HM Government

Developing our capability in cyber security

Academic Centres of Excellence in Cyber Security Research

PHOTO REDACTED DUE TO THIRD PARTY RIGHTS OR OTHER LEGAL ISSUES

Contents

Developing our knowledge and capability to secure UK cyber space

The world is becoming 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 is responding to these challenges. In 2011 the UK ratified the Budapest convention on cybercrime and hosted the first international conference on cyberspace in London, stimulating a global debate on how to protect the economic and social dividends of cyberspace from growing threats. Since then, the UK cyber security strategy – a five-year Government and industry partnership, backed with £860m of funding – has been improving the security and resilience of the UK, and promoting growth in UK cyber sector. As a result of these actions, the UK has 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 eleven universities as Academic Centres of Excellence in Cyber Security Research (ACE-CSRs). Further information on these centres is detailed in this document. These Centres of Excellence form the backbone of the UK's world leading cyber security research. It is crucial for academia to work closely with industry and ensure the UK benefits fully from this knowledge and expertise on cyber security. 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 industrial strategy, helping to generate growth 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 how these centres will provide cutting-edge cyber knowledge and expertise, and contribute towards a secure, resilient and vibrant cyber space.

David Willetts

Rt. Hon. David Willetts MP
Minister for Universities and Science
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 Business, Innovation and Skills (BIS), 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 eleven 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.

During autumn 2014 there will be a further call for universities to apply to be recognised as ACE-CSRs.

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	● Secure software ● Human and economic aspects of security ● Privacy and anonymity ● Cryptology
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
18 – 19	University of Bristol	● Theory, design, implementation & analysis of protocols & systems that use (or relate to) cryptography

Page	Name of centre	Key areas of expertise/specialism
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 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.
24 – 25	University of Oxford	● Analysis and verification of software and security protocols ● Systems security; trustworthiness and usability ● Inter-disciplinary cyber security, policy and governance
26 – 27	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

PHOTO REDACTED DUE TO THIRD PARTY RIGHTS OR OTHER LEGAL ISSUES

PHOTO REDACTED DUE TO

PHOTO REDACTED DUE

Imperial College London

Engineering Secure Software Systems

PHOTO REDACTED DUE TO THIRD PARTY RIGHTS OR OTHER LEGAL ISSUES

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

PHOTO REDACTED DUE TO PHOTO REDACTED DUE TO THIRD PARTY RIGHTS OR OTHER LEGAL ISSUES

Photograph: John Donoghue

PHOTO REDACTED DUE TO THIRD PARTY RIGHTS OR O

Newcastle University

Centre for Cybercrime and Computer Security

PHOTO REDACTED DUE TO THIRD PARTY RIGHTS OR OTHER LEGAL ISSUES

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)

PHOTO REDACTED DUE TO THIRD PARTY RIGHTS OR OTHER LEGAL ISSUES

[redacted]

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

PHOTO REDACTED DUE TO THIRD PARTY RIGHTS OR OTHER LEGAL ISSUES

PHOTO REDACTED DUE TO TI

Queen’s University Belfast

The Centre for Secure Information Technologies

PHOTO REDACTED DUE TO THIRD PARTY RIGHTS OR OTI

Who we are

The Centre for Secure Information Technologies (CSIT) is a Global Innovation Hub for Cyber Security Research. Established in 2009 with initial funding in the region of £30M, CSIT is the EPSRC/TSB Innovation and Knowledge Centre in Cyber Security.

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

Specifically, CSIT has core capabilities in:

- Cyber physical systems security
- Real-time network analytics and virtualisation
- High performance/resource constrained cryptography architectures

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 an environment 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’.

CSIT is engaged in a number of cyber security collaborative research projects with world leading organisations including BAE Systems, Cisco, IBM, Intel, Infosys, McAfee, Thales, numerous SMEs, spin-out ventures (Titan IC Systems, Microsense, Activ Wireless) and leading institutes in USA, South Korea, India and Europe. CSIT are

Queen’s University Belfast

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES active members of ETSI, ADS and Information Security Ireland.

Our Work

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

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 ARIES (Accelerated Real-Time Information Extraction System) EPSRC project is investigating a new generation of data and memory centric parallel processing architectures and data mining algorithms optimised for mining very large, diverse and highly distributed data assets.

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 cyber-crime in the UK.

PHOTO REDACTED DUE TO THIRD PARTY RIGHTS OR OTHER LEGAL ISSUES

The LIOPA (Lip Verification & Online Person Authentication) SBRI project is a novel mobile biometric authentication and speaker verification application, service and application programming interface (API). Liopa won the Software and Digital media category at the 2013 NISP Connect 25K Awards for the most innovative publicly funded research and intellectual property.

