News
Page 2

New research projects
Page 4

Education and outreach
Page 6

Newsletter

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

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

Spring 2021

Welcome

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

To access this newsletter online and view associated web links, please scan the QR code at the top of the page.

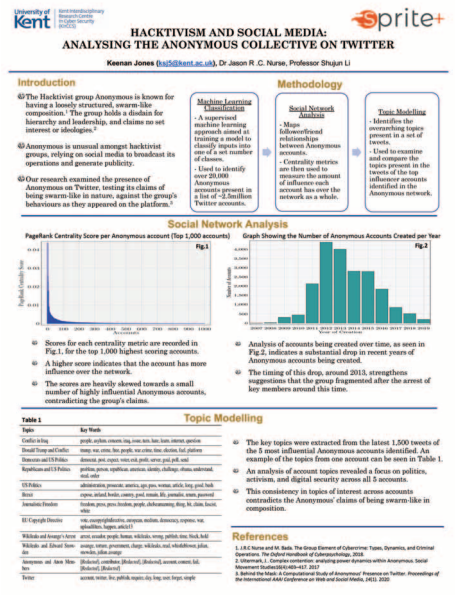
Institute of Cyber Security for Society (iCSS)

News

Kent's Cyber Institute is re-named

In January 2021, the University of Kent announced the establishment of our new interdisciplinary cyber security institute, which was set up to further extend the cyber security research of KirCCS (Kent Interdisciplinary Research Centre in Cyber Security) and coordinate University-wide educational activities around cyber security. The Institute was tentatively named Institute of Advanced Studies in Cyber Security and Conflict (SoCyETAL) but has since been re-named to Institute of Cyber Security for Society (iCSS). We hope you like the shorter and simplified name and acronym.

Keenan Jones highly commended for research poster



PhD student Keenan Jones has been highly commended for his poster on 'Hacktivism and Social Media: Analysing the Anonymous Collective on Twitter' for the SPRITE+ Showcase: Research Snapshot poster competition.

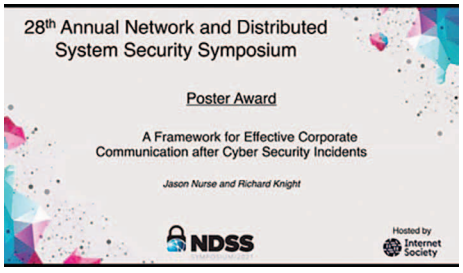
The research poster, based on the paper 'Behind the Mask: A Computational Study of Anonymous' Presence on Twitter', co-authored by Keenan and his supervisors Dr Jason Nurse and Professor Shujun Li, also received a best paper Honourable Mention award at the 14th International AAAI Conference on Web and Social Media (ICWSM 2020).

Best Poster Award for Dr Jason Nurse

Dr Jason Nurse has won an award at this year's Network and Distributed System Security Symposium (NDSS 2021) for his poster on 'A Framework for Effective Corporate Communications after Cyber Security Incidents'.

NDSS is one of the 'top four' conferences in the cyber security research community, normally held physically in San Diego, CA, USA (this year as a virtual event).

The research poster is based on Jason's co-authored paper with the same name, which comprises a practical framework to help businesses, cyber security teams and corporate communications professionals respond more effectively to cyber security attacks.



Dr Jason Nurse said: 'Really excited to have won this NDSS award. It's great to see my research into the more socio-technical problems of security being appreciated at such a well-regarded international conference'.

Professor David Chadwick interviewed by CNBC on Covid passports

Professor David Chadwick, Managing Director and CEO of Verifiable Credentials, iCSS Honorary Member and Emeritus Professor of Information Systems Security at the School of Computing, has been interviewed by CNBC on his company's trialling of Covid-19 vaccination passports.

Verifiable Credentials is a cyber security company which aims to provide everyone with free to use verifiable credentials apps. The company has been testing Covid-19 certificate apps with the NHS in East Kent and believes that this could be rolled out across the rest of the UK.

