News
Page 2

News
Page 5

Public engagement work
Page 9

Newsletter

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

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

Winter 2021-22

Welcome

Welcome to the sixth issue of the iCSS Newsletter. Every quarter we share a round-up of the latest news, activities, and events that we think will be of most interest to our members, colleagues, and partner organisations. We strive for our newsletter to be collaborative, and your feedback is important to us. If you want to share your own news, contribute suggestions and feedback, or if you would like to sign up to our mailing list, please contact us at cyber-info@kent.ac.uk. We also maintain an archive of past newsletters on our website: cyber.kent.ac.uk

Institute of Cyber Security for Society (iCSS)

@UniKentCyberSec @UniKentCyberSec Institute of Cyber Security for Society (iCSS)

News

Higher Education in Europe: Understanding the Cybersecurity Skills Gap in the EU

A new policy report co-led by **Dr Jason Nurse** has found that the number of programmes and students engaged in cybersecurity within higher education are growing. This is also complemented by an increase in state-level initiatives across Europe in cybersecurity skills.

As a consequence, the number of graduates in the next 2-3 years is expected to double in Europe. However, more is still needed to tackle the cybersecurity skills shortage and gap; for instance, gender balance is still an issue with only 20% of female students enrolled.

The new report issued by the European Union Agency for Cybersecurity (ENISA) analyses data gathered by the Cybersecurity Higher Education Database (CyberHEAD) in order to make a prediction on the future trends. It also reflects on national policies and initiatives that have been put forward to address the pressing need for cyber skills.

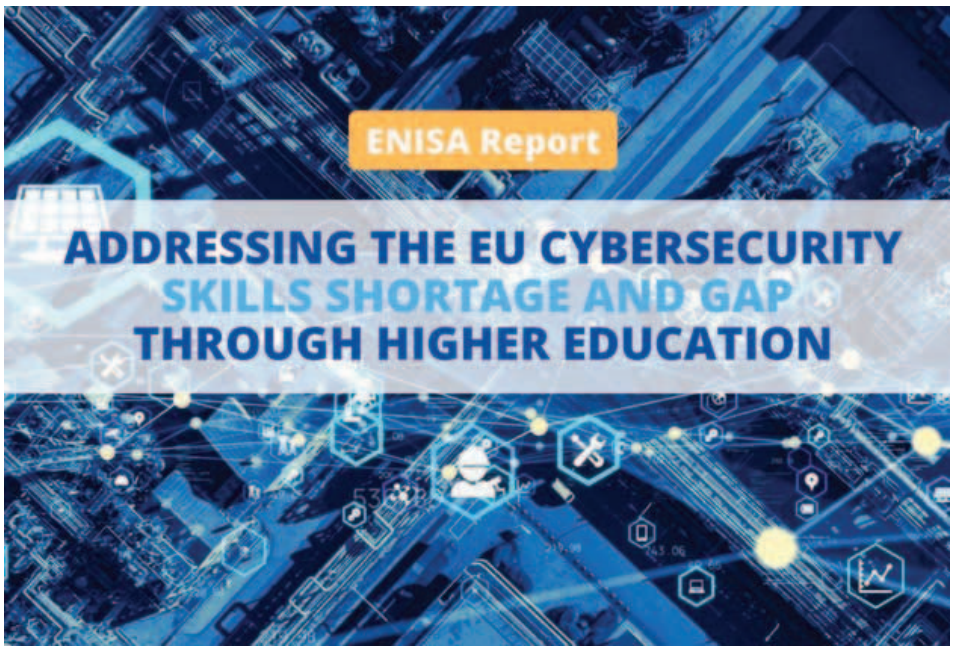
The report's findings are encouraging with the cybersecurity field continuing to expand. Over the past decade a worrying skill gap and shortage had emerged, with the demand for specialists increasing, but a lack of skilled workers entering the field. National labour markets have been disrupted worldwide as a consequence.

The report proposes a series of recommendations to mitigate the cybersecurity skills gap, which are intended for European Nations and Institutions interested in cybersecurity skills and the role that Higher Education has to play, EU Higher Education Institutions (HEIs), Business and industry, and researchers and the academic community. These recommendations centre on actions to increase the student enrolment on cybersecurity degrees and the quality of candidates, equipping them with the skills needed and most in demand in the field. They also focus on how to improve the diversity of graduates and thus the future security workforce.

