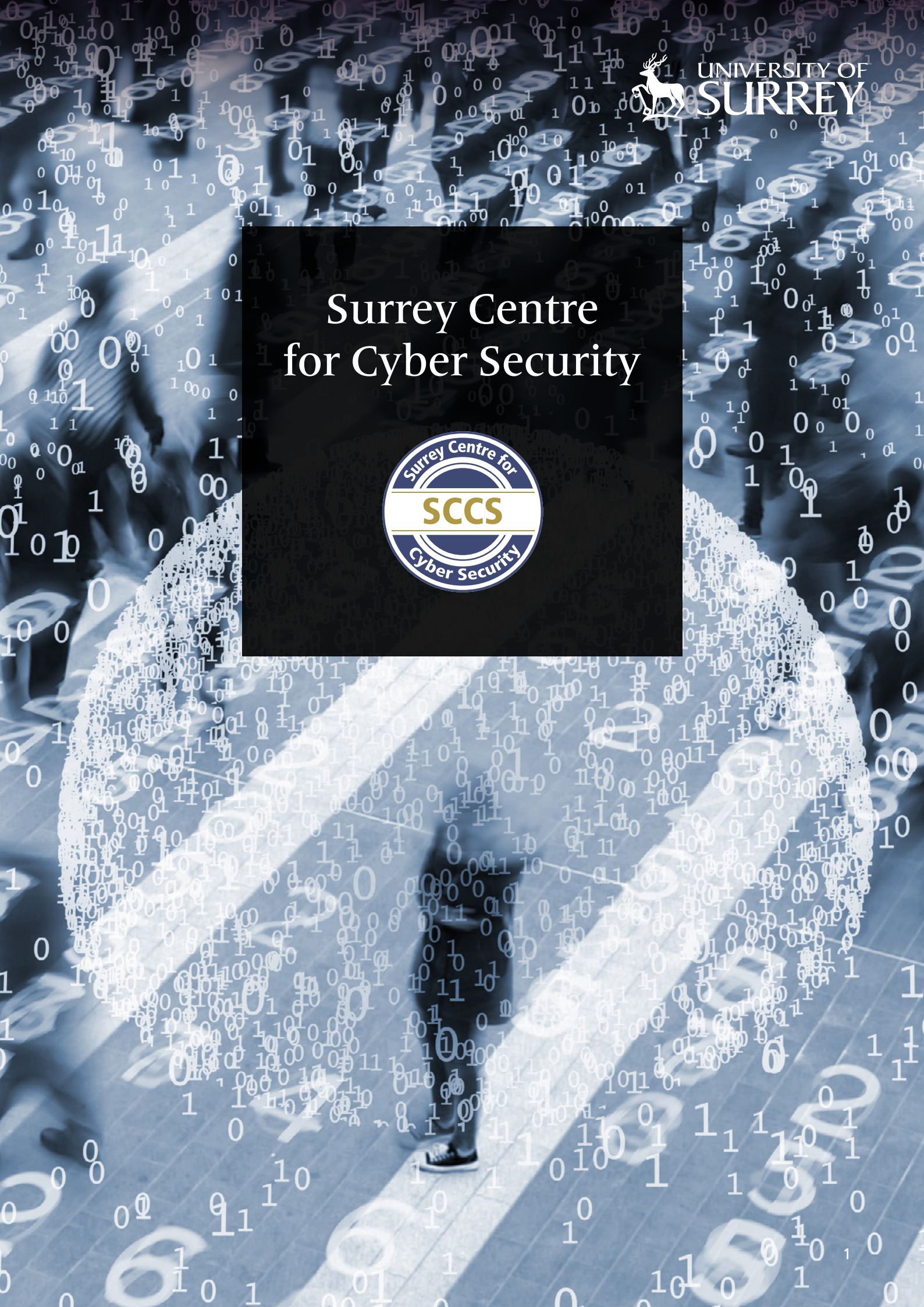

UNIVERSITY OF
SURREY
Surrey Centre
for Cyber Security
Surrey Centre for
SCCS
Cyber Security

"The exponential growth of computer technology has revolutionised the way we do business, organise our lives and interact socially, but has brought new and ever-growing dangers in terms of security. Data leaks and tampering due to cyber attacks can have serious implications in areas such as healthcare, finance and automotive technologies.