David explains in the interview how Verifiable Credentials sees the passport working across different countries with varying privacy laws:

'There are many different certificate formats to adopt and cryptographies that can be used, and we don't have technical inter-working at the moment. Assuming we could address those technical issues and get interworking, what we've done with our particular solution is to make it the most privacy protecting as possible, so that it complies with GDPR and allows the absolute minimum of data to be revealed. In fact, it's possible for no data to be revealed, the passport will just let you know that "I have been vaccinated"'. The CNBC interview is available to watch online

You can also see some of David's talks on Verifiable Credentials and Covid 19 Certificates on the iCSS YouTube Channel: www.youtube.com/channel/UCt8ucQNd57cM4oGlJ4TzUqg

1 Dr Gareth Mott

SOPHOS Naked Security article on Cyber Security risks of home-working

As so many more of us are working at home on a regular basis, Dr Jason Nurse warns of the risks of posting online photos of home-working set-ups and oversharing, in an article for SOPHOS's naked security.

The trend, which has seen the use of hashtags such as #WorkingFromHome and #HomeOffice, has made the job of fraudsters, scammers and cybercriminals substantially easier, as people inadvertently share information about themselves, their families and location.

The article, 'I see you: your home-working photos reveal more than you think!' has also been referenced in a number of other news outlets, including Threatpost and Techradar.pro and News18.com.

'Kentish Cyber' take part in UK Cyber 9/12 Strategy Challenge

A team of Kent students, which includes members of iCSS, took part in the 4th Annual UK Cyber 9/12 Strategy Challenge over two days on 16-17 February 2021.

The Cyber 9/12 Strategy Challenge is an annual cyber policy and strategy competition open to university students from across the globe. In this strategy challenge, competitors take on the role of senior advisors to government and industry, in facing a complex escalating cyber-attack.

The team. 'Kentish Cyber' coached by Dr Gareth Mott, is made up of the following members: Keenan Jones, Nandita Pattnaik (School of Computing), Hala Zein (Kent Law School) and Ben Treacy (School of Politics and International Relations).

Computing PhD student and iCSS member Nandita Pattnaik gives us a rundown of the event:

'We were assigned a realistic scenario, very apt to the current situation relating to a possible zero-day ransomware attack on hospitals, identified within a broader context of Covid vaccine misinformation activity affecting the general public. We familiarised ourselves with the brief and an array of wider interdisciplinary open-source research, to relate it to the current scenario. We then undertook a situational assessment, considering the potential impact, risk and implications and came out with three potential recommendation for the cabinet office.

1

Many afternoons and evenings were spent deciding on the decision document, briefing document and the main presentation. Our team then presented the recommendations on the competition day, to a panel of six judges consisting of senior cyber experts.

Although we didn't get selected for the finals, the whole process was an invaluable learning experience. It was hard work, but what I enjoyed most was that it gave us a flavour of working in a real-life challenge. The event was great to network with many industry professionals. Apart from hosting the main competition, Cyber 9/12 also invited many prominent professionals in the cybersecurity field both from the private and the public sector to share their life experiences, which were very inspiring and useful'.

Dr Gareth Mott said: 'This is a really exciting time to learn about cyber security and become involved, and the dilemmas presented by computing technologies cannot be put back in a box; they're here to stay. The contemporary cyber security environment is increasingly interdisciplinary, and the Cyber 9/12 Competition reflects this. Thank you so much, to Kentish Cyber, for your hard work and dedication in representing the University of Kent and iCSS for the first time at the UK Cyber 9/12 Strategy Challenge'.

Best Paper Award for Professor Shujun Li and Dr Islam at HICSS 2021

Professor Shujun Li and former Computing Research Associate Dr Tasmina Islam have won a Best Paper Award at HICSS 2021 (54th Hawaii International Conference on System Sciences), for their joint work with five other researchers from the University College London (UCL), TRL Ltd and the University of Surrey.

The research paper, titled 'Privacy in Transport? Exploring Perceptions of Location Privacy Through User Segmentation' (open access), was part of the recently completed EPSRC-funded research project ACCEPT (Addressing Cybersecurity and Cybercrime via a co-Evolutionary aPproach to reducing human-relaTed risks), led by Professor Shujun Li.