Dr Nurse said: 'Our findings show that cybersecurity developments (eg, student enrolment, graduates, topics covered by security degrees) in higher education are moving in the right direction, which is great to see. This report advises how we can make the field more attractive to students and graduates, from diversifying the curriculum, through to the education format and provision of scholarships in HEIs. There is also the need for a unified approach across government, industry and HEIs to set a standard of skills and knowledges and a common framework regarding cybersecurity roles.

'It is concerning that only 20% of current cybersecurity students enrolled are female and this, amongst other topics, needs further investigation to understand how greater diversity – in gender and additional areas – can be driven in the field.'

The report titled *Addressing the EU Cybersecurity Skills Shortage and Gap Through Higher Education* can be accessed on ENISA's website.



Consent in the digital age: Protecting your information

As part of Safer Internet Day 2022, iCSS members and Kent academics shared their expertise and tips on keeping ourselves and each other safe in the digital sphere.

It has been said that in 2020 the world moved online. Two years on and, although we are no longer confined to digital spaces, our digital presence is ever increasing. When you visit a website, what do you want the organisation running the website to know about you, and to share with other organisations? What do you feel comfortable having others – friends, family or others – share about you online? These are questions of consent. Digital consent is one of the most important considerations of using the Internet: what do you want to share about yourself online?

We recognise that giving genuine and informed consent is increasingly difficult in a world where requests to 'accept Terms and Conditions' and 'Privacy Policies' are constantly showing up on our screens, so iCSS members provided some tips to help people protect their information.

Have a look at our tips here.

News

iCSS research cited in plans for a new government Bill

In 2021, Institute for Cyber Security for Society (iCSS) member **Dr Jason Nurse**, Senior Lecturer (Associate Professor) at the Institute of Cyber Security for Society (iCSS) and School of Computing, contributed to a government-commissioned Ipsos MORI report, titled *Consumer Attitudes Towards IoT Security*. This report detailed the findings of an online survey of the UK public, exploring consumer purchasing behaviour of, and attitudes towards connected devices.

This report has now been cited in government plans for new legislation, The Product Security and Telecommunications Infrastructure (PSTI) Bill.

The Bill proposes developing new regulatory frameworks that will ensure consumer products, such as smart TVs, smartphones and internet connected speakers, are regulated to protect consumers from cyber harm such as loss of privacy and personal data.

Further information can be found on the UK Government's website, here: www.gov.uk/guidance/the-product-security-and-telecommunications-infrastructure-psti-bill-product-security-factsheet

News

How technology is driving new forms of domestic abuse

Domestic abuse perpetrators are increasingly using digital and online technologies to monitor, threaten and humiliate their victims, according to a new Home Office report co-authored by **Dr Jason Nurse**. Last month, we provided some background into our new report and highlighted some key findings. In a new write-up, published in The Conversation, we outline our findings in the context of current research:

Perpetrators of domestic abuse are increasingly exploiting digital tools to coerce and control their victims. Where there is abuse in a relationship, technology will also feature in how that abuse is conducted. Police forces now expect as much, when responding to cases of domestic abuse.

Such technological abuse features everyday tools, from smart devices to online platforms and mobile phone apps. And the information on where to find them and how to use them is easily accessible online, often using a simple Google search.

To understand the extent of this problem, we conducted a wide-ranging study for the UK government. We reviewed 146 domestic abuse cases reported in British and international media, and conducted in-depth interviews with support charity workers and frontline police officers in England.

We found that abusers often have physical access to their partners' devices and use them to monitor, harass and humiliate. Abusers can force their victims to disclose passwords, PIN codes or swipe patterns to get into their devices so they can install sypware – all without sophisticated tech knowledge.

Geolocation software and other surveillance spyware provide new possibilities for abusers to monitor and track victims' movements. In our study, we found hundreds of tools online that could be used for these purposes.

Read the full article here. The report has also been reported on by Kent Online and the American Institute of Physics.

Inspiring the next generation of mathematicians, computer scientists and cryptographers

Professor Andrew Hone, Associate Member of the iCSS, **Dr Sanjay Bhattacherjee**, Lecturer and Information Services Liaison Lead for iCSS, and Joe Mist, a student of MSc Artificial Intelligence with an Industrial Placement, are working with the Institute for Research in Schools (IRIS) on a new project, *Huge Primes*, which focuses on prime numbers and primality testing.

This project aims to give school students throughout the UK the opportunity to learn techniques from mathematics and cryptography that underpin the security of everyday applications, like online shopping, social media and internet banking.

Participants in the project will not only be able to find out how modern cryptography works, but will also have the chance to get involved in original research. The goal is to inspire the next generation of mathematicians, computer scientists and cryptographers.

