WIND™

AN INTEL COMPANY

SECURING DEVICES IN THE INTERNET OF THINGS

WHEN IT MATTERS, IT RUNS ON WIND RIVER

EXECUTIVE SUMMARY

Security breaches at the device level in the Internet of Things (IoT) can have severe consequences, including steep financial losses, damage to credibility and trust, or even endangerment of human life. Several high-profile data compromises illustrate that large-scale breaches typically result from not one but multiple points of failure. Closing any one of these gaps can help mitigate a breach or at least minimize the damage. Yet designing security into devices poses different challenges from securing enterprise software or networks.

How can developers know how much security is "just enough" to protect a device without hindering performance? Based on a real-world case study, this paper explores the criteria for determining the security requirements of devices connected to IoT infrastructures. It also presents a flexible and scalable approach for implementing cost-effective security measures.

TABLE OF CONTENTS

SECURING THE POINT OF INTERACTION

Device security in the Internet of Things is of paramount importance. After all, devices are the "things" in IoT that actually perform the system function and generate the data the system relies on. They are often the points at which humans interact with the system. Securing devices is particularly problematic because they are vulnerable to both physical tampering and network-borne threats.

The consequences of a compromise can be severe. Large-scale consumer identity theft can destroy a commercial enterprise's reputation and credibility. A breach of a process controller on an industrial shop floor can cause costly downtime and safety hazards. And in the case of networked medical devices, a breach can put lives at risk.

When a large-scale breach of devices occurs, it is typically not the result of a single point of failure but a series of failures at multiple points of vulnerability. Closing the gap at any one of those points can go a long way toward preventing a breach altogether, or at least detecting an attack in progress and limiting the damage.

Developers need to address security at the device design phase, which requires identifying those potential vulnerabilities based on how and where the device will be used. There are a number of security measures device manufacturers can take. The challenge is determining how much or how little security is needed, and which measures will be most effective.

DESIGNING FOR "JUST ENOUGH" SECURITY

Designing security into devices for IoT applications poses different challenges from securing enterprise software or networks. Embedded devices generally have a small footprint, and computing resources are limited. Too much security functionality can hinder the performance of the device or the system and increase the overall cost of development. Yet too little can leave critical points unprotected. The trick is building "just enough" security to mitigate a breach—and the challenge for developers is figuring out how much is "just enough" (see Figure 1).

The answer depends on three key criteria:

1. **The environment in which the device will be deployed:** Is the device in a shopping mall, visible to thousands of people and at risk of tampering? Or is it behind locked doors in a secure facility? These contrasting scenarios raise different types of security considerations.
2. **How the device will connect and communicate:** How is the device connected to a network? Will it communicate over the air via a protocol such as ZigBee or Wi-Fi, which may necessitate some form of encryption? Is it behind a firewall? Is it connected to the public Internet or to a private intranet, where it would be less vulnerable to outside interference?
3. **The type of data the device is storing:** Is the device collecting sensitive data, such as personal financial or medical information? Or is it capturing less-sensitive information such as weather conditions? The latter case would likely require a lower level of security than the former.

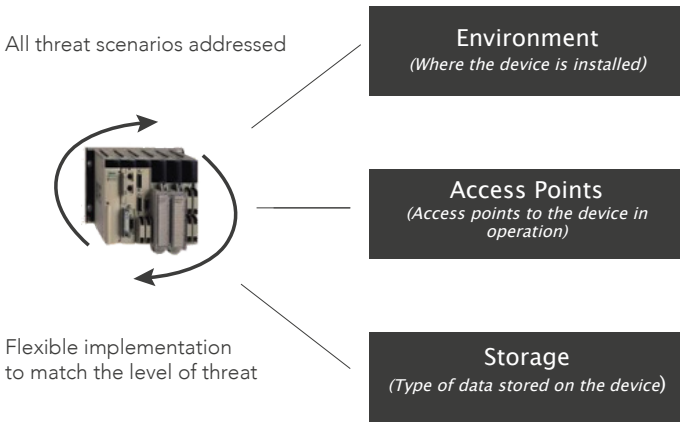

Figure 1: Three criteria for designing "just enough" security

The answers to these questions will help you determine the security features you need to integrate into the device's operating system to ensure the appropriate level of security. To give yourself optimal flexibility, it is helpful to use a real-time operating system that does not lock you into a set of prescribed security functions, but instead gives a menu of security functionality from which you can choose the features you need.

