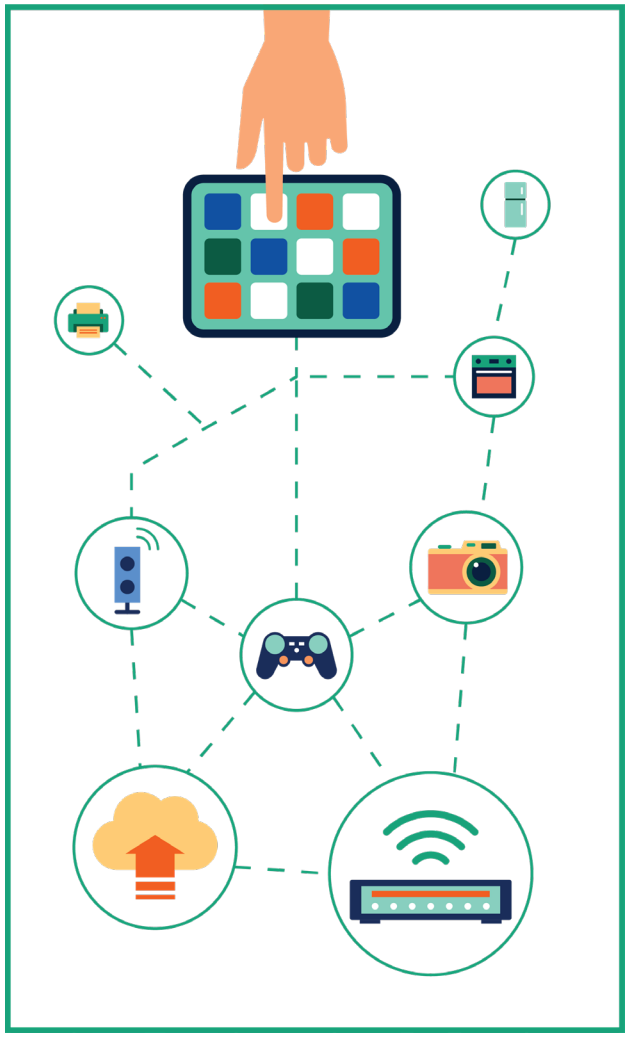
refirm labs

WHITE PAPER

A Herculean Task: Securing the IoT Firmware Supply Chain

There are over 8 billion devices in the Internet of Things, with millions more coming online every day that have no standards or regulations to ensure a security baseline. The firmware on the IoT devices in our world are only as secure as the manufacturer chooses to make them – smart TVs, cell phones, smart watches, security cameras, and even medical devices are all vulnerable to being attacked.



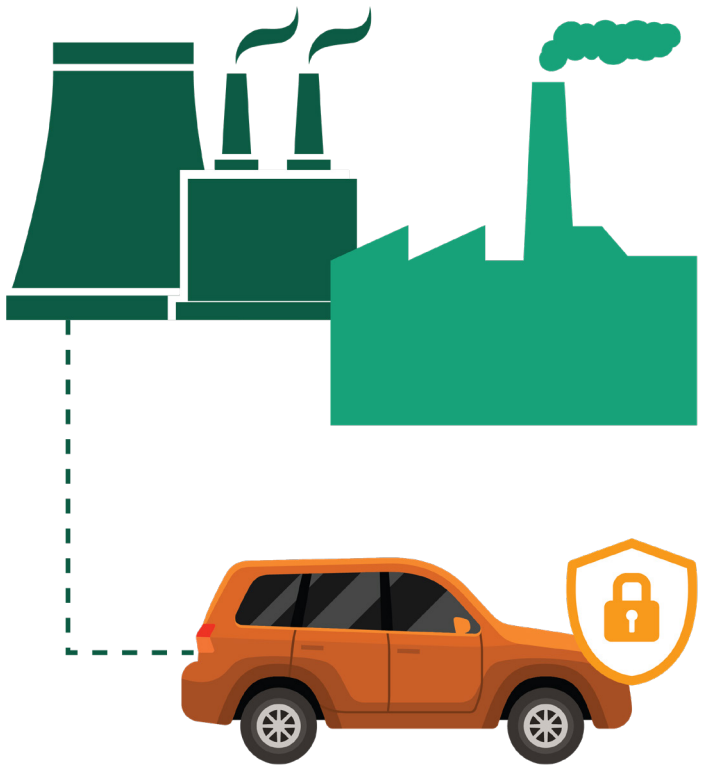
Firmware is a commonly unprotected attack surface in these devices that when hacked, can result in devastating consequences. It is often developed with less attention to security than software, and it frequently involves the integration of 3rd party components that come with unknown security postures. Manual code examination alternatives require source code access and are not scalable given the volume and variety of IoT devices that are being deployed. Additionally, unlike software, firmware is tailor-made for each specific product, making it impossible to run the same firmware on all devices or even within the same product line. This means that each product contains a unique firmware image that needs to be vetted for vulnerabilities. If thorough vetting isn't accomplished, you will be multiplying a hacker's odds of infiltrating the device exponentially.

