RISCS

Research Institute in Science of Cyber Security

Annual Report 2014

RISCS

Research Institute in Science of
Cyber Security

Annual Report 2014

Research Institute in Science of Cyber Security | Department of Computer Science
University College London | Gower Street | London | WC1E 6BT

Research Institute in Science of Cyber Security

Advisory Board Members:

John Adams, UCL

Muffy Calder, Scottish Government Chief Scientific Advisor

Larry Hirst, formerly of IBM

Dario Leslie, MoD

Shari Lawrence Pfleeger, I3P

Martin Sadler, HP

Adam Shostack, Microsoft

Participating Universities:

Imperial College London

Newcastle University

northumbria UNIVERSITY

Queen Mary University of London

ROYAL HOLLOWAY UNIVERSITY OF LONDON

UCL

Introduction

As Research Director of the Research Institute in Science of Cyber Security (RISCS) I am proud to present the second Annual Report of our research activities. During our second year, the 4 research projects have really taken off, and produced visible output in form of 32 publications and 48 presentations of our work at a variety of academic, commercial and public sector events.

The four individual projects have made progress that not only advances research, but has direct benefits to security practice:

- The Games and Abstraction project led by Chris Hankin, with researchers at Imperial, Queen Mary and Royal Holloway have developed more sophisticated modelling techniques. Using knowledge from mathematics, economics, and computer science, their work considers the direct and indirect costs of defending systems against a variety of threats. Game theory is combined with other optimisation techniques, such as the knapsack algorithm, to achieve more accurate predictions. And to ensure their models are relevant to security practice, the researchers have linked their modelling to the SANS Institute Critical Security Controls, which many commercial organisations use as a baseline.

- The Cyber Security Cartographies project led by Lizzie Coles-Kemp at Royal Holloway, University of London, has continued its innovative approach to developing tools that enable organisations to understand and manage their security issues: they have created a visual narrative toolkit (including the Current Experience Comic Strip and Tactile Visual Library) that allows a wide range of stakeholders to engage with security issues and express their view, and a clustering algorithm to identify and understand behaviours at the data network layer.

- The Choice Architecture project at Newcastle and Northumbria Universities, led by Aad Van Moorsel, has developed a design approach for practitioners to create choice architectures ('nudges'), formalised the problem to apply mathematical optimisation techniques to nudges, and applied the approach to a Wi-Fi network selection on mobile devices. The approach is initially being tested with employees of small and medium enterprises (SMEs), who need low-effort and light-touch approaches to managing security.

- The Productive Security researchers at UCL have spent most of year 2 analysing the data collected in two major UK companies in Year 1. A new concept describing employee non-compliance has emerge: shadow security. Rather than ignoring security, we found that employees are aware of many information security risks, and protect assets in the best way can - and still be productive. This forms the basis for a new approach to security design – rather than stamping out non-compliance, it offers a starting point for designing workable security. The modelling work creates a basis for predicting the impact on risk and productivity with security managers in the companies involved.

During our quarterly meetings in 2014, we have had lively and enlightening discussions with leading 'frontline' security practitioners from industry and GCHQ, and with our Advisory Board members; we have identified opportunities for cross-project collaboration that we will pursue in the coming year.

But we have already had collective success in advancing the science of cyber security: RISCS researchers made a strong contribution to the Royal Society project on cyber security research in the UK, especially in identifying the benefits of multi-disciplinary approaches – the RS report will be published towards the end of this year. We also provided evidence to the US National Academies investigation into the state of cyber security as a science last year, since RISCS researchers have long-standing collaborations.

These collaborations of RISCS researchers beyond the RI underpin our final major achievement: in 2015, Oxford University Press will commence publication of a journal for multi-disciplinary cyber security research. The Editors in Chief are David Pym (co-Investigator of Productive Security at UCL) and Tyler Moore from Southern Methodist University, and many RISCS researchers and their collaborators will serve on the editorial board.

Professor M. Angela Sasse

Director

Research Institute in Science of Cyber Security

Games and Abstraction

Games and Abstraction addresses the challenge "How do we make better security decisions?"

We have begun to develop new approaches to decision support based on game theory. Specifically we have formulated a notion of Security Games which model the allocation of resources to protect targets in the attack surface of a system. Our work will support professionals who are designing secure systems and also those charged with determining if systems have an appropriate level of security – in particular, systems administrators. We are developing techniques to support human decision making and techniques which enable well-founded security design decisions to be made.

