RSA Conference 2016

Learning Labs

Securing the Industrial IoT: A Deep Dive into the Future

Post-Conference Summary

Hamed Soroush, Ph.D

Senior Research Security Engineer, Real-Time Innovations (RTI)

@HamedSoroush

Gerardo Pardo, Ph.D

Chief Technology Officer, Real-Time Innovations (RTI)

Rose Wahlin

Principal Software Engineer, Real-Time Innovations (RTI)

@ProjectDerby

rti Your systems. Working as one.

Introduction

The landscape of modern medicine is being dramatically changed by the integration of computing devices and health care. This change brings the promise and the challenge of next-generation integrated medical systems that will interoperate efficiently, safely, and securely. Such integration is anticipated to significantly lower the rate of preventable medical errors, now the third leading cause of death in the U.S., by providing improved patient outcomes at lower costs. Such improvement includes support for automatic diagnosis, real-time checking of medication interaction, and reduced false alarms.

Unfortunately, out of the many communication standards that have been proposed for interoperable medical devices and information systems, few include sufficiently comprehensive or flexible security mechanisms to meet current and future safety needs. There are significant gaps between required security properties and those that can be fulfilled even by combinations of currently standardized protocols. Safety considerations in these standardization efforts are effectively incomplete due to a lack of appropriate security analysis.

DDS is a communications API and an interoperability standard that provides a data-centric publish-subscribe model for integrating loosely coupled real-time distributed systems. A key feature of DDS is that it is data-centric in the sense that it separates state management and data distribution from application logic and supports discoverable data models. This exposes the data model to the communication middleware, enabling the DDS middleware to examine and optimize the performance of data movement within the system. In order to customize run-time behavior and achieve a desired performance profile, DDS allows publishing and subscribing entities to express several quality-of-service (QoS) parameters. The offered versus requested QoS requirements of the participating entities are matched before any communication can proceed. The standard DDS QoS parameters include durability, reliability, deadline, resource limits, ownership, liveliness, etc.

DDS Security provides support for authentication, authorization, access control, confidentiality, integrity, and nonrepudiation for all the data sent over DDS. Moreover, it provides a security auditing capability to evaluate the overall communication state. Secure DDS provides fine-grained access control over the messages and sub-messages that include both data and metadata. It is designed to handle scalable deployment scenarios, specifically the one-to-many distribution of encrypted information, while maintaining real-time quality-of-service.

DDS Security is designed with performance, scalability, robustness, availability, and data-centricity in mind. It substantially facilitates the set of security properties that have been identified for interoperable medical systems. While DDS Security specification may not meet all the fundamental goals of medical connectivity, the standard continuously evolves to bridge the gap between the current state and suitability for medical interoperability. RTI sees this effort as an initial step towards providing general security architectures for interoperable medical systems for each care environment.

RTI delivered a Learning Lab at RSA Conference 2016 to overview recent developments in IIoT secure data connectivity standards, including DDS, explore security threats to the medical IoT and build a secure application that monitors a patient in a demo environment.

Hands-on Lab

Emerging Threats: An Infusion Pump Attack Example

In exploring the infusion pump attack, Learning Lab participants learned that an intruder could deliberately increase the dosage of medication delivered to a patient and alter the pump display screen to indicate that the delivered dose was safe. The attack could be masqueraded as a “medical error”. The intruder would not need a physical access to the pump because its communication module is connected to the hospital network, which is connected to the Internet. If the intruder finds a way to compromise the hospital network, connected medical equipment and applications are vulnerable.

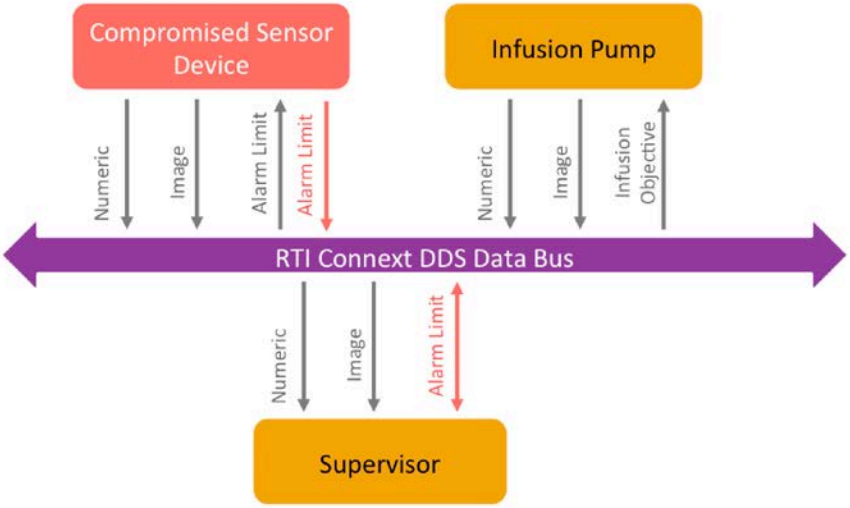
Exercises

The objective of the exercise was to demonstrate fine-grained capabilities of the DDS Secure standard that can be used to implement additional security measures to ensure patient safety in the event that the hospital network is partially or fully compromised.

The provided exercises covered three scenarios:

- Understanding the system with no security
- Securing the system with transport-level security
- Securing the system with fine-grained access control

The Attack scenario:



The Alarm Limit was what we attacked. We compromised a device and made it change the alarm limits for the entire system. This made the patient's healthy vital signs appear as though there was a medical emergency, shutting down their morphine dosage and setting off alarms. The opposite scenario – where a compromised medical device could suppress a valid alarm – is even more frightening.

Lessons learned:

- The Industrial IoT (IIoT) encompasses critical national infrastructure, including the power grid, hospitals, transportation infrastructure and manufacturing. Securing these systems is essential for safety, economic and privacy reasons. This is particularly challenging because security cannot come at the expense of reliability or the real-time performance required for controlling physical-world processes. Even brief unplanned outages can be disastrous.
- The Industrial IoT – such as medical IoT – is much more demanding than the consumer IoT, and breaches are more consequential.
- In the IIoT the volume of data is larger and the systems require protecting real-time data in motion. This task gets increasingly harder as the systems grow in size and complexity.
- Transport-level security does not prevent an intruder from attacking the system and modifying data they should not be allowed to modify.
- The DDS Security standard provides a mechanism for explicitly defining fine-grained permissions that prevent an application from writing (or reading) something it is not entitled to. Thanks to this mechanism, even when the hospital network and some applications are compromised, the permissions can still be enforced.

Learn More

- Current DDS Security Specification Draft:
  - http://www.omg.org/spec/DDS-SECURITY/
- To learn about RTI, visit:
  - www.rti.com
  - https://community.rti.com/
  - http://info.rti.com/ddssecure
- Industrial Internet Consortium:
  - http://www.iiconsortium.org/
  - http://www.iiconsortium.org/connected-care.htm
- Object Management Group's DDS Portal:
  - http://portal.omg.org/dds

Contact Us

Email: RSA-team@rti.com