CDT Newsletter

EPSRC Centre for Doctoral Training in Cyber Security

Winter 2017

CDT update

First CDT students graduate

The EPSRC Centre for Doctoral Training in Cyber Security at Royal Holloway reached a significant milestone on Friday 10th November 2017 when Conrad Williams of the 2013 cohort became the first student to complete his PhD viva. Well done to Conrad, whose thesis on Completeness in Languages for Attribute-based Access Control was successfully defended. Conrad is now working as a Cyber Security Specialist at reinsurance broker Capsicum Re. Several more PhD vivas are scheduled over the coming months as the remainder of the 2013 cohort conclude their studies.

It is thrilling to see CDT theses being completed and, more importantly, to see the extremely rounded and skilled graduates progress in their careers. The primary objective of the CDT is to develop a cohort of highly-trained researchers with a broad understanding of cyber security, and an appreciation of the increasingly important interplay between theoretical, technical and human factors in this field. We are thus delighted to see this reaching fruition. At the time of writing, four students have submitted their theses and commenced fulltime employment. Thalia Laing is a Research Engineer in the Cloud and Security Lab of HP Inc. and Sam Scott is a Software Consultant at Cornell Tech. Excitingly, and testament to the culture of innovation fostered by the CDT, two students have become involved with start-up companies. Sam is about to join a start-up programme at Cornell to prepare the way for commercializing research he has been involved in concerning password hashing. Thyla van der Merwe has recently joined London-based Crypto Quantique as their Principal Cryptography Engineer, where her role involves developing cryptographic algorithms and protocols for use with the company's Quantum Driven Secure Chip. We look forward to reporting on the career destinations of the other students of the 2013 cohort as they follow suit over the coming months.

A new cohort start

October 2017 saw the arrival of our fifth CDT cohort of eleven students. They have an impressively wide range of academic backgrounds, including econometrics, geopolitics, psychology, computer science and political philosophy. Several have held previous employment in careers as diverse as security consultancy, finance and mathematics teaching. Our recent experience suggests this blend of life history will deliver a superb cohort, and early evidence was provided by their thoughtful and inspiring group project on the national cyber security strategy, which they analyzed and critiqued.

End of current funding

Such are the swings and roundabouts of funding that, just as we celebrate our very first PhD graduate, so we place the recruitment adverts for our final student cohort on the current funds. The CDT in Cyber Security at Royal Holloway has been, we hope you agree, a runaway success story. The outstanding students have brought an electrifying energy to our research environment. The innovative training environment has broadened their skill base, and we are now seeing the products of this through quality research that is hitting high standards and winning awards. The CDT has acted as the perfect vehicle to facilitate research beyond traditional disciplinary boundaries, with projects involving computer science, economics, geopolitics, geography, mathematics, psychology, and sociology. The CDT has also helped to bridge conversations between academia, industry and government, some of which you can read about elsewhere in this newsletter. The ultimate fruits of these relationships are the graduate destinations of our first completers.

The CDT has been a joy to facilitate and we hope that it can continue in some form. In early 2018 we will be required to bid for funds for a new CDT, competing against all disciplines and universities conducting engineering and science research work. Please get in touch if you are willing to help us tell the success story of this CDT and supporting a new funding bid. As we have discovered, hosting a CDT is too rich an experience (and far too much fun) to not host one in the future!

Prof. Keith Martin *(acting CDT Director, while Carlos enjoys his sabbatical in Japan).*

Inside the cohort

Amy Ertan

I knew the CDT was going to be an entirely new challenge, having previously studied Philosophy, Politics and Economics, followed by time in industry. It was the multi-disciplinary feature that gave me confidence to take the plunge, and it certainly hasn't disappointed! I've been buried in network security tomes, debated on state cyber-espionage and presented on cryptographic applications. Furthermore, the CDT 2018 cohort themselves have a lot to teach; our backgrounds allow us to 'cross-train' others, and recommend topics we know others might enjoy.

A significant feature this term has been the CDT Group Project, with the 11 of us tasked with dissecting and evaluating the UK's National Cyber Security Strategy. With swift sub-team creation, frequent cohort catch-ups, and some practice runs, we researched, designed and presented a smooth journey from exploring the nature of cyber security strategy, to a detailed analysis of the original 2011 vs current content. It felt very satisfying to present our work to academics in the department - also highlighting the real fear of thorough academic questioning! Working together, our various backgrounds and disciplines often meant we each brought something different to the table. Those with technical grounding made sure the rest of us understood the practical implications of detailed policy, while those with industry experience coached others on effective presenting styles---with our presentation commended as a result!

