CDT Newsletter

EPSRC Centre for Doctoral Training in Cyber Security

November 2015

Information Security Group

CDT Director update

Welcome to the autumn 2015 edition of the CDT newsletter. This has been a busy, and successful year for Royal Holloway's CDT in Cyber Security, teeming with activities and achievements for our students. We are pleased to be able to report the progress of the CDT and its many success stories in this newsletter.

We now have 31 students in the CDT, divided into three cohorts. This is a great group of students, with a broad range of backgrounds and research interests. We have students working on topics ranging from analysis of cryptographic protocols to cybercrime, from machine learning to geopolitics, from code analysis to game theory. CDT students are also all closely located in the McCrea building, and have greatly contributed to the ever more vibrant PhD environment in the Information Security Group.

A new CDT cohort, with 12 students, has just started their studies in late September. They are now engaged in their first-year training, which for many represent a first contact with cyber security as an academic discipline. There will be plenty of opportunities to meet students in the new cohort throughout the next years; but you can read the impressions of two of them in this newsletter.

Students in the second cohort had a busy summer, working on their summer projects. The first-year summer projects mark the transition from training to research in the CDT programme, and this again resulted on a number of high-quality pieces of research. Students had the opportunity to present their work during a "CDT viva day" in late September, in front of an audience of more than 40 attendees. Posters of their research are now on display in the CDT room.

Students from the first two CDT cohorts are now well into the research component of their studies, and as expected, have produced a number of research papers during this year. We are impressed with the high standard of the CDT research output so far, which in our opinion reflects the excellent quality of the CDT student body. We report a few of the CDT research highlights in this newsletter.

In addition to the many research-related activities, a major goal of our CDT is to provide students with a strong exposure to industry and some of the challenges faced by the cyber security sector. We accomplish this by hosting visitors from industry, organising "CDT days out" to get an insight of a typical day of security professionals, by working with partners on joint research projects, but more importantly, by arranging work placements for students with one of the CDT industrial partners. All CDT students are expected to spend approximately three months working with a partner, as part of their industrial internship. Several students from the first CDT cohort had their internship this summer, working with CDT partners in the UK, US, Sweden and Japan. You can read in this newsletter some of their experiences.

Finally, the newsletter has also information about some of the activities our CDT students have been involved that reach out beyond academia: participation in a recent national TV series, and organisation of a workshop focusing on recent high-impact security incidents. Overall, we are delighted to report on the continuing success of the CDT and its students! I hope you enjoy reading about it in this newsletter.

Professor Carlos Cid

Inside the cohort

As a first year CDT student, a lot of our time is taken up attending lectures in extremely interesting areas of cyber security such as computer security and network security. As a mathematician, these lectures are really helping me get a broader feel of the general field and this is one of the main things that make the CDT such an exciting programme to be part of. As expected, our cohort consists of people from a wide variety of academic backgrounds and I would say that we are all being challenged to step out of our comfort zones whether it be taking a cryptography module as an arts student, or a geopolitics module as a computer scientist.

As a cohort, we've been spending a lot of time working together in our office (along with the occasional trip to the campus coffee shop). At our introductory meeting, we were set a task to answer the question "What is Cyber Security?" in whatever way we chose. After much deliberation, we decided to go ahead and make a website outlining various aspects of cyber security to answer the question. Overall, I would say that the presentation we gave as a supplement to the website was well received. Another thing that we've been busy with is reading groups. We recently had our first CDT classical reading group session where a few of us were asked to present a paper on fuzz testing followed by a group discussion.

To summarise, the first few monts of my time at Royal Holloway have been a lot of fun and I look forward to seeing how all of our interests are shaped by the things we learn throughout the year.