We recognise that the emerging trend away from corporate IT systems towards a Bring-Your-Own-Device (BYOD) culture will bring new challenges and changes to the role of systems administrator. However, even in this brave new world, companies will continue to have core assets such as the network infrastructure and the corporate database which will need the same kind of protection. It is certainly to be expected that some of the attacks will now originate from inside the corporate firewall rather than from outside.

Our team includes researchers from the Imperial College Business School who are helping us to ensure that our models are properly reflecting these new threats.

Whilst others have used game theoretic approaches to answer these questions, much of the previous work has been more or less ad hoc. As such the resulting security decisions may be based on unsound principles. In particular, it is common to use abstractions without giving much consideration to the relationship between properties of the abstract model and the real system. Our work will enable a precise analysis of these relationships and hence provides a more robust decision support tool than has been hitherto available.

Progress in the Year to Date

Cyber Security Game Tool

We have developed a Cyber Security Game Tool with a GUI in Python to evaluate different cyber security games. We have also reviewed alternative optimisation algorithms for comparison with our current solutions. On the theoretical side, we have studied the construction of game models with a more explicit modelling of resources and also investigating alternative (to the singular value decomposition approach used in our previous work) approximation methods.

Big Data Assessment

We conducted a 'big data assessment' experiment to analyse trust in big data. We created two large datasets from two pollution sensor networks that monitor the same location; one of which had been attacked. Our goal was to, first, understand if users of big data are able to detect attacks; second, model how users of a particular data set trust the information they see; and finally, identify the tools and technologies that can be used to test the trustworthiness/integrity of open data.

Extension of the "FlipIt" Game

Carlos Cid has developed an extension of the attacker-defender game FlipIt (proposed by Rivest et al.), to include the option of doing a security testing/assessment of the state of the resource before re-taking the resource. The results provide an indication of when (and in what situations) it would be advantageous for companies to perform a security assessment.

Information Sharing in Cyber Security

Carlos Cid and colleagues from RHUL have worked on the game theoretic modelling of the problem of information sharing in cyber security. Based on some previous work which considered the problem of information sharing, the proposed game models the interaction between firms when deciding to share information related to identified security vulnerabilities and/or attacks. They study potential solutions that may lead to firms to decide to share security information.

A Risk Management Model for Optimising Investment in Cyber-security Controls

We have investigated how to optimally invest in cyber-security controls. In particular we have examined cases where the organization suffers from underinvestment or inefficient spending on cybersecurity. We first modelled the cybersecurity environment of an organization. We then modelled non-cooperative cyber-security control-games between the defender, which abstracts all defence mechanisms of the organization, and the attacker which can exploit different vulnerabilities at different network locations

To implement our methodology we used the SANS Top 20 Critical Security Controls and the 2011 CWE/SANS Top 25 Most Dangerous Software Errors. Based on the profile of an organization, which forms its preferences in terms of indirect costs, its concerns about different kinds of threats and the importance of the assets given their associated risks, we derived the Nash Equilibria of a series of control-games. These game solutions are then handled by optimization techniques, in particular multi-objective, multiple choice Knapsack, to determine the optimal cybersecurity investment. Our methodology provides security effective and cost efficient solutions especially against commodity attacks.

Using the points raised in the SANS Top 20 Critical Security Controls, we conducted interviews with system/security admins of SMEs in in areas of finance, accounting, law, economic consultancy, design and IT consultancy and gathered information regarding these SME's size, scope, assets, concerns and vulnerabilities and analysed those SMEs' defence strategies.

We believe that this work can be used to advise security managers on how they should spend an available cybersecurity budget given their organization profile.

Publications

A. Fielder, E. Panaousis, P. Malacaria, C. Hankin, F. Smeraldi) at the 29th IFIP International Information Security and Privacy Conference (IFIP SEC '14) in Marrakech, Morocco, June 2-4, 2014.

Khouzani, Pham, and Cid, Carlos: "Strategic Discovery and Sharing of Vulnerabilities in Competitive Environments" accepted for inclusion in GameSec 2014 (November 6-7, 2014).

Panaousis, Fielder, Malacaria, Hankin, and Smeraldi: "Cybersecurity Games and Investments: A Decision Support Approach" accepted for inclusion in GameSec 2014 (November 6-7, 2014).

Related Activities

Chris Hankin coordinated the UK Computing Research Committee (UKCRC) response to the Royal Society consultation on Cyber Security.

Chris Hankin presented talks at IE'14 (Cheltenham) and at the Oxford UK-Singapore Cyber Security Research Workshop.

Andrew Fielder and Manos Panaousis presented our latest model to the RISCS modelling workshop at Newcastle.

Hankin contributed to a panel at the FT Cyber Security Summit, September 2014

Chris Hankin gave a keynote lecture at the International Conference on Security of Information and Networks (SIN'14) in Glasgow.