Andrew aims to develop the web materials for this project with IRIS in the first half of 2022, so that the research can start trials and gauge interest by getting feedback from a small group of schools in the summer. Ideally, the pilot will be ready to run by September 2022, if not the full project launch. Maplesoft has agreed to sponsor the project by making free Maple licences available to all participating students.

News

UK Cyber Security PhD Winter School

The 3rd Annual UK Cyber Security PhD Winter School, sponsored by the National Cyber Security Centre (NCSC) and co-organised by the UK Cyber Security PhD Network, took place virtually on 10-12 January 2022. **Professor Shujun Li**, Director of iCSS, was a member of the Organising Committee, and core members **Dr Harmonie Toros**, Deputy Director of iCSS, **and Dr Jason Nurse** took part in the event as a speaker and a judge, respectively.

During the event, several talks, keynote sessions and panel discussions were held. Talks were divided into three tracks that participants could choose from:

- Society and Privacy
- AI-related Security
- Protocols and Cryptography

The panel discussions helped guide attendees in building their own international network, and discussed what opportunities were available to them as newly graduated researchers and postdocs.

There were many useful tips mentioned and discussed from the perspectives of more experienced academics, professors and researchers in the industry.

As part of the winter school, the 'Capture the Flag' (CTF) Competition was hosted by Hack the Box. Early Career Researchers **Pierre Mondon**, **Matthew Boakes** and **Yichao Wang** played as a team and came second out of 13 teams. Pierre Mondon, who has played many CTF competitions in the past, scored First Blood (first flag of the competition), and got the most flags in the competition as an individual. The team aimed to tackle 21 challenges over a 10 hour period, each challenge ranging in difficulty. Those challenges included:

- **Web security:** find vulnerabilities on misconfigured servers and break them.
- **Cryptography:** exploit some poorly implemented encryption schemes.
- **Digital forensics:** find secret information hidden within a large number of files and systems.
- **Open-source intelligence (OSINT):** using publicly available sources to find secret information.
- **Full pwn:** exploiting a range of vulnerable programs running on remote servers to gain server administrator privileges.

They managed to achieve an incredible 16 challenges out of the total 21. At the last minute, one hour before the end, they were overtaken by a team who scored one more challenge to take first place. The team who took third place achieved 11 out of 21 challenges.

Yichao said: 'It was a good chance for me to learn something new during the competition, and it was enjoyable to play as a team.'

Following the game, the team are determined to review their weaknesses so that they can target areas to improve on for future CTFs.

News

Kentium 4 tackles *Cyber 9/12 Strategy Challenge*

The University of Kent was represented at the Atlantic Council's prestigious 2022 *Cyber 9/12 Strategy Challenge*, with an interdisciplinary team of postgraduate and undergraduate students. The *Cyber 9/12 Strategy Challenge* is a student-oriented event in which students assume the role of advisors to senior ministers and civil servants, in the midst of a real-time national cyber crisis. Teams must develop policy recommendations and deliver succinct assessments to judging panels comprised of industry experts, in escalating competitive rounds. The all-University of Kent team, Kentium 4, included **Asta Kjerrman** (MA International Relations), **Camille Catania** (MSc Computer Science), **Johann Airieau** (MA International Relations) and **Gabriel Doyle-Finch** (BSc Computer Science), with **Dr Gareth Mott**, Lecturer and Student Engagement Lead with the iCSS, supporting the team as Coach. The 2022 running of the *Cyber 9/12* competition was its most-competitive and in-demand event to-date, and the team were absolutely delighted to have been accepted into the competition, and to have had the privilege to have successfully entered the semi-final rounds in the second day.

Gareth: 'It was a delight to support the University of Kent's participation, for the second year-running, in the Cyber 9/12 Strategy Challenge. This is an utterly brilliant competition, that frankly makes me wish I were a student again! I, and our Institute of Cyber Security for Society colleagues, are extremely proud of the outstanding endeavours undertaken by our Kentium 4 students. Asta, Camille, Johann and Gabriel worked seamlessly as a strong, agile, and competitive team. Their comprehension of the rolling cyber crisis was astute, and their policy recommendations and presentational skills were well-received by judges during the competitive rounds.Each team member demonstrated the keen synergy between technical and socio-political cyber security that is emblematic of the teaching and education culture at the University of Kent, supported by the iCSS. I have no doubt that each team member would excel in a career in cyber security, or a career of their choosing, drawing on the skills that they have deployed and refined during the course of this competition. Well done, Kentium 4!'

