Newsletter

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

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

Autumn 2021

Welcome

Welcome to the fifth 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)

New research projects

Ransomware: The role of Cyber Insurance (RaCI)

A group of iCSS researchers have received funding from the UK's National Cyber Security Centre (NCSC) and the Institute for Sociotechnical Cyber Security (RISCS) for a new project named 'Ransomware: The role of Cyber Insurance' (RaCI).

The project's Kent Principal Investigator is Dr Jason Nurse, Senior Lecturer (Associate Professor) at the School of Computing, and iCSS Public Engagement Lead.

The project also has Dr Gareth Mott (Lecturer in Security and Intelligence, School of Politics and International Relations; iCSS Student Engagement Lead), as a Co-Investigator, and iCSS PhD student Sarah Turner (School of Computing) as a Research Assistant. The Kent Team will work in collaboration with the world-renowned think tank RUSI (Royal United Services Institute), and two other UK universities, De Montfort University and Oxford Brookes University.

The RaCI research project is a new research effort that seeks to understand the role that the Insurance Industry plays in the context of ransomware. The project builds on the consortium's previous research and policy reports investigating the extent to which insurance can incentivise better cyber security practices and risk management.

Dr Jason Nurse commented, 'I'm very excited to continue research into this field. Ransomware attacks are becoming worse daily and there is an urgent need for research to explore how they can be addressed and what the role of insurance is and should be. We have a fantastic opportunity to inform current practice, research and policy, as we did with our earlier work on security and insurance which was covered by the Ransomware Task Force, The AP, ComputerWeekly, ZDNet and others'.

Read the recent project here.

Dr Caoilte Ó Ciardha awarded funding to improve help-seeking by people at risk of perpetrating online exploitation and abuse

The Centre of Research and Education in Forensic Psychology at the University of Kent has been awarded a grant from End Violence's Tech Coalition Safe Online Research Fund. The project, 'Understanding and improving help-seeking by people at risk of perpetrating online child sexual exploitation and abuse', will explore interventions that aim to reach those people who are at risk of offending before they offend.

Led by Dr Caoilte Ó Ciardha, an Associate Member of iCSS, the project will explore the impact of interventions such as online messaging, that aim to deter offenders from perpetuating online child sexual abuse. Dr Ó Ciardha foresees this research having a direct impact on the tech industry by providing an evidence base for what works to divert people at risk of online sexual abuse toward obtaining professional help. The aim of the research is not just to stop people from accessing child exploitation material once, on a given platform, but also to try to link that person to resources that may prevent them from ever accessing this kind of material.

Dr Ó Ciardha says, 'If we can increase – even slightly – the number of people seeking help after seeing these types of messages, this may translate into thousands of people seeking help, and potentially avoiding offending'.

Read the full article here.
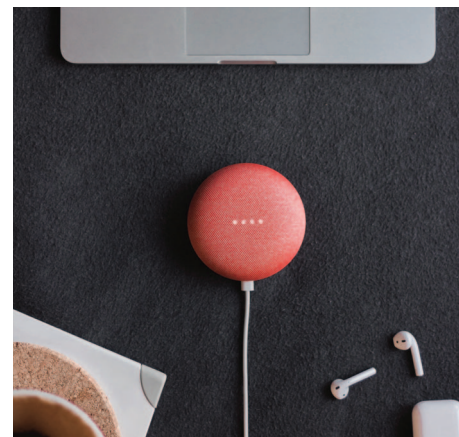
News

Cyber security courses

iCSS members help deliver many cyber security-related educational programmes, and we have already seen some incredible successes in this academic year.

- The new BSc (Hons) Computer Science (Cyber Security), introduced in September last year, had a healthy intake for the 2021-22 academic year and has become a significant pathway into Computer Science.
- The MSc Computer Science (Cyber Security), a new pathway of the MSc Computer Science conversion course, also saw its first cohort in the 2021-22 academic year. The MSc Computer Science conversion course has proven popular, attracting students who do not hold a computing degree into Computer Science. iCSS PhD student Keenan Jones, an alumnus of the MSc Computer Science course (before the Cyber Security pathway was launched), is currently pursuing a PhD degree at iCSS. Read more about Keenan's story in our Team news section.

