UniKentCyberSec

UniKentCyberSec

Institute of Cyber Security for Society (iCSS)

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

NEWSLETTER

Spring-Summer 2022

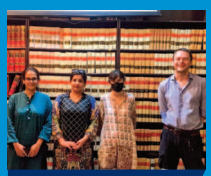
Welcome to the seventh issue of the iCSS Newsletter. Every quarter or half a year we send a roundup of the latest news, activities and events we think members of iCSS, external colleagues and organisations will be interested in. If you have any suggestions or feedback, would like to share your news with us, or subscribe to this newsletter, please email cyber-info@kent.ac.uk

We maintain an archive of past newsletters on our website: cyber.kent.ac.uk

Page 2

Page 6

Page 8



Page 10

News

iCSS research urges need for improving cyber security education in pre-university settings

A research report by iCSS researchers, funded by Global Affairs Canada and commissioned through the Global Forum on Cyber Expertise (GFCE), has revealed major insights about cyber security education in pre-university settings and provided recommendations to various stakeholders on how to address some identified concerns.

The research was conducted by a group of researchers at iCSS from two disciplines (Computing and Sociology), including **Dr Virginia Franqueira**, **Professor Shujun Li**, **Dr Vince Miller** and research assistant **Krysia Emily Waldock** (PhD student). To inform the report, the researchers conducted a systematic review of the research literature, desk research of related policy documents, projects, initiatives and events in 13 countries, and semi-structured interviews with 21 interviewees from 11 countries. The countries are based in five different continents, including both developed and developing countries.

The research team identified two main approaches to embedding cyber security and online safety content in the curriculum, and noticed a lack of practical cyber security skills, security mindset and enough skill-set coverage in the curriculum, towards a cyber security related career path.

In addition, concerns are flagged in the report around a lack of teacher training in cyber security, insufficient time to cover relevant topics, lack of a direction on what schools and teachers should do in cyber security education, and the pressure to prioritise more survival-focused skills than cyber security due to economic considerations. Such findings call for further reviews and improvement of the national curricula in different countries and more support for teachers and schools, which will require a more co-ordinated approach involving all countries, multiple relevant communities and stakeholders.

For many of the countries studied, the research revealed that while many stakeholder organisations in different sectors were active in different aspects of pre-university cyber security education, there is often fragmentation and confusion regarding which organisations have responsibilities of which matters. The report therefore recommends that governments in countries and regions managing its own educational affairs should consider setting up a national or regional steering body or working group with overall responsibility for cyber security and online safety education.

The researchers also noticed a perceived general lack of interest and awareness among children in developing cyber skills and cyber security as a potential career path, and a lack of diversity in terms of student enrolment in optional courses and training events.
Such findings call for more work to enhance awareness among pupils (and parents) and to address the EDI (equality, diversity and inclusion) issues of pre-university cyber security education, especially from less covered and 'non-traditional' groups such as girls, ethnic minorities and pupils from low-income backgrounds.

Professor Shujun Li, Director of iCSS, said: 'Our research demonstrates that there are many gaps in current approaches to cyber security education in pre-university settings. Therefore, there is an urgent need for relevant stakeholders to take actions to improve the situation, including reviewing and refining existing policies and action plans, and supporting more research and innovation activities to support various stakeholders including pupils, parents and teachers. We hope the key findings and our recommendations in the report can help people and organisations across the globe to work together to prepare our children for living a safer life online and for developing themselves to be next-generation cyber security professionals.'

Global Affairs Canada added: 'Canada believes that democracy in the digital age begins with digital inclusion, whereby an informed and engaged public can participate meaningfully in society, both online and offline. Digital literacy empowers users to make informed decisions, promote their access to information and economic opportunities, and protect their human rights and fundamental freedoms. Digital literacy, particularly from a younger age, also enhances the capacity of States to increase their own cybersecurity posture by improving the cyber security knowledge of all citizens and encouraging younger generations to pursue work in the cyber security industry. As the 2022 Chair of the Freedom Online Coalition, Canada is committed to promoting digital literacy to ensure users are empowered to navigate diverse content online and improve our collective cyber security capacity.'

Further findings and recommendations can be accessed in the report titled 'Pre-University Cyber Security Education: A report on developing cyber skills amongst children and young people'.

News

Professor Shujun Li wins the 2022 IEEE Transactions on Circuits and Systems Guillemin-Cauer Best Paper Award

Professor Shujun Li, Director of iCSS, has received the 2022 IEEE Transactions on Circuits and Systems Guillemin-Cauer Best Paper Award from the IEEE Circuits and Systems Society, for a research paper titled 'Dynamic Analysis of Digital Chaotic Maps via State-Mapping Networks', co-authored with Professor Chengqing Li and Mr Bingbing Feng (Xiangtan University, China), Professor Guanrong (Ron) Chen (City University of Hong Kong, China), and Professor Jüergen Kurths (Humboldt University of Berlin, Germany), and published in *IEEE Transactions on Circuits and Systems I: Regular Papers* (Volume 66, Issue 6, pages 2322–2335, June 2019, DOI: 10.1109/TCSI.2018.2888688).

The award was established in 1968 and is awarded annually. The criteria considered include the general quality, originality, contributions, subject matter, and timeliness of the paper. This year's winning paper was selected from over 3,000 papers published at two main journals of the IEEE Circuits and

Systems Society, *IEEE Transactions on Circuits and Systems I: Regular Papers* and *IEEE Transactions on Circuits and Systems II: Express Briefs*, in the past three calendar years preceding the award (2019-2021). The award was announced at the 2022 International Symposium on Circuits and Systems (ISCAS 2022), the flagship annual conference of the IEEE Circuits and Systems Society, which was held in Austin, TX, USA from May 28 to June 1, 2022.

