UCL CYBERSECURITY CDT

UCL

The Future of Cybersecurity:

Industrial / Academic collaboration with the UCL Centre for Doctoral Training in Cybersecurity

ucl.ac.uk/cybersecurity-cdt

The Big Picture

Cybersecurity is a 'wicked problem' — one that spills across disciplines, jurisdictions, and borders of all kinds. It requires individuals with skills that cut across multiple disciplines. Traditionally, cybersecurity practitioners are trained to be technically proficient but don't come with wider skills training or a broader industry perspective. It's easy to understand why: information security, computer science, cryptography, criminology, economics, psychology, public policy, and more combine to form the ecosystem within which cybersecurity problems and solutions are found; but training people to think and work across these boundaries has proven difficult.

The CDT in Cybersecurity brings together three UCL departments — Computer Science, Security and Crime Science, and Science, Technology, Engineering, and Public Policy (STEaPP) — to tackle the problem. The CDT has been established specifically to train high achieving, creative people to think differently and more expansively about cybersecurity problems and solutions. Our students are trained to cross disciplinary boundaries, communicate beyond their own fields, and comprehend the context in which others operate. This is a highly competitive programme that attracts outstanding candidates from all over the world.

How our industry partners benefit — what's in it for you?

Our CDT works closely with a range of partners to drive the most innovative research into complex cybersecurity problems. As a partner, you can benefit in the following ways:

- Accessing our doctoral researchers at an early stage in their training, for instance, by specifying a problem for them to tackle in their Year 1 dissertation
- Helping shape their PhD so that it is aligned with a problem relevant to your organization's agenda
- Providing access to real world expertise and, if relevant, co-supervision
- Providing internships during which our students can work on topics relevant to you
- Being first in line to recruit some of the brightest researchers in this field

Please contact us if you would like to discuss partnering with us.

How our industry partners contribute

Our partners contribute in many different ways. We are happy to discuss all types of input into the work of the CDT:

Research projects:
- Co-supervision of students and projects
- Input into shaping projects or Year 1 dissertations
- Funding of studentships.

Training and placements:
- Provide student placements and internships
- Provide training and workshops
- Participate in or provide events (e.g., poster competitions, career events) and brainstorming sessions.

Provision of technology and expertise:
- Access to relevant data
- Hardware, software, and support
- Site visits
- Guest lectures and teaching support
- Product testing.

Sponsorship:
- Sponsorship of our events or activities
- Hosting conferences.

Advisory Board:
- Participation in our annual review, providing strategic advice for the centre.

Our current partners comprise a spectrum of organizations across the private and public sector including

Amazon Web Services, **Barclays Bank plc**, **Cisco Systems UK, Cybernetica AS**, **Google Deep Mind UK**, **Hatdex Community**, **Kryptic PBC, Microsoft Research Ltd**, **UK National Police Chief's Council**, **UK National Cyber Security Centre**, **Privitar, Ripple, Spherical Defence**, **The Tor Project**, **The Alan Turing Institute**, **Veganetwork io**, **Creditmint**, and **Lloyd's Register Foundation**.

The Programme

Our 4-year programme provides students with knowledge including systems security, (cryptography, software security, network security, ecosystem security), crime science (cybercrime), and management and policy (information security management, security economics, ecosystem security, public policy). Our students work closely with industry to understand real-world needs and to develop the skills to work effectively within the sector.

In the first year of our programme, students undertake a number of taught modules across all three departments. This exposes them to different bodies of knowledge as well as a range of research methodologies. Students acquire knowledge that is conceptual, technical, strategic, and contextualized. It also provides the students with opportunities to work in interdisciplinary groups which is often their first step towards communicating effectively beyond their home discipline. This training continues into the later years, as students develop their theses and become independent cybersecurity researchers.

Real-world Impact

Our focus is on research that has the potential to impact the real world. As part of their work, many of our students produce 'policy briefings' — short, easy-to-digest research summaries — aimed at providing advice and understanding of critical issues to non-academic audiences. For instance, our students have produced briefings on:

- Cyberfraud on individuals — examining the facts and figures
- Security recommendations for consumer routers
- Good practices for cybersecurity behaviour-change interventions.