When 'Googling it' doesn't work for cyber security

In our 2021 Summer edition of the newsletter, we shared a paper presented at HAISA 2021 by iCSS PhD student Sarah Turner, 'When Googling It Doesn't Work: The Challenge of Finding Security Advice for Smart Home Devices'. This research was subsequently presented as a poster at SOUPS 2021, as well as at the 2021 Impact Conference. It was also used as the basis for two talks given as part of the global digital infrastructure firm Equinix's Cyber Security Awareness Month program.

DDD (Digital Data Deception) Technology Watch Newsletters

Since March 2020, iCSS has been editing and publishing a 'DDD (Digital Data Deception) Technology Watch Newsletter' series. The use of DDD by adversaries calls for countermeasures that include methods for detection of such deceptive data, as well as defensive deception mechanisms that can help mislead adversaries. This newsletter series monitors recent research and innovative technology potentially useful for digital deception.

Please visit our DDD newsletter page to find out more.
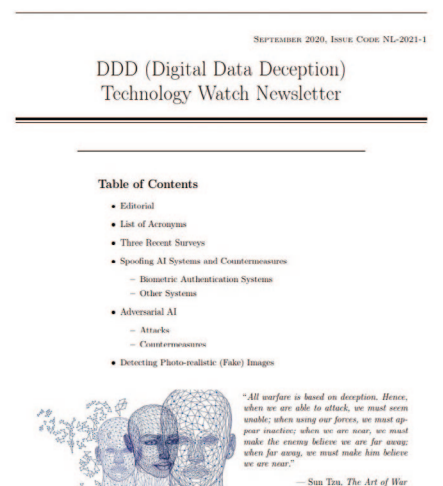
Balancing cyber security and privacy in the remote workforce

Before COVID-19, working from home was a carefully managed reality typically reserved for those who had specific jobs, were at a prescribed level of seniority or had extenuating circumstances. COVID-19, however, changed this situation considerably, with millions of new workers suddenly forced to work remotely with little training and in challenging home and personal environments.

Dr Jason Nurse and his collaborators investigated the range of new cyber security risks present in these environments. Jason discusses some of the key concerns discovered via their research in his article for the Centre for Research and Evidence on Security Threats (CREST).

Read the full research article here.

News

Cyberspace and cyber security at future battlefields

Together with Arthur Duforest from the Inter-Parliamentary Union (IPU), Professor Shujun Li (iCSS Director) and Dr Gareth Mott (iCSS Student Engagement Lead) attended a panel discussion on cyberspace and cyber security at the 'Battlefields of the Future', a student-led hybrid conference held on Saturday 6 November 2021, organised by students from the University of Kent. The video recording and some offline discussions of the panel can be found on Facebook.

More details about the conference can be found on its LinkedIn page.
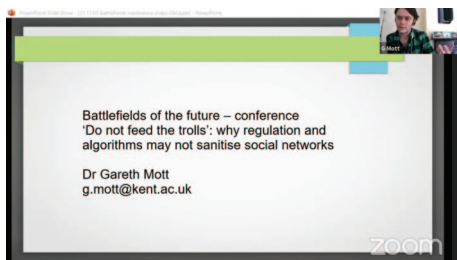

iCSS sponsors Best Paper Awards

iCSS sponsored the Best Paper Award of SecureComm 2021 as part of the 17th EAI International Conference on Security and Privacy in Communication Networks, held from 6-9 September. The virtual Conference was co-organised by iCSS and EAI, and a number of iCSS academics helped in different roles (including Professor Shujun Li as the General Co-Chair).

iCSS also sponsored the Best Paper Award for two workshops co-organised by Virginia Franqueira at the ARES 2021 conference: the 14th International Workshop on Digital Forensics (WSDF 2021) and the 5th International Workshop on Security and Forensics of IoT (IoT-SECFOR 2021).