Professor Li said: 'It is a great honour to receive the award, together with my other four collaborators. This piece of work represents a major development of quantitative and rigorous analysis of digital chaos since my 2005 paper 'On the Dynamical Degradation of Digital Piecewise Linear Chaotic Maps' published at the International Journal of Bifurcation and Chaos in 2005, by extending the analysis from statistical analysis under fixed-point arithmetic operations to network-based analysis under both fixed- and floating-point arithmetic operations. The work itself was the result of an international exchange project 'Dynamical degradation of chaotic systems in digital domain' funded jointly by the Royal Society in the UK and the National Natural Science Foundation of China (NSFC), from 2012-2014. It is interesting to see how the work took more than five years to be mature. Sometimes it does take time to make great things happen! I am very glad to see that the work has gained a substantial amount of attention from other researchers since published in 2019, and we hope it offers new tools for both theoretical analysis of digital chaos and its practical applications in many domains.'

Best Paper Award at IEEE DSC 2022 (5th IEEE Conference on Dependable and Secure Computing)

Sharifah Roziah Binti Mohd Kassim, 3rd Year PhD student at iCSS and the School of Computing, together with her PhD supervisors **Professor Shujun Li** (iCSS Director) and **Dr Budi Arief** (iCSS Innovation Lead), won the Best Paper Award (Experience and Practice Track) at the IEEE DSC 2022 (5th IEEE Conference on Dependable and Secure Computing), which was held on 22-24 June, 2022, in Edinburgh, UK and online as a hybrid event. The title of their award-winning paper is 'How National CSIRTs Operate: Personal Observation and Experience from MyCERT', co-authored with Dr Solahuddin Shamsuddin, Chief Technology Officer of CyberSecurity Malaysia.

This is an outstanding achievement, as the IEEE DSC Conference is a prestigious conference sponsored by the IEEE Reliability Society.

In 2022, the IEEE DSC conference also includes a category for experience and practice papers on recent findings that predominantly contribute to design know-how or the extension of the community's knowledge about how the security protection of known techniques fares in real-world operations.

Sharifah said: 'We are very pleased to have received this award for what we believe is a significant piece of work that connects research with practice for improving the real-world operations of Computer Security Incident Response Teams (CSIRTs) and the wider security operations.'

This paper provides personal observations and opinions regarding critical areas of operational practices in national CSIRTs, ie, the use of tools and data for investigations of cyber incidents, cyber threat information exchange and collaboration with cross-CSIRT organisations. The authors of this paper hope to induce more promising research to address the gaps identified in the study and contribute insights and guidelines that can be useful to national CSIRTs and cyber security practitioners.

News

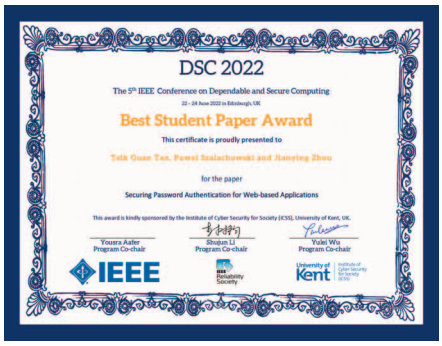
iCSS researcher receives 2022 IEEE SMC Society TCHS Research and Innovation Award

The IEEE SMC (Systems, Man, and Cybernetics) Society TCSC (Technical Committee on Homeland Security) announced its 2022 awards at the 2022 IEEE International Conference on Cyber Security and Resilience (IEEE CSR 2022) on 28th July 2022. Three cyber security researchers received the 2022 IEEE SMC TCHS Research and Innovation Award, including Professor Paul Haskell-Dowland (Edith Cowan University, Australia), Professor Kim-Kwang Raymond Choo (University of Texas at San Antonio, USA), and the iCSS Director Professor Shujun Li. Each of the awardees also gave a keynote speech at the IEEE CSR 2022 conference, with Professor Li's talk on 'Privacy through the Lens of Data Flows' (work of the EPSRC funded research project PriVELT Prof Li is leading) taking place on 29 July.

Professor Shujun Li said: 'It was my great honour to receive one of the three 2022 IEEE SMC Society TCHS Research and Innovation Awards at IEEE CSR 2022. Thank you to the IEEE SMC TCHS Award Committee for selecting me. This came as a (pleasant) surprise as more researchers have done greater work on homeland security than I have. I therefore take this as a recognition of how cyber security and homeland security are more and more connected, like what we are doing at iCSS, for example, my colleagues Dr Harmonie Toros and Dr Gareth Mott from our School of Politics and International Relations have been doing interesting research connecting the two research areas.'

iCSS sponsors Best Paper Awards

iCSS was delighted to sponsor three Best Paper Awards at the 5th IEEE Conference on Dependable and Secure Computing (IEEE DSC 2022). In addition to the Best Student Paper Award (Experience and Industry Track), which was won by **Sharifah Roziah Binti Mohd Kassim** with her PhD supervisors **Professor Shujun Li** (iCSS Director) and **Dr Budi Arief** (iCSS Innovation Lead), iCSS also sponsored the Best Paper Award (Main Track) and the Best Student Paper Award. The Best Paper Award (Main Track) was given to Bowen Zhao, Yingjiu Li, Ximeng Liu, Hwee Hwa Pang and Robert H. Deng. The Best Student Paper Award was given to Teik Guan Tan, Pawel Szalachowski and Jianying Zhou.



iCSS also sponsored two Best Paper Awards at the International Conference on Availability, Reliability and Security (ARES 2022).

Dr Virginia Franqueira, iCSS Deputy Director (Education), chaired the 6th International Workshop on Security and Forensics of IoT (IoT-SECFOR 2022), which focused on bringing together researchers and practitioners from both communities – security and forensics – to discuss problems and solutions regarding IoT. The Best Research Paper of the workshop was awarded to Henri Ruotsalainen.

