RISCS

Research Institute in Science of Cyber Security

Annual Report 2015

RISCS

Research Institute in Science of
Cyber Security

Annual Report 2015

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 third Annual Report of our research activities – and the final one of our initial funding period. During the last year, the 4 research projects have produced tangible impact as well as academic results:

- The Cyber Security Cartographies project (led by Lizzie Coles-Kemp at Royal Holloway, University of London) has applied the innovative tools for eliciting security requirements with a central department in Her Majesty's Government to create a richly detailed picture of the day-to-day information handling practices. The tools allowed security teams to engage deeply with the workforce and uncover hitherto unseen risks and their root causes. And - perhaps even more significantly - the understanding between security and the general workforce improved during the process, and with this understanding are better able to collaborate effectively to improve both security and business performance.

- The Games and Abstraction project (led by Chris Hankin, with researchers from Imperial, Queen Mary and Royal Holloway) have built a database of cyber-data to use for mathematical modelling; (these are tables of numerical values for controls and attacks and built tools that allow users to specify parameters, such as budget and risk appetite and compute optimal investment portfolios. One of the Games & Abstraction researchers, Dr Andrew Fielder, has been appointed the first NTA Postdoctoral Research Fellowship, and will be working with GCHQ to develop the system security modelling further.

- The Productive Security project (led by Angela Sasse at UCL) has also continued its work to model organisations, risks, security policies and mechanisms, and human behaviour to identify (cost) effective ways of delivering security. The effectiveness of current approaches to security education was one line of enquiry, and collaboration with one of the commercial project partners and GCHQ has led to a White Paper that outlines an organisational strategy for ensuring security hygiene (security that is compliable) followed by a behaviour change approach that engages and support employees. The project has also been working on creating workable advice for small and medium sizes enterprises (SMEs), and researcher Dr Simon Parkin spent a 4 month part-time secondment with a company that supports 70 SMEs to learn more about specific challenges and test interventions.

- The Choice Architecture project at Newcastle and Northumbria Universities (led by Aad van Moorsel) has continued its work to identify optimal targets, forms and timings for interventions to encourage choice of secure behaviours. The project's proposed design cycle for influencing techniques has been applied to a number of case studies, including ones with regional SMEs. We identified information security practices that needed to be changed to protect the SME's assets and maintain employee productivity. Using experimental data and by enhancing traditional mathematical business modelling techniques with a notion of influencing, the researchers are now experimenting with approaches to tailor choices to particular settings and users, and to optimize their application in the field.

During our quarterly meetings – where we engage with leading researchers and practitioners from industry and government – we have in-depth discussions that challenge orthodoxy and encourage new thinking and collaboration across projects and with our external discussion partners. CESG's new password guidance (Password guidance: simplifying your approach https://www.gov.uk/government/publications/password-policy-simplifying-your-approach) resulted from a presentation by Dr Cormac Herley at the October 2014 meeting, and subsequent discussions.

I have chosen to highlight the impact of RISCS research in this Introduction, but our academic output is still impressive, with 31 publications in quality venues, and 50 presentations by RISCS researchers. This year we have launched the multidisciplinary Journal of Cybersecurity (http://cybersecurity.oxfordjournals.org/). Editors in Chief are Prof. David Pym (co-Investigator of Productive Security at UCL) and Dr Tyler Moore from University of Tulsa.

Whilst we have made academic and real-world impact, these are only first steps towards effective security for organisations, at a time when many of them are experiencing more sustained and serious attacks. We are currently applying for funding to continue RISCS for a further 5 years to continue our research to inform their security decisions.

Professor M. Angela Sasse FREng

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

We have developed on an approach to compare several methods of allocating a cyber security budget. The approach considers a game theoretic representation of the entire problem, a purely optimisation based approach that does not consider the adversary's strategy and a hybrid method combining the two. We have been able to identify the trade-offs that exist between the optimality of the solutions, computational complexity of generating the solutions and how easily the solutions can be interpreted for practitioners.

