A Sandbox Test Environment for Medical Device System Cybersecurity

Presenting Author: Julian M. Goldman, M.D.
Co-Author(s): David Guffrey, M.S., M.S.M., Michael B. Jaffe, Ph.D., Yi Zhang, Ph.D., Barbara Dumas, and Dave Arney, Ph.D.

Reports of high-impact security vulnerabilities affecting medical devices and hospital IT infrastructures have put the cybersecurity of medical devices in the spotlight [1,2]. As advocated by the US FDA, medical device cybersecurity relies upon collaboration across the healthcare ecosystem [3,4].

A vendor-neutral non-clinical “sandbox” testbed can play a valuable role in enabling and promoting collaboration by providing capabilities to 1) assess medical device security vulnerabilities and their clinical impacts; 2) evaluate mitigation and remediation technologies, including deployment strategies, against security vulnerabilities; and 3) establish trust and share information to support cybersecurity preparedness and response. In collaboration with the US FDA and MITRE, we implemented a medical device cybersecurity sandbox environment for studying the use of these environments for cybersecurity preparedness. The core of the MD PnP Sandbox is a sophisticated network infrastructure with a wide range of networking systems (routers, firewalls, switches, access points, controllers, servers, and network data collection tools), which is capable of emulating hospital environments. Network segmentation and demilitarized zones can be easily configured so that each device assessment can be isolated. Multi-factor VPN enables remote access by collaborators. The sandbox is further distinguished by a wide range of physical and simulated medical devices.

These capabilities enable investigators to rapidly implement clinical scenarios for medical devices and IT equipment under test, so that: 1) the discovery, testing, and validation of vulnerabilities in the device are guided by its real-world clinical use; 2) assessing the impact of security vulnerabilities is made more clinically relevant; and 3) mitigation, remediation, and response plans in face of security incidents and cyber-attacks can be designed and evaluated in a more realistic environment.

We conducted a collaborative exercise with the FDA and MITRE in 2018 to evaluate and validate the capabilities of sandbox environments and their ability to support third-party device security assessment. A key facet of this project was to identify challenges encountered through the application of sandbox environments for collaborative and multi-disciplinary cybersecurity preparedness and response activities. These included governance, legal considerations, technical challenges, lab capabilities, and team expertise. We engaged two major medical device manufacturers with their widely used medical device systems. A clinical scenario based methodology to comprehensively, yet efficiently, identify and demonstrate attack scenarios utilizing previously disclosed (and corrected) vulnerabilities in the devices and how might could be exploited to impact clinical workflows. Further study allowed us to examine manufacturer recommended mitigation measures for effectively protecting against these vulnerabilities.

We believe a sandbox test environment as demonstrated under this contract can bring benefits to the coordinated efforts of the healthcare community in addressing medical device cybersecurity, from supporting third-party medical device security certification, to assisting in coordinated disclosure of device vulnerabilities, and to leveraging the stakeholders’ preparedness for device vulnerabilities and malicious cyber-attacks. We welcome collaborations with stakeholders to leverage our sandbox environment for improving the safety and security of medical device systems.

Supported in part by an FDA CDRH /MITRE CAMH contract. The authors, not FDA or MITRE, bear responsibility for the content of this publication.