CDT Newsletter

EPSRC Centre for Doctoral Training in Cyber Security

March 2023

CDT update

Director's Report

Since the last CDT newsletter in Spring 2022, the return of more in-person events has made the CDT livelier, with more activities and a more energised research environment – both on and off campus. Indeed, the return of in-person events has been a breath of fresh air, and it has been nice to see more people back in the office, attending reading groups and discussing individual and joint research ideas and projects. This is what the CDT has always been about: engaging within and across cohorts. This renewed energy has also translated into our CDT social events, and I would like to extend my appreciation to everyone who has organised and attended these events to make them enjoyable.

Over the last few months, we have also welcomed external visitors again, to share their insights and experiences from industry and government in particular. We have gone back 'on the road' and resumed our visits to external partners. The intention behind the CDT has always been that we would be outward-facing and engage with the wider cyber security community, both 'at home' and 'away'. Hopefully, this will continue to create opportunities for discussions and collaborations within and beyond academia. CDT students have also participated in international conferences and external events, and with fieldwork being possible again CDT students have carried out diverse research in far-flung places such as Svalbard, Nigeria and Lebanon, to mention a few, in the last few months.

We have hosted workshops and events, which are a great way to showcase the fantastic research carried out by CDT students and to remind people of the diversity of exciting work that is done in the CDT. For example, in November last year, we had a great event at

Roehampton, where we welcomed many external attendees as well as CDT graduates for a lively day with a range of talks from current CDT students, and ending with tea and cake! In December, the first-year CDT cohort presented their individual summer projects during lightning talks at the 33rd HPE Colloquium on Information Security, while other CDT students presented posters to a diverse audience from within and beyond academia – all of this despite the snowy and icy conditions.

CDT students were back at Roehampton in March this year, this time for a one-day for-students-only away-day. The event was an opportunity for the different cohorts to get together to share their research experiences and PhD journeys, with invaluable insights from recent graduates Ela, Laura and Nick. A huge thanks to them for joining the current cohorts and offering advice based on their own experiences! All done in "a relaxed atmosphere" according to the Royal Holloway Cyber CDT Twitter feed.

While this would, of course, all have been possible in some form in a virtual set-up – as we now know all too well from the last few years – it just doesn't beat getting together in one place, discussing and sharing research insights, results, experiences and ideas. Now, we're looking forward to the CDT showcase event which will take place at Cumberland Lodge in Windsor in April and where CDT students will present their individual and joint work.

While this update has focused on the return of in-person events, I also want to congratulate CDT students on the many and diverse achievements and successes in the last year – many of which are reported in this newsletter. Finally, I want to end with congratulating everyone who has graduated from the CDT in recent months. The list is pretty long and I'll refrain from mentioning individuals, but

I look forward to following your post-CDT journeys!

Dr Rikke Jensen

Nebuchadnezzar: Entering (and Exiting) the Matrix

A retrospective on my first year and a half of research.

Dan Jones

I am still working on the 'Summer' project I started at the end of my training year. Whilst I believe this is a common occurrence in the CDT, it can still be an occasional source of anxiety!

Before I explain what's taken me so long, I'll quickly explain the project. I worked with my now supervisor, Martin Albrecht, to study Matrix, a protocol for end-to-end encrypted group messaging (think WhatsApp group chats). The protocol has over 80 million users, and is well used among the open source and free software communities as well as several governmental organisations. They have a presence in government organisations within France, Germany and Sweden. This includes healthcare services and, in the case of Germany, their military.

Our initial goal was to analyse the protocol. We would study it, precisely define its intended security goals, then determine whether it fulfils those goals. It's in the final step that we attempt to write a security proof. This would be the first time I would work on a cryptography project and I was excited to give it a go.

Development of Matrix started in 2014, meaning that its design is relatively straightforward (cryptographically speaking). Especially when compared to modern group messaging protocols, such as the IETF's forthcoming Message Layer Security. It seemed like the perfect candidate with which to cut my cryptographic teeth. What we did not expect, however, was the breadth of the protocol. We soon realised that covering the whole protocol in the summer project was not feasible. Instead, we decided to focus on a single component: the Megolm ratchet. By the end of the summer we had a formal description of the Megolm ratchet, a precise definition of its security goals, and a proof that it fulfils them.

As I transitioned into my first year of research, Martin introduced me to Benjamin Dowling[1] who soon joined the project. With one more person on-board (and some added expertise) we got started on a more complete analysis of the whole protocol.

Our first job was to synthesise the various specifications and documents that define it into a single precise description; this would form the basis of our analysis. In addition to documentation, the Matrix foundation also provides libraries to help others develop new software using the protocol. This proved a useful source for resolving ambiguities in the specification. It is sometimes the case that the secure way of completing a task is left implicit in written specifications; checking the source code is an easy way to double check our interpretation.

It is at this point where the project went a little off-track. We found several points of ambiguity in the documentation that could lead to security issues if implemented incorrectly. When we checked the source code, our hunch was right. There was a vulnerability! And another! Before long we had found six potential vulnerabilities: some in the specification, others in the source code. Often their root cause sat somewhere in-between.