Additionally, we have developed a more accurate mapping from the available resources to our model. This allows us to better represent the controls and vulnerabilities in our calculations. The outcome of this improved mapping is that it gives us greater confidence in not only the model, but in the reliability of the results to better reflect the real world environment. The case study considers an SME like entity and currently considers 37 different attacks and 27 different controls. The case study has been developed based on a new platform capable of numerically evaluating a wide range of kinds of cyber attacks.

We have developed a prototype web tool that gives advice to users about the implementation of their cyber defences. The system is designed to assume no technical knowledge of cyber security on the part of the user, but rather for them to supply information about their organisation consisting of their requirements and preferences. This allows us to create a profile of the organisation, which is used to better inform the internal algorithms. The system takes a UI approach based on a simple combination of menus and sliders that provide the input from users, where the advice is given in both a simple text form as well as in a graphical medium. The internal algorithms use lightweight optimisation algorithms to solve the game theory based representation within the tool.

C Cid and A Khouzani have developed on a model of a non-zero-sum game between a hider and a seeker, which was motivated by the problem of selecting and guessing passwords. We studied two cases: in the first model (capped-guesses) we considered a seeker that has a restricted action size, i.e., can make a bounded number of guesses; in the second model (costly-guesses) we investigate a seeker that has no bound on the number of guesses but has to incur a cost per each guess. We obtain the NE and SSE for the two cases; when discussing the motivating example of password choice, we provide insights on optimal password-selection policies and a prediction of how the password defence-attack paradigm is likely to evolve.

Collaborative work has been undertaken with the team at UCL to model cyber security decision making for system administrators. The work focuses on system administrators' discovery of vulnerabilities and exploits in their systems and the allocation of time to decision making regarding pro-active and reactive defensive measures. The work makes use of stochastic games for decision making based on non-static attack graphs.

Publications

A Fielder, EA Panaousis, P Malacaria, C Hankin and F Smeraldi, 'Comparing Decision Support Approaches for Cyber Security Investment', CoRR abs/1502.05532, 2015, http://arxiv.org/abs/1502.05532.

MHR Khouzani, P Mardziel, C Cid, M Srivatsa, 'Picking vs. Guessing Secrets: A Game-Theoretic Analysis'. in IEEE 28th Computer Security Foundations Symposium (CSF 2015), Verona, Italy, 13-17 July 2015.

T Caulfield and A Fielder, 'Optimising Time Allocation for Network Defense', to appear in Journal of Cybersecurity, 2015.

Related Activities

Hankin spoke at the Global Forum on Cyber Security for the Financial Sector, Frankfurt, May 2015.

Hankin chaired the Westminster Briefing Cyber Security Summit, July 2015

Hankin chaired the Daily Telegraph roundtable on Cyber Security skills, September 2015.

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:	Institute for Security Science and Technology
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

The CySeCa researchers have continued to explore visual methods for layering and representing data of different types, some of which have not been used before in data analysis of this kind. The method of exploration has drawn inspiration from a number of fields of study including natural history, examining methods such as the Chaine Operatoire which, in archaeology, is used as a means of combining task flows with anthropological description.

An extensive literature review has also been conducted, covering all aspects of the human-centred research, exploring a wide range of topics in related disciplines.

The team has continued to develop their human-centred analytical framework and have extensively researched analytical techniques with to apply to the data gathered from the previously-conducted SME case study. In particular:

- A Discourse and Concordance Analysis was performed on a subset of the SME case study data;
- A Visual Theme Grid (VTG) has been developed that allows for improved data organisation, analysis and presentation of varied mixed media qualitative research;
- Interview data has been subjected to Thematic Analysis and Thematic Networks Development processes; and
- A narrative tool known as an "Information Sharing Journey" has been created from analysis of visual and audio recordings of users.

The team's Visual Theme Grid (VTG)has been further developed to create a digital Visual Theme Grid (dVTG) that allows for improved presentation and interaction of the VTG.

Three Central Government 11-day case studies were completed using CySeCa's human-centred visualisation methods to identify barriers to information sharing and protection, and to brainstorm responses to those barriers. Interim findings were presented to the Security team at the Central Government department.

This case study has enabled the project to evaluate how the project's creative security techniques can be scaled up within an organisation. The result has been the development of a means of identifying and understanding how social networks within organisations help staff to protect information during times of organisational adversity. This type of capability has the potential to add a resilience dimension to a security management framework.

