RISCS

Research Institute in Science of
Cyber Security

Annual Report 2016

Annual Report

2016

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:

Peter Davies, Thales

Larry Hirst, formerly of IBM

Dario Leslie, MoD

Shari Lawrence Pfleeger, I3P

Martin Sadler, HP

Participating Universities:

Imperial College London

Newcastle University

northumbria UNIVERSITY

Queen Mary University of London

ROYAL HOLLOWAY UNIVERSITY OF LONDON

UCL

This Annual Report and the preceding 2013, 2014 and 2015 Annual Reports may be downloaded from the RISCS web site at

www.riscs.org.uk.

Introduction

As Research Director of the Research Institute in Science of Cyber Security (RISCS), I am proud to present our 4th Annual Report. RISCS started in October 2012, with four projects co-funded by EPSRC, GCHQ and BIS. You can find the final reports on the four original projects on pages 4, 6, 8 and 11, respectively, but I would like to highlight the pioneering work of the *Cyber Security Cartographies project*. Applying a human-centred perspective and design elicitation techniques, the team worked with frontline staff and security experts in the Department of Work and Pensions to identify new forms of secure data sharing needed to support service delivery. In total, RISCS researchers produced 39 publications, and we have founded the Open Access *Journal of Cyber Security*[1], as a leading international publication venue for multidisciplinary, evidence-based research in cyber security. But the mission of RISCS, as with the other RIs, is to engage with the practitioner community – we are trying to understand the challenges they face, and to deliver relevant knowledge in a format they can apply to address those challenges. The new password guidance issued by CESG[2] last year did away with much 'received wisdom' and offered advice that reflects a better understanding of current threats, and that the effort people can expend on security needs to be used to maximum effect. The document has received much attention from the practitioner community – both nationally and internationally. It has empowered many to move beyond existing 'Best Practices' and adopt new policies and technical solutions to deliver effective security that is manageable for individuals and organisations alike.

In April this year, RISCS Phase 2 started. Prof. Lizzie Coles-Kemp from RHUL is now the RISCS Deputy Director. Our immediate aim is to increase our scope in several respects. 1) We are extending the scope from research to improve security decision-making in an enterprise context to effective security for small companies and charities, consumers and citizens. This mirrors the creation of the *National Centre for Cyber Security*, which also has this broader perspective. 2) We are opening the community to both new projects and individual academic members, from a wider range of academic disciplines. The first new project to join is the EPSRC -funded project *Detecting and Preventing Mass-Marketing Fraud*[3], led by Prof. Monica Whitty from Warwick University - among the investigators are the first criminologist and first philosopher to join our community.

We have received funding from EPSRC to continue the coordination activities for a further five years, on the condition that we raise at least £5 Million in research grants over that period. GCHQ has pledged funding of £2.5 Million over that period. Our aim is to raise further project funding via the CyberInvest scheme[4]. These new forms of funding require more flexibility and engagement from the researchers, but also offer access to data and test-beds – which are the lifeblood for evidence-based research. And evidence-based research is the only way to meet the security challenges we face in the years to come.

Professor M. Angela Sasse
Director
Research Institute in Science of Cyber Security (RISCS)

[1]http://cybersecurity.oxfordjournals.org/
[2]https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/458857/Password_guidance_-_simplifying_your_approach.pdf
[3]https://www2.warwick.ac.uk/fac/sci/wmg/research/csc/research/dapm/
[4]https://www.ncsc.gov.uk/articles/cyberinvest-securing-our-future-through-research

Games and Abstraction

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

We have developed new approaches to decision support based on game theory and multi-objective optimisation techniques. 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.

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 enables a precise analysis of these relationships and hence provides a more robust decision support tool than has been hitherto available.

Other distinguishing features of our approach are:

- We model both direct and indirect costs of implementing cyber security decisions.
- We have incorporated several different ways of combining controls into our model.
- We are able to model different types of attacker: passive, i.e. commodity style attacks; reactive attackers; and persistent attackers.
- We consider several different levels of implementation of controls.

We are not aware of any other approach in the literature which takes into account such a variety of features.

Progress in the Year to Date

We have developed a detailed case study which considers an SME like entity and currently involves 37 different attacks and 27 different controls. The dataset is derived from data published by the SANS Institute (for controls) and Mitre (for common vulnerabilities and weaknesses).

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.