The HANDHOLD (HANDHeld OLfactory Detector) FP7 project is developing a modular, reconfigurable sensor system for active stand-off deployment for the detection of chemical, biological, radiological, nuclear and explosive (CBRNE) substances. CSIT became the first team from Northern Ireland to both co-ordinate and win an FP7 security proposal.

CSIT has also delivered industry contract research and development covering malware reverse engineering, Zero Day attacks, network processing hardware design, Video Coding QoS, 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:

- Cyber physical systems security
- Real-time network analytics and virtualisation
- High performance/resource constrained cryptography architectures

PHOTO REDACTED DUE TO THIRD PARTY RIGHTS OR OTHER LEGAL ISSUES

PHOTO REDACTED DUE TO

PHOTO REDACTED DUE TO THIRD PARTY RIGHTS OR OTHE

PHOTO REDACTED DUE TO THIRD PARTY RIGHTS OR OTHER LEGAL ISSUES

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.

ROYAL
HOLLOWAY
UNIVERSITY
OF LONDON

What we do

The activities of the ISG are supplemented by the 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.

The ISG was founded by a group of mathematicians and computer scientists with interests in cryptography, and research in this area remains an important part of the ISG's activities. It has expertise in cryptanalysis, combinatorial cryptography, quantum information theory and cryptography, provable security and message authentication codes. The scope of the ISG's research has expanded dramatically in the last 15 years and now includes access control, authentication and identity management, economics of security and trust, social and organisational aspects of cyber security, malware and botnet detection, the security of systems and technologies (ranging from RFID tags through to global telecommunications networks and critical infrastructure protection), and vulnerability analysis. Royal Holloway has received substantial funding in the last 12 months 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, and security in the internet of energy.

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. Royal Holloway's Smart Card Centre also offers specialised advice on smart cards, mobile devices, near-field communications and associated technologies. The Centre's experts have advised in all these areas, and have also guided external organisations with their own information security research and development programmes.

PHOTO REDACTED DUE TO THIRD PARTY RIGHTS OR OTHER LEGAL ISSUES

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 RFID tags, smart cards, mobile & embedded devices

PHOTO REDACTED DUE TO THIRD PARTY RIGHTS OR OTHER LEGAL ISSUES

PHOTO REDACTED DUE TO TH

University College London

PHOTO REDACTED DUE TO THIRD PARTY RIGHTS OR OTHER LEGAL ISSUES

Who we are

The University College London ACE-CSR spans five research groups within the Computer Science Department and also includes the departments of Chemistry and Security and Crime Science, which hosts the SECReT doctoral training centre. Currently the Centre has 17 academics, with Jens Groth as Director.

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 University of London, Royal Holloway, Newcastle University and Northumbria University, funded by a £3.8m grant from EPSRC, GCHQ and BIS.

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, privacy, identity and trust, and cryptology. The Centre for Research, Evolution, Search and Testing (CREST) develops tools for testing software and eliminating bugs. The Programming Principles, Logic and Verification Group does research on automatic verification 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.

Cyber security research is one of UCL's strategic research priorities and UCL has recently 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.

UCL is educating future cyber security professionals through its MSc and PhD programmes. The MSc in Information Security is a one-year programme where students take taught modules ranging from cryptography, computer security and secure programming languages, to information security management and human aspects of security. At the end of the programme the students write a master thesis based on guided research in information security.

Our work

In the Wedge project our staff, in collaboration with PhD students, designed and built new operating system primitives, new development tools and new least-privilege application architectures which prevent sensitive data from falling into the hands of an attacker, even if the attacker successfully exploits a vulnerability in a network-attached server's (or client's) software. The tools reduced the number of lines of trusted code in the Apache/OpenSSL web server by 94%, while requiring changes to only 1700 of Apache/OpenSSL's 250K+ total lines of code.

The Trust Economics project brought together a multi-disciplinary (technical security, human factors, economics) academia-industry team to model organisational security to support security decision-making. The UCL team led by Angela Sasse contributed by quantifying and modelling impact of security mechanisms on the individual and ultimately organisational productivity level and the risk mitigation achieved. The project team produced the first organisational model of the cost and benefits of a specific security measure, the first model of security compliance decisions made by individuals, and showed how unworkable security policies lead to inefficient business processes and ineffective security.

The CREST centre has developed tools and techniques for generation of test cases and optimisation of regression testing activities using Search Based Software Engineering (SBSE). Test generation can be used to find flaws in software that may be exploited by attacker and the work on regression testing can be used to check that changes to software do not introduce new potential vulnerabilities. The work on SBSE for test data generation is now part of a tool called AUSTIN that is available as an open source tool for C.