"Defending these technologies requires a highly systematic approach, with rigorous analysis against the possible attack vectors, and the use of cryptography to guarantee security, even in the presence of such attackers.

"The SCCS, through its ACE-CSR status, operates within a community of academics, industry and government across the UK and throughout the world dedicated to finding ways of mitigating the cyber security threats faced by individuals and organisations. The Centre's focus is to create methods and techniques which ensure the safety of computer systems, and to apply formal modelling to verify their security. Our areas of expertise include protocol analysis, security verification, trusted computing, data privacy and privacy-preserving computing, user authentication, applied cryptography, distributed ledger technologies, digital forensics, multimedia security and human factors. A growing area for us is 'security through hardware', which focuses on the hardware, and especially TPMs (trusted platform modules), to ensure the security of computer systems.

"Using these techniques, and working in collaboration with industry partners, we strive to develop solutions that will enable society and industry to benefit from advanced technology in a secure way."

Professor Steve Schneider
Director of SCCS

Surrey Centre for Cyber Security (SCCS)

The Surrey Centre for Cyber Security (SCCS) consolidates research activities in cyber security across the University of Surrey. It brings together expertise within the Department of Computer Science (the Centre's technical core) and Department of Electrical and Electronic Engineering, with input from Sociology, Psychology, Business, Law and Economics.

SCCS provides a platform to explore the cyber security challenges being presented by next-generation mobile communications via joint research with Surrey's 5G Innovation Centre (5GIC).

Academic Centre of Excellence in Cyber Security Research (ACE-CSR)

The University of Surrey is recognised as one of the Government's Academic Centres of Excellence in Cyber Security Research (ACE-CSR). The status, which was renewed for a further five years in April 2017, is given by the National Cyber Security Centre (NCSC) in partnership with Research Councils UK (RCUK) and the Department for Business, Energy and Industrial Strategy (BEIS). Surrey is one of only 14 UK universities with ACE-CSR status.

National Cyber Security Centre

EPSRC
Engineering and Physical Sciences Research Council

Academic Centre of Excellence in Cyber Security Research

14 academic core members

21 academic associates

20 researchers

£5m
Funding*

25 projects*

(*since 2012)

Research themes

- SECURITY THROUGH HARDWARE
- TRUSTED COMPUTING
- PRIVACY & AUTHENTICATION
- SECURE COMMS
- MULTIMEDIA & FORENSICS
- HUMAN FACTORS

Key sectors

- AUTOMOTIVE
- DEMOCRACY
- FINANCE
- FUTURE INTERNET
- HEALTH
- LAW ENFORCEMENT
- RAIL

MSc in Information Security

Drawing on the University's research in cyber security, our Masters course in Information Security is fully accredited by the National Cyber Security Centre (NCSC). The course combines a theoretical grounding in cyber security – covering a broad spectrum of disciplines – with the opportunity to gain practical experience through lab sessions and projects, equipping students for careers in the information security sector.

Examples of modules:

Dissertation
Information and Network Security
Symmetric Cryptography
Asymmetric Cryptography
Information Security Management
Multimedia Security and Digital Forensics
Secure Systems and Applications
Information Security for Business and Government
Project Management and Business Strategy
Database Systems
Cloud Computing

SECURITY THROUGH HARDWARE

We can use hardware to make systems more secure; however adding extra hardware is costly and can make the system inflexible. Since security is an evolving problem – where attackers compete to find flaws and vulnerabilities in defensive mechanisms – inflexibility can be a real issue. In SCCS we are working to design security mechanisms that provide some flexibility and can still be cheaply implemented in hardware.

Trusted Platform Module (TPM) – security and privacy

An emerging area of work for SCCS, Security Through Hardware focuses on the development and evolution of TPM – a hardware chip which is used as a root of trust and a cryptographic engine for a computing system. To make its host computer platform trustworthy, the TPM is embedded in the platform and provides evidence about the software state of the platform. The TPM integrates cryptographic keys and algorithms to protect the system from software attacks, and the protection is ensured since the TPM is designed to be tamper resistant.