Since the presentation, other projects have happily emerged. Some of us are forming teams for CaptureTheFlag events, while I am excited to work with others from my cohort on the Royal Holloway – Oxford Inter-CDT Conference in Spring. As the year goes on and our research interests become clearer, we're excited to see where collaboration may lead, having seen that a multidisciplinary approach can add so much value.

Simon Butler

It's a whirlwind, for sure. But in a good way. We all expected a big challenge on joining the latest CDT cohort, and none are disappointed as the first term draws to a close. It feels like only a blink of an eye since we got stuck into lectures and all the activities that come with being part of this programme – yet here we are, Christmas is around the corner. Having completed the MSc Information Security this year, I have been able to choose some alternative modules to the rest of the cohort (a great opportunity to close some skills gaps). Amongst others, I've been working on a programming module from the Computer Science department, presented by Professor Johnstone. We're often welcomed into his lectures by the Clash, or some other great, as he tries to educate his class on matters beyond just Java.

Being part of the cohort has been a refreshing change. A strong team environment has evolved, with everyone helping out as they can. We're benefitting from a varied group that reflects the multifaceted nature of cyber security and the ISG. We have mathematicians, computer scientists, as well as a geopolitician (possibly a new word) and a psychologist. We're learning from each other, and encouraging new experiences.

It's not all work, as you might expect. Christmas offers an opportunity for a few extra social events. We have a trip to Winterwonderland, as well as an ISG Christmas dinner in the final week of term. And this week the cohort will be visiting the Festive Market in Founder's Square. Apparently there will be a reindeer there. A real one. Did someone say a reindeer?

Away from the Ivory Tower

Assemblers Assemble

From January to April, 2017, I spent time as a participant of the Berkman Klein Assembly program, run out of the Berkman Klein Center for Internet and Society at Harvard University. The aim of the programme was to bring together individuals from industry and academia to solve problems in cyber security, a very broad problem statement indeed! As part of the initiative, I started working on two Internet of Things (IoT) projects, both with the intended goal of securing IoT devices in a home network from being exploited as part of Distributed Denial of Service (DDoS) attacks, such as the Dyn DDoS attack of 2016. Together with a fellow Assembly member, we came up with two solutions – Sherlock Homes and Thingerpirnt. The first is a router level solution that detects and reacts to abnormal device traffic, and the second helps to define abnormal traffic by collecting and analysing a large number of IoT device fingerprints. These two solutions were developed under the guidance of an impressive panel of board members, including academic staff from Harvard University and the Massachusetts Institute of Technology (MIT), as well as the Chief Security Officer of Akami, and the Executive Chairwoman of Mozilla. We developed a Proof of Concept (PoC) for both solutions while I was at Harvard, and work on both projects continues, with undergraduate students getting involved to flesh out the details.

Whilst at Harvard, I also completed a first draft of a paper with a collaborator at Harvard Law School, titled Coming in from the Cold: A Safe Harbor from the CFFA and DMCA § 1201 for Security Researchers. This paper proposes a legislative solution to the chilling effects created by legal action that accompanies security research. This paper will be submitted to a Technology Law journal in the US. Doing research of this nature has been both exciting and challenging - quickly learning the necessary aspects of technology law, and how to combine this knowledge with my technical knowledge in order to produce a workable solution for security researchers has been highly rewarding. This paper is also likely to be listed as a Berkman Klein Assembly output. For more on the Berkman Klein Assembly projects, please see the Berkman Klein Assembly website: **http://bkmla.org/**

Thyla Van Der Merwe
student from the 2013 CDT cohort

Crypto Wars 2.0

The 3rd annual inter-CDT workshop took place in Oxford between 3-5 May 2017, this year with the theme 'Crypto Wars 2.0'.