Modern electronic devices are complex systems, containing a wide array of components from a diverse set of suppliers. The firmware supply chain for even a relatively simple, single-processor device consists of many providers including chip vendors, tools vendors, and companies that provide various software components; to add to the problem, each software component has its own chain of sub-suppliers. Because critical security vulnerabilities may be introduced by any supplier, sophisticated devices such as industrial control systems and vehicles utilize dozens, and sometimes even hundreds of processors, which intensifies the problem exponentially.

Eliminating security vulnerabilities across the supply chain is a Herculean task. It is no surprise that new cyber-attacks , which target industrial systems, medical devices, and connected cars, continue to make headlines. Original Equipment Manufacturers (OEMs) can impose secure software development processes on suppliers but have little ability to enforce these procedural standards. Even when followed, these processes don't ensure that the software is actually secure, meaning that a single vulnerability can result in the security of the device being compromised. Ultimately, OEMs lack the tools necessary to effectively manage cybersecurity across an increasingly complex supply chain. The ability to analyze a supplier's firmware in order to determine whether security vulnerabilities are present is possibly the most crucial step to securing their supply chain.

Supply Chain Complexity

Consumers using an IoT device, connected car, or industrial control system are intentionally led to believe they are purchasing a device made by a single manufacturer. In truth, any given device has traceable origins to hundreds, if not thousands of companies. Yet when security is breached, it is the manufacturer whose name makes the headlines. A security vulnerability introduced by a supplier will be viewed as a problem with the OEM's product. Since the OEM's reputation is at risk, they must be able to make certain that all suppliers deliver components with high levels of security.



Why Security Matters for the Supply Chain

OEMs rely on components and subsystems from a wide range of suppliers. To ensure quality and reliability, OEMs impose standards on their suppliers and test components, subsystems, and the final product for compliance with these standards. This has proved effective for addressing traditional issues of reliability, durability, and overall quality of products. Only by ensuring the integrity of all components can a high-quality product be produced. Vehicles, for example, are far more reliable today than they were 20 or 30 years ago.

A similar metrics driven, cybersecurity quality program is needed for the software components of electronic devices. Cybersecurity standards must be defined and enforced for all software and firmware components in order to truly eliminate vulnerabilities. Historically, OEMs did not have the tools needed to enforce meaningful cybersecurity standards on their suppliers, which resulted in the OEMs not knowing what vulnerabilities were present in firmware. It's easy to see why tools that identify security vulnerabilities within the supply chain are instrumental to creating strong, fool-proof, and meaningful cybersecurity requirements.

Security Standards and Practices for the Supply Chain

Defining security standards and practices for internal engineering teams is a cornerstone security practice. These procedural methods are applied to the development process to help make sure security vulnerabilities are not introduced into the code. Because OEMs have control over the internal development processes, they can easily enforce these standards for internal development.

The same security standards can also be imposed on contract engineering groups used as supplemental engineering resources. However, enforcing these standards on outsourced engineering teams is difficult, particularly for off-shore engineering teams. Despite agreeing to follow coding and security standards, off-shore teams often cut corners and disregard these standards when schedule and budget pressures arise. The OEM may not learn that their standards were ignored until a vulnerability is found in their device. Unfortunately, this could be discovered years after the device was mass-distributed.

Practical Considerations

The supply chain for connected devices, be they a connected car, industrial control system, or medical device, is massive. Implementing and enforcing security standards across all levels of the supply chain will require a phased approach. Early phases should be focused on security for newly developed software and safety-critical components. Over time, security standards can be extended to additional software components, allowing suppliers and sub-suppliers time to address their specific security concerns and guarantee full compliance.

Non-technical aspects must also be taken into consideration. Contracts will need to be adjusted to reflect the new compliance procedures, and both cost and schedule impacts must be accounted for. These costs may be significant, especially where legacy software needs to be updated. For some large systems, implementing a comprehensive security program may be a multi-year effort that adds dramatically to the engineering cost. Despite the higher cost, this is an investment that must be made.

As our cars, factories, and critical infrastructures are increasingly connected, failed device security is quickly becoming more than a matter of financial security and privacy; it is a matter of physical safety. As an industry, we must commit to stopping cyber-attacks. This starts with the ability to easily and automatically find security firmware vulnerabilities. Rather than imposing process-oriented secure development standards that may or may not be followed, and that cannot be retroactively applied to existing code, another solution is needed such as the Centrifuge Platform™. Request your free trial today.