CDT Newsletter

Information Security Group

EPSRC Centre for Doctoral Training in Cyber Security

April 2016

CDT Director update

It is hard to believe, but Royal Holloway's CDT in Cyber Security is celebrating three years this month! Since its launch in April 2013, we have recruited 31 students, who are now working on a wide range of research topics, including software security, cyber crime, cryptography and geopolitics of security. Setting up and running the CDT in these past three years have been demanding tasks, but also truly rewarding. The CDT has been a huge success! It has without doubt greatly enhanced the research environment at Royal Holloway. It has also opened several new opportunities for business engagement, and feedback from our external partners in industry and government indicates the great value of the CDT to them. In this newsletter, you can learn more about the research and experiences of some of our CDT students.

The establishment of the Centres for Doctoral Training in Cyber Security was one of a number of initiatives supported by the UK Government as part of the National Cyber Security Strategy, published in November 2011, which had as one of its fundamental goals to develop in the UK the "cross-cutting knowledge, skills and capability" required to support all other cyber security objectives. The UK has been a leader in engaging players from industry, government and academia to create a vibrant and innovative cyber security sector. We are confident that, despite its early age, our CDT has been making a small but noteworthy contribution to this effort.

If in 2011 it was already recognised the crucial importance of cyber security to modern society, this is even more pronounced today. Cyber Security is now frequently featured as front-page news, from reports about high-profile data breaches at UK businesses to the rise of economically-driven cyber crime to the essential debate on the use of encryption to protect digital communication. Citizens can no longer ignore cyber security in our ever-increasing networked world; it will remain a critical aspect of our society in the years to come, particularly with the expected adoption of ubiquitous computing and IoT devices. The need for professionals with leadership and critical thinking skills – in addition to the more conventional 'technical' skills – will be even more pronounced. We are convinced that our CDT students truly have the potential to become leaders in their fields.

In the past three years we have been working diligently with our partners in the industry and government to provide the students with a well-rounded education in cyber security, and develop their specialist skills in an area of the utmost importance to society. Students in all three cohorts have been kept very busy, and the results are exceptional: you will read in this newsletter about the experience of new CDT students putting their heads together and working on their first task in cyber security, and how students used their creative skills to convey the impact of modern security technology to the wider society. You can also get an insight of inter-disciplinary cyber security research being carried out by our students, and the impact that CDT research output is having in the real world.

We are expecting the new National Cyber Security Strategy to be published this spring, with cyber security remaining a top priority for the UK Government. With its many challenges and opportunities, cyber security continues to be a very exciting field to work on. The CDTs in Cyber Security present an exceptional opportunity for some of the country's best minds to be actively involved in cyber security academic research and education. We are now recruiting for a new CDT cohort to start their studies in the autumn, and are looking forward to continuing to work with our partners in the industry and government in training the next generation of leaders in cyber security. In the meantime, I hope you enjoy reading this newsletter.

Professor Carlos Cid

Follow us on Twitter at @RHULCyberCDT

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Inside the cohort

I am now in the third year of the CDT, and have finally reached the stage where I have a structure, methodology and theoretical framework for my thesis that I am happy with, and so can now actually begin writing it.

In September last year I presented my paper 'Language in the Age of Algorithmic Reproduction' at the Royal Geographic Society (RGS-IBG) annual conference at the University of Exeter. The full version of the paper, which uses the framework of Walter Benjamin's famous 'Work of Art in the Age of Mechanical Reproduction' to explore the effect the search engine industry has on language and discourse, is now under review with an academic journal. I also had the opportunity to present a seminar on this topic at the inaugural Prometheus Project event at the University of Warwick in October. The event, which brought together interested parties from industry, intelligence and academia, had been convened to consider the 'human capacity for agency within the cybernetic system of the twenty first century'. It was a very different audience to the ones I am used to, but the event itself was extremely interesting and a great opportunity to share and discuss ideas outside of a purely academic setting.

In March 2016 I made a presentation at the Association of American Geographers (AAG) annual conference in San Francisco. My paper was part of a panel on 'The Geographies of Software', and will hopefully form the basis for the first chapter of my thesis. In it I will be imagining the concept of digital space as being 'populated' or 'socially constructed' by the words and language that make up the corpus of web data. By conceptualising digital space in this way, I can then develop geographical, linguistic and even philosophical theory to think about how and why different actors 'tactically' hide, expose or manipulate linguistic data within these spaces, and the potentialities and consequences this may have on language.

