UniKentCyberSec

UniKentCyberSec

Institute of Cyber Security for Society (iCSS)

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

NEWSLETTER

Spring-Summer 2023

Welcome to the ninth 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 4

Page 7

Page 10

News

Kent recognised as an Academic Centre of Excellence in Cyber Security Education (Gold Award)

The University has been recognised by the National Cyber Security Centre (NCSC) as an Academic Centre of Excellence in Cyber Security Education (ACE-CSE) with a Gold Award for 2023-2029. This means that the University of Kent has met the ACE-CSE standard for Gold Award comprised of eight requirements set by the NCSC and the Department for Science, Innovation & Technology (DSIT). Kent is now one out of only 12 ACEs-CSE in the UK to obtain Gold status.

This new award was led by the University-wide and cross-disciplinary Institute of Cyber Security for Society (iCSS), one of 19 Academic Centres of Excellence in Cyber Security Research (ACEs-CSR) in the UK, jointly recognised by the NCSC and the Engineering and Physical Sciences Research Council (EPSRC, part of the UKRI – UK Research and Innovation).

The news was welcomed by the University's Vice-Chancellor, Professor Karen Cox, who said: 'My congratulations to all those who, in only a few years, have firmly placed Kent on the map for cyber security education. We are very proud to have been awarded this Gold status which is a reflection of the teaching, training and public engagement skills, research expertise and dedication of our cyber security staff.'

Dr Virginia Franqueira, Director of Kent's ACE-CSE and Deputy Director (Education) of iCSS, said: 'Our journey towards such successful outcome started three years ago when we established an action plan aligned with the ACE-CSE requirements. This recognition feels like a really amazing achievement allowing Kent to become a cyber security education and research hub in the region. It will empower us to continue pursuing our aim to equip a large range of beneficiary groups with the skills and knowledge to become cyber-specialists or cyber-aware professionals, organisations and individuals regardless of age. These groups include Kent students at all levels and subject areas, schools, industry, government bodies and wider communities.'

Professor Shujun Li, Deputy Director of Kent's ACE-CSE and Director of iCSS, explained that the activities of the ACE-CSE will draw from the wider socio-technical expertise of members of iCSS who are from the School of Computing and 15 other academic schools. He said: 'Gaining the ACE-CSE is a new milestone for iCSS and the University as a whole. It reflects our growing interests and efforts in connecting our decade-long activities in cyber security research and education and also our wider activities in other areas including but not limited to school outreach, business and public engagement and external collaboration with all sectors. We look forward to making more contributions on education-informed research and research-informed education in cyber security and other closely related topics such as online safety and media literacy.'

Chris Ensor, NCSC's Deputy Director for Cyber Growth, said: 'I am delighted we can recognise the University of Kent as an Academic Centre of Excellence in Cyber Security Education. The award is testament to the dedication of academics, support staff and senior management who have ensured that cyber security remains high on the University's agenda. We very much look forward to working with them over the coming years and encourage other universities to work towards achieving similar recognition in the future.'

iCSS hosted the 17th IFIP International Symposium on Human Aspects of Information Security & Assurance (HAISA 2023)

iCSS was delighted to host the 17th IFIP International Symposium on Human Aspects of Information Security & Assurance (HAISA 2023), which took place on 4-6 July 2023. This symposium, the seventeenth in the series, brought together leading figures from academia and industry to present and discuss the latest advances in information security from research and commercial perspectives.

The keynote, Preparing for Tomorrow's Threats: Strengthening Cyber Resilience through a People-First Approach, was given by Dr Sanjana Mehta. Dr Mehta supports (ISC)²'s global advocacy strategy while also operating as the lead advocate in advancing the organisation's public policy and thought leadership goals in the United Kingdom.

News

New research to help SMEs improve cyber security with targeted support

Dr Jason R C Nurse, Public Engagement Lead of iCSS, is involved in a new research project which will help businesses understand and improve their cyber security and streamline access to targeted support.

The Engineering & Physical Sciences Research Council (EPSRC) of the UK Research and Innovation (UKRI) has awarded almost £700,000 funding for the project to enhance understanding of small and medium-sized enterprises (SMEs)' cyber security support needs and their ability to address them. The funding was secured as a response to the EPSRC call on 'Research aligned with cybersecurity research institutes' and the new project is aligned with the Research Institute for Sociotechnical Cyber Security (RISCS).

The research aims to establish pilot Cyber Security Communities of Support (CyCOS), bringing together SMEs and advisory sources for practical help and support. The DCMS (Department for Digital, Culture, Media & Sport)'s UK Cyber Security Breaches Survey 2022 indicates that half of small and a third of micro businesses experienced breaches or attacks in the last year. Whilst they do seek external guidance in relation to cyber security, they do so via a huge range of sources and often find themselves overwhelmed with information and unable to understand the advice.

Dr Nurse will work alongside Professor Steven Furnell at the University of Nottingham, who is leading the project and Dr Maria Bada from Queen Mary University of London.

The research will investigate the support needs of small businesses, to establish their current understanding and confidence around cyber security and their awareness and perceptions of available support. The investigation will seek to determine the scenarios in which cyber security advice is sought (eg during product evaluation, at point of purchase, in response to threats and incidents) and whether it is deemed effective.

The project will also analyse support routes available to these businesses, focusing on the coverage and consistency of advice, as well as the confidence and capacity of those providing it. Research findings will be used to establish three pilot CyCOS which will include the creation of an online Support Broker, enabling the SMEs to identify support needs and contact advisory sources positioned to help them (which, as the community develops and grows in experience, may include peer support from other SMEs). The project offers upskilling opportunities for advisors and interested SMEs, via foundational cyber security certification to increase their related knowledge and capability.

Dr Nurse said: 'SMEs represent about 99.9% of the business population in the UK. Cybercriminals know this and target them with a wide range of cyber-attacks, scams and digital threats. At the same time, SMEs struggle to keep up with these threats and source appropriate cyber security support. The CyCOS project aims to provide a much-needed support platform for SMEs to significantly improve their security posture. We do this through the development of a set of novel communities and an excellent team of industry partners including the Home Office, IASME, (ISC)^2 and CIISec (Chartered Institute of Information Security).'

The research is supported by strong industry collaboration, with partners including the Home Office, (ISC)^2, IASME, CIISec, the Centre for the New Midlands and three regional Cyber Resilience Centres (CRCs).

This year, iCSS in partnership with HAISA introduced scholarships for groups and regions traditionally underrepresented at HAISA and in the fields of Cyber Security, Privacy, Cyber Psychology and related areas of research. This enabled us to provide registration to students who may not otherwise have been able to attend. We reached out to some of the scholarship recipients to hear what they had to say. Here is what some of the recipients had to say about the conference.

Oshada, from ESOFT Metro Campus in Sri Lanka, said: 'Attending HAISA 2023 has been an exceptional experience. The symposium has successfully brought together leading experts and professionals from both academia and industry, fostering insightful discussions on the latest advancements in information security. Despite attending the conference online, the virtual platform has been seamless and conducive to networking and knowledge sharing. The organisers have done an excellent job in creating an interactive environment that fosters meaningful connections and encourages active participation. I extend my heartfelt gratitude to the organisers, speakers and fellow participants for making HAISA 2023 a resounding success. This symposium has undoubtedly provided valuable insights and has inspired me to further contribute to the field of information security.'

Sarah, from University of Oxford in the UK, said: 'Attending the HAISA conference was an incredible experience, made possible by the generous scholarship from HAISA and iCSS. Their support allowed me to delve into the dynamic world of cybersecurity, gaining insights into current research and interventions while connecting with experts in field. This scholarship not only funded my attendance but also strengthened my belief in the transformative impact of organisations dedicated to nurturing talent, driving innovation and supporting early career researchers.'

iCSS also sponsored two Best Paper Awards (Best Overall Paper and Best Student Paper). Marcus Gerdin, Åke Grönlund and Ella Kolkowska won Best Overall Paper for *What goes around comes around; effects of unclear questionnaire items in information security research*. Elham Rostami and Fredrik Karlsson won Best Student Paper for *A qualitative content analysis of actionable advice in Swedish public agencies' information security policies*. We would like to congratulate all the winners on their brilliant papers.

Dr Jason R C Nurse, iCSS Public Engagement Lead and Local Organising Chair, said: 'It was an honour to host this year's HAISA event. It is one of the few conferences that priorities the human aspect of cyber security and aims to advance the field in a significant way. This year we welcomed attendees from all over the world, we engaged in critical research discussions and even had a chance to tour the beautiful Canterbury Cathedral.'

To hear more about upcoming conferences and events hosted by iCSS, subscribe to our newsletter by emailing cyber-info@kent.ac.uk.

News

iCSS hosted two co-located international conferences, NSS 2023 and SocialSec 2023

From 14 to 16 August 2023, iCSS hosted two co-located international conferences, NSS 2023 (17th International Conference on Network and System Security) and SocialSec 2023 (9th International Symposium on Security and Privacy in Social Networks and Big Data), in the Grimond Building on the main campus of the University of Kent in Canterbury, UK.