New research projects

New project to research safe and secure software systems

Dr Budi Arief is collaborating with PhD student Tom Seed and Emeritus Professor Andy King on a new project titled 'Symbolic Computation for Mainstream Verification'.

The project is funded by the National Cyber Security Centre (NCSC), via the Research Institute in Verified Trustworthy Software Systems (VeTSS) – a UK Academic Research Institute in Cyber Security at Imperial College London, funded by the Engineering and Physical Sciences Research Council (EPSRC). VeTSS supports world-class academics and industrialists to develop novel techniques for keeping software systems safe and stable.

The project will run for one year from April 2021 to March 2022 and aims to develop advanced SMT (Satisfiability Modulo Theory) solvers, which are used to verify and test the vulnerability of software.

Dr Budi Arief said: 'As software continues to play a bigger role in our society, it is imperative to ensure its security and trustworthiness, hence the interest in verification. We are really pleased we have been given funding for this project. It is a particularly significant achievement since the acceptance rate for VeTSS has been around 25% in the previous four years of calls. Furthermore, the project demonstrates the continued collaboration between the Cyber Security and Programming Languages and Systems research groups at Kent'.

New project mapping PhD theses in the UK to CyBOK

Dr Virginia Franqueira, Dr Jason Nurse and Professor Shujun Li from the School of Computing have been awarded funding for a new project that will map cyber security PhD theses of UK HEIs (higher education institutions) to the CyBOK (Cyber Security Body of Knowledge).

The work is funded by the NCSC (National Cyber Security Centre, part of GCHQ) through a competitive open call from the CyBOK project led by the University of Bristol. The aim of the CyBOK project is to create a body of knowledge for cyber security education and professional training.

This new project will map research topics of PhD theses, published by UK HEIs in the past five years, to the CyBOK knowledge areas and sub-topics. Findings from the project will provide insights about how PhD research in the UK relates to the CyBOK, including how such relation has evolved over time. Such insights can help inform future cyber security capacity building activities of UK HEIs.

Research to investigate prevalence of technology facilitated domestic abuse

iCSS members have formed a multidisciplinary research team to carry out an investigation examining the role of technology in intimate partner domestic abuse.

The research, funded by the Home Office Domestic Abuse Perpetrators fund, will explore the prevalence of Technology Facilitated Domestic Abuse (TFDA) in the UK and the particular types of technology used to perpetrate TFDA.

The project will be led by psychologists Dr Afroditi Pina and Dr Jennifer Storey from the School of Psychology's Centre of Research and Education in Forensic Psychology [CORE-FP], alongside Dr Virginia Franqueira (School of Computing) and Dr Marian Duggan (School of Social Policy, Sociology and Social Research), all members of iCSS with extensive experience in domestic abuse, online abuse and cyber security. Research will be carried out in partnership with The Cyber Helpline, the only UK not-for-profit helpline directly supporting victims of cyber-crime. By utilising case data and conducting in depth interviews with front-line responders of The Cyber Helpline, the researchers will look to identify the specific technologies used by perpetrators and establish the requirements for high quality victim assistance from a cyber security perspective.

The findings of this research will produce necessary data for government, law enforcement, practitioners, front-line responders and stakeholders to inform on appropriate interventions with perpetrators and victims of TFDA, as well as the most suitable technical support.

Dr Afroditi Pina said: 'Domestic abuse cases have risen during the Covid-19 pandemic, with many victims unable to escape from abusive partners at home. This research project is timely and necessary to identify the evidence base on intimate partner domestic abuse and a newly established constellation of methods of TFDA perpetration'.

In another project funded by the Home Office Domestic Abuse Perpetrators fund, Dr Jason Nurse will collaborate with researchers from the Institute of Criminal Justice Studies at the University of Portsmouth to study the relationship between technology and abuse, and how these types of crimes often fall under the framework of the Computer Misuse Act (CMA).