Asta: 'The competition was a unique learning opportunity for me. It enhanced my skills in working across fields, both in developing understandings in new areas and communicating my knowledge to other students outside my field. During the competition, I was able to apply my skills in working under high pressure and adapting to the changes in circumstances. Lastly, *Cyber 9/12* was a great opportunity to get an insight into daily livelihoods in cybersecurity'.

Johann: 'The *Cyber 9/12 Strategy Challenge* was an incredible opportunity for me as a postgraduate student in International Relations. Cybersecurity's importance is growing due to a lot of cyber threats looming on companies, public administrations, and private citizens. The scenario gave us the opportunity to link theoretical knowledge learned at the university – for instance, deploying knowledge from Dr Mott's *Governance and War in Cyberspace* module – and from our own experiences to (almost) real life events. This event challenged our time management skills and made us work very hard to produce a report with credible answers to propose to decision makers of Her Majesty's Government. Events and deadlines bonded the team and created a real cohesion. I recommend to any student interested in cybersecurity, defence affairs, or policy making to get involved in this competition next year!'

University of Kent students attended the NCSC Innovators Challenge Event

Three students enrolled on the MSc Cyber Security course at the University of Kent had the opportunity to take part in the NCSC Innovators Challenge event in Manchester, held by the National Cyber Security Centre – a part of GCHQ. This 3-day event, held between 28 February and 2 March 2022, aimed to facilitate discussion between students from NCSC-certified courses and industry to encourage innovative solutions to cyber security challenges.

Dr Virginia Franqueira, Deputy Director (Education) of the Institute of Cyber Security for Society (iCSS), said: 'We were very pleased to see three of our students selected for this amazing opportunity of creative thinking about cyber security challenges in a professional setting.'

Students came back from the event enthusiastic about their experience:

Urmila Sridharan said: 'The event was brilliantly practical and working together with some of the best students from other universities in person was a great experience. I also got the opportunity to interact with a lot of industry experts from NCSC, GCHQ, Deloitte, Plexal, Lloyds bank, etc. who shared the most efficient and effective strategies for bringing an idea to life. Overall, it was a very engaging and focused workshop.'

Keira Pascua said: 'I had a great time during the event! It was very insightful to learn new ways of developing solutions that would target cyber security issues of today. The rapid implementation of the design thinking process suits the ever changing environment of cyber security and was useful when getting ideas out to develop them further, especially within just three days.'

Daniel Thomas said: 'I liked meeting other students and hearing about their course and talking about cyber security topics with them. I have never spent a whole afternoon just talking about different cyber security topics before. It also gave me a whole new way to think about modern cyber security problems.'

Chris Ensor, Deputy Director for Cyber Growth of the NCSC, said: 'I'm delighted students have come together to take part in our Innovators Challenge, giving them an invaluable opportunity to learn from industry professionals and put their cyber studies into practice.

Creating opportunities for young people to work together and apply their skills is vital for inspiring the next generation of cyber talent to innovate and keep the UK safe online.

We thank the industry mentors for their support with this event.'

We'd love to celebrate the work of our members! If you have a story or a piece of news you'd like to share, please email us or let us know here.

iCSS Team news

New members

iCSS welcomes the following new members:

Associate Members

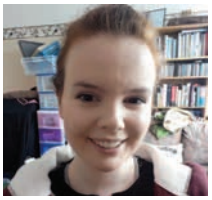
Mu Yang is Senior Lecturer at Kent Business School. She has a PhD in Computer Science from the University of Southampton, Cyber Security Centre. Her research interests include data anonymisation, adaptive privacy, trust and digital innovation. She has over 30 publications published in top international journals and conferences, including IEEE Cloud Computing, IEEE Transactions of Engineering Management, Information Technology & People, Journal of Business Research, International Journal of Product Economics, Technological Forecasting and Social Change, Annals of Tourism Research, ASE, CLOUD, AsiaCCS, SEAMS@ICSE, POST and CONCUR. She has received two best paper awards at SEAMS'2018 and TrustCom'2014 for her research in adaptive privacy and security. More information about Mu can be found at: www.kent.ac.uk/kent-business-school/people/3780/yang-mu

Maggie (Jing) Zeng is a Senior Lecturer in Entrepreneurship at the Kent Business School, University of Kent. She has a PhD from the Newcastle University. Her main research interests include emerging strategies in the digital economy, organisational (re)-configuration for digital transformation, and digital innovation. She has published in leading journals such as British Journal of Management, Strategic Organisation, Industrial and Corporate Change, Information & Management, Management and Organisation Review, International Business Review. More information about Maggie can be found at: www.kent.ac.uk/kent-business-school/people/2554/zeng-maggie-jing

