RISCS

Research Institute in Science of Cyber Security

Annual Report 2013

RISCS

Research Institute in Science of
Cyber Security

Annual Report
2013

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

Duncan Hart, Bank of England

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

UNIVERSITY OF ABERDEEN

UCL

Introduction

Welcome to the first Annual Report of the Research Institute in Science of Cyber Security (RISCS). RISCS is the first of a group of Research Institutes funded by EPSRC, GHCQ and BIS as part of the UK Government's National Cyber Security strategy* published in 2011. It is a virtual organization, consisting of four multidisciplinary projects funded for 3.5 years, in which researchers from seven UK universities participate. The common goal of those projects is "what it says on the tin" of the RI: to conduct empirical, evidence-based research that will create a scientific basis for cyber security.

To date, information security practitioners have been guided by rules and mechanisms that have evolved as part of a "Best Practice" based approach. Whilst this approach may manage the risks that organisations face today, in the absence of repeatable measurements and benchmarks, it is not possible for them to answer the simple question "How secure is my organisation?" They do not know how much the addition of a new security measure has improved security, whether another measure might have achieved better risk mitigation, or the same mitigation at lower cost. RISCS researchers are working to provide models of organisations and the threats they face, and measurement techniques and benchmarks, together with tools that will help private and public sector organisations to make better security decisions.

The first year of the Research Institute in Science of Cyber Security has been a busy one. We have created a collaboration infrastructure that supports accumulation and integration of our findings, and communication to the research and practitioner communities. All researchers involved meet four times a year to exchange ideas, report results, and develop measurements and toolkits. These quarterly meetings give the researchers the opportunity to benefit from the experience of the leading industry representatives and international researchers on our Advisory Board. The RISCS Advisory Board members have provided most valuable guidance on key cyber security challenges, feedback on results, and guidance how to present these to the wider community.

Several of our researchers have been deeply embedded in private and public sector organisations to collect data and test their ideas, and this has enabled us to test and progress the research presented in our Annual Report. We look forward to broadening this engagement over the remaining years of the Research Institute.

In the following pages, you will find an overview of the each of our four projects, their goals and our progress towards them during this first year of the Research Institute in Science of Cyber Security.

Professor M. Angela Sasse

Director

Research Institute in Science of Cyber Security

* Available at www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf

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 to Date

Nash Equilibrium and Strong Stackelberg Games

We have developed a model of a stochastic non-cooperative game between a network administrator who needs to defend the network entities (such as routers, clients, and servers) against external or insider adversaries which are modelled as an omni-present attacker. Network entities run various protocols whilst attackers are attempting to compromise these entities by launching attacks against them. Although the administrator has knowledge of the different attacks (strategies) and the outcomes (payoffs), he is not always aware of the actions taken by the adversary. We have developed a java-based game theoretic simulator which derives the Nash Equilibrium (NE) of this "imperfect information" game, using evolutionary game theoretic algorithms. Assuming that network resources are limited and there is always a cost for defending, such NE can provide network administrators with "optimal" defending strategies.

Fielder, Hankin, Malacaria, Panaousis, and Smeraldi have worked on Stackelberg games for cyber-security. By using Stackelberg games we plan to provide an optimal task scheduling for systems administrators, e.g. how many hours in a week to allocate for protecting different possible targets. With the help of expert system administrators we have built a stochastic cyber-security graph modelling possible attack scenarios, concentrating on a cyber-thief attacking an SME.

Malacaria and Smeraldi have investigated Stackelberg games in terms of Information Theory and defined two iterative algorithms for Strong Stackelberg Solutions based on Kullback-Leiber divergence. One is equivalent to a minimax solution; the second is a more realistic constrained solution which takes into account different costs involved in protecting different targets.

We have validated the Nash Equilibria and Strong Stackelberg Solutions by comparing their performance with non game theoretical task scheduling. Subsequently, we have worked on correctness proofs for our approach and have successfully proven that the minimax and Nash strategies are equivalent for the non-zero sum games that we have been studying.

Malacaria has worked on implementing several game theoretical solutions; he has implemented the algorithms devised together with Smeraldi and more recently has implemented a solver generating all Nash Equilibria (pure and mixed) for normal form games.

