SECURITY CHALLENGES FOR MEDICAL DEVICES

Image created by ChatGPT

On Wednesday, March 26, 2025, INCS-CoE held an on-line seminar on security challenges for medical devices. Three speakers presented their ongoing research: Jorge Blasco Alís (Universidad Politécnica de Madrid, Spain), Emil Lupu (Imperial College London, UK) and Phil Englert (Health-ISAC, USA) – see biographies at the end of this note.

Jorge Blasco Alís presented a security review of Bluetooth Low Energy which has now become one of the most prominent wireless communication mechanisms for short-range and low power communications. BLE is now available on fitness trackers and many different “smart” devices that range from locks, cars and even medical devices. Increasingly, these use cases require the storage of sensitive user data or critical device controls on the BLE device, as well as the access of this data by an augmentative mobile application. Uncontrolled access to such data could violate user privacy, cause a device to malfunction, or even endanger lives. He gave an overview of BLE and the different security mechanisms available both in the BLE protocol and devices that implement it. He then reviewed some of the threats that can affect BLE devices and some of the most recent vulnerabilities that have been published, looking at the possible implications if these were found on medical devices.

Emil Lupu made the case that ensuring the security, safety and resilience of future medical devices is an ideal use-case to confront some of the most difficult problems in cyber-physical security. He observed that confronting this challenge will force us to develop novel thinking and novel techniques for "secure-by-design" that go beyond the application and evolution of existing security solutions for cryptography, anomaly detection, authentication and access control. Our processes and practice of system design needs to align with the reality of a cyber-physical world where trade-offs between apparently conflicting requirements need to be constantly made. Addressing challenges in this space will not only lead to better security across a broad spectrum of cyber-physical systems but also open the door to new generations of medical devices to improve health.

Phil Englert started from the observation that securing embedded medical devices is challenging due to their limited computing power, constrained energy resources, minimal user interfaces, and reduced visibility once deployed. To ensure these devices remain resilient throughout their operational life, it is essential to use lightweight encryption algorithms, regularly update firmware, and implement strong audit capabilities. Additionally, robust access controls and secure boot mechanisms can significantly enhance device security. These measures collectively protect patient data and ensure the reliable functioning of medical devices in the field. He explored the technical and environmental challenges of developing and maintaining cyber-resilient embedded medical devices.

The talks covered important topics ranging from the communication protocols, through device specifics to the implications for system design. Challenges arise because of the particular nature of the application domain and cover patient safety, appropriate care delivery and patient confidentiality issues. Some of the key research challenges which emerged during the seminar Included:

- To find mitigations for the fact that, on Android platforms, applications are granted permissions to use Bluetooth (not tied to a specific device); data exchanged between two devices is visible to all apps on the user's device. More generally, it is estimated that 70% of medical apps don't protect BLE data.

- To develop design methodologies which lead to safety and security being considered much earlier in the design process.

- To explore ways in which the physiology of the body can be used to provide localised communication and thus avoid wireless communication using vulnerable protocols.

- To develop more secure methods for device pairing.

- To understand and quantify conflicting risks; there may be a cyber security vulnerability in an embedded device but the risk of an invasive procedure to change it may be much higher. This is a novel instance of the ongoing discussion about interactions between safety and security.

- A patient with comorbidities may have multiple embedded devices from different vendors and with different interfaces; issues of interoperability and secure and seamless communication between such devices are an urgent topic for study.

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

Jorge Blasco Alís, Universidad Politécnica de Madrid (Spain)

Jorge Blasco Alís obtained his PhD from Carlos III University in 2012. In July 2014, he moved to City, University of London, where he worked on Android malware. In September 2016, Dr Blasco moved to the Information Security Group (ISG) at Royal Holloway, University of London. In 2018, Jorge Blasco founded the System And Software Security Lab (S3Lab) which included two other members of staff and, overall, supervises the dissertations of 10 PhD students. The S3Lab was founded to consolidate the research addressed by Dr Blasco in the area of software and system security for smartphones and expand these into new platforms. Overall, Dr Blasco has been able to secure up to £1M on competitive grants and has published more than 40 research papers in prestigious international conferences and journals on cyber security. In August 2022, Dr Blasco moved to Universidad Politécnica de Madrid as an Associate Professor (Professor Titular) where he now leads SeCLab, a cybersecurity research group focused on software and hardware security.

Emil Lupu, Imperial College London (UK)

Emil Lupu is a professor of computer systems at Imperial College London. He leads the Resilient Information Systems Security Group (RISS - rissgroup.org) and is a co-director of the Research Institute in Trustworthy Inter-Connected Cyber-Physical Systems (RITICS - ritics.org). His research interests include the security, safety and resilience of cyber-physical systems, techniques for the consilience of security and safety, and to enable systems to continue operating even when they have been partially compromised.

Phil Englert, Health-ISAC (US)

Phil Englert is the VP of Medical Device Security for Health-ISAC, working with Medical Device Manufacturers (MDMs) to help improve privacy and security while coordinating with Health Delivery Organizations (HDOs) to ensure implementations are practical and achievable. Phil has over 30 years of technical and operational leadership in the healthcare and life sciences focused on strategy, operations, data, and technology-enabled business optimization, IoT security, and privacy with deep knowledge of healthcare & clinical settings and extensive knowledge of medical technology and innovation. As the National Director of Technology Operations at Catholic Health Initiatives, Phil led strategic and tactics development to support 380,000 medical devices for a $250m in-house service organization supporting over 130 Acute Care facilities across 22 states.