News
Page 2

New research projects
Page 5

Expert comments
Page 8

Newsletter

University of Kent | Institute of Cyber Security for Society (iCSS)

News from the Institute of Cyber Security for Society (iCSS) Summer 2021

Welcome

Welcome to the fourth issue of the iCSS Newsletter (previously KirCCS Newsletter). Every quarter we send a round-up of the latest news, activities and events we think members of iCSS, external colleagues and organisations will be interested in. If you have any suggestions or feedback, would like contact, share your news with us, or subscribe to this newsletter, please email cyber-info@kent.ac.uk. We maintain an archive of past newsletters on our website: http://cyber.kent.ac.uk

Institute of Cyber Security for Society (iCSS)

News

iCSS is officially launched at Kent Cyber Security Forum (KCSF) 2021

Speakers (left to right). Top: Professor Shujun Li, Director of iCSS and Professor of Cyber Security, School of Computing, University of Kent; **Professor Sander van der Linden**, Professor of Social Psychology in Society and Director of Cambridge Social Decision-Making Laboratory, University of Cambridge; **Dr Harmonie Toros**, Deputy Director of iCSS and Reader in International Conflict Analysis, School of Politics and International Relations, University of Kent; **Lyric Jain**, Founder and CEO, Logically. **Middle: David Klepper**, Report, The Associated Press; **Dr Virginia Franqueira**, Deputy Director of iCSS and Lecturer in Cyber Security, School of Computing, University of Kent; **Professor Julia Davidson** OBE, Professor of Criminology and Director of Institute of Connected Communities, University of East London; **Professor David Wall**, Chair in Criminology, School of Law, University of Leeds. **Bottom: Dr Hans Henseler**, Digital Forensic Advisor, Division of Digital and Biometric Traces, Netherlands Forensic Institute, The Netherlands ; **Chris Crute**, Digital Forensics Team Leader (Computers), Digital Forensics Unit, Forensic Investigation Department, Kent and Essex Serious Crime Directorate; **Dr Budi Arief**, Innovation Lead of iCSS and Senior Lecturer, School of Computing, University of Kent

On Monday 28 June we saw the official launch of iCSS as part of our annual Kent Cyber Security Forum (KCSF) event series. KCSF is an annual public engagement forum for cyber security experts, policy makers, researchers, innovation experts, businesses, the general public and various other organisations, to come together and discuss current and future cyber security threats and opportunities. The series was previously run by the Kent Interdisciplinary Research Centre in Cyber Security (KirCCS) and has been running since 2018. A video of the KCSF 2019 physical event can be seen here. Last year we were unable to host KCSF due to the pandemic, but this year we were determined to go ahead, albeit with an online event.

The whole-day event kicked off with a warm welcome from Professor Karen Cox, Vice Chancellor and president of the University of Kent. In the morning we heard from the Team Lead of the Sociotechnical Security Group at the National Cyber Security Centre (NCSC), in a talk about how socio-technical research, such as that conducted at Kent, contributes to and supports the mission and work of the NCSC.

The morning keynote talk was given by Professor Julia Davidson from the University of East London who drew on her research focusing on the changing policy and practice landscape in the UK in the context of the Online Safety Bill. Julia was then joined by four other experts on Cyber Crime and Digital Forensics for the panel discussion that followed.

In the afternoon, Professor Shujun Li, Director of iCSS, opened the session with an Introduction to iCSS. He outlined the history of cyber security research at Kent, Kent's recognition as an Academic Centre of Excellence in Cyber Security Research (ACE-CSR), our wide-ranging expertise and commitment to interdisciplinary education and research. Additionally, he explained how iCSS's activities can support the UK's cyber security strategy and society as a whole.

Following the iCSS introduction, Professor Sander van der Linden from the University of Cambridge gave a very interesting talk on the psychological factors involved in the proliferation of misinformation. He also suggested the techniques we can use to protect people from the effects of misinformation, for example through the development of a psychological 'vaccine'.

Alongside the keynote talks and panel discussions, attendees were invited to visit our Gather.Town virtual conference space to learn more about iCSS, take a look at some of our research posters, network and play some interactive games.

Thank you to all those who attended, we hope you enjoyed it and a special thanks to our keynote speakers, panellists and all those who helped behind the scenes. We look forward to welcoming you back next year!

Ipsos MORI report influencing government policy on IoT connected device security


Press release

New cyber security laws to protect smart devices amid pandemic sales surge

Groundbreaking plans to protect people from cyber attacks

From: Department for Digital, Culture, Media & Sport and Matt Warman MP
Published 21 April 2021

- Apple, Samsung, Google and other manufacturers will say when smartphones, smart speakers and other devices will stop getting security updates
- Easy-to-guess default passwords to be banned on virtually all devices under new law
- Rules will make it easier for people to report software bugs that can be exploited by hackers

Makers of smart devices including phones, speakers, and doorbells will need to tell customers upfront how long a product will be guaranteed to receive vital security updates under groundbreaking plans to protect people from cyber attacks.