We have also developed a second prototype tool which uses Mixed Integer Linear Programming. This prototype has been used to evaluate different methods for combining the effect of controls and also for modelling different types of attackers.

In both cases the tools suggest optimal investment plans given the user budget constraints. In both cases, for sufficient budget, the suggested investments align well with the Cyber Essentials scheme and the SANS Institute top 5 controls.

Collaborative work has continued with the team at UCL to model cyber security decision making for system administrators. Earlier work focused 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 made use of stochastic games for decision making based on non-static attack graphs.

Subsequently, we have been investigating more nuanced advice for SMEs. SMEs do not really constitute a homogenous group; covering a spectrum which ranges from micro-SMEs who might outsource their IT and use cloud services to quite large companies with their own IT and in-house data storage. This work has re-visited the Cyber Essentials scheme to consider modified advice depending where on this spectrum an SME is situated.

Publications

A Fielder, EA Panaousis, P Malacaria, C Hankin and F Smeraldi, 'Decision Support Systems for Cyber Security Investment', Decision Support Systems 86, 13-23, 2016.

MHR Khouzani, P Malacaria, C Hankin, A Fielder, F Smeraldi, 'Efficient Numerical Frameowrks for Multi-objective Cyber Security Planning'. In ESORICS(2), 179-197, 2016.

Related Activities

Hankin co-chaired the Westminster Briefing Cyber Security Summit, June 2016

Hankin gave a keynote at the Law Firms and Cyber Attack Conference, October 2016.

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 information security controls.

Prior to the CySeCa project, little research has, to date, 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 communities within an organisation to protect information. 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.

During the project we have developed a storyboard approach called "Current Experience Comic Strip" which has enabled security practitioners to document and reflect upon how organisational controls are selected and maintained.

We have also developed a participative toolkit that enables security practitioners to engage with different communities within an organisation in order to identify the security practices that communities undertake. This toolkit has been trialled in the context of open government in three separate case study programmes.

Progress in the Year to Date

(CySeCa) finishes its four year programme in December 2016. In its last 18 months, CySeCa has focused on stakeholder engagement working with both the practitioner and academic communities. Case studies have been undertaken within open government as the main focus of the project's practitioner engagement. In the UK the CySeCa storyboard technique has been used in central government (DWP) and in third sector job seeker support organisations in the North East of England. In Australia the storyboard techniques have been deployed in local government in Queensland. As part of academic engagement the CySeCa project has worked along side the EU FP7 TREsPASS project to deliver participative security risk visualisation workshops at the International Association of Societies of Design Research congress in Brisbane in November 2015 and at the TREsPASS' Summer School held at Royal Holloway in June 2016.

Case study programme: In 2015 CySeCa ran a six-month project in the UK with Department for Work and Pensions (DWP) as part of CySeCa's practitioner engagement programme. CySeCa's current experience comic strip techniques were used to storyboard the security challenges experienced by frontline staff at DWP.

The CySeCa storyboard approach enabled the department to see and appreciate the peripheral practices that are fundamental to successful information sharing and protection within that part of open government. The approach also enabled participants to explore how security policies might be re-designed and shortened to improve their effectiveness. As a result of the participative engagements the participants had greater visibility of what other teams did within the welfare delivery workflows and as a result could identify where information might be more effectively shared. A video has been made by DWP that describes the engagement process, the use of the tools and articulates the benefits of the case study programme. Working with the stakeholder community in this way has enabled CySeCa to begin the process of delivering real-world impact within the lifetime of the project.

The CySeCa storyboard techniques have also been used to deliver phishing awareness training within local government in Australia. The CySeCa team worked with the Australian Information Security Association to develop a bespoke Current Experience Comic Strip and associated icon library to be used by a consultant to deliver phishing awareness training to Cessnock Council, New South Wales, Australia. Similar to the work with DWP, this type of engagement enabled participants to identify where security guidance conflicted with their everyday activities and also to share practices that communities of users had developed to respond to the problem of phishing.

Academic engagement: In the last year of the project, CySeCa worked together with EU FP7 project TREsPASS to develop and deliver a series of participative workshops that encourage collaboration across academic disciplines. These collaborations have the goal of developing innovative ways of exploring, understanding and communicating social aspects of information security risk. Between November 2015 and October 2016, CySeCa has worked with design academics, law scholars, academics from geopolitics, computer scientists, mathematicians, socioligists and psychologists.