Being a newbie, I wasn't particularly confident in these findings (thinking such things as "Maybe I've just misunderstood the code?"). To quell these thoughts, we created proof-of-concepts for the more intricate attacks. That is, we implemented each attack in code, spun up a test server and ran the attacks.[2] After verifying they worked, we disclosed our findings to the Matrix development team. During this time, we were contacted by Sofía Celi[3] who was also studying Matrix and had found a similar set of issues. We joined together, collated our findings and disclosed the new vulnerabilities to Matrix. This work turned in to my first paper and has been accepted to the 44th IEEE Symposium on Security & Privacy.

It turns out that there can be a lot of public relations work involved when disclosing security vulnerabilities. After we agreed upon a public release date with Matrix, we prepared an explanatory website and even emailed a few journalists we thought would be interested. This is not something I would have thought to do, but my more experienced co-authors certainly did. Thanks to them this work was picked up in more places than I could have imagined and led to a bunch of new opportunities. It was featured in Ars Technica (syndicated to Wired) and The Register. We were fortunate enough to be invited to speak at Blackhat Europe, an IETF meeting and we even made a podcast appearance.

During much of this time, work on our analysis of the protocol was mostly stalled. This is something I was worried about. In fact, I initially resisted investigating these attacks to ensure we finished our analysis work first. In hindsight, going off-track to follow a lead was the best decision we could have made. All of this is to say, having the time and freedom to pursue new and interesting ideas that come up is a rare privilege that pursuing a PhD gives you. Use it!

Regarding the original project, you'll be pleased to know we have completed our security analysis of Matrix and thus, my summer project is now complete. Well, almost...

[1] Now a lecturer at the University of Sheffield, Benjamin Dowling was previously a post-doc at the ISG!
[2] The attacks were tested on local copies of the server and client software. Not in the real world!
[3] Sofía Celi is a cryptographer at Brave Software.

Digital Security in Latin America

Early Perspectives on Establishing a Research Group

James Barr

"Some other countries are struggling, such as Mexico. They need to tackle crime, not cyber security."

"The price of Chinese technology is much more accessible compared to European or American companies. Paraguay does not produce any technology."

"In Latin America we can confuse some platforms with the internet itself. The experience of going online is through social media apps, this is a challenge."

"Latin America is the most peaceful region regarding interstate conflict and most violent in interpersonal conflict and/or violence. We have to shift focus more towards everyday violence and the use of technology to oppress people."

These quotes, captured in a workshop held by the Digital Security in Latin America Research Group (DLSA) in December 2022, illustrate a very important (if sometimes overlooked) point: the importance of context. By context we refer essentially to how the digital relates to, shapes, and is shaped by the on-the-ground realities emergent in a specific time and place.

Sofia, Jess and I are all social, broadly qualitative researchers by background, with a strong interest in Latin America. In early 2022, we started to chat about our research ideas, proposals and plans. In doing so, we began to note some rather intriguing themes. For instance, although some literature existed on issues of digital security in Latin America, it was somewhat limited when compared to a relative abundance written around other regions such as the USA and Europe. Secondly, whilst interesting work was emerging from and on Latin American digital security, much of it has been relatively siloed (though this in fairness is a typical issue across all of academia). Indeed, our chats often led to light academic crossover, where gaps apparent in one field had already been addressed in another - we just needed pointing in its direction.

This got us thinking. What do we need to research? How can we start to bridge the gap between disciplines, and explore the interplay between these various approaches in the context of Latin America specifically? Then it came to us ... a workshop would be a vehicle to bring together people from across the disciplines and facilitate interdisciplinary dialogue! Great stuff! Indeed, we soon realised that a workshop could, in the longer term, facilitate a research group. Even better! But then, reality quickly hit us. Before considering that lofty research group-based ambition, we first had to address a rather pressing issue: how do you organise a workshop? Though we had some ideas, we thought it best to start by consulting Professor Google.

After a few weeks, we started to make headway. Initially, progress was made through reflections on our own experiences at workshops, and simple chats with more experienced heads versed in the art of workshop design. They pointed us to certain people, who pointed us to other people, and over time we developed an idea of what needed doing. This included:

- Planning a theoretical workshop session, including some starter questions and themes for keynote speakers to address.
- Finding some keynote speakers to attract the masses.
- Making a list of potential participants with relevant expertise.
- Finding an online venue (being a workshop on Latin America, we ensured we could facilitate participation from researchers who are based in Latin America).

Of course, progression is never linear. It was challenging finding the right people to talk to. For instance, it took us far too long to realise that we should look to support from within the Royal Holloway CDT, particularly considering the weight of experience, and the CDT's interdisciplinary focus. Indeed, our own project reflected this latter ethos. Over time, with a bit of thought and elbow grease, we managed to pull together a surprisingly lengthy and strong list of names who, after a round of emails, were more than happy and indeed excited to attend!

So, we had the idea, the plan of action, the list of participants, and amazing keynote speakers. However, we quickly realised that we needed some extra hands to run the sessions. From moderation to note taking, we wanted the workshop to allow all participants a voice and for that voice to be properly noted down for a report. Those people were absolutely crucial in the smooth running of the workshop, and we could not have done it without them.

After months of planning and hard work the day of the workshop came.