Grant Details

EPSRC Reference:	EP/K005790/1
Title:	Games and Abstraction: The Science of Cyber Security
Principal Investigator:	Hankin, Professor C
Other Investigators:	Hoehn, Professor T
Department: and Technology	Institute for Security Science
Organisation:	Imperial College London
EPSRC Reference:	EP/K005820/1
Title:	Games and Abstraction: The Science of Cyber Security
Principal Investigator:	Malacaria, Dr P
Other Investigators:	Smeraldi, Dr F
Department:	School of Electronic Engineering & Computer Science
Organisation:	Queen Mary, University of London
EPSRC Reference:	EP/K006010/1
Title:	Games and Abstraction: The Science of Cyber Security
Principal Investigator:	Cid, Professor C
Department:	Information Security
Organisation:	Royal Holloway, University of London

Cyber Security Cartographies (CySeCa)

In the cyber environment the balance between benefit and harm can be found at the organisational, as well as national and global, level. It could be said that cyber security research is focused on the exploration of research problems related to striving for the "right" balance. In order to protect their estate security practitioners strive to achieve this balance by combining organisational, physical and technical controls to provide robust information asset protection. In the complex cyber environment a security practitioner has limited visibility of technical, physical and organisational compliance behaviours and controls and this makes it difficult to know when and how to select and combine controls.

Prior to the CySeCa project, research has, to date, not been undertaken to understand how a security manager selects the appropriate control combination. In addition, risk management techniques do not include visualisation methods that can present a combined picture of organisational and technical asset compliance behaviours. This problem is exacerbated by the lack of systematic research of the cultural and organisational techniques used by security practitioners. This paucity of research results in limited practical guidance on cultural and organisational security management approaches.

The goals of the project are to:

- Explore how a security manager develops, maintains and uses visibility of both organisational and asset compliance behaviours for the management of cyber security risks;
- Better understand how organisational controls and technical controls are used in combination;
- Evaluate the use of different visualisations in the risk management process as a means to extend a security manager's ability to deploy combinations of organisational and technical controls in the cyber context.

Progress in the Year to Date

Human-centred Research

Our Current Experience Comic Strip approach has been further developed to support a Tactile Visual Library. This has been used in two case studies:

- A study at a community centre in the North East aimed at further exploration of the nature of data protection in on-line public services. This work was presented at a workshop at CHI 2014.
- A 10-day interactive exploratory case study in an SME, using our tools together with user experience storytelling methods. Visual SME narrative artifacts are being developed from the data and social network analysis of SME using a communication matrix.

Discussions regarding a future central government case study are currently in progress.

The tools developed by the project were also tested by recording a session in which 19 risk management participants completed Current Experience Comic Strips using the Tactile Visual Library. We are currently analysing this data and producing visual representations from it.

We have commenced a joint study with the University of Queensland aimed at creating an improved understanding of the professional identities of information security practitioners in Australia, and a visiting academic, Helen Armstrong, has worked with the CySeCa team to develop a networks integration framework using social network analysis. A number of potential integration frameworks were identified and work is now underway to develop these within inside a responsible innovation framework

Data-centred Research

The Data-centred work has mainly focused on researching and implementing new methods for network trace analysis. Our analysis method makes use of clustering applied to a feature set extracted from network flows, including both traffic flow and host behaviour. These are analysed independently, with the possibility of merging these two views and identifying dependencies between them.

We have researched and implemented dimensionality reduction methods, and these have resulted in improved efficiency and effectiveness of the method, allowing discrimination between meaningful and redundant or irrelevant features.

We have also refined the clustering methods, to leverage the framework for automatic analysis. We have used both hierarchical clustering and, latterly, density-based algorithms such as DBSCAN. This makes the analysis more resilient to network changes and more generic, as it takes out the dependency to some parameters intrinsic to hierarchical clustering.

We have researched on and implemented algorithms for tracking network behaviours over time. We have also improved on the analysis by including timing features that we have used to identify hosts that show periodic behaviours.

Although this is often expressed by benign software such as OS updates or email checking, it can also be indicative of malware or botnets. We have compared normal network traffic with similar traffic injected with a botnet network trace expressing periodic behaviour. Results were very promising, with the distinctive periodic behaviour of the malicious traffic being visible.

Initial results were presented to a commercial collaborator and they have become actively involved in the research process. We have recently begun data gathering from their network to feed into our analysis.

Ethical Principles of Data Collection

We have created a document specifying ethical principles of data collection practices, covering potential unintended consequences for research participants from network monitoring, and this has been approved for use by Royal Holloway.