This area of work is being led at SCCS by Professor Liqun Chen who, during her 19 years with Hewlett Packard (HP) Labs – latterly as principal research scientist – made important contributions to the development of first and second generation TPMs (TPM 1.2 and TPM 2.0) which are now incorporated into over a billion computers worldwide.

The Trusted Computing Group, founded by HP, IBM, Microsoft, Intel and Compaq, is a global industrial standard organisation and develops the specifications of TPMs. As part of the TPM technology, Professor Chen co-designed Direct Anonymous Attestation (DAA), a special digital signature scheme which provides the signer with authentication while maintaining their privacy. This solved an issue which previously prevented the TPM specification from being accepted – the fact that by authenticating their systems, users would also be revealing sensitive information.

SCCS is now focusing on developing the next generation TPM which will be required to maintain security in the era of quantum computers.

Professor Chen commented: "The National Institute of Standards and Technology predicts that quantum computers will become a reality in 2030. These computers will be able to break some cryptographic algorithms currently used in TPMs. An important part of our current work is therefore developing quantum-resistant algorithms suitable for inclusion in future TPMs."

Three PhD projects within this area of research are exploring areas such as lattice-spaced cryptography and quantum-resistant cryptography implementation.

In addition, SCCS is providing a unique opportunity for Masters students to conduct experiments using TPMs, as a result of equipment donated by industry partner Infineon Technologies AG (in Germany) and a small grant from NCSC (the National Cyber Security Centre).

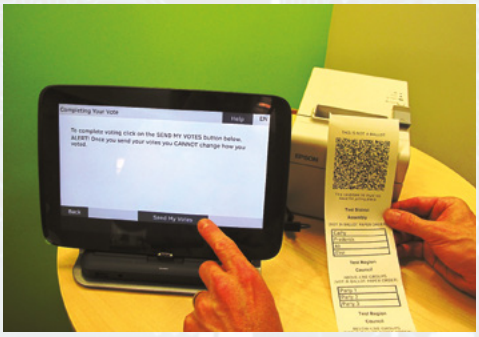
TRUSTED COMPUTING

Consumers need to have trust when they interact with technology, but as the range of devices we use grows, the number of vulnerabilities which attackers can exploit is rapidly increasing. Drawing on a breadth of expertise in trusted computing, we embrace a 'security by design' principle, embedding security into the fabric of the systems we build rather than seeing it as an 'add-on'.

Case study: Trustworthy voting project

Representing a world first, computer scientists at SCCS developed an end-to-end verifiable electronic voting system which was successfully deployed in the State of Victoria election in Australia in November 2014.

In a controlled deployment during the Victoria election, there was a very low level of spoilt ballots (1.9 per cent compared with 4.3 per cent for paper voting).



While various 'e-voting' systems have been piloted around the world, this system – developed by Professor Steve Schneider and Dr Chris Culnane – for the first time enables voters to cast their vote and verify that the vote has been correctly cast, while also ensuring voting secrecy.

Based on open source code, the system features a printed ballot form with the candidates listed in a randomised order (ie in a different order on different ballot forms). The voter makes their selection and then destroys the list of candidates, retaining and casting their marked preference list for verifiable tallying.

The system was developed in conjunction with the State of Victoria to meet the needs of its 2014 election. With voting compulsory in Australia, the election authorities are obliged to make every effort to enable people to vote, so better accessibility for the blind, partially-sighted and motor-impaired voters was a key requirement. The system also needed to cater for the broad range of languages spoken by Victoria's citizens and, since Victorian elections are based on the single transferable vote, the ballot is very complex, with voters required to rank a list of around 40 candidates in their preferred order.

Surrey's verifiable voting system was able to meet these needs and – by incorporating an audio interface – also enable blind and partially-sighted voters to cast a fully secret vote in a verifiable way. In a controlled deployment during the Victoria election, there was a very low level of spoilt ballots (1.9 per cent compared with 4.3 per cent for paper voting), and a survey of voting at the Australia Centre in London, where it was also tested, found that 75 per cent preferred the electronic system to paper voting.