Inside the cohort

We had two brilliant keynotes to prompt discussion, and it was a hugely productive session. We covered quite a variety of topics and perspectives, derived largely, we suspect, from the breadth of experience and backgrounds present at the workshop. There were plenty of insights from the workshop, as the report indicates, but some of the key points were as follows:

- There are many restrictions to researching cyber security in Latin America. Though more courses are becoming available, challenges remain as research areas remain siloed and there is little interdisciplinarity.
- Cyber security policy in the region is for the most part reactive. It draws from international best practices but is not always adjusted to fit the Latin American context.
- There exists a duality between Latin American approaches to cyber security and relationships with the west in shaping them. Partnerships with western states, and in turn the emulation of western state practice, are often seen as measures of cyber security maturity or capability. However, there also exists an appetite amongst Latin American states to pursue their own independent cyber security approaches.
- Processes of political change and the impacts that these have on issues of cyber security, must be understood against a broader backdrop of historical and current conflict.
- When it comes to the practice of cyber security, a divide exists between the policy and the grassroots level. Strategies and policies may satisfy international standards and requirements, but may do little to address local realities and concerns (what might be termed the cyber security of the 'everyday').

The report analyses these points in a more concise and nuanced manner. Some of the more subtle findings on the tensions between the emulation of western best practice, versus the want for independent cyber security approaches, were of real interest. This issue and the constant references to the need for everyday perspectives and approaches, calls which again reflect the motives of our own PhD programme, are something we think merit further inquiry. Moreover, it is fascinating to note that many of our initial conceptions around the state of the field were reflected in the comments of our participants: research is siloed and at times limited.

Pulling this workshop together was not an easy process, but it was a worthwhile one for the voices foregrounded, the people it brought together and as a means to generate new research (and hopefully further research opportunities). We plan to keep up the momentum and put together a few more workshops over the year, addressing some of the themes mentioned above, alongside short articles, blog posts and more. We will keep you posted!

Read our report: DSLA 03/23- Beyond the Usual Suspects (squarespace.com)
Follow us on Twitter DSLA_Research
Find out more about the research group
Contact: dsla.connect@gmail.com

2021 Cohort perspective on moving to research phase of their PhD

We are now at a pivotal moment in our PhD journeys: halfway through our second year and, thus, about halfway through our doctorate degrees. The transition from first to second year in the CDT has enabled us to build on the knowledge and skills we developed in our summer projects; in fact, it has been helpful to reflect on the successes and failures of our summer projects, allowing us to lay the groundwork for our PhD research.

The second year has brought us a better understanding of what doing a PhD constitutes. From an impossible (in the eyes of some of us!) project, it started splitting into smaller, less daunting stages. We are also starting to get to grips with our research areas, and even feel we can extend it in some directions. It is fair to say that we are far from being independent researchers, but we can now wade through the academic waters with some knowledge of what lies in their depths.

Whilst this has been an exciting time for developing new research, it has been a much quieter period as we have moved away from cohort-based work. We are lucky to capitalise on events like those at Roehampton and Cumberland Lodge to continue building and maintaining relationships across the CDT and with the external community.

We are also reaching out to other academic circles, becoming members of particular associations and laboratories. As such, we are now actively ensconcing ourselves and our work in the wider community, gaining new perspectives on our research and methodological practices. Some of us have begun attending conferences, summer schools, and workshops and even working on papers to submit to various academic journals.

We also continue to deepen our engagement at Royal Holloway. For example, some of our cohort have contributed to a new reading group—the Ethnography Reading Group—begun at Royal Holloway (see https://rikkebjerg.gitlab.io/ ethnography-group/reading-group/). This has been a wonderful space to build our own cross-disciplinary community where we discuss issues involved in ethnographic research from and with(in) security issues.

Other readings groups include: Crypto Chats, Quantum Seminar and the joint PQC seminar with ENS Lyon and CWI Amsterdam. In these, we are integrating into the groups of cryptographers, mathematicians studying quantum computers and theoretical computer scientists in and outside of Royal Holloway; these groups also continue to be stimulating and fun ways to build bridges and knowledge across borders and institutions. Furthermore, several of us have had the chance to conduct, or begin planning fieldwork, where we anticipate further on-the-ground research, whether in Beirut, in Svalbard, or in Thailand's cities.

We greatly anticipate the remainder of our PhD journeys and experiences of all the opportunities provided by the CDT at Royal Holloway.

Student journeys

Luke Stewart

Having now reached the end of the process, this is a good time to reflect upon my CDT and PhD experience as a whole.

I have separated out 'PhD' from 'CDT' for a reason. The CDT approach of a first year of learning within a cohort environment offers many advantages compared to a PhD solo venture. The interaction with fellow cohort members, and the ability to experiment with other areas of cybersecurity that I wouldn't otherwise have gone anywhere near, provided an experience that I believe is far more valuable than just the PhD research portion alone.

Something I didn't consider was how it would feel to actually finish the programme. By the time my viva arrived, I had already been in work for a number of months. Passing the viva was a strange experience – whilst it was somewhat anticlimactic (probably due to the fact I hadn't been working fulltime on my PhD in the run-up), something certainly felt different. It took a few minutes sitting in the car for it all to sink in!