Publications

Lewis. M, Coles-Kemp, L. (2014) Are You Feeling It? The Use Of Comic Strips To Encourage Empathy in Design. Extended Abstract for Workshop on Enabling Empathy in Health and Care: Design Methods and Challenges at CHI'14 Human Factors in Computing Systems, Toronto, Canada.

Lewis, M., Coles-Kemp, L., Siganto, J. (2014) Picture This: Tools To Help Community Storytelling. Tactile User Experience Evaluation Methods Workshop at CHI'14 Human Factors in Computing Systems.

Lewis. M, Coles-Kemp, L. (2014) Who Says Personas Can't Dance? The Use Of Comic Strips To Design Information Security Personas. Extended Abstract at CHI'14 Human Factors in Computing Systems, Toronto, Canada.

Lewis. M, Coles-Kemp, L. (2014) I've Got Something To Say: The Use of Animation to Create a Meta-Story about Professional Identity. Extended Abstract for Workshop StoryStorm: A Collaborative Exchange of Methods for Storytelling at DIS'14 Designing Interactive Systems, Vancouver, Canada.

Lewis. M, Coles-Kemp, L. (2014) "A Tactile Visual Library To Support User Experience Storytelling". NordDesign2014.

Grant Details

EPSRC Reference:	EP/K006266/1
Title:	Cyber Security
Cartographies:	CySeCa
Principal Investigator:	Coles-Kemp, Dr L
Other Investigators:	Cavallaro, Dr L Hancke, Dr G Price, Dr G Tomlinson, Dr A
Department:	Information Security
Organisation:	Royal Holloway, University of London

Related Activities

A cartoon poster was presented at an HP colloquium at Royal Holloway.

An analysis of a public anonymous dataset provided by University of Brescia [1] was presented at the HP colloquium at Royal Holloway on the 18th of December 2013.

CySeCa researchers attended the 7th European Trusted Infrastructure and Systems School (ETISS) at TU Graz in Graz Austria.

CySeCa project presentations took place at the University of Lancaster and at the Commonwealth Telecommunications Organisation In Nov 2013.

Lizzie Coles-Kemp has presented CySeCa work at Bournemouth University, Defence Academy, Shrivenham and at Royal Melbourne Institute of Technology.

A field visit to Oxford Brookes Movement Lab was undertaken to investigate a potential case study to explore the management of information related to rehabilitation and traumatic brain injury.

Lizzie Coles-Kemp presented CySeCa at a Digital Policy Alliance Meeting at the Royal Society on the 21st May 2014.

Lorenzo Cavallaro presented a first static visualization for tracking behaviours at the July 2014 RISCS meeting.

Choice Architecture for Information Security (ChAISe)

The problem of data loss is exacerbated by the practice of consumerisation, i.e., the use of personal hardware and software within the workplace. ChAISe develops and evaluates an advanced set of tools and techniques, informed by an understanding of human behaviour and rigorous quantitative assessment. The tools are designed to improve organisational and individual decision-making around data loss protection via a process of 'nudging' behaviour towards maximal decisions.

The project develops the tools and techniques that assist in defining a 'choice architecture', as the nudge literature calls it. A choice architecture refers to the manner in which decisions are influenced by the way choices are presented. At the core of the ChAISe choice architecture, we use rigorous model-based and other quantitative techniques to determine an optimal decision and assess the remaining uncertainty about that decision. This choice architecture targets all three parties that make decisions: business leaders (CISOs), IT administrators and employees (i.e., end users).

The project takes the following approach: (1) define the problem area and scenarios that capture consumerisation; (2) identify those psychological factors that affect people's security behaviours and decisions; (3) with this knowledge, develop and implement the choice architecture and a set of tools for influencing or 'nudging' behaviour based on the architecture and (4) evaluate those tools, i.e., develop or appropriate a measure of organisational security and use it to assess the effectiveness of the intervention.

To develop the choice architecture we need to understand how human decision making is influenced, and biases it is prone to. We take inspiration from the work on nudging and MINDSPACE, which provides a framework to influence decision makers as effectively as possible. In particular, we need tools and techniques to form a choice architecture tailored to information security. Information security has particular well-known characteristics, which we exploit to provide sufficient rigour underlying the choice architecture. In particular, the project is establishing rigorous mathematical approaches to include uncertainty about unknowns in our analysis, and will derived a theory about the 'value of rigour', allowing experts to judge which elements of rigour pay off further investment.

We carry out our research in connection to one overarching information security issue of high practical importance, namely 'consumerisation', that is, the use in the workplace of people's own devices, a bring your own device (BYOD) strategy widely used by companies nowadays. This is possibly the main challenge that IT departments face in the coming years, to keep the workplace secure as the boundaries between work and personal life become more blurred.

