GCHC Workshop 4

The Connected Healthcare Cybersecurity Integrated Systems Design Workshop, held on 22 September 2021, was the fourth in the IEEE Global Connected Healthcare Cybersecurity (GCHC) Virtual Workshop Series presented by the IEEE Standards Association Healthcare and Life Science Practice and the Northeast Big Data Innovation Hub. It attracted 50 attendees including healthcare, technology, and policy experts and advocates.

Welcoming remarks were delivered by the hosts of the workshop series, Maria Palombini, Director of the IEEE Standards Association Healthcare & Life Sciences Practice, and Florence Hudson, Executive Director of the Northeast Big Data Innovation Hub. After opening remarks, the conversation moved to the main panel session on the path to connected health cybersecurity with integrated systems design, moderated by Maria Palombini. Panelists included Xavier Bignalet, Security Product Manager at Microchip Technology Inc., Jigar Kadakia, Chief Information Security and Privacy Officer (CIO/CPO) at Mass General Brigham, and Chris Riha, Health Systems Engineering Lead at MITRE.

After opening statements, participants were asked in an on-line polling question: "*Do you find that a single Reference Architecture (RA) is suitable to address the growing challenges in the connected healthcare domain?"* In response to participants' votes, the speakers agreed that a representative architecture could probably meet only around 60% of requirements. RAs help identify and communicate good practices, but their compatibility may present a bottleneck in individual situations with unique requirements.

The panel then responded to the question from the moderator, posed in an on-line poll: *"What do you find to be the greatest challenge to designing integrated Systems of Systems (SoS) for connected healthcare?"* The answers presented for participants to choose from were:

- Privacy and security vulnerabilities at the edge
- Lack of standard data formats and communication protocols for information flow
- Lack of system-wide trust among users, partners, and everyone in between
- New technology solutions, such as "swarm AI", are not yet fully developed

After participants cast their opinions, the panelists agreed that all these challenges are valid and significant, further elaborating that trust is lacking from both sides of the equation. Hospitals, for example, see a need and a push to have more connected devices which present even more risks and liability to their systems. Another point raised by the panelists is that device manufacturers often tend to follow the minimum standards, and that each manufacturer follows

different standards. Also, after completing the intensive process of obtaining FDA approval, manufacturers tend to be hesitant about making updates and requiring further FDA engagement, and leave new gaps which need to be handled by the security team. Organizations must make conscious decisions about which standards to choose and follow. Another series of questions arise when dealing with different authorities of data which is being shared or communicated across institutions, as well as across regulatory boundaries in international situations: Who is the governing reference? Should companies, or can companies, set up a central reference, and which authorities do they abide by?

When discussing room for improvement for better interoperability, Kadakia mentioned modifications of standards for interoperability with older systems. Newer systems have modern technology. Organizations will eventually have to decommission older systems and replace them with newer systems, but in the meantime there needs to be a way to enable interoperability with safety and security in mind.

The participants shared a key question in the chat about what work is being done with senior living centers and in response to the booming movement of mobile care at home. The panelists mentioned that they are indeed seeing more of this conversation recently, especially with the onset of the COVID-19 pandemic when the need for remote monitoring systems became evident. Whether it's diabetic monitoring, blood pressure monitoring, or other types of monitoring, there are several valuable solutions that patients can leverage with very minimal technical or system knowledge to monitor values from the comfort of their own homes and alert doctors or hospitals if things change. The COVID-19 pandemic environment highlighted the benefits of remote monitoring systems and showed the need for them, but there remains the requirement of validating these devices and ensuring they are up to standards from all aspects. The reliability, consistency, and usability of data generated from wearables is still under speculation for use in clinical decisions, versus data from a certified system. As the world continues to be more remote and more connected technologically, the use of connected healthcare devices and systems is expected to witness tremendous growth. It was noted that the American Recovery and Reinvestment Act of 2009 neglected nursing homes, so senior living centers are now playing catch-up to establish the infrastructure that they were lacking. Hudson mentioned a use case from the P2933 – IEEE/UL standards working group for Clinical Internet of Things (IoT) Data and Device Interoperability with TIPPSS – Trust, Identity, Privacy, Protection, Safety, Security: Wearables in the Wild, which addresses patients with wearables that are outside any of the typical facilities. The P2933 working group is developing the standards needed to enable trusted communication, with validated patient and provider identities, to ensure privacy, protection, safety, and security, to allow connected healthcare devices and wearables to monitor the patient's health and enable communication to health and emergency medical providers to intervene and protect them in urgent healthcare situations.

The discussion then turned to the question: "*How do medical device regulations shape the manufacturer's preparedness for cybersecurity attacks during the design phase?"* It was noted that FDA guidance states that any changes done to a device, even a software update, will classify it as a different device. Riha mentioned that the FDA published guidance documents from manufacturers over the last several years on how to "bake in" cybersecurity, and risk-modeling procedures for vendors and Original Equipment Manufacturers (OEMs) to consider as they design their system. This shows that they are trying to be proactive and get ahead of attacks. Kadakia added that despite the FDA's proactive approach, "guidance isn't law," and people and manufacturers tend to dismiss recommendations if they are expensive and complex even though they may be best practices. Riha also noted that this may change as manufacturers take a more market-driven approach, if more consumers start requesting or demanding increased cybersecurity provisions.

