Security Requirements for Embedded Devices – What is Really Needed?

By Alan Grau, Icon Labs

alan.grau@iconlabs.com  www.iconlabs.com

Recently there have been a number of well documented attacks on embedded devices ranging from hacked vehicle anti-theft and control systems to hijacked printers that sent copies of documents to the hacker’s computer. Many embedded devices include password protected logins and encrypted protocols such as SSH or SSL, but this is not sufficient. If these methods were enough, we would not be reading about security breaches in the media.

Use of multiple layers of protection is the driving principle for enterprise security. It includes firewalls, authentication/encryption, security protocols and intrusion detection/intrusion prevention systems. These are well established and proven security principles. Despite this, firewalls are virtually absent in embedded systems and most embedded devices rely on simple password authentication and security protocols. This is based on assumptions that embedded devices are not attractive targets to hackers, embedded devices are not vulnerable to attacks, or authentication and encryption provide adequate protection for embedded devices. These assumptions are no longer valid; the number and sophistication of attacks against embedded devices continues to rise and greater security measures are needed.

Cybersecurity has been a critical focus for large enterprises for 25 plus years, whereas it has only recently become a focus for most engineers building embedded computing devices. “Experience is the best teacher, but the tuition is high”, or so goes the saying. Rather than learn all the lessons by experience, embedded engineers can take a page from the enterprise security playbook.

Embedded Security Challenges

Embedded devices are very different from standard PCs. They are fixed function devices designed specifically to perform a specialized task. Many of them are designed using a specialized operating system such as VxWorks, MQX or Integrity, or a stripped down version of Linux. Installing new software on the system in the field either requires a specialized upgrade process or is simply not supported. In most cases, these devices are optimized to minimize processing cycles and memory usage and do not have a lot of extra processing resources available.
As a result, standard PC security solutions won’t solve the challenges of embedded devices. In fact, given the specialized nature of embedded systems, PC security solutions won’t even run on most embedded devices.

Other challenges for embedded device security include:

1. Critical functionality: Embedded devices control transportation infrastructure, the utility grids, communication systems and many other capabilities modern society relies upon. Interruption of these capabilities by a cyber-attack could have catastrophic consequences.

2. Replication: Once designed and built, embedded devices are mass produced. There may be thousands to millions of identical devices. If a hacker is able to build a successful attack against one of these devices, the attack can be replicated across all devices.

3. Security assumptions: Many embedded engineers have long assumed that embedded devices are not targets for hackers. These assumptions are based on outdated assumptions including the belief in security by obscurity. As a result, security is often not considered a critical priority for embedded designs. Today’s embedded design projects are often including security for the first time and do not have experience and previous security projects to build upon.

4. Not easily patched: Most embedded devices are not easily upgraded. Once they are deployed, they will run the software that was installed at the factory. Any remote software update capability needs to be designed into the device to allow security updates. The specialized operating systems used to build embedded devices may not have automated capabilities that allow easy updates to of the device firmware to ensure security capabilities are frequently updated.

5. Long life cycle: The life cycle for embedded devices is typically much longer than for PCs or consumer devices. Devices may be in the field for 15 or even 20 years. Building a device today that will stand up to the security requirements of the next two decades is a tremendous challenge.

6. Proprietary/industry specific protocols: Embedded devices use specialized protocols that are not recognized and protected by enterprise security tools. Enterprise firewalls and intrusion detection system are designed to protect against enterprise specific threats, not attacks against industrial protocols.

7. Deployed outside of enterprise security perimeter: Many embedded devices are mobile or are deployed in the field. As a result, these devices may be directly connected to the Internet with none of the protections found in a corporate environment.

Cyber warfare and the motivated hacker

The level of security required for an embedded device varies dramatically depending upon the function of the device. Rather than asking if the device is secure, the OEMs should be asking if

Icon Labs Whitepaper
Copyright Icon Laboratories, Inc. 2014
www.iconlabs.com
the device is secure enough. A military communication satellite or nuclear power plant control system clearly needs a very different level of security than a water softener equipped with Internet connections for remote diagnostics and automated reordering of salt.

If there is one lesson to be learned from StuxNet it is that hacking is not just the domain of bored teenagers, hacking drones or even the small groups of motivated hackers. When the stakes are high enough, Cyberattacks are multi-phased, multi-year efforts carried out by large, well-funded teams of hackers.