ECR (Early Career Researcher) Members

Nusrah Binti Abdul Razak is a current postgraduate in Business Analytics with three years professional working experience in oil and gas engineering. Before joining the University of Kent, Nusrah was an instrument engineer in Malaysia's oil and gas operator based in Terengganu. She is a certified engineer granted by Board of Engineers Malaysia (BEM) commencing in May 2018. She supervised analytical instruments in daily operations and designed system architecture for automated monitoring. She led installation and execution of Continuous Emission Monitoring System with analytics monitoring on protected environment website in 4 gas processing plants. After much experience in engineering, she dabbled into data analytics in her line of work. She integrated all critical plant data and advanced analytical tools in an online hub in supporting safe, reliable, and efficient plant operations. Currently, she is pursuing MSc Business Analytics with the interest of machine learning implementation in enterprise resource management.

Rahime Belen Saglam received her PhD from the Middle East Technical University in 2006 and since then she has worked as a research assistant at the same university and lecturer at Computer Engineering department of Ankara Yildirim Beyazit University before joining University of Kent as a Research Associate in the Cyber Security Group in 2018. She worked in the Cyber Security Group for more than two years and her research focused on personal information disclosure, personal information sensitivity and GDPR compliance of different technologies including blockchain and chatbots. She also conducted studies on cyber security and digital literacy skills pre-university education and technology misuse to facilitate domestic abuse. She left Kent and iCSS in July, 2021 but recently rejoined as a Research Associate, working on the EPSRC-funded project PriVELT (https://privelt.ac.uk/) as a Research Associate, under supervision of Professor Shujun Li. More information about Rahime including her contact email address can be found at: www.kent.ac.uk/computing/people/3146/belen-saglam-rahime



Krysia Waldock received a BA(Hons) in German and French (first class honours) at the University of Kent in 2014, and transitioned into social sciences with an MA in Autism Studies (with distinction) at the University of Kent's Tizard Centre in 2018. Currently working on a part-time PhD in Intellectual and Developmental Disabilities in the Tizard Centre, Krysia joined the School of Computing and iCSS as a Research Assistant, working on projects related to pre-university cyber security and online safety education, co-supervised by Dr Virginia Franquiera and Professor Shujun Li. Within cyber security, Krysia's main interests are educational and social policy, and the landscape impacting cyber security education. Outside of cyber security, Krysia's research interests include critical autism studies, inclusion and belonging, participatory and qualitative methods, and intersectionality. More information about Krysia, including her contact email address, can be found at: www.kent.ac.uk/social-policy-sociology-social-research/people/1687/waldock-krysia%3E and krysiawally.blogspot.com

Haiyue Yuan received his BEng in Mobile Communication Systems and MSc in Finance at the University of Sheffield. He earned his PhD in Electronic Engineering/ Human Computer Interaction (HCI) with the research focus on user aspects of stereoscopic 3D video interaction from the Centre for Vision, Speech, and Signal Processing at the University of Surrey in 2013. Then, he continued to work as a Research Fellow at Department of Computer Science and CVSSP at the University of Surrey, on a number of inter-disciplinary projects. He joined the School of Computing and iCSS as a Research Associate working on the EPSRC-funded projects PriVELT (https://privelt.ac.uk) and MACRO (https://gow.epsrc.ukri.org/NGBOViewGrant.aspx?GrantRef=EP/V039164/1) on cybersecurity within the transportation sector, under the supervision of Professor Shujun Li. His research interests include Human Computer Interaction, Usable Security, Computational Cognitive Modeling, 3D video processing/applications, and Artificial Intelligence (AI) applications.

More information about Haiyue including his contact email address can be found at: www.hyuan.co.uk and https://research.kent.ac.uk/cyber/person/haiyue-yuan

iCSS Team news, new institutional members and new research work

Keenan Jones joins Truth and Trust Online as Website Chair

Truth and Trust Online has a mission to bring together all parties working toward improving the truthfulness and trustworthiness of online communications. TTO is an annual forum for academia, industry, non-profit organizations, and other stakeholders to discuss the problems facing (social) media platforms and technical solutions to understand and address them.

The annual Conference for Truth and Trust Online is organised as a unique collaboration between practitioners, technologists, academics and platforms, to share, discuss, and collaborate on useful technical innovations and research in the space. Keenan Jones, iCSS Early Career Researcher, joins the conference's Organising Committee for 2022 as Website Chair. Congratulations, Keenan!