C2C Capture the Flag 2021
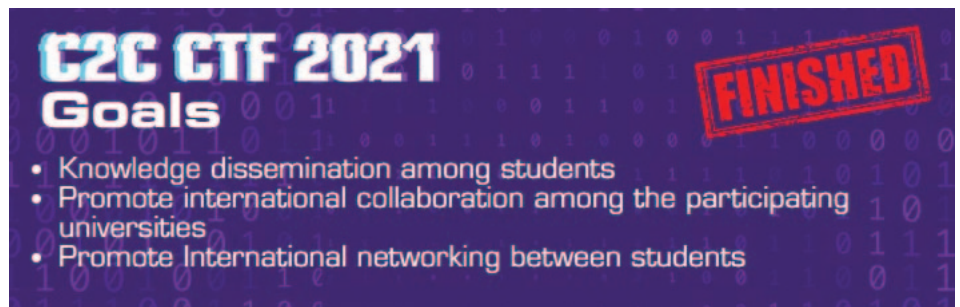
Our PhD student Matthew Boakes took part in the C2C (Country-to-Country) CTF (Capture the Flag) Student Competition in the summer. Matthew and his team-mates were thrilled to achieve the maximal score, despite an extremely challenging competition with all other teams. Their score entitled them to receive an 'honorary award', which is a reflection of their brilliant hands-on skills on solving realistic cyber security problems.

For more information on the competition topics and the score board from the event, visit www.c2c-ctf-2021.org/about

Matthew's Team (Team 6) were awarded the fourth honorary award to acknowledge their efforts. The team consisted of the following five members:
- **Matthew Boakes** – University of Kent (UK)
- Paulina Keifer – George Mason University (USA)
- Adam O'Conghaile – University of Cambridge (UK)
- Asaf Rubinfeld – Technician (ISR)
- Kahir Archarya – Macquarie University (AUZ)

Rising Star: Keenan Jones

The Rising Stars Series of SPRITE+, a UK-wide research network on TIPS (trust, identity, privacy, and security), is a platform celebrating talented individuals who are at an early stage of their research careers and prides itself on recognising the stars of the future. Within the SPRITE+ network, there are various Early Career Researchers (ECRs), such as the Institute's own Keenan Jones, who tackle important and challenging issues on subjects that matter. Using innovative methods, making new discoveries, and asking important questions are fundamental to ECR's research practice. Members are passionate about what they do and are committed to making a positive difference in their speciality subject. These inspirational individuals are recognised as the next generation of leaders and the Rising Stars of tomorrow.

Each month, one member is selected and recognised for their contribution to research in their selected field, judged predominantly on a short, self-written reference that reflects their excellence and substantiates why they are deserving of the title. Holding the title enables many benefits and opportunities, and significant, invaluable advantages. Rising Stars get to effectively showcase their talent through an established company that is widely recognised.

The named star can maximize their own benefits by using a multi-faceted approach to establish themselves amongst other talented individuals, and build upon professional relationships, networks, and future collaborators. In October, Keenan, who is co-supervised by Dr Jason Nurse and Professor Shujun Li, was named a Rising Star, and Keenan continues to impress us with his talent. Keenan's research is shaped around the use of powerful language models as a means of deceiving authorship analysis models. Keenan is interested in the capacity of powerful language models, and the vast improvement of such that give rise to opportunity to malicious threat.

To find out more, or to sign up for yourself, visit the SPRITE+ network's website.

iCSS Team news and new institutional members

## New members

iCSS welcomes the following new members:

Core Member

Vineet Rajani is Lecturer in the School of Computing at the University of Kent, where he is affiliated with the Programming Languages and Systems research group. Vineet's interest lies in type-theory and formal verification with applications to problems in resource analysis and language-based security. Before joining Kent, Vineet was a post-doctoral researcher at the Max Planck Institute for Security and Privacy, and before that he earned his PhD from the Max Planck Institute for Software Systems.

