HM Government

Developing our capability in cyber security

Academic Centres of Excellence in Cyber Security Research



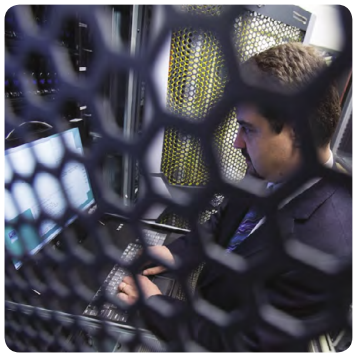












Updated July 2015

Contents

Developing our knowledge and capability to secure cyber space

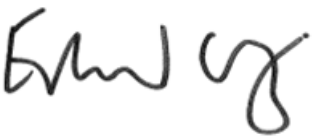
The world has become increasingly interconnected, with the digital revolution helping to deliver huge advances in freedom, knowledge, health, commerce and wellbeing. As we continue to rely ever more heavily on networked information systems, the security of those systems becomes increasingly important for citizens, businesses and governments.

The UK Government has responded to these challenges by developing the National Cyber Security Programme, a five-year Government and industry partnership backed with £860m of funding, to improve the security and resilience of the UK. By working with our international partners, the UK has also established itself in a position of leadership in cyber security. The UK has key strengths and capabilities in cyber security and many countries regard the UK as a preferred and trusted partner for cyber security. I am proud that cyber security is yet another area in which the UK research base excels.

To identify and promote these capabilities, the UK Government has recognised thirteen universities as Academic Centres of Excellence in Cyber Security Research (ACE-CSRs). Further information on these centres is detailed in this document, including the new centres at the University of Kent and University of Surrey which were recognised in March 2015. These Centres of Excellence form the backbone of the UK's world-leading cyber security research and will help develop the tools to secure digital technologies for consumers, businesses and Governments. It is crucial for academia and industry to work closely together and ensure the UK and its international partners benefit fully from the knowledge and expertise being developed. The UK Government is therefore playing a key role in making sure the relationships between Government, industry and academia enable us to achieve this. I hope our businesses and partners around the world are able to gain real value from the excellent work the ACE-CSRs can provide.

This work on cyber security is part of our wider effort to invest in research, support innovation and build the UK's knowledge and skills. These are key elements of the Government's long-term economic plan, helping to generate growth, jobs and ensure the UK competes in the global economy.

I would like to thank GCHQ and the Engineering and Physical Sciences Research Council (EPSRC), part of Research Councils UK, for the key role they are playing in the development of these Centres of Excellence, and the universities and staff themselves for their expertise and dedication to this hugely important discipline. I look forward to seeing the real-world applications of the centres' cutting-edge knowledge and expertise, and their contributions towards a secure, resilient and vibrant cyber space.



Ed Vaizey MP
Minister for Culture and the Digital Economy
Department for Culture, Media and Sport/
Department for Business, Innovation and Skills

Academic Centres of Excellence in Cyber Security Research

Academic Centres of Excellence in Cyber Security Research (ACE–CSRs) are part of the UK Government's National Cyber Security Strategy, *Protecting and Promoting the UK in a Digital World*. The strategy describes how Government is working with academia and industry to make the UK more resilient to cyber attacks.

The ACE–CSRs are based at UK universities which have been recognised as having an established critical mass and pedigree of good quality cyber security research. The initiative is sponsored by the Department for Culture, Media & Sport (DCMS), GCHQ, the Engineering and Physical Sciences Research Council (EPSRC), part of Research Councils UK, the Office of Cyber Security and Information Assurance (OCSIA) in the Cabinet Office and the Centre for the Protection of National Infrastructure (CPNI).

As the UK Government's National Technical Authority in Information Assurance GCHQ worked closely with EPSRC to lead the initiative to recognise the ACE-CSRs on behalf of the Government. GCHQ continues to actively manage the relationships and associated activities and collaborates with a range of organisations to ensure that the partnership between the public, private and academic sectors flourishes.

By recognising the ACE-CSRs, the UK Government aims to:

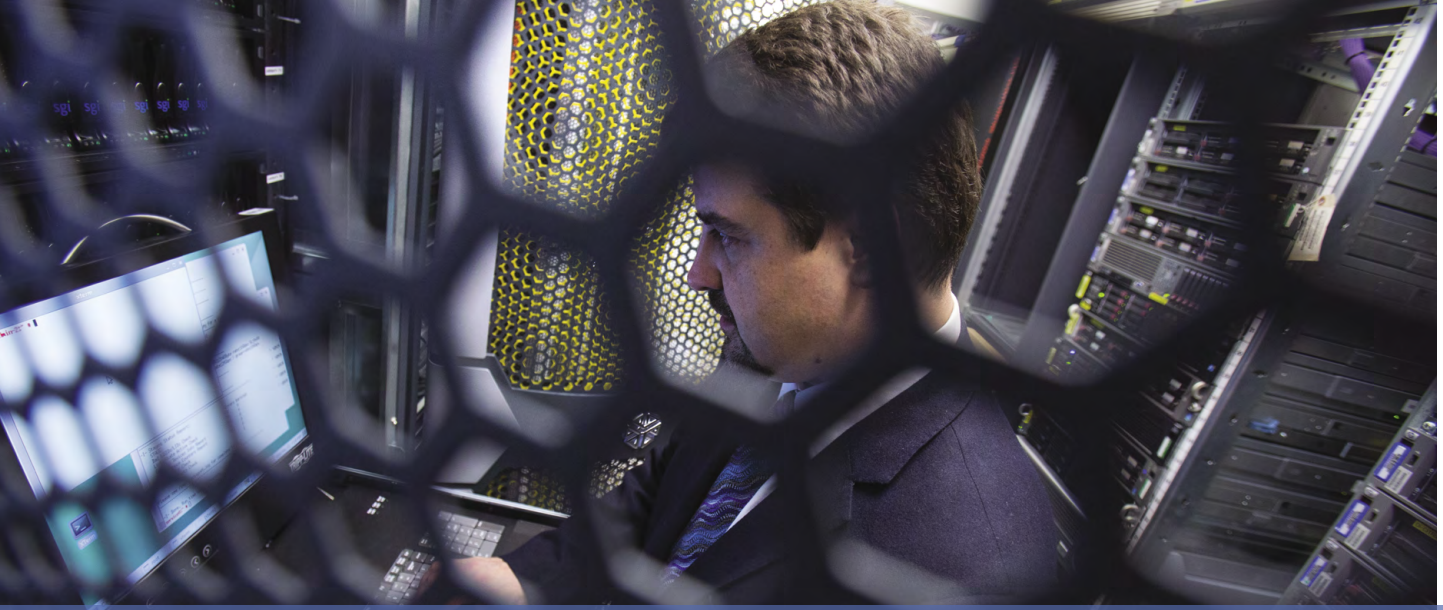
- enhance the quality and scale of academic cyber security research and postgraduate training being undertaken in the UK;
- make it easier for potential users of research to identify the best cyber security research and postgraduate training that the UK has to offer, and
- help to develop a shared vision and aims among the UK cyber security research community, inside and outside academia.

This document contains details of the thirteen ACE–CSRs and is intended to be a useful reference guide to help stakeholders and potential customers understand the broad range of work happening in the centres. Please contact the centres directly if you would like to discuss your research needs or find out more about what is on offer.