EC-Council

EC-COUNCIL | ACADEMIA PARTNER

iCSS has joined the EC-Council as a new Academic Partner. The International Council of E-Commerce Consultants, also known as EC-Council, is the world's largest cyber security technical certification body. They operate in 145 countries globally and have trained and certified over 200,000 information security professionals globally that have influenced the cyber security mindset of countless organisations worldwide.

Dr Virginia Franqueira, iCSS Deputy Director, represents iCSS as the main point of contact, and will be working with EC-Council over the coming months in relation to the institute's educational activities.

Selected new publications

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

Baker-Beall, C., & **Mott, G.** (2021). "Understanding of the European Union's Perception of the Threat of Cyberterrorism: A Discursive Analysis." *Journal of Common Market Studies*, doi:10.1111/jcms.13300.

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, doi:10.1016/j.cose.2021.102545.

Kassim, S.R.B.M., **Li, S.** & **Arief, B.**, (2022). "How national CSIRTs leverage public data, OSINT and free tools in operational practices: An empirical study." *Cyber Security: A Peer-Reviewed Journal*, 5(3):251-276.

Kassim, S.R.B.M., **Li, S.** & **Arief, B.**, (2022). "Incident Response Practices Across National CSIRTs: Results from an Online Survey." Accepted to *OIC-CERT Journal of Cyber Security*.

Lu, Y. & **Li, S.** (2022) "From Data Flows to Privacy-Benefit Trade-offs: A User-Centric Semantic Model," *Security and Privacy*, published online first by John Wiley & Sons Ltd, doi:10.1002/spy2.225.

Panteli, N., **Nurse, J. R. C.**, Collins, E., & Williams, N. (2021). "Privacy and Security in the Covid-19 Work from Home Context Tensions and Challenges." Presented at the 42nd International Conference on Information Systems (ICIS 2021) as a TREO (Technology, Research, Education, and Opinion) talk, 12 December 2021.

Toros, H. (2022). "Better researchers, better people? The dangers of empathetic research on the extreme right." *Critical Studies on Terrorism*, doi:10.1080/17539153.2022.2031127.

Turner, S., **Nurse, J. R. C.**, & **Li, S.** (2021). "'It was hard to find the words': Using an Autoethnographic Diary Study to Understand the Difficulties of Smart Home Cyber Security Practices." Accepted to the 2022 ACM CHI Conference on Human Factors in Computing Systems (CHI 2022), 30 April – 5 May 2022, doi:10.1145/3491101.3503577.

Turner, S., **Pattnaik, N.**, **Nurse, J. R.C.**, **Li, S.** (2022) "'You Just Assume It Is In There, I Guess': Understanding UK Families' Application And Knowledge Of Smart Home Cyber Security." Accepted to the 25th ACM Conference On Computer-Supported Cooperative Work And Social Computing (ACM CSCW 2022), 12-16 November 2022.

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." Accepted to the 37th ACM/SIGAPP Symposium On Applied Computing (SAC 2022), 25-29 April 2022.

Public engagement work

iCSS Researchers deliver Safer Internet Day sessions at local school

On Tuesday 8 February 2022, three members of the Institute of Cyber Security for Society (iCSS), **Professor Shujun Li**, Postdoctoral Research Associate **Dr Rahime Belen Sağlam** and PhD student **Sarah Turner**, delivered five one-hour-long sessions to pupils in Years 3-8 at St Edmund's School in Canterbury. This event formed part of iCSS's outreach activities and the 2022 Safer Internet Day activities of St Edmund's School.

Three of the five sessions were delivered by Sarah Turner for Year 6-8 pupils, focusing on the topic of risks related to sharing personal data online. In those sessions, based on pupils' experience of playing video games and online platforms, Sarah guided them through a series of questions:

- How much personal data did they provide to these systems?
- Were they comfortable with that?
- Did they notice being nudged into doing things that they had not intended to do, eg, providing more personal data, spending money, and playing online with strangers?

The other two sessions were delivered to pupils in Years 3-5. They were designed to introduce pupils to the concept of misinformation, and to teach them how to rely on experts to judge whether a piece of information is trustworthy or not.The sessions also covered deepfakes as a special type of misinformation, and introduced some other different but related concepts to pupils – disinformation, 'little white lies parents tell kids' and 'lies science communicators tell kids to explain complicated scientific concepts'. Each of the sessions involved three interactive games (two physical and one computer-based), which the children played enthusiastically. Professor Shujun Li and Dr Rahime Belen Saglam each delivered one session.