The project works with large organisations and SMEs through well-established channels. Ultimately, it targets demonstrating the benefits of the advocated choice architecture through a case study in an SME or larger organisation.

Progress to Date

The SCENE Methodology

We have developed a methodology to allow practitioners to develop nudges in collaboration with stakeholders. We have named the methodology "SCENE", from the five-stage process: (i) **S**cenario elicitation; (ii) **C**o-creating nudges; (iii) **E**lection of nudges; (iv) **N**udge prototyping and (v) **E**valuation of prototypes.

The SCENE methodology has been described in a paper at HCI International 2014, and a more detailed report is in preparation.

Wi-Fi Nudge Evaluation

We have completed two phases of the Wi-Fi nudge evaluation experiment, which uses an android app to nudge the participants towards Wi-Fi options that are best in terms of the trade-off between security and productivity. The second phase uses an eye tracking system to observe the participants' eye movement as they make their decisions (72 participants). Results were consistent with the first phase, showing significant increase in selection of better Wi-Fi options when nudged by colour coding. It also showed that personality factors and cognitive biases play a role in security decisions, such as impulse control effects, convenience bias, and control of risk.

Scenario Development

SME-specific and generic security-related scenario templates have been developed.

We have compiled a portfolio of scenarios based on real-life end-user focused incidents, such as fraud and other security risks. This will form a resource and evidence base of the types of security threats that users and organizations encounter.

Social Referent Nudging

We have designed a new experiment to study the effect of social referent nudging using cookies. This has been tested using Mechanical Turk participants, and we are currently analysing this data.

Security Behaviour Analysis

We have conducted a thematic analysis of a series of interviews with people who use mobile devices for their work. The PaCT team are using this data to examine security behaviours in relation to mobile devices and published evidence. The results of this thematic analysis will also be examined in relation to existing theoretical models.

Decision Making Model

We have formalised an abstract decision-making model and developed a model for nudge efficiency evaluation. These models have been applied to our Wi-Fi selection scenario, using a utility-based approach.

We have further developed the generic formalisation to facilitate rigorous quantitative analysis of influencing security behaviour, providing a theoretical basis for studying, optimising, comparing and evaluating approaches.

We have extracted parameters for the decision-making model from the analysis of the results of the Wi-Fi experiment and have used MATLAB to create a prediction model based on this data.

Publications

Coventry, L., Briggs, P., Jeske, D., & van Moorsel, A. (2014). "SCENE: A Structured Means for Creating and Evaluating Behavioral Nudges in a Cybersecurity Environment". In Design, User Experience, and Usability, Design, User Experience, and Usability. Theories, Methods, and Tools for Designing the User Experience, Volume 8517, 2014, pp 229-239.

Charles Morisset, Thomas Gross, Iryna Yevseyeva and Aad Van Moorsel (2014) "Nudging for Quantitative Access Control Systems". In Human Aspects of Information Security, Privacy and Trust, LNCS, Springer, Volume 8533, 2014, pp. 340-351.

Jeske, D., Coventry, L., Briggs, P., & van Moorsel, A. (2014). Nudging whom how: IT proficiency, impulse control and secure behaviour. CHI Workshop on Personalizing Behavior Change Technologies, CHI 2014.

Jeske, D., Coventry, L., & Briggs, P. (2014). Decision justifications for wireless network selection. Socio-Technical Aspects of Security and Trust (STAST) Workshop, Vienna, Austria, 18 July 2014.

Christopher Laing. A Year is a Short Time in Cyber-Space' [published: Industry & Parliament Trust Report: 'Cyber Security 2.0: Reflections on UK/EU Cyber-Security Co-Operation'.

Christopher Laing. Network Situational Awareness: Sonification & Visualization in the Cyber Battlespace; Handbook of Research on Digital Crime, Cyberspace Security & Information Assurance.

Christopher Laing. An investigation into the security of HTML5 IndexedDB. 7th International Conference on Security of Information & Networks.

Coventry, L., Jeske, D. & Briggs, P. (2014). "Perceptions and actions: Combining privacy and risk perceptions to better understand user behaviour" at the Workshop, Symposium on Usable Privacy and Security (SOUPS) 2014, July 9-11, 2014, Menlo Park, CA.

Iryna Yevseyeva, Charles Morisset, Thomas Groß and Aad van Moorsel: "A Decision Making Model of Influencing Behavior in Information Security" Computer Performance Engineering, LNCS, Springer. 8721, 2014, pp. 194-208.