The Urban Prototyping London Crackathon

Gurguc organised the "Crackathon", a live cyber security exercise, as part of the UP London festival. This event helped us examine whether existing and emerging systems exhibit the desired level of security, and identify key research challenges to generate trust and long-term sustainability of ICT within urban areas.

Monoidal Computer Model

Pavlovic worked towards bridging the gap between game theory and computibility and formalized the notion of learning equilibrium, modifying the notion of Nash equilibrium to the framework where the players are computers. This extends several strands of existing work from A. Rubinstein's theory of bounded rationality, to Halpern and Pass, where the players are Turing machines computing Nash Equilibria.

Publications

Trajce Dimkov, D.Pavlovic, and Woter Pieters, Security policy alignment: A formal approach. IEEE Systems Journal 7/2 (2013) 275-287

Catherine Meadows and D.Pavlovic, Formalizing Physical Security Properties. In: Security and Trust Management, STM 2012, Lecture Notes in Computer Science vol 7783 (Springer Verlag 2013) 193-208

Chris Hankin and Pasquale Malacaria, Payoffs, Intensionality and Abstraction in Games. In: Computation, Logic, Games and Quantum Foundations. The Many Facets of Samson Abramsky, Lecture Notes in Computer Science vol 7860 (Springer Verlag 2013) 69-82

Related Activities

- Gurguc organised the Crackathon event, which took place in mid-April.
- Hankin gave a talk on the Science of Cyber Security to the London Section of the Institute of Measurement and Control on 8th April 2013.
- Pavlovic presented talks at ACCAT (Rome, March 26 2013), C3E Workshop (Washington DC, April 29, 2013)
- Hankin and Pavlovic gave presentations at the Abramsky Festschrift (Oxford, May 2013)
- Pavlovic presented a course and seminar in Economics and Security
- Visits by Viktor Winschel (Dept of Economics, University of Mannheim), Whitfield Diffie and Catherine Meadows to RHUL.
- Hankin participated as a member of the Technical Advisory Group for the selection of a Government preferred organisational standard for cyber security.
- Papers under submission:
  - Chasing Diagrams in Cryptography
  - Optimal Allocation of Limited Resources for Cyber Security Best Practises
  - Smooth Coalgebra: Testing Vector Analysis (with Bertfried Fauser)

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:	Pavlovic, Professor DD
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 to Date

Human-centred Research

Interviews with security practitioners have been conducted and thematically analysed, followed by a verification study to validate this analysis. Segmentation of the practitioner community has been undertaken using organisation-type, age and gender.

Literature surveys of the use of personas in design and the use of visual narratives in design have been conducted and synthesised with the fieldwork to develop novel methods in persona development.

Initial social analysis has explored the type and quality of the links between the practitioners and other parts of an organisation, communication methods and spheres of influence.

The human-centred researchers have explored methods of visualising data and results, and a novel method has been developed that uses visual narratives in the form of cartoons to ground the design of user personas. Using this method, nine information security practitioner personas have been created. These are grounded in the qualitative research that has been undertaken and represent a nuanced analysis of the different professional characteristics that can be found in the field of information security practice. Much progress has also been made to turn the visual narrative method into a toolkit that practitioners can use. An early prototype of the toolkit will be available for demonstration at the RI First Annual Conference.

Data-centred Research

The project has had a strong focus on literature review and establishment of the state of the art.

An initial data visualisation scheme, a framework for gathering and analysing data and a rudimentary visualisation prototype have been developed. Features for identifying asset behaviour have also been explored and an initial approach defined.

The visualisation prototype uses dynamic coloured graphs to represent data, rendered using Gephi software. This prototype has been tested against an anonymous dataset provided by university of Brescia.

Ethics questions have had to be addressed, related to potential unintended consequences for research participants from network monitoring, and we have undertaken an analysis of potential risks to participants from their employer organisations. We have developed a draft document detailing ethics practices involved in the data collection, maintenance and analysis processes.

Synthesised work

The next stage of the project will explore how to synthesise the data network and the social network analysis.

External Review Panel

A panel formed from organisations that participated in the first year of the project acts as the external review panel for the remainder of the project.

Related Activities

- Talks have been given at: AUSCERT 2013, the I4 Conference in June, in an I4 webinar and at Econique's Information Security and Risk Management Dialogue Conference.
- A poster was presented at a summer school titled "Building Trust in the Information Age" in Cagliari (Italy) in September and also later at ESORICS.
- A paper on the novel visual narrative method is currently under review.