Since the PhD, I have moved abroad and started a new job and qualifications in finance and IT. Whilst my current role may not be directly related to the subject of my thesis (applications of mathematics to key predistribution in wireless sensor networks, soon to be available in the library...), it has already benefitted me. Roles not open to others within the company have been offered, and there is a certain kudos that comes with being nicknamed "Dr Luke".

Despite not actually being at Royal Holloway for some time now (Covid hit partway through), in some ways I feel like I haven't left. I am still working on a paper which comes directly from my thesis, and I am looking forward to being there for the graduation ceremony in the summer. I really do miss it, even if I didn't always know that would be the case whilst I was there – whether that's the interaction with fellow cohort members (this is still going in some ways, even if we mostly now just congratulate the latest person to pass their viva on WhatsApp!), or the nature of PhD life. It can be difficult at times, but it's very different from a regular 9-5. My one piece of advice to current students would be – treasure this experience whilst you can!

Jeroen Pijnenburg

My CDT journey began in September 2017 when I moved to England, and settled in leafy Egham, an otherwise quiet town in Surrey that is home to thousands of students, I was one of them..

The CDT management explicitly stressed we should use the first year to broaden our horizons and work on our skills deficit, rather than deep dive into our narrow field. For me, that definitely included improving my social skills and adapting to British society. So I quickly acquainted myself with all the different pubs in the area, where many Sundays where spent watching Spurs with the locals and betting on which team would score the next goal.

At the start of the PhD I was told that, ideally, your supervisor helps you a lot in the beginning of your studies and then `lets go' so you become more independent. I did not realise how literally I should take this advice until my supervisor announced he was leaving after the first year of my research! Half a year later the pandemic started and both my housemates then left and returned to their home countries. I felt very `let go'! At this point I found myself at a crossroads - I could either give up and return home to the Netherlands, or power through somehow. I ended up publishing three papers that year, so I guess it turned out alright for me.

I think we all reach a point, during a PhD, when you are stuck with your research problems and do not feel that you are making any progress. At such times it is natural to feel that you are completely on your own. However, it is important to realise that most PhD students go through similar moments (my supervisor sometimes referred to these times as the `mid-PhD blues'). Having been through the process, I believe these moments can define your PhD and are the moments when you `grow up' and achieve your independence.

A PhD is never easy and requires determination. I often said that, when doing a PhD, every day is the weekend, but you must work on the weekend! It was said not merely in jest, since it recognises both the fact that you can go for a walk in the Surrey hills on a Tuesday afternoon if you feel like it, but also that you are constantly thinking about your research on that walk. If you are stuck on a problem, it will follow you around like a dark cloud. But a PhD can be very rewarding. You can spend all week thinking about a problem and getting nowhere, but then feel amazement when you get a key insight on the top of Scafell Pike!

During my first year I learned that it is very important to know the right people, which can be difficult if you are new to the country. The CDT recognises this and encourages everyone to network and communicate their research. The interdisciplinary nature of the CDT also helped me prepare to connect with people outside my own research community. This is important because it is often the assistance of unexpected people that helps you advance. As an example, during my writing-up period I applied for many jobs and did not even get a response, which was a demotivating experience. However, a friend of mine forwarded my resume to their manager, who immediately invited me for an interview and then offered me a job. Fired with motivation, I subsequently wrote my entire thesis in two months after only managing the title page in the preceding four months! It is funny how things can work out...

In the end, I believe life is a combination of both skill and luck, but you can load the dice. Choices you make now that seem inconsequential may have unanticipated impact on the future, but you never know beforehand which choices matter. I would advise everyone to embrace every opportunity that presents itself, especially ones that connect with people. I think this is particularly true for opportunities that lie outside your comfort zone - like writing this article!

Eamonn Postlethwaite

It's a surprisingly difficult task to reflect on the almost five years of my life that my time in the CDT represents, and even more so given the extreme change in tone brought on towards the end of my studies by the pandemic. Although we were eventually able to celebrate together, many of us who submitted and graduated during that time completed our studies by sending a pdf, wandering around campus a few times, and then walking away. It felt like our PhD studies had ended with a slight whimper.

Student journeys

Nonetheless, I loved my time as part of the CDT, and the people in it, so let me do my best to pass on some wisdom to the PhD generations coming after me...

Firstly, and perhaps most importantly, never lose sight of the value of having so many fellow PhD researchers studying in one place. Having since moved on to postdoctoral research, I hear many descriptions of more standard PhD experiences, involving the carving out of some academically brilliant, but oftentimes lonesome, furrow. The CDT allowed me to carve out some kind of furrow (whose academic brilliance I leave to my peers to judge), but it was never lonesome. Make the most of your peers, as both friends and intellects.

Secondly, research is going to frustrate you far more than the promotional videos and pseudo-inspiring pep talks might make out. So when (not if) you get stuck, talk to anything that will listen to you about the problem that is vexing you, whether 'anything' is a peer, a tenured academic, or a pot plant! Even if you receive nothing more than a stupefied glare in response, this will help – believe me. And expect to find yourself in the reverse of this scenario, so be prepared to listen (or at least pretend to) and consider this exchange part of the academic social contract.