The joint event saw 35 presentations about research work of authors from 18 different countries. The presentations cover a wide range of cyber security topics such as network security, system security, AI and security, applied cryptography, blockchain, mis- and disinformation, social media analytics, privacy, malware and hardware security. Slides of all presentations can be downloaded from the conferences' website at nss-socialsec2023.cyber.kent.ac.uk/program.php

Three established cyber security researchers gave their keynote talks at the event. The first keynote talk on '*The Future of Passwords*' was delivered by Dr Julia Hesse from the IBM Research Zurich in Switzerland. The talk was chaired by the NSS 2023 PC Co-Chair Professor Atsuko Miyaji from the Osaka University and Japan Advanced Institute of Science and Technology (JAIST) in Japan. The talk's slides can be downloaded from nss-socialsec2023.cyber.kent.ac.uk/presentations/Keynote_Julia_Hesse.pdf

The second keynote talk on '*Monitoring & Mitigating Online Harms: Is Re-decentralisation the Answer to Partisanship, Hate Speech, Tracking etc?*' was given by Professor Nishanth Sastry from the University of Surrey in the UK. The talk was chaired by the SocialSec 2023 PC Co-Chair and the joint event's General Co-Chair Dr Budi Arief from iCSS. The talk's slides can be downloaded from nss-socialsec2023.cyber.kent.ac.uk/presentations/Keynote_Nishanth_Sastry.pdf

The final keynote talk on '*Trustworthy AI... for Systems Security*' was delivered by Professor Lorenzo Cavallaro from the University College London (UCL) in the UK. The talk was chaired by the NSS 2023 PC Co-Chair and the joint event's Publication Chair Professor Shujun Li from iCSS. The talk's slides can be downloaded from nss-socialsec2023.cyber.kent.ac.uk/presentations/Keynote_Lorenzo_Cavallaro.pdf

NSS 2023 and SocialSec 2023 PC Co-Chairs selected four papers to receive an award and iCSS sponsored a cash prize for each award.

The four award-winning papers and their authors are:

- **NSS 2023 Best Paper Award:** '*Modular Polynomial Multiplication Using RSA/ECC coprocessor*', authored by Aurélien Greuet, Simon Montoya and Clémence Vermeersch from the Cryptography and Security Labs of IDEMIA in France
- **SocialSec 2023 Best Paper Award:** '*People Still Care About Facts: Twitter Users Engage More with Factual Discourse than Misinformation*', authored by Luiz Giovanini, Shlok Gilda, Mirela Silva, Fabrício Ceschin,

1

2

3

News

1 First keynote talk
2 Second keynote talk
3 Third keynote talk
4 NSS 2023 Best Paper Award
5 NSS 2023 Best Student Paper Award
6 SocialSec 2023 Best Paper Award (awarded in absentia)
7 SocialSec 2023 Best Student Paper Award

4

5

6

7

Prakash Shrestha, Christopher Brant, Juliana Fernandes, Catia Silva, André Grégio and Daniela Oliveira from the University of Florida in the USA and Federal University of Paraná, Curitiba in Brazil

- **NSS 2023 Best Student Paper Award:** '*Security Analysis of Mobile Point-of-Sale Terminals*', authored by Mahshid Mehr Nezhad, Elliot Laidlaw and Feng Hao from the University of Warwick in the UK
- **SocialSec 2023 Best Student Paper Award:** '*The Impact of Synthetic Data on Membership Inference Attacks*', authored by Md Sakib Nizam Khan and Sonja Buchegger from the KTH Royal Institute of Technology in Sweden.

The awards were announced at the conference banquet in the evening of 15 August, inside the Canterbury Cathedral Lodge. Before the conference dinner, participants enjoyed a guided tour of the old city of Canterbury. Participants also had a pre-dinner drink on the lawn of the Canterbury Cathedral Lodge, which is on the beautiful ground of the Canterbury Cathedral, part of a UNESCO World Heritage site at the heart of the old city of Canterbury.

The joint event was accompanied by a stand of Springer, the scientific publisher with which the two co-located conferences' proceedings are published. At the end of the event, Springer donated 30+ displayed books to iCSS.

The Springer books, together with a copy of a recently published book co-authored by a conference participant (Dr Niyati Baliyan from the National Institute of Technology, Kurukshetra in India), were distributed to the conferences' participants towards the end of the event using random numbers generated by ChatGPT. The conferences ended with a short presentation of the next year's edition of NSS and SocialSec, to be held in the UAE.

Another social activity of the joint event was the Welcome Reception on the first day (14th August). Together with the other social activities (conference banquet, the pre-banquet drink, the guided city tour, lunch sessions and breaks), the Welcome Reception allowed participants to network more casually to learn from each other's research work and life beyond the academic world.

More about the joint event including a full list of its organisers can be found at nss-socialsec2023.cyber.kent.ac.uk. The conference proceedings can be found online at Springer's website link.springer.com/book/10.1007/978-3-031-39828-5 (NSS 2023 proceedings) and link.springer.com/book/10.1007/978-981-99-5177-2 (SocialSec 2023 proceedings).

We thank all the participants for coming to the conferences and we look forward to meeting with them again at the University of Kent and/or elsewhere in the future!

News

Cyber insurance is not fuelling the ransomware epidemic

Contrary to perceived wisdom, there is no compelling evidence that victims of ransomware with cyber insurance are much more likely to pay ransoms than those without.

That is the conclusion of a new piece of analysis titled *Cyber Insurance and the Ransomware Challenge*, conducted by the Royal United Services Institute (RUSI), the University of Kent, Oxford Brookes University and De Montfort University.

The report explores the extent to which cyber insurance might help to mitigate the threat of ransomware at a societal level.

Ransomware stands out as one of the most destructive cyberthreats that businesses encounter. This software has the potential to inflict irreparable harm to a company's systems, data and reputation, leading to severe financial consequences. According to the Cyber security breaches survey 2023, 'just over half of businesses (57%) and four in ten charities (43%) have a rule or policy to not pay ransomware payments – this is in line with last year, when this question was introduced.'

The new report's findings include:

- No compelling evidence found that the cyber insurance market is fuelling the ransomware epidemic, but nor are insurers doing enough to ensure ransom payments are paid as a genuine last resort.
- The authors do not advocate for an outright ban of ransom payments or stopping insurers from providing coverage for them. Instead, they advocate for interventions that could result in fewer victims pay ransoms or pay lower demands but without punishing victims. Ultimately, this involves creating more pathways for victims that do not result in ransom payments.
- Insurers' role as convenors of ransomware response services (eg incident response, legal advice, crisis communications, ransomware negotiations etc) gives them considerable power to reward firms that drive best practices and only guide victims towards payment as a last resort. But the lack of clearly defined negotiation protocols and the challenges around learning from incidents make it difficult to develop a sense of collective responsibility and best practices.

- Beyond ransom payments, the report finds that cyber insurance has a growing role in making organisations more resilient against ransomware and other cyber threats. The authors argue that cyber insurance is currently one of the few market-based levers for incentivising organisations to improve their cyber security and resilience.
- However, low market penetration of cyber insurance and ongoing challenges around the evidence base used for underwriting cyber risk means that it should not be treated as substitute for the kind of legislation and regulation required to improve minimum cyber security standards and resilience.

Kent's Dr Jason R C Nurse, Reader in Cyber Security and a member of the University's Institute of Cyber Security for Society (iCSS), said: 'Cyber insurance has a significant role to play in organisational cyber resilience and particularly in the response to ransomware attacks. Our research has clarified this positioning and found that cyber insurance is not – as many believe – directly fuelling the ransomware epidemic. However, there is much more that needs to be done by insurers, organisations and governments if we are to truly address the threat of ransomware to society.'

The paper forms part of a 12-month research project conducted by RUSI, the University of Kent, De Montfort University and Oxford Brookes University entitled 'Ransomware and Cyber Insurance'. It is funded by the National Cyber Security Centre (NCSC), in collaboration with the Research Institute in Sociotechnical Cyber Security. The project aims to explore the relationship between ransomware and cyber insurance.

The Kent team also included Dr Gareth Mott, Lecturer in Security and Intelligence at the School of Politics and International Relations and School of Computing cyber security PhD student Sarah Turner.

The team also recently led on the paper Between a rock and a hard(ening) place: Cyber insurance in the ransomware era, a study of the extent to which cyber insurance can mitigate the ransomware threat.

News

Success of Kent Computing Students at Oxford University Hackathon

A University of Kent team of three School of Computing students have been awarded a $5,000 grant after competing at a blockchain hackathon (see immersiveeducation.org/news/2023-Oxford-Hackathon-Winners for a news release from the hackathon's organiser). Joseph Kearney, a PhD Student at the School of Computing and an ECR (Early Career Researcher) Member of the Institute of Cyber Security for Society (iCSS) and two final-year School of Computing students Ben Martin and Gopi Gnallingam took part in the event at the University of Oxford. The challenge was to create a token dashboard (wallet) for NFTs awarded to the user for excellence in self-driven education. This challenge was based on a project currently being undertaken by the Knowledge Foundation, supported by the United Nations.

Talking about the event, the Director of the Knowledge Foundation Aaron E Walsh stated: 'The inaugural Knowledge Token hackathon, which was held at the University of Oxford from 28 to 30 March 2023, was a resounding success. Over 50 individuals from around the world registered to participate in the hackathon. The competitors represented a range of countries, including England, Switzerland, Nigeria, South Africa, Kenya, Senegal, Sri Lanka and India.

The intention of the hackathon was to involve the global software development community directly in the development of Knowledge Token by awarding professional developer grants to the winners specifically to enable them to continue working on the project after the hackathon concluded.