Publications

Mark Burdon, Jodie Siganto, and Lizzie Coles-Kemp. "The regulatory challenges of Australian information security practice." Computer Law & Security Review (2016).

Jodie Siganto, Mark Burdon and Lizzie Coles-Kemp. “Cyber Security Cartographies (CySeCa) Down Under AISA Report” Australian Information Security Association (2016)

Related Activities: Engagement Activites

November 2015, IASDR Interplay congress, Brisbane Australia

November 2015, Perth Western Australia “Trust in Information Security Conference”, Australian Information Security Association.

June 2016, TREsPASS Summer School, Social Aspects of Cyber Security Risk.

Grant Details

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

Social Referent Nudging For Cookie Acceptance

We 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 accepted as a Frontiers in Psychology journal paper.

Impulsivity and Wireless Network Selection

Researchers at Northumbria have recently had a journal article accepted for Personal and Ubiquitous Computing that explores the security vulnerabilities associated with Bring Your Own Device (BYOD) in general, but looks at the effects of impulsivity on personal device decisions, noting that impulsive people may behave less securely when using personal devices to access wireless networks.

Error Reporting Study

We 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 work has been submitted to the Journal Transactions in Social Computing and is currently under review.

Security Survival Task

Researchers at Northumbria completed work on a study comparing expert perceptions of the importance of security behaviours with end user perceptions. This has resulted in a new process based on the management desert survival task that will let companies explore the difference in perceptions of importance across an organisation and which behaviours may require more focus than others.

Improve the Effectiveness of Pentesting

We undertake a study to determine and improve the effectives of penetration testing, particularly focusing on the relationship between customer and tester. In close collaboration with an international pentesting company we first aim to understand pen testers as well as users. Then we study whether any of our influencing techniques may improve the current situation, for instance through improved reporting or through other means that improve the communication and understanding between tester and customer.

Strengthening passwords through length

The team carried out a study to explore the role of simple instructions when creating a new password. We compared asking

participants to create a “strong” password and a “long” password (as per new guidance). Passwords created under the “long” condition were in fact longer and stronger than in the “strong” condition

Everyday Surveillance

Members of the Northumbria team ran an international workshop on Everyday Surveillance associated with the CHI (Computer-Human Interaction) conference in San Jose earlier this year.

Publications

Yevseyeva I., Morisset C., van Moorsel A. Modeling and analysis of influence power for information security decisions. Performance Evaluation, April 2016, vol. 98, pp. 36-51, doi:10.1016/j.peva.2016.01.003.

Iryna Yevseyeva, Vitor Basto Fernandes, Aad van Moorsel, Helge Janicke, Michael Emmerich, Two-stage Security Controls Selection, Procedia Computer Science, Volume 100, 2016, Pages 971-978, ISSN 1877-0509, http://dx.doi.org/10.1016/j.procs.2016.09.261.

Personality and Social Framing in Privacy Decision-Making: A Study on Cookie Acceptance, Front Psychol. 2016; 7: 1341. Lynne M. Coventry, Debora Jeske, John M. Blythe, James Turland, and Pam Briggs

Jeske, Debora, Briggs, Pam and Coventry, Lynne (2016) Exploring the relationship between impulsivity and decision-making on mobile devices. Personal and Ubiquitous Computing, 20 (4). pp. 545-557.

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.

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 (2014,2015,2016)

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

Nicholson was on the poster jury for SOUPS 2016 and Coventry and Nicholson were paper reviewers.

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.

Lynne Coventry gave a general public talk on cybersecurity and older adults at Lancaster Town Hall.

Briggs, Coventry, have submitted a grant to the EPSRC Human Dimensions of Cybersecurity with Joinson and Ashenden. Through to final panel.

Coventry and Briggs have both submitted cybersecurity grants to Nordforske

Iryna Yevseyeva gave a conference presentation: Yevseyeva I., Basto-Fernandes V., van Moorsel A., Janicke H., Emmerich M.T.M., Two-stage security controls selection. CENTERIS’16, 8th Conference of ENTERprise Information Systems, Porto, Portugal 5-7.10.2016.

Yevseyeva organised and ran a workshop: Multicriteria Decision Making in Enterprise Information Systems workshop in ENTERprise Information Systems. International Conference, CENTERIS 2015, 5 – 7.10.2016, Porto, Portugal.