Charles Morisset, Iryna Yevseyeva, Thomas Gross and Aad Van Moorsel: "A Formal Model for Soft Enforcement: Influencing the Decision-Maker". In Security and Trust Management, LNCS, Springer, Volume 8743, 2014, pp. 113-128.

Kovila P.L. Coopamootoo and Thomas Groß. Mental Models of Online Privacy: Structural Properties with Cognitive Maps. BCS HCI 2014.

Yevseyeva I, Morisset C, Turland J, Gross T, Coventry L, Laing C, van Moorsel A. Consumerisation of IT: Mitigating risky user actions and improving productivity with nudging. Accepted for CENTERIS 2014 - Conference on ENTERprise Information Systems.

Budi Arief, Kovila Coopamootoo, Martin Emms, Aad Van Moorsel. Sensible Privacy: How We Can Protect Domestic Violence Survivors Without Facilitating Misuse. Accepted for Workshop on Privacy in the Electronic Society, Nov. 2014.

Related Activities

Iryna Yevseyeva presented ChAISe project at the research seminar in Portsmouth Business School, UK on 27th November 2013 and at the research seminar in Leiden University, Leiden Institute of Advances Computer Science (LIACS), The Netherlands on 9th of December 2013.

A meeting of PaCT with Lizzie Coles-Kemp and Makayla Lewis from CySeCa Project was held on 16th December 2013.

A ChAISe Away-Day meeting of the whole team at the Dove Marine Laboratory of Newcastle University was held on 8th and 9th January 2014.

Lynne Coventry and Christopher Laing visited two SMEs in the Northeast to present the methodology and explore the possibility of future collaboration.

Pam Briggs was invited to join the European Commission Joint Research Centre panel on "Nudging Internet citizens: lessons from behavioural studies on online privacy", on 23rd January, as part of the 7th International Conference on Computers, Privacy and Data Protection (CPDP), Brussels.

Lynne Coventry acted as a commissioner for The Industry and Parliament Trust's (IPT) Cyber Security 2.0 project.

Lynne Coventry served as a Keynote panellist at Information Security Europe (Earls Court) 29th April, on Usability versus Security.

Debora Jeske presented the preliminary results of the ChAISe project at Jacobs University Bremen in Germany as part of their Spring 2014 Transdisciplinary Colloquium Series.

Christopher Laing hosted whole day session on information & network security at Ignite100 [Newcastle; May 14th 2014]

Christopher Laing hosted 'How a digital forensics investigation is conducted' at Crime Writers Festival [May 31st – June 1st]

Christopher Laing hosted digital forensics break-out session at Crime Writers Festival [May 31st – June 1st]

Aad van Moorsel Presentation at CSR Away Day at Chester, UK: Information Security Research in Newcastle, June 3 2014.

Chris Laing is organizing Girls Into Cybersecurity day at the Northern Design Centre in Gateshead, October 2014.

Charles Morisset, Thomas Gross, Aad van Moorsel: GCHQ PhD studentship accepted on "Modelling for Defending against Influencing Attackers"

Lynne Coventry is a participant in a proposal PassParTu: User Network Security using Endpoint Sensors to the Digital Security: Cybersecurity, Privacy and Trust.

Iryna Yevseyeva gave a talk "Predicting security choices considering a set of models and behavioural features" at the Behavioural Operational Research stream of UK Operational Research Society Annual Conference (OR56) on 9-11 September 2014 at Royal Holloway.

A Project report for GCHQ outlined and demonstrated the use of eye tracking in security using a small wireless study.

Kovila P.L. Coopamootoo, Thomas Groß, Mental Models for Usable Privacy: A Position Paper HCII'14 (Poster paper)

Kovila P.L. Coopamootoo; Thomas Gross Preliminary Investigation of Cognitive Effort in Privacy Decision-Making: Sharing Personal Information vs. 3 X 4 SOUPS'14 (Poster paper)

Kovila P.L. Coopamootoo and Thomas Groß. Cognitive Effort in Privacy Decision-Making vs. 3 x 4: Evaluation of a Pilot Experiment Design. At WIPS of LASER'14, without proceedings.

Grant Details

EPSRC Reference:	EP/K006568/1
Title:	Choice Architecture for Information Security
Principal Investigator:	van Moorsel, Professor A
Other Investigators:	Laing, Dr CD Gross, Dr T R Briggs, Professor P Coventry, Dr L
Researcher Co-investigators:	
Project Partners:	
Department:	Computing Sciences
Organisation:	Newcastle University

Productive Security

The Productive Security project is conducted by researchers in the Information Security Research Group at University College London (UCL) Department of Computer Science, led by Professor Angela Sasse and Professor David Pym (formerly of the University of Aberdeen).