The Oxford winners will be further recognised during a special awards ceremony to be held in front of Einstein's doctoral certificate (PhD diploma) at the University of Zurich, Switzerland, on opening day of IMMERSIVE SWITZERLAND 2023 and the Fall 2023 Blockchain in Education Summit.'

For their submission, the University of Kent team created a fully working cryptocurrency wallet, style dashboard. This dashboard called data from the Ethereum blockchain for NFTs that were minted using smart contracts created by the team.

About the experience, Ben Martin said: 'The Oxford Blockchain Hackathon was a surreal experience that allowed me to not only exercise skills I already utilised, but also to augment them with a newer, more diverse, range of skills. These vary from both soft and hard skills such as the need for both exceptional teamwork and self-dependence. With thanks to this new experience and practice in these skill sets, it has allowed me to better distinguish myself in a professional environment.'

Gopi Gnallingam said: 'Attending the Oxford Blockchain Hackathon was an incredible experience filled with challenges that I overcame. Despite the time constraints, I persevered, enhancing my problem-solving skills and deepening my understanding of blockchain technology. Moreover, the event provided an invaluable opportunity to network with like-minded individuals, fostering innovative discussions and forging new friendships. The hackathon not only expanded my technical expertise but also introduced me to a vibrant community of talented individuals I hope to collaborate with in the future.'

All three entrants would like to thank iCSS for providing the travel funding to participate in this competition on site, Dr Sanjay Bhattacherjee for his support throughout the event and the Knowledge Foundation for organising the event and providing the grant.

Education

Kent & Medway Cyber Security Student Society (KMCS3)

KMCS3 is a student-facing society on cyber security, for all students at the University of Kent in its Canterbury and Medway campuses. In the future, we have a plan to extend the society to students at other universities based in or with a presence in Kent and/or Medway, which include the Canterbury Christ Church University (CCCU), the University of the Creative Arts (UCA) and the University of Greenwich.

KMCS3 is independent of the Kent Union, the Students' Union of the University of Kent, in order to be a more agile organisation and to allow the future extension to cover other above-mentioned universities in Kent and Medway. It is formally associated with the Institute of Cyber Security for Society (iCSS), University of Kent, as its financial sponsor and administrative supporter (eg, for overseeing the operation, providing necessary funding and resources for various activities, booking rooms, recommending speakers and co-organising events).

KMCS3 is assisted by an Advisory Group, whose members include representatives from iCSS, selected past members of the leadership team of KMCS3 and optionally some independent members (eg, University of Kent alumni who are interested in supporting student-facing cyber security activities of KMCS3). The Advisory Group is chaired by the Student Engagement Lead of iCSS, currently Dr Alexandra Covaci from the School of Engineering.

From the Welcome Week of the 2023-24 academic year, iCSS is launching a new student engagement cyber security campaign for all University of Kent students. This is a major area of activities of iCSS and the University of Kent, as a newly recognised ACE-CSE (Academic Centre of Excellence in Cyber Security Education) with a Gold award status (2023-29) by the UK Government (see blogs.kent.ac.uk/staff-student-news/2023/09/25/cyber-security-awareness-and-engagement-campaign to read a news article about this new achievement).

A major component of the campaign is a new Moodle space DP101010 'Cyber Security: Training, Awareness and Engagement for All Students', which is made open for all University of Kent students to self-enrol. This new Moodle space will be used as a 'one-stop shop' for all students to learn about cyber security and other closely related topics such as online safety, cybercrime and mis-/disinformation and to benefit from / participate in a wide range of student-facing resources / activities such as training materials and opportunities, competitions, placement and student ambassador opportunities and a diverse range of events organised by the University of Kent and other organisations. The Moodle page has already been populated with a wide range of useful information and we call more students to have a look and self-enrol.

Among many activities iCSS and KMCS3 will be co-organising, one of them is the 2023 iCSS-KMCS3 Cyber Security 'Anything' Competition. This competition is based on the 2022 iCSS Cyber Security Photography Competition, which attracted many to submit photos they took to express their real-life experience about the cyberspace. In 2023, the new competition will enlarge acceptable submissions to other categories of artefacts, including not just photos, but also drawing, short videos, essays, poems and even physical objects such as 3D printed objects and hand-crafted artefacts. A number of prizes has been selected at the end of the competition and Amazon e-vouchers has been awarded to prize winners. To learn more about the competition, please visit cyber.kent.ac.uk/survey/index.php/168859

Gold Award
in association with National Cyber Security Centre
Department for Science, Innovation & Technology
Academic Centre of Excellence in **Cyber Security Education**

Education

Two data protection officers delivered guest talks on data protection impact assessment to our students

On Tuesday 21 March 2023, two data protection officers (DPOs), Laura Pullin from the University of Kent and Adrian Leung from Equifax UK, delivered guest talks on data protection impact assessment (DPIA) for students of the module COMP8340/6660 'Information Security Management'. This module is designed for a wide range of students to gain knowledge about how real-world information security systems and processes can be managed, particularly for students studying the three cyber security degree courses of the School of Computing, University of Kent: MSc Cyber Security and MSc Computer Science (Cyber Security) and BSc Computer Science (Cyber Security).

Professor Shujun Li, the module convenor, said: 'I was very glad to see two DPOs coming to share their rich experience on DPIA and legal compliance matters about data protection with our students. The fact that they come from two very different sectors also allowed our students to see how different sectors and organisations could manage data protection matters and DPIA very differently.'

Laura Pullin, DPO of the University of Kent, said: 'I was delighted to have been asked by Professor Li to contribute to this module and to see how engaged the students were. Data protection impact assessments (DPIAs) are a fundamental part of identifying the risks associated with data processing and the technical and organisational controls required to mitigate and manage these risks. With so much personal data being processed electronically nowadays, it is inevitable that students on these degree courses will be required to contribute to DPIAs when they join the workforce and their interest and enthusiasm will no doubt be of great support to the Data Protection Officers that they work with!'

Adrian Leung, DPO of Equifax UK, said: 'It was a great pleasure to deliver a guest lecture to a group of very engaging MSc students on a very pertinent Data Protection topic about Data Protection Impact Assessments (DPIAs). DPIAs should be a precursor to any business initiative that an organisation undertakes to help the early identification of privacy related risks and to then support the incorporation of any risk reduction mechanisms into projects from the outset. Students also had the opportunity to get their 'hands dirty' and work on example DPIAs which led to some thought-provoking discussions. It is extremely encouraging to see a curriculum that promotes and embeds the concept of responsible data use.'

Many of our students enjoyed the guest talks of both DPOs and below are two quotations from them.

Cristina said, 'Meeting both Data Protection Officers Adrian Leung and Laura Pullin during our 3rd class for Information Security Management was a pleasure. Having both of them share their extensive experience in Data Protection Laws with all of us as well as their personal experience in the field has helped me personally understand better how important Data Protection is and how Data Protection works from a professional perspective. During this class, we practiced dummy DPIAs in groups with other students whilst having the support of Adrian and Laura, both helping us and giving us tips on how to fill in the ICO template to later share with the rest of the class.

Overall, this session has helped me understand from a cyber security perspective just how important DPIAs are to identify and mitigate against any data protection related risks that businesses may have and just how important it is to keep data as secure as possible following guidelines and laws to mitigate as much as possible any risk of a data leak.'

Frank said, 'The DPOs help to give ideas on how businesses handle the data transfer needs between EU and US. European Court of Justice [ECJ] ruled down two data transfer agreements between EU and US. ECJ invalidated Safe Harbour agreement in 2015 and Privacy Shield agreement in 2020 with the same reason. It is hard to understand how businesses operate and the DPOs helped to give rough ideas in how business contracts are structured to cover such data transfer needs.'

Outreach activities

iCSS hosts CyberFirst Advanced Course on Canterbury campus

From 24 to 28 July, iCSS hosts around 50 school pupils on the Canterbury campus of the University for a one-week-long CyberFirst Advanced Course, delivered by QA Ltd and Smallpeice for the CyberFirst programme of the NCSC (National Cyber Security Centre).

The CyberFirst Advanced Course is for pupils of 16 or 17 year old who are already studying computer science or who have an interest and aptitude for computer science as a subject. Through the course, the pupils can expand their knowledge, skills and behaviours that are needed to prepare them for more advanced study in computer science and cyber security.

The cyber security related skills they can learn include:

- Implementing digital forensics
- Understanding encryption technologies
- Using open source intelligence techniques
- Penetration testing

The course is completely free for participating pupils, and costs are fully covered by the NCSC for travel, accommodation and meals, and the University of Kent for rooms and computing infrastructure.

This course is the second time iCSS hosted CyberFirst courses on campus in 2023, after the Trailblazers and Adventurers courses hosted on 28th February for over 70 school pupils of Years 8 and 9 (see the news article about the February event).

As a major next step of iCSS's school outreach activities, it is helping the University of Kent to become a member of the CyberFirst programme so that iCSS can deliver CyberFirst-branded events without relying on external suppliers.

Kent & Medway Cyber Cluster

iCSS has a role in facilitating the establishment of the KMCC (Kent & Medway Cyber Cluster) to develop the local cyber security ecosystems in Kent and Medway. KMCC is recognised by the UK Cyber Cluster Collaboration (UKC3), the national body of all local cyber security clusters funded by DSIT, as the local cyber security cluster for Kent and Medway.