Also in March, I co-hosted 'Being Human/Human Being', a screening and discussion panel event in London as part of the academic film society Passenger films. We showed Alex Garland's 2015 film 'Ex Machina' and hosted a panel of invited academic speakers that discussed issues such as ethics, morality and law which surround the concept of Artificial Intelligence, questions of gender, and representations of virtual, imagined, digital and physical spaces which the film provokes.

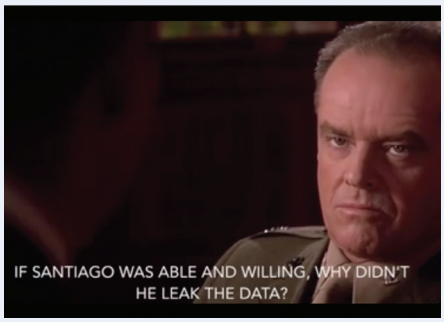
As well as starting writing my thesis, I have been trying to use my blog Linguistic Geographies to articulate some of the ideas which come up in the course of my research which either need further development, or are peripheral to the thesis itself.

Pip Thornton, Year 3 Student

Solving Old Problems with New Solutions*

What happens if we take famous old problems and try and fix them using new solutions? If we give historical figures the technologies and security practices we have today, things might have been different for them. After all, most 'old' problems have modern equivalents, and we would hope that new technology would fix some of the disasters that happened.

Take Romeo and Juliet. Giving them smartphones would mean they could communicate more easily without needing to go loitering under each other's balconies. They could have used messaging apps that claim secure end-to-end encryption to stop them worrying about their families intercepting messages. Brilliant! ...Unless



of course Juliet's message to Romeo telling him about her plan to fake her own death still doesn't go through. As could happen if Romeo's phone were to run out of battery. Or he wasn't with his phone. Or one of them lost signal. Or network delays withheld the message...

Consider Macbeth. Instead of aspiring to become king of Scotland, a modern Macbeth could be trying to become CEO of a company. Instead of using murder to rise to power, he can coerce people to step down using extortion, for example by accessing their browser histories and blackmailing them. He wouldn't necessarily have to do this in person so could keep his dirty tactics hidden, unlike in the past when the bloody trail left him in suspicion. Furthermore, in comparison to having to cause physical violence, both Macbeth and Lady Macbeth can emotionally distance themselves from the crime they are committing and not feel so guilty, and Lady Macbeth won't commit suicide. Whilst this ends better for the Macbeths, it leaves the question as to whether it's now easier for a psychopath to become 'King' of Scotland.

Or what about Mary, Queen of Scots, whose famous use of a bad cipher meant that her plot to overthrow Elizabeth I was revealed, so that she and her conspirators were executed? Now that we have better cryptography (which isn't broken using frequency analysis!), Mary's messages could have remained secret and she could have been successful. However, looking at it another way, Mary was under surveillance in the past as she likely would be with modern solutions in place. Either the state could have used their superior understanding of cryptography to read the messages as they had done before, or they could simply assume she had something to hide and force her to reveal the information. In fact, mass surveillance is even easier with new technology, so this could have been possible without Mary even being a political prisoner. ■

Ela Berners-Lee, Year 2 Student, based on the CDT presentation at the 2015 HP Colloquium.

*Whilst most people agree that modern technology has given us greater freedom of expression, technologies may be misused and have unintended consequences, and it's not clear we always understand repercussions.

Broadening Horizons

During my first few months in the CDT, my personal goal has been to broaden my horizons. Look away from mathematics, my background, and find other things in the field of cyber security that excite me.

When we were given our first task as a cohort, to answer the question 'What is cyber security?' I was given the opportunity to do just that. Throughout this task I was able to learn more about the various aspects that make up cyber security, in particular cyber warfare and privacy.

At first look, the task seemed to be relatively simple. It soon became clear, however, that there was a lot more in this question than met the eye. It was a much more intricate question than it first appeared.

It was for this reason that we abandoned our initial idea: a skit in the style of 'The Apprentice', in which one team was set to interview students on campus and the other would build a website.

In the end, we decided that it would be a better idea to focus solely on the website. It was more important that we expressed our answer to the question in a succinct way; to be as concise as possible, and to create something useful. The goal of the website, we decided, would be to build a tool which people of all backgrounds could use to learn about cyber security.

