# CDT Newsletter

Information Security Group

EPSRC Centre for Doctoral Training in Cyber Security

November 2016

## CDT Director update

**This month saw the launch of the new National Cyber Security Strategy, which was announced by the Chancellor of the Exchequer, Philip Hammond MP, during the Future Decoded conference in London. The five-year strategy will see an investment of £1.9 billion into defending UK cyber systems and infrastructure, deterring adversaries, and developing national cyber security capacity. One of the highlights of the new strategy is the creation of the National Cyber Security Centre (NCSC) as the single, central body for cyber security at a national level.**


The strategy also brought excellent news for Royal Holloway's CDT in Cyber Security: it confirmed the renewal of funding for our CDT, with a new grant of £3.45M to provide funding for three further cohorts of PhD students in cyber security. The new strategy also carried several other initiatives for promoting cyber security science and technology in the UK, such as the continuing funding of the Centres of Excellence in Cyber Security Research (ACE-CSR) and Cyber Security Research Institutes, confirming the long-term commitment of the government to supporting the UK's cyber security academic sector.

The renewal of the CDT in Cyber Security also reaffirms Royal Holloway's pivotal position as a national centre for cyber security education and research. The Information Security Group, established 25 years ago, is one of the largest academic cyber security research groups in the world. Royal Holloway was one of the first academic institutions in the country to be recognised as an ACE-CSR. Its highly successful MSc in Information Security programme was one of only four to gain full GCHQ certification in 2014, and now has well over 3,000 alumni around the world.

The CDT is now in its fourth year, and we have for the first time a *full house:* 37 CDT students divided into four cohorts, working on topics ranging from embedded security to cybercrime, from cryptography to geopolitics of security, from software security to cyber economics. In this newsletter you can learn more about what some of our CDT students have been up to.

In September, we welcomed eight new students as part of the 2016 CDT cohort. They are now going through their first year of training; you can read here about their first impressions of the CDT, and the expectations from two of them. Students from the first three cohorts are likewise busy with their research, internships and extra-curricular activities. In this newsletter you can learn about the WISDOM group, which aims to encourage diversity in the department, and in which our CDT students have been playing an active role since its formation. We also take a peek outside the ivory tower, to report the experiences and work of some of our CDT students during their summer internships. Finally we highlight some of the recent research achievements of our CDT students, including a best paper award at CCS 2016, one of the world's top-ranked annual security conferences.

Royal Holloway has been producing PhDs in cyber security for over 30 years, with many its PhD graduates occupying senior cyber security roles in academia and industry. The launch of the CDT in 2013 has however provided a significant boost to our doctoral-level training and research programmes. It has given us the opportunity to attract and recruit excellent students to join our annual cohorts of PhD students, to work on a wide range of cyber security topics. As anyone attending one of our CDT events can attest, Royal Holloway has today one of the most vibrant and productive post-graduate environments in cyber security in the UK, and this is something that we all – CDT students and staff – can be very proud of. I hope you enjoy learning more about it in this newsletter.

**Professor Carlos Cid**

# Inside the cohort

The first few weeks of life as part of the new CDT cohort have been a massive gear change from undergraduate studies. While we are all feeling the pressure, the level of support we have had from the professors, post-grads and especially the previous CDT cohorts has been phenomenal. We've been kept busy with the seminars, reading groups and cross-discipline lectures, and reading frantically in the leftover time to try and catch up with previous work in the field. The atmosphere in the office is definitely one of excitement and ambition.

The idea of sharing a room populated exclusively with people much smarter than me is a little intimidating but the reality is nothing short of inspirational. Some of my favourite moments of the course have involved watching my new colleagues take turns in front of a whiteboard, swapping ideas between them and sharing knowledge from their fields that was previously alien to me as a computer scientist. As well as learning a new mathematical or engineering tidbit each day, it has been hugely satisfying to speak to those with a background in geopolitics, law or social sciences. Not only is it great to learn more about their area but their expertise brings context and perspective to my work in ways I had never thought of before.

Having our minds introduced to so much new information in such a short space of time feels a bit like living through the star gate sequence from 2001: A Space Odyssey, but continues to be more exciting than overwhelming. I think we are all eager to continue developing our understanding of cyber security and looking forward to everything yet to come, especially next year's summer projects!

**Feargus Pendlebury**, first-year CDT student

Embarking upon a four-year research degree as a CDT student is both daunting and exciting. I have enjoyed meeting and getting to know the other members of my cohort and have been inspired by their wide and varied interests. However, having come from a background in mathematics, it has become obvious that mathematics has a very small role in the wider field of cyber security.