Iryna Yevseyeva gave a conference presentation: Yevseyeva I., Basto-Fernandes V., van Moorsel A., Janicke H., Emmerich M.T.M., Two-stage security controls selection. CENTERIS’16, 8th Conference of ENTERprise Information Systems, Porto, Portugal 5-7.10.2016.

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

Productive Security

The aim of the Productive Security project – led by Profs Angela Sasse and David Pym at UCL – was to help organisations achieve effective risk mitigation and enhanced productivity. To do this, we carried out a series of empirical studies in organisations to collect data, and developed tools to model the risk mitigation specific tools can achieve, as well as the impact of those measures on individual and organisational productivity.

The data we collected in 2 large organisations provided evidence that security policies and controls were not effective because employees either can't, or won't, comply. Too often, they are left to make choices between complying with security, and getting their work done. They overwhelmingly choose the latter – often with tacit encouragement by management. 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). The workarounds employees chose are not generally reckless – they deploy their own security measures (shadow security) to manage risks they understand – but they often do not aware of all threats. When employees are compliant, productivity can suffer because they reorganise their primary tasks, to minimise the exposure to security mechanisms that are too onerous.

We want to improve decision-making through tools that 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, science-based 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.

Progress in the Year to Date

User-centred security awareness

Security awareness is currently seen as the measure of choice to persuade employees to care more about security and comply with security policies. We found that current efforts in the organisations we studied were not targeted, and not designed in way that supports behaviour change. Our collaboration with security awareness experts at Hewlett Packard Enterprise (HPE) confirmed that many companies are wasting employee time and goodwill that this is a wider problem. This collaboration led to a Business White Paper "Awareness is only the first step: A framework for progressive engagement of staff in cyber security" [2][1] which explains why behaviour change is not a cheap option, and can't be achieved by communication about security risks. (CESG staff observed the process and endorsed the White Paper.) The white paper sets out a framework for engaging employees, and to empower them to become the strongest link—rather than a vulnerability. We have since joined forces with researchers from the Chaise project, to work with the UK government website Cyber StreetWise to develop effective security awareness for individuals and small companies.

[1]http://www.riscs.org.uk/wp-content/uploads/2015/12/Awareness-is-Only-the-First-Step.pdf

Evaluating security solutions

Productive Security researchers Kat Krol, Simon Parkin and Angela Sasse conducted a study to test the usability and user acceptance of a set of commercial human verification solutions – traditional CAPTCHAs, gamified CAPTCHAs and a novel face biometric solution. These mechanisms are often used on ticket-purchase websites and forums – a user study with 87 participants explored issues of effort and comprehension around these controls. The paper on the results [7] won a Special Contribution Award at the IEEE ISBA conference.This work also contributed to the definition of five study design principles for security and privacy usability research in a lab-based environment, including evaluation of security technologies around a realistic primary task (ticket purchasing), which was presented at the LASER workshop this year [9].

Usable security and the development process

Productive Security researchers analysed a corpus of 21 interviews with developers, security and usability experts in three US organisations that claimed to develop usable security solutions. The results are being published in [3]. We applied Sentiment Analysis to the Grounded Theory coded data to focus statistical analysis to areas of strongly represented sentiment between the different experts. The analysis found that developers have negative perceptions of usability, and that the absence of metrics for usability and security enables the rhetoric of a usability-security trade-off [8]. That trade-off becomes a shortcut to discounting usability – since security is important, it has to 'come first'. These insights lead to new research – being undertaken as part of RISCS Phase 2 - on how to change software engineering tools and processes.

Systems modelling and decision support

Productive Security researchers Tristan Caulfield and Simon Parkin applied systems modeling techniques to assess a planned physical security intervention at a specific site in one of our partner companies. The model was used to explore the potential individual cost of security for employees when replacing a secure door with a turnstile. We worked with managers at the site as part of preference elicitation to identify meaningful model parameters. Direct observation of employee entry behaviours captured data to situate the model.

The researchers continue to work with a large partner institution in the Higher Education sector. A study of the institution's helpdesk password reset data has been completed, including analysis of monthly password reset events over a period of 30 months, and coding and analysis of interviews with a set of 20 system end-users. This identified potential improvements to the end-user experience of self-service support for users and their passwords [4].