Dr Jason Nurse has contributed to a new government-commissioned Ipsos MORI report, which is being used to influence government policy on regulating consumer smart product cyber security.

The Ipsos MORI report, titled 'Consumer Attitudes Towards IoT security' reveals the findings of an online survey of the UK public, exploring consumer purchasing behaviour of, and attitudes towards connected devices.

Consumer IoT (Internet of Things) products or connected devices, including smart devices such as TVs, cameras, mobile phones, watches and speakers, offer a huge range of benefits to users but can also be vulnerable to cyber-attacks. The survey found that since March 2020, approximately 50% of UK residents have purchased at least one new smart device and when this is paired with other research showing significant increases in cybercrime since the start of the pandemic, it is easy to see the urgency of policy development in this area.

Key findings of the report include:

- Smartphones are the most commonly owned devices among UK consumers (87%).
- Only one in five consumers (20%) report checking the minimum support period (the length of time the product will receive updates for) when purchasing a smart device.
- Seven in ten consumers (71%) agree it is important that information on minimum support periods is made publicly accessible for consumers.
- Nine in ten consumers (87%) say smart devices should have basic embedded features to protect user privacy and security.
- Around eight in ten consumers (84%) agree that those in the supply chain have a responsibility to make such checks and be aware of security features in products before they are sold.

Combined with other research, such as that conducted by the consumer group Which?, which found that a third of people kept their last phone for four years, while some brands only offer security updates for a little over two years, this report has helped shape the planning of a new law proposal by the UK government, which will state:

1 Customers must be informed at the point of sale the duration of time for which a smart device will receive security software updates.
2 A ban on manufacturers using universal default passwords, such as 'password' or 'admin', that are often pre-set in a device's factory settings and are easily guessable.
3 Manufacturers will be required to provide a public point of contact to make it simpler for anyone to report a vulnerability.

Dr Jason Nurse said: "Smart devices and connected products offer a range of opportunities to streamline and enhance our lives. As we've shown in this report however, security is not always a primary factor with these devices, but it should be. I am glad to see our work be used to influence government policy and look forward to seeing more secure consumer smart products."

Professor Shujun Li's book on cognitive modelling makes it to BookAuthority's best new Human-Computer Interaction books

A book co-authored by Professor Shujun Li, Director of iCSS and Professor of Cyber Security at the School of Computing, entitled *Cognitive Modeling for Automated Human Performance Evaluation at Scale*, has made it to BookAuthority's list of the 10 best new Human-Computer Interaction books.

BookAuthority identifies and rates the best books in the world, using a range of indicators such as public mentions on online social networks, expert recommendations, ratings of readers, popularity, and sales history.

In today's highly digitized and networked world, people regularly interact with computer systems of different kinds (e.g. personal computers, laptops, mobile devices, IoT devices, video games, online social media). To help researchers and user interface/experience (UI/UX) designers to develop more usable computer user interfaces (UIs), cognitive modelling software tools have been widely used, CogTool being one of them. The book provides readers with a systematic overview of state-of-the-art cognitive modelling theories, techniques and software tools, and their applications.

It also introduces a new cognitive modelling software framework and a research prototype that can support large-scale modelling and simulation tasks more easily.

Professor Li said, "I'm glad to see our book has been rated by BookAuthority as one of the 10 best new books in human-computer interaction to read in 2021. The book was written not just for computer science researchers, but also for psychologists, UI/UX designers and practitioners who want to learn about or use cognitive modelling tools for different purposes. I hope our readers find the book useful, and some can join our ongoing efforts to develop more powerful cognitive modelling techniques and tools in future."

News

Kent cyber security spin-out acquired by Crossword Cybersecurity

Verifiable Credentials Ltd (VCL), a University of Kent spin-out, has recently been purchased by technology commercialisation company, Crossword Cybersecurity Plc, following CEO and Professor, David Chadwick's work to prove the commercial viability of the cyber security technology developed at Kent.

Crossword Cybersecurity was first introduced to VCL when David Chadwick, as Professor of Information Systems Security at the University of Kent, brought his academic team to participate in the InnovateUK / UKRI CyberASAP programme in 2019. The programme aims to help academics commercialise their cyber security ideas and includes support and training from Crossword. This helped David Chadwick to convert the new technology resulting from his academic research into a commercial product.

The technology, known as *Identiproof*, is central to the issuing of digital certificates and documents that cannot be forged or transferred, and that respect the privacy of the holders of those certificates. It does this through the process of selective disclosure, whereby the recipient requests the minimum of information in conformance with GDPR. It is currently being used in a UK Government funded trial of COVID-19 certificates for East Kent Hospitals University NHS Foundation Trust (EKHUFT), and has applications including digital ticketing, certificates, licenses, memberships, passports, proof of ownerships, and more.

