Systematic processing. People process information in different ways; heuristically (relying on available cues) and systematically (searching out information), for example. They may be motivated by information sufficiency, privacy calculus or subjective norm, and context. People generally decide based on readily available information rather than make a concerted effort to gather their own data, but this in all likelihood varies with motivation and context.

Privacy through obstinacy. A working phrase, ‘privacy through obstinacy is, I posit, not dissimilar to the ‘head in the sand’ modus operandi. A scenario where users, policy makers and those in industry are all for technical innovation but the human element is left behind (Google ABACUS builds a continuum of trust from facial, speech, keyboard and location patterns to authenticate a user - what happens when they do not match their own pattern? Is interception avoided?). Despite the not inconsiderable investment in Cybersecurity by the public and private sector, continued ignorance seems to exist at a very base level.

Impact. I believe that people need space for ideas to grow, automation is limited. The ‘paranoid’ few who do not subscribe to habit-tracking do not necessarily have something to hide. Technology is streamlined into everyday routine but how do we keep our eyes open? Having a right to privacy also means being aware of our own responsibilities. Ignoring or relegating the issue of privacy will not help - it needs to be discussed. People need their own idea of what ‘privacy’ means, both to them as an individual and as part of a wider community. How do we foster this - at school? At industry level [2]?

A Stage Structured Hybrid Model for Disease Dynamics Modelling

Soumya Banerjee
Mathematical Institute, University of Oxford
soumya.banerjee@maths.ox.ac.uk

Keywords: stage structured hybrid model; immune system modelling; viral dynamics modelling; agent based models; ordinary differential equation models

Stochasticity and spatial distribution of the pathogen play a critical role in determining the outcome of an infection. 1 in a million immune system cells are specific to a particular pathogen. The serendipitous encounter of such a rare immune system cell with its fated antigen can determine the mortality of the infected animal. Moreover, pathogens may remain initially localized in a small volume of tissue. Hence stochastic and spatial aspects play an important role in pathogenesis, especially early on in the infection. Current efforts at investigating the effect of stochasticity and space in modeling of host immune response and pathogens use agent based models (ABMs). However, these are computationally expensive. Population level approaches like ordinary differential equations (ODEs) are computationally tractable. However, they make simplifying assumptions that are unlikely to be true early on in the infection. We proposed a stage-structured hybrid model that aims to strike a balance between the detail of representation of an ABM and the computational tractability of an ODE model. It uses a spatially explicit ABM in the initial stage of infection, and a coarse-grained but computationally tractable ODE model in the latter stages of infection. Such an approach might hold promise in: 1) modeling of other pathogens where the initial stochasticity of the pathogen dictates the trajectory of pathogenesis, and 2) lead to insights into immune system inspired strategies and architectures for distributed systems of computers.
Are We Managing the Risk of Sharing Cyber Situational Awareness? A UK Public Sector Case Study

Michael Davies, Menisha Patel
Department of Computer Science, University of Oxford
{michael.davies, menisha.patel}@cs.ox.ac.uk

Keywords: cyber situational awareness; information risk; consequence management

The development of effective cyber situational awareness, that makes a significant contribution to the decision making process around information risk management, is an important goal for organizations across all sectors. The sharing of such information between and within organizations is seen as a key security enabler. This paper considers a case study of a UK Public Sector organization. The aim is to establish if the decision to share cyber situational awareness has been taken from an information risk management perspective, and to examine whether or not the organization is suitably well-placed, to manage the consequences of information loss, occurring as a result of the sharing process.

Mapping the Coverage of Security Controls in Cyber Insurance Proposal Forms

Daniel Woods, Ioannis Agrafiotis and Jason R. C. Nurse
Department of Computer Science, University of Oxford
daniel.woods@univ.ox.ac.uk

Keywords: cyber insurance; ISO/IEC 27000; risk assessment

Cyber insurance is now a $2 billion market, with that expected to double by 2020 [1]. This means that insurers are taking on liability for ever more cyber risk; this risk is assessed during the insurance application process, which involves on-site audits, telephone interviews and a self-assessed proposal form [2]. The forms contain a number of questions relating to the applicant’s organisation and its cyber security practices.

This talk will present our analysis of 24 insurance proposal forms. From the type of information collected in these forms, we analyse the questions related to cyber security. Our aim is to determine whether the collection of security controls mentioned in the analysed proposal forms corresponds to the controls asked for in ISO 27002 [3] and the CIS Critical Security Controls [4], which are the guider of best practice.

Based on our analysis, we identify gaps in the assessment process and suggest improvements so that the assessment process collects information more relevant to a firm’s cyber security. This would give an insurer a better understanding of the risk that they are liable for and allow them to work with the insured to ensure that appropriate security controls are in place.

Costs and Benefits of Greater Cooperation Between the E.U. and U.S. in Cybersecurity

Benjamin Dean
Columbia University
bcd2120@columbia.edu

Keywords: cybersecurity; cybercrime; economics; cost-benefit analysis; programme evaluation

The European Parliament Research Service has requested an analysis of the costs and benefits of greater cooperation between the E.U. and U.S. in bolstering cybersecurity and combating cybercrime. This draft paper provides such an analysis by integrating and expanding the cybercrime/cybersecurity cost framework developed by Anderson et al (2012) and benefit framework developed by Hughes et al (2014). It provides a taxonomy of areas where cooperation might be achieved cybersecurity policies. It concludes by proposing that evaluations of cybersecurity policies be conducted - potentially jointly by the E.U. and U.S. - using quasi-experiment methods. The final paper will be delivered to the E.U. Parliament Research Service at the end of October 2016.