We are no longer talking about protecting a device from just malformed IP packets or DoS packet floods. Hacking organizations invest significant resources in gathering information on the device or devices they wish to attack. They hack corporate networks to steal design information. If possible they obtain target devices they wish to hack and attempt to reverse engineer the device and use it to test out possible attacks. It’s likely that they have attempted to obtain design information on networks and devices using other methods of espionage including attempts to hire engineers involved in designing the devices they wish to hack. Any OEM building a device that would be a prime target for terrorists or cyber warfare should consider how to protect the device from attack from a group led by a member of their own engineering team, or from someone with detailed knowledge of the inner workings of the RTOS, or other vendor solutions included in your product.

**Security requirements for embedded devices**

A security solution for embedded devices must ensure the device firmware has not been tampered with, secure the data stored by the device, secure communication and protect the device from cyber-attacks. This can only be achieved by including security in the early stages of design.

There is no one one-size fits all security solution for embedded device. Security requirements must take into consideration the cost of a security failure (economic, environmental, social, etc.), the risk of attack, available attack vectors, and the cost of implementing a security solution. Features that need to be considered are:

<table>
<thead>
<tr>
<th>Security feature</th>
<th>Implementation in embedded devices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure boot</td>
<td>Achieved using cryptographically signed code from the manufacturer along with hardware support to verify code is authenticated. This ensures that the firmware has not been tampered with.</td>
</tr>
<tr>
<td>Secure code updates</td>
<td>A method of secure code updates ensure that the code on the device can be updated for bug fixes, security patches, etc. Use of signed code (secure boot) ensures that malicious code cannot be introduced into the system.</td>
</tr>
<tr>
<td>Data Security</td>
<td>Prevent unauthorized access to the device, encrypted data storage and/or encrypted communication.</td>
</tr>
<tr>
<td>Authentication</td>
<td>All communication with the device should be authenticated using strong passwords (at a minimum) or use of an authentication protocol such as Kerberos.</td>
</tr>
</tbody>
</table>
Secure communication

Communication to/from the device needs to be secured using encrypted communication (SSH, SSL, etc.). Care must be taken to avoid the use of insecure encryption algorithms. I.e., 40 bit encryption keys that were once state-of-the-art are no longer considered secure.

Protection against cyber attacks

Embedded firewalls provide a critical layer of protection against attacks. A firewall can limit communication to only known, trusted hosts, blocking hackers before they can even launch an attack. A layer of defense to protect against common attacks such as packet flood attacks, buffer overflow attacks and known protocol exploits. A firewall can implement many of these protections, but some must be built into the embedded applications.

Intrusion detection & security monitoring

Existing embedded devices can be attacked and no one would even know they are being attacked. A hacker could execute thousands or millions of invalid login attempts without any knowledge of an attack having taken place. Embedded devices must detect and report invalid login attempts and other potentially malicious activities. NOTE: Monitoring requirements for embedded devices are very different than enterprise requirements. The IDS requirements for embedded devices will depend upon the protocols supported by the device.

Embedded security management

Integration with a security management system allows security policies to be updated to mitigate against known threats.

Device tampering detection

Some new processor/board designs include device tamper detection capabilities. They provide the ability to detect that the seal on the device enclosure has been broken, indicate that someone may be attempting to tamper with the device.

**Integrating security into the device**

Building protection into the device itself provides a critical security layer - the devices are no longer depending on the corporate firewall as their sole layer of security. In addition, the security can be customized to the needs of the device.

Security needs to be considered early in the design of a new device or system. Support for secure boot or device tamper detection requires specific hardware capabilities. Since hardware is typically selected early in the design phase, this capability must be considered very early in the process. Since many embedded devices are deployed outside of the standard enterprise security perimeter, it is critical that security be included in the device itself.

**Summary**

Many of today’s modern embedded devices and systems are complex connected computers charged with performing critical functions. Including security in these devices is a critical design task. Security features must be considered early in the design process to ensure the device is protected from the advanced cyber-threats they will be facing.

*Alan Grau is the President and cofounder of Icon Labs, a leading provider of security solutions for embedded devices. You can reach him at alan.grau@iconlabs.com*

---

Icon Labs Whitepaper
Copyright Icon Laboratories, Inc. 2014

www.iconlabs.com