E-Guide

THE BIGGEST SECURITY CHALLENGES FOR EMBEDDED AND MOBILE DEVELOPMENT AMID THE RISE OF IOT
As more devices become Internet-enabled, experts fear an embedded systems security worst-case scenario for enterprises, many of which are unaware of the risks or unable to mitigate them.

This expert e-guide explores the major challenges that complicate embedded and mobile security. Ahead, we discuss why security for embedded systems must begin during the development stage and reveal the key considerations to keep in mind when developing security measures for mobile devices.
EMBEDDED SYSTEMS SECURITY A GROWING CONCERN AMID RISE OF IOT

Some fear the rapid increase in nontraditional Internet-enabled devices could mean more potential enterprise entry points for attackers. Many of these devices fall into the category of embedded systems, and experts in that field fear a worst-case security scenario for organizations because of embedded technology’s troubling security history.

Traditionally, an embedded system device is a type of appliance with a minimal chipset and a “lite” version of an operating system, often Linux. The most popular examples for enterprise would be USB sticks, which were used to initially load the infamous Stuxnet malware, networked printers, and even now hard drive firmware, which is where the recently revealed Equation spyware lived.

However, the devices in that category are expanding rapidly with the arrival of the Internet of Things (IoT), which bestows networking capability to a broad spectrum of devices that have never had that capability before, such as office appliances like thermostats and refrigerators. As a result, enterprises may soon
find they have a whole host of new attack points on their networks, but experts aren’t sure that the new generation of embedded devices has overcome the security flaws of their predecessors.

According to Benjamin Jun, CTO of San Francisco-based security consultancy firm Chosen Plaintext Partners, embedded systems have historically used a lot of proprietary components and not shared much common circuitry with other systems, meaning when bugs were found, they were less likely to be fixed due to cost or resource restraints.

Modern embedded systems have moved away from this paradigm by sharing some of the same internal systems components, such as ARM chips, with other popular mobile devices, Jun said, but embedded devices must often be supported for years or even decades, which causes a new set of problems.

“Mobile phones iterate quickly, but embedded systems tend to live much longer,” Jun said. “The process of rapid obsolescence in mobile doesn’t translate to devices that are expected to last 10 to 20 years. The teams that debug these things move on, so the security process is limited.”

Beyond the level of support that embedded systems need, Jun said that even when there are software updates available, enterprises may overlook these devices because the cost per node is much lower in terms of support and
upgrading.

“Laptop costs are pretty high, but those costs can be justified, because you have the idea that productivity will rise with more laptops. But, what about printers, or smart thermostats?” Jun said. “How much are you going to spend to secure something where the incremental value is assumed to be low?”

According to Jun, one of the more overlooked embedded threats are VoIP conference phones and other devices with microphones, where the mic can be turned on to record sensitive information without notice.

But that’s just the beginning, Jun added. The prevalence of the IoT will mean that enterprises will face security concerns related to a much wider variety of devices. This means that in addition to devices like USB sticks and printers, wearables and other cutting-edge devices may find their way onto corporate networks, often without built-in security controls.

Similarly, it also means new risks from devices like smart thermostats or refrigerators, where the responsibility for support can be blurry, according to Jun, because they may be owned by a building manager and not under the purview of the corporate IT department.
SECURE DESIGN

Experts noted that only time will tell if new embedded devices will be better supported over the long term than past embedded systems have been, but the key to secure embedded devices is in securely designing them from the beginning.

“You have to design the hardware and firmware from the ground up to prevent access from malware or physical tampering,” said Ken Jones, vice president of engineering and product management at IronKey, a division of Oakdale, Minn.-based Imation Inc. “It’s extremely common that firmware can be updated in the field to fix bugs and security vulnerabilities, but once you have that process and don’t think it through fully, you’ve opened a Pandora’s box of problems.”

According to Jones, secure design includes protection against physical tampering of the device, encryption and firmware digital signatures.