The project will explore how domestic abusers are using computers and other digital technology to monitor, threaten and humiliate their victims and will help guide future police investigations into domestic abuse. New technologies including smart tech, internet connected devices and apps are also within scope of the research.

Dr Nurse said: 'There is clearly a pressing need to investigate the technologies used by perpetrators for domestic abuse, how they are sourced and applied, and to what extent are smart and internet-connected devices exacerbating the problem. Through the project, we hope to strengthen the evidence base in this domain, and further help inform what actions may work in addressing perpetrator behaviours'.

New commercialisation project on blockchain analysis

Dr Sanjay Bhattacherjee from the School of Computing has secured funding from Innovate UK as part of their Cyber Security Academic Startup Accelerator Programme (CyberASAP). CyberASAP is a competition for cyber security researchers to realise the commercialisation potential of their innovations.

The funding received is for a project entitled 'ViBS: Voting in Blockchain Systems'. The project aims to produce a new web-based service to dynamically measure the security and protocol stability of permissionless blockchains – primarily cryptocurrencies like Bitcoin and Ethereum.

These two aspects are at the foundation of trust on such systems and are both determined by the votes of the participants (miners) through every newly created block. The innovation lies in modeling this voting process using techniques from cooperative game theory. Professor Palash Sarkar from the Indian Statistical Institute (ISI), also an Honorary Member of iCSS, is a co-inventor of the system. Jack Moyler, our PhD student in the School of Computing and also a member of iCSS, will be contributing to the project. The project will also be advised by industrial specialists in the UK and the US.

The web-based service should be of particular interest to investors and traders seeking to understand and monitor the trustworthiness and associated risks of cryptocurrencies. The system developed will also appeal to all existing businesses involved in blockchain analytics.

The initial phase of the project will last up to four months and will be used to determine the value of the perceived product and its potential for commercialisation.

New project to investigate cyber-enabled wildlife trafficking

iCSS members Dr David Roberts from the School of Anthropology and Conservation and Professor Julio Hernandez-Castro from the School of Computing are to work on a new project entitled 'Dismantling wildlife trafficking cybercrime networks in Southeast Asia'. The 2.5 year project is funded by the Illegal Wildlife Trade Challenge Fund (Defra) and seeks to develop and test an enhanced set of tools to identify, monitor and report online Illegal Wildlife Trafficking (IWT), as well as to train government, civil society and private sector partners in these tools. For more information about the project, see https://iwt.challengefund.org.uk/project/XXIWT079

Education and outreach

Kent responds to demand for cyber security and AI expertise

Kent has responded to the increasing demand for cyber security and Artificial Intelligence (AI) expertise and skills with the launch of two new MSc Computer Science conversion courses designed for graduates from any discipline.

With AI and cyber experts becoming increasingly sought after by companies and organisations in sectors such as healthcare, finance and transport, the MSc Computer Science (Cyber Security) course will provide postgraduate students with the opportunity to establish a foundation in cyber security from technical and multidisciplinary perspectives. It will also enable them to acquire the technical skills and knowledge necessary to identify and solve complex security and privacy problems, including, encryption, authentication, information security management and cyber security risk.

Both programmes are available with an optional industrial placement of between eight and 50 weeks. The industrial placement provides graduates with opportunities to work in real-world, technical and business roles, enhancing their study experiences and having a dramatic impact on their options after graduation.

Dr Rogério de Lemos, iCSS member and Director of Graduate Studies (Taught) at the School of Computing, said, 'There are often misconceptions that computer science specialisms such as cyber security and artificial intelligence would only be higher education routes for those who already have a background or undergraduate degree in computing. This is not the case, and we look forward to welcoming graduates from various disciplines to develop their studies in the world of computing'.

KeCSEC and Law School join forces for interdisciplinary workshop

On Wednesday 17 February 2021, Kent Law School and Kent Cyber Security Educational Centre (KeCSEC), part of iCSS, hosted a virtual workshop entitled 'Children's Social Media Sites: Can they meet the ICO Age Appropriate Design Code of Practice?'