Contact

Director of the Centre: **Dr Jens Groth**,
Reader in Cryptology

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

+44 (0)20 7679 7214

j.groth@ucl.ac.uk

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

Key areas of expertise and specialism

- Secure Software
- Human and Economic Aspects of Security
- Privacy and Anonymity
- Cryptology

PHOTO REDACTED DUE TO THIRD PARTY RIGHTS OR OTHER LEGAL ISSUES

PHOTO REDACTED DUE TO THIRD PARTY RIGHTS OR OTHER LEGAL ISSUES

PHOTO REDACTED DUE TO TH

University of Birmingham

PHOTO REDACTED DUE TO THIRD PARTY RIGHTS OR OTHER LEGAL ISSUES

The School of Computer Science

Who we are

The computer security team at the University of Birmingham was founded in 2005 by Professor Mark Ryan and has steadily grown with expertise in cyber security research.

The team is comprised of ten academics and currently five postdoctoral fellows, nine PhD students and one research assistant. The key academics involved are; Professor Mark Ryan (trusted computing, electronic voting, balancing privacy and security, access control and cloud computing), Dr Rami Bahsoon (cloud computing security, software engineering security and information flow), Dr Behzad Bordbar (cloud computing security and software engineering security), Dr Tom Chothia (statistics and information theory, anonymity, distributed systems and RFID), Dr Marco Cova (web security, vulnerability analysis, intrusion detection and electronic voting), Dr Flavio Garcia (cryptographic protocols and primitives, cryptanalysis and reverse engineering, embedded devices security, RFID and privacy), Dr Mirco Musolesi (software engineering, security and human factors in security), Dr Shishir Nagaraja (network security and privacy, anonymity, privacy, graph theory, network resilience and malware analysis), Dr Eike Ritter (modelling and analysing protocols, operating systems and security of pervasive systems) and Dr Hayo Thielecke (software security, program logics and programming language constructs).

UNIVERSITY OF
BIRMINGHAM

What we do

The effective ethos of the computer security team at Birmingham is working with Government and industry to tackle cyber security problems which are important to society. Critical issues which underpin the research within the team include the analysis and verification of systems, privacy and security, malware, intrusion detection, web security, botnets and secure software engineering.

Our work

Research currently underway in the computer security team includes *'Trustworthy Voting Systems'*. Led by Professor Ryan, this specific research project is helping to create systems for electronic voting which are secure and usable in large scale elections. The team have developed 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.

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 Birmingham group 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 a serious flaw in e-passports that jeopardises the privacy of anyone who carries an e-passport. 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 detecting botnets (networks of private computers infected with foreign agents or malicious software unbeknownst to computer owners) and defending computer users against them. Dr Shishir Nagaraja is working on research which examines the communication structures and patterns of peer-to-peer botnets and is using this as a basis for developing botnet defence.

PHOTO REDACTED DUE TO THIRD PARTY RIGHTS OR OTHER LEGAL ISSUES

Securing anti-theft devices is a 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 immobiliser industry. The flaws that have been illustrated by Dr Garcia include serious attacks which can recover the secret key from a car in less than six minutes using ordinary hardware.

The Security and Privacy Group at the University of Birmingham are vigorously researching the impact on national resilience around financial services, electronic voting, personal privacy, mobile phones, passports and the effective development of scalable and secure cloud computing and services. These are all important issues that need to be addressed in a world where technology is advancing. The team are committed to finding long-term solutions to these 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

m.d.ryan@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

PHOTO REDACTED DUE TO THIRD PARTY RIGHTS OR OTHER LEGAL ISSUES

PHOTO REDACTED DUE TO T

University of Bristol

Bristol Security Centre

PHOTO REDACTED DUE TO THIRD PARTY RIGHTS OR OTHER LEGAL ISSUES

PHOTO REDACTED DUE TO THIRD PARTY RIGHTS OR OTHER LEGAL I

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).

University of BRISTOL

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.

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.

PHOTO REDACTED DUE TO THIRD PARTY RIGHTS OR OTHER LEGAL ISSUES

PHOTO REDACTED DUE TO 1

PHOTO REDACTED DUE

University of Cambridge

PHOTO REDACTED DUE TO THIRD PARTY RIGHTS OR OTHER LEGAL ISSUES

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:

PHOTO REDACTED DUE TO THIRD PARTY RIGHTS OR OTHER LEGAL ISSUES

- 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

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

PHOTO REDACTED DUE TO THIRD PARTY RIGHTS OR OTHER LEGAL ISSUES

PHOTO REDACTED DUE TO

PHOTO REDACTED DUE TO THIRD PA

University of Lancaster

Security Lancaster

PHOTO REDACTED DUE TO THIRD PARTY RIGHTS OR OTHER LEGAL ISSUES

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).

Security Lancaster | LANCASTER UNIVERSITY

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.