Sarah said: 'It's great to be able to engage with pupils directly about topics that are clearly a huge part of their lives. Being able to have that time to pose questions to them about how the software, apps and devices they use every day capture their personal data is a helpful way to spark interest, and raise awareness of topics that are typically not given much thought.'

Dr Sağlam said: 'The internet is filled with misinformation. The session revealed to us that young kids are indeed exposed to different types of misinformation, so we urgently need to do something. We were very pleasant to see that complicated concepts like misinformation and disinformation can be introduced to young kids so that they can better understand when and from whom they can seek help.'

Professor Li said: 'At iCSS, we have been increasing our outreach activities on cyber security and online safety education. It is our belief that such education should start as early as possible, even before kids start formal education at school. This is the second time we helped St Edmund's School on Safer Internet Day, and we hope to support more schools, teachers, parents and pupils on such activities in the future.'

More information on our outreach activities can be found on our website.

Rethink insider risk and data loss

Improperly managed staff can cause an incredible amount of damage, whether due to negligence, because they've been targeted, or malice. A Ponemon report conducted on behalf of Proofpoint claimed insider threats caused as a result of compromised insiders almost doubled since 2020, when much of the world was working remotely due to the pandemic, and the average annual remediation cost for insider-led incidents caused by careless or negligent users was a staggering $6.6m. This is all complicated by the emergence of a hybrid work world, where the traditional understanding of perimeter defence no longer applies and 'bring your own device' was flipped on its head – with staff bringing their work into their homes and therefore all the devices in them.

Read more on this article by Raconteur, supported by expert contributor and iCSS Public Engagement Lead, **Dr Jason Nurse**: https://insights.raconteur.net/rethink-insider-risk-and-data-loss-prevention

Cyber security education

Kent Police delivers guest talk to our students

On Thursday 24 February 2022, Adam Shortall, Digital Forensic Analyst from the Digital Forensics Unit of Kent Police, delivered a guest talk for students of the module "Introduction to Digital Forensics". This is a new module for the current academic year 2021-22 which is optional for the *MSc Cyber Security* and *MSc Computer Science (Cyber Security)* of the School of Computing, University of Kent.

Dr Virginia Franqueira, module convenor, said: 'It was great to be able to give the opportunity for students to get insights about the daily work of a Digital Forensics (DF) laboratory, supported by Kent Police.'

Adam Shortall said: 'It was great to have an opportunity to talk to students interested in Digital Forensics. The students were very engaged and asked some great questions. We look forward to working with you again!'

Many of our students enjoyed the guest lecture, and below are some quotations from them:

- 'I really liked the transparency of what sort of actions the job role entails on a normal basis as it was nice to see the theory learned in my university course being reflected in real life such as the use of hashing. And how impactful UNIX regex functions like grep have been in cutting down evidence analysis tremendously, as hardware storage sizes grew exponentially.'
- 'I found this talk captivating, as I identified a lot to Mr. Shortall's career plan. It was very interesting to have a glimpse of a forensic analyst's life and duties, both on the positive and negative parts. He showed a real habit in public speaking, with a great balance of humour, facts, and personal opinions.'
- 'In particular, Adam Shortall was a very great speaker and had our attention throughout the session. He had anticipated our questions and incorporated them in his slides/discussions. It was also interesting to see, that despite the 'dark' nature of the work he was very upbeat and took delight in his work.'

iCSS events, talks and panel discussions

Kent Technology Fair

Organised by the University of Kent, this two-day event is designed for people who work in the space of innovation are looking for a way to see how the latest research can help their business.

The event will showcase the latest research being carried out at the University of Kent in the fields of Computing, Engineering and Mathematical Sciences. It will focus on three areas:

- Healthcare Technology
- Security
- Environmental Sustainability

For more information on the event or information on how to participate as a speaker or business, email CEMSRI@kent.ac.uk. To register as an attendee for free, please visit: www.eventbrite.co.uk/e/kent-technology-fair-tickets-274210510017

Date: 20-21 June 2022
Location: University of Kent, Canterbury, UK

24th International Conference on Information and Communications Security (ICICS 2022), September 2022

The 24th International Conference on Information and Communications Security (ICICS 2022) is the next event in a series of highly successful international conferences on information and communications security that have been running annually since 1997.

This year's event will have Best Paper and Best Student Paper awards with cash reward sponsored by Springer. It will be organised by iCSS and hosted physically on the Canterbury campus of the University of Kent.

Date: 5-8 September 2022
Location: University of Kent, Canterbury, UK

More future events

iCSS will host the following conferences on the Canterbury campus of the University of Kent in 2023.