Dr Franqueira also chaired the 15th International Workshop on Digital Forensics (WSDF 2022), which focused not only on digital forensics in the investigation of crime, but also security applications such as automated log analysis, forensic aspects of fraud prevention and investigation, policy and governance. The Best Research Paper Award of the workshop was given to Vaia-Maria Angeli, Ahmad Atamli and Erisa Karafili.

Congratulations to the recipients of the Best Paper Awards!

Cyber security awareness videos

Over the summer, iCSS filmed a group of our members and Early Career Researchers on what interests them about studying and researching cyber security. We have collated a series of short videos that will be released over the coming weeks.

In addition, iCSS have been working with two companies, Scriberia and Science Animated (Research Publishing International Ltd), to produce three animated videos for children on the importance of cyber security awareness. Stay tuned for more updates!

News

Survey results on cyber security in UK schools

iCSS and SWGfL, supported by Bitdefender, have created the **Cyber Security in UK Schools Report**, which provides an up-to-date review around the current state of cyber security of schools in England and Wales.

The report compiles a list of findings around behaviours, issues and risks within the field of cyber security of schools, derived from results of a survey that was run in late 2021. The responses gathered comprised 183 valid respondents from more than 170 schools in 126 different local authorities of England and Wales.

With malicious actors in the cyber space continuing to threaten our schools, this report highlights just how important it is that educational establishments put cyber security among the top entries on their risk register. Some of the key findings of the reports include:

- 76% of respondents said that the internet was key to their job
- 62% of schools did not receive any cyber security training
- 48% of all cyber security attacks reported by respondents were related to ransomware
- 35% of respondents said that their school regularly updates risk and business continuity plans
- 31% of respondents did not have an IT security policy
- 17% of respondents reported that they had no cyber security concerns

Andrew Williams, Online Safety and Information Security Consultant at SWGfl, said, 'This report is concerning, and highlights a need to invest in cyber security as cyber attacks continue to increase both in frequency and sophistication. There is a need for a cultural shift in schools. Cyber security should be the number one risk for all educational establishments in the UK. With a potential to impact on finance, attainment and reputation, establishments are advised to take prompt action now: assess organisational risk and record this in a risk register, run regular cyber security training for staff and identify what you would do and who would support you in the event of a cyber incident.'

Professor Shujun Li, a co-designer and co-analyst of the survey, said, 'As cyber security has been identified a priority of the country and many sectors, the education sector should not be left behind. Improving cyber security of schools is not just about protecting physical and digital assets of the school, but also about protecting people associated with the school, including pupils, school staff and parents, and their personal data. The report reveals a very worrying lack of sufficient cyber security measures at most schools in England and Wales, so we would like to urge all relevant parties to take urgent actions to raise the priority of cyber security within the education sector.'

Read about the top findings here https://swgfl.org.uk/research/cyber-security-in-uk-schools

Shanghai data breach exposes dangers of China's Trove

Bloomberg UK reported on a recent Shanghai police data breach claimed to be the largest cyberattack in Chinese history. If verified, the purported theft of 23 terabytes of personal information on as many as a billion Chinese citizens from a Shanghai police database would rank as the country' largest ever known data breach, if not one of the biggest leaks the world has seen. The allegations that emerged over the weekend have set tech circles buzzing and prompted rare public comment from high-profile industry figures such as Binance co-founder Zhao Changpeng.

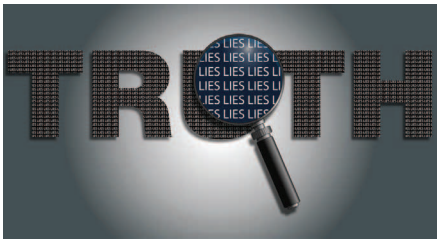
'It's common to see personal data offered for sale on Chinese cybercriminal forums but the scale and amount of personal data being offered here is unheard-of,' said Dr Budi Arief.

Read the full article here https://www.bloomberg.com/news/articles/2022-07-05/hacker-s-record-theft-claim-exposes-dangers-of-china-data-trove

Digital Data Deception (DDD) Technology newsletters

Between August 2020 and March 2022, the Institute produced 12 issues of the Digital Data Deception (DDD) Technology Watch newsletters. They cover a wide range of selected research papers, with real-world solutions and datasets.

The topics covered include both offensive and defensive deception, deepfake, adversarial AI, natural language generation (NLG), biometric spoofing and anti-spoofing, misinformation and fact checking, information hiding, and deception in different applications such as recommender systems, conversational agents and chatbots, cyber-physical systems, and cybercrime. From the third issue, the newsletter also started including substantial coverage of Chinese literature. Please visit https://research.kent.ac.uk/cyber/digital-data-deception-technology-watch-newsletters to download PDF files of all the 12 issues.



The managing editor of the newsletter series was **Dr Virginia Franqueira**, iCCS's Deputy Director (Education), and other editors who contributed to one or more issues included Enes Altuncu (PhD student of iCSS), Keenan Jones (PhD student of iCSS), Dr Sanjay Bhattacherjee (iCSS's Information Services Liaison Lead), Professor Shujun Li (iCSS Director), Yichao Wang (PhD student of iCSS), Ali Raza (PhD student of iCSS), Haiyue Yuan (PDRA of iCSS) and Li Qin (PhD student of School of Engineering).

iCSS technical reports

We have compiled a selection of recent technical reports co-authored or contributed by members of iCSS. Such technical reports were mostly produced for non-academic organisations especially policy makers.

Organisations that we have produced reports for include:

- Department for Digital, Culture, Media and Sport (DCMS)
- Cabinet Office
- National Cyber Security Centre (NCSC)
- Government Communications Headquarters (GCHQ)
- European Union Agency for Cybersecurity (ENISA)
- Global Forum on Cyber Expertise (GFCE)
- South West Grid for Learning (SWGfL)

Visit our website for more information.