Many older embedded systems require updates be performed in the field, said Jones, so enterprises should prefer systems that use digitally signed firmware that is not only checked prior to installation, but also before it runs for the first time. This can be difficult though, Jones noted, so organizations may need to crack down on embedded device policy.
“From an enterprise perspective, it is all about what you allow to connect to your network, using endpoint protection that can block everything except whitelisted products,” Jones said. “It behooves companies to be very restrictive about what can be connected. I think we’ll see a lockdown on what will be allowed on the network.”

Alexander Damisch, senior director of IoT Solutions at Alameda, Calif.-based Wind River Systems Inc., agreed with this assessment. Damisch recommended that enterprises securely design their infrastructure, which would include requiring devices be authenticated before sending or receiving data on the corporate network; because it can be difficult to detect malware in embedded firmware, monitoring traffic is key.

“This would mean that IT takes over personal devices to an extent, which people don’t like,” said Damisch, “but the other option is that they simply don’t get access. The key is that it isn’t personal blocking, the system is designed that way,” which Damisch said could help employees accept the practice easier.

Damisch also advocated isolating vulnerable embedded systems behind gateways or on a virtual system, which he said is often a more cost-effective option, and allows for updating gateway rules to stop new threats where embedded systems may falter, because they aren’t designed to be updated that often.
“Redesigning is difficult, so you find the weak point and either put it on the virtual system, or put gateways in front so all traffic is monitored and encrypted,” Damisch said. “Security is something that starts with the development process.”

**WHAT ARE MOBILE DEVELOPMENT BEST PRACTICES FOR APP SECURITY?**

Answering your question regarding mobile development best practices is tricky, given all of the variables. With all applications, including traditional client/server and Web applications, developers have to consider things such as:

- What features must be available to the user? This often defines many of the security aspects.
- How can rich functionality be balanced with minimal attack surface?
- What information is being input and processed? Again, this has big security implications.

Then, of course, there are all the security “best practice” documents such
as the OWASP Top 10 Project and SANS Top 25 that cover input validation, user authentication, session management and the like.

In many ways, mobile can be more simplistic because functionality is often limited. That said, when considering additional security measures for mobile devices, you need to be thinking about the following things:

How can information be input into the application? There aren’t as many automated tools for fuzzing and injection on mobile as there are for Web applications, but you still need to ensure this information is valid.

How can information be extracted from the application? This is often an afterthought for mobile applications. However, the forensics artifacts that are accessible when connecting to a phone or tablet in device firmware upgrade mode, using tools such as Elcomsoft iOS Forensic Toolkit and Oxygen Forensic Suite, can be very eye-opening.

How is information transmitted? Encrypted transmission is front and center for traditional applications, but it’s often overlooked with mobile. I’ve seen plenty of applications that transmit everything in clear text HTTP.

Where will the information ultimately be transmitted to or stored indefinitely, and how will it be protected? This has security and legal implications -- especially when unsecured mobile devices and third-party cloud applications
are involved.

Getting back to the original question, I’d say the single most important application security practice for mobile developers is to see the big picture. Step back and look at how everything will operate and interact to make sure you’re covering all your bases. Otherwise, you’re putting everything at risk, and that’s not a position you want to be in.
THE BIGGEST SECURITY CHALLENGES FOR EMBEDDED AND MOBILE DEVELOPMENT AMID THE RISE OF IOT

FREE RESOURCES FOR TECHNOLOGY PROFESSIONALS
TechTarget publishes targeted technology media that address your need for information and resources for researching products, developing strategy and making cost-effective purchase decisions. Our network of technology-specific Web sites gives you access to industry experts, independent content and analysis and the Web’s largest library of vendor-provided white papers, webcasts, podcasts, videos, virtual trade shows, research reports and more —drawing on the rich R&D resources of technology providers to address market trends, challenges and solutions. Our live events and virtual seminars give you access to vendor neutral, expert commentary and advice on the issues and challenges you face daily. Our social community IT Knowledge Exchange allows you to share real world information in real time with peers and experts.

WHAT MAKES TECHTARGET UNIQUE?
TechTarget is squarely focused on the enterprise IT space. Our team of editors and network of industry experts provide the richest, most relevant content to IT professionals and management. We leverage the immediacy of the Web, the networking and face-to-face opportunities of events and virtual events, and the ability to interact with peers—all to create compelling and actionable information for enterprise IT professionals across all industries and markets.