KMCC's main aim is to develop the local cyber security ecosystem in Kent and Medway. It will focus its activities in the following three areas:

1 Building a local community on cyber security matters in all sectors
2 Promoting innovation in cyber security to grow local cyber security capabilities
3 Facilitating cyber skills development for all from children to professionals and local citizens.

KMCC will work closely with a number of local partners and stakeholders such as local authorities and public bodies, local businesses, higher education institutions (HEIs) and schools. Nationally, KMCC will work closely with the UKC3 and other local cyber security clusters to contribute to the development of the cyber security ecosystem in the whole UK.

The leadership team at KMCC is comprised of dedicated individuals. Jason Steer serves as Director and Chief Executive Officer (CEO), while Clare Patterson takes on the roles of Director and Chief Finance Officer (CFO). Chris Solomon assumes the responsibilities of the Chief Operating Officer (COO). iCSS Director Professor Shujun Li oversees the strategic development of KMCC as the Chair of the Steering Group (SG), supported by iCSS Innovation Lead Dr Budi Arief and iCSS Honorary Member Professor Gareth Howells as members of the SG.

More members of the SG are to be appointed. This cohesive team is poised to drive KMCC's mission forward.

KMCC will work closely with iCSS of the University of Kent as a strategic partner in all three key areas of its activities.

New research projects

Countering HArms caused by Ransomware in the Internet of Things (CHARIOT)

The aim of the three-year CHARIOT project (funded by EPSRC, value to Kent £448,162, 2023-2026) is to reduce the risk and potential adverse consequences of ransomware attacks in Industrial IoT (IIoT) network deployments comprising severely constrained wireless embedded and other cyber-physical devices. Through the proposed research, we want to increase the difficulty of mounting successful ransomware attacks against IIoT and cyber-physical systems, making them less attractive targets for perpetrators.

To that effect, CHARIOT will devise, design and prototype creative, cutting-edge solutions for the detection, prevention, recovery and immunisation of/from ransomware attacks in IIoT environments.

Research outcomes and artifacts will be made available to industry professionals and the IoT security research community, to benefit from our findings and to foster collaboration towards creating more secure IoT and cyber-physical ecosystems. Artifacts will include IoT ransomware datasets, a ransomware proof of concept prototype and a toolkit for the detection, prevention and recovery of/from ransomware attacks. These engineering artifacts will be accompanied by a set of recommendations and best practices for IoT developers and industries in general.

The proposed research is aligned with the aim and objectives of the Research Institute in Trustworthy Interconnected Cyber-Physical Systems (RITICS). CHARIOT is a collaboration between the University of Kent and the University of Bristol, who is the overall coordinator of this joint project. The University of Kent is led by Dr Budi Arief (as the Principal Investigator) and Professor Julio Hernandez Castro (as the Co-Investigator). Dr Calvin Brierley is the named Research Associate on the project, while Mr Adel Elzemity's PhD research is closely affiliated to this project.

Other new research projects funded

A number of other new research projects have been funded in the period of the newsletter. Some selected ones are as follows:

Richard Guest and Gareth Howells, 'Age Estimation Testing and Evaluation: Ingenium Biometrics/University of Kent KTP,' funded by Innovate UK, value to Kent £148,495, 2024-2026

Mark Batty and Vineet Rajani, 'Safe and secure COncurrent programming for adVancEd aRchiTectures (COVERT),' funded by EPSRC, value to Kent £374,699, 2023-2026

Virginia Franqueira, Budi Arief and Julio Hernandez Castro, 'Child-protection based strategies to fight against sexual abuse and exploitation crimes (ALUNA),' funded by the European Commission (Horizon Europe), value to Kent £212,918, 2023-2025

Vineet Rajani, 'TYPDSEC: TYPe-based information Declassification and its SEcure Compilation,' funded by EPSRC, value to Kent £160,392, 2023-2025

Shujun Li, 'AISA4AI: AI-Assisted Security Analysis for Automotive Industry,' funded by Honda Research Institute Europe (HRI-EU), Germany, funding amount (all to Kent) £126,043.48, 2023-2024

Rogerio de Lemos, Marek Grzes, Virginia Franqueira and Tracee Green, 'A Pragmatic Approach for Generating Synthetic Data for Protecting Young People from Online Harm,' funded by EPSRC via the 2023 REPHRAIN Strategic Funding call, funding amount (all to Kent) £84,409, 2023-2024

Marek Grzes and Rogerio de Lemos, 'Reward shaping for network defence based on reinforcement learning,' funded by Dstl, funding amount (all to Kent) £301,229, 2023-2024

New publications

Selected new publications

Below are some selected recent research publications of our members:

Altuncu, E, **Nurse, J R C**, Bagriacik, M, Kaleba, S, **Yuan, H**, Bonheme, L & **Li, S** (2023) aedFaCT: Scientific Fact-Checking Made Easier via Semi-Automatic Discovery of Relevant Expert Opinions. In *Workshop Proceedings of ICWSM 2023*, Article Number 27, 10 pages, presented at MEDIATE 2023, AAAI. doi:10.36190/2023.27

Bada, M & **Nurse, J R C** (2023) Exploring Cybercriminal Activities, Behaviors and Profiles. In *Applied Cognitive Science and Technology*, Chapter 7, pp. 109-120, Springer. doi:10.1007/978-981-99-3966-4_7

Belen-Saglam, R, **Altuncu, E**, **Lu, Y** & **Li, S** (2023) A systematic literature review of the tension between the GDPR and public blockchain systems. *Blockchain: Research and Applications*, 4(2):100129, 23 pages, Elsevier. doi:10.1016/j.bcra.2023.100129

Bhattacherjee, S & Sarkar, P (2023) Voting Games to Model Protocol Stability and Security of Proof-of-Work Cryptocurrencies. In: Decision and Game Theory for Security. In *Proceedings of GameSec 2022*, volume 13727, pp. 297-318, Springer. doi:10.1007/978-3-031-26369-9_15

Connolly, L, Borrion, H, **Arief, B** & Kaddoura, S (2023) Applying Neutralisation Theory to Better Understand Ransomware Offenders. In *Proceedings of Euro S&P 2023 Workshop*, pp. 177-182, IEEE. doi:10.1109/EuroSPW59978.2023.00025

Knott, J, **Yuan, H**, **Boakes, M** & **Li, S** (2023) Cyber Security and Online Safety Education for Schools in the UK: Looking through the Lens of Twitter Data. In *Proceedings of SAC 2023*, pp. 1603-1606, ACM. doi:10.1145/3555776.3577805

de Moura, R L, **Franqueira, V N L** & Pessin, G (2023) Cybersecurity in Industrial Networks: Artificial Intelligence Techniques Applied to Intrusion Detection Systems. In *Proceedings of CSCE 2023*, in press, IEEE.

Mahaini, M I & **Li, S** (2023) Cyber Security Researchers on Online Social Networks: From the Lens of the UK's ACEs-CSR on Twitter. In *Proceedings of SocialSec 2023*, volume 14097, pp. 129-148, Springer. doi:10.1007/978-981-99-5177-2_8

Mohd Kassim, S R B, **Li, S** & **Arief, B** (2023) Understanding How National CSIRTs Evaluate Cyber Incident Response Tools and Data: Findings from Focus Group Discussions. *Digital Threats: Research and Practice*, 4(3):45, 24 pages, ACM. doi:10.1145/3609230

Mott, G, **Nurse, J R C** & Baker-Beall, C (2023) Preparing for future Cyber Crises: Lessons from governance of the coronavirus pandemic. *Policy Design and Practice*, 6(2):160-181, Taylor & Francis. doi:10.1080/25741292.2023.2205764

Nadeem, M S, Kurugollu, F, Saravi, S, Atlam, H F & **Franqueira, V N L** (2023) Deep labeller: automatic bounding box generation for synthetic violence detection datasets. *Multimedia Tools and Applications*, i83:10717-10734, Springer. doi:10.1007/s11042-023-15621-5

Ozturk, O S, Ekmekcioglu, E, Cetin, O, **Arief, B**, & **Hernandez-Castro, J C** (2023) New Tricks to Old Codes: Can AI Chatbots Replace Static Code Analysis Tools? In *Proceedings of EICC 2023*, pp. 13-18, ACM. doi:10.1145/3590777.3590780

Pattnaik, N, **Nurse, J R C**, **Turner, S**, **Mott, G**, MacColl, J, Huesch, P & Sullivan, J (2023) It's more than just money: The real-world harms from ransomware attacks. In *Proceedings of IFIP HAISA 2023*, volume 674, pp. 261-274, Springer. doi:10.1007/978-3-031-38530-8_21

Yuan, H, **Boakes, M**, Ma, X, Cao, D & **Li, S** (2023) Visualising Personal Data Flows: Insights from a Case Study of Booking.com. In *Proceedings of CAiSE Forum 2023*, volume 477, pp. 52-60, Springer. doi:10.1007/978-3-031-34674-3_7

Patterson, C M, **Nurse, J R C** & **Franqueira, V N L** (2023) Learning from cyber security incidents: A systematic review and future research agenda. *Computers & Security*, 132:103309, 16 pages, Elsevier. doi:10.1016/j.cose.2023.103309

Raza, A, Tran, K P, Koehl, L, & **Li, S** (2023). Proof of Swarm Based Ensemble Learning for Federated Learning Applications. In *Proceedings of SAC 2023*, pp. 152-155, ACM. doi:10.1145/3555776.3578601