Trusted and transparent voting systems

The VOLT (Voting on Ledger Technologies) project beginning in September 2017, funded by EPSRC (Engineering and Physical Sciences Research Council), will focus on developing systems that both enable verifiable voting and manage voting rights. Based on distributed ledger technologies, these systems will be designed for voting within corporate companies and organisations where, for example, shareholders may hold differing voting rights. The project is being conducted in collaboration with Kings College London and three industry partners: Electoral Reform Services, Crowdcube and Monax Industries.

PRIVACY & AUTHENTICATION

Modern web and mobile computing technologies, combined with changing paradigms in cloud computing, seamless mobility and social media computing, mean we need new protection mechanisms for securing huge amounts of data while, at the same time, protecting the privacy of individuals and organisations.

Case study: Improving the customer experience for rail passengers

Cyber security is increasingly relevant in the rail industry where the introduction of real-time customer service using mobile technology will require passengers to reveal personal information about themselves and their journeys. Three current projects are aimed at improving and influencing the customer experience while ensuring data privacy.

The EPSRC-funded DICE (Data for Improved Customer Experience) project, which began in September 2016, looks at the protection of personal data while using it to provide real-time customer service for passengers throughout a journey. Aimed at building a framework to manage the trade-off between sharing private data and the benefits this can bring, the project is currently investigating the concept of 'smart ticketing', looking at ways of anonymising the ticket purchaser's data. DICE is supported by the Rail Delivery Group (RDG) and the Rail Safety and Standards Board (RSSB), Pervasive Intelligence Ltd and the Digital Catapult. It was one of three projects awarded to Surrey – together worth nearly £3m – by EPSRC on the theme of TIPS (Trust, Identity, Privacy and Security).

SCCS researchers have also begun work on a project which aims to effectively evaluate the influence that enhanced information – for example the sequence of a train's carriages – could have on passengers' positioning and boarding behaviour at the PTI (Platform Train Interface). This will include identifying what relevant information could be collated from existing, publically-available data feeds and train operator data, and finding novel ways of using mobile technologies to collect additional information about an approaching train.

Finally the £1.4m TOC Ability project, launched in March 2017, is aimed at enhancing accessibility to rail services. TOC Ability is a digital platform concept that could bring real improvements to train journeys for disabled customers by enabling their requirements to be shared with train companies, bus and taxi firms, food and beverage retailers, and even chemists, through an 'intelligent accessibility hub'. In this project, which involves collaboration with Transport for London, Arriva UK Trains and Atkins among other partners, SCCS researchers will help to develop a unique consent management system which will protect passengers' personally identifiable information.

Case study: Creating trust from a 'TAPESTRY' of everyday signals

"The first challenge is to understand what makes up a person's online presence, which can include interactions on social media and with many different IoT devices."
– Dr Mark Manulis

Online fraud and scams currently cost the UK economy around £670m each year, with crimes often perpetrated through false identities, so there is an urgent need for people and services to be able to provide proofs of trust in order to interact safely in the Digital Economy.

The aim of the TAPESTRY (Trust, Authentication and Privacy over a DeCentralised Social Registry) project is to investigate, develop and demonstrate new technologies that will enable people, businesses and digital services to connect safely online. A collaboration between Surrey and the Universities of Dundee and Northumbria, and a number of industry and government partners, the project explores the complex 'tapestry' of signals woven by people's everyday digital interactions: their 'digital personhood'.

"The first challenge is to understand what makes up a person's online presence, which can include interactions on social media and with many different IoT devices," explained Dr Mark Manulis of SCCS. "People and businesses need to build the trust of other users but at the same time, their privacy must also be protected."

The solution being developed in the TAPESTRY project will use cryptographic protocols to securely collect trust evidence within distributed ledgers with no central control (such as Blockchain). The idea will be that users 'opt in' to the service in order to provide evidence to verifiers for a given time period and a given granularity. One concept being explored in the project is 'zero knowledge proofs' which would, for instance, enable a verifier to prove that they are over 18 without disclosing their date of birth.

TAPESTRY is being led at Surrey by academics within SCCS, CVSSP (the Centre for Vision, Speech and Signal Processing) and the 5G Innovation Centre.