Key areas of expertise and specialism

Page	Name of centre	Key areas of expertise/specialism
6 – 7	Imperial College London	Engineering secure and resilient software systems, including: ● Operational systems and information assurance ● Security analysis and system verification
8 – 9	Newcastle University	● Cybercrime as a socio-technical issue ● Security assurance of infrastructures (e.g. identity, cloud computing) ● Science of cyber security
10 – 11	Queen's University Belfast	● Cyber physical systems security ● Real-time network analytics and virtualisation ● High performance/resource constrained cryptography architectures
12 – 13	Royal Holloway, University of London	● Theoretical & practical applications of cryptography ● Social, technical & organisational aspects of cyber security ● Information assurance & security for RFID tags, smart cards, mobile & embedded devices
14 – 15	University College London	● Human, organisational and economic aspects of security ● Secure software ● Malware detection ● Privacy-enchancing technologies ● Cryptology and cryptanalysis ● Financial security and virtual currencies
16 – 17	University of Birmingham	● Design of secure systems ● Security of embedded systems ● Cloud computing security ● Privacy technologies for individuals ● Network security and malware ● Analysis and verification of systems

Page	Name of centre	Key areas of expertise/specialism
18 – 19	University of Bristol	• Theory, design, implementation & analysis of protocols & systems that use (or relate to) cryptography
20 – 21	University of Cambridge	• Systems security • Network and operating system security • Security and human factors including psychology and usability • Security and privacy of mobile systems and social networks • Smart card and banking security • Cybercrime, frauds and phishing • Anonymity and censorship
22 – 23	University of Kent	• Identity management and authorisation, biometrics • Malware and vulnerability analysis • Formal methods and security • Digital forensics and steganography • Mobile and RFID security • Cloud security
24 – 25	University of Lancaster	• Resilience, with a key focus on resilience of networks, cyber-physical systems and studies of user behaviour in order to improve cyber security of large-scale socio-technical systems • Development of cyber security solutions that benefit the society at large, particularly vulnerable user groups.
26 – 27	University of Oxford	• Analysis and verification of software and security protocols • Systems security; trustworthiness and usability • Inter-disciplinary cyber security, policy and governance
28 – 29	University of Southampton	• Analysis & design of trustworthy software, bio & cyber metrics, cyber identity, cyber risk analysis • Cybercrime, data privacy, international cyber law, provenance and trust • Safety & security by design, secure embedded systems, secure web technologies
30 – 31	University of Surrey	• Systems security and reliability: formal analysis and verification, protocols, applied cryptography, human factors • Digital forensics, cybercrime and criminology • Secure communications: networks, mobile, satellite, 5G



Imperial College London

Engineering Secure Software Systems

Who we are

The Imperial College London ACE-CSR focuses on the engineering and design of secure and resilient software systems, addressing security issues both early in the design cycle through formal analysis and verification, and during its operation through maintenance and system adaptation. The ACE-CSR comprises 17 members of staff across three College departments covering a broad research portfolio that focuses on methods, tools and techniques for Engineering Secure Software Systems. Over the last five years, members of the Centre have supervised over 53 doctoral students, published over 158 reviewed papers on topics within the Centre's interests and have held grants totalling over £25m of funding from a wide range of sources, including EPSRC, the European Union, industry and defence. Several further associate members bring in additional expertise in specific areas. The Centre is led from within the Institute for Security Science and Technology (ISST), which coordinates and applies interdisciplinary and cross-departmental research and innovation to national security and resilience.

Imperial College London

What we do

Broadly, the activities are grouped in two research themes that concern:

Security Analysis and System Verification – The security and reliability of a software system depends upon the correctness and robustness of its component parts and of the system behaviour as a whole. Work at the Imperial College ACE-CSR has focused on formal techniques for characterising and verifying the system behaviour at design time, but also within the context of web and cloud environments that rely on the sharing of programs. Imperial's research covers: Static and Probabilistic analysis; Secure Web Programming; Symbolic Execution Tools that can characterise inputs that exploit software vulnerabilities, and Protocol Analysis and Formal Verification.

Operational Systems and Information Assurance – The security and resilience of systems depend on their design and implementation, but also on their ability to enforce the security policy, to adapt to changes, and react to attacks. In addition to detecting intrusions and anomalous behaviour, systems must be able to operate in their presence whilst taking into account risk trade-offs of damage versus functionality. Imperial's research covers:

Access Control and Authorisation Management; Secure System Adaptation; Security in Cyber Physical Systems; Intelligent Network Protection; and Data Centric Security. Work in this area also includes techniques for hardware-based acceleration of policy enforcement, cryptographic algorithms, and hardware security mechanisms.

Both themes are applied in a variety of contexts, from embedded sensing systems such as sensors for healthcare, through infrastructure monitoring, unmanned autonomous systems, operating systems, middleware and large scale distributed systems architectures, to web-based and cloud computing environments.

Our work

Imperial has built faithful formal models for key components of the web ecosystem (JavaScript, PhP, HTTP protocol, etc.) and developed tools and techniques to verify the information flow, privacy and authorisation properties of web applications. Imperial's work on JavaScript subsets has shown some to be safe (e.g. Google Caja) and uncovered vulnerabilities in others (e.g. Facebook).

The ACE-CSR's work on statistical monitoring and anomaly detection is applied to both computer networks and social networks where new techniques have been developed to predict hidden links and nodes, and identify community structures. In network infrastructures we have developed novel characterisations of distributed denial of service (DDoS) attacks, models for the spread of malware, techniques for reacting to compromise to ensure network resilience and techniques for attack-resilient cognitive packet networks.

Imperial has developed information-centric security models that track the data flow through systems end-to-end and prevent data disclosures. Based on this work it has designed a secure middleware platform that is used by the NHS to protect medical records in a distributed event-processing environment.

Imperial's work on policy-based adaptive security management and authorisation has led to open source software Ponder2 (ponder2.net), which has been used to build solutions for, amongst others, the management and security of sensor networks for e-health, autonomous vehicles, mobile ad-hoc networks, pervasive workflows and fixed network infrastructures. Their software has been used by others in industry and academia. They have pioneered techniques for policy analysis, policy refinement from high-level requirements, and automated learning of policies from decisions made by legacy systems or human administrators.

Imperial contributes in other cyber security funded programmes. It leads the Research Institutes in Automated Program Analysis and Verification and in Trustworthy Industrial Control Systems. It leads a collaborative project on Games and Abstraction in the Research Institute on the Science of Cyber Security. It also investigates aspects of Privacy Dynamics as part of the Global Uncertainties programme on Consortia for Exploratory Research in Security (CEReS) and of Intelligent Protection of Cloud Environments at Run-Time as part of the Business-Academic Collaborations in Cybersecurity to Harness Underpinning Science (BACCHUS).

Contact

Dr Emil C Lupu, Associate Director

Institute for Security Science and Technology, Imperial College London
South Kensington Campus
London SW7 2AZ

+44 (0)207 594 8249

e.c.lupu@imperial.ac.uk

http://www3.imperial.ac.uk/securesoftwaresystems

Key areas of expertise and specialism

Imperial's work focuses on engineering secure and resilient software systems, including:

- Operational Systems and Information Assurance
- Security Analysis and System Verification

Photograph: John Donoghue

Newcastle University

Centre for Cybercrime and Computer Security

Who we are

The Newcastle ACE-CSR is based at the Newcastle Centre for Cybercrime and Computer Security (CCCS). The CCCS grew out of an unusual case in 2008 when Northumbria Police took report of stolen virtual sword from the 'World of Warcraft' game. A student studying at a local college asked the police to intervene in its sale on eBay. This intriguing case ultimately led to the development of CCCS at Newcastle University. The CCCS enables police, academics, businesses and public sector organisations to pool their resources to address the challenges of cybercrime, thereby providing the core capability of the ACE-CSR.

The ACE-CSR is led by its Director, Dr. Thomas Groß, and Associate Director, Professor Aad van Moorsel. The core research team is based in the Schools of Computing Science, and of Electrical and Electronic Engineering. The Centre also benefits from a broad spectrum of 25 associates in formal methods, dependability, cloud, systems, social sciences, psychology, law, business and international relations, reinforced by lively collaboration with Newcatle University's Centre for Software Reliability and the CultureLab. It maintains active connections with specialists in local businesses and industry.

What we do

The Centre pursues a vision of *Protecting Society's Fabric*. Its spectrum ranges from establishing the security of critical infrastructures (e.g. identity, cloud or e-voting) to researching the science of cyber security, including the quantitative side of human factors and usable/experience-centred security. To date, 12 PhDs in cyber security have been awarded and 15 more are in progress; supervision is available for various programmes for industrial PhD candidates.

The Centre's aim is to deliver effective support to all who need cyber security: to provide security solutions, educate people, assist (and create) businesses – and to enlighten government. We

Centre for Cybercrime and Computer Security

Newcastle University

offer services to government bodies, police and businesses, organise public events and training (e.g. with the North East Fraud Forum) and supply expert witnesses with a unique combination of police experience and technical expertise. The Centre also hosts the EPSRC Cybercrime Network.

The Centre is founded on wide-ranging technical expertise encompassing: cryptography, privacy, systems engineering, security analysis, trustworthy systems, information and operational assurance, the security of strategic technologies (such as cloud, identity or web), risk management, resilience, the science of cyber security and human factors. Uniquely, the Centre also offers hands-on expertise on criminal investigations.