News

Technology-facilitated intimate partner violence surged during Covid-19 pandemic

There was a 420% increase in reports of technology-facilitated intimate partner violence (TFIPV) during the Covid-19 pandemic, according to a new Home Office report led by researchers at iCSS.

Research carried out in partnership with The Cyber Helpline, the only UK not-for-profit helpline directly supporting victims of cybercrime, found that methods of TFIPV differed to those pre pandemic. Perpetrators were found to take advantage of an increased use of video calls and social media (particularly Facebook) and were more likely to engage in extortion., the only UK not-for-profit helpline directly supporting victims of cyber-crime, found that methods of TFIPV differed to those pre pandemic. Perpetrators were found to take advantage of an increased use of video calls and social media (particularly Facebook) and were more likely to engage in extortion.

Across the study period unwanted contact/communication and extortion were the most common types of TFIPV reported, with extortion most common in brief relationships. Whereas in long term partnerships, unwanted contact/communication and unauthorised access to smart devices and accounts were more common.

Perpetrators accessed accounts and smart devices via easily guessed or known passwords, with a lack of ID verification by online platforms flagged as a concern in the report.

Perpetrators were found to use simple methods and technologies to abuse, often using their knowledge of the victim's online habits and activities (eg, email, social media, GPS-enabled trackers, family sharing accounts, known passwords).

Shared spaces or physical proximity to victims allowed TFIPV perpetrators to manipulate devices, create fake accounts, install bugs and track locations. They used their knowledge of the victim's online habits and activities to abuse.

The researchers utilised case data and conducted in depth interviews with front-line responders of The Cyber Helpline, identifying the specific technologies used by perpetrators and establishing the requirements for high quality victim assistance from a cyber security perspective. This has helped to produce necessary data for government, law enforcement, practitioners, front-line responders and stakeholders to inform on appropriate interventions with perpetrators and victims of TFIPV, as well as the most suitable technical support.

Dr Afroditi Pina, a forensic psychologist at the University of Kent and an Associate Member of iCSS who co-led the project, said: 'Online service providers need to make it easier to identify and sanction perpetrators, while improving accessibility to talk to personnel via customer service helpdesks. TFIPV is a serious form of domestic abuse, but currently it is not considered as part of the Domestic Violence Act. It needs to be adequately represented in legislation as part of Intimate Partner Violence (IPV) and coercive control, with more action taken. There also needs to be further investment in police, IPV practitioner and responder training on cyber security and the recognition of TFIPV.'

Dr Jennifer Storey, also a forensic psychologist at the University of Kent and an Associate Member of iCSS who is the other co-lead of the project, added: 'While specialist support for victims is available, synergy between safeguarding agencies is urgently required, along with consistent funding. This would better support victims by allowing a single view of cases while improving perpetrator accountability.'

Dr Virginia Franqueira, a co-investigator on the project, said: 'Victims are often tasked to gather digital evidence themselves showing that TFIPV is taking place for a police investigation to be launched. This shifts the burden of proof to the victims, rather than the perpetrators, adding to their frustration and risk of escalation to serious physical harm. This calls for training about TFIPV, especially for first responders, and a greater resourcing for follow-up investigations.'

The Home Office report titled 'Technology-Facilitated Intimate Partner Violence: A multidisciplinary examination of prevalence, methods used by perpetrators and the impact of COVID-19' can be accessed from the technical reports page of the iCSS website: https://research.kent.ac.uk/cyber/technical-reports

In addition to the two co-leads, Drs Afroditi Pina and Jennifer Storey (both from the School of Psychology's Centre of Research and Education in Forensic Psychology [CORE-FP]), the project also involved two other academics at the University of Kent, **Dr Marian Dugga**n (School of Social Policy, Sociology and Social Research [SSPSSR]) who is an Associate Member of iCSS, and **Dr Virginia Franqueira** who is iCSS's Deputy Director (Education).

New research projects

Industrial grant awarded to study blockchain technologies in the quantum world

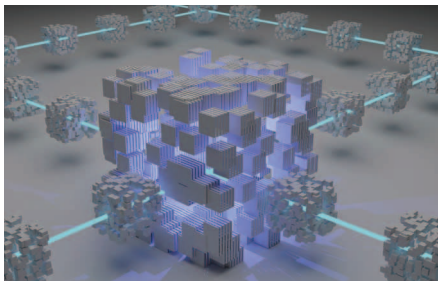
The Institute of Cyber Security for Society (iCSS) and the School of Computing are celebrating a new industrial grant awarded to University of Kent Lecturer, **Dr Carlos Perez-Delgado**, for research into the intersection of cybersecurity, blockchain technologies and quantum information. The grant, provided by the Casper Association, starts in June 2022 and is worth £155,000 for its initial period until September 2023, with further funding for up to three years afterwards.

Blockchains and cryptocurrencies are now deeply embedded in society. The highly-volatile cryptocurrency market hit a high market capitalisation mark of $3 trillion USD in November 2021. While this market currently faces many challenges, quantum technological advances could become its greatest threat. These same advances could also potentially open the door to yet untapped, and even unimagined economic opportunities. It is only through comprehensive research of the intersection of these two technologies (quantum and blockchains) that society will be able to unlock and exploit these opportunities, as well as avoid potential disasters.

This grant will allow Carlos and his research group to thoroughly investigate the consequences–both positive and negative–of quantum technology advances into blockchains, cryptocurrencies, and their markets. They will create protocols and algorithms to exploit quantum tech to improve blockchains, where possible, and develop strategies to mitigate the negative impacts of quantum tech, such as attacks from quantum-enabled malicious actors.

The funder, The Casper Association, is a non-profit organisation that oversees the ongoing evolution and decentralisation of the Casper Network. It provides resources to help accelerate the adoption of Casper and its growing ecosystem of decentralized applications. The Casper network is a scalable, enterprise-optimised, proof-of-stake blockchain system that aims to be future-proof. The research at Kent will help the Casper network to achieve its aim of remaining future-proof.