Associate Members

Giovanni Masala is Senior Lecturer in the School of Computing at the University of Kent, where he is affiliated with the Computational Intelligence research group. Giovanni's interest lies in in Computational Intelligence in Robotics. He also worked on Machine Learning with applications on medical images, biomedical data and IoT (car, wearable devices). Before joining Kent, Giovanni was a Senior Lecturer in Computer Science at Manchester Metropolitan University and before that he was Lecturer in Networks and Cloud Computing, and Leader of the Big Data research group at University of Plymouth, UK. In Cyber Security, Giovanni's interests are in preserving digital identity using multimodal biometric authentication and data security (data fragmentation) in Cloud public servers (PaaS, SaaS). Between 2008-12 he was Director/System Administrator of the CybersarHPC/GRID supercomputing cluster, security officer and GRID registration authority (RA) at the Porto Conte Research Centre (Italy).
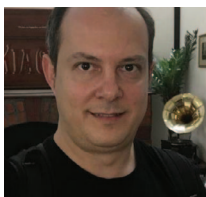
Zhen Zhu is Senior Lecturer in Big Data Analytics at Kent Business School. He obtained a PhD in Economics from the Sam M Walton College of Business at the University of Arkansas in the United States in 2013. Prior to joining Kent Business School, Zhen worked at the Networks & Urban Systems Centre, the Centre for Business Network Analysis, and the Department of Economics & International Business at the University of Greenwich.
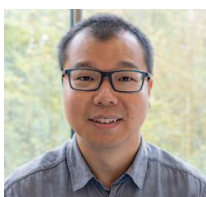
He previously held fellowships at the Stockholm China Economic Research Institute at the Stockholm School of Economics in Sweden and at the IMT School for Advanced Studies Lucca in Italy. Zhen's research fields are data science, network science and business analytics.

ECR (Early Career Researcher) Members

Ramsha Ashraf started as a new PhD student at iCSS. She is co-supervised by Dr Gareth Mott and Dr Harmonie Toros. She completed an MA in International Relations from the University of East Anglia, Norwich, in September 2021. Previously she received an MA and MPhil in English Literature from Kinnaird College for Women and Government College University, Lahore, Pakistan. She was awarded an honorary fellowship by the International Writing Program at the University of Iowa, USA 2017. She has taught courses related to English literature, Media and Arts in private and public universities in Pakistan for almost a decade and provided consultancy on Oral History for Peacebuilding in Somalia to the UN Developmental Program. Her current research aims to highlight the relationship of weak cyber security legal frameworks and their impact on transitional democracies.
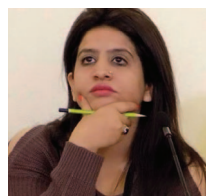
Clare Patterson started as a new PhD researcher and Graduate Teaching Assistant on 20 September 2021, supervised by Dr Jason Nurse. She joins Kent after a 25-year long career in cyber security and IT. This work experience has led her to focus her PhD research in the area of human aspects of cyber security. She completed a BSc in Management Science and Computer Science, and an MSc in Information Security at Royal Holloway, University of London in the 1990s, as well as an Executive MBA at the University of Edinburgh and ENPC part-time in the noughties.

New institutional members

Information Security Forum

ISF | Member

The University of Kent has joined the Information Security Forum (ISF) as an Academic Member. The ISF has been helping organisations develop cyber resilience for over 30 years, and its members range from Fortune 500 and Forbes 2000 listed corporations to public sector bodies and government departments. Dedicated to meeting the increasing demand for practical business-driven solutions to cyber security and risk management problems, the ISF undertakes a leading-edge research programme, providing Members with the opportunity to develop best practices and share a wealth of expertise.