Thirdly, now that we are once again permitted to, travel, attend workshops whenever possible - these are the most fun and the most likely places you will actually learn something or meet future coauthors. Talk to everyone you meet and ask them all stupid questions with the skin crawling self-confidence of an entrepreneur, even if you feel like a fraud. And remember that if you have the capacity to feel like a fraud, you are probably less of a fraud than you think! Don't worry – research papers will come, in time, and soon you will find yourself with too much to possibly do or think about. Speaking of travel, go abroad, if you can, for your internship.

Finally, never forget that London is on your doorstep – it's a fun and happening city, so make the most of it. And, most important of all, be nice to Claire.

Internship experiences

CDT students are expected to undertake the equivalent of a three-month internship with an external project partner at some stage during their studies. This is an important aspect of the CDT as it introduces students to what life could be like post PhD!

Below we hear from four students who have recently returned from their internships.

Wrenna Robson:

Quantinuum

During the Winter of 2022-2023, I completed a remote internship at Quantinuum, a quantum computing company formerly known as Cambridge Quantum, based in the UK and US. While I am based in Manchester, the quantum cryptography team I worked with had members located in various locations, and remote work was the norm.

Although the work I did was not directly related to my PhD, which focuses on formal methods for cryptography verification, I acquired several skills that will prove useful in my future career, including experience with the Rust programming language. I had the opportunity to deliver two presentations to the team, one on my research and another on error reconciliation in quantum error correction, which I found fascinating to learn about. I received positive feedback on my presentation skills, which I attribute to my training at CDT, as well as the opportunity to deliver my second presentation in person at Quantinuum's London offices. I also had the chance to visit their Cambridge offices during an internal conference.

This internal conference was another highlight of my internship. I was able to meet the various teams within Quantinuum and gain insight into their diverse research areas and exciting research directions. There was a real feeling of a company pushing to innovate and expand the horizons of knowledge. Of course, a business must also make money, and the team I was working in is one of those that has produced one of Quantinuum's products that are available to external customers, Quantum Origin. This is a cloud-based service designed to supply cryptographic keys which are "quantum-enhanced" – what this means in technical terms is that they are produced from an entropy source that is verifiably truly random in a particular sense. One of the challenges for a knowledge-based R&D company is transforming into a profitable product-orientated company. Quantinuum is facing this challenge and observing how these problems manifest first-hand was very educational. However, I am confident that Quantinuum has the potential to become an extremely strong company with a bright future.

During my internship, I gained proficiency in Rust, which I had not previously used. I learned the basics of Rust and how to port a Python program, which has proven useful since returning to my PhD. My manager, Matty Hoban, was supportive of my learning and provided ample opportunities for growth. I appreciated working with Matty and gained valuable insights from him. I learnt a lot from Matty and I think he was really glad of the chance to work with me too. I brought a perspective to things that was useful to the team and we'd often spend time just talking through ideas to understand them. One of the challenges of quantum cryptography is that cryptographers and quantum information scientists speak very different languages in a sense, and learning to bridge that gap was a challenging process in a good way! One of the most interesting concepts I learned about was device-independent cryptography, which involves reasoning about quantum devices while knowing little about their internals. The idea of verifying the presence of quantum behaviour without having access to a device was unexpected and underscored the counter-intuitive nature of quantum thinking.

Overall, I am glad I completed the internship at Quantinuum, and I anticipate referencing it when applying for jobs after completing my PhD. While I am uncertain about whether I would personally work for Quantinuum in the future, I believe that they have the potential to become an exceptionally strong company.

Natasha Rhoden:

Clementine

After deciding that I would like to seek out an internship during the Summer of 2022 and receiving helpful advice from staff and students within the CDT, I reached out to tech founders of UK-based app start-ups. I created a shortlist of start-ups after identifying how I could leverage my understanding of digital accessibility gained through my PhD studies, alongside my practical psychology experience, to contribute to the quality of experience of their users. I also wanted to work with an organisation which aimed to contribute towards a social good, so I targeted apps focussed on mental health, the circular economy, and support for workers in the care industry.

Clementine, an app focussed on providing wellbeing support through hypnotherapy, was keen for insights around user experience ahead of an upcoming high street product launch. User experience (UX) research aims to improve understanding of the factors driving user behaviour and involves application of research methods to meet user needs through product design. My work with Clementine as an UX researcher centred around exploration of user interactions with the app, communication to users around protection of their personal data, and the effect of app functionality on users' ability to achieve their mental health goals.

I really enjoyed designing human-centred, qualitative research projects based on the brief I received from Clementine's founder and product manager. For instance, when combining semi-structured qualitative research with live navigation of prototypes and usability testing to develop user experience solutions. Despite this internship being remote, I had the opportunity to review my progress regularly within a small, tightly knit, and supportive team. I was also given the freedom to determine my own day-to-day tasks and independently solve problems to achieve broad objectives.

The most fulfilling part of this internship was giving feedback directly to the founder and decision makers on the

Internship experiences

product management team. It was extremely rewarding and satisfying to have my research valued, to the extent that I can see my functionality and design solutions within the latest version of the app. My internship has helped me to develop interview strategies which effectively prompt users to offer insights about their own human-computer interaction experiences. These strategies will be applied to my PhD fieldwork. This experience has motivated me to continue to work with a variety of social good tech start-ups in future.