Having agreed to pay up to £2.75 million to acquire VCL, Crossword will not only gain this innovative technology, but also access to David Chadwick's expertise in the field of digital identity and verifiable

credentials, when he takes on the role of Product Director at the company. He will be joined at Crossword by VCL's specialist development team.

David Chadwick said of the relationship, "Identiproof is unique in the market and with Crossword's great structure, connections and sales team – we're expecting to achieve excellent revenue growth."

Tom Ilube, CEO of Crossword Cybersecurity plc, added, "VCL has unique knowledge and a fantastic product in the new era of W3C verifiable credentials – which can and should power COVID certificates as well as all manner of digital, secure and privacy-respecting credentials, certificates, tickets and proofs of ownership. We know Professor Chadwick and his start-up team well from CyberASAP and believe Identiproof is a perfect fit for Crossword as our third product. This acquisition comes at a time when we are experiencing great success from strategies to increase Rizikon market penetration, particularly the launch of Rizikon Pro. In the last 6 months this has increased 10 fold, with the number of Rizikon users exceeding 250."

Shane Weller, Deputy Vice-Chancellor of Research & Innovation at Kent, commented, "The acquisition of Verifiable Credentials Ltd by Crossword Cybersecurity is a fantastic opportunity for both parties. Since first engaging with David and his team at Innovate UK's Cyber ASAP programme two years ago, Crossword have shown enthusiasm and support for the start-up, driving a strong collaborative relationship between the two. This acquisition further confirms Crossword's recognition of the value that academic knowledge fostered at Kent can bring to the process of innovation."

Professor David Chadwick has an ongoing association as an Honorary member of the Institute of Cyber Security for Society (iCSS).

Cyber insurance struggling to counter threat of crime online

A new research report by the University of Kent and the Royal United Services Institute for Defence and Security Studies (RUSI) has found that the contribution of the insurance sector to improving cyber security practice is 'more limited than policymakers and businesses might hope' and recommends action by government and industry.

The authors of the *Cyber Insurance and the Cyber Security Challenge report* (James Sullivan, Director of Cyber Research at RUSI;

Dr Jason Nurse and Jamie MacColl, Research Analyst in cyber threats and cyber security at RUSI) have found that to date, cyber insurance has failed to live up to expectations that it may act as a tool for improving organisations' cyber security practices.

Based on interviews and workshops with experts across the insurance and cyber security industries, government, academia, the report identifies an insurance industry that is not only struggling to understand cyber risk itself, but that it is struggling to collect and analyse reliable cyber risk data. Without this, there are significant questions around the insurability of cyber risk. Meanwhile ransomware has become an existential threat for some insurers. At a time of mounting losses and rising public criticism, the report argues for a reset in the industry.

Dr Nurse said: "The role of cyber insurance as it pertains to cyber security has been discussed for decades, but still there has been little substantial progress on understanding whether insurance can incentivise better security practices in organisations, or if it can, how best can this be facilitated.

This report and our findings draw on a year-long study involving experts in policy, practice and research to answer many of these outstanding questions, thereby making a significant contribution to existing knowledge. More importantly, we provide several well-informed policy recommendations for the UK cyber insurance market, including UK policymakers, regulators and insurance providers and brokers, covering exactly is needed for cyber insurance to play a more significant role in allowing the robust management of cyber risk."

Since being released on the 28th June, the RUSI cyber insurance report has already been covered in numerous media stories including AP News, ZDNet, Infosecurity Magazine, Computer Weekly, SC Magazine, ITProPortal and The Register.

New research projects

Professor Karen Douglas awarded €2.5M to investigate consequences of conspiracy theories

Professor Karen Douglas from the School of Psychology has been awarded a European Research Council Advanced Grant of 2.5 million Euros for a five-year project examining the consequences of conspiracy theories.

The project will focus on when and how conspiracy theories affect the decisions and wellbeing of individuals and society, and what people can gain and lose from spreading conspiracy theories.

Using a range of research methodologies and drawing on insights across several academic disciplines, the project will provide empirical evidence of the impacts that conspiracy theories have on individuals and important foundations of society such as voting behaviour, faith in government, and vaccination behaviour.

The funding will enable Professor Douglas to recruit and lead a team of postdoctoral researchers and postgraduate students to study these issues.

Professor Douglas is a leading researcher on the psychology of conspiracy theories, having worked on this topic for more than 10 years.

She said: "I am incredibly grateful to receive this funding from the European Research Council. Conspiracy theories have flourished in recent times and it is now crucial that scientists better understand their impacts. This funding will enable me to conduct research that is essential for addressing one of the world's most current and persistent concerns. The findings from this project will help inform strategic approaches to discourage people from basing important life decisions on false information."

HEROES project to look at human trafficking, child exploitation and victim protection

Researchers from the University of Kent will form part of a new, multi-national, interdisciplinary research project funded via the European Commission Horizon 2020 programme. The project will run for three years and is titled "Novel Strategies to Fight Child Sexual Exploitation and Human Trafficking Crimes and Protect their Victims" (HEROES).