Data-centred Research

The data-centred research team have developed a situational awareness system composed of two main parts: a machine learning network analysis core and the visualisation system.

This analysis can be performed with minimal network traffic sources, but the system is modular, with the capability of using data coming from multiple sources (e.g. logs or events collected by a SIEM). The more sources that are available, the richer the picture becomes.

A major part of the project's data-centred efforts have focused on understanding the practical application space for the methods that have been developed so far, and how these methods could be effectively employed within the industry. To this end, the team have met with security practitioners who have a technical background, explaining the technical aspects of the data-centred research methods and demonstrating the visualisation methods. The objectives of these meetings were to:

- Understand the practical needs of the industry so as to concentrate effort in useful directions;
- Ensure that the team understands existing tools that are being used in practise; and
- Examine the differences between the CySeCa approach and any existing tools where functionality partially overlaps.

Feedback from this process was positive and may be summarised as:

- The automatic analysis and tracking of behaviours is potentially very useful as it allows for selective and precise exploration of events, allowing the analyst to focus on specific details by aggregating and filtering out noisy or irrelevant events; and
- Compared to current tools that are often too complex, the straightforward and minimalistic visualisation makes it ideal

and accessible to people that have a basic technical background (e.g. junior analysts), who need to interact with security awareness tools on a daily basis and have, therefore, to spend time learning how to use such tools.

In response to the feedback from practitioners, the team have refined their techniques further, and added some new features to the framework. In particular, it is now possible to generate signatures of specific network behaviours for use with certain intrusion detection systems (including the open-source "Bro" monitoring system). This allows the framework to be used in real time for alerting practitioners to network activity of interest. Other refinements in the framework include the ability to track clusters of events across multiple days.

The team have gone on to perform experiments with different datasets, including benign and malicious traffic. It is possible to clearly identify some benign behaviour, e.g., connections to data-centres and news polling. They are also able to clearly identify some specific malicious activities: typically, given a specific piece of malware, several clusters can be seen which partly blend in with benign activity but also produce some very specific and isolated new behaviour.

Integration of Human-centred and Data-centred Research

A major activity for CySeCa over the last year has been to bring together the human-centred and data-centred research into a single integrated visualisation system.

The initial SME case study has been used as a starting point for this integration. This data was initially gathered and analysed separately by the human-centred and data-centred researchers but the researchers have now explored potential touch points between the two lines of analysis, looking for areas where the weaknesses in one approach can be addressed by corresponding strengths in the other.

In one significant example of this process, the researchers have found that unexplained silences in data are potential spaces in which unwanted information management behaviours can emerge. They have developed a model that enables gaps in the social network to be further explored at the data network level. Such a model also enables unexpected gaps or silences at the data network level to be examined in terms of the relationships at work within an organisation. This type of capability has the potential to add another means for security practitioners to identify potential attack vectors before they are exploited.

In addition, the researchers have also been examining situations in which the two analysis methods have similarities, and have been investigating the ways in which these can point towards general principles and a "bigger picture".

CySeCa's central government case study of 2015 has enabled the project to evaluate how the project's creative security techniques can be scaled up within an organisation. The result has been the development of a means of identifying and understanding how social networks within organisations help staff to protect information during times of organisational adversity. This type of capability has the potential to add a resilience dimension to a security management framework.

Presentations

M Lewis: Abstract paper “Seeing What You See: Collecting and Analysing Participatory Design Data” at the 4th International Visual Methods Conference, Brighton (IVM2015).

Related Activities

Human-centred and data-centred work was presented at the HP Colloquium at RHUL in December 2014.

CySeCa project results and outputs were presented at Queensland University of Technology in November 2014.

CySeCa project results and outputs were presented to local government (Havant CC and Sunderland CC) in November and December 2014.

An overview of CySeCa was presented to the Thames Valley Cluster, a network of SMEs.

Human-centred narrative tools were presented to ANZ Bank (Australia) and AISA (Australian Information Security Association).

A meeting was held with three security practitioners to review data-centred methods and output.