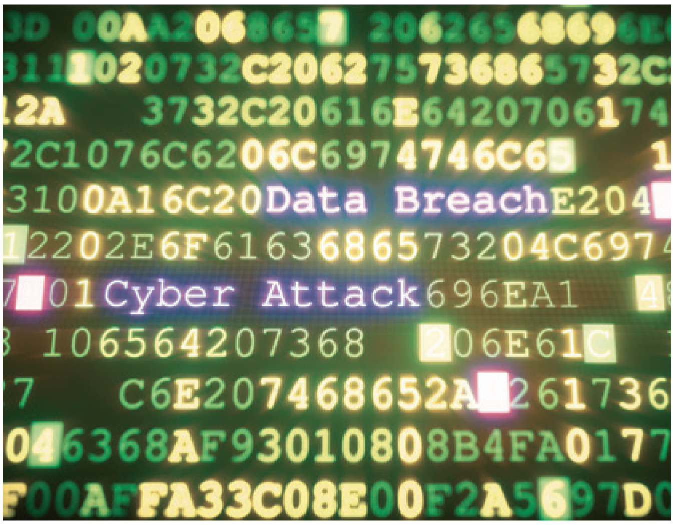
Amit Deo, first-year CDT student

The initial foray into CDT life has been a busy, yet enjoyable experience so far. Given my background in Geopolitics and Security, my pathway into cyber security has differed slightly to years gone by - but starting the program with a focus on cryptography, network and computer security, and security management has been both refreshing and challenging. What's more, I've been presented with an opportunity to broaden my interests, of which I'm sure my future research will benefit from.

As the 'token' political geographer in this year's cohort, I'll admit that there was some slight trepidation in stepping into a CDT dominated by mathematicians and computer scientists. However, this has all but vanished during the first few months and, in many ways, we have already become a sociable, cohesive unit. Life in the CDT doesn't just revolve around the work, as we have already organised pub quiz teams, pub lunches/ dinners and fireworks displays, to name but a few.

The program has also allowed us to attend regular workshops and seminars, which go a long way in complimenting our modules and wider interests. They also allow us a greater insight into the current work our peers within the department, and within the field more generally, are up to. Attending career events and hearing from industry professionals have been great introductions into what life in information and cyber security potentially holds for us in the future – also testifying to different perspectives outside of academia. The next months will hopefully bring more of the same and I am looking forward to the opportunity of attending modules focused on legal aspects of e-Commerce and cyber crime in the new year – before embarking on our summer projects!

Nicholas Robinson, first-year CDT student



CDT student takes part in Channel 4's *'Hunted'*

Steve Hersee, a student from the first CDT cohort recently appeared on Channel 4's *'Hunted'*, a programme which challenged 14 ordinary members of the public to disappear for 28 days.

He was one of a team of 'hunters' who were tasked with tracking down the contestants using a range of surveillance techniques. Steve explains what it was like to take part in the programme and what he learned from the experience:

What was taking part in *'Hunted'* like?
Taking part in Hunted as an analyst was a hugely exciting and eye opening experience for me. In my previous lives I have worked in the military, police and within corporate intelligence and in these roles you rarely get to see the other side of the story; what it is actually like to be targeted. Watching Hunted every Thursday has been a unique opportunity for me to observe how the people we studied actually behaved, to judge how much we really knew about them and how accurate our assessments of their personalities were.

What makes *'Hunted'* unique as a programme?
The concept of the show itself is fantastic. It's a manhunt and a huge game of hide and seek, a thrilling chase full of near misses mistakes and suspense and it's a reality TV show with a difference. From the first few episodes you can really see the stress that the fugitives are under and the strain on their relationships. The audience gets to see how the different fugitives cope with the increasing pressure and paranoia and this, for me is fascinating. Hunted also arrived at an interesting time in the debate over privacy and surveillance. By attempting to show both sides of the picture the show adds a unique perspective.

What insight did you gain from being part of the programme?
From an academic perspective it was fascinating to witness the practical use of exploits, phishing, physical exploitation of hardware and other techniques, against ordinary members of the public. This was information security playing out live and in real time with real positive consequences for us if we could break into accounts and access the information we needed. Within the Information Security Group and the CDT, security techniques such as two factor authentication and password managers are considered best practice but surprisingly few of the fugitives actually used these techniques. There is a huge gap between the security techniques that are available and those that ordinary people use.

The first series of *'Hunted'* ran in the autumn of 2015. Episodes can still be watched in Channel 4's website. ■

Industry Connection: summer internships

Several students from the first CDT cohort spent the summer working with some of our industrial partners, as part of their internships. They typically worked for three months on projects of practical relevance, and potential real-world impact, in the field of cyber security. Below we can get a bit of insight into the experience of two students.

This summer I was fortunate enough to be able to complete a three-month internship at HP Labs in Bristol. I worked with a team of researchers that were considering security in the Internet of Things.