Mark Greenslade, Head of R&D at Casper Association, said: 'Securing blockchain systems is a serious topic that requires continuous review of the emerging threat landscape. Few if any of the cryptographic schemes leveraged by existing networks are quantum resistant in any meaningful way. By collaborating with University of Kent the Casper Association is sending a strong signal that it takes this issue seriously. Furthermore, and perhaps more importantly, the Association is confident that the work of Carlos and his team will prove beneficial not only to the Casper network but to the wider blockchain community as a whole.'



Funding awarded for new research project, 'Transparent pointer safety: Rust to Lua to OS components'

iCSS member **Professor Mark Batty**, and Early Career Researchers **Simon Cooksey** and **Michael Vollmer**, have been awarded a research grant by EPSRC for a new project entitled 'Transparent pointer safety: Rust to Lua to OS Components.'

Digital Security by Design (DSbD) is an initiative supported by the UK government to transform digital technology and create a more resilient, and secure foundation for a safer future. Through collaboration between academia, industry and government, these new capabilities will pave the way business and people can use and trust technology.

This project forms part of this challenge, by developing a vertical stack in the DSbD eco-system in three parts: a Rust compiler; an implementation of Lua in Rust; and integration of this Lua interpreter into FreeBSD, replacing a core component of the FreeBSD bootloader with software built in DSbD tech. These elements, together with a theoretical case study, will demonstrate scalable security reasoning enabled by the new capability features.

Dr Jason Nurse to co-investigate how small and medium-sized enterprises (SMEs) can become more privacy aware

Dr Jason Nurse, iCSS's Public Engagement Lead, will join Maria Bada (Queen Mary University London) and Steven Furnell (University of Nottingham) in investigating current practices in relation to the drivers and unique obstacles that SMEs face, in making privacy-aware decisions. The project, funded by REPHRAIN (the National Research Centre on Privacy, Harm Reduction and Adversarial Influence Online), aims to help SMEs understand the significance of privacy threats to their business, and support them in applying appropriate measures to face them.

The 12-month project will address three key challenges: the lack of wider research and understanding around the extent to which SMEs understand and use Privacy Enhancing Technologies (PETs); how best they could be supported in order to use PETs more effectively, given their constraints; and how to enable effective communication and engagement with SMEs.

Dr Jason Nurse said about the project: 'Organisations and users face numerous occurrences of privacy incidents and data breaches. Small and Medium Enterprises (SMEs), in particular, often do not fully appreciate the importance of privacy threats, with owners and operators more immersed in day-to-day business operations and dedicating primary resources elsewhere. This research project aims to help SMEs address privacy concerns through the development of a SME Privacy Starter Pack (SPSP). This pack would promote awareness about privacy tailored to SMEs and their context, and support SMEs in identifying how privacy and related privacy-enhancing technologies are pertinent to them.'

iCSS Team news and new publications

New members

iCSS welcomes the following new members

Associate Members

Dr Eddie Luo is currently Lecturer of Marketing at Kent Business School. He received his PhD in Business Management from a joint programme at Southwest Jiaotong University, China and Aston Business School, UK. He holds a BSc in Management Information System. Prior to joining KBS, he was Associate Professor and served as Head of Marketing and Director of International Cooperation in Business School, Southwest University of Political Science and Law, China. Eddie's research interests focus on consumer behaviour/psychology and marketing communications. He is also interested in technology innovation, sharing economy, strategy, and entrepreneurship. He has published in leading journals such as International Journal of Research in Marketing and Journal of Business Research.

More information about Eddie can be found at: www.kent.ac.uk/kent-business-school/people/2927/luo-eddie

Professor Frank Zhigang Wang is Professor in Future Computing at the School of Computing. Five years after his PhD degree, he was promoted to a full professorship at the Cambridge Cranfield High Performance Computing Facility in 2004. He was made the Head of School of Computing at the University of Kent in 2010. So far, Frank has attracted research grants from the EC/UK government/industries that total £5m. He served as a panel member for the UK government EPSRC 'e-Science' and 'Hardware for Efficient Computing' programmes. He is a Fellow of British Computer Society (BCS). He is currently the Chairman of the UK and Ireland Chapter, IEEE Computer Society.

More information about Frank can be found at www.kent.ac.uk/computing/people/3083/wang-frank-zhigang

iCSS members receive Above and Beyond Teaching Awards

The Above and Beyond Awards were launched by Kent Union to celebrate outstanding members of staff, both academic and non-academic. Students nominate staff who they believe have gone the extra mile in their role.

Since March 2020, over 1000 Above and Beyond nominations were submitted by students, but, because of the pandemic, the University wasn't able to properly administer the nominations and reward those incredible staff until now.

In May earlier this year, the University of Kent held its Above and Beyond Award Reception to celebrate staff who have been working hard to make the lives and experiences of students as positive as possible during challenging times. We are delighted that a number of iCSS staff were nominated for an Above and Beyond Award from across the institute, and we congratulate them wholeheartedly.

KENT UNION
KENTUNION.CO.UK

iCSS Team news and new publications

Matthew Boakes wins Postgraduate Teacher Prize

iCSS are delighted to congratulate its ECR (Early Career Researcher) Member **Matthew Boakes** on winning the Postgraduate Teacher Prize at the recent 2022 Graduate and Researcher College (GRC) Prize ceremony held by the University of Kent. Here's what Matthew had to say:

'I am incredibly humbled to have been awarded this year's GRC Postgraduate Teacher Prize 2022. First, I want to express my sincere gratitude to Anna Jordanous, who did not hesitate and was overly willing and accommodating to provide a letter of recommendation to support my application (at a somewhat late notice of the deadline).

'Second, I have always enjoyed my teaching commitments at Kent in supporting foundation level students through to master's level across a range of modules in the School of Engineering and School of Computing, sometimes to the detriment of my research goals and timelines. However, the feedback from students in helping them overcome difficulties and understand topics has always made it worthwhile to me.