A researcher from University of Queensland was seconded to CySeCa for two months in order to participate in work on a Central Government case study.

L Coles-Kemp presented CySeCa activities to Deputy Chief Executive of Sunderland City Council.

Grant Details

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

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 in the Year 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 model of physical security. 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.

To support this, we have developed dedicated data-collection software to capture system events and facilitate efficient collection of relevant data from observed systems. Such collection of data over time has the potential to suggest targeted interventions to improve security within the organisation.

Data collection has now been completed for a "Site Entry Observation" study. This data is being used to calibrate our existing physical security models and may be used in calibration of physical security mechanisms at the observed site. Follow-up observations have identified potential changes to physical security.

Two additional separate sites have also been observed, one for detailed arrival and departure behaviours, and the other for its entry configuration.

A tailored model of the original site is now being constructed incorporating data gathered from CCTV observations of entry behaviour in order to explore possible implications - for both employees and security - of replicating potential newer entry configuration at that site.

Work with Industrial Partner B (Telecoms)

A PhD student was embedded for 6 months at the head office to work with the company on a culture change programme targeted at problem areas identified by UCL researchers. This secondment identified many sources of evidence for security behaviour, including the leavers process, usability and availability of information storage and sharing systems, and clear desk processes. Measurements were proposed for analysing such systems to determine the prevalence of the security behaviours encouraged within the organisation.

An analysis of interviews with staff in Company A and Company B revealed that security behaviour is driven by a combination of risk perception and emotional stance towards security policy. An analysis framework has been developed which offers diagnostic and intervention-shaping tools for improving security culture. The framework can be used to identify groups of employees that potentially pose a risk to the organization, as well as those with beneficial skills and expertise.

Work with Industrial Partner C (Security Technology Services)

Following on from the interest generated within Company C by an online presentation by Angela Sasse about the group's research, a report summarising the group's published research approach was disseminated internally to security innovation staff.

This has led to collaboration over the past year with Company C staff on a whitepaper on security awareness, which is due for publication in the near future.

Work with Industrial Partner D (Higher Education)

Over the last year, we have conducted interviews with Company D staff using an interview protocol that integrates insights from complementary system modelling and risk perception.

A study of the institution's helpdesk password reset data has also been conducted, complemented with focused interviews with 20 end-users, allowing comparison of 2 years of helpdesk password reset logs with user perspectives on the perceived usability of the system. The combined study of system data and user perspectives contributes to our work on measuring the impact of security on productivity.

Publications

Iacovos Kirlappos, Simon Parkin, M. Angela Sasse, "'Shadow Security' as a tool for the learning organization", ACM Computers & Society Special Issue on Security, Privacy, and Human Behavior, 2015.

M. Collinson, K. McDonald, and D. Pym, "Layered Graph Logic as an Assertion Language for Access Control Policy Models", Journal of Logic and Computation, 2015

Tristan Caulfield and David Pym, "Modelling and Simulating Systems Security Policy", Proceedings of the Eighth International Conference on Simulation Tools and Techniques (SIMUTOOLS 2015), 2015.

Angela Sasse, "Scaring and Bullying People into Security Won't Work ", Security & Privacy Economics, IEEE Security & Privacy Magazine, 13:3, May/June 2015, IEEE.

Workshop Presentations

Kat Krol, Eleni Philippou, Emiliano De Cristofaro, M. Angela Sasse: "'They brought in the horrible key ring thing': Analysing the Usability of Two-Factor Authentication in UK Online Banking", Workshop on Usable Security (USEC) '15, February 2015.

Iacovos Kirlappos, M. Angela Sasse, "Fixing Security Together: How trust relationships develop in organizational security implementations and how they can be used to improve security compliance", Workshop on Usable Security (USEC) '15, February 2015.

Simon Parkin, Kat Krol, Position Paper: "Appropriation of Security Technologies in the Workplace", Experiences of Technology Appropriation: Unanticipated Users, Usage, Circumstances, and Design, in conjunction with the European conference on Computer-Supported Cooperative Work (ECSCW '15), Oslo, Norway, September 2015.