Day 1 began with a scene-setting talk from Royal Holloway's Keith Martin covering the history of the crypto wars, followed by Eerke Boiten from De Montfort University assessing the current state of the crypto wars in the UK. Corrinne Cath of the Oxford Internet Institute presented a case study of the work of human rights NGO ARTICLE 19 and the IETF, after which Cian Murphy from the University of Bristol rounded off the morning speaking about the legal and technological challenges to law enforcement access to encrypted communications. Reinvigorated by lunch, the afternoon consisted of talks by Frederike Kalthenuer who presented the Privacy International viewpoint, and independent consultant Lars Hilse joining us via Skype from Germany to talk about his Global Magna Carta Initiative. Rounding off Day 1 was a student-led debate on the question 'Everything Encrypted: Utopia or Dystopia?', moderated by Steve Hersee. The pre-debate audience poll showed a 14/3 split in favour of Utopia, giving Rob Markiewicz and Nick Moore (Dystopia) an uphill battle against Pete Beaumont and Will Seymour (Utopia). After a lively debate with plenty of audience involvement the final poll came in at 18/2 in favour of Utopia – perhaps unsurprising in a room full of cryptographers. Discussions resulting from the day's talks continued into the wonderful evening dinner at Somerville College and beyond.

Day 2 was opened by Brigadier Fred Hargreaves presenting the official line from a defence and national security point of view, after which infosec veteran Alec Muffett give an entertaining and enlightening talk on end-to-end encryption and the nature of identity. Post-lunch, our final invited speaker was Phil Garnett from the University of York who presented on crypto wars in the context of arms control, and questioning whether the wars 2.0 was any different from 1.0. The final session of the workshop was a series of 5-minute lightning talks from CDT students presenting on aspects of their research. The participants were: Thyla van der Merwe (via pre-recorded video), Katriel Cohn-Gordon, Steve Hersee, Will Seymour, Carlton Shepherd, Mary Bispham, and Ela Berners-Lee.

Although concrete answers are hard to come by in the crypto wars debate, the workshop was highly valuable in helping us explore the intricacies and nuances of this complex topic. We now look forward to the 2018 edition, with Royal Holloway assuming hosting duties. See Tweets from the workshop on the hashtag #CDTWars.

Should I really have just clicked on that? Bringing Human Factors into the Information Security equation

Marco Cinnirella, Royal Holloway.

This year the CDT welcomed its first psychology student and we are delighted to be working with Dr Marco Cinnirella to support research on the human factors behind employee behaviours in organisations. Here, Marco outlines the background to his research agenda

On 15th March this year I stood on stage at the Institute of Engineering and Technology in London with two Royal Holloway colleagues from the Information Security Group (Lorenzo Cavallaro and Stephen Wolthusen). Our task was to deliver the College's annual Stevenson public science lecture. This was a pivotal moment for me, and I believe it signifies a wider shift in the Information Security (IS) space. It was the first time I had shared a stage with academics who work on the technical side of IS, and indeed the first time in my academic career I had engaged in any kind of academic dialogue with computer scientists.

The path that led to the delivery of this public lecture, and which ultimately got computer scientists talking to social scientists like myself, started some twenty months earlier. At that time I, together with colleagues David Denney and Rikke Jensen (Law, Royal Holloway), were approached by a CISO who had the vision to recognise that the landscape of IS could be better charted if a technical approach found synergy with a human factors one. Professor Robert Coles, CISO at GSK, commissioned the three of us to develop a new multi-disciplinary approach to understanding the human factors behind employee information security beliefs and behaviours within large multi-nationals like GSK. I headed up the psychological arm of this work.

When an organization thinks about Information Security, there is a natural tendency to see this as a technological issue, both in terms of problems and solutions. This technological framing is understandable, given that many CISOs and their teams have a background in computer science. However, despite automation encroaching further into the workplace, humans remain an integral component, at least for now, in most work environments, and there is one certainty that is irrefutable – when humans interact with technology, one can expect the unexpected. Plugging security vulnerabilities and fixing the mess caused by human error absolutely requires technological solutions, however there comes a point when an organization may want to go beyond reactive firefighting, and instead seek to be proactive and to understand why those fires are lighting in the first place. This is where technology alone can no longer provide an answer, and the different lens offered by social science has something to offer.

As employees grapple with day-to-day work tasks, under increasing pressure to hit ever tighter deadlines, to multi-task their way through the use of different systems, to navigate a sea of emails, and to abide by regularly changing and expanding regulations, they cope as best they can. One way in which our brains assist with such challenges is to help us learn mental short-cuts that generally serve us well, even if at times they can leave us vulnerable. By deploying these short-cuts - what psychologists call heuristics – we conserve our cognitive processing power in the same way that mobile devices save power and energy by throttling CPU clock speeds. Ellen Langer was one of the first social psychologists to demonstrate how these mental heuristics can sometimes leave

