Medical Device Security—Beyond the Password

Alan Grau, President and Cofounder, Icon Labs

The FDA and Department of Homeland Security recently issued an alert urging medical device makers and medical facilities to upgrade security protections to protect against potential cyber threats. This came in response to an ICS-CERT publication of a list of more than 300 devices with hard coded passwords.

Clearly hard-coded passwords are a huge and unacceptable security loophole but the ultimate solution (and problem) runs much deeper than just ensuring the devices have user configurable passwords. The fact that the only security provisions that many of these devices have is basic password-based authentication demonstrates just how little attention has been given to device security.

Upgrading these devices to use a user-defined password, and to require the use of a strong password (i.e., at a minimum, an eight character long password that includes a number, an upper case letter, a lower case letter, and a special character) is a quick and important patch. While important, it still falls far short of providing the type of security that is truly required to reliably protect against today’s cyber threats.

Security Requirements for Medical Devices
A security solution for medical devices must provide the ability to control communications, detect and report attacks or suspicious traffic patterns, and allow centralized control of security policies. These capabilities would provide medical devices with a much higher level of security than password only security and protect them from the majority of cyber-attacks.

The security solution must provide:

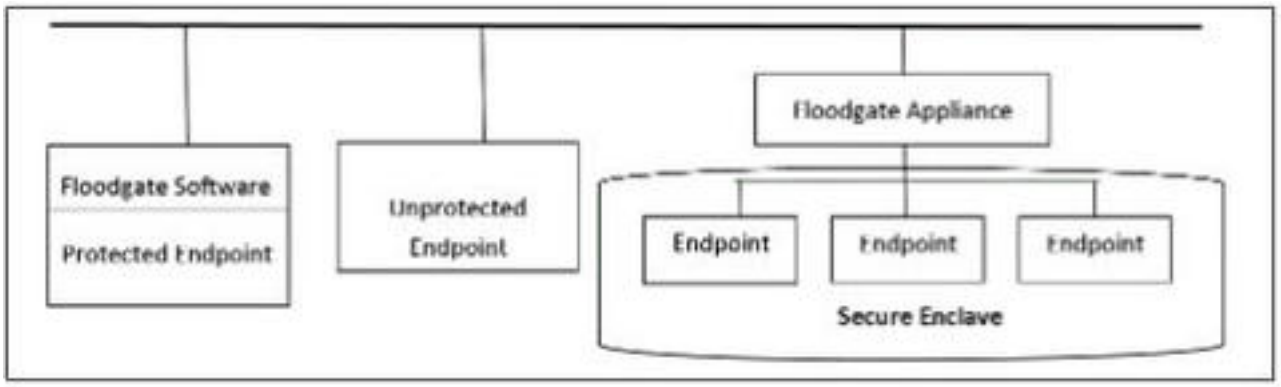
- Control of the packets processed by the device
- Protection from hackers and cyber-attacks which may be launched from the Internet, inside the corporate network, or WiFi networks
- Protection from DoS attacks and packet floods
- Ability to detect and report traffic abnormalities, probes or attacks
- Ability to manage and control changes to filtering policies

Securing Legacy Devices—The ‘Bump-in-the-Wire’ Solution

As shown by the ICS-CERT report, many legacy medical devices and systems that are already in place have been manufactured with inadequate security. Upgrading these devices to improve security requires the device manufacturer develop a newer software or firmware version with improved security. Once the new version is available the devices can be upgraded to provide enhanced security.

Unfortunately, the upgrade process may be difficult and expensive. Some devices cannot be upgraded without being returned to the factory to be updated In some cases the manufacturer may no longer support the device, or may be out of business. Replacing these devices is often simply too expensive to be an option and newer devices may not yet be available with improved security.

For medical equipment and systems that cannot be easily or affordably replaced or upgraded, a “bump-in-the-wire” appliance solution provides the required security. This type of solution can protect legacy devices by creating a “secure enclave” in which these devices can operate. Only trusted devices should be deployed within the secure enclave. These devices can freely communicate with each other; however - communication outside of the enclave is controlled for security. The “bump-in-the-wire” appliance provides security by enforcing communication policies, ensuring that only valid communication is allowed with the endpoints within the secure enclave.



By limiting communication to the secure enclave, the bump-in-the-wire appliance will:

- Prevent probes and hacking drones from discovering endpoints. Hackers and automated drones send out ping requests or other messages to a range of IP addresses looking for responses. The security appliance drops these requests making the endpoints undiscoverable.
- Prevent access from unauthorized machines. Many specialized medical devices only need to communicate with a few known, trusted hosts. Enforcing these communication restrictions prevents communication with unauthorized machines. If a hacker cannot communicate with the endpoint, they cannot compromise it.
- Close security loopholes. Many cyber-attacks utilize services on an endpoint that are not required for fixed function devices. Blocking unused ports and protocols closes these commonly exploited security loopholes.

Securing New Devices—The Integrated Solution

For new devices, enhanced security can be built into the device itself. This is the same approach taken with PCs today. While a PC may sit behind a firewall on a home or corporate network, it also has a built in firewall and other security software.

Building protection into the device itself provides another security layer and the devices are no longer depending on the corporate firewall as their sole layer of security. An integrated firewall provides a basic, but critical level of security for a networked device by controlling which packets are processed by the device. The embedded firewall resides on the device and is integrated into the communication stack of the device. The communication requirements of the device are encoded into a set of policies defining allowable communication. The firewall enforces these polices, limiting communication to the required IP address, ports and protocols specified in the policies.

Since each packet or message received by the device is filtered by the firewall before being passed from the protocol stack to the application, many attacks are blocked before a connection is even established, thereby providing a simple, yet effective layer of protection missing from most devices.

Blocking Attacks with a Firewall

In a system without a firewall, a hacker may attempt to remotely access the device using default passwords, dictionary attacks or stolen passwords. Such attacks are often automated, allowing a huge number of attempts to break the system's password. However, by protecting the system with an embedded firewall configured with a whitelist of trusted hosts, can effectively block such attacks. The firewall blocks packets from the hacker before the packet is passed to the application to attempt to login.

Rules-based filtering provides a simple and effective tool to enforce communication polices, blocking communication from a non-trusted IP address and isolating the device from attack.

Summary

Many of today's modern medical devices and systems are complex connected embedded computers charged with performing critical functions. Firewalls provide the cornerstone of security both for PCs and for home or corporate networks. Including a firewall in new medical devices themselves, or by placing several devices within a secure enclave, provide a simple and effective layer of security. These firewalls provide protection even if the corporate firewall and security has been breached. A small embedded firewall, such as Floodgate from Icon Labs can be used to protect devices from a wide range of cyber-attacks. By controlling who the device talks to, most attacks can be blocked before a connection is even established.

For more information, visit www.iconlabs.com [1].

Links:
[1] http://www.iconlabs.com