Simon Parkin, Sanket Epili, "A Technique for using Employee Perception of Security to Support Usability Diagnostics", 5th Workshop on Socio-Technical Aspects in Security and Trust (STAST 2015), Verona, Italy.

Zinaida Benenson, Gabriele Lenzini, Daniela Oliveira, Simon Parkin, Sven Übelacker, "Maybe Poor Johnny Really Cannot Encrypt - The Case for a Complexity Theory for Usable Security", New Security Paradigms Workshop (NSPW 2015), Twente, The Netherlands

Odette Beris, Adam Beautement, Angela Sasse, "Employee Rule Breakers, Excuse Makers and Security Champions: Mapping the risk perceptions and emotions that drive security behaviors", New Security Paradigms Workshop (NSPW 2015), Twente, The Netherlands.

Related Activities

Talk: MA Sasse: 27th October 2014: invited talk, "Convenient and trustworthy biometrics – let's get it right this time", Workshop on "Preserving Privacy in an Age of Increased Surveillance – A Biometrics Perspective", IBM & European Association for Biometrics (EAB), London.

Talk: MA Sasse: 31st October 2014: session speaker, UK-US Cyber Security Symposium, UK Science & Innovation Network, Boston.

Talk: MA Sasse: 4th November 2014: invited lecture, "How Much Security Can We Afford?", Cyber Corp lecture, George Washington University, Washington DC.

Talk: MA Sasse: 19th November 2014: invited panel speaker, "What your employees really think about your security policies", IAAC Private Discussion Meeting (PDM), London.

Co-organiser and speaker: MA Sasse: 1-5th December 2014: "Socio-technical Security Metrics" seminar, Dagstuhl Seminar 14491, Dagstuhl, Germany.

Pitch presentation: S Parkin: 1-5th December 2014: "Metrics for Security Behaviour in Organisations", "Socio-technical Security Metrics" seminar, Dagstuhl Seminar 14491, Dagstuhl, Germany.

Pitch presentation: T Caulfield: 1-5th December 2014: "Metrics and Models", "Socio-technical Security Metrics" seminar, Dagstuhl Seminar 14491, Dagstuhl, Germany.

Talk: MA Sasse: 8th December 2014: session chair, "Toward Rational Cybersecurity", Sackler Forum, Washington DC.

Invited Talk: MA Sasse: 28th January 2015: "Cyber Security", Cyber Innovation Day at the Cyber Startup Summit, IDEALondon, London.

Invited Talk: MA Sasse: 23-25th March 2015: "Biometrics For Implicit Authentication – Usability Triumph or Privacy Nightmare?", IEEE International Conference on Identity, Security and Behavior Analysis (ISBA 2015), Hong Kong.

Invited Talk: S Parkin: 23-24th March 2015: "What Makes An Effective Security awareness Programme?", Infosec Dialogue, Noord Group, Oxfordshire.

Invited Talk: MA Sasse: 26-27th March 2015: "The Future of Identity: Technology, Money, or Authenticity?", EPSRC Identity Event.

Talk: MA Sasse: 31st March 2015: "Adventures in Policy Land", UCL MSc Open Evening, UCL.

Invited Talk: MA Sasse: 4-6 May 2015: "Protecting Users Against Online Attacks", Frankfurt German Online Banking Security Workshop, Heppenheim, Germany.

Distinguished Lecture: MA Sasse: 7-8 May 2015: "Implicit authentication via biometrics: usability triumph or privacy nightmare?", TU Darmstadt

Keynote: MA Sasse: 12 May 2015: "Better design for a resilient digital society", ESRC Cyber Security workshop, London

Invited Panel Member: MA Sasse: 30 May 2015: End of Privacy event, Web We Want Festival, Southbank Centre, London

Invited Talk: A Beautement: 9 June 2015: "Influencing behaviour through system design", UK Chapter Summer Meeting, Information Security Forum, London.

Invited Workshop: A Beautement: 10 June 2015: "User Behaviour Workshop", UK Chapter Summer Meeting, Information Security Forum, London.

Invited Panel Member: MA Sasse: 10 June 2015: "Cybersecurity & The New Government: What Changes Should We Expect?", The New Government & Cyber Security – Breakfast Briefing, The Cyber Security Summit, London.