Grant Details

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

Choice Architecture for Information Security (ChAISe)

The motivation for researching choice architecture stems from previous research using model-based approaches to optimise decisions. We found that business leaders (including Chief Information Security Officers, CISOs) do not tend to change their decisions, but seek data to confirm a decision already taken. We concluded that decision making tools need to be designed to defeat such confirmation bias and 'nudge' decision makers to beneficial decisions. This relates to choice architecture. ChAISe will design a choice architecture specific for information security.

Rigorous approaches may introduce a false sense of security to decision-makers by not fully disclosing assumptions (e.g., a model may assume a restricted attack scenario); ignores Buffett's mantra that it is better to be approximately right than precisely wrong; and ignores the fact that decision makers tend to ignore the information they receive through rigorous assessment, unless it validates the decision they already intended to make.

To address these issues 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 will exploit to provide sufficient rigour underlying the choice architecture. In particular, the project will establish 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 will work with large organisations and SMEs through well-established channels. It will demonstrate the benefits of the advocated choice architecture through a case study in an SME.

Progress to Date

Risk Framework

We created a risk framework for SME's identifying assets, threats, vulnerabilities and risks, developing generalised matrices of potential threats for corporate data; potential per device threats and vulnerabilities from corporate use of BYOD; human vulnerabilities that might be exploited in security breaches.

Scenario Development

We have developed ten scenarios for demonstrating and working out potential security threats with 'BYOD'. We have analysed these scenarios with the risk framework.

Understanding security behaviours: Interviews

We have conducted a series of interviews with people who use mobile devices for their work, examining their behaviour and perception of risks and the security decisions they make.

Understanding security behaviours: Literature

This review of user behaviours and security risks promoted by security awareness web sites helped us to identify the first problem for a choice architecture intervention – the use of unsecured public Wi-Fi.

MINDSPACE Brainstorm

We have used the behavioural influencers identified in the MINDSPACE project to generate ideas for "nudges", to nudge people towards the selecting the most secure, and trusted Wi-Fi provider. We then evaluated the ideas and prioritised those to explore in a prototype.

Decision Making

We developed a utility-based model for decision making behind the order of the available WiFis based on preferences of the Chief Information Security Officer.

Secure WiFi Connection - Mobile Application

A prototype of a mobile phone app has been developed to address WiFi selection behaviour, incorporating some nudges and the decision making model. We are now in the planning phase to evaluate if the nudged version affects WiFi selection decisions using a student sample.

Publications

Yevseyeva I. Gross T. van Moorsel A., "Nudging towards security in BYOD (bring your own device)". Abstract in First Annual Cyberpsychology Conference, Leicester, UK, September 19, 2013.

Coventry, L. "Influencers of security behaviour" presented at the SASIG group meeting on Human Factors of Security September 2013.

van Moorsel hosted a meeting with Metropolitan Police representatives who visited CCCS/ Newcastle University on the 30th of August.

Grant Details

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

Productive Security – improving security compliance and productivity through measurement

The Productive Security project is a collaboration between University College London (UCL) and University of Aberdeen. Researchers from the Information Security Research Group of Professor Angela Sasse within UCL's Computer Science department will be partnering with a team led by Professor David Pym within University of Aberdeen's Department of Computing Science.

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

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

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

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

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

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

Productive Security is about:

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

Progress to Date

Work with Industrial Partner A (Critical National Infrastructure)

Previous collaboration resulted in a detailed study of human-facing security concerns, which subsequently informed a series of targeted security campaigns.

UCL researchers have analysed the induction process for new employees to understand how security and organisation goals are communicated to new starters. Working with the company's UK Risk Manager and Security Policy Manager, findings have been related to an analysis of the organisation's security policy.

Two studies are in the planning stage; one to identify and characterise new employees' experience of interacting with internal security communications, and the other to facilitate direct instrumentation within the organisation to measure the effectiveness of a specific security mechanism. Both studies will be conducted with a view to identifying specific interventions to improve both security and the security experience of users, with the effectiveness of these interventions being measured.

Researchers at Aberdeen University have developed a model of "tailgating" behaviour based on survey responses previously collected at the organisation.

