WARWICK
THE UNIVERSITY OF WARWICK

in association with
National Cyber Security Centre

Engineering and Physical Sciences Research Council

Academic Centre of Excellence in **Cyber Security Research**

Post Event Summary Report

for

ACE-CSR Summer Event

25th – 26th July, 2024

Report Date:

18th October, 2024

Prepared by:

ACE-CSR Team at Warwick

Location:

University of Warwick, Coventry, United Kingdom

EXECUTIVE SUMMARY

The ACE-CSR Summer Event 2024, held on 25th and 26th July at the University of Warwick, brought together thought leaders from academia and industry to address contemporary challenges in cybersecurity. The event aimed to bridge the gap between academic research and practical application, with a focus on tackling the most pressing cybersecurity issues of today and preparing for future challenges.

Professor Carsten Maple, Director of Cyber Security Research at WMG, opened the event by emphasising the critical need for interdisciplinary collaboration in the face of evolving cyber threats. He highlighted the rapid growth of digital technologies and the increasing complexity of the systems they create, calling for deeper integration between academic research, industry expertise, and policy-making to ensure robust cybersecurity measures.

The keynote speaker, Peter Davies, Technical Director at Thales e-security, delivered a compelling talk on the cybersecurity challenges of connected vehicle systems. Davies pointed out the rising complexity of these systems, which are increasingly intertwined with global networks, making them vulnerable to cyberattacks. His presentation underscored the need for resilience, not just in preventing cyberattacks but also in recovering from them and maintaining system functionality. He discussed the importance of a resilience-based approach to managing failures in these complex, connected environments.

Following the keynote, research presentations from ACE-CSR members showcased cutting-edge work in the cybersecurity domain. Professor Yi Yu from the Department of Statistics presented research on differential privacy, a framework for ensuring the security of sensitive data in complex environments. Dr Matt Spencer from the Centre for Interdisciplinary Methodologies discussed how social sciences can inform better cybersecurity practices by examining the human factors involved. Professor Feng Hao introduced the Owl protocol, a new approach to password-authenticated key exchange, offering advancements in secure communication protocols.

An interactive session provided participants with an opportunity to assess their expertise across key cybersecurity domains using the Cyber Security Body of Knowledge (CyBOK) framework. The session also explored the impact of emerging technologies such as artificial intelligence (AI), quantum computing, and the risks posed by misinformation. This was followed by a visit to Warwick's research labs in the Lord Bhattacharya Building and the International Manufacturing Centre, where participants saw firsthand the practical applications of research in cyber-physical systems.

The event concluded with a group activity in which participants discussed the future of the ACE-CSR network. They called for more hands-on learning experiences, such as hackathons and Capture The Flag (CTF) competitions, alongside enhanced collaboration between academia and industry to address real-world cybersecurity challenges.

TABLE OF CONTENTS

1. EVENT OVERVIEW

The ACE-CSR Summer Event 2024, held at the University of Warwick on 25th and 26th of July, brought together leading experts from academia and industry to explore key cybersecurity challenges. Organised by the Academic Centre of Excellence in Cyber Security Research (ACE-CSR), the event focused on bridging the gap between research and practical application, particularly in response to the increasing complexity of digital technologies and interconnected systems. The event covered topics such as privacy-enhancing technologies, artificial intelligence in cybersecurity, and the resilience of complex infrastructures against emerging cyber threats.

Participants engaged in panel discussions, research presentations, and lab visits, gaining insights into the latest advancements in the field. A highlight of the event was the keynote address by Peter Davies, Technical Director of Thales e-Security, who discussed the vulnerabilities in connected vehicle systems and emphasised the importance of resilience in managing cybersecurity risks. Attended by cybersecurity professionals, researchers, and policymakers, the event promoted collaboration to advance secure and trustworthy digital systems. This report captures the key discussions and strategic directions that emerged, highlighting the importance of ongoing collaboration between academia and industry in addressing evolving cybersecurity challenges.

2. AGENDA

The two-day event, held on 25th - 26th July 2024 at the University of Warwick, featured in-depth discussions, hands-on activities, and research presentations, providing a comprehensive exploration of key cybersecurity issues.