Professor Julio Hernandez-Castro, Dr Budi Arief and Dr Laura Bocchi from the School of Computing will partner with experts from organisations in 18 countries across Europe, South America and Asia, including the lead project partner Dr Luis Javier Garcia Villalba from UCM (Universidad Complutense de Madrid, Spain).

The project considers how new and evolving technologies have changed the face and operation of child sexual abuse and exploitation (CSA/CSE) and trafficking of human beings (THB), and uses a victim-centred approach to develop new strategies to address these challenges. The project aims to improve the way in which law enforcement agencies and civil society organisations carry out criminal investigations, assist rescued victims, and prevent the occurrence of these crimes.

Dr Laura Bocchi said, "This project provides a unique opportunity to work with experts from all over the world in the fields of law, psychology, sociology, health and social work, computer security and forensics, to improve the way help and support is provided to victims of THB and CSA/CSE and prevent the occurrence of these horrendous crimes."

New research projects

New project to understand cyber security skills development in pre-university education

Three members of iCSS, Dr Virginia Franqueira and Professor Shujun Li from the School of Computing, and Dr Vince Miller from the School of Social Policy, Sociology and Social Research (SSPSSR), have been awarded funding for a new project that aims to understand how cyber security skills development is currently covered in pre-university curricula in different countries and regions. It will also investigate technical and non-technical approaches used to develop cyber security skills for different age groups up to 18, and the role of different stakeholders (e.g. teachers, parents, public bodies and NGOs) in such skills development activities. It forms a natural part of the wider cyber security research and educational activities of iCSS.

The project is supported by the Global Forum on Cyber Expertise (GFCE), a multi-stakeholder community with the mission to strengthen cyber capacity and expertise globally through international collaboration. As part of their Global CCB Research Agenda 2021, the topic of the project was identified and put forward by their working group on "Cybersecurity Skills & Education".

Dr Virginia Franqueira said, "Young people are more and more connected, owning smartphones from an early age, and increasingly engaging with smart devices, online services and social media platforms. Despite the benefits derived from such accessibility to resources and friends in the cyberspace, a side effect is their increasing susceptibility to harmful content and the intrinsic difficulty to stay safe online. Therefore, it becomes paramount that young people start developing cyber security skills to raise their awareness of online risks, to build their capacity in countering those risks from young age, and to attract more young talents to pursue a cyber security career. Education at schools and pre-university colleges plays a key role, and we are very excited to have a great opportunity to enhance our understanding, through this project, about the state of development of cyber security education in the UK and worldwide."

Kent awarded EPSRC funding to study cyber security risks for mobility-as-a-service (Maas)

Mobility-as-a-service (MaaS) offers travellers a unified service that combines various forms of transport from a single point of delivery. MaaS carries the potential to reduce traffic congestion, improve customer convenience and reduce social inequalities and carbon emissions through the use of public transport.

Professor Shujun Li from the School of Computing and Director of the Institute of iCSS will work with researchers at Cranfield University to look into the cyber security risks posed by a digitally enabled, low-carbon mobility-as-a-service (MaaS) ecosystem. The project, titled "Mobility as a service: MAnaging Cybersecurity Risks across Consumers, Organisations and Sectors (MACRO)", is funded by the Engineering and Physical Sciences Research Council (EPSRC), part of UK Research and Innovation (UKRI), and will run for two years.

Ensuring success for MaaS will require a single application to plan and conduct journeys, a software system allowing multiple providers and AI-based analytics allowing journey and resource optimisation. All these interactions are susceptible to a wide range of cyber-attacks, which can affect different stakeholders of the ecosystems. The complexity of the MaaS ecosystem, including customers, transportation providers and data providers, and its dependence on the data, creates unique challenges from a cyber-security perspective.

The project is led by Dr Nazmiye Ozkan, Senior Lecturer in Energy Economics and Head of Centre for Energy Systems and Strategy at the Cranfield University. Professor Shujun Li will lead the work package on Modelling Cyber Security Risks and contribute to other work packages. The project team will work closely with a number of supporting bodies including University of Bath, Oxfordshire County Council, Kent County Council, South East Midlands Local Enterprise Partnership and Transport for the South East.