Invited Talk: MA Sasse: 17 June 2015: "Cyber Security and Financial Crime", International Centre for Parliamentary Studies (ICPS), London.

Talk: MA Sasse: 10th July 2015: "A New Approach to Transforming Security Behaviour", SANS Security Awareness Summit.

Invited Talk: MA Sasse: 16th July 2015: "Awareness is only the first step: A model for changing user behaviour", CAST, Usable Security Day, CAST-Seminar, Competence Center for Applied Security Technology (CAST e.V.), Darmstadt.

Invited Talk: MA Sasse: 20th August 2015: "There is no 'privacy paradox' – just technology that does not support users' privacy preferences", IFIP Summer School

Invited Talk: MA Sasse: 2nd-3rd September 2015: "Can we Transform Security Behaviour?", BX2015, London.

Quoted Expert: MA Sasse: 11th September 2015: "How to pick the perfect password", BBC News, http://www.bbc.co.uk/news/technology-34221843.

Keynote: MA Sasse: 15th September 2015: "'Rule breakers, excuse makers, and security champions' – working with people to improve security", Future Security, Berlin.

Quoted Expert, MA Sasse:"Cybercrime 2015: No one is safe", Work Magazine, Winter 2015, Pg. 28, CIPD.

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

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 in the Year to Date

Influencing Users' Choice of Wi-Fi

Following on from the project's earlier work on nudging users to make better Wi-Fi choices and building a model of this process, the Newcastle team have moved on to carry out measurements of the amount of nudging influence that is needed to affect users' choices. In this, they have been examining:

- How much nudging influence is needed to change the choice of a decision maker;
- How influential each criterion that the user applies is in making their final decision; and
- How accurate is the prediction of the decision makers' choices.

As a result two journal papers are produced: one on testing the accuracy of prediction of Wi-Fi choices for users with various preferences (under preparation), and the other one on measuring influence power needed for changing decision makers' choices (under final submission).

Social Referent Nudging For Cookie Acceptance

Researchers at Northumbria have completed the data collection and analysis of results in a study on social referent nudging for the acceptance of cookies, using a web site developed by Northumbria and Newcastle together. Results have been submitted as a journal paper by the Northumbria team.

Error Reporting Study

Researchers at Northumbria have carried out a study evaluating social nudges in the process of error reporting. Data was collected from a set of Mechanical Turk users in three randomised groups: a control group, a group who were nudged to report errors in order to benefit others, and one in which the participants were nudged to benefit themselves. The results are submitted as a conference paper.

Classification of Phishing Emails

A new experiment on nudging users in their identification of phishing emails was designed by Northumbria and Newcastle together. Participants were asked to classify suspicious emails, with and without nudging. The study uses signal detection analysis to identify the sensitivity of users towards correct and incorrect classifications. Three randomised groups were used: a control group, a sender salience nudge and a time salience nudge. The conference paper with results of this work is under preparation.

Security Desert Survival Task

Researchers at Northumbria have commenced work on a study collecting expert knowledge on the process of selecting security countermeasures, considered as analogy of the process of selecting Items for desert survival.

Modelling Influence for Security

The Newcastle team have started summarising their experience of designing and analysing influence into a journal paper with conclusions and findings of the project.

Publications

Jason Crampton, Charles Morisset, Nicola Zannone, On Missing Attributes in Access Control: Non-deterministic and Probabilistic Attribute Retrieval. 20th Symposium on Access Control Models and Technologies (SACMAT), 1-3 June 2015.

Ana Ferreira, Lynne Coventry, and Gabriele Lenzini (2015). What principles of persuasion rule phishing attacks? HCI International, August 2015.

John Mace, Charles Morisset and Aad van Moorsel, Modelling User Availability in Workflow Resiliency Analysis, HotSoS 2015.

Turland J., Coventry L., Jeske D., Briggs P., van Moorsel A. Nudging towards security: Developing an Application for Wireless Network Selection for Android Phones, British HCI 2015, July 13 - 17, 2015, Lincoln, United Kingdom.