THE FOUR PILLARS OF DEVICE SECURITY

In addition to addressing these three key criteria for determining the right level of security, developers need to account for security at each phase of the device lifecycle (see Figure 2).

- **Design:** At the inception, it's critical to prevent the introduction of malicious code during the development process. Prevention measures might include signed binary delivery, assuring the authenticity and non-alteration of code, and developing on a software platform that has been certified under industrial security standards such as IEC 62443 and IEC 27034.
- **Execute:** In the execution phase, the goal is to establish a "root of trust" to prevent untrusted binaries from running, which in turn ensures that the right software is in place on the right hardware and that they trust each other. Establishing a root of trust might entail the use of secure boot technology and cryptographic key signatures to prevent unsigned code from executing.
- **Operate:** Multiple measures can be deployed to prevent malicious attacks in operation mode, including controls to prevent unauthorized access and securing networks using encryption.
- **Power down:** When the device is at rest, measures such as encrypted storage and secure data containers should be in place to prevent onboard data access.

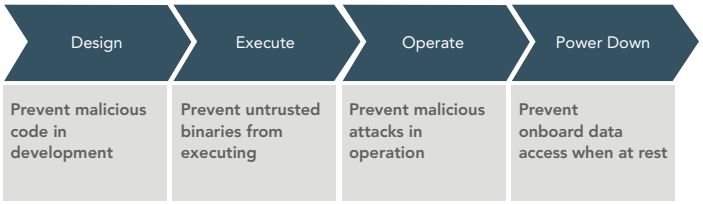

Figure 2. The four pillars of device security

CASE STUDY: IDENTITY THEFT AT THE POINT OF SALE

A major U.S. retailer suffered a security breach that resulted in the theft of millions of customer credit and debit card numbers. The breach actually compromised the point of sale (POS) devices that capture credit card information from customer transactions. How did this happen?

As shown in Figure 3, first the hackers obtained stolen credentials from a maintenance vendor that allowed access to the company's HVAC systems, which happened to be on the same network as the POS devices. This afforded the hackers virtually unfettered access to the company's cash registers.

Once inside, the hackers were able to reverse engineer the code running the POS devices. They then inserted malware that fooled the cash registers into running compromised binary code, allowing them to capture, extract, and transmit credit card data in real time as customers swiped their cards through the machines. The breach went undetected for weeks, and could potentially have gone on indefinitely had outside investigators not discovered it and alerted the retailer.

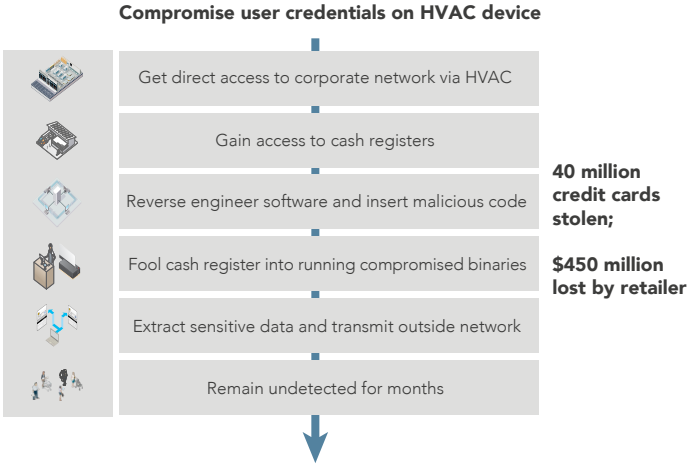

Figure 3. Case study: Identity theft at the point of sale

In deconstructing the incident, it became clear that it was not the result of a single failure, but rather a series of failures at various points throughout the system:

- The retailer had not isolated the HVAC system from the corporate network.
- The POS devices themselves were allowed to accept any type of connection.
- The code running the devices was not encrypted.
- There was no capability of screening for unknown or unrecognized code entering the system.
- The operating system had no access control.
- There was no overall health monitoring system.

Had the designers, developers, or operators of the system addressed even a few of these vulnerabilities, they might have been able to thwart the attack, or at least diminish its scale.

