# SECURITY CHALLENGES FOR IMMERSIVE TECHNOLOGIES

*Image generated by ChatGPT.*

On Thursday, October 9, 2025, INCS-CoE held an on-line seminar on security challenges for immersive technologies. Two speakers presented their ongoing research: Bo Ji (Virginia Tech, US), and Jesus Martinez-del-Rincon (Queen's University Belfast, UK) – see biographies at the end of this note.

Bo Ji focused on Augmented Reality (AR) devices which distinguish themselves from other mobile devices by providing an immersive and interactive experience. The ability of these devices to collect information presents challenges and opportunities to improve existing security and privacy techniques in this domain. He discussed how readily available eye-tracking sensor data can be used to improve existing methods for assuring security and protecting the privacy of those near the device. He presented three new systems, BystandAR, ShouldAR, and GazePair, leveraging the user's eye gaze to improve security and privacy expectations in or with AR. As these devices grow in power and number, such solutions are

necessary to prevent perception and privacy failures that hindered earlier devices. This work is presented in the hope that these solutions can improve and expedite the adoption of these powerful and useful AR devices.

Jesus Martinez-del-Rincon and his team at Queen's University Belfast completed a two-phase Metaverse technologies horizon-scanning project in July 2023 and 2025. He gave a summary of the most relevant findings and outcomes. In the first phase, the project produced a broad landscaping report of UK interests and activity in related technical areas. Building on areas where the UK might benefit from the emerging Metaverse, the second phase, deepened the analysis in three main areas: a) interoperability an standards: where they highlighted current metaverse standards development organisations and identified the strategic aims of such participation; b) privacy, security and regulations: investigating two complementary aspects: (1) the evolving regulatory and legal landscape related to data collection by metaverse service operators; (2) a threat analysis of the metaverse and a technical analysis of the privacy preserving technologies that could enable metaverse data platforms ; c) a horizon-scanning of Distributed Ledger Technology and its application to the Metaverse.

Some of the key research challenges which emerged during the seminar included:

1. How to address the privacy and security of bystanders when using AR devices coupled with face recognition? BystandAR offers an innovative solution to this challenge but there is more to be done in environments where there are many individuals.
2. How could privacy enhancing technologies be deployed in future metaverse applications?
3. What should be the priority actions for policy makers and regulators in developing interoperable standards for the metaverse?
4. How to protect the large volumes of personal data collected by AR devices?
5. How can security and privacy and goals be achieved by resource-limited AR devices?
6. How can techniques be scaled to large multi-user environments?
7. How can security and privacy aspects be robustly evaluated?
8. How to trade-off security against other desirable attributes such as acceptability, etc…?

More information about the individual presentations and the resulting research questions may be found on the INCS-CoE website (incs-coe.org) or by contacting the speakers. We encourage the community to start conversations which might lead to the solutions of some of these challenges.

# Speakers

## Bo Ji

Bo is an Associate Professor of Computer Science and a College of Engineering Faculty Fellow at Virginia Tech. His research interests include interdisciplinary intersections of computing and networking systems, artificial intelligence and machine learning, security and privacy, and extended reality. More information about his research can be found here: https://people.cs.vt.edu/boji.

## Jesus Martinez-del-Rincon

Jesus is a Professor in Secure and Trustworthy AI at the School of Electronics, Electrical Engineering and Computer Science, Computer Science, Queens University Belfast (QUB). He leads the Centre for Secure Information Technologies (CSIT)'s Secure Intelligence (SI) group. An expert in Machine Learning and computer vision, deep learning and data analytics for cyber and physical security applications, he has published >170 journal and conference papers, and attracted >£15M in grant funding from EPSRC, NCSC and InnovateUK. He is also the director for the CSIT's Doctoral Training Programme (DTP) and co-director for the EPSRC Centre for Doctoral Training in Future Open SecuRe NeTworks (CDT-FORT). Among many other topics, he published the first paper on NLP-inspired deep learning architectures for malware detection on bytecode sequences and the first paper to use deep-learning for video-based person re-identification at the prestigious CVPR conference. He has won 3 paper awards in international conferences, such as BMVC. He is also recipient of other awards such as the Best KTP award 2022 by InnovateUk, the Best Thesis awards by the Spanish Association for Pattern Recognition and Image Analysis and the ICE East Midlands Merit Awards 2019.