The aim of the Productive Security project is to scientifically assist decision makers in the field of information security to make more optimal choices with respect to both their organisation's security and productivity.

Over recent years, there has been a growing body of evidence that security policies and controls are not effective because employees either can't, or won't, comply. Many employees are left to make choices between complying with security, and getting their work done - and overwhelmingly choose the latter. Most organizations do not measure the effort associated with compliance, nor invest in integrating security into their business processes, leaving their employees to deal with the 'friction' this causes.

When it comes to security controls used within companies, the workload placed on employees still seems to be ignored, with negative consequences for security and productivity. Non-compliance can undermine security – inflexible access control systems, for instance, lead to informal sharing of restricted information through channels outside the system. This means that the organisation loses both control and the audit trail (which is often a regulatory requirement). Employees reorganise their primary tasks to avoid or minimise the amount of exposure to security mechanisms that are too onerous.

What is missing is a systematic investigation of how much individual and accumulated effort leads to such responses, and what the approximate impact is on risk and productivity.

Decisions about security controls are currently most often guided by the need to comply with legal and regulatory requirements, and industry standards or 'best' practice. Without hard evidence about the resulting risk mitigation or impact on productivity, decision-makers have little choice but to be guided by these factors.

Security decision-making can be changed through tools which enable decision-makers to consider a wider range of options than those they habitually choose, and which show the predicted impact on productivity as well as risk mitigation. There exists a strong requirement for a structured, scientifically-grounded decision-making framework into which existing data can be inserted, alongside the key 'missing link' measurements of employee's workload, risk perception, and resulting security behaviours.

Productive Security is about:

- Creating methods and analytic tools to measure the impact of security controls on employees, and further determine how well they fit with business processes and employees' tasks, based on a foundation of empirical evidence.
- Improving, by way of positively altering existing perceptions, employees' understanding of: organizational risks; the role of security controls, and; how their own behaviour can prevent or facilitate security breaches.

Progress to Date

Work with Industrial Partner A (Critical National Infrastructure)

We have used information from ongoing discussions with Company A's physical security managers to inform a physical security model. The creation of a model identified "touchpoints" for further discussion with Company A managers, as well as creating a structure to support the ongoing data collection. Further site visits are planned to collect data for the "Site Entry Observation" study.

Work with Industrial Partner B (Telecoms)

Findings of our analysis of interview data and scenarios have been reported at Board level within Company B, and had an immediate impact on the organisation's security agenda for the coming year.

Data collected during the company-wide survey was examined to identify results relevant to tailgating and screen locking models being developed within the project - this data was then structured for use in calibrating the models, towards supporting a methodology for the composition of separate models.

A PhD student was embedded for 6 months at head office to work with the company on a culture change programme targeted at problem areas identified by UCL researchers.

Work with Industrial Partner C (Security Technology Services)

In November 2013, Angela Sasse delivered an online presentation of the group's research to partner security specialists based at various sites globally, resulting in requests for one-to-one follow-up discussion. A report summarising the group's (published) research approach to date was disseminated internally to security innovation staff as part of a regular electronic newsletter.

A shared goal of producing a collaborative Security Awareness whitepaper has been established.

Work with Industrial Partner D (Higher Education)

To support application of the Productive Security method, interviewer training material has been produced and training sessions for interviewers have been conducted. This will support repeatable development of specialised interviewing skills for researchers. User interviews will be coordinated using a recently developed purpose-built, customisable remote study and study participant signup system. The design of this system and its modes of use for researchers embody many lessons learnt from prior security usability studies within the wider research group at UCL.

Teaching Material

In advance of the new academic year, case studies and scenarios for different organisational contexts have been updated reflecting observations made during interactions with partner organisations. These will figure foremost in teaching materials for Information Security students.

Publications

I. Kirlappos, S. Parkin, M. A. Sasse, "Learning from "Shadow Security": Why understanding non-compliance provides the basis for effective security", Workshop on Usable Security (USEC), 2014.

C. Ioannidis, D. Pym, J. Williams, I. Gheyas, "Resilience in Information Stewardship", Workshop on the Economics of Information Security (WEIS) 2014, Penn State University, 23-24 June, 2014.

T. Caulfield, D. Pym, J. Williams, "Compositional Security Modelling: Structure, Economics, and Behaviour", Proceedings of the Foundations, Tools, and New Concepts in Trusted Computing track of the 2nd International Conference on Human Aspects of Information Security, Privacy and Trust, HCI International 2014, Heraklion, June 2014.