Lessons Learned: How to Prevent IoT Infrastructure Breaches

For each of the vulnerabilities cited in the case study, there is at least one countermeasure that could have been employed:

- System virtualization could have isolated the HVAC system from the corporate network. Isolating the system would have closed a fairly easy point of intrusion into the POS devices.
- Device firewalling might have prevented access to the POS devices, and the devices could have been programmed to accept only recognized, trusted code. This would have made it far more challenging for intruders to gain unauthorized access to the cash registers.
- Encrypting the application binaries running the devices would have made reverse engineering more difficult, if not impossible. With a root of trust in place, unrecognized and malicious binaries would not have been allowed to install themselves and could not have executed and fooled the cash registers.
- With proper access controls to sensitive processes, the operating system could have restricted specific tasks to specific users, preventing unauthorized users from extracting transaction data from the devices and blocking data from transmitting out of the network.
- Health monitoring might have enabled IT operators to detect anomalies in device behavior and improved chances of detection before the attack did serious damage.

Any one of these measures might have helped avert such a large-scale data security catastrophe, or at least minimized the damage.

And such preventive measures apply to any type of device that an attacker may want to target. Imagine a similar scenario with a network of medical or industrial devices, where the damages from a security breach could be far more serious than just financial or reputational.

The good news is that there are a number of ways to implement adequate security measures quickly and without harming device performance or slowing time-to-market.

A SCALABLE APPROACH TO DEVICE SECURITY

Security does not always require preventive measures at every point of vulnerability. Often it makes sense to start with a few measures to secure the device for deployment, then add security functionality as you progress through the device lifecycle. You can achieve this with an operating system that allows you to scale and add features over time as new threats become apparent.

Security Profile for VxWorks® is an example of a technology that allows this type of scalable approach. Security Profile provides a set of security capabilities designed for easy integration into the core VxWorks real-time operating system.

As shown in Figure 4, the profile enhances the VxWorks Core Platform with features that address each of the four pillars of security across the device lifecycle typical of any type of networked device (the same vulnerabilities exposed in the retail breach case study).

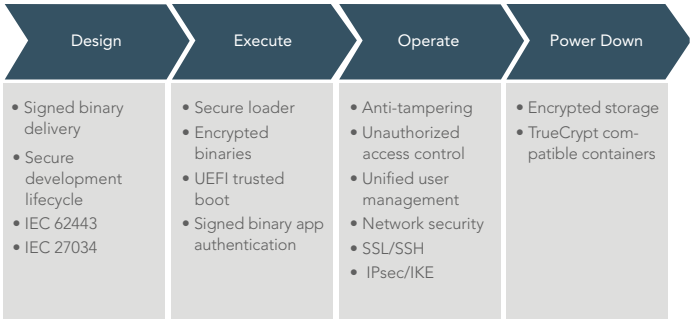

Figure 4. Security Profile for VxWorks addresses the four pillars of device security

With Security Profile, developers can select the security features they need based on their design criteria: deployment environment, communication and connectivity, and sensitivity of data stored. It enables them to implement blocking features at various levels to make it more difficult to break through security and breach the device. And it gives them the flexibility to add security functionality over time.

CONCLUSION

Security of devices has to be a prime concern of IoT system developers and device manufacturers, and needs to be addressed at the design stage. Building security into devices poses unique challenges—devices require "just enough" security to mitigate intrusions without compromising device performance.

Experience shows that attacks on devices typically exploit multiple points of vulnerability. Closing even a few of these gaps can mitigate the damage.

Fortunately, technology such as Security Profile allows developers to take a scalable approach to security, adding as much or as little as the device requires for its purposes, making it possible to control costs and deliver devices on schedule while reducing the risks of security breaches.

Wind River® works closely with IoT developers and device manufacturers to solve security issues while addressing their project and budget constraints. Contact us at windriver.com/company/contact to learn how Wind River experts and Security Profile for VxWorks can help you better protect your devices and data.

WIND
AN INTEL COMPANY

Wind River is a global leader in delivering software for the Internet of Things. The company's technology is found in more than 2 billion devices, backed by world-class professional services and customer support. Wind River delivers the software and expertise that enable the innovation and deployment of safe, secure, and reliable intelligent systems.