As a cohort, we have all been challenged to step outside our comfort zone and take taught courses that may be different from anything we have done in the past. I feel that this challenge has been well received by the cohort in general. This year's cohort has also been busy taking part in other, CDT specific, activities. At the induction meeting we were tasked with giving a presentation and preparing a report on the Target Corporation financial data breach in 2013. We acted as a team of advisers to Target's board of directors and disseminated the technical details of the breach into language that could be understood by a non-technical board member. We then gave recommendations to the board to rectify the impact of the breach and prevent further breaches. This was an interesting task as it allowed us to work together as a cohort and apply our varied knowledge base to the problem at hand.

For the remainder of the first year I am looking forward to further exploring the subject of cyber security and hope that this will lead me to a specific idea for my summer project. I am enjoying learning new things and am looking forward to continuing this over the remainder of this first year in the CDT.

**Ashley Fraser**, first-year CDT student

# WISDOM

The WISDOM (Women in the Security Domain and/or Mathematics) group was set up in May 2016 to encourage diversity in the School of Mathematics and Information Security. The aims include supporting women by developing a network of female researchers, highlighting issues in the School where more could be done to encourage diversity, and encouraging more women to study in these fields, including creating an atmosphere that is welcoming to all.

Women are currently underrepresented in these areas, particularly at postgraduate level, so it's important to take a proactive approach in recruiting female students and to develop female networks of support.

We have organised activities such as a filmed Q&A session with Professor Averil MacDonald, a fascinating insight on STEM. We also enjoyed a networking lunch with our masters students. At monthly meetings we discuss issues relevant to diversity in the department and have interesting discussions such as the use of titles in academia, and provision for students or staff with children. We have also set up a WISDOM twitter account (@WisdomRhul), Facebook group and blog where we discuss what we have done, as well as our own perspectives as female researchers.

We have recently received EPSRC funding for improving diversity. Several ideas to use this funding include a conference with female speakers, hosting a student from a developing country for a research project and an event encouraging undergraduate students to stay in academia, as well as a networking event. We are also considering ways to encourage students from lower socio-economic backgrounds into academia. We welcome anyone interested to get involved with WISDOM and would love to hear your views and ideas.

**Lydia Garms,** second-year CDT student, and member of WISDOM (@WisdomRhul)

# Away from the Ivory Tower

**Students are expected to spend three months away from the CDT, on an industrial placement. This is typically done at the end of their second year, and gives them a fantastic opportunity to work on real-world problems in cyber security, where they can broaden their knowledge and potentially apply some of what they have learned during their CDT training. Read the experiences of three of our students.**

I spent this summer at Cloudflare. The company hosts a content delivery network that ensures websites perform better by distributing content across their points of presence worldwide; they also use their vast network structure to mitigate threats to website security such as DDoS attacks and spam generation. A considerable amount of work is also spent on developing novel cryptographic solutions to real-world problems that the company faces and this was the main reason why I wanted to spend my internship there. I worked within the cryptography team, led by Nick Sullivan, on a project to make Cloudflare protected websites more accessible to Tor users, spending time in both their London and San Francisco offices.

The project involved developing solutions that reduced the number of challenge pages that users of Tor would have to pass when navigating to such a webpage. Such challenge pages are usually represented in the form of CAPTCHAs that require the user to perform a task to distinguish whether they are actually human or not.

My work involved designing and implementing a cryptographic solution in the form of a blinded token protocol that allowed users to submit signed tokens instead of having to complete a CAPTCHA solution for each access, where a user receives these tokens after completing an initial solution. The blind aspect of these tokens guarantees that the tokens are not linkable on Cloudflare's side and thus anonymity is ensured.

The opportunities to work in rapidly growing companies such as Cloudflare on state-of-the-art cryptographic solutions are very few and for this reason I am grateful to be given this chance. Working at Cloudflare in particular allowed me an unparalleled insight into how cryptographic solutions can be employed in the real world. I intend to revisit these connections and the work I did in both an academic and an industrial context in the future.

**Alex Davidson**

This summer I completed an internship at VASCO Data Security Inc. – a NASDAQ-listed financial security firm headquartered in Wemmel, on the outskirts of Brussels. The company is recognised for its multi-factor authentication and electronic signature products, as well as mobile app security and risk management solutions.

I worked within the VASCO Innovation Center, which is responsible for envisioning new product areas and creating prototypes and intellectual property accordingly. I worked specifically on risk management for the Internet of Things, namely methods for forecasting future security risks on financial services, such as insurance, blockchain-related products and frictionless payments. I was exposed to various standards for threat modelling and risk assessment which I hadn't used previously on the CDT.

I was slightly apprehensive initially, since I knew neither of the languages spoken in the Brussels region – Dutch and French – other than *'hallo', 'tot ziens'* and the myriad of French phrases we use in English. However, this was put at ease immediately after arriving: Brussels is very accessible for newcomers!

I thoroughly enjoyed my time and I remain in contact with those at VASCO. I already find that my internship is informing the research I'm currently conducting at the CDT.

**Carlton Shepherd**

This summer I completed an internship at NXP Semiconductors at their offices in Leuven, Belgium. For three months I worked on extending a side-channel analysis tool that was originally developed by a previous intern a couple of years ago.

