WIND™

AN INTEL COMPANY

OPEN FOR BUSINESS

Securing Open Source Solutions to Leverage Opportunities in the Internet of Things

By Philipp Michel, Field Application Engineer, Wind River

AGENTS OF CHANGE™

EXECUTIVE SUMMARY

The Internet of Things (IoT) is driving business transformation on an unprecedented scale, which in turn is driving demand from enterprises for solutions that enable them to accelerate adoption of IoT strategies. Developers are looking at all the options available to them to help meet that demand, chief among them open source software. Open source affords developers a high degree of flexibility in development and can improve device interoperability, which IoT functions frequently require.

But open source also raises a question. Security is a foundational requirement of IoT solutions. Can software with source code that is "open" and easily viewed really be secure enough for critical IoT gateways?

This question is based on a common but unfounded misconception. Open source is not inherently less secure than closed software. What makes any solution, open or closed, vulnerable to outside threats is the failure to build in and implement strong security functionality from the ground up. This white paper examines what is required to ensure the security of open source solutions so developers can build them with confidence and their customers can begin reaping the business advantages of IoT.

TABLE OF CONTENTS

CONNECTING TO TRANSFORM BUSINESSES

The ability to connect thousands of intelligent devices that can collect and transmit data among themselves and to central controllers has already demonstrated enormous business potential. In capital-intensive industries, IoT gives operators of plants and heavy machinery the opportunity to drive down costs by managing and monitoring equipment remotely, reducing energy consumption, and performing predictive maintenance. Data delivered from thousands of devices can be synthesized and analyzed for more precise and timely decision making. IoT provides the infrastructure and the intelligence for smart buildings, smart energy, smart cars, and other smart applications that are emerging rapidly.

Perhaps even more compelling is the emergence of new business models made possible by IoT. Chief among these is the ability of equipment manufacturers to lease equipment on a subscription basis to generate steady revenue instead of selling it outright, which also benefits the user by turning a capital expense into an operating expense. Another opportunity companies are exploring is the ability to repackage and sell the data that their field assets are generating.

OPEN SOURCE IN IOT

In a typical IoT configuration, data travels back and forth from networked devices and sensors to cloud-based platforms and applications via a gateway. The gateway makes it possible and far more efficient to collect data inputs from hundreds or thousands of devices, as well as connect previously standalone legacy devices to an intelligent network.

As IoT has advanced, developers have increasingly turned to open source technologies to build solutions. Open source gives developers more flexibility by freeing them from being locked into a proprietary vendor's standards. It offers practical benefits for IoT applications, too. Interoperability—enabling disparate systems to work together—is a key factor in many IoT functions. Open standards support interoperability. Moreover, the cloud-computing server systems that run IoT solutions are increasingly built on open source Linux-based operating systems.

At the same time, security from intrusion is critical to the reliable functioning of an IoT solution, to the data it collects, and to the safety of its users. The question thus arises: Is open source inherently less secure than proprietary software? The logic behind the question is that in open source, the source code is plainly visible and therefore more vulnerable to tampering. IT security experts dispute this idea, however, pointing out that hackers do not use the source code when trying to break into a system. On balance, open source is neither less nor more secure than proprietary software. What makes either vulnerable in an IoT solution is the lack of strong built-in security functionality or the failure to implement security features.

A study by the Open Web Application Security Project found that most security threats arise from insecure web, cloud, or mobile interfaces; insecure network services; weak authentication and authorization protocols; lack of encryption; and other factors outside the software itself. These issues can and should be addressed in the design and development process.

OPEN SOURCE ESSENTIAL SECURITY ELEMENTS

One important lesson in the evolution of IT security is that there is no silver bullet to stop increasingly sophisticated attacks. Security is achieved through multiple layers of protection designed into gateways. In an open source solution, the layers are built up from the operating system level:

- **Secure boot**: Establishing a "root of trust" when a system is initially booted through a sequence of steps to validate the integrity of a downloaded Linux kernel by verifying its cryptographic signature
- **Application integrity measurement:** Implementing an integrity measurement architecture that provides a tamper-proof file system that allows only authorized applications to run on the device
- **Secure package management:** Measures to ensure that software updates issued in the form of secure packages do not expose the system to external threats
- **Remote attestation:** The means used to verify the identity of a device and to detect any tampering with the Linux kernel
- **GRsecurity**: A set of Linux kernel patches designed to increase system security by adding role-based access control policies and system resource management capabilities
- **Encrypted storage:** Making the data stored on a device unusable if it is accessed without authorization

- **Firewall:** Protection to control traffic that is destined to terminate at the embedded device, with filtering protocols that are specific to the device's function
- **IPsec/SSH/SSL/TLS:** Various methods of encrypting data in transit over an IoT network

WIND RIVER SOLUTIONS COVER SECURITY

Wind River® alleviates much of the security burden on IoT solution developers by delivering open source technologies in which the essential security elements are already configured. The Wind River Linux operating system is the market-leading industry standard for commercial embedded Linux, with security features designed to support the evaluation process against the Common Criteria for various Protection Profiles (PPs). With increasing device connectivity, using a Common Criteria standards-based approach during development can help address security concerns as IoT expands. Wind River Linux is also backed by technical support and long term maintenance plans that include software updates, patches, and monitoring for vulnerabilities.

Linux-based Wind River Intelligent Device Platform XT is a customizable development environment that enables the rapid development and deployment of secure IoT gateways, with built-in features to protect data traveling across a network and minimize exposure to untrusted applications. It is built into Intel® IoT Gateway, a family of platforms that make possible the seamless interconnection of devices and systems, while helping ensure that data can travel securely and safely from the edge to the cloud and back.

Connected devices powered by Wind River Linux are kept secure against vulnerabilities by a security response team that monitors security threats 24/7 and provides a prompt response. Wind River security teams responded in less than 24 hours with hot patches to the market's highest profile open source attacks, including Heartbleed, Shellshock, and others. One of the chief advantages of open source is its vast developer community, which helps accelerate the process of finding and fixing vulnerabilities.

Every year, the Wind River security team analyzes about 4,000 vulnerabilities, around 10% of which require resolution. With security monitoring and remediation from an experienced, highly reliable team, enterprises can dramatically reduce their risks in employing open source technologies in an IoT infrastructure.

CONCLUSION

Connecting intelligent devices has given enterprises the power to create value, either by boosting productivity and efficiency in their existing businesses or by leveraging their data to develop new business models and revenue streams. Security is absolutely critical, however, to the successful functioning of IoT solutions.

Developers are increasingly embracing the flexibility of open source technologies to meet the demand for IoT. Contrary to some misconceptions, open source is not inherently more vulnerable to external threats than proprietary software. Whether open or closed, however, any solution needs multiple layers of security built in at the design stage.

Fortunately, the technology already exists that incorporates the essential open source security elements for embedded systems. Taking advantage of these technologies enables developers to accelerate the delivery of secure IoT solutions to the market, which in turn enables their enterprise customers to start realizing the business benefits of IoT more quickly.

WIND
AN INTEL COMPANY

Wind River is a world leader in embedded software for intelligent connected systems. The company has been pioneering computing inside embedded devices since 1981, and its technology is found in nearly 2 billion products. To learn more, visit Wind River at www.windriver.com.