Security for Small and Medium Enterprises (SMEs)

The principles of the Productive Security engagements with large organisations are

being applied to explore compliance factors for employees in smaller organisations. This includes collaboration between Simon Parkin, Andrew Fielder (Imperial College), and partner IT service providers, to model the collective investment of effort and skills in managing security within diverse SME IT environments [1]. Basic controls and variants have been modelled, based upon the Cyber Essentials scheme.

Publications

Tristan Caulfield and Andrew Fielder. Optimising time allocation for network defence. Journal of Cybersecurity, Nov 2015, pp 37-51.

Marcus Beyer, Sarah Ahmed, Katja Doerlemann, Simon Arnell, Simon Parkin, M. Angela Sasse, M.A., and Neil Passingham. Awareness is only the first step: A framework for progressive engagement of staff in cyber security. Business White Paper, Hewlett Packard Enterprise, 2015. http://www.riscs.org.uk/wp-content/uploads/2015/12/Awareness-is-Only-the-First-Step.pdf

Deanna Caputo, Shari Lawrence Pfleeger, M Angela Sasse, Paul Ammon, Jeff Offut, and Lin Deng: Barriers to Usable Security? Three Organizational Case Studies. To appear in IEEE Security & Privacy Magazine, September/October 2016.

Simon Parkin, Samy Driss, Kat Krol, and M. Angela Sasse, Assessing the User Experience of Password Reset Policies in a University. In: Proceedings of the 9th International Conference on Passwords, Cambridge, UK, 2015. Technology and Practice of Passwords (Volume 9551 of the series Lecture Notes in Computer Science), pp 21-38, Springer

Tristan Caulfield, David Pym, and Christos Ioannidis. "Discrete choice, social interaction, and policy in encryption technology adoption" [short paper]. In Financial Cryptography and Data Security 2016. February 22-26 2016, Barbados

Kat Krol, Simon Parkin, and M. Angela Sasse. "Better the Devil You Know: A User Study of Two CAPTCHAs and a Possible Replacement Technology". In: Workshop on Usable Security (USEC) '16, 2016.

Kat Krol, Muhammad Sajidur Rahman, Simon Parkin, Emiliano De Cristofaro, and Eugene Y Vasserman. "An Exploratory Study of User Perceptions of Payment Methods in the UK and the US". In: Workshop on Usable Security (USEC) '16, 2016.

Kat Krol, Simon Parkin, M. Angela Sasse, "I don't like putting my face on the Internet!": An acceptance study of face biometrics as a CAPTCHA replacement. In: Proceedings of The IEEE International Conference on Identity, Security and Behavior Analysis (ISBA 2016), Sendai, Japan, 2016. IEEE

Ingolf Becker, Simon Parkin, and M. Angela Sasse. "Combining Qualitative Coding and Sentiment Analysis: Deconstructing Perceptions of Usable Security in Organisations". In: The LASER Workshop: Learning from Authoritative Security Experiment Results. IEEE, 2016.

Kat Krol, Jonathan M Spring, Simon Parkin, and M. Angela Sasse. "Towards robust experimental design for user studies in security and privacy". In: The LASER Workshop: Learning from Authoritative Security Experiment Results. IEEE, 2016.

Simon Parkin, Kat Krol, Ingolf Becker, and M. Angela Sasse. "Applying Cognitive Control Modes to Identify Security Fatigue Hotspots". In: Workshop on Security Fatigue, Denver, Colorado, USENIX, 2016.

Adam Beautement, Ingolf Becker, Simon Parkin, Kat Krol, and M. Angela Sasse. "Productive Security: A scalable methodology for analysing employee security behaviours". In: Twelfth Symposium on Usable Security and Privacy (SOUPS), Denver, Colorado, USENIX, 2016.

Tristan Caulfield, Michelle Baddeley, and David Pym. "Social learning in systems security modelling". In Social Simulation Conference 2016. Rome, Italy, September 19-23, 2016

Related Activities

Invited Talk: MA Sasse, 5th October 2015: "Cybersecurity Challenges facing Society", Science and Technology in Society Forum (STS), Kyoto.

Invited Talk: MA Sasse, 13th October 2015: "Are our lives safe online?" Keynote, Biometrics 2015, London.

Invited Talk: MA Sasse, 4th November 2015: "Cyber Security and the Human-Technology Interface", Vodafone Technical Excellence Programme, Imperial College London

Panel Member: MA Sasse, 9th November 2015: "The Skills Balance", IA 15: Secure Digital Transformation, London.