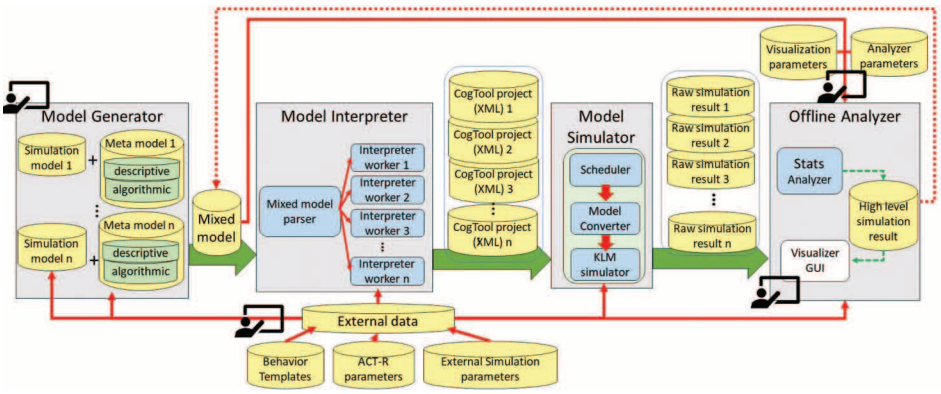
Professor Shujun Li said: "I am very pleased to have the opportunity to work with my collaborators from Cranfield University. The UK Government's ambitions to reach net zero carbon emissions by 2050 and other governments' similar goals mean that MaaS becomes an important component of this long-term vision. The complicated data flows and interactions between different stakeholders of a MaaS ecosystem requires careful consideration of various cyber security and privacy risks and development of corresponding solutions, including new tools, techniques, policies and procedures. By following a modelling-based approach, the project will produce useful tools and information for governments, transport service providers and travellers to co-develop healthy MaaS ecosystems."

New publications

iCSS Director Professor Shujun Li publishes in top journal

Professor Shujun Li has co-authored an article entitled 'CogTool+: Modeling human performance at large scale', which has recently been published in the top tier computer science journal *ACM Transactions on Computer-Human Interaction*. The journal is considered the No 1 journal in the sub-area of computer-human interaction and is ranked as an A* journal by the Computing Research and Education Association of Australasia (CORE).

Cognitive models and software tools have been widely used by researchers in multiple disciplines to simulate how human users conduct different kinds of tasks that require cognitive workload. For example, they can be used to automatically evaluate the usability of computer security systems for user authentication, without the need to conduct experiments involving human participants. CogTool is one of the widely used cognitive modelling tools, however, despite its usefulness, large-scale modelling tasks can still be very challenging due to the amount of manual work users of the tool still need to do. To address this challenge of modelling and simulating large-scale systems with reduced manual work, Professor Shujun Li and co-authors Dr Haiyue Yuan (Research Fellow at the University of Surrey) and Dr Patrice Rusconi (Lecturer in Social Psychology at the University of Messina in Italy, formerly Lecturer in Psychology at the University of Surrey) have proposed CogTool+, a new cognitive modelling framework and a software prototype developed on top of CogTool.



CogTool+ enhances the capability of CogTool for supporting large-scale modelling and simulation tasks by adding the following new features: (1) a higher level of automation; (2) the possibility to add algorithmic components such as randomised user interface elements; (3) using external data to inform the modelling and simulation process; and (4) a clearer separation of tasks, allowing user interface (UI) designers, programmers and psychologists to work together more effectively. CogTool+ also supports mixed cognitive models, which are required in many large-scale modelling tasks. It provides an offline analyser of simulation results. In order to show how CogTool+ can reduce human efforts required for large-scale modelling tasks, the researchers illustrate how it works using a pedagogical example about a simple graphical user authentication system and demonstrate its improved performance by applying it to modelling tasks of two real-world user authentication systems involving more complicated procedures.

The full article is freely available at the publisher's website: https://doi.org/10.1145/3447534. The source code of the CogTool+ and the modelling examples shown in the article are made open source on GitHub: https://github.com/hyyuan/cogtool_plus. Readers who are interested in learning more about cognitive modelling are recommended to read the same researchers' monograph published by Springer Nature in 2020: *Cognitive Modeling for Automated Human Performance Evaluation at Scale*.

Below are some recently published/accepted research publications of our members:

Belen Sağlam, Rahime; **Nurse, Jason R C**; Hodges, Duncan (2021) "Privacy Concerns in Chatbot Interactions: When to Trust and When to Worry". In: *23rd International Conference on Human-Computer Interaction*, 24-29 Jul 2021, Online.

Buckley, Oliver; **Nurse, Jason R C**; Wyer, Natalie; Dawes, Helen; Hodges, Duncan; Earl, Sally; **Belen Sağlam, Rahime** (2021) "Sharing Secrets with Agents: Improving Sensitive Disclosures using Chatbots". In: *23rd International Conference on Human-Computer Interaction*, 24-29 Jul 2021, Online.

Yuan, Haiyue; **Li, Shujun**; Rusconi, Patrice (2021) "CogTool+: Modeling human performance at large scale", in *ACM Transactions on Computer-Human Interaction*, 28 (2). Article Number 7.

Jones, Keenan; **Nurse, Jason R C** & **Li, Shujun** (2021) "The Shadowy Lives of Emojis: An Analysis of a Hacktivist Collective's Use of Emojis on Twitter". In: *Workshop Proceedings of the 15th International AAAI Conference on Web and Social Media* (ICWSM-21).

