GROVE SCHOOL
OF ENGINEERING

CSE H0240: Law and Policy Issues in Cybersecurity

Position Paper On

Cybersecurity Regulations (Healthcare)

Created By:

MD ABDUL KADIR

Submitted To:

Professor Benjamin Dynkin & Professor Barry Dynkin

CSE H0240 Course Instructor

Department of Cybersecurity (MS Program)

Grove School of Engineering

The City College of New York

Academic Session- Spring 2023

With the rapid increase of IoT devices, security becomes an afterthought especially when referring to medical devices. There are a multitude of aspects to investigate when it comes to security requirements that medical devices must follow. In addition, a newly emerging area in development is Internet of Medical Things (IoMT). Many devices are considered as IoMT. For example, various consumer-grade devices like fitness watches. Devices worn on the body was coined as "wearable IoMT." Clinical-grade devices, another type of IoMT, are approved for specific health applications like detecting irregular heartbeats or other medical conditions. In-hospital IoMT devices are used by trained medical professionals within a medical facility. There are many applications for these particular devices which include personal management, asset management of high-demand devices, patient flow devices, monitoring, adjusting certain parameters, and conditions of various patient-connected devices. Many threats and attacks have been found targeting medical devices. Medical device security is challenging but essential for any health organization.

With the advances in IoT healthcare applications, it has become a reality for many patients to benefit from remote monitoring, reducing the need for frequent visits to doctors or prolonged stays in hospitals. Elderly care, remote health monitoring, medical emergencies, and early diagnosis are all aspects of healthcare that are becoming easier with IoT applications. However, as technology is getting popular, adversaries use innovative ways to harm the overall system

According to a 2019 report by the ECRI Institute, when considering the top 10 health technology hazards, remote access and malicious changes to data were identified as the top technical risk in healthcare. In addition, researchers reported attacks (eavesdropping wireless communication or controlling other gadgets) on insulin pumps and security breaches in implantable medical devices in order to modify the expected treatment. Therefore, the interconnection of large amounts of potentially 'untrusted' things with 'untrusted' communication media in IoT based environments enables various cyber-physical attacks. To keep an eye on these attacks, the Health Insurance Portability and Accountability Act (HIPAA) requires technical safeguards to be in place for electronic protected health information (e-PHI), and many countries introduce similar acts and regulations. However, compliance with such regulation currently relies on audits and is often not continuously monitored. One approach is to bind information on safeguards are actually in place to the data moving through multi-layered, inter-operable IoT health systems. This would complement audits by a mechanism that enables real-time checks on compliance.

Data in an IoT network needs to traverse through various layers from source to destination. Understanding this data propagation through the data life cycle plays a crucial role in monitoring and maintaining overall IoT security. In particular, it is

challenging to ensure/monitor that every part of a multi-layer IoT architecture maintains an appropriate security deployment. Hence, understanding security risks and trust issues in systems and steps involved in data collection and operation need to become a priority. Furthermore, the end-user also needs to be empowered with the right level of situational awareness with regards to system's risk assessment and compliance management.

Recent research identifies device registration and data generation to be the most vulnerable phase, as IoT devices are physically exposed and heterogeneous in nature. Many researchers discuss authentication approaches (for example, hashing with element extraction, secure key establishment using elliptic curve cryptography, lightweight authentication protocol for securing RFID tags) in the initial phases of data propagation. These methods can provide an initial root of trust for origin authentication, but relating this trust to the end-user remains open.