Invited Talk: MA Sasse, 12th November 2015: "Citizen and Civic Engagement (including Privacy and Trust)", Arup Smart Cities Event, Imperial College London.

Invited Talk: MA Sasse, 18th November 2015: "The Human Factor: Designing Employee Centred Policies Which Will Maximise Secure Behaviour", CSCA summit, London

Invited Talk: MA Sasse, 1st December 2015: "Cybersecurity: Mind the gap, or it will divide and conquer us." How To Change the World Academy Conference, Royal Institution, London.

Panel Member, MA Sasse, 1st December 2015: "Can you protect your digital reputation and brand?", High Level Fireside Briefing, European Association for e-Identity & Security (EEMA), London

Co-organiser: D Pym, 3rd December 2015: "Data Protection and Security at Scale", one-day workshop, Alan Turing Institute, London

Keynote: MA Sasse, 8th December 2015: "Users hate passwords - so are they on their way out?", Passwords15, Cambridge

Invited Talk, MA Sasse, 17th December 2015: "Frontiers in Digital Health: Mind the Gap - 'Big Data' and understanding behavioural change", Institute of Digital Health, UCL

Panel Member: MA Sasse, 28th January 2016: "Technologies for Border Control and Beyond: How to Integrate Privacy and Data Collection", Computers, Privacy & Data Protection Conference, Belgium

Panel Member: MA Sasse: 2nd March 2016: "Identity, Security and Behaviour Analysis: Where Will We be in 10 Years?", IEEE International Conference on Identity, Security and Behavior Analysis, Sendai, Japan

Invited Talk: MA Sasse, 10th March 2016: Compliance: Art or Science? Breakfast Briefing, Blue Goose (RIBA), London

Distinguished Lecture: MA Sasse, 14th March 2016: "'Smile to pay'? You must be joking", University of British Columbia, Vancouver

Panel Member: MA Sasse, 16th March 2016: "Building Business Defenses for the New Battlefield", FT Cyber Security Summit USA

Invited Talk: MA Sasse and O Beris, 27th April 2016: "Influencing security behaviour:

improving risk understanding is not enough", IA Technical 2016, Cheltenham

Invited Talk: MA Sasse, 6th May 2016: "Cyber Security – Beyond Compliance", BTO Cyber Security Event, London

Quoted Expert: MA Sasse: 11th May 2016: “How to hack the hackers: The human side of cybercrime”, Nature Magazine, 533, 164–167 (12 May 2016)

Invited Talk: MA Sasse, 25th May 2016: “Who wears the gloves? Owning the security hot potato”, Cyber UK in Practice, Liverpool

Invited Talk: MA Sasse, 25th May 2016: “Mind the many skills gaps: why we keep creating unworkable security”, Karen Spärck Jones lecture, British Computing Society (BCS), London

Invited Talk: MA Sasse, 31st May 2016: "Influencing security behaviour: improving risk understanding Is not enough", Security and Human Behavior (SHB), Harvard University

Panel Member: MA Sasse, 7th June 2016: “Securing the Connected Human: Winning Hearts and Minds to Drive Secure Behaviour”, Infosecurity Europe 2016, London

Invited Talk: MA Sasse, 9th June 2016: "The Research Institute in Science of Cyber Security", BT Insights, Imperial College

Invited Talk: MA Sasse, 21st June 2016: “Lessons from the Security Awareness Trainwreck”, ESRC Behaviour Change Seminar: Changing Behaviour Around Online Security and Privacy, London

Invited Talk: MA Sasse, 29th June 2016: “Do you care if Johnny can encrypt?”. Cryptovision Mindshare

Keynote: MA Sasse, 15th July 2016: “Busting the Usability-Security Tradeoff Myth”, British HCI2016, Bournemouth

Keynote: MA Sasse, 20th July 2016: “Goodbye passwords hello biometrics keynote”, Privacy Enhancing Technologies Symposium (PETS), Darmstadt

Invited Talk: MA Sasse, 26th July 2016: “Is there such a thing as a secure society? Security, resilience and societal values”, EuroScience Open Forum (ESOF), Manchester

Invited Talk: MA Sasse, 25th August 2016: “Privacy of Personal Health Data”, 11th International IFIP Summer School on Privacy and Identity Management, Karlstad, Sweden

Invited Talk: MA Sasse, 6th September: "Smart Cities, Future Homes", Data Protection Forum, 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

DAPM: Detecting and Preventing Mass-marketing Fraud

The Internet has opened up the floodgates to mass marketing fraud (MMF) given that criminals can use it to target many more potential victims with very limited marginal effort, to trick them into making electronic and even crypto-currency transfers for a mistaken charity, investment or love. This crime can also have an impact on the digital economy, as citizens start to mistrust particular online sites that criminals use to target individuals (e.g., dating sites, social networking sites, trading sites).