Khanna, Pooja & **Howells, Gareth** (2021) "Using Dynamic Operational features to Identify Embedded Devices". *XXXIV General Assembly and Scientific Symposium (GASS) of the International Union of Radio Science*. (In press).

de Moura, Ralf L; Gonzalez, Alexandre; **Franqueira, Virginia N L**; Neto, Antonio L M; Pessin, Gustavo (2021) "Geographically Dispersed Supply Chains: A Strategy to Manage Cybersecurity in Industrial Networks Integration". In: *Daimi K, Peoples C (eds) Advances in Cybersecurity Management*. Springer, Cham.

Jaffray, Alice; Finn, Conor; & **Nurse, Jason R C** (2021) "SherLOCKED: A Detective-themed Serious Game for Cyber Security Education". In: *15th International Symposium on Human Aspects of Information Security & Assurance (HAISA)*, 7-9 July 2021. Springer.

Uchendu, Betsy; **Nurse, Jason R C**; Bada, Maria; Furnell, Steven (2021) "Developing a Cyber Security Culture: Current Practices and Future Needs", in *Computers & Security*.

Nurse, Jason R C; Williams, Nikki; Collins, Emily; Panteli, Niki; Blythe, John; Koppelman, Ben (2021) "Remote Working Pre- and Post-COVID-19: An Analysis of New Threats and Risks to Security and Privacy". In: *23rd International Conference on Human-Computer Interaction*, 24-29 Jul 2021, Online.

Turner, Sarah; **Nurse, Jason R C** & **Li, Shujun** (2021) "When Googling it doesn't work: The challenge of finding security advice for smart home devices". In: *15th International Symposium on Human Aspects of Information Security & Assurance (HAISA)*, 7-9 July 2021. Springer.

Kearney, Joseph J & **Perez-Delgado, Carlos A** (2021) "Vulnerability of blockchain technologies to quantum attacks", in *Array*, Volume 10, 100065.

Ellavarason, Elakkiya; **Guest, Richard M**; **Deravi, Farzin**; Sánchez-Reillo, Raul; Corsetti, Barbara (2021) "Touch-dynamics based Behavioural Biometrics on Mobile Devices - A Review from a Usability and Performance Perspective". In: ACM Computer Surveys 53(6): 120:1-120:36

Expert comments

Expert comment on best response to a ransomware attack

Ransomware is a growing threat as seen with the recent incident involving meat processing company JBS paying the equivalent of $11m (£7.8m) in cryptocurrency to cyber hackers.

Dr Budi Arief, iCSS Innovation Lead and Senior Lecturer at the University's School of Computing, provides comment on how to best manage a ransomware attack or avoid one altogether.

He said: "The latest incident involving JBS demonstrates the real difficulties faced by victims. To pay or not to pay has been one of the key dilemmas, and this is indeed a tricky question to answer.

As a security researcher, I would definitely recommend not to pay the ransom demand, for two main reasons. First, by paying, you are indirectly funding cybercriminal activities. Cybercriminal gangs would be emboldened by getting paid, and they would continue or increase their attacks. Second, there is no guarantee that you would be able to recover everything, nor would you be immune from being attacked again. If anything, if you had paid the ransom demand before, it would make you more attractive for the ransomware operators to attack you again.

Sometimes there is no other way for victims, apart from paying the ransom demand, because the recovery costs would be too high, or the business would suffer terribly. If you decided to pay, it is imperative that you also patch all of the security vulnerabilities that allowed the ransomware to infect your system in the first place, because otherwise you might become a victim of the same ransomware gang again.

It might be possible to recover some of the ransom money – as shown in the case of the Colonial Pipeline ransomware attack – but this is still quite rare and it would rely on the ransomware operators being inexperienced or sloppy.

The best defence is by following a set of key security hygiene procedures, such as employing regular and effective backup of your data; applying security patches; and making sure that you do not let ransomware get into your system in the first place, for instance by not clicking on potentially malicious links or opening suspicious email attachments."