Simon Philip-Merz:

IBM Research Europe

Last Summer, I had the privilege of doing an internship at IBM Research Europe in Zurich. The mission of the Zurich Lab is to pursue cutting-edge research related to information technology without the goal of generating revenue. In many cases the groups work on foundational research spanning a vast range of areas such as nanotechnology, atomic force microscopy and quantum technology. Many groups maintain a close relationship with ETH Zurich.

The research environment was not dissimilar to an academic one, with PhD students and postdocs also in the labs of IBM. I joined the 'Foundations of Cryptography' group for the summer under the supervision of Luca De Feo. We worked on multiple problems related to the design and analysis of new post-quantum cryptographic group actions.

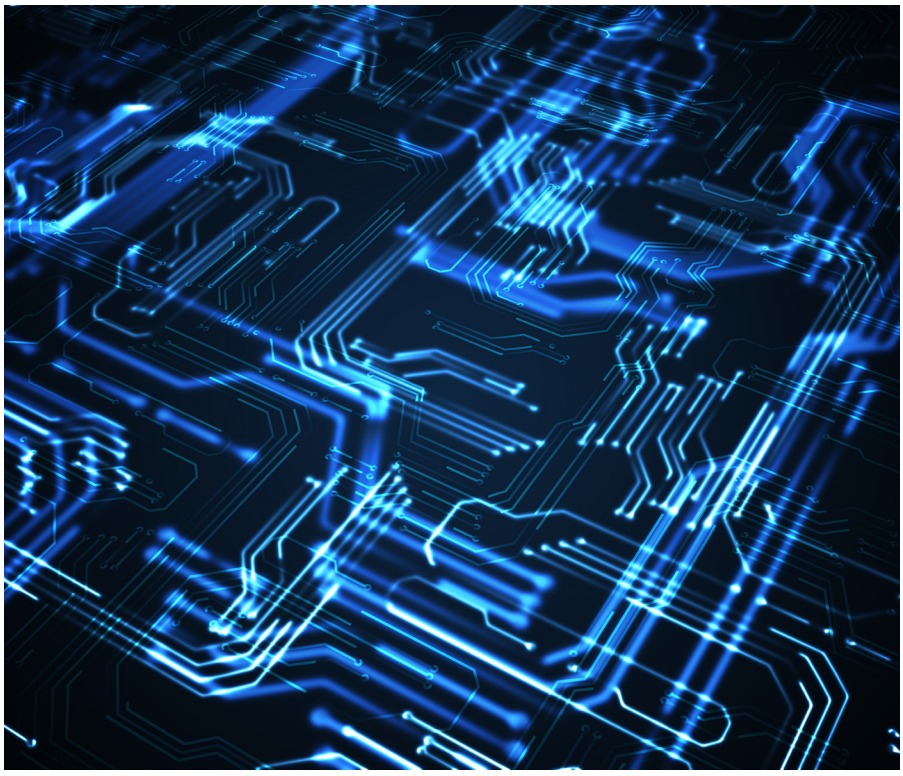
The researchers in the cryptography group were working on many interesting projects in a variety of directions, e.g. lattice- and isogeny-based cryptography, zero-knowledge proofs, and protocols. Moreover, they were a social crowd who made it a great pleasure to spend some months in Zurich inside and outside the lab. The great weather facilitated further wonderful exploration into the Swiss Alps.

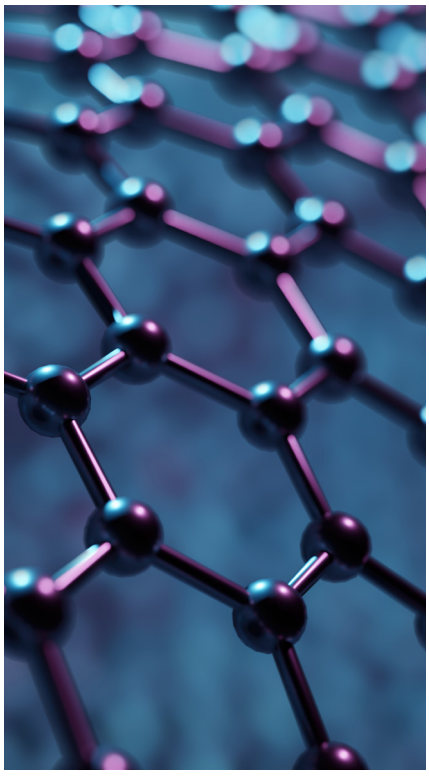
Erin Hales:

UK Health Security Agency

I completed a three-month internship in the Autumn term based at the UK Health Security Agency. I worked in the Environmental Monitoring and Health Protection team. This internship was part of the UKRI policy internship scheme, and so I took off my cryptography hat and got stuck into reviewing the latest literature to prepare reports on the most recent science for my team. The team I worked with primarily focused on wastewater surveillance, so it was interesting to learn about an area of science that is quite far removed from what I have worked on during my PhD. The same skills of needing to communicate new and complex ideas under pressure were very useful, but now I was communicating about something I had only just learned myself. Learning how to pitch things at the right complexity level to the different stakeholders involved a steep learning curve, and it was interesting to meet so many different people.