Side-channel analysis is a powerful attack that is a major threat to many of the devices that are deployed in settings such as transport ticketing, payments and many more. Being able to detect the presence of side-channel leakage is important to anyone wishing to produce secure hardware. Before starting at NXP I thought I had a fairly good understanding of the topic, but I learned that performing the attacks requires far more knowledge than just understanding them. Definitely a case of theory vs practice in action!

I found the internship to be a great opportunity to work on some real-world security problems and to work on a tool that is in use today. It was a big change to be working on research in industry instead of the academic setting at Royal Holloway; I enjoyed the opportunity and found the experience invaluable.

**Robert Lee**

# CDT News

## Hunting your Academic Research

Earlier this year I had the privilege of taking part in the second series of the television show Hunted, which was recently broadcast on Channel 4. The show featured 10 members of the public (Fugitives), charged with the task of going on the run and evading capture for 28 days. Opposing them were a number of experts (Hunters) who could use the 'powers of the state' to track them down. I worked in Hunted HQ as the Lead Analyst amongst the Hunters.

We utilised several different sources of intelligence to help with this task, each of which made a unique contribution to the investigation. These included technical Intelligence such as CCTV and phone tracking, Open Source Intelligence such as information from Social Media accounts, Covert Intelligence acquired though hacking or bugging and Human Intelligence acquired from members of the public. Each of these sources was crucial but also varied in its precision, accuracy, coverage, timeliness and analytical effort. CCTV for example could provide us with an accurate and precise location of a fugitive but CCTV coverage in the countryside is poor and can only be requested for precise areas. With Human Intelligence coverage is great as humans are spread widely throughout the country but the accuracy of the information can be doubtful.

The amount of data available to us was vast and intimidating so the process of navigating through that data relied on the skills and experience of the Hunters. We needed to understand the attributes of each source, how they can be used together and how one piece of information can lead to another. We usually started with a broad search, wading through masses of information looking for elements of interest to focus in on. As the search narrowed, we collected different sources of intelligence with different attributes until eventually we could hone in on our target. The process was difficult and often monotonous and it was easy to drown in data or wander off down false trails.

I found being a Hunter analogous to academic research. Research often starts with a broad interest and a researcher reads a large volume of papers before focussing on a specific topic. They might then study this in more detail before further developing their research by collecting new data. Just like for the Hunters it's easy to get lost in information overload and it's easy to pursue interesting but ultimately fruitless lines of enquiry. And like a Hunter, the researcher must pursue their goals doggedly but when they finally discover what they're looking for, they will have their reward.


**Steve Hersee,**
fourth-year CDT student

## CDT research newsbites

- **Andreas Haggman's** paper *Training day: Joint UK-US cyber exercise tests preparedness* appeared in the August edition of the Jane's Intelligence Review. Andreas was awarded the 3rd prize at the CyCon 2016 Student Award, issued by NATO Cooperative Cyber Defence Centre of Excellence at the 8th International Conference on Cyber Conflict, held in June in Tallinn, Estonia.
- **Joanne Woodage** was a co-author of the paper *Backdoors in Pseudorandom Number Generators: Possibility and Impossibility Results*, which she presented at the CRYPTO 2016 conference in Santa Barbara, USA, in August.
- **Suleman Ibrahim's** paper *Social and Contextual Taxonomy of Cybercrime: Socioeconomic Theory of Nigerian Cybercriminals* accepted for the International Journal of Law, Crime and Justice.
- At the ACM Conference on Computer and Communications Security (CCS 2016) on 24-28 October in Vienna, Austria: **Alex Davidson** and **Gregory Fenn** were co-authors in the paper *A Model for Secure and Mutually Beneficial Software Vulnerability Sharing*, which Alex presented in the 3rd ACM Workshop on Information Sharing and Collaborative Security. **Amit Deo** presented his work *Prescience: Probabilistic Guidance on the Retraining Conundrum for Malware Detection*, written in collaboration with colleagues at Royal Holloway, at the 9th ACM Workshop on Artificial Intelligence and Security. Finally, **Torben Hansen** presented his paper *A Surfeit of SSH Cipher Suites*, also written in collaboration with colleagues at Royal Holloway, at the main conference and received one of the CCS 2016 best paper awards!
- **Thyla van Der Merwe** was the co-author of the paper *Proactive and Reactive Standardisation of TLS*, which she will present at the Security Standardisation Research (SSR 2016) conference, to be held in Maryland, USA, in December 2016.
- **Giovanni Cherubin's** paper *Website Fingerprinting Defenses at the Application Layer* (with co-authors from KU Leuven) will appear in the Issue 2 of the 2017 edition of the journal Proceedings on Privacy Enhancing Technologies. The paper will be presented at the Privacy Enhancing Technologies Symposium in Minneapolis, USA, in July 2017.

7573 11/16

EPSRC
Engineering and Physical Sciences Research Council

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