80th Anniversary of the Enigma Code being cracked

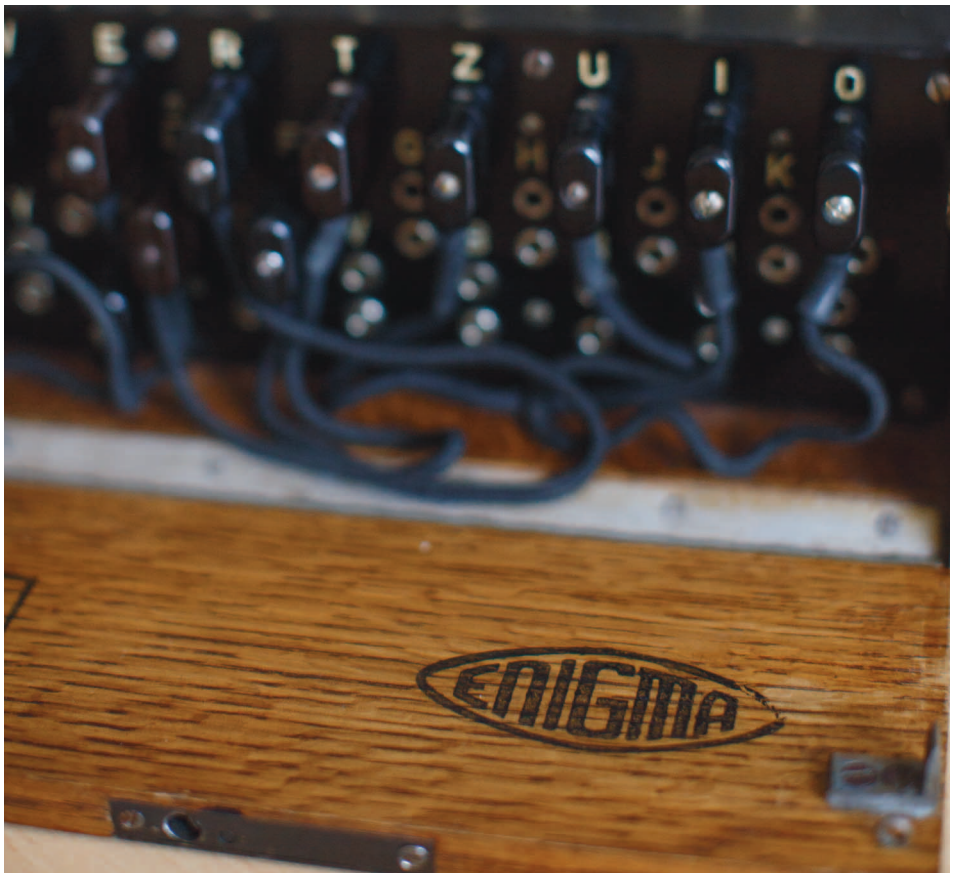
Friday 9 July 2021 marked the 80th anniversary of the cracking of the Enigma Code by a team at Bletchley Park, led by the British mathematician Alan Turing.

Professor Andy Hone at the University's School of Mathematics, Statistics and Actuarial Science comments on this pioneering event in history and the impact that pure mathematics has on modern life. He says: "This anniversary is a chance to celebrate not only the work of Turing, but also the achievements of pure mathematics more generally.

Turing designed the Bombe, an electro-mechanical device which ran through all the possible ways that a message could be encrypted and allowed his group of cryptologists to decode communications intercepted from the German navy. This gave Britain a strategic advantage which experts believe may have shortened the Second World War by at least two years.

Earlier pioneering work by Turing in mathematical logic laid the foundations for the theory of computing, but his Bombe had a 19th century predecessor in the form of the Analytical Engine. This mechanical computer was designed by Charles Babbage, with instructions written by another British mathematician, Ada Lovelace, who can lay claim to be the world's first computer programmer, although the machine itself was never built. Turing was involved with making some of the first modern electronic computers in Manchester just after the war.

Pure mathematics lies behind many other developments that are vital to modern life, ranging from the modelling of infectious diseases like Covid-19 (which is based on differential and difference equations), to secure online banking and shopping (which relies on number theory and abstract algebra). It is estimated that pure mathematics adds £200bn annually to the UK economy, or 10% of GDP, which demonstrates its critical role in today's world and the future."



Calls for participation

Safer Online Lives survey

The Safer Online Lives project is researching internet use and safety for adults with Intellectual Disabilities. They want to hear from family carers, paid carers and practitioners with a safeguarding part in their role, who have experience with adults with Intellectual Disabilities. Please consider taking part in this important research and share with your networks: https://kentsspssr.eu.qualtrics.com/jfe/form/SV_5pT3kJcoBJaIT9s?Q_CHL=qr

iCCS Team news, events and talks

iCSS welcomes the following new members

Jordan Montford Robinson has joined the School of Anthropology as a Research Associate on a cyber-enabled wildlife trafficking project entitled "Dismantling wildlife trafficking cybercrime networks in Southeast Asia, funded by Defra, the illegal Wildlife Trade Challenge Fund. Jordan has recently finished his degree in Computing at Kent and will now work under the supervision of iCSS members **Dr David Roberts** from the School of Anthropology and Conservation and **Professor Julio Hernandez Castro** from the School of Computing.

Dr Allison Holmes joins iCSS as an Associate Member. Allison is a Lecturer in Law at Kent Law School and teaches on Criminal Justice modules. Allison's research interests lie at the intersection of information technology law and criminal law, with a focus on privacy and data protection rights.

Dr Caroline Li joins iCSS as an Associate Member from the School of Computing. Caroline's main area of research is in signal processing and its applications in body sensors, including, EEG-based biomarker discovery for brain diseases, neurofeedback applications for medical and sport applications and brain computer interface. She is also working on signal processing methods including, adaptive filtering, tracking methods and machine learning methods for pattern classification.

