WIND™

# Internet of Things Security Is More Challenging Than Cybersecurity

WHEN IT MATTERS, IT RUNS ON WIND RIVER

## EXECUTIVE SUMMARY

Widespread adoption of the Internet of Things (IoT) depends on security. IoT security is more challenging than cybersecurity because of two key factors: the enormous attack surface presented by the anticipated billions of IoT devices, and the increased vulnerability of many of those devices. Device manufacturers need to employ traditional cybersecurity techniques—including a defense-in-depth approach with multiple complementary security technologies—in their devices, then adapt those techniques for the unique aspects of IoT devices, and finally incorporate other device-specific countermeasures where necessary to provide comprehensive and adaptive IoT security.

## TABLE OF CONTENTS

Executive Summary . . . . . 2
Introduction . . . . . 3
IoT Securty Starts with Cybersecurity . . . . . 3
Open Virtualization . . . . . 4
Identify . . . . . 4
- Security Policies . . . . . 4
- Security Model . . . . . 4
- Assets: What Needs to Be Protected? . . . . . 4
- Attackers and Threats . . . . . 4

Protect and Detect . . . . . 5
- Implement Security Measures . . . . . 5
- Defense-in-Depth: Many Silver Bullets Are Better Than One . . . . . 5
- Adapting Cybersecurity for IoT Security . . . . . 5
- Incorporating Device-Specific Security . . . . . 5

Respond and Recover . . . . . 6
Conclusion . . . . . 6
References . . . . . 7

## INTRODUCTION

IoT is more than just the "things": it comprises systems that connect things, machines, and humans to the cloud to enable improvements in efficiency, services, and customer satisfaction at the edge while providing cost savings and new business models to IoT providers.

Security is the number one issue facing IoT deployments and must be properly addressed before broad adoption can begin. Cybersecurity has become a high priority for information technology (IT) systems, yet there continue to be major security breaches, such as the hacks of major organizations including Anthem[1], Home Depot[2], the U.S. Office of Personnel Management (OPM)[3], Sony[4], Target[5], and the French naval contractor DCNS[6]. The threat of cyberattacks is very real; every day there are nearly 1 million new malware threats identified and millions of actual cyberattacks[7].

In today's atmosphere of frequent breaches, most IT professionals are well versed in the latest techniques to protect corporate assets. But providing security in IoT is more complicated, due to two main factors:

1. The IoT presents an exponentially larger attack surface.
2. The points on that surface (the "things") have increased vulnerability.

If the prediction of tens of billions of connected things comes to pass, the IoT will present an enormously large attack surface to defend. Furthermore, these devices will be more vulnerable and accessible to attackers than traditional IT systems for several reasons:

- Many devices will be low-cost end nodes, with low (or no) budget for security measures such as physical tamper-proofing.
- Many devices will have resource constraints that lead to vulnerabilities (e.g., insufficient compute power for encryption capability).
- Many IoT devices will be more readily physically accessible (e.g., smart light bulbs, smart thermostats, smart power meters, smart roadside sensors) than traditional IT equipment.
- The great diversity in IoT devices—from tiny microcontroller-based sensors to powerful server-class computers—will make it difficult for device manufacturers to incorporate a single standard of security.
- IoT devices will be created by a much larger pool of developers, whose range of security experience may be quite broad.
- The devices will be deployed for years and even decades, prolonging their exposure to attack as well as exposing older systems to newer attack vectors.

Even as IoT is in its infancy, there have already been some infamous hacks: Jeep Cherokee automobiles[8], medical infusion pumps[9], even home baby monitors[10]. A recent light bulb hack[11] proved that simple security mistakes can provide attackers with easy access to not just the "things" but the networks they're connected to—and therefore to anything else on the same networks.

## IOT SECURITY STARTS WITH CYBERSECURITY

The techniques developed to provide cybersecurity can be used to secure IoT, but further security measures will be necessary. Rather than applying measures in an ad hoc manner, a well-defined process will need to be followed to ensure thorough consideration of all security aspects.