Our Work

Self-Enforcing E-Voting: Develops a new generation of e-voting systems that do not rely on any trusted authorities. (European Research Council (ERC) funded)

FutureID: Establishes an e-ID card based electronic identity infrastructure that offers secure identity protocols and brokering. (EU-funded)

Cloud Security Assurance: Realises tools to analyse virtualized infrastructures for security properties, adopted by IBM PowerSC Trusted Surveyor. (IBM-collaboration)

Cyber Security Research Institute ChAISe: Establishes choice architectures and 'nudges' to improve decision-making. (EPSRC-funded)

Photograph: Simon Veit-Wilson

Research in the Wild of Hyper-Privacy Technologies: Supports survivors of domestic violence. (EPSRC-funded)

UNCOVER: Investigates complex system evolution through structured behaviours, e.g. for crime investigation support systems. (EPSRC-funded)

NIFTy: Develops novel image forensic tools to combat sexual abuse images of children. (EU-funded)

Trust Economics: Established a science of security methodology for trust, leading to new consulting practices at Hewlett-Packard and two spin-off companies. (TSB/HEFCE-JISC-funded)

J-PAKE: Developed efficient secure channels over insecure networks without a PKI, adopted by Mozilla, OpenSSL and OpenSSH. (EPSRC-funded)

CAPTCHAs: Developed automated Turing tests to protect web resources, which impacted the system design of Google, Microsoft and Yahoo!

Contact

Director: **Dr Thomas Groß**
thomas.gross@newcastle.ac.uk

Associate Director and PI:
Professor Aad van Moorsel
aad.vanmoorsel@newcastle.ac.uk

Newcastle University
UK Academic Centre of Excellence in Cyber Security Research, School of Computing Science, Claremont Tower
Newcastle upon Tyne NE1 7RU
United Kingdom

+44 (0) 191 208 8788

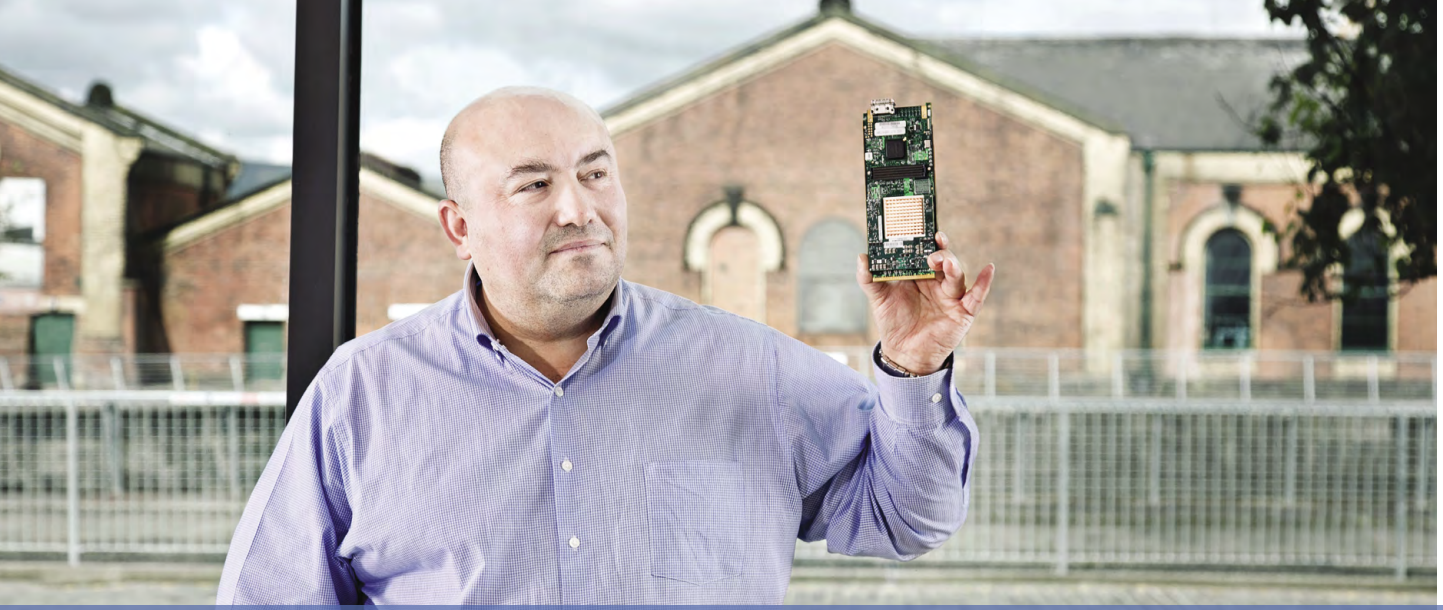
cccs@ncl.ac.uk

http://cccs.ncl.ac.uk

Key areas of expertise and specialism

Newcastle pursues the theme *Protecting Society's Fabric*, in particular considering:

- Cybercrime as a socio-technical issue
- Security assurance of infrastructures (e.g. identity, cloud computing)
- Science of cyber security



Queen's University Belfast

The Centre for Secure Information Technologies

Who we are

The Centre for Secure Information Technologies (CSIT) is a Global Innovation Hub for Cyber Security Research. Originally established in 2009, the Centre's significant achievements over its initial five-year period have been recognised by core funders. The EPSRC and Innovate UK have just confirmed a new five year package worth £5 million, whilst the University has committed a further £9 million, to sustain the National Innovation & Knowledge Centre (IKC) and help it raise the bar on translating its world leading research into commercial impact right up to 2020.

CSIT employs over 80 people and has world leading research expertise in areas such as network security, biometrics, video analytics, cryptography, security informatics, SCADA security, malware detection and embedded security.

Specifically, CSIT has core capabilities in:

- Security analytics
- Secure ubiquitous networks
- Device authentication

Dr Godfrey Gaston is CSIT Director with overall responsibility for the Centre.

What we do

Uniquely for a university, industry experienced engineers and business development people work alongside CSIT academics, researchers and PhD students to facilitate a culture of innovation that is industry focused and measured on impact and commercial exploitation.

Operating an Open Innovation model to drive collaboration with member organisations, CSIT carry out contract research, license intellectual property, spin-out companies and have a membership program where industry can invest in the vision of CSIT and join in developing the research strategy that has the overarching theme of 'securing our digital tomorrow'.

Queen's University Belfast

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

CSIT is engaged in a number of cyber security collaborative research projects with world leading organisations including Allstate, BAE Systems, IBM, Intel, Infosys, McAfee, Thales, numerous SMEs, spin-out ventures (Titan IC Systems, Sensurity, Activ Wireless) and leading institutes in USA, South Korea, Japan, India and Europe. CSIT is a core member of the UK National delegation to the security standardisation Study Group 17 of the International Telecommunication Union (ITU) and are active members of ETSI, ADS and Information Security Ireland.

Our Work

CSIT has delivered, is co-ordinating and is involved in numerous projects, including:

SAFEcrypto (Secure Architectures of Future Emerging Cryptography), a Horizon 2020 project which CSIT is leading, will provide a new generation of practical, robust and physically secure post-quantum cryptographic solutions that ensure long-term security for future ICT systems, services and applications. Novel public-key cryptographic schemes (digital signatures, authentication, identity-based encryption (IBE), attribute-based encryption (ABE)) will be developed using lattice problems as the source of computational hardness.

The Converged Approach towards Resilient Industrial control systems and Cyber Assurance (CAPRICA) project is investigating vulnerabilities within the national grid as wind or solar generated electricity comes on stream. Where the grid operates over the telecoms network it could be vulnerable. It is one of four projects that make up the Research Institute in Trustworthy Industrial Control Systems (RITICS) initiative co-funded by the Engineering and Physical Sciences Research Council (EPSRC) and UK's National Cyber Security Programme.

The Leverhulme Interdisciplinary Network on Cybersecurity and Society (LINCS) at Queen's University Belfast has been established to support pioneering research at the interface between the social sciences and electronic engineering & computer science. LINCS brings together the Centre for Secure Information Technologies (CSIT) and the Institute for the Study of Conflict Transformation and Social Justice (ISCTSJ) to develop a distinctive cohort of doctoral students working across the boundaries of their disciplines.

The PRECYSE (Prevention, protection and REaction to CYber attackS to critical infrastructures) FP7 project is defining, developing and validating a methodology, an architecture and a set of technologies and tools to improve by design the security, reliability and resilience of the ICT systems supporting critical infrastructures.

The NIMBUS (Network in Internet and Mobile Malicious Software) EPSRC project will act as a catalyst to develop a balanced programme of both blue skies research and near term applied research that will assist in the fight against cybercrime in the UK.

CSIT has also delivered industry contract research and development covering malware reverse engineering, Zero Day attacks, network processing hardware design, driver condition detection and driver authentication, Processor Architecture and secure antenna design.