us vulnerable. In what is now regarded as a classic experiment demonstrating what she calls 'mindlessness', she took down all photocopiers in a US college library apart from one, with the result being that a long queue formed at the one functioning machine. At various points in time a confederate working with Langer would approach the person at the front of the queue and recite one of three pre-prepared requests aimed at being allowed to push in. In the first variant, a request was given without any justification, in the second a reasonable justification followed the request ("because I am in a rush"), and in the final variation, the justification given was facile ("because I need to make copies"). Langer postulated that when we hear a request followed by the start of a justification ("because…") our minds switch into a mental autopilot which she calls mindlessness and many psychologists today called heuristic processing. According to Langer, this mental shortcut tells us that usually the request is genuine, and its effect is to reduce the attentional resources we devote to properly processing the reason mode – this means that even an illegitimate or facile reason can sometimes generate the desired response. Indeed, the experiment showed that the illegitimate/facile reason condition generated 93% compliance with the request, compared to 94% compliance when a genuine reason was given.

Heuristic or 'mindless' processing occurs more often than we like to admit. In terms of IS behaviours, the only way employees can navigate their work challenges is through the regular deployment of a whole army of such mental heuristics. What does a genuine email look like, what does a phishing email look like, what is a safe link to click on, which senders are usually or always safe? Answers to these kinds of question are provided by heuristics, which equip us with stereotypical knowledge in such a way that our perception is guided and targeted to pay more attention to some cues in the environment than others. Of course for the social engineer aware of such heuristics, they provide an opportunity to exploit everyday mental shortcuts to their advantage, by tailoring threats in such a way that they 'fly under the radar' of what heuristics lead us to expect threats to look like. Only in the last two to three years have social scientists began to apply these insights to Information Security, and as yet organizations are unsure quite how to leverage such insights to their advantage.

Part of the challenge facing organizations is to therefore better predict the interaction between humans and technology. This is by no means a new problem. The need to understand it was brought home very painfully via accidents in the civil aviation and nuclear industries, yet such lessons are seldom seen as relevant to Information Security, which is regrettable. What they tell us, is that employees dynamically make judgements about the costs versus benefits of doing what management expect them to do, and balance risk against convenience. When employees judge that a policy or procedure is an unwelcome impediment to their productivity, they may seek (sometimes creative) means to subvert the policy, whether it be by, for example, using public wi-fi in nearby cafes to usurp restrictions on the company network, through to using unsecured personal mobile devices to complete work that is otherwise hampered (in their eyes) by the restrictions imposed on company devices.

The determinants of such judgements are not mathematical decision schemes (as per behavioural economics models) but instead a complex interaction of individual level factors (e.g. personality dimensions such as 'sensation-seeking'), work environment factors (such as peer pressure, 'psychological work contract' and management style) together with broader cultural factors such as the degree to which a national culture fosters what psychologists call uncertainty avoidance, which reflects a society's general orientation to accepting or minimising risk.

This complex mix of individual, work and societal/cultural factors together help determine an employee's response to both Information Security threats and the organization's Information Security policies/procedures. Understanding this complex puzzle is the only way to properly predict how employees will interact with technology, and seeking to do so will provide organizations with a degree of resilience that technological solutions alone can not provide. Ignoring such human factors is, I predict, something that organizations will not be able to sustain for much longer.

Dr Marco Cinnirella is a Senior lecturer in Psychology at Royal Holloway.

m.cinnirella@rhul.ac.uk

The Stevenson Lecture 2017 can be viewed at: **https://tv.theiet.org/?videoid=10011**

CDT research newsbites

- **Ela Berners-Lee** presented her paper on Improved Security Notions for Proxy Re-Encryption to Enforce Access Control at the Fifth International Conference on Cryptology and Information Security in Latin America, La Habana, Cuba.

- **Alex Davidson** took up a second internship at CloudFlare. He worked on a full-stack implementation of a novel cryptographic protocol "Privacy Pass" for anonymous client authentication to service providers. The motivation behind the work is to provide users with anonymity constraints (e.g. users of Tor/VPNs) with the ability to bypass Cloudflare CAPTCHA challenges if they had already proved themselves in the past, whilst preserving the anonymity of the users. Alex's work was released in CloudFlare's production environment and in a browser extension compatible with Chrome and Firefox. For more information about Privacy Pass go to https://privacypass.github.io.

- **Amit Deo** has a paper accepted at AsiaCrypt 2017, one of the three flagship cryptography conferences worldwide. His work establishes the equivalence of some problems (the Module Learning with Errors problem and the Ring Learning with Errors problem) that are currently being used to construct quantum-resistant encryption and signature schemes.