We started off by creating a 'mind map' of what we believed cyber security to be; we ended up with six initial topics, for instance cryptography, and then broke each topic down further into sub-topics such as key management. Each topic or sub-topic was represented by the node of a graph and any two nodes which are linked in some way would be connected by an edge.

It was clear from our mind map that we had not covered the field of cyber security exhaustively, and we viewed attempting such as unrealistic. It represented our perception of cyber security and we were happy with the structure.

When our mind map was fully built we had a total of 22 nodes with various edges in-between. We decided to build the website to match our mind-map: in the form of a graph. Clicking on a node redirects to a page with a short summary of the topic.

In the future we see this website being added to and improved. Perhaps it could even take the form of a repository, which can be edited or contributed to by anyone who visits.

It is certainly the case that in the few months since this task was initially given to us, our view of cyber security is more well-rounded. Indeed, it would be interesting for us to attempt this task again now and see how our perception of cyber security has changed: a true measure of horizon-broadening. ■

The website is currently live at: **www.parsed.uk/WICS/index.html**

Benjamin Curtis, Year 1 Student

CDT News

Securing Internet Communication

TLS (standing for 'Transport Layer Security') is the *de-facto* world standard for securing communication over the Internet.

The TLS standard is undergoing a radical facelift. TLS 1.3 is The Internet Engineering Task Force (IETF)'s answer to the weaknesses in TLS 1.2 and the TLS Working Group is in the process of finalising its design. As part of its new 'analysis-prior-to-deployment' design process, the IETF has welcomed analyses from the academic community. In the spirit of contributing towards this new design philosophy, **Sam Scott** (a fellow CDT cohort member) and I teamed up with Prof. Cas Cremers and Marko Horvat of the University of Oxford to produce a symbolic analysis of TLS 1.3. A lot of the work was completed whilst Sam and I were interns at Mozilla, working under the guidance of Eric Rescorla, the editor of the TLS 1.3 specification.

In January of this year, Sam presented the work at the Real World Crypto conference held at Stanford University in Palo Alto, and at the end of February, I spoke on the subject at the TLS 1.3 Ready or Not (TRON) workshop in San Diego. The workshop, co-located with the Network and Distributed System Security Symposium (NDSS), brought together members of the TLS Working Group, academics and industry professionals with the aim of verifying the current the status of TLS 1.3 by attempting to answer the question: Is the TLS 1.3 specification ready to be released? The simple answer is 'no'. Our work, in particular, provides security guarantees for draft 10 of the specification but there is still much discussion surrounding proposed changes to the protocol. Our team is in constant contact with the TLS Working Group and we are in the process of updating our formal model to reflect these changes. Our work on draft 10 of the specification has been accepted at the IEEE Symposium on Security and Privacy and will presented at the conference in May. ■

Thyla van der Merwe, Year 3 Student

CDT research newsbites

- **Conrad Williams** was a co-author of *Obligations in PTaCL*, which was presented at the 11th International Workshop on Security and Trust Management, in Vienna, Austria, in September 2015.
- **Pip Thornton**'s paper *Diary of a Plastic Soldier* was published in the journal "Critical Military Studies" in March 2016.
- **Giovanni Cherubin** was a co-author of the paper *Hidden Markov Models with Confidence,* which he will present at the 5th Symposium on Conformal and Probabilistic Prediction with Applications (COPA), in Madrid in April 2016.
- **Sam Scott** and **Thyla van der Merwe** had their paper (co-authored with collaborators from the University of Oxford) *Automated Analysis and Verification of TLS 1.3: 0-RTT, Resumption and Delayed Authentication* accepted at the 2016 IEEE Symposium on Security and Privacy, one of the world's top-ranked annual security conferences, which will be held in May 2016 in San Jose, USA.
- **Robert Lee** and co-authors from RHUL had their paper *Binding Hardware and Software to Prevent Firmware Modification and Device Counterfeiting* accepted at the 2nd ACM Cyber-Physical System Security Workshop (CPSS 2016). Rob will present their work at the workshop in China in May 2016.
- **Suleman Ibrahim** will be presenting his paper *Socioeconomic Cybercrime Theory of Nigerian Cybercriminals* at the 4th International Conference on Cybercrime and Computer Forensics (ICCCF 2016) in June 2016 in Vancouver, Canada.

743004/16

EPSRC
Engineering and Physical Sciences Research Council

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

@RHULCyberCDT