It was great to get a taste of life outside academia, and I was glad to practise my communication skills in a new environment. It was interesting to work as part of a much larger structure than my normal research group. I also got a taste for how government works, and got to see how government policy is formed. This was quite different to a more traditional industry-based internship, and also to the research visits that I've been on throughout my PhD. It was interesting to apply my skills to real-life problems, and also problems that I heard about in the news during the pandemic, such as wastewater monitoring of covid spread. Now I'm certainly at least considering a career in civil service once I've finished my PhD...





UK Cyber 9/12 Strategy Challenge

Tash Buckley

The UK Cyber 9/12 Strategy Challenge is an annual competition which sees teams of four take on the role of advisors to the Cabinet Office during a (fictional) escalating cyber-attack against the UK.

We've had many successes over the years in this competition, in which we've seen teams progress to the final stages and win on two occasions (2018 & 2021). This year, we're delighted that one of our students stepped up and coached to victory a mixed university team. Below, Tash Buckley tells us about this experience.

In February I had the honour and the pleasure of being invited to coach the fantastic team Krack-In Security for this year's Cyber 9/12 competition, a mixed university team made up of four students from Durham, Edinburgh, and St Andrews. I entered Cyber 9/12 as a competitor for Royal Holloway in 2020, coming in as finalists, and I got so much value from the experience that the next year I volunteered to be part of the organising team. It was brilliant to experience the competition this year in person again for the first time since 2020, and from a different perspective.

In the lead up to the competition students receive an intelligence brief containing a range of artefacts from news reports through to government communications. Their job is to digest and analyse the information to try and get a handle on what is actually going on. My role as the coach was to help develop their ideas and theories, and help to rein in some of the more out-of-the-box suggestions. With lots of hard work done up front, the team and I went to BT Tower in London to take part in the two-day event made up of a fantastic range of keynote speakers, interactive workshops, and everyone's favourite – the lock-picking station. The first round sees teams deliver a pre-prepared 10-minute presentation on their initial thoughts and recommendations, to a panel of judges from across government, industry, and academia. The teams then receive a thorough grilling from the expert judges, to really test their knowledge and rationale. Krack-In Security did fantastically well in the first round, working together brilliantly as a team, confidently handling the questions and absorbing the feedback that they were offered. The thing that really struck me was their confidence in their deductions.

At the end of the first day the teams that made it through to the semi-finals day were announced and I was very proud to see Krack-In Security were justifiably successful. The teams were given a second intelligence briefing, that takes the scenario off into new and, sometimes, unexpected directions. This time the team only had one, sleepless, night to create a new set of recommendations for the judges! This night is notoriously long and gruelling and really tests the team's abilities to work together. Thankfully they managed to get some sleep that night, although it is not unusual for teams to still be working at 3am. (I know!) Meanwhile, the coaches and guests from industry and government were invited to a fantastic dinner hosted by the Foreign and Commonwealth Development Office. The grand setting, the scale of the venue and the prestigious company, made this a night to remember, with amazing food and ample chances to network with a host of exceptional people. I felt a little guilty that while my team was slogging away, I was enjoying myself at the dinner, but not guilty enough to join them!

With bleary eyes, the competitors (and dinner guests), started bright and early with more keynotes and then the semi-final round. Krack-In Security once again did fantastically well under pressure as a team, and we were all very excited to find out that they had made it to the final three teams! The final round really ramps up the pressure as the teams are given 20 minutes to prepare their final recommendations, and they are kept in isolation until their turn to present. If that was not daunting enough, the final presentations and recommendations are delivered on stage, under spotlights, to the entire audience and a panel of VIP judges, which this year included Aurorah Cheney (-Co-director of strategy and growth at BT Security), Andrew McCosh (Group security director at BAE Systems), Trey Herr (Director of the cyber state craft initiative at the Atlantic Council), Bella Powell (Cyber Director at the Cabinet Office) and Pete Cooper (Deputy Director of Cyber Defence at the Cabinet Office). It is an intimidating experience I remember well from my time as a competitor. After the presentation there was another gruelling 10 minutes of questioning from the judges, after which they gave some constructive feedback on the performances.

I really could not have been prouder of the teamwork, the work ethic and the critical thinking I had seen from Krack-In Security over the two-day competition, so I was really excited for them when they were announced as the winning team! The late-night work I am certain will have seemed worth it when they received their prizes, a MacBook and a goody bag supplied by Rapid7 and individual career coaching supplied by BAE Systems. To round the competition off, there was a drinks reception on the 34th floor of the BT Tower, with stunning panoramic views of the entirety of London as the sun went down on the second day - a truly memorable experience.

Industry perspective

The CDT benefits from great relationships with a range of external partners, who support the centre in a variety of ways, such as inviting students on visits to their business premises, speaking at CDT events and hosting students on internships.

Below we hear from one of our partners who tells us what it's like to be involved with the CDT.

Stuart Murdoch

Surevine

Surevine have an association with Royal Holloway which stretches back to before Surevine was founded in 2008: one of our founders and a number of other Sureviners have studied at Royal Holloway.