Kent and Cyber Readiness Institute organise Ransomware Webinar

On 5 May 2021, the University of Kent, in affiliation with the Cyber Readiness Institute (CRI), gave a webinar on "Ransomware and You: The Human Element of Ransomware". In this talk, Dr Budi Arief from Kent's School of Computing and Lessie Longstreet from CRI looked into some of the human aspects of ransomware. The webinar can be viewed on YouTube here: www.youtube.com/watch?v=BtQC2-Y0Qwk

Dr Jason Nurse talks at University of Maryland Sociotechnical Cybersecurity Lecture series

On Tuesday 21 April, Dr Jason Nurse gave a talk entitled, "A Framework for Effective Corporate Communication after Cyber Security incidents" as part of the University of Maryland (US) Sociotechnical Cybersecurity Lecture series. You can watch Jason's lecture on YouTube here: https://www.youtube.com/watch?v=eC0y9b_UxRA

Kent hosts series of Royal Institution Masterclasses

The University of Kent recently hosted a series of four virtual Royal Institution Computer Science Masterclasses for Year 12 and Year 11 students progressing to A level Maths. The series ran from Saturday 12 June to Sunday 10 July 2021.

The Royal Institution Masterclass programme opens young people's eyes to the diversity of STEM. Through a series of extra-curricular workshops, students all over the UK met to explore the subjects in new and exciting ways.

Dr Carlos Perez Delgado, iCSS member and Lecturer in the School of Computing, led the first Masterclass of the series: *3700 years of Computer Science: From Ancient Babylon to Quantum Computing*, which explored what computer science is, when and where it got started, and where it might be heading.

Özgür Kafalı HoTSoS 2021 conference

iCSS member Özgür Kafalı, a Lecturer from the Cyber Security Group at the School of Computing, co-chaired the 8th Annual Hot Topics in the Science of Security (HoTSoS) Symposium virtually hosted by the US National Security Agency (NSA) on 13-15 April, 2021. Prior to joining the University of Kent, Özgür worked as a postdoctoral researcher on NSA's Science of Security project.

Historically an event mainly for the US audience, this year the event saw high participation from an international audience, with great interaction among the participants and speakers. Keynote speakers included an NSA researcher Nick Felts, the winner of NSA's 8th Annual Best Scientific Cybersecurity Research Paper Competition, Awais Rashid from University of Bristol, and Paul Waller from UK NCSC.

Following last year's format, HotSoS 2021 featured work in progress discussion sessions as a forum to give feedback to authors on early research directions. The full program can be seen here: https://cps-vo.org/group/hotsos/agenda

Congratulations

Congratulations to **Dr Jason Nurse** who has been appointed to the Editorial Board (as an Associate Editor) of the ACM Digital Threats: Research and Practice (DTRAP) Journal.

Congratulations to **Professor Shujun Li** who is now a member of the journal editorial board for IEEE Transactions on Dependable and Secure Computing (IEEETDSC).

Kent takes part in UK Security and Privacy Seminar Series

The UK Security and Privacy Seminar Series (UK-SPS) is a newly formed collaboration between nineteen UK Universities offering a UK-wide programme of world leading seminars, showcasing speakers from across the globe with the aim of sharing world leading research and expert insights into the current Cyber Security and Privacy landscape.

Dr Sanjay Bhattacherjee will assist with the organisation of seminars on behalf of Kent. The seminars will be held weekly, every Wednesday at 3pm.

For further details, please check the website: www.uk-sps.org. You may also want to subscribe to the public Google calendar iCal for regular updates. On Twitter, the handle is @UKSPSeminars and the talks will also be streamed on YouTube.

Upcoming conferences and workshops 2021

ARES 2021

17-20 August 2021

The 16th International Conference on Availability, Reliability and Security ("ARES – The International Dependability Conference") will bring together researchers and practitioners in the area of dependability. ARES will highlight the various aspects of dependability – with special focus on the crucial linkage between availability, reliability and security. iCSS Deputy Director Dr Virginia Franqueira will Co-Chair the following Workshops, held in conjunction with ARES 2021:

- 5th International Workshop on Security and Forensics of IoT (IoT-SECFOR 2021)
- 14th International Workshop on Digital Forensics (WSDF 2021)

SecureComm 2021

3-6 September 2021

17th EAI International Conference on Security and Privacy in Communication Networks, to be hosted at the University of Kent, Canterbury, UK.

Professor Shujun Li is co-chairing the Conference, and a number of iCSS Core Members are on the Organising Committee.

In conjunction with the main event, EAI SecureComm 2021 will hold the following international workshops:

- Cyber attribution: challenges, possibilities, solutions.
- Cyber-Physical Systems Strategic and Technical Security (CPS-STS)
- Post-quantum Cryptography for Secure Communications (PQC-SC)

DPC 13100 07/21