IoT Security: Building Security in from Chips to Cloud

The Internet of Things (IoT) Promises to Revolutionize Modern Society.

IoT devices take the shape of standalone devices or components in other systems and can be found in various environments including automotive, medical, aerospace and industrial systems. If you trace the roots of IoT back to a time when "things" were called embedded devices, you will discover a wide array of security weaknesses. These weaknesses have not disappeared. Instead, they have been amplified by adding multiple connectivity options to resource-constrained, tiny computing platforms that perform mission critical functions.

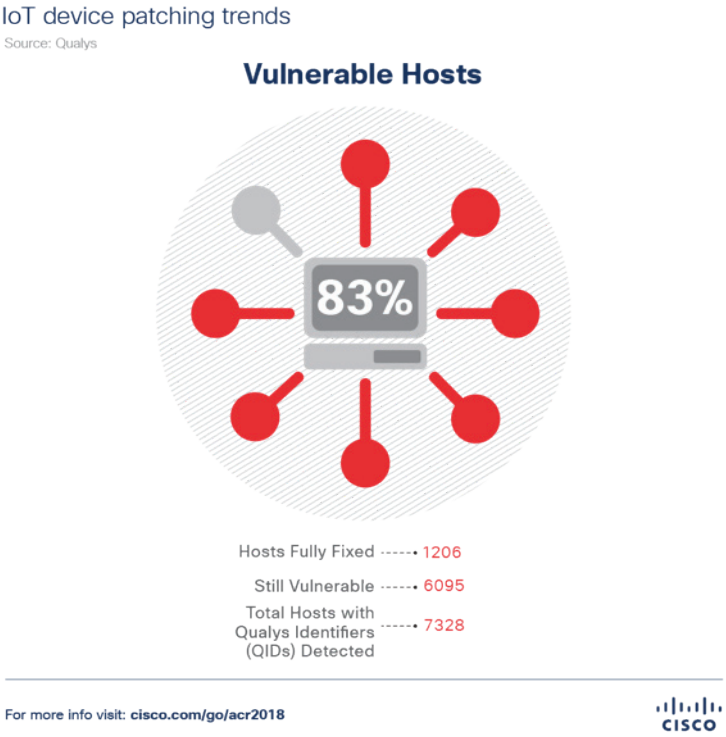
In Cisco's recent Annual Cybersecurity Report, we found that even when vulnerabilities are known, steps are not being taken to proactively find and patch IoT devices on the network.

In most cases, vulnerabilities are discovered after the device has been purchased and deployed in the network. For product developers, vulnerabilities uncovered after a product is released to market are costly to address and present a significant impact in terms of public safety (in the case of medical devices, an exploitable flaw could result in loss of life), time, dollars and reputation. When paired with current threats such as ransomware, IoT devices present truly frightening new opportunities for attackers.

What if you need help?

Product developers necessarily have deep expertise in project management, engineering, quality assurance and many other aspects of bringing a product to market. It can be very challenging for product development teams to also have expertise in cybersecurity, such as security threat intelligence, regulatory compliance, and data breach avoidance or response requirements. In these cases, outsourcing to dedicated security experts is recommended and increasingly common. This is true even for IT departments' core security staff: according to the 2018 Annual Cybersecurity Report, more than 50% of respondents outsource to security advice and consulting services.

Whether provided by in-house resources or outside consultants, security experts can help product developers uncover vulnerabilities.



The solution is clear: embed security in products from the very beginning of product development – before they are introduced to market and deployed in networks. In this paper, we'll outline steps you should take to build security into your development lifecycle of IoT devices.

Why is it so difficult to build secure IoT devices?

Creating a new IoT device typically requires careful coordination of different development teams to deliver a product on time while accounting for features that maintain a competitive edge. Layered onto this are pricing and budgetary pressure from competition and shareholders. These development teams must work together to design a hardware and firmware platform, mechanical enclosure(s), physical connections, interface specifications, mobile applications and supporting cloud services. Moreover, firmware and hardware components are interdependent; firmware testing will result in hardware changes and vice versa. Certain classes of devices are also subject to functional testing in order to meet regulatory compliance requirements.