Nicholson J., Coventry L., Briggs P., Methods and ethical considerations of persuasive technology in HCI for behaviour change, British HCI 2015, July 13 - 17, 2015, Lincoln, United Kingdom.

Nicholson J., Coventry L., The ethical considerations of persuasive technology/design in usable security, SOUPS 2015.

Blythe, J. M., Coventry, L., & Little, L. (2015). Unpacking security policy compliance: The motivators and barriers of employees' security behaviors. In 11th Symposium on Usable Privacy and Security (SOUPS) USENIX Association.

Dunphy, P., Vlachokyriakos, V., Thieme, A., Nicholson, J., McCarthy, J., & Olivier, P. (2015, July). Social Media as a Resource for Understanding Security Experiences: A Qualitative Analysis of #Password Tweets. In Eleventh Symposium on Usable Privacy and Security (SOUPS 2015). USENIX Association.

John Mace, Charles Morisset and Aad van Moorsel. Impact of Policy Design on Workflow Resiliency Computation Time. QEST 2015 The International Conference on Quantitative Evaluation of SysTems Madrid, Spain at the Universidad Complutense de Madrid, September 1-3, 2015.

John Mace, Charles Morisset and Aad van Moorsel. Resiliency Variance in Workflows with Choice, SERENE 2015: The 7th International Workshop on Software Engineering for Resilient Systems, 7-8th September 2015, Paris.

Basto-Fernandes V., Yevseyeva I., Ruano-Ordas D., Zhao J., Fernandez-Riverola F., Mendez J.R., Emmerich M.T.M. Quadcriteria optimization of binary classifiers: error rates, coverage, and complexity. In Proceedings of the International Conferences EVOLVE - A Bridge between Probability, Set Oriented Numerics, and Evolutionary Computation, July 18-24 (2015), Iasi, Romania, (Springer AISC Series).

Yevseyeva I., Turland J., Morisset C., Coventry L., Gross T., Laing C., van Moorsel A. Addressing consumerisation of IT risks with nudging. International Journal of Information Systems and Project Management. September 2015, vol. 3, N. 3, pp. 5-22, http://www.sciencesphere.org/ijispm/archive/ijispm-0303.pdf.

Yevseyeva I., Basto-Fernandes V., Emmerich M.T.M., van Moorsel A. Selecting optimal subset of security controls. CENTERIS'15, 7th Conference of ENTERprise Information Systems, Procedia Computer Science (vol. 64), Elsevier, 2015, pp. 1035-1042.

Emmerich M.T.M., Deutz A., Yevseyeva I., A Bayesian approach to portfolios selection in multicriteria group decision making. CENTERIS'15, 7th Conference of ENTERprise Information Systems, Procedia Computer Science (vol. 64), Elsevier, 2015, pp. 993-1000.

Briggs, P. and Thomas, L (2015). An Inclusive, Value-Sensitive Design Perspective on Future Identity Technologies. In press ACM Transactions on Computer-Human Interaction (TOCHI), 22 (5).

Dunphy, P., Schöning, J., Nicholson, J., & Olivier, P. (2015, April). Captchat: A Messaging Tool to Frustrate Ubiquitous Surveillance. In Proceedings of the 33rd Annual ACM Conference Extended Abstracts on Human Factors in Computing Systems (pp. 639-646). ACM.

Ferreira, A., Lenzini, G. & Coventry, L. (2015) Principles of Persuasion in Social Engineering and Their Use in Phishing. Human Aspects of Information Security, Privacy, and Trust Third International Conference, HAS 2015. Springer Lecture Notes in Computer Science, 9190, 36-47

Kharrufa, A., Nicholson, J., Dunphy, P., Hodges, S., Briggs, P., & Olivier, P. (2015). Using IMUs to Identify Supervisors on Touch Devices. In Human-Computer Interaction–INTERACT 2015 (pp. 565-583). Springer International Publishing.

Publications Accepted

Yevseyeva I., Morisset C., van Moorsel A. Modeling and Analysis of Influence Power for Information Security Decisions. (Accepted with minor changes to Performance Evaluation journal).