Contact

Dr. Godfrey Gaston, Director

Centre for Secure Information Technologies,
ECIT Institute, Queen's University Belfast,
Northern Ireland Science Park,
Queen's Road, Queen's Island,
Belfast BT3 9DT

+44 (0) 28 9097 1700

info@ecit.qub.ac.uk

www.csit.qub.ac.uk

Key areas of expertise and specialism

CSIT has core capabilities in:

- Security analytics
- Secure ubiquitous networks
- Device authentication

Royal Holloway

University of London

Who we are

Most of the research in information and cyber security at Royal Holloway is undertaken by members of the Information Security Group (ISG), which is one of the world's largest research groups working in cyber security. The ISG is also one of the oldest groups of its type, having worked on cryptography since the mid-1980s. Royal Holloway was the first institution in the world to offer a degree in information security, accepting its first students in 1992. There are now over 2500 alumni of the course from over 100 countries, many working in senior information security roles in Government and industry. The ISG currently has around 40 PhD students and is one of two new doctoral training centres for cyber security, funded by EPSRC and the UK Government.

The ISG is a department within the School of Mathematics and Information Security. It employs sixteen full-time and two part-time members of staff, all of whom are actively involved in information and cyber security research and teaching. Some members of the group focus on academic research, while others also undertake industrial research and consultancy. Of the sixteen full-time academics, seven are full professors. The ISG is privileged to have several distinguished visiting professors who are among the most prominent academics and industry figures in information security research. The Group also employs 10 post-doctoral research assistants, working on a wide range of funded projects.

What we do

The ISG was founded in 1990 by a group of mathematicians and computer scientists with interests in cryptography. Research in this area remains an important part of the ISG's activities and covers cryptanalysis, combinatorial cryptography, quantum information theory and cryptography, provable security and message authentication codes.

As the Group has grown over the last 25 years, the scope of its research has expanded dramatically and now covers a very broad range of information and cyber security areas. Current research includes theoretical and applied work on access control; authentication and identity

ROYAL HOLLOWAY UNIVERSITY OF LONDON

management; economics of security and trust; social and organisational aspects of cyber security; malware and botnet detection; the security of systems and technologies (which ranges in scale from RFID tags and the Internet of Things through to global telecommunications networks and critical infrastructure protection); and vulnerability analysis. Royal Holloway has received substantial funding in recent years to support its research in cyber security, including large awards for research on access control in workflow systems, cryptography in theory and practice, adaptive security and economics, malware analysis, and security in the Internet of Energy. The ISG has two dedicated research labs, the Smart Card Centre and the Systems Security Lab.

The activities of the ISG are supplemented by research undertaken by members of the Mathematics Department. There is also increasing collaboration between the ISG and the Department of Computer Science, in particular the Theory of Computing and Computer Learning groups. Royal Holloway hosts one of two UK Centres for Doctoral Training in Cyber Security. Our research in cyber security has been enriched by the recruitment of several students with backgrounds in the social sciences and has led to fruitful collaboration with the Department of Geography.

Our work

The ISG provides advisory and research services on cyber security and associated topics, drawing on the expertise of its research staff and, as appropriate, a network of trusted professional associate consultants and external researchers. ISG members have advised over 100 companies and organisations worldwide, including multinational corporations, Government departments, trade and standards associations and SMEs. As one of the world's largest academic research groups in information security, the Group's expertise is wide-ranging, including cryptography, key management and related areas, systems engineering and security analysis, information and operational assurance methodologies, the security of technologies and products, and building trusted and trustworthy systems. The Smart Card Centre offers specialised advice on embedded systems, including smart cards, mobile devices, near-field communications and associated technologies. The Centre's experts have advised in all these areas (most recently on payments, transport ticketing and mobile communications security), and have also guided external organisations with their own information security research and development programmes.

Contact

Jason Crampton/Keith Mayes

Information Security Group
Royal Holloway, University of London
Egham Hill, Egham TW20 0EX

+44 (0)1784 443117

Jason.Crampton@rhul.ac.uk

Keith.Mayes@rhul.ac.uk

www.isg.rhul.ac.uk

Key areas of expertise and specialism

Royal Holloway specialises in:

- Theoretical & practical applications of cryptography
- Social, technical & organisational aspects of cyber security
- Information assurance & security for RFIDs, smart cards, mobile/NFC, IoT & general embedded devices
- Malware analysis & system security

Photograph: UCL's JDI Secure Data Laboratory

University College London

Who we are

University College London's ACE-CSR includes 21 academics across five research groups within the Computer Science Department and the departments of Chemistry, Electronic and Electrical Engineering, Security and Crime Science, STEaPP, Statistics and the Institute for Risk and Disaster Reduction.

UCL hosts the Science of Cyber Security Research Institute, which is the UK's first academic research institute to focus on understanding the overall security of organisations, including their constituent technology, people and processes. The institute is a virtual collaboration with Imperial College, Queen Mary College, Royal Holloway, Newcastle University and Northumbria University, funded by a £3.8m grant from EPSRC, GCHQ and BIS.

Cyber security research is one of UCL's strategic research priorities and UCL has launched the JDI Research Laboratory, a £1m secure data analysis centre run jointly by the Computer Science Department and the Security and Crime Science Department. The facility is undergoing certification to allow sensitive and confidential datasets to be brought into the university so that they may be worked upon by researchers in a secure, controlled environment.

What we do

The ACE-CSR conducts a broad range of research in cyber security. The Information Security Group has expertise in human, organisational and economic aspects of security, identity and trust, privacy-enhancing technologies, smart cards and financial security, cryptography and cryptanalysis and in conjunction with the Dept. of Security and Crime Science works on understanding and preventing cybercrime. The Centre for Research, Evolution, Search and Testing (CREST) develops tools for testing software and eliminating bugs and has recently made significant advances in detecting malware. The Programming Principles, Logic and Verification Group does research on automatic verification and analysis of programs. The research of the Networked Systems Group includes secure network protocols, DoS defences, secure routing, exploit resistance and wireless security. The Centre for Computational Complexity works on secure access to e-Science infrastructures accessing patient data.

UCL is educating future cyber security professionals through its MSc and PhD programmes. The MSc in Information Security is a one-year programme where international security experts teach a balance of established theory and cutting edge practice, equipping graduates with the broad expertise necessary to succeed in information security.

Our work

We research and solve real-life problems across a broad range of areas. A few illustrative examples include web security, malware and censorship.

Collaborating with Stanford, Google, Chalmers, and Mozilla we have built the 'Confinement with Origin Web Labels' (COWL) system that works with Mozilla's Firefox and the open-source version of Google's Chrome web browsers. Web users' privacy can be compromised by malicious JavaScript code hidden in seemingly legitimate web sites. The web site's operator may have incorporated code obtained elsewhere without realising that the code contains bugs or is malicious. Such code can access sensitive data within the same or other browser tabs, allowing unauthorised parties to obtain or modify data without the user's knowledge. The COWL system prevents malicious code in a web site from leaking sensitive information to unauthorised parties, whilst allowing code in a web site to display content drawn from multiple web sites. The system thus solves a central challenge in computer security giving both privacy for the user and flexibility for the web application developer.

The SeMaMatch project studies the application of the Normalised Compression Distance (NCD), a computable approximation of the Normalised Information Distance based on Kolmogorov complexity, to the malware arms race. The main question is: "How well does NCD measure malware similarity?" Our key finding is an approach that classifies malware with 98% accuracy and a false positive rate of 1.5%. We do this with off-the-shelf compressors and a standard machine learning classifier and without any specialised knowledge or use of static or dynamic analysis.

Due to the lack of publicly available information, it is often hard for the research community to study Internet censorship. Therefore, access to 600GB worth of logs from hardware appliances used to filter traffic in and out of Syria provided a unique opportunity to examine the workings of a real-world censorship ecosystem. Our research revealed a relatively stealthy, yet quite targeted, censorship. Traffic was filtered in several ways, using IPs, URLs, and keywords. We also highlighted that Syrian users tried to evade censorship and that encrypting traffic using HTTPS would make many policies much harder to implement.

Contact

Academic Centre of Excellence in Cyber Security Research
University College London
Department of Computer Science
Gower Street, London WC1E 6BT

j.groth@ucl.ac.uk

http://sec.cs.ucl.ac.uk/ace_csr/

Staff List

Jens Groth (Director), Angela Sasse, David Pym, George Danezis, Nicolas Courtois, Emiliano De Cristofaro, Sarah Meiklejohn, Gianluca Stringhini, Steven Murdoch, Gordon Ross, David Clark, Jens Krinke, Earl Barr, Peter O'Hearn, Byron Cook, Brad Karp, Mark Handley, Kyle Jamieson, Shi Zhou, Peter Coveney and Brian S. Collins.