Professor Shujun Li (iCSS Director) and Dr Budi Arief (iCSS Innovation Lead) are representing the University as the main points of contact. All Kent academics who are interested in being informed about ISF activities can contact them to be added to the ISF system.

National Cyber Deception Laboratory

NATIONAL CYBER DECEPTION LABORATORY

The University of Kent also joins the National Cyber Deception Lab (NCDL) as an Academic Partner. The NCDL brings together a unique range of practitioners, technology vendors, and researchers in the field of Cyber Deception. The 3 Pillars of the NCDL are:

Research – Facilitating a platform of industry and enterprise vendor solutions. Using this platform lab participants will be able to conduct research, share activities and their findings when exploring the concepts of Cyber Deception. Through these activities, the NCDL aims to be a force multiplier in the advancement of Cyber Deception understanding and capability within the UK and its partners.

Collaboration – The NCDL connects individuals and organisations, from across multiple sectors to deliver innovative and novel approaches to the development of Cyber Deception capabilities.

Guidance – The NCDL develops advice and guidance on the effective use of Cyber Deception as part of a Cyber Defence strategy. The NCDL seeks to enhance the capability of existing practitioners and support those discovering it for the first time. This knowledge will be curated and made accessible to partners across Government, industry, and academia, in order to help the UK and its partners become a harder target in cyberspace.

Representing the University of Kent within the NCDL, the iCSS will actively participate and support activities of the NCDL, from research exchanges to participation in events such as the National Cyber Deception Symposium 2021. We're looking forward to developing our relationship with the NCDL in future.

Public engagement work and new research work

Cyber attacks on schools

Ransomware attacks on schools are on the rise, according to the National Cyber Security Centre (NCSC). Since September 2020, it has published three separate alerts, warning of a spike in ransomware attacks affecting the education sector. In an article by TES, Dr Jason Nurse advises that schools take a 'holistic' security risk management approach. 'It's about adopting policies, procedures and techniques to prevent attacks,' Jason says.

Read more in Cyberattacks on schools: the facts.

St Edmund's School Sixth Form Expo

iCSS participated as an exhibitor of the first Sixth Form Expo at St Edmund's School Canterbury that took place on 15 November 7-9pm.

The institute was represented by two PhD students Matthew Boakes and Calvin Brierley. They talked to pupils and parents about careers in cyber security, course options available at the School of Computing to fulfil cyber security careers, and iCSS activities especially related to pre-university cyber security education and awareness.

New publications

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

Filiz, Burak; **Arief, Budi**; Cetin, Orcun; **Hernandez-Castro, Julio** (2021) 'On the Effectiveness of Ransomware Decryption Tools,' *Computers & Security*, Volume 111, Article Number 102469, 12 pages. DOI: 10.1016/j.cose.2021.102469.

Brierley, Calvin; **Arief, Budi**; **Barnes, David**; **Hernandez-Castro, Julio** (2021) 'Industrialising Blackmail: Privacy Invasion Based IoT Ransomware,' accepted to the 26th Nordic Conference (NordSec 2021), to be held on 29-30 November 2021. To be published by Springer.

Moura, Ralf Luis de; Pessin, Gustavo; **Franqueira, Virginia N L** (2021) 'Towards Safer Industrial Serial Networks: An Expert System Framework for Anomaly Detection,' accepted to the 33rd IEEE International Conference on Tools with Artificial Intelligence (ICTAI 2021), held on 1-3 November 2021 as a virtual event. To be published by IEEE.

Ioannou, Athina; Tussyadiah, Iis; Miller, Graham; **Li, Shujun**; Weick, Mario (2021) 'Privacy nudges for disclosure of personal information: A systematic literature review and meta-analysis', *PLoS ONE*, Volume 16, Number 8, Article Number e0256822, 29 pages, PLoS. DOI: 10.1371/journal.pone.0256822.