Given these challenges, paired with a shortage of security talent and the high cost of security expertise, it is no wonder that security is usually an afterthought. This is a significant issue, considering the top security concerns affecting IoT devices include:

- Loss of life
- Extortion (e.g. ransomware)
- Privacy
- Intellectual property protection
- Brand protection

IoT devices may make use of microcontrollers and protocols that are not widely understood. This has been a barrier to entry for security researchers and attackers alike. Vulnerabilities historically hid behind complexity and obscurity, but this veil is slowly being lifted by steadily increasing research activity. While these devices present more of a challenge to researchers, recent findings have demonstrated that the stakes are high enough to justify the effort. VPNFilter malware is just one example. Discovering vulnerabilities in these systems requires rare skill combinations, familiarity with embedded systems, and specialized hardware and software tools.

A regular cadence of firmware updates can also be a challenge for IoT devices. Many IoT devices do not have a persistent Internet connection. Intermittent access to the Internet translates to an unpredictable cadence for firmware updates. As a result, known bugs have a longer lifetime which extends the window of opportunity for exploitation. In other cases, devices were designed and deployed without consideration for maintenance over time. These devices may be running outdated operating system software that contains known vulnerabilities, or worse, may be running completely unsupported operating systems (e.g. Windows 95 or XP).

In addition, IoT devices often communicate with other network nodes wirelessly through a combination of near field technologies such as Bluetooth, Zigbee, or NFC. In the case of implantable devices, firmware updates must often be delivered wirelessly. Leveraging wireless technologies increase convenience at the expense of heightened exposure to attack. Recent vulnerabilities, such as BlueBorne, highlight the security concerns in wireless devices.

And finally, securing IoT devices is challenging because devices may act as sensors, gathering and relaying information, or act as collectors of said information. Eventually this information is typically transmitted to cloud services over the Internet. There may also be local command and control capabilities engaged through the use of a mobile application or specialized device. If that information is sensitive in any way, consideration must be given to how the information is stored and transmitted at each link in the chain. Moreover, each of the nodes in an IoT network will share a need for mutual authentication and encryption in order to communicate securely. The constrained resources of these devices often lead to weak or missing communications security.

For example, a Bluetooth controlled door lock may only require a static password in order to receive and execute commands from a mobile application. This password can be obtained through a variety of methods and used by an attacker.

These challenges are not trivial, but IoT product developers must find ways around them – ideally in the product development process.

Key security activities for IoT product developers

Despite the many complexities and pitfalls of security within an IoT environment, there are several key steps product developers can take to reduce the risk of security breaches involving IoT Devices. Our recommendations fall into two main sections of the IoT product development lifecycle: 1) during development and 2) post-release.

During Development

IoT devices are composed of electronic components, software components, network communications protocols, and supporting infrastructure. Product developers need to use threat modeling to identify relevant threats and develop countermeasures during the design phase to minimize the attack surface of the device and mitigate vulnerabilities before they can materialize. This can drastically reduce the likelihood of successful attacks and in turn reduce costs.

Top activities to incorporate into your product development process include:

1. **Include security experts on the design team.** Optimal product development requires security experts that are integrated members of the development team, with active roles in product design and development.
2. **Review initial high-level system design with security experts.** Performing this activity during the design process will build understanding and enable you to develop architectures that mitigate security vulnerabilities before they are introduced.
3. **Develop a threat model.** Threat modeling aims to identify real world threats that apply to the system under development. The threat model documents key assets, data flows, system components, user roles, threats and countermeasures. The countermeasures documented in the threat model must then be merged into technical product requirements so they can be tracked during development.
4. **Integrate static and dynamic analysis tools.** These tools will help you identify security issues during the development lifecycle, which will in turn help limit the introduction of security vulnerabilities before your new IoT product is introduced to market.

Post-Release

While product introduction is a rewarding milestone, the job of ensuring IoT security on your product is not done. You must track and improve the security of a system that has already been deployed. This in itself may be very challenging: in many cases, the team responsible for defending against security threats only has a limited understanding of how the system works. You'll need to develop a solid understanding of the system and its components, threats and countermeasures.

Key activities to ensure security at this stage include:

1. **Architecture assessments.** Architecture reviews are performed by reviewing documentation and interviewing personnel while vulnerability assessments are technical, hands-on assessments.
2. **Vulnerability assessments.** These aim to provide a broad picture of the vulnerabilities affecting one or more systems. In a vulnerability assessment, the interfaces exposed by live system components are interrogated to identify vulnerabilities and quantify the risk of each one. Vulnerability assessments are useful for broadly determining the size and scale of known security problems. These metrics are useful when planning and prioritizing fixes.
3. **Penetration testing.** These are goal-oriented attack simulations. In this scenario, you identify your worst-case security nightmares affecting one or more targets. The threat model from a design review or architecture review make a great basis for goals to pursue during a penetration test. Good examples of goals might be ransomware targeting pacemakers or remotely unlocking car doors while the vehicle is in motion.