Key areas of expertise and specialism

Cryptography and cryptanalysis, Language-based Security, Program Verification and Analysis, Human and Organisational Factors in Security, Network and Systems Security, Malware Detection, Privacy-enhancing Technologies, Cybercrime, Smart Cards and Financial Security.

University of Birmingham

The School of Computer Science

Who we are

The School of Computer Science at the University of Birmingham, a UK Academic Centre of Excellence in Cyber Security Research.

The ***Security and Privacy group*** in Birmingham was founded in 2005 and has steadily grown with expertise in cyber security research. The team is comprised of seven permanent academics and two academics having significant involvement. There are also six postdocs, and 16 PhD students. Its historic strength is in the analysis of security systems using formal and mathematical methods, but via its recent appointments it has deliberately broadened its aims and scope to cover all aspects of cyber security. Since 2008, the group has acquired over £5.5 million in research funding, from EPSRC, TSB, EU, GCHQ, Microsoft, IBM, BT, Vodafone, L-3 TRL, Rail Safety and Standards Board, Jaguar Land Rover, and additional in-kind funding from HP, and Google. The group has a funded automotive security lab, which includes a 2015 Land Rover Range Rover Evoque and security diagnostic equipment.

The Security and Privacy group has recently been awarded significant funding from the University, and will expand its permanent academic members from 7 to 10 persons. This investment will allow us to become one of the strongest and largest security groups in the UK.

What we do

The effective ethos of the computer security team at Birmingham is to work with government and industry to tackle cyber security problems that are important to society. We analyse critical cyber security issues from their high level design down to specific hardware and software implementations. Some of the topics of research within the team include the analysis and verification of protocols, embedded systems, and hardware. Application areas include: automotive security, secure electronic voting, privacy and security tension, contactless payment cards, Internet of things, cloud security, secure software engineering, and wireless networking.

UNIVERSITY OF BIRMINGHAM

Our work

We do research in all aspects of cyber security. Some examples of recent work are given below.

Research currently underway in the computer security team includes ***Secure online voting***. Led by Professor Ryan, this research project is helping to transform electronic voting into a secure and usable system in large scale elections. The team have designed a new electronic voting system that allows the authorities to identify and monitor votes that may have taken place under coercion, whilst simultaneously keeping the privacy of peoples' votes. They have also developed techniques to allow people to cast their election vote online – even if their home computers are suspected of being infected with viruses.

One aspect of cyber security is to identify '***privacy***' concerns which affect society at large. As people's lives are lived increasingly online, large quantities of data about them and their actions and thoughts are stored on computers all over the world. The Security and Privacy group at Birmingham is working on figuring out how to avoid abuse of this information.

Another activity at Birmingham is the analysis of currently deployed systems. Dr Tom Chothia's research has uncovered flaws in the wireless protocols used in e-passports that jeopardises privacy. This revelation has prompted further research into radio-frequency identification tags which allows the said tracking of individuals via the passport.

In a similar vein, the team at Birmingham have brought to light a vulnerability of 3G standard mobile phones which leaves users unprotected from potential stalkers and other enemies. The solution for this problem has also been addressed by the team which included Dr Eike Ritter. Collectively they found that public key cryptography needs to be deployed within networks in order to thwart these privacy attacks on mobile phone users.

In addition to this research, the team is also working on the security and protection of embedded systems. Dr David Oswald focuses on implementation attacks, i.e., methods that exploit physical properties of cryptographic devices to break mathematically secure algorithms. For numerous real-world systems, either passive observation (side-channel analysis) or active manipulation (fault injection) could allow an attacker to extract cryptographic keys of ciphers like AES.

Securing automotive anti-theft devices and contactless payment cards is another component of the research the team is involved with. Dr Flavio Garcia has revealed several weaknesses in the design of anti-theft devices within the car immobilizer industry. The flaws that have been illustrated by Dr Garcia include serious attacks which can recover secret keys from car components in less than six minutes using ordinary hardware.

The security and privacy group at the University of Birmingham are continuously researching important issues that need to be addressed in a world where technology is advancing. The team are committed to finding long-term solutions to the problems that will ultimately benefit the future government, industry and society.

Contact

Professor Mark Ryan
Professor of Computer Security

School of Computer Science
University of Birmingham, Edgbaston
Birmingham B15 2TT

+44 (0) 121 414 7361

ace-csr@cs.bham.ac.uk

http://www.cs.bham.ac.uk/research/groupings/security_and_privacy/

Key areas of expertise and specialism

- Design of secure systems
- Security of embedded systems
- Cloud computing security
- Privacy technologies for individuals
- Network security and malware
- Analysis and verification of systems

University of Bristol

Bristol Security Centre

Who we are

ACE-CSR activity at the University of Bristol is organised within the Bristol Security Centre (BSC). A range of University-wide efforts and events are coordinated under this umbrella, including a series of popular “open house” evening lectures on cyber-security.

In addition to the Centre for Quantum Photonics, Centre for IT and Law and GCHQ-funded Heilbronn Institute, the most significant and directly relevant research and teaching activities relate to cryptography. Housed within the Department of Computer Science, the Cryptography Group is led by Professor Nigel Smart. Since being established in 2000 by Professor Smart, it has expanded to include six members of permanent academic staff, 10 Post Doctoral Research Assistants and 16 PhD students. The Group maintain close links and a portfolio of ongoing research projects with national and international industrial partners and academic research groups, and is guided by a dedicated Industrial Advisory Board (IAB). It is represented at board-level in the International Association for Cryptologic Research (IACR).

What we do

The ACE-CSR fosters a diverse, highly inter-disciplinary research programme spanning theoretical and practical aspects of cryptography and information security. Specific interests and expertise include:

- Foundational research and number theory
- Design and formal security analysis of existing and novel cryptographic primitives, protocols and applications
- Applied attack techniques on cryptography (such as side-channel and fault attacks)
- Effective implementation of cryptography in hardware and software

Various flavours of consultancy, standardisation and commercialisation are evident throughout related output.

University of BRISTOL

Our work

The following highlight a selected set of both completed and active projects:

The Centre/Group as a whole has deep, long standing expertise with public key cryptography. Elliptic Curve Cryptography (ECC) is a particular focus, in part because of the emerging trend toward phased replacement of RSA over the medium- to long- term.

Among a large body of output, selected highlights include:

- Underlying Mathematics (e.g., point counting, difficulty of discrete logarithms)
- Low-level algorithms and arithmetic (e.g. ate pairing, point and field arithmetic, efficient scalar multiplication)
- High-level protocols (e.g., pairing-based encryption and key agreement)
- Efficient implementation (e.g., hardware and/or software realisations)
- Standardisation (e.g. pairing based cryptography through IEEE P1636.3, DAA through ISO/IEC CD 20008-2)

Based on aspects of this work, members of the group formed a spin-out company in 2001 that was later acquired by Trend Micro.

The analysis of deployed protocols and implementations forms a central activity within the Group. Selected highlights include:

- Theoretical models and proofs of security for TLS, EMV and SSH
- Analysis and refinement of the Helios electronic voting system
- Concrete attacks on implementations of TLS within OpenSSL

Supported by an EPSRC Leadership Fellowship, Dr. Elisabeth Oswald has focused on improving formal understanding of vulnerabilities based on information leakage. This has long represented a problem for embedded and mobile computing devices, which are often tasked with storing and processing security-critical information.

As a result however, many cross-cutting opportunities have emerged; for example, techniques to exploit information leakage from smart-cards can be applied to better understand emerging threats to web-applications (e.g. via analysis of communication flows). Understanding, detecting and preventing attacks of this type represents ongoing work.

In part supported by an ERC Advanced Grant, Professor Nigel Smart leads a large team focused on the related topics of Fully Homomorphic Encryption (FHE) and secure Multi-Party Computation (MPC). Both technologies offer solutions within the context of computation on encrypted data: the idea is to compute operations directly on said data, avoiding performance and security impacts of decrypting, then computing, then re-encrypting.

Following numerous theoretical breakthroughs over the last few years, the team is now exploring robust, concrete implementations that can support industrial workloads.

Contact

Dr. Daniel Page

University of Bristol
Department of Computer Science
Merchant Venturers Building
Woodland Road, Bristol BS8 1UB.