Mahaini, Mohamad I; **Li, Shujun** (2021) 'Detecting Cyber Security Related Twitter Accounts and Different Sub-Groups: A Multi-Classifier Approach,' accepted to the 2nd International Symposium on Foundations of Open Source Intelligence and Security Informatics (FOSINT-SI 2021), co-located with the 13th IEEE/ACM International Conference on Advances in Social Network Analysis and Mining (ASONAM 2021). To be published by ACM. DOI: 10.1145/3487351.3492716.

Mott, Gareth; Baker-Beall, Christopher (2021) 'The new EU counter-terrorism Agenda: pre-emptive security through the anticipation of terrorist events,' *Global Affairs*, in press (already published online). DOI: 10.1080/23340460.2021.1995461.

Nurse, Jason R C; Vargas, Francielle; Hassan, Naeemul; Wang, Dakuo; Andriotis, Panagiotis; Ghenai, Amira; Jaidka, Kokil; Mustafaraj, Eni; Joseph, Kenneth; Foucault Welles, Brooke (2021) 'Towards A Diverse, Inclusive, Accessible and Equitable AAAI International Conference on Web and Social Media (ICWSM),' in *Proceedings of the 15th AAAI International Conference on Web & Social Media* (ICWSM 2021). DOI: 10.36190/2021.00.

Raza, Ali; Tran, Kim Phuc; Koehl, Ludovic; **Li, Shujun** (2021) 'Designing ECG Monitoring Healthcare System with Federated Transfer Learning and Explainable AI,' accepted to *Knowledge-Based Systems*, to be published by Elsevier. Preprint available at https://arxiv.org/abs/2105.12497.

Wang, Yichao; **Arief, Budi**; **Hernandez-Castro, Julio**; 'Toad in the Hole or Mapo Tofu? Comparative Analysis of English and Chinese Darknet Markets,' accepted to the 15th Annual APWG Symposium on Electronic Crime Research (eCrime 2021), to be held on 1-3 December 2021 as a virtual event.

Yilmaz, Yagiz; Cetin, Orcun; **Arief, Budi**; **Hernandez-Castro, Julio** (2021) 'Investigating the impact of ransomware splash screens,' *Journal of Information Security and Applications*, Volume 61, Article Number 102934, 13 pages, Elsevier. DOI: 10.1016/j.jisa.2021.102934.

Conferences and events

3rd UK Cyber Security PhD Winter School, January 2022

The 2022 3rd UK Cyber Security PhD Winter School, sponsored by the NCSC and co-organised by the UK Cyber Security PhD Network, will take place on 10-12 January 2022. A number of iCSS members are involved in organising or coordinating local participation of the event:

- Professor Shujun Li is on the Winter School's Organising Committee.
- Two iCSS PhD students and Kent reps to the UK Cyber Security PhD Network, Nandita Pattnaik and Matthew Boakes, as well as Dr Gareth Mott, will help coordinate participation of Kent PhD students and staff in the Winter School.

Register for free at: www.eventbrite.co.uk/e/2022-uk-cyber-security-phd-winter-school-tickets-198863274407

International Studies Association (ISA) Conference, March-April 2022

Dr Harmonie Toros (iCSS Deputy Director) and Dr Gareth Mott (iCSS Student Engagement Lead) will be attending the 2022 International Studies Association Conference in March and April 2022, hosted in Nashville, TN, USA. iCSS is a sponsor of the event and will be hosting a booth in the conference hall to promote iCSS's activities. The ISA conference is one of the largest conferences in the field of Political Science and presents a great opportunity to create impactful connections and raise awareness of iCSS. Harmonie and Gareth will also be presenting separate research papers at the conference.

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) & 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 https://research.kent.ac.uk/cyber/events

Recent events and workshops

'Can lessons be learnt from the governance of the coronavirus pandemic to help preparations for future cyber crises?' Hague Program for Cyber Norms conference. Speakers: **Dr Gareth Mott** and **Dr Jason Nurse**. November 2021.

