A Secure Interoperability Platform to Facilitate Anesthesia Technology Innovation

Presenting Author: Julian M. Goldman, MD (jmgoldman@mgh.harvard.edu)
Co-Authors: Yi Zhang PhD, David Arney PhD, Simon Kelly, Sandy Weininger, PhD
Medical Device Plug-and-Play Interoperability & Cybersecurity Program
Dept. of Anesthesia, Critical Care, and Pain Medicine, Massachusetts General Hospital, Boston, MA *U.S. Food and Drug Administration/CDRH/OSEL

Introduction: With the improvement of data integration capabilities, medical devices connected to "software as a medical device" apps can accelerate the development and deployment of anesthesia technology innovations. For example, a closed-loop control algorithm to maintain a target depth of anesthesia or blood pressure can be rapidly prototyped and evaluated (either in-silico or hardware-in-the-loop) if implemented on an open health platform (OHP) where the interaction of algorithms and candidate infusion pump and monitors is managed.

OHPs need to demonstrate acceptable safety, security, and reliability when they are used to compose medical systems, especially when algorithms, devices, and sensors are from different vendors. As cybersecurity concerns have grown in healthcare, securing these platforms has become one of the deciding factors for their adoption.

We developed an OHP complying with the Integrated Clinical Environment (ICE) architecture defined in the AAMI 2700-1 standard [1]. It incorporates a rich library of device interfaces, simulated devices, example clinical algorithms, and utility apps to support R&D of interoperable medical systems [2]. Within OpenICE, medical devices, clinical and utility apps and other supporting equipment (such as a database for data logging) communicate with each other using the RTI Connext DDS network middleware [3] in which entities in the system communicate in a publish-subscribe paradigm - entities publish their data to pre-specified topics while consumers of such data subscribe to these topics to receive the published data.

Methods: Even though RTI's latest Connext DDS middleware (version 6.0.1) provides a collection of security capabilities at the network layer, such as encryption of data communication, we have established a holistic approach to security controls at the platform level for authentication, authorization, and access control of entities (i.e., devices, apps, users, and equipment) with the intention of generalizing this knowledge to assess other OHPs.

Our approach implements security controls for the following entities:
User Security. A mechanism has been added to lock the screen after user inactivity for a configurable period and re-authenticate when the user logs back in, including requirements accommodating multiple caregivers and handoffs.
Device Security. Devices with security credentials issued by trusted Certification Authorities are allowed to connect to the system. Medical devices need to present permission files issued by CAs that prescribe the security keys to decrypt the DDS network communication and the topics to which the devices can publish or subscribe. Attempts to communicate data beyond the permission files will be rejected by the DDS middleware. This achieves topic-level, fine-grained access control of connected devices.
App Security. We implemented an anti-compromise check of apps during system startup, where the Message Authorization Code (MAC) of each app is checked for potential compromise. A mismatch between an app's JAR file and its MAC will prevent the app from being launched.

Conclusion: We were able to use secure OpenICE as the basis of a DDS reference implementation of JHU APL Medical Device Interoperability Reference Architecture [4] and we will be using it to pilot remote ventilator control and closed-loop sedation systems. The secured OpenICE platform is freely available for public use [5].

References:

1. AAMI, AAMI 2700-1 Medical Devices and Medical Systems - Essential safety and performance requirements for equipment comprising the patient-centric integrated clinical environment (ICE) - Part 1: General requirements and conceptual model, 2019.
2. J. Plourde, D. Arney, J. M. Goldman, OpenICE: an open, interoperable platform for medical cyber-physical systems, 2014 ACM/IEEE International Conference on Cyber-Physical Systems, 221-221, 2014.
3. https://community.rti.com/documentation/rti-connext-dds-601
4. https://secwww.jhuapl.edu/mdira
5. https://github.com/mdpnp/mdpnp/releases/tag/SecureOpenICE

This work was supported under the U.S. Army Medical Research Acquisition Activity Contract W81XWH-17-C-0251. The views, opinions and/or findings contained in this paper are those of the authors and should not be construed as an official Department of the Army position, policy or decision unless so designated by other documentation.