Time	Session (Day 1)
13:30 - 14:00	Welcome and Setting the Scene
14:00 - 15:00	Panel Discussion: Current Issues and Future Directions • Andrew Rice, Chief Vision Officer, Pelion Consulting • Jez Goldstone, Director, Innov8cyber Limited • Tammy Archer, CISO, Inchcape
15:00 - 16:00	ACE-CSR Presentations • Yi Yu, Professor, Statistics • Matt Spencer, Associate Professor, Social Science • Feng Hao, Professor, Computer Science
16:00 - 17:00	Interactive Session
Time	**Session (Day 2)**
09:00 - 09:15	Welcome and Recap
09:15 - 10:15	**Keynote**: Identifying and Addressing the Cyber Security Challenge • **Peter Davies,** Technical Director, Thales
10:15 - 11:15	Engaging with the ACE-CSR at Warwick

3. OVERVIEW OF CYBERSECURITY AT WARWICK

Professor Carsten Maple, Director of Cyber Security Research at WMG, opened the ACE-CSR Summer Event 2024 by highlighting Warwick's commitment to advancing cybersecurity research. The University of Warwick, through its 'Academic Centre of Excellence in Cyber Security Research' recognition, has firmly positioned itself as a leader in this field, achieving significant growth in both research and practical applications. Warwick's interdisciplinary approach brings together expertise from computer science, statistics, and engineering to address pressing cybersecurity challenges. The university aims to lead globally in cybersecurity research, with the centre tripling PhD recruitment in recent years and securing double the funding for competitive projects. Its research covers key areas such as risk management, privacy, adversarial behaviours, and network security. State-of-the-art facilities, including the Secure Lab and IoT Security Testing Centre, are vital to its work in safeguarding digital infrastructures and testing connected systems. By integrating cutting-edge research with real-world applications and strong

partnerships with industry and government, Warwick continues to develop robust solutions to meet today's cybersecurity challenges.

4. PANEL DISCUSSION: CYBERSECURITY – PAST, PRESENT AND FUTURE

The panel discussion, chaired by **Professor Carsten Maple**, explored the evolution of cybersecurity and its future challenges, with a particular focus on how the landscape has changed over the past decade. Panellists **Andrew Rice**, **Jez Goldstone**, and **Tammy Archer** reflected on the shift from traditional, reactive cybersecurity measures to more proactive and adaptive approaches in response to increasingly complex threats. Emerging risks, such as AI-driven attacks, sophisticated ransomware, and supply chain vulnerabilities, were highlighted as growing concerns. The panellists stressed the need for collaboration between academia, industry, and government to address these evolving challenges. Privacy-Enhancing Technologies (PETs) were also discussed, with a focus on their role in safeguarding data while allowing secure sharing and analysis, particularly in sectors with sensitive information. The discussion further emphasised the integration of technical, social, and legal perspectives as vital for creating robust cybersecurity frameworks that not only address threats but also align with societal and regulatory expectations. The panellists concluded by underscoring the importance of workforce development and cross-sector collaboration to build resilience against future cybersecurity challenges.

5. RESEARCH SHOWCASE: ACE-CSR AT WARWICK

The ACE-CSR Summer Event 2024 featured three research presentations that showcased innovative developments in cybersecurity. These presentations highlighted advances in privacy, the intersection of social sciences with cybersecurity, and improvements in authentication technologies.

A. DIFFERENTIAL PRIVACY IN COMPLEX ENVIRONMENTS

Professor Yi Yu (Department of Statistics) presented her research on differential privacy, focusing on how sensitive data can be protected while allowing for useful analysis. She explored the challenges of implementing privacy-preserving mechanisms in complex environments, such as ensuring data utility while maintaining privacy. Her work emphasised the importance of differential privacy techniques, especially in sectors like healthcare and finance, where data sharing without compromising privacy is critical.

B. SOCIAL STUDIES OF CYBER SECURITY

Dr Matt Spencer (Centre for Interdisciplinary Methodologies) explored the role of social sciences in understanding cybersecurity practices. His research highlighted how human behaviour, cultural norms, and organisational structures affect cybersecurity outcomes. By incorporating insights from anthropology and sociology, Dr Spencer underscored the importance of considering the social context in which cybersecurity systems operate, advocating for a more comprehensive approach that goes beyond technical fixes.

C. OWL: AN AUGMENTED PASSWORD AUTHENTICATED KEY EXCHANGE (PAKE) PROTOCOL

Professor Feng Hao (Department of Computer Science) introduced the Owl protocol, a new augmented Password Authenticated Key Exchange (PAKE) scheme designed to enhance security in password-based authentication systems. He discussed how Owl improves upon existing protocols by addressing vulnerabilities and increasing resistance to attacks while maintaining efficiency. This research has important implications for secure communication and system integrity in both personal and enterprise-level applications.