Siqueira, B R, Ferrari, F C, **de Lemos, R** (2023) *Design and Evaluation of Controllers based on Microservices*. In *Proceedings of SEAMS 2023*. doi:10.1109/seams59076.2023.00013

Stevens, A, Hendrie, N, Bacon, M, Parrott, S, Monaghan, M, Williams, E, Lewer, D, Moore, A, Berlin, J, **Cunliffe, J** & Quinton, P (2023) *Evaluating police drug diversion in England: protocol for a realist evaluation*. *Health and Justice*, 11:46, 10 pages, BMC. doi:10.1186/s40352-023-00249-2

Storey, J E, **Pina, A,** & Williams, C (2023) The impact of stalking and its predictors: Characterising the needs of stalking victims. *Journal of Interpersonal Violence*, 38(21-22):11569-11594, Sage. doi:10.1177/08862605231185303

Sunde, N & **Franqueira, V N L** (2023) Adding transparency to uncertainty: An argument-based method for evaluative opinions. *Forensic Science International: Digital Investigation*, 47:301657, 10 pages, Elsevier. doi:10.1016/j.fsidi.2023.301657

Taylor-Gooby, P. Petricek, T & **Cunliffe, J** (2023) Covid19, Charitable Giving and Collectivism: a data-harvesting approach. *Journal of Social Policy*, 52(3):473-494, Cambridge University Press. doi:10.1017/S0047279421000714

Wright, D, Dalvandi, S, **Batty, M** & Dongol, B (2023) Mechanised Operational Reasoning for C11 Programs with Relaxed Dependencies. *Formal Aspects of Computing*, 35(2):10, 27 pages, ACM. doi:10.1145/3580285

Wang, Y, **Arief, B**, **Franqueira, V N L**, Coates, A G & **Ó Ciardha, C** (2023) Investigating the Availability of Child Sexual Abuse Materials in Dark Web Markets: Evidence Gathered and Lessons Learned. In *Proceedings of EICC 2023*, pp. 59-64, ACM. doi:10.1145/3590777.3590812

Wang, Y, Roscoe, S, **Arief, B**, Connolly, L, Borrion, H & Kaddoura, S (2023) The Social and Technological Incentives for Cybercriminals to Engage in Ransomware Activities. In *Proceedings of SocialSec 2023*, volume 14097, pp. 149-163, Springer. doi:10.1007/978-981-99-5177-2_9

Yang, S, **Hoque, S** & **Deravi, F** (2023) Adaptive template reconstruction for effective pattern classification. *Sensors*. 23(15):6707, 21 pages, MDPI. doi:10.3390/s23156707

iCSS Team news

iCSS welcomes the following new members:

Associate Members

Richard Pendry is a Senior Lecturer in Broadcast Journalism, at The Centre for Journalism, University of Kent. He conducts ethnographic research into how news is currently gathered in areas of conflict in the digital era. His particular focus is on how individuals work with staff journalists on the ground, including news fixers and other locally hired journalists and those who verify news remotely in order to conduct complex investigations using freely available, open-source online tools. In particular, Richard has worked with the Bellingcat investigative collective to interview individuals in-person in Ukraine whose posts were later used as evidence in the MH17 war crimes trial in the Hague. Richard is a BAFTA-winning former conflict journalist who worked at the television news agency Frontline News in Chechnya, Afghanistan and the Congo. His research page can be found at: kent.ac.uk/journalism/people/2250/pendry-richard

Emma Soutar is the Lead Trainer in the Law Society and Social Justice's Centre for Child Protection (CCP). She has over twenty years' experience in the voluntary and education sector during which time she has developed broad knowledge of issues affecting the most vulnerable in society and the frameworks in place to protect and support them. Her passion lies in sharing this knowledge through training. As part of her work at CCP, she has developed an expertise in grooming, child exploitation, online safety of young people and child protection more broadly. She uses this knowledge in the development of innovative serious game simulations built in collaboration with key safeguarding stakeholders. She delivers training packages to professionals; including her recent collaboration in developing 'May and Bay' a serious game aimed at tackling trafficking and sextortion in Thailand and Cambodia. This was funded through UNICEF's, End Violence Against Children Fund. She is also co-investigating an Economic and Social Research Council project aimed at developing specialist trauma informed training for police officers investigating child sexual exploitation. More information about Emma and her work can be found at kent.ac.uk/social-policy-sociology-social-research/people/3491/soutar-emma

Dr Aravinda Kosaraju is a Senior Lecturer in child protection at the Centre for Child Protection, University of Kent. She is also the deputy director of studies for the postgraduate programme in Advanced Child Protection. Aravinda is a qualified lawyer and social worker specialising in Criminology and prior to joining the University of Kent, Aravinda has worked for many years with national and international non-governmental organisations including Parents against Child Sexual Exploitation (PACE), Lawyer's Collective, Commonwealth Human Rights Initiative (CHRI). Aravinda's research focuses on sexual exploitation of children, trafficking and safeguarding of children broadly and draws from critical perspectives in law and criminology broadly engaging with issues of violence against women and children; criminal justice responses to sexual offending; and safeguarding children policy and practice. Her faculty research page can be found at kent.ac.uk/social-policy-sociology-social-research/people/2861/kosaraju-aravinda

Dr Will Mbioh holds the position of Senior Lecturer at Kent Law School. His scholarship spans several areas of study, primarily focusing on the intersection of European Union Law, surveillance, fundamental rights and media and telecommunications law. His particular area of interest is in social media regulation and governance, which he approaches with an interdisciplinary and socio-legal perspective. Will's research contributions are unique due to the theoretical frameworks he employs. He is notable for his application of affect theory, a critical perspective that emphasizes the role of emotions and non-conscious experiences in human behaviour and society, to his studies on social media governance. Moreover, Will also incorporates insights from feminist and postcolonial studies into his research. These perspectives provide him with nuanced understandings of power relations, identity and societal structures, which further enrich his analysis of the legal and regulatory aspects of social media. Overall, Will's interdisciplinary approach to social media regulation and governance—blending legal scholarship with affect theory and critical studies—makes him a unique voice in his field. He consistently pushes the boundaries of traditional legal scholarship and offers innovative insights into the complex dynamics of contemporary digital communication. More information about Will and her work can be found at kent.ac.uk/law/people/1258/mbioh-will

Dr Rubrick Biegon is Lecturer in International Relations in the School of Politics and International Relations at the University of Kent. He is a member of Kent's Conflict Analysis Research Centre (CARC). He teaches undergraduate and postgraduate modules on international security, terrorism and political violence and foreign policy analysis, among other subjects. His research interests focus on foreign policy and international security, particularly around the phenomenon of 'remote warfare' and its relationship to the foreign policy of the United States. Rubrick is the lead editor of Global Society, an interdisciplinary journal of international studies. His faculty research page can be found here: kent.ac.uk/politics-international-relations/people/505/biegon-rubrick

ECR Members

Danni Zhang earned her BA Degree in Business Management (Marketing) from Middlesex University in the UK and her MA Degree in International Relations from the University of York in the UK. Danni is currently pursuing a PhD in Politics & International Relations at Northeastern University London in the UK, under the supervision of Dr Xuechen Chen and Dr Pablo Calderón Martínez of the Northeastern University London (NUL), Professor Shujun Li and Dr Jason Nurse of the University of Kent. Her research focuses on digital transformation in the EU and China, with a particular focus on digital economic and cyber security. More details about her can be found at research.kent.ac.uk/cyber/person/danni-zhang

iCSS Team news

Dr Tracee Green is the Head of the Centre for Child Protection (CCP) and Senior Lecturer at the University of Kent's School of Social Policy, Sociology and Social Research (SSPSSR). She has taught on CCP's multidisciplinary postgraduate programmes, provided CPD training in child protection and led in the creation of the University of Kent's Social Worker Degree Apprenticeship. She is a registered social worker with 14 years of experience working with children and families. She is currently the PI on an ESRC funded collaboration between CCP and Kent Police aimed at creating a simulation trailing tool promoting trauma informed approaches within police work with young girls who have lived experiences of child sexual exploitation. She is also working on a REPHRAIN funded project looking to develop a synthetic database for research exploring online harms. Tracee's interests are in child protection and education-based research. Her faculty research page can be found at kent.ac.uk/social-policy-sociology-social-research/people/1970/green-tracee

Dr Lex Mauger is a Reader in Exercise Physiology and the Director of Research and Innovation in the School of Sport and Exercise Sciences. His principal interests are in restoration and optimisation of human performance and his research primarily focuses on how unpleasant sensations during exercise impair physiological function and psychological desire to exercise. He is particularly interested in how science and technology can help overcome these deleterious effects. Within the scope of iCSS, Lex has worked on projects where AI techniques have been paired with wearable technology to help restore (or make decisions on) human physical performance. Therefore, Lex's current interests in iCSS collaborative research are around how enhancing/optimising the human might improve HCI and human-in-the-loop systems and how AI and HCI technologies might be used to enhance or restore human performance. Lex regularly collaborates across disciplines including computer sciences, psychology, engineering, neuroscience and pharmacy and has worked with partners and multidisciplinary teams in industry, healthcare, academia and the public. His research encompasses young, old, healthy, clinical and elite athlete populations and has employed interventions that include non-invasive brain stimulation, virtual reality, pharmacological analgesia, experimental pain induction and environmental extremes. Using a psychophysiological approach, Lex uses a range of laboratory techniques in his experiments, that include transcranial magnetic stimulation, peripheral nerve stimulation, electromyography, online gas analysis, think aloud and post-exercise interview. Over the last 10 years his work has received significant funding from NIHR, Dstl, the World Anti-Doping Agency, Research England EIRA and Arthritis Action. Lex is based in the Division of Natural Sciences and his webpage can be found here: kent.ac.uk/sport-sciences/people/2190/mauger-lex