You then identify live instances of the target for testing purposes and attack components to realize these situations and how they can be stopped. The paths eventually taken are referred to as attack-chains or kill-chains and often involve multiple chained steps exploiting vulnerabilities in different components. Penetration tests provide a practical sense of how much progress an attacker with certain means and knowledge would make towards the stated goals in a limited amount of time. They also give a "real world" sense of how well your defenses are working.

Case Study: Throw Away Your Keys

Challenge

A large automotive manufacturer completed designing a new connected car technology that would allow vehicle owners to unlock and start their vehicles with a mobile phone. The technology relied on Bluetooth Low Energy ("BLE") and cellular connectivity. They were concerned about the potential risks associated with the project, especially those related to theft and privacy, and decided to engage Cisco to perform a security architecture assessment.

Solution

Cisco Security Services experts participated in multiple design review sessions with different teams that spanned hardware, wireless channels, antenna systems, firmware, mobile technologies, and cloud services. These design review sessions invariably required digging deep into technical specifications in order to help identify and mitigate threats. Cisco performed a gap analysis of the current system architecture against best practices, identifying several areas that presented challenging security problems; including:

- Preventing BLE relay attacks that could allow an attacker to unlock and drive away with a vehicle while the owner is not close to the vehicle
- Registration of mobile applications with vehicles
- Vehicle key provisioning and binding
- Secure communication between the mobile application and vehicle
- Backup security features that can be invoked when phone is unavailable
- Proving ownership of the vehicle
- Secure handling of secrets securely on the in-vehicle module and mobile application

Cisco created threat models for variants of the solution that resulted in countermeasures and security controls. These controls were then translated into security requirements embedded in official software design specifications and requirements documents. Cisco identified many high-risk threats affecting the system. Cisco was able to:

- Find ways for an attacker to take control of a vehicle if an end user lost their mobile or if the mobile were stolen
- Illustrate common attacks affecting BLE devices such as relay attacks and long-distance Bluetooth connections
- Identify security weaknesses in the BLE communication protocol
- Identify an exploitable condition where anyone could drain the battery of a vehicle supporting the feature
- Identify dangerous scenarios affecting vehicle fleets or rental organizations
- Find ways to deny access to legitimate users

Outcome

By working with security experts to evaluate multiple variants of the solution during development, this manufacturer was able to quantify and compare the risks presented by each variant. The threats identified allowed them to make technically informed decisions on their strategic roadmaps.

Case Study: Aging Connected Car Infrastructure

Challenge

A large automotive manufacturer was concerned about the security of their aging connected car, in-vehicle components and supporting infrastructure. The objective of the engagement was to paint an accurate picture of what an attacker with reasonable knowledge and means could achieve in a few months.

Solution

Cisco Security Services experts engaged with the manufacturer to perform a penetration test of selected in-vehicle components and backend services. The manufacturer supplied fully provisioned test benches that emulate the major features of a vehicle.

Through penetration testing, the team was able to discover credentials to functionality that should have only been accessible from the specialized hardware for the vehicle. They further uncovered insufficient security controls in the backend infrastructure. They were able to observe backbone traffic and was able to replay specific command and control traffic. In addition, the security experts were able to demonstrate that an attacker could extract information and hardware components from the in-vehicle systems to construct a prototype system which demonstrated unmetered cellular-based Internet connectivity. Cisco worked with the manufacturer to eliminate findings and harden the overall security of its vehicles.

Outcome

By chaining together the vulnerabilities found, security experts were able to accomplish several real-world, worst-case security nightmares for the client. The manufacturer received remediation advice to prevent these issues while still being able to maintain their current service offering.

Conclusion

IoT devices can enhance, save and possibly end lives. As a result, it is important for IoT device manufacturers to meet their security challenges head-on.

Cisco Security Services can help to identify and defend against vulnerabilities in IoT devices and their associated infrastructure throughout the product development lifecycle. These services span the entire chips-to-cloud landscape and include early stage security design reviews, secure code analysis and penetration testing of devices, applications, and networks. Cisco's industry-leading subject matter experts can also be engaged on a flexible as-needed basis to support projects throughout their development.

Cisco employs over 3,000 security professionals globally with expertise in embedded security, application security, network security, reverse engineering, electrical engineering, network communications protocols, wireless technologies, and cryptography. Moreover, Cisco also has dedicated state of the art hardware security testing labs where security researchers perform in-depth testing of devices.