6. KEYNOTE: IDENTIFYING AND ADDRESSING THE CYBERSECURITY CHALLENGE

Peter Davies, Technical Director of Thales e-Security, delivered a keynote address that focused on the increasing complexity of cybersecurity threats in modern connected systems. He highlighted the growing vulnerabilities faced by industries, particularly in the automotive sector, as reliance on interconnected digital infrastructures deepens. Davies explained how the complexity of these systems, coupled with their dependence on external

networks and digital components, leaves them exposed to sophisticated cyber threats. He emphasised that these vulnerabilities have far-reaching implications for safety, privacy, and system integrity, making robust cybersecurity measures essential.

Peter stressed that, while total security is impossible, resilience should be at the core of cybersecurity strategies. Instead of solely focusing on prevention, he advocated for systems designed to anticipate, absorb, and recover from cyberattacks, ensuring continuity even when breaches occur. This resilience-based approach allows organisations to minimise the damage from security incidents while maintaining system functionality. He also emphasised the need for greater collaboration between industry, academia, and government to address the evolving cybersecurity landscape, calling for more adaptive and innovative frameworks to manage ongoing and future challenges.

7. SURVEY REPORT ON CYBOK AND EMERGING TRENDS

This report outlines the expertise levels of participants across various CyBOK domains and explores their perspectives on emerging technologies and trends that are anticipated to have a profound impact on cybersecurity. The findings reflect both strengths and areas for improvement within participants' knowledge base, as well as future-oriented concerns related to technological advancements.

A. EXPERTISE IN CYBOK DOMAINS

Strong and Moderately Developed Domains

In areas like Risk Management & Governance, Malware & Attack Technologies, Adversarial Behaviours, and Human Factors, most participants reported basic to strong knowledge. Privacy & Online Rights also saw a mix of basic, strong, and expert-level knowledge, indicating good awareness of its significance in the cybersecurity landscape.

Gaps in Expertise

Several domains revealed significant gaps. Law & Regulation had the highest proportion of participants with no expertise beyond a layperson level, highlighting a major area of concern. Domains such as Forensics, Security Operations & Incident Management, and Cryptography had moderate representation but lacked advanced expertise. Additionally, areas like Formal Methods for Security, Network Security, and Software Security showed a lack of expertise, indicating the need for critical knowledge training in technical areas.

B. EMERGING TECHNOLOGIES AND TRENDS IMPACTING CYBERSECURITY

AI and Quantum Technologies

Artificial intelligence (AI) and quantum technologies emerged as dominant concerns. Generative AI was the most frequently mentioned trend, underscoring the growing anxiety around the potential misuse of AI in generating sophisticated cyber threats, including deepfakes and automated hacking tools. The discussions around AI extended to its broader implications in the cybersecurity landscape, where participants also mentioned AI in manufacturing and Large Language Models (LLMs) as potential game-changers.

Quantum technologies were another area of concern, with mentions of Quantum AI, Quantum Cryptography, and Quantum Technology. These references indicate an awareness of the looming impact of quantum computing on encryption standards and the vulnerabilities that could arise as quantum computing capabilities grow. As this technology continues to evolve, it is expected to render many current cryptographic methods obsolete, posing a critical challenge for cybersecurity professionals.

Misinformation and Deception Technologies

Another key trend was the rise of misinformation and deepfakes, reflecting a heightened awareness of the role that disinformation campaigns and synthetic media play in cybersecurity. These technologies are increasingly being used to manipulate public opinion, deceive users, and exploit vulnerabilities in systems reliant on digital

trust. Participants also mentioned hallucination as a potential threat, likely in reference to AI systems generating misleading or incorrect outputs, which could further complicate the cybersecurity landscape.

Blockchain, IoT, and Decentralised Finance

Emerging technologies such as Blockchain and IoT were highlighted as having a significant impact on cybersecurity. These technologies introduce both opportunities and risks, with blockchain offering enhanced security through decentralisation but also posing regulatory challenges, while the proliferation of IoT devices increases the number of entry points for cyber attacks. Decentralised finance (DeFi) was another trend mentioned, reflecting concerns about the security implications of these new financial technologies, where traditional banking security measures are not always applicable, leaving them vulnerable to exploitation.