Dr Ben Turner is Senior Lecturer in Political Theory in the School of Politics and International Relations. His research interests lie at the intersection of political theory and the philosophy of technology. He completed his PhD in Political and Social Thought at Kent in 2018 on the work of the philosopher of technology Bernard Stieger and his first monograph on the relationship between technology and political judgment in the work of Stiegler was published in 2023 with State University of New York press. His current research projects explore the normative foundations of post-work politics, the impact of algorithmic management on workplace democracy and the political and social impact of quantum computing. In the latter project he is particularly interested in the way that technology can shape democratic and epistemic agency. Up to date information on his work can be found here: benturnerpoliticaltheory.com

Mark J Hill is Lecturer in Computational Social Science in the School of Social Policy, Sociology and Social Research. Prior to his role at Kent, he was a Postdoctoral Researcher in Digital Humanities with the Computational History Research Group at the University of Helsinki, a Political Theory Fellow in the government department at the London School of Economics and completed his DPhil in the History of Political Thought at the University of Oxford. His substantive interests grow from a background in political theory and intellectual history with a particular interest in the structural and cultural factors behind political change. His methodological interests meet at the intersection between qualitative data and quantitative methods with a current focus on quantitative text analysis and social network analysis. His current research looks at structural similarities between historical and contemporary social networks. He has been invited to speak at various international events and won awards for both his research and teaching. Mark's faculty page can be found at kent.ac.uk/social-policy-sociology-social-research/people/research-centres/3842/hill-mark-j

Nikhaela Wicks is a Lecturer in Criminology and she joined the School of Social Policy, Sociology and Social research in September 2021. Prior to this, she taught at the University of Portsmouth (2020-2021) and the University of Westminster (2016-2019). Nikhaela's interests are in policing (both formal and informal methods), race and ethnicity and nightlife and she is a keen ethnographer. Her PhD research, which was awarded a studentship from the University of Westminster, involved a year-long police ethnography with the police, door staff, licensing officers, venue manager and street pastors in the South of the UK. This research involved day and night-time participant observations, interviews and group discussions and draws critical conclusions regarding the racist and discriminatory ways nightlife is governed. Nikhaela is passionate about sharing her research findings and connecting with scholars in this field both nationally and internationally. She is a member of the International Night Studies Network and the Night Governance working group. She regularly shares her research findings at conferences in the UK and won the 'Best Presentation Award' at the 14th Annual Ethnography Symposium at the University of Portsmouth in 2019. More information about Nikhaela and her work can be seen at kent.ac.uk/social-policy-sociology-social-research/people/research-centres/3882/wicks-nikhaela

Giuseppe Maglione is a Lecturer in Criminology in the School of Social Policy, Sociology and Social Research at the University of Kent, where he is also the Director of the Restorative Justice Clinical Program. He has conducted research on the historical development, philosophical underpinnings and local delivery of restorative justice at the universities of Durham, Cambridge, Oslo and at the Max Planck Institute in Freiburg. His recent works have been published in The International Handbook of Restorative Justice, Theoretical

iCSS Team news

Criminology, Criminology & Criminal Justice, Critical Criminology and Social & Legal Studies. Additionally, he has worked extensively as a victim-offender mediator and trainer in restorative justice in Italy, Scotland and Norway. More information about Giuseppe and his work can be seen at kent.ac.uk/social-policy-sociology-social-research/people/3846/maglione-giuseppe

Joshua Sylvester received a bachelor's degree in computer science from the University of Kent in 2022. After graduating, he joined Orange Cyberdefense in applying natural language processing to identify potential threats from cyber security news feeds. Currently, he is pursuing a PhD at the University of Kent, focusing on detecting novelty and change to build more robust and resilient intrusion detection systems in the presence of adversarial drift. Currently, Joshua is collaborating on an ARCD sponsored project, named 'Reward shaping for network defence based on reinforcement learning' looking into the detection of novelty in computer networks. If you would like to learn more about Joshua's work or get in touch, please visit his LinkedIn page at linkedin.com/in/joshua-sylvester-37272b223 or send him an email at jrs71@kent.ac.uk.

Honorary Members

Sue Chadwick is the Strategic and Digital Planning Advisor at Pinsent Masons LLP. Sue's background is as a planning solicitor and academic. She has worked in the private sector and in local government and combined this with lecturing in planning law for Cambridge University and as the Director of Studies for Land Economy at Magdalene College and her doctorate is in planning law and policy. Since 2017 Sue has specialised in Digital Planning, including a year as a Research Fellow with the Open Data Institute. She is a Member of the London Data Board, Brent Council Data Ethics Board, Profusion Data Ethics Board and the Linear Infrastructure Planning Panel. She is also Chair of Business London Data Working Group and the Real Estate Foundation Data Ethics Steering Group. Sue's research interest is in the intersection of existing regulation with emerging technologies, with a particular focus on data ethics and the built environment, specifically embedded surveillant technologies, algorithmic opacity, algorithmic bias and uncertainty. She maintains the LexisNexis practice note on digital planning and has authored and co-authored articles in the Journal of Planning and Environmental Law on digital exclusion and automated decision making. More details about Sue can be found at pinsentmasons.com/people/sue-chadwick and she can be contacted via Sue.Chadwick@pinsentmasons.com

Brian Ball is Head of Faculty in Philosophy at Northeastern University London. A Senior Fellow of the Higher Education Academy, he was previously a Lecturer in Philosophy at St. Anne's and then Balliol College, Oxford. His expertise is in the theory of knowledge, the philosophy of mind and the philosophy of language. His recent work engages with artificial intelligence and information ethics. More about Brian can be found at brianandrewball.wordpress.com and nulondon.ac.uk/faculty/dr-brian-ball

Pablo Calderon Martinez is Associate Professor in Politics and International Relations and Head of Politics, International Relations, Sociology & Anthropology at Northeastern University London. Prior to joining Northeastern University London, Pablo was a Lecturer in Spanish at Aston University, a Visiting Assistant Professor in International Political Economy at the Centre for Teaching and Research in Economics (CIDE) in Mexico City and a Teaching Fellow in Spanish and European Studies at King's College London. Pablo has also held research positions at the Centre for Advanced Study in the Social Sciences at the Juan March Institute and at the Department of International Relations at ITESO University. He is member of the Mexican National System of Researchers (SNI), Level 1. Pablo's research interests include comparative regionalism in the Americas and Europe, the political implications of Free/Preferential Trade Agreements, norm diffusion as part of regional integration projects, security in Latin America and organised labour movements in Spain and Latin America. Pablo is currently working on the collaborative PhD project 'Creating, Regulating and Securing Cyberspace: from AI Governance to Digital Trade and Norm Diffusion' with colleagues at iCSS and NU London. More about him can be found at nulondon.ac.uk/faculty/pablo-calderon-martinez

Early Career Researcher Members

Temesgen Kitaw Damenu earned his MSc Degree in Information Security and IT Management from Edge Hill University in the UK and his BSc Degree in Electrical Engineering from Bahir Dar University in Ethiopia. He has managerial and technical experience on cybersecurity and worked for more than twelve years in the field. He was working in Information Network Security Agency of Ethiopia at different technical and managerial positions, including leading the Cyber Security Governance and Management Division. He was also providing cyber security course at Addis Ababa University in Ethiopia. He achieved different professional certifications including the Certified Information Security Manager (CISM) credential. Temesgen is currently pursuing a PhD in Computer Science at the University of Kent in the UK under the supervision of Prof. Shujun Li and Dr Alexandra Covachi. His research focuses on virtual reality-based cyber security awareness trainings particularly for youth and teenagers. He is eager to utilise and further develop his knowledge and skills by working and collaborating on human and managerial aspects of cyber security. You can learn more about Temesgen's work or contact him by visiting his LinkedIn profile.