As Artificial Intelligence (AI), Machine Learning (ML), and similar technologies have been quietly integrated into systems for many years, and are becoming more prominent in Systems of Systems, there are questions about the role that AI/ML can play in connected healthcare. For instance, AI/ML can be leveraged to enable safe and secure data and device verification, validation, security, privacy, and interoperability, as well as provide other major benefits. As hospitals have access to more and more data from devices and humans, they can use AI/ML tools and concepts to analyze the data more readily and effectively, and develop insights and potential conclusions about pertinent tactical situations, as well as for far-reaching abstract concepts or clinical or fundamental research that would potentially be undiscovered through normal data analysis. Another benefit of AI/ML can be for monitoring devices, both to authenticate devices through trust and identity mechanisms, as well as identifying anomalies in device behavior which may unearth a device issue. Despite the promise that AI/ML technologies offer, data scientists still spend large durations of time normalizing data for analysis which could be sped up by establishing standards for more efficient data collection and cleaning. Hudson adds that AI/ML can be used not only at the server level but also all the way down to the chip level of devices. IBM, for example, has applied artificial intelligence for behavior assessment of technology, which presents an opportunity to think about how AI/ML can be used on different levels (e.g.,hardware, software, firmware, service) and then across at the System of Systems level.

Since healthcare is moving from a hospital approach to a patient-device centered approach, the efficacy of devices is going to be evermore paramount in the future as we rely on devices in clinical care. Telehealth has proven that basic care can be performed remotely and can be applied to a 24/7 situation where instead of patients waiting for appointments the next day, there would always be a healthcare practitioner available through one of the online platforms to help patients with minor medical issues. The better the device is and the more capabilities it has, the more power it will give to at-home care for monitoring and observation. The COVID-19

pandemic has encouraged people to work through the uncomfortable aspects of telehealth, encouraged its adoption, and made people accustomed to this service. Younger generations will come to expect these types of services for basic healthcare activities. The shift to a patient-device centered approach also presents patients with the opportunity to take ownership of their data. Bignalet added that from a device standpoint, there should be standards to manage access privileges from a security perspective, given that patients, service companies, and device companies all have some level of access to the device. Security across different levels is a major area for improvement in existing and future devices as reliability on them increases. Another challenge is tracking device and human identity and validating the data and device calibration and accuracy for decision making.

Hudson shared P2933's Trust, Identity, Privacy, Protection, Safety, and Security (TIPPSS) Architecture Framework for Clinical IoT & Data Interoperability that showcases the many layers in a framework, starting with the users (UI/UX), through the devices, interoperability protocols, and software and service layers, to the data sources. This presents the pieces that could be part of a complex System of Systems and provides policymakers with the opportunity to consider all important aspects of a standard while developing it.

When asked about applications of blockchain in their fields, panelists mentioned that current applications are still limited in the field and more widely used in other industries such as finance. There are, however, promising applications of blockchain in healthcare such as Distributed Digital Ledger Technology (DLT) for organizations that don't have a central authority to share data in a peer-to-peer fashion. Another useful application of blockchain would be to help pharmaceutical companies and providers find suitable participants for clinical trials to have statistically significant results. Other use cases also exist for pharmaceutical supply chains to manage and track various stages of the process.

Given that doctors have access to their patients' health records but these patients are part of a network, other doctors can also access their health records without their permission. In a world of connected healthcare that is centered heavily around the patient's data, the workshop participants discussed how credentialing can be different with an integrated system. This ties to the issue of identity of workforce members and patients and ensuring that these two profiles interchange appropriately and privately in a secure manner combined with the expectation of easy access. While no current direct solutions are being applied, stakeholders definitely see the need for this extra layer of protection that could be the next step in standards work and integrated systems design to realize the benefits of connected healthcare with cybersecurity.

SPECIAL THANKS TO THE FOLLOWING INDIVIDUALS AND SUPPORTERS OF IEEE SA GCHC VIRTUAL WORKSHOP SERIES:

THE EXPERT SPEAKERS

- **JIGAR KADAKIA**, Chief Information Security and Privacy Officer (CIO/CPO), **Mass General Brigham**
- **CHRIS RIHA**, Health Systems Engineering, Lead, **MITRE**
- **XAVIER BIGNALET,** Security Product Manager, **Microchip Technology Inc.**

THE PLANNING ADVISORY BOARD

- Dr. Mohd Anwar, Professor, North Carolina Agricultural and Technical State University
- Florence Hudson, Executive Director, Northeast Big Data Innovation Hub; IEEE/UL P2933 Working Group Chair
- Ms. Grace Wilson Marshall, Cybersecurity Consultant, FSS TECHNOLOGIES (FSST), IEEE SA
- Ms. Macy Moujabber, Graduate Student, Columbia University
- Maria Palombini, Director, Healthcare and Life Sciences Practices Leader, IEEE SA
- Mitchell Parker, CISO, Indiana University Health; IEEE/UL P2933 Co-Vice Chair
- Dr. Nada Y. Philip, Associate Professor, Kingston University, London; IEEE/UL P2933 Privacy Subgroup Leader
- David Snyder, MBA, PE, CISSP, Consultant, 42TEK, Inc.; IEEE/UL P2933
- Parthiv Shah, Sr. Manager, Security Consulting, Cerner Corporation; IEEE/UL P2933 Security, Protection and Safety Subgroup Co-Leader
- Konstantinos Votis, Researcher, CERTH/ITI; IEEE/UL P2933

WORKSHOP UNDERWRITER

Special thanks to Microchip Technology Inc. for supporting the fourth edition of the 2021 IEEE SA Global Connected Healthcare Cybersecurity Virtual Workshop Series.

REPORT AUTHOR

Special thanks to Ms. Macy Moujabber, Graduate Student Ambassador from Columbia University for her diligent note-taking during the session and organizing this paper from the proceedings of the workshop held on 22 September 2021.