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).

PHOTO REDACTED DUE TO THIRD PARTY RIGHTS OR OTHER LEGAL ISSUES

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.

PHOTO REDACTED DUE TO THIRD PARTY RIGHTS OR OTHER LEGAL ISSUES

PHOTO REDACTED DUE TO

PHOTO REDACTED DUE TO THIRD PARTY RIGHTS OR OTHER LE

PHOTO REDACTED DUE

University of Oxford

Oxford University Cyber Security Centre

Who we are

The Oxford University Cyber Security Centre works over six departments within the University, integrating the work of around twenty 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 Centre, 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 Centre 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 Centre 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, and operations management. The Centre's work 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.

UNIVERSITY OF OXFORD

CYBER SECURITY CENTRE

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 the Centre to win a major CPNI-sponsored project in Corporate Insider Threat Detection. The project combines perspectives from across the Centre'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 new initiative is the Centre 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.

PHOTO REDACTED DUE TO THIRD PARTY RIGHTS OR OTHER LEGAL ISSUES

[redacted]

The Global Centre for Cyber Security Capacity-Building, 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.

The research of the Centre 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, PI for ACE-CSR and Director of the CDT in Cyber Security

Sadie Creese, Professor of Cyber Security

Cyber Security Centre
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

PHOTO REDACTED DUE TO THIRD PARTY RIGHTS OR OTHER LEGAL ISSUES

PHOTO REDACTED DUE TO

University of Southampton

CyberSecurity Southampton

PHOTO REDACTED DUE TO THIRD PARTY RIGHTS OR OTHER LEGAL ISSUES

Who we are

CyberSecurity Southampton focuses on the security of cyberspace from malicious digital threats. The Centre's multidisciplinary expertise contributes knowledge, understanding and innovation to the protection of critical infrastructures, users, their data and interests, and connects activities across electronic and software systems, advanced networking and protocols, cyber-risk behaviour, cybercrime, social and legal acceptability of cyber regulations, and physical and cyber identity management.

The team is led by Professor Vladimiro Sassone, a leading figure in Computer Science. The Centre, however, draws expertise from across the university, including criminology, law, management, mathematics, (nano) electronics, psychology, sociology and web science. This places the Centre in a unique position. It can respond to the need to help UK Government, business and consumers become more resilient to cyber-attacks. In addition, it 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 privacy.

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.

CyberSecurity Southampton has decennial experience in joint hardware/software operations and world-class expertise on critical infrastructures, such as communications and the web, an in-house nano-fabrication facility and a well integrated research portfolio linking together in a full circle (opto) electronics, computer science and engineering, social and human aspects of cyber security.

The Centre's vision is informed by such strengths, and by the understanding that outsourcing the manufacturing of even the most elementary component unwisely may lead to unacceptable security risk. In particular, the 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 cyber space 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 advising, consultancy, training and education
- 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

Professors Jennings, Moreau and Rogers have secured the programme grant *ORCHID* (£5.5m) which supports CyberSecurity 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 Rogers leads industry-funded *IDEAS* on future power-grid infrastructures in which intelligent sensing devices allow users to make informed choices, and smart appliances can negotiate and coordinate for optimal energy use.

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 (de-)anonymisation of open linked data.

Professor Shadbolt has secured the programme grant *SOCIAM* (£6.2m), which aims to derive the characterisation of social systems on the web as "social machines," computational entities governed by both computational and social processes.

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

Dr. Stevenage's *SuperIdentity* aims to develop a rich understanding of identity, drawing on who we are in the cyber world as well as the real world. The fusion of cyber and real world information supports robust identification decisions, guiding intelligence and surveillance efforts and revealing previously hidden information.

Contact

Professor Vladimiro Sassone

Electronics and Computer Science
University of Southampton
University Road, Southampton SO17 1BJ

+44 (0)2380 599009

vsassone@soton.ac.uk

http://www.cybersecuritysoton.org

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, cybercrime, data privacy, international cyber law, provenance and trust, safety-and-security by design, secure embedded systems, secure web technologies.

Glossary of terms

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
DoS/DDoS	(Distributed) denial of service attack
ENISA	European Network and Information Security Agency
EPSRC	Engineering and Physical Sciences Research Council
ERC	European Research Council
ESRC	Economic and Social Research Council
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
TSB	Technology Strategy Board
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 biscybersecurity@bis.gsi.gov.uk

HM Government

This publication is available from www.gov.uk/bis

Any enquiries regarding this publication should be sent to:

Department for Business, Innovation and Skills
1 Victoria Street
London SW1H 0ET
Tel: 020 7215 5000

If you require this publication in an alternative format, email biscybersecurity@bis.gsi.gov.uk, or call 020 7215 5000.

BIS/14/660