At this joint event, Professor Jane Reeves – Emeritus Professor at Kent's Centre for Child Protection gave a presentation on 'Children and Grooming; innovative pedagogical approaches in preventative education'. Four Kent Law School and School of Computing Master's students, who have critically assessed compliance of children's social media apps to the 2020 ICO Age Appropriate Design Code of Practice, also shared the results of their preliminary exploratory studies.

The workshop was the first in a series of planned, co-organised events for students, exploring different aspects of cyber security, from a multidisciplinary perspective.

iCSS works with local school and provides top tips for Safer Internet Day

On Monday 8 February, iCSS researchers Professor Shujun Li, Dr Virginia Franqueira and PhD student Sarah Turner, all from the School of Computing, gave a talk at St Edmund's School in Canterbury, to share their experience on cyber security research and education.

The key message to pupils, parents and staff was that cyber security is a highly interdisciplinary topic, meaning anyone, no matter what their interests, can play an active role in cyber security and online safety and go on to develop a career in this field.

For Safer Internet Day (Tuesday 9 February), Sarah went on to support the School with one of five different interactive sessions, aimed at getting pupils to delve deeper into the world of cyber security. In this session, children took on the role of a Cyber Security Inspector in their own home.

Sarah Turner said: 'It was a great opportunity to spend time with a group of students who were keen to learn and think more about cyber security beyond what they may learn in the curriculum. In helping with a session where the students acted as cyber security investigators in their own home, it was exciting to be able to share ideas of cyber security practice with them that they could immediately put into practice and discuss with their friends and family'.

In support of Safer Internet Day, iCSS members Dr Budi Arief, Dr Sanjay Bhattacherjee, Dr Virginia Franqueira, Professor Shujun Li, Dr Jason Nurse, and Dr Jennifer Storey, from the Schools of Computing and Psychology, provided top tips for staying safe online.

The annual event, which started in 2004 as part of the EU SafeBorders project, is now celebrated across the globe and aims to bring people together to make the internet a safer and better place for all, and especially for children and young people.

The theme this year was 'Together for a better internet' and our experts provided their tips within this context. See our experts' tips in the related news story: https://research.kent.ac.uk/cyber/news/?article=2749

New publications

1 Professor Julio Hernandez-Castro and Professor Gildas Avoine
2 Dr Jason Nurse

New book: *Security of Ubiquitous Computing Systems* is published

1

A new book titled *Security of Ubiquitous Computing Systems*, published by Springer, is now free for all to access and download. The book was co-edited by iCSS member Professor Julio Hernandez-Castro from the School of Computing, alongside Professor Gildas Avoine from the National Institute of Applied Sciences, in Rennes, France.

Security of Ubiquitous Computing Systems is designed to help engineers and researchers in computer sciences, mathematics, and electrical engineering, who are not necessarily experts in security, to gain a quick grasp of this field of work.

The book has been more than two years in the making and is the final result of an EU COST project called Cryptacus. This was a 4 year project that engaged cryptanalysts all across Europe in a joint effort to improve the security of IoT primitives and protocols.

Covid related cyber attacks leveraged Government announcements

A consortium of researchers including Dr Jason Nurse, has found that there has been a surge in cyber-security crime experienced during the Covid-19 pandemic, with a particular correlation between governmental policy announcements and cyber-crime campaigns.

2

Their study, published in the journal *Computers & Security*, found that some days as many as three to four new cyber-attacks were being reported.

The Covid-19 pandemic created a new normal for billions of people around the world, with people working from home, ordering shopping and socialising online as shops and businesses were closed. However, with an increased amount of people being online, an increase in cyber-attacks has also been found.

By using the UK as a case study, the paper reveals the explicit connection between governmental policy announcements and cyber-crime campaigns. Read more in the Kent News Centre article: www.kent.ac.uk/news/society/28205/covid-19-related-cyber-attacks-leveraged-government-announcements

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

Ali, Asad, **Hoque, Sanaul, Deravi, Farzin** (2021) 'Directed Gaze Trajectories for Biometric Presentation attack Detection', in *Sensors*, 21 (4). Article Number 1394.