July 2023: 17th IFIP International Symposium on Human Aspects of Information Security & Assurance (IFIP HAISA 2023)

September 2023: 17th International Conference on Network and System Security (NSS) and 9th International Symposium on Security and Privacy in Social Networks and Big Data (SocialSec 2023)

To view more details of future events, upcoming talks and seminars of iCSS, please visit our website at research.kent.ac.uk/cyber/events

Recent talks and panel discussions

"A Framework for Effective Corporate Communication after Cybersecurity Incidents." University of Nottingham. March 2022. Speaker: **Dr Jason Nurse**.

"Addressing Skills Shortage and Gap Through Higher Education." Digital Transformation and Upskilling in Europe. European Commission. March 2022. Speaker: **Dr Jason Nurse**.

"Connected Community Lunch and Learn Event." DG Cummins Inc. March 2022. Speaker: **Dr Jason Nurse**.

"Training Staff and Breeding a Cyber Risk Culture." Ransomware Resilience Summit Europe 2022. March 2022. Speaker: **Dr Jason Nurse**.

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

"Remote Working Security and Privacy." University of Kent Global Skills Award (GSA). February 2022. Speaker: **Dr Jason Nurse**.

End-to-End Encryption Virtual Roundtable. Digital Regulation Cooperation Forum (DRCF). Jointly organized by Competition and Markets Authority (CMA), Information Commissioner's Office (ICO), Office of Communications (Ofcom), and Financial Conduct Authority (FCA). January 2022. Discussant: **Professor Shujun Li**.

"Funding opportunities for ECRs (Early Career Researchers)." 2022 3rd UK Cyber Security PhD Winter School, organized by the University of Surrey, University of Bristol, University of Kent, University of Lancaster, RHUL (Royal Holloway, University of London), Northumbria University, and NCSC (National Cyber Security Centre), UK. January 2022. Speaker: **Professor Shujun Li**.

"Socio-technical Aspects of Privacy: Looking through the Lens of Time." PriCom 2021 (7th International Symposium on Privacy Computing), organized by CISPC (Chinese Information Processing Society of China). December 2021. Speaker: **Professor Shujun Li**.

"Net-Zero and Digital Technologies." Roundtable discussion. UK-China Tech Summit 2021, organized by the Chinese Students and Scholars Association (CSSA) of Imperial College London. December 2021. Discussant: **Professor Shujun Li**.

"Blockchains: Decentralised and Distributed Public Ledgers." Foundation Program 2021. Indian Institute of Technology Jammu. December 2021. Speaker: **Dr Sanjay Bhattacherjee**.

"Privacy through the Lens of Data Flows." Keynote. 2021 4th International Conference on Big Data Security and Privacy Computing, organized by CISPC (Chinese Information Processing Society of China). November 2021. Speaker: **Professor Shujun Li**.

"Cybersecurity Education in Schools." Cyber Security Education & Research Conference 2021. November 2021. Speaker: **Dr Virginia Franqueira**.

"Battlefields of the Future." Panel discussion. University of Kent student-led hybrid conference (Facebook; LinkedIn), organized by the Brussels School of International Studies (BSIS), University of Kent. November 2021. Panellist: **Professor Shujun Li**.

Calls for papers/participation

24th International Conference on Information and Communications Security (ICICS 2022)

iCSS will host the 24th International Conference on Information and Communications Security (ICICS) from September 5-8, 2022, at the Canterbury campus of the University of Kent. The following people from iCSS will be part of the Organising Committee: Professor Shujun Li as a General Co-Chair, Dr Budi Arief and Dr Sanjay Bhattacherjee as Local Arrangement Co-Chairs, Dr Özgür Kafalı and Dr Vineet Rajani as Poster/Demo Co-Chairs, and Ali Raza as the Web Chair. The call for papers is now open and the submission deadline is April 11, 2022.

The TPC will select one paper to receive the Best Paper Award, and another paper whose first co-author is a student to receive a Best Student Paper Award. Recipients of both awards will receive a certificate from the Conference and a cash award sponsored by Springer.

For more information, visit https://icics2022.cyber.kent.ac.uk

Privacy-preserving methods and applications in big data processing

A unique and innovative feature of this conference track is that the accepted papers will also be published in a special issue of *Information Processing & Management* (impact factor 6.222).

The submission system will be open from January 15, 2022 and be closed on June 15, 2022. More information about this track can be found at https://tinyurl.com/ybpudsr3. You may also find other thematic tracks relevant to your research at https://tinyurl.com/2p948ndr

Deadline: June 15, 2022

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://research.kent.ac.uk/cyber

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

DPC 131815 03/22