Case study: Privacy-preserving authentication in smart vehicle communications

Smart vehicles are expected to significantly improve driving experience and increase safety on public roads, as well as opening the door to new applications requiring communication between vehicles and their environment.

However since many of the applications envisioned for smart vehicles – such as collision avoidance and traffic management – are safety critical, it is vital that these communications are authenticated. Privacy is also a major concern because the ability to track smart vehicles could lead to profiling of drivers.

This project is developing new protocols for authentication in smart vehicle communications, based on novel attribute-based signatures. These signature schemes will potentially offer a more effective solution than existing schemes, which rely on pseudonyms, and are known to have scalability limitations as well as privacy concerns.

SECURE COMMUNICATIONS

With the seamless integration of embedded devices into the global communication network infrastructure (the Internet of Things) and ultra-high speed mobile and wireless connectivity on the horizon, future communication systems need to incorporate novel protection mechanisms to ensure security, reliability, and adequate fault tolerance.

Case study: Secure communications for Intelligent Transport Systems

Future Intelligent Transport Systems – which promise to help improve road safety and traffic management, and provide 'greener' roads – also present challenges in terms of security and privacy.

Under an iCase bursary, sponsored by EPSRC and Thales UK, PhD student Jorden Whitefield is conducting security protocol analysis in this field, focusing both on how Intelligent Transportation Systems behave and how individuals using these systems can be protected from being tracked or profiled.

Jorden explained: "In the vehicle domain, drivers are constantly broadcasting their location, which could make them vulnerable to someone wishing to cause them harm, or to a malicious party who would have the ability to profile a person's travel patterns. Another important challenge is revocation. If a vehicle is malfunctioning or malicious, we need to remove its effect from the network."

Conducted in collaboration with Thales UK, the project is focused on identifying 'symbolic protocol analysis' based on descriptions of behaviour and message exchange. The aim is to use formula to check whether the necessary behavioural, security and privacy properties are present within a system's design. The work draws on SCCS's expertise in TPMs (Trusted Platform Modules) and TEEs (Trusted Execution Environments) and could be adopted by standard bodies in the future

Safeguarding privacy in our digital society

Led by Dr Ioana Boureanu, the LV-Pri20 project has been aimed at safeguarding our security and privacy in the digital age, in line with the EU H2020 Flagship Initiative on a Digital Agenda.

The focus of the project is identifying different ways of verifying both privacy and security properties in today's ICT systems – from IoT-driven lightweight authentication schemes to modern architectures of established protocols such as the TLS (Transport Layer Security) suite. In addition to cryptographic proofs, which are typically devised to ascertain the security of systems in a one-session scenario, the researchers are developing automatic analysis techniques which assess the security of multi-session execution of systems.

Case study: Enabling trust in location-based services

Researchers in SCCS and 5GIC are working on the GEOSEC project, in partnership with Ordnance Survey, which aims to analyse the security and privacy weaknesses of existing techniques for location-based information delivery services, and design a new lightweight integrated security/privacy solution with low networking overheads.

GEOSEC is part of the PETRAS IoT Research Hub – a consortium of nine leading universities including Surrey – which explores critical issues in privacy, ethics, trust, reliability, acceptability and security. The Hub is funded by a £9.8m grant from EPSRC, along with partner contributions of around £13m.

MULTIMEDIA AND FORENSICS

SCCS is leading research into multimedia security and digital forensics, helping to develop technical solutions to tackle cybercrimes such as online grooming and digital piracy. We work closely with law enforcement agencies such as Surrey Police, National Crime Agency, Europol's European Cybercrime Centre (EC3) and other government bodies in this field.

Case study: ANPR data analysis to identify criminal behaviour

The organised nature of some crimes, such as drug trafficking and terrorism, makes it difficult to identify the perpetrators. One solution employed by police is to utilise ANPR (automatic number plate recognition) data to determine offenders travelling in convoy, but this is typically done manually and relies on having prior information about one known vehicle.

Aimed at making criminal investigations more effective, accurate and resource-efficient, the POLARBEAR (Pattern of Life ANPR Behaviour Extraction Analysis and Recognition) project has focused on developing a data processing system that enables large-scale ANPR convoy analysis. Funded by Innovate UK, the POLARBEAR project was a joint project between SCCS and the technology company Thales UK, supported by Surrey Police as an end user.