Other Trends

Other technologies and frameworks mentioned include Zero Trust Architectures, which are gaining traction as a security model that assumes no actor, whether inside or outside the network, should be trusted by default. Participants also highlighted the potential of Formal Proofs to enhance the security of systems through rigorous mathematical validation. Autonomous vehicles were also cited, reflecting concerns about the intersection of cybersecurity and physical safety in emerging sectors.

8. GROUP ACTIVITY: FUTURE DIRECTIONS FOR THE ACE-CSR NETWORK

The ACE-CSR Summer Event 2024 featured a group activity that gathered insights from participants, focusing on their expectations from the Warwick Cyber Network, contributions they could offer, and their preferences for future events. These insights provide a roadmap for the network's future development, helping to align academic and industry efforts with real-world cybersecurity challenges.

A. EXPECTATIONS FROM THE WARWICK CYBER NETWORK

- **Enhanced expertise sharing** through more frequent seminars featuring both international and internal speakers, with a focus on interdisciplinary topics like autonomous vehicles and emerging technologies.
- **Increased interdisciplinary collaboration** by strengthening ties with industries, especially SMEs, and fostering cross-domain interactions with fields such as engineering.
- **More practical learning opportunities**, such as Capture The Flag (CTF) competitions and consultancy experiences that enable participants to apply theoretical knowledge in real-world scenarios.
- **Community outreach** initiatives, including educational and mentorship programmes for younger students and underrepresented groups, alongside efforts to raise public awareness about cybersecurity.
- **Resource development**, including the creation of a centralised repository for cybersecurity resources and intellectual challenges such as brainstorming sessions and collaborative problem-solving activities.

B. CONTRIBUTIONS TO THE WARWICK CYBER NETWORK:

- **Expertise sharing** through research presentations, demonstrations, guest speaking, and mentorship from both academic and industry participants.
- **Industry insights and practical support**, including offering industry-aligned research challenges, technical experiments, and placements or internships for students and early-career researchers.
- **Event organisation support** for conferences, workshops, and other gatherings, with participants also offering to assist in forming strategic partnerships and supporting commercialisation efforts.

C. PREFERRED EVENTS FOR THE WARWICK CYBER NETWORK:

- **Academic conferences, workshops, and seminars** covering a broad range of topics such as cybersecurity, AI, and the Internet of Things (IoT), with recurring seminar series to maintain engagement.
- **Practical and interactive events**, including regular hackathons, CTF competitions, sandpits for collaborative brainstorming, and write days focused on bid writing.

- **Community and outreach events** targeting schools through outreach activities and roadshows, along with diversity and social events to foster inclusivity within the cybersecurity community.
- **Specialised and thematic events**, such as field-specific interest groups, industrial visits, and accelerator programmes to provide insights into real-world applications and support for start-ups.

9. CONCLUSION

The ACE-CSR Summer Event 2024 highlighted the increasingly complex nature of cybersecurity, and requires a multidisciplinary, collaborative approach, integrating technical innovation with legal, social, and behavioural insights. Discussions highlighted the shift from reactive to proactive strategies, with resilience emerging as a key principle in managing complex, interconnected systems. By integrating academic research with real-world applications, the Warwick's ACE-CSR network is well-positioned to lead in addressing evolving cybersecurity challenges by developing practical solutions that align with industry needs and global security demands.

10. NEXT STEPS FROM ACE-CSR AT WARWICK

Based on the insights from the ACE-CSR Summer Event 2024, the ACE-CSR at Warwick will prioritise several key areas to continue advancing cybersecurity research and its real-world application.

- **Strengthening collaborations** with industry, government, and academic institutions to create impactful solutions that address pressing cybersecurity challenges across sectors.
- **Expanding practical learning opportunities** through hackathons, Capture the Flag (CTF) competitions, and workshops that provide hands-on experiences for students, researchers, and professionals.
- **Developing resilience-based strategies** to ensure systems can adapt, recover, and maintain functionality in response to evolving threats, integrating this approach into ongoing research and industry partnerships.
- **Engaging with emerging technologies** like AI and quantum computing to build security frameworks that remain robust as new technologies disrupt traditional security models.
- **Enhancing educational initiatives** by increasing seminars, workshops, and mentorship programs, preparing the next generation of cybersecurity experts to address the growing complexities of the digital world.