'Truthfully, I'm not sure what I will spend the money on yet as hopefully (fingers crossed) I am coming towards the end of my PhD journey. Still, I hope to find a good use for it in future research or development opportunities.

'Finally, I would like to thank all the students, friends and colleagues who have provided me with positive well-being and constructive feedback to adapt my teaching and the GRC for recognising my achievement. I look forward to future working in academia alongside the fantastic support of the academics across the university and within the iCSS on supporting existing and new cybersecurity-related courses as we help prepare the next generation for a cyber world. Winning this prize further encourages me to pursue a career in education and academia.'

Selected new publications

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

Belen Sağlam, R; Nurse, J R C, & Hodges, D (2022). 'An Investigation into the Sensitivity of Personal Information and Implications for Disclosure: A UK Perspective,' *Frontiers in Computer Science*. doi: 10.3389/fcomp.2022.908245.

Bhattacherjee, S; Sarkar, P (2022) 'Voting Games to Model Protocol Stability and Security of Proof-of-Work Cryptocurrencies,' accepted to GameSec 2022, to be published in a volume of Lecture Notes in Computer Science by Springer.

Delgado-Santos, P; Stragapede, G; Tolosana, R; **Guest, R**; Deravi, F and Vera-Rodriguez, R (2022) 'A Survey of Privacy Vulnerabilities of Mobile Device Sensors,' *ACM Computing Surveys*. ACM. doi: 10.1145/3510579.

Erola, A; Agrafiotis, I; **Nurse, J R C**, Axon, L; Goldsmith, M & Creese, S (2022). 'A system to calculate cyber-value-at-risk,' *Computers & Security, 113*, 102545. doi: 10.1016/j.cose.2021.102545.

Jones, K; **Nurse, J R C** & **Li, S** (2022, May). 'Are You Robert or RoBERTa? Deceiving Online Authorship Attribution Models Using Neural Text Generators,' in *Proceedings of the International AAAI Conference on Web and Social Media* (Vol. 16, pp. 429-440).

Jones, K; **Nurse, J R C** & **Li, S** (2022). 'Out of the Shadows: Analyzing Anonymous' Twitter Resurgence during the 2020 Black Lives Matter Protests,' in *Proceedings of the International AAAI Conference on Web and Social Media* (Vol. 16, pp. 417-428).

Mohamed, E; Sirlantzis, K; **Howells, G** (2022) 'A review of visualisation-as-explanation techniques for convolutional neural networks and their evaluation,' *Displays*, 73:102239. doi: 10.1016/j.displa.2022.102239.

Mohamed, E; Sirlantzis, K; **Howells, G** (2022) 'Analysing the Impact of Vibrations on Smart Wheelchair Systems and Users,' in *Pattern Recognition and Artificial Intelligence: Third International Conference, ICPRAI 2022, Paris, France, June 1–3, 2022, Proceedings, Part I*, pp. 25–33.. doi: 10.1007/978-3-031-09037-0_3.

Mohd Kassim, S R B; Shamsuddin, S B; **Li, S** & **Arief, B** (2022) 'How National CSIRTs Operate: Personal Observations and Opinions from MyCERT,' in **Proceedings of the 2022 5th IEEE Conference on Dependable and Secure Computing** (IEEE DSC 2022), doi: 10.1109/DSC54232.2022.9888803.

Pan, S; **Hoque, S**; Deravi, F (2022) 'An Attention-Guided Framework for Explainable Biometric Presentation Attack Detection', *Sensors*, 22 (9). Article Number 3365. ISSN 1424-8220. doi:10.3390/s22093365.

Panteli, N; **Nurse, J R C**; Collins, E & Williams, N (2022). 'Trust disruption and preservation in the Covid-19 work from home context,' *Journal of Workplace Learning*. doi: 10.1108/JWL-02-2022-0017.

Pattnaik, N; **Li, S** & **Nurse, J R C** (2022) 'A Survey of User Perspectives on Security and Privacy in a Home Networking Environment,' accepted to *ACM Computing Surveys*, in press. doi: doi/10.1145/3558095.

Shere, A R; **Nurse, J R C** & Martin, A (2022). 'Threats to Journalists from the Consumer Internet of Things.' Presented at the International Conference on Cybersecurity, Situational Awareness and Social Media (Cyber Science 2022), Cardiff, Wales.

Turner, S; **Nurse, J R C** & **Li, S** (2022, April). '"It was hard to find the words': Using an Autoethnographic Diary Study to Understand the Difficulties of Smart Home Cyber Security Practices," in CHI EA '22: Extended Abstracts of the 2022 *CHI Conference on Human Factors in Computing Systems* (Article Number 34, pp. 1-8). doi: 10.1145/3491101.3503577.

Xu, Y; Guo, J; Qiu, W; Huang, Z; **Altuncu, E** & **Li, S** (2022) '"Comments Matter and The More The Better!': Improving Rumor Detection with User Comments," accepted to TrustCom 2022 (21st IEEE International Conference on Trust, Security and Privacy in Computing and Communications) as a regular paper, in press.

Yuan, H & **Li, S** (2022) 'Cyber Security Risks of Net Zero Technologies,' in *Proceedings of the 2022 5th IEEE Conference on Dependable and Secure Computing* (IEEE DSC 2022). doi: 10.1109/DSC54232.2022.9888883.

Zahrah, F; **Nurse, J R C** & Goldsmith, M (2022). 'A comparison of online hate on reddit and 4chan: a case study of the 2020 US election,' in *Proceedings of the 37th ACM/SIGAPP Symposium on Applied Computing* (pp. 1797-1800). doi: 10.1145/3477314.3507226.