I. Kirlappos, M. A. Sasse, "What Usable Security Really Means: Trusting and Engaging Users", Proceedings of the Human Aspects of Information Security, Privacy and Trust track of the 2nd International Conference on Human Aspects of Information Security, Privacy and Trust, HCI International 2014, Heraklion, June 2014.

A. Sasse, M. Steves, K. Krol, D. Chisnell, "The Great Authentication Fatigue - And How To Overcome It", Proceedings of the Cross-Cultural Design track of the 2nd International Conference on Human Aspects of Information Security,

Privacy and Trust, HCI International 2014, Heraklion, June 2014.

M.A. Sasse, I. Kirlappos. "Design for Trusted and Trustworthy Services: Why We Must Do Better". In Trust, Computing, and Society (pp.229-249). Cambridge University Press, 2014.

C. Ioannidis, D. Pym, J. Williams, I. Gheyas, "Resilience in Information Stewardship", Workshop on the Economics of Information Security (WEIS) 2014, Penn State University, 23-24 June, 2014.

T. Caulfield, D. Pym, J. Williams, "Compositional Security Modelling: Structure, Economics, and Behaviour", Proceedings of the Foundations, Tools, and New Concepts in Trusted Computing track of the 2nd International Conference on Human Aspects of Information Security, Privacy and Trust, HCI International 2014, Heraklion, June 2014.

I. Kirlappos, M. A. Sasse, "What Usable Security Really Means: Trusting and Engaging Users", Proceedings of the Human Aspects of Information Security, Privacy and Trust track of the 2nd International Conference on Human Aspects of Information Security, Privacy and Trust, HCI International 2014, Heraklion, June 2014.

A. Sasse, M. Steves, K. Krol, D. Chisnell, "The Great Authentication Fatigue - And How To Overcome It", Proceedings of the Cross-Cultural Design track of the 2nd International Conference on Human Aspects of Information Security, Privacy and Trust, HCI International 2014, Heraklion, June 2014.

M.A. Sasse, ""Technology Should Be Smarter Than This!: A Vision for Overcoming the Great Authentication Fatigue", Secure Data Management, Lecture Notes in Computer Science 2014, pp 33-36

Related Activities

Talk: MA Sasse: 8th November 2013: "Federated Identity To Access e-Government Services – Are Citizens Ready For This?", DIM Workshop, Berlin

Talk: MA Sasse: 5th December 2013: "Federated Identity To Access e-Government Services – Are Citizens Ready For This?", Royal Holloway University of London (RHUL), Egham

Invited Seminar: S Parkin: 10th December 2013: "Approaching Metrics for User Security Behaviour in Organisations", Bournemouth University, Bournemouth

Talk: MA Sasse: 12th February 2014: "User-centric security", Public sector conference, Edinburgh

Distinguished Lecture: Angela Sasse: 5th March 2014: "The Great Authentication Fatigue - End of an Era?", Distinguished Lecture, Southampton

Invited Keynote: MA Sasse: 18th March 2014, Cisco Breakathon, Greenwich

Invited Keynote: MA Sasse: 8th April 2014, IAP (Analysts and Programmers) Symposium, Cue Gardens, London

Invited Talk: MA Sasse: 30th April 2014: "Learning from Shadow Security", Royal Holloway CDT in Cyber Security, Royal Holloway University of London (RHUL), Egham

Invited Session Talk: MA Sasse: 17th June 2014: "Why do people not comply?", Information Assurance (IA14)

Invited Keynote: MA Sasse: 1st July 2014: "What's wrong with usable security?", Distinguished Lecture, Surrey

Invited Opening Keynote: MA Sasse: 3rd July 2014: "Do you care if Johnny can encrypt?", Fourth International Workshop on Cryptography, Robustness, and Provably Secure Schemes for Female Young Researchers (CrossFyre), Bochum University

Invited Keynote: MA Sasse: 10th July 2014: "Security Awareness and Education - Time for a Re-Boot", ISSA Cyber Security Day

Opening Keynote: MA Sasse: 30th July 2014: "How much security can we afford?", IBM security community day, London

Opening Keynote: MA Sasse: 25th August 2014: “It’s Requirements, Jim – But Not As We Know Them”, ESPRE Workshop, Karlskrona, Sweden

Invited Panel Member: MA Sasse: 11th September 2014: "How assured is your information?", IAAC Symposium, BT Newgate St, London

Grant Details

EPSRC Reference:	EP/K006517/1
Title:	Productive Security – Improving security compliance and productivity through measurement
Principal Investigator:	Sasse, Professor MA
Other Investigators:	Pym, Professor D
Department:	Computer Science
Organisation:	University College London