+44 (0)117 3315146

page@cs.bris.ac.uk

http://bsc.bris.ac.uk/

Key areas of expertise and specialism

Bristol specialises in the theory, design, implementation and analysis of protocols and systems that use (or relate to) cryptography.

University of Cambridge

Who we are

The University of Cambridge has been responsible for world-leading work on digital network protection since before the internet existed: it was at Cambridge, for example, that the use of a one-way function to protect the password file was first conceived and deployed (Needham et al, 1966). The ACE-CSR, located at the Computer Laboratory, includes 11 staff members, complemented by world-leading domain experts across the university.

Dr Frank Stajano, head of the Cambridge ACE-CSR and a Reader in Security and Privacy, says: "We believe cyber security is inherently a systems problem and must be addressed as such. Our strongest asset as a cyber security research institution is our unique combination of depth and breadth: we offer a core of systems security expertise at the Computer Laboratory and, through the rest of the University, we have ready access to world-class domain experts from other disciplines. We are therefore uniquely placed to critically analyse and contribute to all aspects of the cyber security problem. Without false modesty, no other academic institution in the whole of Europe has the mix of skills, knowledge and creative people to do this as effectively as the University of Cambridge. We will continue to research long term solutions to the fundamental cyber security problems that will affect the society of tomorrow."

UNIVERSITY OF CAMBRIDGE

What we do

The University's current work touches on areas of great impact for society such as securing global infrastructure (banking security, smart card security, satellite navigation security, civil infrastructure security) and securing the building blocks of the digital world (operating system security, secure computer architectures, network protocol security, security of mobile devices), as well as the fundamental problem of the interaction between people and computers (the intersection of security and psychology, the usability and security problems of password authentication, location privacy, privacy in social networks, anti-censorship systems). Much of this research is carried out in close collaboration with commercial and industrial bodies, both in the UK and abroad, with a view to tackling real-life problems.

Recent projects have, for example, focused on how to identify cyber security vulnerabilities in the computer systems that control major power plants; or on the protection of sensor networks that monitor potential damage to vital infrastructure like bridges and tunnels.

Our work

The entrepreneurial spirit of Cambridge academics and graduates has created hundreds of start-up companies, of which several are in the security space. For example Xensource, founded by former Computer Lab staff, on whose Xen hypervisor now runs Amazon's EC2 cloud (the world's largest), was acquired by Citrix for $500M in 2007. Ncipher, a company founded by a Computer Lab graduate that made cryptographic accelerators, was bought by Thales for $100M in 2008. Cronto, co-founded by an academic staff member of the Cambridge ACE-CSR, licenses its secure online banking device to major banks in Germany, Switzerland and Chile and was acquired by VASCO for $20M in 2013.

Besides founding start-up companies, Cambridge ACE-CSR members have attracted significant grants towards cyber security research from both industry and government agencies, from UK and abroad. Around 40 cyber security-related grants have been received in the past five years, including the following which all exceed a million pounds each:

- REMS, rigorous engineering for mainstream systems (£5.6m from EPSRC)
- IKC, innovation knowledge centre on smart infrastructure and construction (£5m from EPSRC, UK)
- CTSRD, a CPU architecture supporting fine-grained software compartmentalization (£2m from DARPA, USA)
- MRC2, data centre switching security and resiliency; and secure cloud computation (£2m from DARPA, USA)
- INTERNET, intelligent energy-aware networks (£1.44m from EPSRC, UK)
- Pico, eliminating passwords (€1.35m from ERC, EU)

Contact

Dr Frank Stajano
Reader in Security and Privacy
Head, ACE-CSR

University of Cambridge
Computer Laboratory, William Gates Building, 15 JJ Thomson Avenue
Cambridge CB3 0FD

frank.stajano@cl.cam.ac.uk

+44 (0) 1223 763 500

http://www.cl.cam.ac.uk/projects/ace-csr/

Key areas of expertise and specialism

- Systems security
- Network and operating system security
- Security and human factors including psychology and usability
- Security and privacy of mobile systems and social networks
- Smart card and banking security
- Cybercrime, frauds and phishing
- Anonymity and censorship

University of Kent

Who we are

The University of Kent interdisciplinary centre for Cyber Security Research was established in 2012. The vision of the Centre is to address cyber security challenges holistically, including not just world-leading technological expertise but ensuring that also social, legal, and psychological aspects of these challenges are covered. This multidisciplinary diversity of experience stimulates security-related research across all areas.

Around 10 core academics and 20 associated academics are spread across several Schools, such as Computing (Security research group), Engineering and Digital Arts (EDA, Intelligent Interactions research group), Physical Sciences, Law, Psychology, Sociology, and Conservation. Research projects in the centre, many of them crossing discipline boundaries, are funded through EPSRC, the EU, DSTL, InnovateUK, and others.

University of Kent

What we do

At the heart of cyber security is the issue of identity of actors and how and why they can be trusted. Thus, *trust and identity management* forms a critical research area for Kent. It is central to Chadwick's work on PERMIS, the open source policy based authorisation infrastructure. There are also important social science aspects, in particular through medical law and ethics (Mackenzie) and sociology. *Biometrics*, as a basis for authentication, is a closely related topic that has been a core research area for the Intelligent Interactions group (Deravi, Howells, Guest, Fairhurst) for many years. Related to this work significant *privacy* aspects also arise. Chadwick, in collaboration with Dimitrakos (Kent/BT Research) is applying authorisation infrastructures also in *cloud security*.

Computer forensics and steganalysis is a core area of research, with foundational work by Hernandez-Castro, and Gibson and Solomon on digital images. It finds its application in a variety of contexts such as face recognition, and internet illegal wildlife trade (with Roberts). Hernandez-Castro also applies related techniques in image and video *steganalysis*.

Connected to the research strength in the EDA Antennas group (Batchelor), *small device security* is also being explored by Hernandez-Castro for

RFID security protocols and through applications of Howells' ICmetrics.

Advanced program analysis techniques from Andy King's research group are being applied in *malware analysis*, including two projects in the GCHQ Research Institute in Automated Program Analysis and Verification. Further research involvement with cyber crime incidence and analysis is in progress.

Boiten looks at increasing confidence of cryptography based security protocols and primitives through the use of formal methods. Kent is the lead site for the EPSRC Network of Excellence CryptoForma in this topic (2009-2015).

In addition to research and enterprise, the centre also supports education through its involvement in MSc programmes in Information Security and Biometrics, Computer Security, and Networks and Security, as well as contributions to the Kent Law School LLM.

Contact

Dr Eerke Boiten, director of the Cyber Security Centre and PI for the ACE-CSR

School of Computing,
University of Kent,
Canterbury CT2 7NF

Dr Gareth Howells, deputy director of the Cyber Security Centre

School of Engineering and Digital Arts
University of Kent,
Canterbury CT2 7NT

ace-csr@kent.ac.uk

www.cybersec.kent.ac.uk

Key areas of expertise and specialism

- Identity management and authorisation, biometrics
- Malware and vulnerability analysis
- Formal methods and security
- Digital forensics and steganography
- Mobile and RFID security
- Cloud security

University of Lancaster

Security Lancaster

Who we are

Security Lancaster is one of the few multi-disciplinary centres internationally which embeds computer science and communication systems researchers with behavioural and social scientists to tackle both human and technological challenges to cyber security. With over 45 researchers (including 17 academics) focusing on cyber security research, Security Lancaster is internationally renowned for its research on network resilience, security of communications, securing mobile networks and embedded systems, intelligent systems for analysing large, heterogeneous information sources and studies of user behaviours and human factors leading to cyber security threats.

The centre's research is funded from a variety of sources including research councils (EPSRC, ESRC), the European Commission, JANET and direct investment from security organisations such as Centre for Protection of National Infrastructure (CPNI), Defence Science and Technology Lab (DSTL), the UK Home Office, Her Majesty's Government Communications Centre (HMGCC) and the Ministry of Defence (MoD).

Two key principles permeate the Centre's research ethos and hence distinguish it from typical cyber security research: (i) its focus on multi-disciplinary research, which combines traditional network security and communications mechanisms with approaches for large-scale data analysis and human behaviours, informed by psychological and linguistic approaches, and (ii) its close engagement with stakeholders, especially practitioners in cyber security in both Governmental organisations and industry, who provide key requirements for our research and directly use our outputs.