Events and talks

iCSS members visit Digital Rights Foundation (DRF) in Pakistan

In July 2022, **Dr Gareth Mott**, iCSS Student Engagement Lead and Lecturer in Security and Intelligence, and **Miss Ramsha Ashraf**, an iCSS Doctoral Student, visited the headquarters of the Digital Rights Foundation in Lahore, Pakistan. The Digital Rights Foundation is a prominent non-governmental organisation in Pakistan, which promotes and researches digital privacy and security, develops policy reports, and operates a helpline for victims of cyber harassment. Dr Mott and Miss Ashraf met with colleagues at the DRF, including Shmyla Khan, the DRF's Research and Policy Director, to discuss and substantiate planning for future research and grant collaboration.

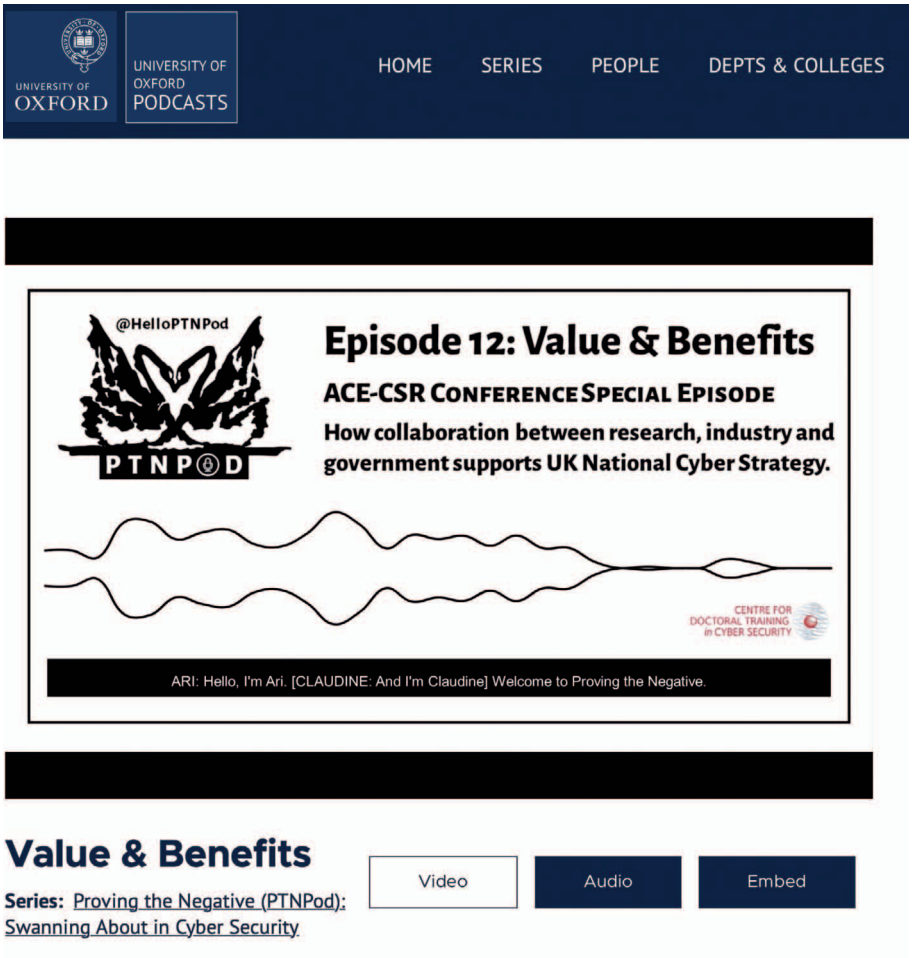
UK cyber strategy at the Academic Centres of Excellence in Cyber Security Research (ACE-CSR) 2022 Annual Conference

Dr Harmonie Toros, iCSS Deputy Director (Interdisciplinarity), and PhD student **Matthew Boakes** spoke on podcast Proving the Negative (PTNPod) at the Academic Centres of Excellence in Cyber Security Research (ACE-CSR) conference. This episode takes a deep dive into how collaboration between research, industry and government supports wider national objectives, and looks at how cutting edge research is done, and drawn into the wider UK ecosystem in support of the National Cyber Strategy (to be confident, capable and resilient).

Dr Toros examined the importance of bringing in key considerations that have emerged in critical security studies over the past 30 years into cyber security. She talked about the need to avoid some of the real mistakes that marred the study and practice of security (and terrorism for example) in cyber security and a key way of doing this is to learn from those mistakes.

Matthew spoke about his work in biometrics and where he sees biometrics providing the most value, helping towards the goal of a passwordless society with sensors now embedded into the majority of (mobile) devices. They also spoke about the ethical considerations in using the technology and how this is something that will require further input to gain the public's trust, using the current use of facial recognition technology in Russia and Ukraine as an example.

You can listen to the episode here: https://podcasts.ox.ac.uk/value-benefits



Events and talks

'We Are Listening' Workshop

On 17 May 2022, Jim Lamprell, Business Relationship Officer, and **Dr Budi Arief**, iCSS's Innovation Lead, represented the University of Kent and iCSS in delivering a consultancy service, as part of the 'We Are Listening' Workshop. The event was organised and hosted by the Kent Invicta Chamber of Commerce at their venue in Ashford, and it was attended by 15 delegates from various SMEs from all around Kent.

The workshop's topic was 'Cyber Security Challenges', in which delegates discussed various cyber security challenges they have faced in running their businesses. Budi contributed his cyber security knowledge and experience during the Q&A session. Towards the end of the workshop, Jim outlined several ways to collaborate with the University of Kent and iCSS, while Budi presented his work on ransomware, which is still one of the most pressing concerns faced by many organisations. Through this event, Budi helped in raising security awareness among delegates, and he also provided some practical advice that delegates can take home and apply for improving their cyber security resilience.