Mallios Y., Bauer L., Kaynar D., Martinelli F., Morisset C. Probabilistic Cost Enforcement of Security Policies. (accepted to Journal of Computer Security)

Related Activities

Pam Briggs was an invited speaker at Identity Management 2014 (IDM2014) – the 10th annual gathering for technology professionals and security specialists in London (Nov 12th, 2014).

Pam Briggs spoke at the 3rd International workshop on identity management organised as part of the EPSRC Network on Identity Management (City University, London, 13-14th Nov, 2014).

Charles Morisset gave talk: Jason Crampton, Charles Morisset, Nicola Zannone, Access Control with Non-deterministic and Probabilistic Attribute Retrieval 3rd Workshop on Hot Issues in Security Principles and Trust, 18 April 2015.

Aad van Moorsel gave talk: Choice Architecture for Information Security: Influencing the Decision-Maker IFIP Working Group 10.4, Jan. 26, 2015, Bristol, UK.

Aad van Moorsel gave talk: Centre for Cyber Crime and Computer Security, NCCU visit, Jan. 14, 2015

Charles Morisset gave talk: John Mace, Charles Morisset and Aad van Moorsel Modelling User Availability in Workflow Resiliency Analysis at 4th International Conference on Principles of Security and Trust London, 16-17 April 2015.

Iryna Yevseyeva gave a tutorial at EVOLVE 2015 - A Bridge between Probability, Set Oriented Numerics, and Evolutionary Computing 18-24.06.2015, Iasi, Romania. http://evolve-conference.org/2015-tutorials on "Multicriteria decision aiding: Compensating and non-compensating methods".

Charles Morisset gave talk at HotSpot 2015 on "Access Control with Non-deterministic and Probabilistic Attribute Retrieval", Jason Crampton, Charles Morisset and Nicola Zannone.

Charles Morisset gave talk at SACMAT 2015 on "On Missing Attributes in Access Control: Non-deterministic and Probabilistic Attribute Retrieval", Jason Crampton, Charles Morisset and Nicola Zannone.

Talk given by John Mace at HotSoS 2015 on joint paper "Modelling user availability in workflow resiliency analysis", John Mace, Charles Morisset and Aad van Moorsel.

Interview for BBC Crimewatch Roadshow by Martin Emms on crime in electronic payments.

Briggs, Coventry and Gross: Completed a review of the future of cybersituational awareness for ESRC/DSTL.

Briggs is a program committee member and attended the IFIP 2015 Conference on Trust Management.

Nicholson, Briggs, Coventry: Organised and ran a workshop on influencing technology in different domains at British HCI 2015 in Lincoln (July)

Nicholson and Coventry: Organised and chaired a Panel discussion on the ethics of persuasive technology in the usable security domain (SOUPS 2015, July, Ottawa Canada) (Lynne also participated in the panel discussion as one of the experts);

Coventry was a program committee member, session chair and attended the International Workshop on Human Aspects of Security, Privacy and Trust

Nicholson and Briggs have submitted a workshop proposal to Chi 2016: Everyday Surveillance

Nicholson will be on the poster jury for SOUPS 2016

Yevseyeva organised and ran a workshop: Multicriteria Decision Making in Enterprise Information Systems workshop in ENTERprise Information Systems. International Conference, CENTERIS 2015, 7 – 9.10.2015, Vilamoura, Portugal.

Pam Briggs gave a seminar talk: St. Andrews SACHI group seminar on Designing for Trust (29th Sept)

Iryna Yevseyeva gave a conference presentation: Yevseyeva I., Morisset C., van Moorsel A. Adaptive soft influence for information security. 23rd International Conference on Multiple Criteria Decision Making MCDM 2015 - Bridging Disciplines, Helmut Schmidt University, University of the Federal Armed Forces Hamburg, Hamburg, Germany, 2-7.08.2015.

Iryna Yevseyeva gave a conference presentation: Yevseyeva I., Basto-Fernandes V., Emmerich M.T.M., van Moorsel A. Selecting optimal subset of security controls. CENTERIS'15, 7th Conference of ENTERprise Information Systems, Vilamoura, Portugal 7-9.10.2015.

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
Department:	Computing Sciences
Organisation:	Newcastle University