Security Lancaster | LANCASTER UNIVERSITY

What we do

Traditional research on cyber-security tends to bifurcate online/offline and to treat humans as wholly separate from technologies. In contrast, Security Lancaster takes the perspective that cyber behaviour is shaped by individual and group processes and, equally, technology is made vulnerable and is exploited by the individual. Taking such an embedded view

of cyber security enables the Centre to more insightfully encapsulate the behavioural and technological aspects of existence and security in the digital world. This stimulus underpins two key themes of research: 1) network resilience, which encapsulates Lancaster's traditional network security and communications research with a user focus; and 2) intelligent behaviour-based systems for cyber security, integrating analysis of large heterogeneous data sources with human behavioural models based on psychological and linguistic insights. This multi-disciplinary perspective has been a key to establishing an understanding of how the constantly changing or new digital environments entwine within the everyday lives of individuals, groups and organisations, and what constitutes security and risk in this context.

Our work

An example project from each research theme is included below:

Isis: Protecting Children in Online Social Networks

The project involved development of sophisticated language analysis of online conversations to detect the age and gender of participants with a high degree of accuracy (80- 94%) and identification and resolution of multiple online identities used by offenders in online social networks. These techniques are at the heart of a sophisticated Language Forensics Toolkit which enables the building and comparing profiles of individuals and groups based on their online linguistic footprint. The research has been trialled and is used by law enforcement agencies, is a commercial product via a spin-out company Isis Forensics Ltd, and was highlighted as one of the 100 Big Ideas for the Future in a report jointly published by Research Councils UK and Universities UK in 2011. In June 2010, the project toolkit's 94% accuracy in identifying adults masquerading as children online made headline news in the UK (e.g. BBC 6 o' Clock News, various radio stations, The Independent) and internationally (e.g. German news Heute, Austrian radio, ABC News in Australia, The New Zealand Herald).

ResumeNet: Resilience and Survivability for Future Networking: Framework, Mechanisms, and Experimental Evaluation

The project developed mechanisms for network resilience, including a framework for evaluating the resilience of networks, approaches to understanding the likely high-impact challenges a network deployment may face and architectures for the dynamic adaptation of networks in response to challenges. The work has influenced a number of white papers produced by ENISA (European Network and Information Security Agency). Consortium members organised a workshop on network resilience and produced teaching material on the fundamentals of network resilience.

Contact

Professor Awais Rashid
Director, Security Lancaster
Infolab21, Lancaster University
Lancaster LA1 4WA
+44 (0)7807 125 817
marash@comp.lancs.ac.uk
http://www.security-centre.lancs.ac.uk

Key areas of expertise and specialism

- Resilience, with a key focus on resilience of networks, cyber-physical systems and studies of user behaviour in order to improve cyber security of large-scale socio-technical systems
- Development of cyber security solutions that benefit the society at large, particularly vulnerable user groups

University of Oxford

Oxford University Cyber Security Network

Who we are

The Oxford University Cyber Security Network works in over seven departments within the University, integrating the work of over forty academics, with associated doctoral students and research staff. A rigorous and scientific integration of these diverse fields of study is central to the vision of the Network, expressed in collaborative research, teaching at Masters level, and both informing and being informed by the practice of Cyber Security within the University itself. The Cyber Security Network is a virtual entity spanning the University, having several tangible expressions in particular significant collaborative projects, as well as opportunities to interact through seminars and other shared activities.

What we do

This breadth allows the University to create impact in numerous areas, including the theory of security protocols and their automated analysis (Casper/FDR, Scyther, Tamarin), applied cryptography, and stenography; the security of systems, particularly the technical and human factors contributing to trust and security in distributed contexts (including mobile and cloud systems); wireless security; network operations situational awareness and security; insider threat detection; ad hoc collaboration; privacy and governance; trusted computing, and operations management. The Network also draws on wider expertise in software engineering and verification; quantum computation; management of large datasets and compute resources; medical informatics and privacy; modelling and understanding of risk; and programming language design.

Our work

These research interests contribute to numerous research projects with sponsors from the public and private sectors. These find application in areas such as smart power grids, sensor networks, fraud detection, secure web applications, sensor networks, personalized medicine, home networking and services, sustainable ICT, and security standards.

Integration across the disciplines named – and others outside the University – enabled an Oxford team to win a major CPNI-sponsored project in

UNIVERSITY OF OXFORD

CYBER SECURITY

Corporate Insider Threat Detection. The project combines perspectives from across the Network's areas of expertise to develop models for insider threat, understand the behaviours which might indicate a potential threat, develop algorithms to detect problematic patterns and provide visual analytics for decision-making. In addition, the project works to understand relevant enterprise culture and practice, and the organisational roles impacted by such detection systems.

A major element is the Network for Doctoral Training in Cyber Security, supported by EPSRC and BIS, which recruits a cohort of around 17 students each year, training them in the diverse disciplines which contribute to cyber security and equipping them to make a lasting research contribution in this cross-disciplinary area. Its particular research themes are the security of 'big data', cyber-physical security, effective systems assurance, and real-time security controls. Through industrial partnerships and visits, these students' research will remain focused upon real-world problems, whilst informed by and using the best available scholarship in the contributing disciplines.

The Global Cyber Security Capacity Centre, based at the Oxford Martin School and funded by the UK Foreign and Commonwealth Office, sets out to understand how to deliver effective cyber security within the UK and internationally. By collating best practice stories and case studies, it is developing a model for improving capacity across the areas of policy, risk management, society and culture, legal frameworks, a skilled workforce, and security controls. Resources are available via the online Cybersecurity Capacity Portal.

In 2014 the Department of Politics opened the Cyber Studies Programme which seeks to create a new body of knowledge that clarifies the consequences of information technology for the structures and processes of political systems.

The research of those in the Network also contributes to the very successful MSc in Software and Systems Security. With Software Engineering, it recruits around 90 students each year to study part-time, whilst retaining professional roles in high technology companies and Government departments. This is a crucial aspect of our technology transfer work, and is one of the means by which we develop long-term relationships with external partners for mutual benefit.

Contact

Andrew Martin, Professor of Systems Security PI for ACE-CSR and Director of the CDT in Cyber Security

Sadie Creese, Professor of Cyber Security

Cyber Security Network
University of Oxford
Department of Computer Science
Wolfson Building, Parks Road
OXFORD OX1 3QD

enquiries@cybersecurity.ox.ac.uk

www.cybersecurity.ox.ac.uk

Key areas of expertise and specialism

- Analysis and verification of software and security protocols
- Systems security; trustworthiness and usability
- Inter-disciplinary cyber security, policy and governance

University of Southampton

CyberSecurity Southampton

Who we are

Cybersecurity Southampton aspires to lead the academic agenda towards a secure cyberspace. Our multidisciplinary expertise contributes understanding, knowledge and innovation to the protection of critical infrastructures, users, their data and interests. Our activities connect across electronic, software and cyber-physical systems, advanced networking and protocols, cyber-risk analysis, cyber criminology, social acceptability of cyber regulations, and cyber identity management.

Led by Professor Vladimiro Sassone, the centre includes researchers from Computer Science, Engineering, Law, Management, Mathematics, Nano-Electronics, Psychology, Sociology and Web Science. This places us in a unique position to respond to the need for the UK Government, infrastructures, business and consumers to become more resilient to cyber attacks. In addition, we can respond to issues of privacy, trust and anonymity alongside social, ethical and legal responsibilities. Together, these address the need for security, efficiency and ownership around personal and institutional security and privacy.

Cybersecurity Southampton

Advancing Cyber Security

UNIVERSITY OF Southampton

What we do

Cybersecurity Southampton delivers a wide spectrum of interwoven research ranging from electronic (nano) devices to (physical and cyber) biometrics, passing through world-leading research on cyber-enabling infrastructures – viz., fibre-optics, internet and the web – using behavioural and cognitive psychology, and deploying both formal and experimental methods.

We have long-standing experience in joint hardware/software operations and world-class expertise on global infrastructures such as communications and the web, software engineering and formal methods, human/machines teams. We operate an in-house nano-fabrication facility and own a well integrated research portfolio linking together in a full circle (opto) electronics, computer science and engineering, social and human aspects of cyber security.

Informed by such strengths, the Centre's vision is:

- to supply secure (embedded) systems and their design methodologies via an integrated hardware-software approach, and focus on the creation and use of security-enhancing computer-aided design and verification tools;
- to secure the cyberspace by design, analysis, simulation and proof, in order to protect infrastructures and data, users and their interests;
- to support policy-makers, strategy-designers, government, industry and society at large to

enhance the national and international cyber security capacity, via research, advising, consultancy, training and education;

- to form partnerships with industry, government agencies, and local communities in order to further our institutional mission more effectively;
- to adopt a holistic and multidisciplinary approach, which takes into full account human aspects and behaviour, as well as social and legal acceptability issues;
- to foster excellence in research, depth in impact, and to educate top-class cyber security experts.