Adel ElZemity earned a bachelor's degree in computer science from Nile University in Egypt. During his undergraduate studies, he spent exchange semesters at Riga Technical University in Latvia and Fayetteville State University in the USA, broadening his knowledge in computer science. His passion for machine learning led him to become a Machine Learning Engineer at CNIO in Spain, specializing in Natural Language Processing (NLP) to develop advanced solutions for various purposes. His work at CNIO significantly advanced NLP techniques in healthcare and biomedical research. Adel is currently pursuing a Ph.D. in Computer Science at the University of Kent, UK. His research focuses on using federated learning to enhance cybersecurity on the Internet of Things (IoT), particularly addressing the rising threats of ransomware attacks in IoT as part of the 'Countering HArms caused by Ransomware on the Internet of Things (CHARIOT)' project, in collaboration with his Ph.D. supervisor, Budi Arief. To learn more about Adel's work or contact him, you can visit his LinkedIn profile or email him at ae455@kent.ac.uk. Adel is open to collaboration and networking in the fields of machine learning and cybersecurity.

iCSS Team news

Alex Coleman received a bachelor's degree in computer science from the University of Kent in 2023. In his undergraduate thesis (titled 'Towards Game-theoretic Analysis on the Closing Protocol in the Lightning Network') supervised by Dr Vineet Rajani and Dr Sanjay Bhattacherjee, he undertook an exploration of formal game-theoretic analysis for the lightning network using a model-checking framework called PRISM-games. During the summer, he worked as a summer tutor at Tonbridge School, teaching children Python, Unreal Engine and Kali Linux. Currently, he is pursuing a PhD at the University of Kent, focusing on developing new type-theoretic methods that would facilitate quantitative and relational cost analysis for game-theoretic properties. Besides game-theoretic methods, he intends to look at other variations of this framework both from a theoretical and application standpoint. By incorporating a cost analysis information flow, building a type-theory framework for side-channel analysis and protection. If you would like to learn more about Alex's work or get in touch, please visit his LinkedIn page or send him an email at ac2049@kent.ac.uk

Kai Maurer is a CAA certified Flight Instructor and Flight Examiner for Autogyros. He has been in the aviation industry for two decades and is a published author of three aviation training books, specifically in the field of General Aviation and Autogyros. As a father with two daughters, his passion has long been in child safety outside of aviation when he started to work for Kent Police. Within the policing sector, Kai works specifically with missing children, the missing child exploitation team (MCET) and within child protection (CP), where cyber technology and safety play a crucial part in investigations and subsequent discoveries, especially when uncovering wider aspects of child abuse and exploitation. He graduated from the University of Kent with a master's in advanced child Protection. Kai has recently started his PhD in Sociology here at the University of Kent under the supervision of Dr Aravinda Kosaraju and Dr Tracee Green. His research focuses on Child Sexual Abuse Material (CSAM) online and child protection: A critical exploration of the notion of online harm as understood by multi-agency professionals. This exploration is focussing on how harm, experienced by children, is understood and acted upon by professionals. Technological advancements play an enormous role in understanding the dangers of children experiencing harm and he is eager to further develop his knowledge and widen his understanding of cyber security and further technological developments. You can learn more about Kai's work or contact him via his university's profile at: kent.ac.uk/social-policy-sociology-social-research/people/4981/maurer-kai

iCSS PhD student Ali Raza passed PhD viva

On Monday 28 August 2023, Ali Raza, a PhD student at the School of Computing and iCSS, passed his PhD defence successfully with minor corrections.

Ali is co-supervised by Professor Ludovic Koehl and Dr Kim Phuc Tran of ENSAIT (École nationale supérieure des arts et industries textiles), University of Lille in France and the iCSS Director Professor Shujun Li towards a cotutelle degree between the University of Lille and the University of Kent. His study was funded by a three-year joint PhD scholarship, in the form of a PhD project 'Smart Healthcare System with Federated Learning' (SHSFL).

The PhD scholarship was funded by the project I-SITE Université Lille Nord-Europe 2021 of France under the grant number I-COTKEN-20-001-TRAN-RAZA (funding amount €135,000) and by the University of Kent in the form of a full overseas fee waiver (equivalent funding amount over £60,000).

The I-SITE project is part of the grant (REF LABEX/EQUIPEX), a French State fund managed by the National Research Agency (ANR) under the frame program 'Investissements d'Avenir' and the reference number I-SITE ULNE/ANR-16-IDEX-0004 ULNE.

His thesis and the defence were examined by the following five academics from the UK and France:

- Professor Patrick Siarry, Université Paris-Est Créteil, France
- Dr Ramla Saddem, Université de Reims Champagne-Ardenne, France
- Professor Hongmei (Mary) He, University of Salford, UK
- Dr Rehmat Ullah, Cardiff Metropolitan University, UK
- Dr Peng Liu, University of Kent, UK

Ali's defence was organised following an agreement between the University of Lille and the University of Kent so that both sides' procedures were followed. It took place as a hybrid event with Dr Peng Liu and Professor Shujun Li attending remotely and all others attended in person at ENSAIT in France. Ali gave a public presentation at the beginning of the defence, which was followed by examiners' questions and his answers. The examiners praised Ali's work and presentation highly and found that only minor corrections are required to finalise his PhD thesis.

Ali's PhD thesis is titled 'Secure and Privacy-preserving Federated Learning with Explainable Artificial Intelligence for Smart Healthcare System'.

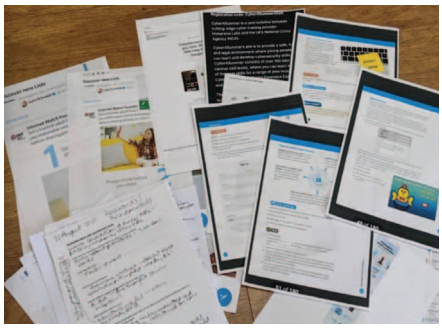
iCSS Team news

iCSS PhD student Sarah Turner passed her PhD viva

On Wednesday 2 August 2023, Sarah Turner, a PhD student at the School of Computing and iCSS, defended her PhD thesis and passed the viva subject to minor corrections.

Sarah's external examiners were Professor Lynne Coventry from the Abertay University in the UK and Dr Simon Parkin from the Technische Universiteit Delft (TU-Delft) in the Netherlands. She was supervised by Dr Jason Nurse (iCSS Public Engagement Lead) as the principal supervisor and Professor Shujun Li (iCSS Director) as the secondary supervisor. Her study was funded by the National Cyber Security Centre (NCSC, part of GCHQ) via a competitive process, leading to the project 'Approaches and Technologies to Support Home Users' Engagement with Cyber Security' (01/2020-12/2022) with a funding amount of £115,153, which covered both a stipend and some research costs.

Her thesis is entitled 'Approaches to support families' engagement with cyber security for home IoT devices.' The thesis explored the levels of awareness that UK-based families exhibited in relation to the cyber security requirements of home IoT devices use and when the awareness was found to be very low, why this was the case. The final piece of research used this information to produce a board game to facilitate learning for participant family groups around how they might improve their cyber security behaviours in relation to their home IoT use.



Seminars

iCSS hosts weekly seminars every Friday where attendees can join in person or virtually via Teams. Staff and students are all welcome to attend! The following are seminars that took place during the period covered by the newsletter.

Smart contracts and a cryptocurrency wallet: A 52 hour race

On 9 June 2023, by Joseph Kearney, Ben Martin, Gopinath Gnallingam (University of Kent)

Abstract

Across a three-day hackathon ran by Immersive Education our team from Kent looked to deploy a Dashboard for education-based cryptocurrencies. For which we have been awarded a grant by Immersive Education. In 3 days, we implemented a reactive dashboard using the Vardin framework. NFT's were deployed as the education tokens by creating new ERC-721 tokens through the use of Solidity smart contracts. Through the use of JWeb3 as well as the Etherscan API the dashboard to actively updates according to the movement of tokens on the Ethereum network. New accounts created on the dashboard will automatically create a corresponding Ethereum account and securely store the key pairs. The final goal of this is to create a dashboard that would allow students to be rewarded with cryptocurrency tokens as a result of accomplishments in academic areas. In this talk we will discuss, the brief, what we accomplished within the short time frame and what remaining work is to be done on this project. The repositories for the project can be shared upon request.

Speaker bio

Joseph is a third year PhD candidate expecting to complete in September 2023. Having graduated with an MSc in Computer Science from the University of Kent he worked as Blockchain researcher at Atlas City designing a novel blockchain system. His PhD has focused on the impact of quantum computation on blockchain technologies with research in the area of security concerns, the use of quantum devices as Proof of Work miners and is currently looking at the energy expenditure of a quantum mining device. Ben Russell Martin is a software engineer with 10 years+ experience in full stack and a passion for back-end and platform engineering. Professional experience working at the International Telecommunications Company: Sky, he has been able to accelerate his understanding into modern technology and development practices — TDD (Test Driven Development) and BDD (Behaviour Driven Development) — which has pushed his projected grade at graduation to 1st Class with Hons. Gopinath Gnallingam is a third-year computer science student at the University of Kent, with 5+ years in Software Development and a passion for blockchain technology. Gopinath's academic performance has been consistently impressive, with expectations of graduating with first-class honours.

Between a rock and a hard(ening) place: Cyber insurance in the ransomware era

On 2 June 2023, by Gareth Mott (University of Kent)

Abstract

Cyber insurance and ransomware are two of the most studied areas within security research and practice to date and their interplay continues to raise concerns in industry and government. This talk offers substantial new insights and analysis into the complex question of whether cyber insurance can help organisations in mitigating the threat of ransomware, particularly its impacts. Having conducted an interview or workshop with 96 industry professionals spanning the cyber insurance, cyber security, ransomware negotiations, policy and law enforcement sectors, we identify that ransomware has been a key cause of the 'hardening' of the cyber insurance market, which is exhibited at almost all levels of the market. Such hardening has been beneficial in raising the security standards required prior to purchase but has also created a situation where some organisations may not be able to acquire viable cyber insurance at all. In presenting the outcomes of our thematic analysis of the interview and workshop outputs, the paper provides significant new empirical evidence to support the theory that cyber insurance can act as a form of governance for improving cyber security amongst organisations. Nonetheless, the hardening market does nothing to increase the penetration of cyber insurance. Questions were also raised as to the likelihood of unintended unethical – and potentially illegal – outcomes given the professionalisation of a remediation process that has to determine the most cost-effective solution to an organisation being held ransom. We conclude that insurance, at best, can help to mitigate the ransomware threat for those that can access it, as part of a wider basket of actions that must also come from different stakeholders. The paper related to this talk can be found here: doi.org/10.1016/j.cose.2023.103162

Speaker bio

Gareth Mott is a Lecturer in Security and Intelligence in the School of Politics and International Relations at the University of Kent. Dr Mott's research specialises in the interchange between technology and software and its socio-political implications. He has conducted research on issues including cyberterrorism, extremist (mis)use of peer-to-peer technologies, efforts to mitigate ransomware and the role of 'identity' in the security politics of cyberspace. He convenes a popular research-led module entitled 'Governance and War in Cyberspace.' He is an Organisational Lead of the Institute of Cyber Security for Society and is a keen advocate of a 'big tent' approach to the interdisciplinary researching and teaching of cybersecurity.