Year 1

In Year 1, students complete four compulsory modules plus one optional module.

The four compulsory modules are:
- Information Security Management
- Cybercrime
- Analytic Methods for Policy
- Philosophy, Politics, and Economics of Security and Privacy.

Students choose one optional module from:
- Computer Security 1 (a general introduction to security at an advanced level)
- Introduction to Cybersecurity
- Digital Technology and Policy.

Years 2 and 3

Students attend further elective modules and complete transferable skills training. We also encourage our students to carry out an internship within a partner organization.

Note: We do not organize the internships, but provide training and forums to help students connect with industry partners and the skills needed to interact effectively with them.

Year 4

Students focus on completing their theses. Students are encouraged to continue interacting with industry partners as they prepare for graduation and employment. Some of our students go on to positions with the organizations with which they have held internships.

Student Case Studies

Our students' projects range across the cybersecurity domain. For instance, current projects include:

- Detecting hate and analysing narratives of online fringe communities
- Explaining prosecution outcomes for cryptocurrency-based financial crimes
- Protecting the UK's News propagation systems against the threat of 'deepfake' injection
- Cyber-insurance: what is the right price?

We are always looking for project proposals that are of interest to industry and the public sector. Please contact us if you have such suggestions.

Student profiles

You can view profiles of all our students on our website at

ucl.ac.uk/cybersecurity-cdt/student-profiles

Working with Practitioners

So successful have our students been in this type of communication that they are routinely invited to non-academic forums to present their work.

For one example, our student Arianna Trozze, together with UCL Dawes Centre for Future Crime student Josh Kamps, delivered a presentation on cryptocurrencies to an audience of over 100 professionals from the UK Home Office as part of the Home Office's Future Crime / Changing World Series. This has led to further requests from around the world including police forces as far afield as the Dubai Police.

Why is UCL the best place for the Cybersecurity CDT?

The UCL Cybersecurity CDT team is led by the Department of Computer Science, which was **the top UK department by research output in the UK REF 2014** and which hosts research ranging from hard engineering, through AI, human-centred systems, systems and network sciences, information security, and more, to logic, mathematics, and philosophy. This breadth is complemented by UCL's Science, Technology, Engineering, and Public Policy Department — with its depth of expertise in public policy, both domestically and internationally — and the Department of Security and Crime Science, which brings crime prevention and futures thinking to the security perspective through the Dawes Centre for Future Crime.

The departments involved hold **active research grants worth £17.9M in cybersecurity**, funded by the EPSRC, Royal Society, EU H2020, ERC amongst others, including £300K of active direct financial gifts from industrial partners.

UCL leads the PETRAS project on IoT security (£9.5M) as well as its successor, SDTaP (£13M), the IRIS project on secure interfaces (£6.1M); the Glasshouses project on distributed ledgers (£0.9M); Cyber Readiness for Boards (£1M), ECSEPA (£250K) and BARAC on Algorithmic transparency (£0.6M).

The Department of Security and Crime Science hosts **the £7.4M Dawes Centre for Future Crime at UCL**, which focuses on understanding and addressing the changing nature of crime.

UCL is recognized by GCHQ as an Academic Centre of Excellence in Cybersecurity Research and Teaching.

Research Excellence Framework (REF) 2014, **100% of the Department of Security and Crime's research was rated 4*** in terms of impact.

UCL's Departments of Security and Crime Science and Computer Science also **contributes a secure data lab — the only such facility in a UK** university — which is police-assured to hold sensitive data classified up to the level of Secret.

For further information please contact the Centre Manager, Pui Sin, at cybersecuritycdt@ucl.ac.uk

ucl.ac.uk/cybersecurity-cdt

University College London, Gower Street, London WC1E 6BT

This CDT is funded by the Engineering and Physical Sciences Research Council (EPSRC)

UKRI Engineering and Physical Sciences Research Council