Our work

Professor Sassone has secured the H2020 project ***SUNFISH*** (€4.5M), whose partners include the UK and the Italian governments. SUNFISH focusses on the secure sharing of information in federated heterogeneous private clouds, and aims at developing the middleware to federate data clouds belonging to different public sector entities whilst maintaining the required security levels.

Professor Sassone has obtained government grants to investigate the cyber security of the ***Internet-of-Things*** (with Dr Rathke), of the ***UK Smart Metering*** Implementation Programme (with Professor Butler) as well as the effectiveness of ***Cyber Security Controls*** (with Dr Surridge and Dr Wills).

Professor Sassone and colleagues have established solid working relationships with several agencies of the UK government, in particular the Foreign and Commonwealth Office. They ideated and promoted a series of workshops, the ***Southampton Cybercrime Symposium***, to provide a first common forum between cyber law enforcement, the College of Policing and academia.

Professors Jennings, Moreau and Rogers have secured the programme grant ***ORCHID*** (£5.5M) that supports cyber security research. ORCHID seeks to understand, build, and apply human-agent collectives to symbiotically interleave human and computer systems with a view to realising our tremendous potential whilst avoiding the pitfalls that come with dependence.

Professor Shadbolt leads the ***Open Data Institute***, a £10M research institute which catalyses the evolution of open data culture to create economic, environmental, and social value. Among other things, it investigates privacy and anonymisation of open linked data.

Professor Butler conducts research on software verification and validation in cyberspace: project ***ADVANCE*** aims to develop of a unified tool-based framework for automated formal verification and validation of cyber-physical systems.

Professors Al-Hashimi and Butler lead the programme grant ***PRiME*** (£5.6M) on many-core technology and its profound implications on the energy efficiency, dependability and reliability of future embedded systems.

Professors Sung, Ma and Johnson were awarded the `Certificate of Excellence' by TSB for ***Developing a real-time models to strengthen risk management strategy***, a project with London Capital Group.

Under Professor Moreau's leadership, our research on provenance is thriving in new directions, including provenance anonymisation, summarisation and analytics, with services being exposed to the community at provenance.ecs.soton.ac.uk.

Contact

Professor Vladimiro Sassone

Cyber Security Research Centre, Director
University of Southampton
Southampton SO17 1BJ
United Kingdom

+44 (0)2380 599009

vsassone@soton.ac.uk

https://blog.soton.ac.uk/cybersecurity

facebook and twitter @CybSecSoton

Key areas of expertise and specialism

Southampton's core research expertise includes: analysis and design of trustworthy software; bio- and cyber-metrics; cyber identity; cyber risk analysis; cyber criminology; data privacy; international cyber law; provenance and trust; safety-and-security by design; secure embedded systems; secure web technologies; security of cyber-physical systems and internet-of-things; security of critical infrastructures, transport networks, and power grids.

University of Surrey

Surrey Centre for Cyber Security

Who we are

Surrey Centre for Cyber Security (SCCS), established in 2014, consolidates all the research activities in Cyber Security across the University of Surrey and is housed in the Department of Computing. The Centre is led by Prof Steve Schneider and has 8 core members with established track records in key technical areas of Cyber Security, and a further 20 associate members with interdisciplinary expertise. It has links with the 5G Innovation Centre, which opened in Surrey in 2015. Over the past five years, SCCS members supervised 36 PhD students and secured around £3.5M funding for research projects and PhD support from various funding bodies including EPSRC and industry. The Centre maintains close collaborative links with national and international partners and is guided by a dedicated Advisory Board. SCCS research covers Privacy and Data Protection, Secure Communications, and Human-Centred Security. SCCS also offers an Information Security MSc which was awarded provisional GCHQ Masters certification in 2014. A modern Applied Security Laboratory supports practical research and teaching activities.

What we do

SCCS research focuses on the technical foundations of information security, and on the design and development of cyber security technologies and their applications to real-world systems.

At the foundational level, the Centre has a strong capability in formal methods, with expertise in developing new methods for the modeling and analysis of large-scale complex systems. These have been applied in particular domains such as secure electronic voting, access control, identity management, secure communications, and rail control systems. A growing area is the design and deployment of new secure systems underpinned by these methods. The Centre has expertise in cryptography, and has developed new ways of protecting privacy in the digital world. In addition, the Centre also has a strong capability in multimedia security and digital forensics which enables the development of automated techniques and systems for crime

investigation and prevention. Human factors have almost as much to play in developing safe and secure systems as technology. Consequently the Centre has built up capability on human factors as part of a strongly interdisciplinary team which include experts from computer science, electronic engineering, criminology, psychology, law and economics.

Our work

Research by members of SCCS has led to a range of projects, including the following:

The ***Trustworthy Voting Systems*** project designed and developed a secure and robust voter-verifiable e-voting system, combining ballot secrecy and election integrity. The system's design is underpinned by cryptography, including mechanisms for key management and secure and private vote processing. The system was deployed by the Victorian Electoral Commission, Australia, for their 2014 State Election.

Work on ***Privacy-Preserving Authentication*** has designed new multi-party authentication protocols featuring additional privacy guarantees. One protocol was adopted in 2015 for integration into a popular privacy-preserving group chat platform Cryptocat.

A tool for analysing ***Role-Based Access Control Systems*** has been developed which allows the automated checking of policies against security requirements within administrative RBAC systems. Templates for relationship-based access control have also been developed.

Work on ***Forensic Analysis of Automated Number Plate Recognition Data***, in collaboration with Surrey Police and two industrial partners, aims to identify new behavioural information about criminals to enable proactive law enforcement. Specific attention is paid to protect privacy of non-criminal drivers.

Work on ***Protection of Digital Media Content*** developed an innovative framework for protecting digital media content without the disadvantages of traditional digital rights management.

Work on ***Security Architecture for Satellite services*** led to a hierarchical and distributed security architecture which can protect data transmitted over cryptographically heterogeneous networks. The results are also applicable to mobile, ad-hoc and sensor networks.

Contact

Prof Steve Schneider

University of Surrey
Department of Computing
Guildford GU2 7XH

+44 (0) 1483 68 9637

s.schneider@surrey.ac.uk

http://sccs.surrey.ac.uk

Key areas of expertise and specialism

- Systems security and reliability: formal analysis and verification, protocols, applied cryptography, human factors
- Digital forensics, cybercrime and criminology
- Secure communications: networks, mobile, satellite, 5G

Glossary of terms

5G	5th generation mobile network
ACE-CSR	Academic Centre of Excellence in Cyber Security Research
BIS	UK Department for Business, Innovation and Skills
CPNI	Centre for the Protection of National Infrastructure
DCMS	UK Department for Culture, Media & Sport
DoS/DDoS	(Distributed) denial of service attack
DSTL	Defence Science and Technology Laboratory
ENISA	European Network and Information Security Agency
EPSRC	Engineering and Physical Sciences Research Council
ERC	European Research Council
ESRC	Economic and Social Research Council
EU	European Union
GCHQ	UK Government Communications Headquarters
HEFCE	Higher Education Funding Council for England
IT	Information Technology
ICT	Information Communications Technology
JANET	A private, UK Government-funded organisation providing computer services to UK education and research
JISC	Represents the UK further & higher education sector on the use of digital technologies
MoD	UK Ministry of Defence
MSc	Master of Science, a UK post-graduate qualification
PhD	Post-graduate doctoral qualification available in the UK
RCUK	Research Councils UK
RFID	Radio Frequency Identification
TSB	Technology Strategy Board, now renamed as Innovate UK
UKTI	UK Trade and Investment

Further information

UK Government www.gov.uk
UK Trade & Investment www.ukti.gov.uk
Engineering and Physical Sciences Research Council www.epsrc.ac.uk
UK Cyber Security Strategy www.gov.uk/government/publications/cyber-security-strategy
Contact point for general information cybersecurity@bis.gsi.gov.uk

HM Government

This publication is available from www.gov.uk

Any enquiries regarding this publication should be sent to:

Department for Culture, Media & Sport
100 Parliament Street
London SW1A 2BQ
Tel: 020 7211 6000

If you require this publication in an alternative format, call 020 7211 6000.

DCMS/15/999