Threat models over space and time: A case study of E2EE messaging applications

On 26 May 2023, by Partha Das Chowdhury (University of Bristol)

Abstract

Threat modelling is foundational to secure systems engineering and should be done in consideration of the context within which systems operate. On the other hand, the continuous evolution of both the technical sophistication of threats and the system attack surface is an inescapable reality.

Seminars

In this work, we explore the extent to which real-world systems engineering reflects the changing threat context. To this end we examine the desktop clients of six widely used end-to-end-encrypted mobile messaging applications to understand the extent to which they adjusted their threat model over space (when enabling clients on new platforms, such as desktop clients) and time (as new threats emerged). We experimented with short-lived adversarial access against these desktop clients and analyzed the results with respect to two popular threat elicitation frameworks, STRIDE and LINDDUN. The results demonstrate that system designers need to both recognise the threats in the evolving context within which systems operate and, more importantly, to mitigate them by rescoping trust boundaries in a manner that those within the administrative boundary cannot violate security and privacy properties. Such a nuanced understanding of trust boundary scopes and their relationship with administrative boundaries allows for better administration of shared components, including securing them with safe defaults.

Speaker bio

Dr Partha Das Chowdhury is a research associate at the National Research Centre on Privacy, Harm Reduction and Adversarial Influence Online (REPHRAIN). Partha was part of the scoping team for the £11m node projects that were funded by REPHRAIN. He is also part of the core team that is responsible for the REPHRAIN map of online harms. His research career started with investigating the extent to which anonymity and trust can coexist building on mathematical foundations. Partha has published work which uses the mathematical foundations to construct security protocols; he leads the development of a testbed operating system to test mobile application security and has interdisciplinary research contributions. He is the first to propose the adoption of the capability approaches a foundation of privacy enhancing technologies. He has presented at the New Security Paradigms Workshop (NSPW), Usenix PePR, IEEE SecDev, Security Protocols Workshop held annually at Cambridge, among others. He organised The First Capability approach workshop comprising key academics from Universities of Bristol, Cambridge, Lancaster and NCSC. The Capability Approach manifesto found a notable mention in the RISC annual report 2023. Partha has spent more than a decade in the industry implementing systems for large steel companies, city traffic management and large mining companies. He has co-authored the blockchain toolkit for the World Economic Forum.

Learning the hard way – how can we learn from cybersecurity incidents?

On 19 May 2023, by Clare Patterson (University of Kent)

Abstract

Cyber security incidents are now prevalent in many organisations. Arguably, those who can learn from security incidents and address the underlying causes will reduce the prevalence of similar ones in the future. The first part of this seminar reviews the academic research on organisational learning from cyber security incidents. This is based on a systematic review of the literature where from a total of 3,986 articles, a relevant set of 30 were analysed. The second part builds on the results of the literature review to share early insights into a recent interview study with senior security practitioners from 34 organisations. Key findings and areas for further research will be presented.

Speaker bio

Clare Patterson is a PhD research student in cyber security at the University of Kent. Her research is focused on how organisations can learn the most from the cyber security incidents they experience. She received her MSc degree in information security from Royal Holloway University of London in 1999. Clare also has over 27 years of experience in industry across IT and cyber security project management and leadership roles. Most recently as the General Manager for Information Risk Management Strategy & Assurance for Shell, leading Shell's cyber strategy and policies, cyber security investments, IT controls assurance and cyber security awareness and training. Prior to Shell she was a Director at KPMG helping a wide variety of organisations to deliver technology programmes and provide independent reviews.

A Greedy Global Framework for LLL-style lattice basis reduction algorithms

On 12 May 2023, by Jack Moyler (University of Kent)

Abstract

Post-quantum cryptography (PQC) describes systems running on classical computers which are believed to be resistant to both quantum and classical attacks. Lattice-based cryptography is arguably the most promising direction in PQC. A lattice is the set of all discrete points attained as integer linear combinations of linearly independent vectors (its basis). The security of lattice-based cryptosystems is based on the computational hardness of finding the shortest vector in a lattice, called the shortest vector problem (SVP). LLL was introduced in 1982 as the first lattice basis reduction algorithm that provides approximate SVP solutions and is still widely used in practice. This talk will begin with an overview of PQC and lattice basis reduction, before describing our new framework of LLL-style algorithms with a novel greedy global search step. We prove that our algorithms are polynomial time and the output bases are of assured quality. Experiments show that one of our algorithms yields approximate short vectors comparable to the BKZ-12 algorithm, whilst having efficiency second only to LLL. The draft of the paper is available here: eprint.iacr.org/2023/261

Speaker bio

Jack Moyler is a PhD student in the Institute of Cyber Security for Society (iCSS) at the University of Kent. He is currently researching lattice-based cryptology with a focus on algorithmic improvements for lattice basis reduction algorithms. He graduated with a degree in Mathematics from the University of York, before completing an MSc in Cryptography and Communications at Royal Holloway, University of London. His PhD work is supervised by Dr Sanjay Bhattacherjee and Professor Julio Hernandez-Castro.

Cyber Awareness Activity

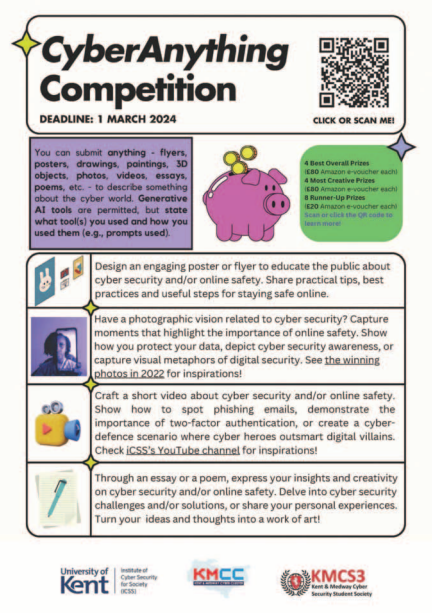
2023-24 iCSS-KMCC-KMCS3 CyberAnything Competition

Together with KMCC (Kent & Medway Cyber Cluster) and KMCS3 (Kent & Medway Cyber Security Student Society), iCSS is co-organising a CyberAnything Competition.

The competition started in late September 2023 and KMCC joined the initiative as a co-organiser and a co-sponsor in late December, 2023.

We increasingly rely upon digital, networked and smart technologies such as mobile devices and the internet to live our lives. Or we can say that we are living in the Internet of Everything (IoE), a cyber-physical world where so many hardware devices, software systems, physical things, systems and people are now interconnected. However, the cyber elements of our lives and how security, privacy and safety of such elements affect our lives are not always visible or overlooked and sometimes intentionally concealed. They are often so entrenched in our way of being that we overlook our reliance upon them until they stop functioning, eg, when a power cut, server downtime or an empty battery hits us.

This competition welcomes anything that is cyber-related in our daily lives. You can use your camera or other image-capturing device to capture a moment as a photo or a short video, or create a drawing, or prepare an infographic such as a flyer or a PowerPoint slide, or write an essay or even a poem, or make a 3D printed object or a hand-crafted artefact, etc., which can tell a story about living, learning and connecting in the cyber or cyber-physical world in the past, at present, and/or in the future. You are also welcome to try generative AI for creating your submission, but in this case please describe which generative AI tool(s) were used and how you used it/them, eg, prompt(s) you used to create the submission.



Cash prizes

Submitted artefacts will be judged anonymously by a judging panel for the following prizes in the following four categories:

1 current staff of the University of Kent
2 current students of the University of Kent
3 alumni of the University of Kent
4 other UK residents who have never been affiliated with the University of Kent.

The cash prizes will be jointly sponsored by iCSS and KMCC. More cash prizes are available for sub-competitions and more may be added for the main competition.

- **Four best overall prizes:** (one per category, £80 Amazon e-voucher per prize)
- **Four most creative prizes:** one per category, £80 Amazon e-voucher per prize
- **Eight runner-up prizes:** two per category; £20 Amazon e-voucher per prize.

Eligibility

Please note that this competition is designed for current staff/students and alumni of the University of Kent and UK residents only. If you are/were not affiliated with the University of Kent, you will be asked to confirm that you are a UK resident to be eligible for the competition. In addition, you must be 13 years old or above so that you can legally provide your own consent according to the UK data protection law (UK GDPR).

How to submit and by when

The deadline for submission is Friday 1 March 2024, 23:59. We plan to announce the prize winners in late March 2024.

To submit your entry, please go to: https://cyber.kent.ac.uk/survey/index.php/168859

↲ SCAN ME FOR MORE INFORMATION

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 134233 12/23