Work with Industrial Partner B (Telecoms)

Members of the research group at UCL have conducted 86 interviews with staff from a number of sites in the operations division. They also made field visits to retail stores and call centre facilities, observing security-related activity and engaging with staff to understand issues around security. This information was used to identify pertinent security issues.

Findings formed the basis for development of scenarios representative of security-related issues within the organisation, which were incorporated into tailored survey tools, which have been used in an organisation-wide survey, covering employees in operations, retail stores and call centres. Results of analysis have been reported to the company's Security & Fraud Manager, and subsequently to Board members, to be followed with further collaboration to improve security culture based upon these results.

Work with Industrial Partner C (Security Technology Services)

Productive Security researchers have been actively advising on material relating to human factors, to be disseminated internally to the organisation and potentially to clients. Articles are actively being developed jointly to improve awareness of human factors in information security both internally and with existing and potential clients.

Work with Industrial Partner D (Higher Education)

We have identified "hotspots" within the organisation's information security programme where Productive Security principles and related expertise can support effective security management activity and interventions. These included security awareness material and reviewing the organisation's security policy. As a result of this work, the Partner will be making changes to their security policy.

Productive Security researchers have been directly involved in workshops organised by the Partner's IT Security Services for the purpose of planning service improvements. These workshops have identified a series of Work Packages which directly involve researchers, including an exercise to assess user and student perception of IT security across the university through interviews, and involvement in a campus-wide risk assessment exercise, amongst others.

Publications

I Kirlappos, A Beautement, MA Sasse, ""Comply or Die" is Dead: Long live security-aware principal agents", 2013 Workshop on Usable Security (USEC '13), Okinawa.

S Bartsch, MA Sasse, "How Users Bypass Access Control - and Why: the impact of authorization problems on individuals and the organisation", Proceedings of the 21st European Conference on Information Systems (ECIS 2013), Utrecht.

Related Activities

- Talk: MA Sasse, "e-Government Service and Federated Identity: Happy or Toxic Mix", Royal Holloway, University of London, Opening Keynote, IFIP IDMAN 2013 conference.
- Talk: MA Sasse, "Cyber Security as a Science", Cyber Security & Electronic Terrorism conference, London Olympia, 24 April 2013.
- Panel Speaker: MA Sasse, "Security - the end user perspective", Payments Council Innovation conference 2013, King's Fund London, 7 May 2013.
- Talk: MA Sasse, "Avoiding collateral damage: protecting people, not just systems", Armageddon in Cyberspace, A joint event hosted by Gresham College and The Worshipful Company of Stationers and Newspaper Makers, Stationers' Hall London, 28 May 2013.

- Panel Speaker: MA Sasse, “Deception Security and Human Behaviour”, University of Southern California Los Angeles, 3 June 2013.
- Keynote: MA Sasse, “Busting The Myth Of Dancing Pigs: Angela’s Top 10 Reasons Why Users Bypass Security Measures”, European OWASP Conference, Hamburg, 22-23 August 2013
- Keynote: MA Sasse, “How to overcome the great authentication fatigue”, Emerging Securities Technologies Seminar, Cambridge, 9-11 September 2013
- Talk: MA Sasse, “Want Effective Security Solutions? Let’s Re-Think The Design Approach”, Microsoft Research Cambridge, 11 September 2013
- Talk: MA Sasse, as part of UCL Innovation Day visit to IBM Hursley, 19 September 2013
- Talk: MA Sasse, “Rule bending: what really goes on under the hood of the enterprise?”, Investment Banking SiG, Ernst & Young, 20 September 2013
- Talk: Adam Beautement, “Utilising Human Factors in the Science of Security”, 2nd International Cyberpatterns Workshop, Abingdon, Oxfordshire, 8-9 July 2013
- Talk: Adam Beautement, “Human Behaviour and Security Compliance”, The Institution of Engineering and Technology (IET) Cyber Security for Industrial Control systems, Glasgow, 11 July 2013
- Panel Member: Simon Parkin, “Where are we going with mobile apps engineering?”, Human Aspects of Mobile Apps Engineering (HAMAE) workshop, BCS HCI 2013 Conference, 9 September 2013
- Poster: Simon Parkin, “Productive Security”, IAAC (Information Assurance Advisory Council) Annual Symposium 2013, BT Centre, London, 11 September 2013

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