In the project, SCCS's researchers applied automated data analytic techniques to ANPR data (using anonymised ANPR data to protect the privacy of drivers, and some public databases) to develop the system. This included using visual analytic approaches in HMI (human-machine interface) to help ANPR operators to interpret the data and results more easily and effectively. The solution developed could enable criminal investigations to focus on medium and high priority issues such as organised crime, as opposed to minor traffic infringements, and could also help to justify the growing use of ANPR by law enforcement agencies to the public at large.

The project team worked closely with Thales UK and Surrey Police to generalise the convoy analysis work to other types of suspicious behaviours and activities that can be detected from ANPR data – potentially enabling the system to highlight criminal behaviours that currently go undetected. They also explored the use of additional data sources (such as public databases from the Highway Agencies and the Crime Map from police.uk) to improve both the accuracy and efficiency of the convoy analysis results.

The project, which was completed in March 2016, has already led to some algorithms and a software prototype which are being commercialised through a technology transfer company.

HUMAN FACTORS

Understanding human behaviour is key to solving cyber security challenges. As the UK Cyber Security Strategy (Cabinet Office 2011) states, "Ordinary people have an important role to play in keeping cyberspace as a safe place to do business and live our lives". Work on Human Factors, therefore, runs across all the research themes being tackled by SCCS.

Case study: Understanding how human behaviour can lead to cybercrime

It is widely accepted that human-related risks are among the most important factors in cyber security – for example an IBM report in 2014 shows that over 95 per cent of security incidents involved 'human errors'. However there is a perception that 'cybercrimes' occur purely within a non-physical cyber space, and are divorced from the human/social components of traditional crime.

"We believe that this research will open up new opportunities for the cybersecurity research community and society at large, and will provide new knowledge and tools that make our highly digitised and connected world a safer place to live and do business."
– Dr Shujun Li

The £1.1m ACCEPT (Addressing Cybersecurity and Cybercrime via a co-evolutionary approach to reducing human-related risks) project, being led by the University of Surrey, explores how people's behaviour can lead to cybersecurity risks, how people become the victims of cybercrimes, and how we can help reduce human-related risks. The project is a collaboration between SCCS and UCL, University of Warwick and TRL (an independent company providing transport consultancy and research services). It will be supported by a number of international cybersecurity and cybercrime experts, and a range of stakeholder organisations including law enforcement agencies, industry and NGOs.

The overall aim of the project is to develop a framework to analyse the behaviours of a range of stakeholders including criminals, victims and people who operate or are users/customers of cybersecurity systems, and business and government organisations. It will also highlight human behaviours that leave individuals and companies vulnerable to cyber attacks and create tools for capturing, analysing and influencing those behaviours.

The project, which is funded by EPSRC, began in April 2017 and will run for two years.

Data loss prevention with minimal human intervention

A Knowledge Transfer Partnership between the University of Surrey and Clearswift Ltd is exploring how hybrid human-machine computing could bring wider safeguarding of sensitive data and documents.

The project between Surrey and Clearswift Ltd, one of the market leaders of data loss prevention (DLP) products, was awarded funding for a three-year Knowledge Transfer Partnership (KTP) by Innovate UK (the government's innovation agency). A response to the 2015 KTP signpost 'Innovation in the Cyber Security Sector', the project is co-funded by DMCS (Department for Culture, Media & Sport).

DLP systems are designed to ensure that sensitive data and documents are only accessed by authorised users, and that safeguards are in place against data leaks. However, high initial human effort and cost needed to define and configure rules around data and document classification is hindering wider deployment of DLP systems in the real world.

The KTP project aims to solve this problem by leveraging observable human behaviours in handling sensitive data and documents, allowing semi-automated bootstrapping and continuous adaptation of DLP systems in real-world environments. The project is drawing on Surrey's knowledge of machine learning (within the Department of Computer Science) and behavioural science (within the School of Psychology) to produce a hybrid human-machine computing system which will minimise the need for human intervention in the deployment and fine-tuning processes of DLP systems. Highly innovative, this hybrid human-machine approach has not yet been used effectively for DLP or broader cyber security problems.

