Device Authentication for the Medical Device Coordination Framework

Carlos Salazar and Eugene Vasserman
Kansas State University

Abstract (presentation)

Medical devices have a history of being implemented as stand-alone units. Most devices currently used in clinical environments stay true to this paradigm and even when a device manufacturer has implemented some interoperability features, they are not designed to work with other devices/software from other manufacturers, and connectivity is typically only used for passively logging device data. Simply put, medical devices do not play well with each other. As a result, there is increasing movement within the clinical and medical device community toward a "system of systems" approach for medical devices, similar to other safety-critical areas such as power generation and aviation. Integrated medical systems can provide numerous benefits such as improved patient safety through "smart" alarms that gather patient data from multiple sources, and automated clinical workflows that automatically reduce common medical errors. The exploration of this idea has lead to the creation of the emerging Integrated Clinical Environment (ICE) standard and the Medical Device Coordination Framework (MDCF) project. The MDCF is a framework for coordinating medical devices and is currently the most complete implementation of the ICE standard. However, there are serious safety and security concerns in the "system of systems" paradigm, given the importance of completeness, correctness, and privacy of patients' medical data. An attacker who can alter data or prevent its transmission could seriously harm patients. Therefore, we need to ensure that only authenticated devices can connect.

This paper describes the implementation of a flexible device authentication framework within the existing MDCF. To accomplish this, we located the points within the MDCF device connection process at which authentication must occur and inserted, "hooks" where modular security providers can attach. This architecture allows arbitrary protocols to be implemented as drop-in modules in the future. For added flexibility, the MDCF can be configured via a local policy to either require authentication or not (accept to reject unauthenticated devices). The authentication providers are entirely self-contained, incorporating all protocol logic and reporting the failure or success of device authentication to the rest of the MDCF, in the latter case also returning negotiated cryptographic material for later usage in encrypted communication channels. All providers implement common interfaces and are lazily instantiated by the MDCF as requested by the device ("call-by-name"). The currently implemented proof of concept "null" authentication provider is similar to IPsec null encryption -- it does not provide cryptographically sound authentication. We evaluated the performance of this null provider (giving us the pure overhead of the authentication system and not a particular authentication algorithm) using various device connection rates and in various MDCF configurations -- prior to authentication implementation, with authentication but set to accept all devices, and with authentication required to connect.