Global Forum on Cyber Expertise (GFCE) Annual Meeting 2022

Dr Virginia Franqueira, iCSS's Deputy Director (Education), attended the GFCE's Global Annual Meeting 2022 in The Hague (Netherlands) on 13-15 September 2022, representing iCSS as an official partner of the GFCE. The cyber capacity building meeting this year focused on 'co-ordination for the future' and was attended by more than 200 delegates from many member and partner organisations from all around the world including regional hub co-ordinators, and representatives from governmental bodies, NGOs, tech communities and civil societies. It was rewarding to meet familiar faces we worked with or interviewed as part of our research on 'developing cyber skills amongst children and young people', commissioned by the GFCE. It was also amazing to see that so much has been done and the potential big impact that can be achieved with such a strong sense of community around improving cyber capacity globally.

REF 2021 Research Excellence Framework

Recent talks and panel discussions

'Voting in the Goods and Services Tax (GST) Council of India.' National Institute of Science Education and Research, India. August 2022.
Speaker: **Dr Sanjay Bhattacherjee**.

'When Humans and Computers Come Together: A New or Resurged Old Research Paradigm?' Keynote talk at 4th International Conference on Artificial Intelligence Technologies and Applications (ICAITA 2022). August 2022.
Speaker: **Professor Shujun Li**.

'Round table discussion: IoT Security for eHealth.' SecHealth workshop, ARES 2022. August 2022.
Speaker: **Dr Virginia Franqueira**.
Panellists were: Sokratis Katsikas (Norwegian University of Science and Technology, Norway), Bian Yang (Norwegian University of Science and Technology, Norway), Reijo Savola (University of Jyväskylä, Finland)

'Privacy through the Lens of Data Flows.' Keynote talk at 2022 IEEE International Conference on Cyber Security and Resilience (IEEE CSR 2022). July 2022.
Speaker: **Professor Shujun Li**.

'Truth, Trust and Harm Online: Who is responsible?' The 64th London International Youth Science Forum. July 2022.
Speaker: **Dr Jason Nurse**.

Panelist of a panel discussion 'Tackling Human Error.' Panel discussion, Public Sector Cyber Security 2022. July 2022.
Speaker: **Professor Shujun Li**.

'Privacy through the Lens of Data Flows.' Cyber Quarter Seminar Series, organized by Cyber Quarter – Midlands Centre for Cyber Security. July 2022.
Speaker: **Professor Shujun Li**.

"'You're never left alone:' the use of digital technologies in domestic abuse." Computer Laboratory Security Seminar, University of Cambridge. May 2022.
Speaker: **Dr Jason Nurse**.

'Is Cyber Insurance Right for Your Organisation?' The Richmond Cyber Security Forum. May 2022.
Speaker: **Dr Jason Nurse**.

'Reducing Third-Party Identity Risk During the Great Resignation and Beyond.' Infosecurity Magazine Webinar. May 2022.
Speaker: **Dr Jason Nurse**.

'How to Do (Good) Research? Starting from Scientometrics...' School of Computing, University of Kent, UK. May 2022.
Speaker: **Professor Shujun Li**.

'Introducing the Institute of Cyber Security for Society (iCSS).' Honda Research Institute Europe, Germany. April 2022.
Speaker: **Professor Shujun Li**.

'The Big Breach: Communicating with the Citizen and Businesses.' ASEAN-Singapore Cybersecurity Centre of Excellence (ASCCE)-UK Cyber Conference & Workshop on Strategic Communications with the UK Government Communication Service International (GCSI). March 2022.
Panel Chair and Speaker: **Dr Jason Nurse**.

"How to train more Cybersecurity experts: 'Addressing Skills Shortage and Gap Through Higher Education.'" Keynote talk at Digital Skills and Jobs Platform webinar, European Commission. March 2022.
Speaker: **Dr Jason Nurse**.

'Tackling a multidisciplinary cyber security problems.' RISCS Away Day for Early Career Researchers. March 2022.
Speaker: **Dr Jason Nurse**.

'Communicating after Cyber Security Incidents.' University of Nottingham Cyber Security Group seminar. March 2022.
Speaker: **Dr Jason Nurse**.

iCSS photo competition

Remember to submit your photo to our competition, Living Learning and Connecting in Cyberspace

We increasingly rely upon networked technologies and the internet infrastructures upon which these rely; the myriad miles of fibreoptic cables, the banks of servers, the lofty data centres and the ever-encircling satellites. However, these integral systems are often unseen, overlooked, and sometimes intentionally concealed. Additionally, the software and hardware that we see in our everyday environments – laptops, desktops, smartphones, smart devices and so forth – are often so entrenched in our way of being that we overlook our reliance upon them until they stop functioning; a power cut, server downtime, an empty battery.

This competition welcomes photograph submissions that engage with the human experiencing of cyberspace and its interconnected hardware and software. Use your camera or other image-capturing device – whether SLR, polaroid, smartphone camera, webcam, Game Boy® pocket camera – to capture a moment that tells a story about living, learning and connecting in cyberspace.

Submitted photographs will be judged for **up to 26 prizes in three categories** (University of Kent staff, University of Kent students and non-UniKent participants who are UK residents and aged 13 or above):

- Three best overall photo prizes (one per category, £100 Amazon voucher per prize)
- Three most creative photo prizes (one per category, £100 Amazon voucher per prize)
- 20 runner-up prizes (five for University of Kent staff, five for University of Kent student, and ten for non-UniKent participants; £20 Amazon voucher per prize).

Please note that this competition is designed for University of Kent staff and students, and UK residents aged 13 or above only. The deadline is **31 October 2022**. Submit your photograph on our website.

Institute of Cyber Security for Society
Keynes College, University of Kent, Canterbury, Kent CT2 7NP
E: cyber-info@kent.ac.uk

UniKentCyberSec **UniKentCyberSec**

Institute of Cyber Security for Society (iCSS)

https://cyber.kent.ac.uk

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

DPC 132801 10/22