Boakes, Matthew, Guest, Richard, Deravi, Farzin (2021) 'Adapting to Movement Patterns for Face Recognition on Mobile Devices', in Del Bimbo A. et al. (eds) Pattern Recognition. ICPR International Workshops and Challenges. ICPR 2021. Lecture Notes in *Computer Science*, vol 12668. Springer, Cham. pp 209-228. Matthew's presentation is available to watch on Youtube: www.youtube.com/watch?v=RKx1mp_gb6M&list=PL5awuA2KTI5GBIfbh-Lx3KAGIRJhsx8iQ&index=14&t=5s

Douglas, Karen (2021) 'Covid-19 conspiracy theories' in *Group Processes and Intergroup Relations*, 24 (2). pp. 270-275.

Dui, Hongyan, Zheng, Xiaoqian, **Wu, Shaomin** (2021) 'Resilience analysis of maritime transportation systems based on importance measures', in *Reliability Engineering & System Safety*, 209, Article Number 107461.

Fleetwood, Jennifer, Aldridge, Judith and **Chatwin, Caroline** (2020) 'Gendering research on online illegal drug markets', in *Addiction Research & Theory*.

King, Timothy, Koutmos, Dimitrios (2021) 'Herding and Feedback Trading in Cryptocurrency Markets', in *Annals of Operations Research*.

Lalli, Harjinder Singh, Shepherd, Lynsay A., **Nurse, Jason R.C.**, Erola, Arnau, Epiphaniou, Gregory, Maple, Carsten, Bellekens, Xavier (2021) 'Cyber Security in the Age of Covid-19: A Timeline and Analysis of Cyber-Crime and Cyber-Attacks during the Pandemic', in *Computers & Security*. Article Number 102248.

Nurse, Jason R.C. (2021) 'Cybersecurity Awareness', in Jajodia S., Samarati P., Yung M. (eds) *Encyclopaedia of Cryptography, Security and Privacy*. Springer, Berlin, Heidelberg.

Ó Ciardha, Caolite, Ildeniz, Gaye, Karo lu, Nilda (2021) 'The prevalence of sexual interest in children and sexually harmful behavior self-reported by males recruited through an online crowdsourcing platform' in *Sexual Abuse*.

Travaglino, Giovanni, Moon, Chanki (2021) 'Compliance and Self-Reporting during the Covid-19 Pandemic: A Cross-Cultural Study of Trust and Self-Conscious Emotions in the United States, Italy and South Korea' in *Frontiers in Psychology*.

iCCS Team news, events and talks

iCSS welcomes the following new members:

Eamonn Grennan is a Cyber Security and Risk Analyst at NATO and joins iCSS as a new Honorary member. Eamonn's interests encompass digital forensics, cybercrime and state actor nexus, information confrontation and cyber warfare. He is particularly interested in the leverage of new and emerging cyber technologies and techniques prior to and during conflict.

Dr Darren Hurley-Smith is an Information Security Lecturer with the Information Security Group at the Royal Holloway University of London and joins iCSS an Honorary member. Darren's research interests include internet-of-things security, distributed decision-making systems, swarm robotics, smart cities, resilient smart networks, and statistical evaluation of random number generators.

Yichao Wang started as a new PhD student in January 2021. He is co-supervised by Dr Budi Arief and Professor Julio Hernandez-Castro. His research topic is on human aspects of computer security and cybercrime, in particular using data science and machine learning techniques for analysing security incidents and profiling cybercrime stakeholders.

Dr Anna Jordanous is a Senior Lecturer in the School of Computing at Kent and joins iCSS as an Associate member. She is also a member of both the Computational Intelligence and Data Science research groups. Her research interests include NLP, creativity, information retrieval and knowledge representation.