Surevine's involvement with the ISG and, more specifically, the CDT programme, stems back to Surevine being one of the only SMEs to be a founding signatory to the NCSC's CyberInvest programme, which promotes industry investment into cyber security research in the UK, more specifically in the UK's Academic Centres of Excellence in Cyber Security Research (ACE-CSRs.) At the launch event in 2016, Surevine re-established a relationship with the ISG and the CDT programme, initially through Professor Carlos Cid.

Since then, we have worked together on a number of research proposals to be jointly funded by the NCSC, the first of which was on the 'Economics of Cyber Security Information Sharing: design and incentives', which at the time of writing remains an area of active research.

We have also been fortunate to have a standing invite to the annual CDT research showcase, the annual HP/HPE colloquium on information security, the CDT research presentation events, and since 2020, we have fielded one of the speakers at the annual cyber innovation session for the CDT. We are very pleased to be supporters of the bid for the next incarnation of Cyber Security CDT at Royal Holloway.

In addition, Surevine have been involved in the establishment of the UKC3 recognised Surrey Cyber Security Cluster (SCSC) which has active support from Royal Holloway. It was great to see a number of students at the first public event.

Surevine's involvement with the CDT has, I hope, been one of mutual benefit. Hopefully those at Royal Holloway benefit from our active support, whether that be in challenging current research students to understand the perspectives of and opportunities from industry, making useful connections and providing valuable experience for them, but likewise we gain the benefit of being able to have researchers consider those topics that we perceive to be the most valuable topics of applied research, and also to understand what might be the future state of the art in cyber security.

As Surevine, founded by an ex-Hollowegian, continues to grow through R&D driven work that matters, hopefully our ability to support Royal Holloway will continue to grow with it.

CDT Students Away Day

Emma Smith

On 7 March 2023, a CDT student-only away day was held at Roehampton University. The main purpose of the day was to enable students to share useful research tips with one another outside of the academic environment (and beyond the hearing of supervisors!). The day also provided an opportunity to listen to some of our alumni and hear about their experiences of the PhD journey. Since the pandemic many students have relocated away from the Royal Holloway campus, so the day also provided a rare chance to meet up with other CDT researchers and generally catch up.

Around 20 current students attended the event, representing the 2018-2022 cohorts. We were joined by three alumni, Laura Ship, Nick Robinson and Ela Lee, who all gave presentations about their time in the CDT. Their talks sparked a range of discussions, with everyone sharing their ideas on how to get the most out of the PhD. It was a great reminder that there are many important opportunities that we can explore whilst part of the CDT, outside of our academic work, to help us become better cyber security professionals.

Below, we hear from Sam Smith from the 2022 cohort who was one of the students who attended the Away Day.

When I heard the Student Away Day was being hosted at Roehampton, I knew I couldn't pass up another opportunity for their mini scones. But the day was so much more than just good hospitality, with the time being packed with truly useful insights from the CDT alumni and current students.

Throughout my time so far in the first year of the CDT, I've really enjoyed all the opportunities I've had to talk with students in the later years - getting their perspectives on various parts of the course, hearing about their research, and having the chance to ask 'stupid questions' to people who have been through it all already. So I found it incredibly useful to have a day dedicated to doing just that!

It was really interesting to hear about the experiences that the alumni had throughout their studies: attending conferences, going on internships, navigating supervisor relationships, managing personal working practices, and lots more. I personally got a lot from the discussions around how to approach the PhD while looking after yourself, with it really helping me to positively frame my outlook on the next few years.

I hope that events like this one can continue to run in the future, and if they do then I would highly recommend that everyone heads along. Whether that may be to pick up tips and advice, hear what others have gone through, or for a chance to share your own experiences. I'm certainly looking forward to the coming years when I might have useful stories of my own to tell, and to pass on all the great advice I've received.

CDT news

Celebrating graduation

The CDT always look forward to celebrating with our graduates, and since our last newsletter, we have had the pleasure to attend two graduation ceremonies for nine of our students.

Congratulations to all of you!

Dr Feargus Pendlebury, Dr Fernando Virdia, Dr Ashley Fraser, Dr Pallavi Sivakumaran, Dr Ela Lee, Dr Eamonn Postlethwaite & Dr Nick Robinson. (Summer 2022) and Dr James Patrick-Evans and Dr Georgia Crossland (Winter 2022)

2023 entry applications invited

We are now open to receive applications for students to start their PhD studies in September 2023. To be awarded one of the four-year fully funded studentships, candidates will need to have an undergraduate and/or masters qualification in a relevant discipline. Suitable backgrounds are (but not limited to) computer science, criminology, economics, electronic engineering, geography, geopolitics, information security, law, mathematics, philosophy, politics, psychology, software engineering and war studies. We will also consider applicants with a professional background, so long as they are able to provide evidence of demonstrable academic skills as well as practical experience. For more information on how to apply and a selection of potential research topics, see our website royalholloway.ac.uk/CDT

8902 04/23

UKRI Engineering and Physical Sciences Research Council

www.royalholloway.ac.uk/CDT
CyberSecurityCDT@rhul.ac.uk
@RHULCyberCDT

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