MMF is a serious, complex and (in the flexible definition used by the Home Office) organised crime. Examples include: foreign lotteries and sweepstakes (in which the victim believes they have won money from a lottery and are told to pay a fee in order to release the funds), '419' scams (advance fee fraud, in which victims believe that for a small amount of money they will make a large fortune), and romance scams (taken in by a fake online dating persona, in which the victim sends the 'fake persona' money). Some MMFs are low-value one off scams on large numbers of victims, whilst others involve developing a relationship (e.g., romantic, business, friendship) where money is defrauded over time, again with multiple simultaneous or sequential victims.

DAPM is an EPSRC funded project that will develop novel techniques to detect and prevent 'online' MMF. The project will establish new foundations for (a) detecting assumed identities and persuasive messaging used by fraudsters and (b) delivering much needed insights into the psychological and technical factors that lead to poor decision-making on the part of existing and prospective victims of such frauds.

The research team includes a psychologist (University of Warwick, WMG), computer scientists (University of Lancaster, UCL), a Human Computer Interaction expert (UCL), a criminologist (Cardiff University) and a philosopher (University of Warwick). We anticipate developing and evaluating multiple 'ethical' solutions to prevention and detection – including offline and cyber techniques and methods. Through its multi-disciplinary approach and close focus on co-designing the solutions with its project partners and testing them in-the-wild during live MMF-detection settings, the project will generate not only new scientific understanding of the anatomy of MMF but also tools and techniques that can form the basis of practical interventions in tackling MMF.

The project will draw from partners' support to help create and test techniques, 'in the wild', developed by the researchers. Partners include: ACCC (Australian Competition and Consumer Commission), Barclays, CIFAS, City of London Police, Federal Trade Commission, Fraud Help Desk (Netherlands), Fraud Women's Network, Hampshire County Council, My Mate Your Date, Royal Canadian Mounted Police, Scamalytics and Western Australian Police.

The overall objective of DAPM is to work with our partners to develop ethical (respecting privacy where appropriate) and usable methods that demonstrably detect and prevent online MMFs. In order to achieve this objective the work here aims to:

- Map out the clusters of different types of scams, based on psychological, sociological, situational and technical variables - i.e., to enable better design MMF reduction and criminal justice pursuit.
- Research the anatomy of MMF by examining psychological, sociological and technical variables and examining whether this differs for different types of MMFs.
- Research the kinds of personal identity and data that users find acceptable in the development of methods to detect and prevent MMF.
- Examine the variables that distinguish those who have become single or repeat victims from non-victims (including psychological, sociological and technical variables).
- Examine the variables that distinguish a criminal from a non-criminal (examining psychological, sociological and technical variables).
- Based on the above findings to develop new methods to detect and prevent mass-marketing fraud.
- Conduct an evaluation of methods that 'work' and do not 'work' to detect and prevent mass-marketing fraud.
- Inform and disseminate widely our findings, providing a clear account of the actions that could be taken by various organisations to detect and prevent MMF. This includes ensuring our findings are taken up to help develop public policy (e.g., the work here might be used to advise industry on how to better protect themselves from scammers, guidelines set up by regulation bodies, law enforcement practices etc.).
- To ensure breadth of usage we will disseminate our findings using multiple methods, communicate to different types of general public, business and public sector audiences in the application to more broad areas such as cybersecurity, crime prevention, deception and persuasion).

Updates of our latest findings can be found on our webpage: http://www2.warwick.ac.uk/fac/sci/wmg/research/csc/research/dapm/

Presentations

Rashid, A. (September, 2016). Your words betray you: The role of language in cybercrime investigations. *Keynote at 1st International Workshop on Requirements Engineering for Investigating and Countering Crime, September 12, 2016, Beijing, China.*

Whitty, M. (September, 2016). Tackling MMF from a Multi-Disciplinary Approach. *Invited talk for Silence of the scams: Progress, practice and prevention conference. Brunel, University 29th September, 2016, UK.*

Everyday Safety-Security for Everyday Services: A fellowship about information security and everyday life

RISCS' CySeCa project has examined the intersection between societal security and digital security from the perspective of developing practical tools that security practitioners can use to understand how digital security techniques such as passwords and file permissions affect how employees perceive their own safety and security. However, there is still a considerable amount to be understood about this intersection and about how we can better design digital security to more effectively support societal security.