"Working with colleagues from the Centre for the Digital Economy (CoDE) in Surrey Business School, and our industrial collaborators from Clearswift, we aim to convert our exciting research ideas on hybrid human-machine computing into usable commercial products."
– Dr Shujun Li

SCCS core team

Professor Steve Schneider

Director of SCCS, Professor in Secure Systems

Research interests: secure e-voting systems, verification, security protocols, distributed ledger technology, trust, privacy, formal modeling.

Dr Mark Manulis

Deputy Director of SCCS, Senior Lecturer in Security

Research interests: identity management, privacy and authentication, applied cryptography, key management.

Dr Shujun Li

Deputy Director of SCCS, Senior Lecturer

Research interest: human factors, user authentication, user privacy, security visualisation, multimedia security, digital forensics, network security.

Dr Ioana Boureanu

Lecturer

Research interests: provable security, automatic verification, authentication, key-exchange, formal methods for security/privacy.

Professor Liqun Chen

Professor in Secure Systems

Research interests: cryptography, trusted computing, hardware security.

Dr Haitham Cruickshank

Senior Lecturer

Research interests: secure mobile and satellite communication, key management, IPSEC.

Dr François Dupressoir

Lecturer in Secure Systems

Research interests: Verification, cryptography, implementations, protocols, security design.

Dr Thannasis Giannetsos

Lecturer in Secure Systems

Research interests: secure and privacy enhancing technologies, trusted computing, IoT and devices, vulnerability detection and malware analysis.

Dr Lee Gillam

Director of Learning & Teaching in the Department of Computer Science.

Research interests: cloud computing, IP protection, private search, cybercrime.

Professor Anthony T S Ho

Professor of Multimedia Security

Research interests: forensics and e-crime, multimedia security, steganography.

Professor Zhili Sun

Professor of Communication Networking

Research interests: secure mobile/satellite networking.

Dr Helen Treharne

Head of Surrey's Department of Computer Science

Research interests: data privacy, rail, intelligent mobility, verification, formal modelling, trusted computing.

Dr David Williams

Lecturer in Secure Systems

Research interests: protocol verification, formal methods, trusted execution environments, federated identity management.

Professor Alan Woodward

Visiting Professor

Research interests: cryptography, steganography, watermarking and general computer security.

SCCS associates

Dr Adrian Banks
School of Psychology

Dr Payam Barnaghi
5G Innovation Centre (5GIC), Department of Electrical and Electronic Engineering

Professor Richard Bowden
Centre for Vision, Speech and Signal Processing (CVSSP), Department of Electrical and Electronic Engineering

Dr Christopher Bridges
Surrey Space Centre (SSC), Department of Electrical and Electronic Engineering

Professor Alan Brown
Centre for Digital Economy (CoDE)
Surrey Business School.

Dr Tim Brown
5GIC, Department of Electrical and Electronic Engineering

Professor Indira Carr
Surrey Business School

Dr John Collomosse
CVSSP, Department of Electrical and Electronic Engineering

Professor Nigel Fielding
Department of Sociology

Dr Emily Finch
School of Law

Dr Chuan Heng Foh
5GIC, Department of Electrical and Electronic Engineering

Professor Nigel Gilbert
School of Sociology

Professor Josef Kittler
CVSSP, Department of Electrical and Electronic Engineering

Professor Paul Krause
Department of Computer Science

Professor Roger Maull
CoDE, Surrey Business School

Dr Michael McGuire
Department of Sociology

Dr Sotiris Moschoyiannis
Department of Computer Science

Dr Patrice Rusconi
School of Psychology

Professor Rahim Tafazolli
Director of 5GIC, Department of Electrical and Electronic Engineering

Dr Wenwu Wang
CVSSP, Department of Electrical and Electronic Engineering

Professor Robert Witt
School of Economics

Surrey Centre for Cyber Security
University of Surrey
Guildford, Surrey, GU2 7XH, UK

T: +44 (0)1483 686058
W: surrey.ac.uk/sccs
E: SCCS@surrey.ac.uk
twitter: @SCCS_UniSurrey