- **Giovanni Cherubin** won an "Andreas Pfitzmann Best Student Paper Award" at the Privacy Enhancing Technologies Symposium (PETS) 2017 for his single author paper "Bayes, not Naïve: Security Bounds on Website Fingerprinting Defenses". PETS is the premier venue for research on privacy-enhancing technologies. His presentation can be viewed at https://www.youtube.com/watch?v=rQ5MfHAZ3zk.

- **Andreas Haggman** is the CDT curator of awards. In 2017 he added 1st place (team) at the Playtest UK Games Jam at the V&A Museum of Childhood and 1st place in the Retail Cyber Security Student Challenge, British Retail Consortium.

- **Torben Hansen** was a co-author on A Surfeit of SSH Cipher Suites, one of the best paper award winners at the 23rd ACM Conference on Computer and Communication Security in Vienna, Austria.

- **Jonathan Hoyland**, **Sam Scott**, and Thyla van der Merwe, in collaboration with researchers from the University of Oxford, published a paper at the 2017 IEEE Symposium on Security and Privacy, a top tier conference. Their work gives a comprehensive symbolic analysis of TLS 1.3, the new version of TLS that is currently under development in the IETF. They are now listed in the draft specification of TLS 1.3 as contributors.

- **James Patrick-Evans** won the best paper award at the USENIX Workshop on Offensive Technologies for his work on finding bugs in USB device drivers. His key idea was to simulate summaries of all possible behaviours of a virtual device, which led to the discovery of two critical vulnerabilities in Linux.

- **Dusan Repel** published his work on the automatic generation of exploit attacks for heap-based memory corruption vulnerabilities at the ACM CCS Workshop on Programming Languages and Analysis for Security. The work is the first to explore automated program analysis to reason about complex and vulnerable heap memory layouts – a task that's been so far confined to the realm of human reasoning – to trigger arbitrary code execution attacks. The work has natural implications for the security software development lifecycle (e.g., security vulnerability prioritization) as well as the offensive technology landscape (e.g., automated exploitation of heap-based software vulnerabilities and bug bounty programs).

- **Nick Robinson** is co-author of the paper Distributed denial of government: the Estonian Data Embassy Initiative, published in a special issue of the journal Network Security.

- **Sam Scott** published a research paper at CRYPTO 2017. The paper concerns the security of key rotation for symmetric encryption - this is a common practice in cloud storage services, but has only received a very limited formal security treatment to date. Sam's work develops security models for this setting, provides an analysis of schemes used in practice and presents new, efficient constructions enabling secure key rotation. This work was done in collaboration with researchers from RHUL, Cornell Tech and University of Madison, Wisconsin.

- **Pip Thornton's** research has involved critiquing Google's commodification of language through an artistic intervention called {poem}.py. Work from this project has been exhibited at the 2017 Inter/Sections event on Politics & Ethics in Media Art Technology at Mile End Arts Pavilion in London, and at the After Money 48 hours exhibition at the City Arts Centre in Edinburgh. A collection is also currently on display at the Open Data Institute in London on a 12 month loan commission.

- **Fernando Virdia** has a paper accepted at AsiaCrypt 2017, one of the three flagship cryptography conferences worldwide. His work (co-authored with his supervisor and a team from TU Darmstadt in Germany) verifies a conjectured cost model for establishing the concrete security of several quantum-resistant encryption and signature schemes.

- **Joanne Woodage** spent three months as an intern with Microsoft Research, Redmond, USA, working in the crypto research team led by Dr Brian LaMacchia. In 2017, she also published research papers at the top-tier conferences CRYPTO and ACM CCS. The work in these papers was done whilst Joanne was visiting the research group of Prof. Tom Ristenpart at Cornell Tech, New York.

CDT News

Cyber 9/12 Student Challenge

20–21 April 2017
Geneva, Switzerland

The Cyber 9/12 Challenge is a scenario-driven policy competition for teams of students, organised by the Atlantic Council and hosted at the Geneva Centre for Security Policy.

Royal Holloway was represented by Team CDT Mavericks, comprising Ela Berners-Lee, Andreas Haggman, Rory Hopcraft and Pip Thornton. A week before the event we received a briefing pack containing intelligence reports and news stories about an unfolding threat of ransomware against medical devices. We were required to digest this information into a short, written summary and construct a Decision Document containing four proposed policy options to tackle the situation.