During my internship I learnt a lot about security in practice. Although I knew industry faced different challenges and had potentially contrasting focuses to academia with their research, these were highlighted further as I gained experience in identifying and discussing potential concerns regarding real world applications. My three months at HP also reinforced the masters-level courses I had completed in the first year of my PhD.

Towards the end of my internship I participated in an HP poster fair where I presented my work to other researchers. This was a fantastic opportunity to explain my work and to network and discuss other people's research interests. Overall, the internship was a fantastic opportunity for me to sample working in industry.

Thalia Laing

This summer I completed an internship at Mozilla Corporation in Mountain View, California, and was fortunate enough to be mentored by Eric Rescorla. Eric is the editor of the TLS 1.3 specification, the next incarnation of the TLS protocol. TLS 1.3 is the Internet Engineering Task Force's answer to the weaknesses in TLS 1.2, and the TLS Working Group is in the process of finalising its design. Under Eric's guidance and together with **Sam Scott**, a fellow CDT cohort member and Mozilla intern, I worked on the symbolic verification of TLS 1.3. The TLS protocol is used by millions of users on a daily basis and verification of its security properties is of critical importance.

We conducted our analysis in collaboration with Professor Cas Cremers and Marko Horvat of the University of Oxford and have just submitted our findings to one of the top-ranked annual security conferences in the US. The team has been in constant contact with the TLS Working Group and has made several comments and recommendations regarding the new specification. As part of my internship, I also attended a TLS Interim Meeting in Seattle and was able to meet several of the TLS Working Group members.

The opportunity to work in the US, and in Silicon Valley in particular, has been invaluable to my development as researcher in the field of security, and I am very pleased that my internship provided a chance for academia-industry collaboration.

Thyla Van Der Merwe

CDT News

Workshop on the Hacking of Sony Pictures

A two-day workshop focusing on the hacking incident of Sony Pictures was jointly organised by the CDTs in Cyber Security at Royal Holloway and Oxford. The event was held at Oxford University in May 2015, with presence of students and academics from both universities.

The workshop was designed as an interdisciplinary event, covering a multitude of facets of the Sony hack which came to prevalence in November 2014. This topic is replete with both technical and geopolitical details, and it was intriguing to explore how a seemingly innocuous data breach came to have such widespread international effects. Special focus was afforded to the attribution of the hack to North Korea, which has proven especially contentious.

Speakers included Andrea Nini from Aston University, Dmitri Alperovitch from Crowdstrike, Jeffrey Carr from Taia Global, Hardin Tibbs from FutureLens, Michael Drury, former Director of Legal Affairs at GCHQ, Madeline Carr from Aberystwyth University, and a member of the media. This wide variety of speakers provided a broad yet insightfully illuminating exploration of the Sony hack and its implications. The schedule also included a panel session and an interactive scenario where participants had to devise responses to a Sony-esque breach from the perspective of different actors.

Overall the event was a brilliant success and the different angles of analysis ensured participants from varying backgrounds could find material to relate and engage with. A white paper summarising the workshop is in production; in the meantime, a short write-up can be found at **http://tinyurl.com/o7ar83a** ■

CDT research newsbites

- **Naomi Farley** was a co-author of the paper *Optimal Constructions for Chain-based Cryptographic Enforcement of Information Flow Policies*, which was presented at DBSec 2015, in July in Fairfax, USA.
- **Andreas Haggman** presented his paper *Curb Your Enthusiasm: Why the Future is Not Stuxnet* at the 14th European Conference on Cyber Warfare and Security (ECCWS 2015), held in Hatfield in July 2015.
- The CDT had two papers at **USENIX 2015**, one of the world's top-ranked annual security conferences: **Sam Scott** was a co-author of the paper *The Pythia PRF Service*, and **Thyla Van Der Merwe** presented her paper (written with collaborators from RHUL and JHU) *Attacks Only Get Better: Password Recovery Attacks Against RC4 in TLS*. USENIX 2015 was held in August in Washington DC.
- **Thalia Laing** had her paper *Security in Swarm Robotics* (co-authored with colleagues from RHUL) published in the "Handbook of Research on Design, Control, and Modeling of Swarm Robotics".
- **Pip Thornton's** paper *The meaning of light: seeing and being on the battlefield* was published in the journal "cultural geographies" in October 2015.

EPSRC
Engineering and Physical Sciences Research Council

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