'Cyber Security and the Internet of Things', Invited Lecture at Cranfield University's Critical Networks and Cyber-Physical Systems course. Speaker: **Dr Jason Nurse**. November 2021.

'Personal Threat Modelling'. NCSC's EmPower Cyber Week for 11–13-year-olds. Speaker: **Sarah Turner**. November 2021.

'Using Autoethnography as a Lightweight Research Method'. Research Methods e-Festival, hosted by the National Centre for Research Methods and the University of Manchester. Speaker: **Sarah Turner**. October 2021.

'Understanding cyber security skills development in pre-university education'. CIISec LIVE, 2021, September 2021, and Cyber Secure Event, October 2021. Speaker: **Dr Virginia Franqueira**.

'Privacy through the Lens of Data Flows'. Webinaire Cybersécurité et véhicules connectés, organised by GIS CybCOM. Speaker: **Professor Shujun Li**. September 2021.

'From AI for Security to Secure, Privacy-Friendly And 'Good' AI'. AI Summit London UK. Speaker: **Professor Shujun Li**. September 2021.

'The Evolving nature of Cyber threats'. Cybersecurity Capacity Centre for Southern Africa (C3SA). Speaker: **Dr Jason Nurse**. September 2021.

'Does Cyber Insurance Help or Hinder Online Crime?' Sophos Security SOS Week. Speaker: **Dr Jason Nurse**. September 2021.

'Understanding cyber security skills development in pre-university education'. CIISec LIVE 2021. Speaker: **Dr Virginia Franqueira**. September 2021.

Keynote: 'Privacy in the Cyber-Physical World: Challenges and Solutions'. KSA (Kingdom of Saudi Arabia) Hybrid Cloud and Cybersecurity Summit 2021. Speaker: **Professor Shujun Li**. August 2021.

'Is Cyber Insurance Fuelling the Ransomware Crisis?' #RansomAware Movement. Speaker: **Dr Jason Nurse**. August 2021.

'A Framework for Effective Corporate Communication after Cybersecurity Incidents'. UK Security and Privacy Seminar (UK-SPS) Series. Speaker: **Dr Jason Nurse**. August 2021.

'Cybersecurity incentives and the role of cyber insurance'. Cybersecurity Investment Supporting SMEs. Speaker: **Dr Jason Nurse**. August 2021.

'Digital forensic research: the challenges of the next 10 years'. DFRWS EU 2021 and DFRWS USA 2021 conferences. Speaker: **Dr Virginia Franqueira**.

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, and Ali Raza as the Web Chair. The call for papers is now open and the submission deadline is March 21, 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

ACM Digital Threats: Research and Practice (DTRAP) special issue on ransomware

ACM DTRAP is soliciting papers on all areas related to ransomware, in order to get a better understanding of ransomware from a variety of lenses and disciplines, from psychological and criminological perspectives to economic and legal approaches. The ultimate purpose of this combined effort is to find mechanisms to fight ransomware crime more effectively. The special issue is led by iCSS Innovation Lead Dr Budi Arief, and iCSS Core Member Professor Julio Hernandez-Castro is a co-guest-editor.

For more information on submissions, visit
https://dl.acm.org/pb-assets/static_journal_pages/dtrap/pdf/CFP_Ransomware-1631043326117.pdf

Call for participation: Survey on 'Cyber security practices at schools'

SWGfL, iCSS and Bitdefender are jointly organising a survey on cyber security practices and education at schools in the UK. It aims to understand the priority and extent of protection and educational experiences given to cyber and information security personnel. The survey should take 10-15 mins to complete. The first 150 successfully completed surveys will each receive five complimentary licences for Bitdefender Total Security software for home use as a thank you for completing this survey.

Please circulate this survey to any educators or schools who may find it of interest. Link to the survey: http://tiny.cc/CSSurvey

---

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

DPC 131465 11/21