On the first day of the competition we were put before a panel of six judges to present our policy alternatives, including our recommended option. The judges were given two minutes to read our Decision Document after which we had ten minutes to give an oral presentation, followed by ten minutes of rigorous questions and answers from the judges.

We were delighted to win the award for the Most Creative Policy Response, thanks perhaps to our policy to insert human intelligence agents into the attackers' organisations, or our advocacy of a Robin Hood model for security updates. As a result, we qualified for the semi-final round the following day. This involved receiving another briefing pack moving the scenario forward, which needed to be analysed overnight. The team stayed up until 03:30 working out brand new policy options, which we had to be ready to present by 08:00.

Although our presentation went well, with the judges praising "the best teamwork seen in the whole competition", we did not make the final four. Despite this, we were extremely pleased with our efforts and results. None of us had any experience of such an event but all found it hugely rewarding, both in terms of the skills we developed and the exposure it gave us to a high-pressure policymaking environment. As a testament to the CDT- ethos, we felt the breadth of backgrounds and knowledge of our team members served us very well as everyone was able to contribute in a different way.

We wholeheartedly recommend this competition to other students. Although we may have set the bar high with an award-winning Royal Holloway debut, our performance is not unbeatable. Watch out for announcements about a UK-version later this year. And most importantly, we did better than all three Oxford CDT teams! Beers well-earned.

Internships

An important component of the CDT programme is internships, which provide students with a different perspective on cyber security by engaging with the subject in partnership with an external organization. We see this as not just useful experience for the student, but also a valuable opportunity for CDT partner organizations to access skilled workers and meaningfully connect with the work of the CDT. The last few months have seen CDT students in placements at Cloudfare, The Cabinet Office, Crypto Quantique, Thales Australia, HP Inc., Microsoft Research Redmond, and NATO SHAPE.

CDT News

‘Curating (in)security: Unsettling Geographies of Cyberspace’

This year the annual meeting of the American Association of Geographers (AAG) took place in Boston, MA. The AAG is the largest meeting of Geographers in the world, with well over 9,000 participants from all corners of the discipline. The conference is therefore a great opportunity to meet other researchers interested in potentially more niche subjects, and to debate and develop ideas.

With the uncertainties of global politics and a rapidly changing media and security landscape in mind, Andrew Dwyer (Oxford CDT) and I decided to use the 2017 AAG to convene a session exploring the emerging geographies and (in)securities of digital technologies, and put out a call for papers asking for responses to the title: Curating (in)security: Unsettling Geographies of Cyberspace. The aim of our session was to call for the unsettling of current theorisation and practice, and to initiate an exploration of the contributions geography can bring to cybersecurity and space. Our CfP was thus an attempt to move away from the dominant, often masculinist and populist discourses around conflict and state that are often prevalent in international relations, politics, computer science and security/war studies. Instead, we aimed to provoke alternative ways we can engage and resist in the mediation of our collective technological encounters, exploring what a

research agenda for geography in this field might look like, why should we get involved, and pushing questions in potentially unsettling directions.

We ended up filling two very successful sessions, with papers including provocations on the dangers of humans as vectors in algorithmic decision-making spaces, the subversive potentials of digital advertising space, and the production of racialised spaces in the visual narratives of #blacklivesmatter. We were also very pleased to accept fellow CDT student Nick Robinson’s fantastic paper on the problems and potentials of the ‘data embassy’, and I also had the opportunity to present my own work – a critique of linguistic capitalism – and demonstrate my own ‘curation’ with my {poem}.py project and receipt printer. With the addition of two fantastic discussion pieces from established geographers Jeremy Crampton and Nat O’Grady, Andrew and I were both very pleased with how the sessions went, and we are hoping to be able to produce an edited collection bringing all the papers together.

Pip Thornton
student from 2013 CDT cohort

We are now open to receive applications for students to start their PhD studies in September 2018. If you are interested in applying, please contact us directly to discuss your suitability for the programme. Selected applicants are awarded fully-funded PhD studentships for four years. To be awarded one of the studentships, candidates will need to have undergraduate and/or masters qualification in a discipline relevant to cyber security and satisfy the EPSRC funding eligibility criteria.

CyberSecurityCDT@rhul.ac.uk

royalholloway.ac.uk/isg/cybersecuritycdt/home.aspx

RHULCyberCDT

7573 12/17

EPSRC
Engineering and Physical Sciences Research Council

Royal Holloway, University of London
Egham, Surrey, TW20 0EX
T: +44 (0)1784 434455
royalholloway.ac.uk