The importance of understanding this intersection within open government can be seen in this statement: "Cyber security is the biggest challenge for Universal Credit" David Freud, Welfare Reform Minister (Computer Weekly 2012).

Freud made this strong statement to a Commons Select Committee in 2012 and it is interesting that he singled out cyber security as the biggest challenge when there are so many challenges related to the delivery of services to communities that are often marginalised and underserved. In his speech, Freud highlighted the tension between two aims: protecting Universal Credit (reformed welfare) services from fraud; and being able to pay people the right amount on time. He places in sharp focus the tension between protecting a service and protecting people. The implications of fraud for the public purse is significant and at the same time any delay of payment to some of society's most vulnerable can have a catastrophic effect on the individual and their families. The latter can also trigger significant costs for local social and community services. The safety and security of an individual lies in the continuation of payment; the fear of cessation of payments can result in the fraudulent behaviour that concerns David Freud. The everyday safety and security of people is therefore entwined with the secure provision of services used by people on an everyday basis. It is cyber security in the form of service design that allows the secure, reliable and cost-effective delivery of these services to the right people, but it is everyday safety and security that enables people to take advantage of these services.

For the next five years RISCS will be home to a research fellowship programme led by Lizzie Coles-Kemp at Royal Holloway University of London. It examines the tension between protecting people and protecting digital services within the context of open government. The fellowship's start point examines the concept of "ontological security," a term used to describe the ability of an individual to go about their everyday activities with confidence and trust in the world around them. Much of ontological security is derived from the relationships within the kinship and friendship networks that people build and maintain and plays an important part in the development and maintenance of societal security.

There are many touch points between ontological security and digital service protection. The fellowship terms this intersection "everyday security" to highlight the space where relational and digital forms of security are enmeshed. For example, research shows that grandmothers are, in some families, an important source of stability, often acting as a safety valve when relationships between mothers and daughters become too tense. In some families, grandmothers bond with their granddaughters through shared experiences in social media. Grandmothers may not directly interact with social media but often sit and watch their granddaughters' social media activity, exchanging views with granddaughters on what is being shared or taking part in on-line games such as Candy Crush. This relational engagement touches on areas of trust, personal information sharing and privacy. The grandmother is an active non-user, the sharing of social media is a part of building and maintaining of everyday security, not only for the granddaughter but also for the grandmother and the wider family. With an understanding of this relationship, internet safety support and know-how can be targeted, not only to the granddaughter but, also to the grandmother. In particular, grandmothers can be supported to help granddaughters make personal information sharing decisions and negotiate conflicts that emerge during social media use. This relational dimension to managing service security is key. This understanding enables targeted interventions and, at the same time, opens up new areas of digital innovation and technology design, for example: interactive information sharing maps to visualise how personal information moves across a kin and friendship network.

A further example of everyday security can be seen in the use of passwords to regulate access to digital services. Whilst much focus in internet safety research and guidance is on the one user-one password security mechanism, research shows that in reality many communities of public service users rely on informal social proxies within the kin and friendship network that carries out the registration, maintenance as well as login for a service. Members of the kin and friendship network proxy for the intended user and are an important means of helping an individual secure their everyday by supporting the procurement of household income, managing health conditions and retaining housing. All of these activities are fundamental to creating and maintaining a stable and secure day-to-day environment that enables an individual to be free to focus on needs and wants. In this reality, the digital service security question is not one of secure passwords but one of enabling the individual to manage their social proxy and to be able to detect if that social proxy begins to work against their interests rather than for them.

This fellowship programme seeks to develop a clear understanding of the everyday resulting in service designs that respond to the complexities of entwined relational and digital securities. Without this understanding, open government initiatives will struggle to provide the safe environment necessary to create confident citizens able to take advantage of the empowering spaces that reimagined government services seek to provide.

Grant Details

EPSRC Reference:: EP/N02561X/1

Project: EPSRC Fellowship ESSfES: Everyday Safety Security for Everyday Services

Researchers: Lizzie Coles-Kemp and Claude Heath