Dr Fernando Otero is a Senior Lecturer in the School of Computing at Kent and joins iCSS as an Associate member. His research interests include machine learning, bio-inspired algorithms, data mining and knowledge discovery with a particular interest on fairness and interpretability. Fernando was recently interviewed by BBC radio Kent on the new £50 featuring Alan Turing. Read the related news story: www.kent.ac.uk/computing/news/2833/fernando-otero-interviewed-by-bbc-radio-kent-on-new-50-note-featuring-alan-turing

Congratulations to Dr Jason Nurse who has been made an Associate Fellow of the Royal United Services Institute (RUSI). RUSI is the world's oldest and the UK's leading defence and security think tank. Its mission is to inform, influence and enhance public debate on a safer and more stable world. RUSI is a research-led institute, producing independent, practical and innovative analysis to address today's complex challenges. Jason has been collaborating with RUSI over the last year on the topic of Cyber insurance as a way to incentivise improved security risk management practices.

Celebrating STEM for British Science Week

For British Science Week (5-14 March 2021), the Divisions of Computing, Engineering and Mathematical Science (CEMS) and Natural Sciences (NATS) held a series of online public lectures from experts in science, technology, engineering, and mathematics (STEM).

Dr Jason Nurse kicked off the week's events with his lecture 'Innovating for the Future at Kent: The fight against Online Misinformation and Fake News'.

The lecture is available to view on YouTube: www.youtube.com/watch?v=vw4f9XiWRs0&list=PL5awuA2KTl5GBIfbh-Lx3KAGlRJhsx8iQ&index=14

Interdisciplinary Quantum Physics panel event

Physoc, the Physics Society at the University of Kent, hosted an interdisciplinary Quantum Physics Panel on Tuesday 9 February 2021, featuring iCSS member Dr Carlos Perez Delgado, Lecturer at the School of Computing.

The panel explored quantum mechanics from the point of view of physics, philosophy, quantum computing, and mathematics. Dr Perez Delgado's presentation was on quantum technologies, in general, and quantum cybersecurity technologies in particular.

You can watch the event on YouTube: www.youtube.com/watch?v=BNHn465nZec&t=2697s

Kent Cyber Security Forum 2021 and official iCSS launch event

On Monday 28 June 2021, we will see the official launch of Kent's Institute of Cyber Security for Society (iCSS), as part of the annual Kent Cyber Security Forum (KCSF 2021) event series. We were unfortunately unable to run KCSF last year due to Covid-19 but are determined not to let it stop us again this year. The event will be hosted online and feature carefully selected talks and panel discussions from a range of cyber security experts from different disciplines. We will also have some fun and interactive sessions available throughout the day for you to join in. More information and a full schedule will be available in due course, but for now – hold this date!

Upcoming conferences and workshops in 2021

Calls for papers/participation

8th Annual Hot Topics in the Science of Security Symposium (HoTSoS 2021)

13-15 April 2021

HoTSoS is a research event centred on the Science of Security, which aims to address the fundamental problems of security in a principled manner. The eighth annual HoTSoS event will be held virtually and hosted by The National Security Agency. iCCS member Dr Özgur Kafali will act as the Program Co-Chair.

15th International Conference on Web and Social Media (ICWSM 2021)

7-10 June 2021

ICWSM is a forum for researchers from multiple disciplines to come together to share knowledge, discuss ideas, exchange information, and learn about cutting-edge research in diverse fields with the common theme of online social media. iCSS member Dr Jason Nurse will act as the General Chair.

16th International Conference on Availability, Reliability and Security (ARES 2021)

17-20 August 2021

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

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

14th International Workshop on Digital Forensics (WSDF 2021)

Please click on the links above for more information and topics of interest. Call for papers Deadline: 7 May 2021

17th EAI International Conference on Security and Privacy in Communication Networks (SecureComm 2021)

6-9 September 2021

SecureComm 2021 is calling for high-quality research contributions in ALL areas of secure communications and networking, including those addressing interdisciplinary challenges in different application domains. This event will be co-chaired by iCSS Director Shujun Li and co-organised by several other iCSS members: Budi Arief, Theodosios Dimitrakos, Julio Hernandez-Castro, Gareth Howells, and Jason Nurse. It will take place at the University of Kent's Canterbury campus.

DPC 130918 06/21