One useful and comprehensive guide for manufacturers is the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity[12], a set of industry standards and best practices to help organizations manage cybersecurity risk. The framework defines the following five core functions as high-level steps to follow for implementing cybersecurity: identify, protect, detect, respond, and recover. A similar process is defined by the NIST Risk Management Framework[13] for managing the risk to an information system and includes the following steps: categorize, select, implement, assess, authorize, and monitor. Both of these processes apply equally to IoT security as to critical infrastructure cybersecurity or IT systems. In the following sections, the NIST Framework is used as an example.

A third resource, NIST's Networks of 'Things' (NoT)[14], "offers an underlying and foundational science to IoT based on a belief that IoT involves sensing, computing, communication, and actuation." The paper defines five primitives, or building blocks, for IoT and NoT systems: sensors, aggregators, communication channels, external utilities, and decision triggers. For each, basic properties, assumptions, recommendations, and general statements are made, including security concerns. Networks of 'Things' provides a model and vocabulary for developers to use when designing and implementing their IoT/NoT devices.

## IDENTIFY

Cybersecurity begins with identification of the cybersecurity risk to systems, assets, data, and capabilities, and IoT security should start with this step as well. There are multiple categories in this phase. Manufacturers will need to consider the categories relevant to their devices, some of which are covered below.

### Security Policies

The risk management strategy for the device should be defined. Risk management involves identifying the desired security policies that will be enforced to manage the perceived risks to the information system. Manufacturers will need to define relevant security policies for their IoT devices based on their risk management strategy. The most relevant security policy for IoT devices covers information security: "Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction, in order to provide integrity, confidentiality, and availability."[15] Policies to cover password control, physical access, and privacy would also help manage risk to consumer IoT devices, and manufacturers may additionally consider defining security policies to govern device development, testing, and analysis for vulnerabilities.

### Security Model

With security policies defined, the security model then needs to be developed. The model translates the abstract, desired security policies specifically into how the device will implement and enforce them. The model is usually the basis for the device's security architecture, but the model alone is insufficient and further information is needed. For example: How strongly should device security be implemented? What physical tamper-proofing measures will suffice? To answer these types of questions, the manufacturer will need to define the device assets that must be protected, which threats and attacks the device is to protect against, and how the device will react when (and not if) such attacks are detected.

### Assets: What Needs to Be Protected?

One basic question to be answered is: What exactly needs to be protected? What are the assets, and how valuable are they? For example, is the asset simply a $5 light bulb? A $150 IoT gateway? Or a multimillion dollar commercial wind turbine? And it's not just the physical asset that needs protection, it's also the data the device is generating, processing, sending, and receiving. This is where traditional cybersecurity techniques can help: Residential power meter information sent over the cellular network to the power company can be protected just as credit card data from a web browser is protected when sent over the Internet.

It's crucial to remember that a specific end device may not be the final target of an attack. Its manufacturer might have considered it low risk for attack and thus unworthy of extra protection (especially protection that could add to its cost). But that relatively unprotected device might then become attractive as a target by providing a gateway into its connected networks. A breach here would enable attackers to gain access to an ultimate target, such as valuable corporate data. (Recall the hacked light bulb example: an attacker starts by accessing the bulb's smartphone app, then moves on to the Wi-Fi network the bulb is connected to, and then on to any device on that network.) When considering which assets to protect in the chain of IoT devices and machines, the security of an entire system is only as strong as its weakest link.

### Attackers and Threats

Knowing the assets to protect and their value will help identify potential attackers. That list[16] includes national governments, terrorists, criminals, spies, black hat and grey hat hackers, "hacktivists," and script kiddies. Not all of these may be relevant for a given device, so the device's security model will need to hone in on potential attackers who are most interested in the device's assets, as well as those assets accessible from the device.

Identifying who might attack a device provides insight into possible motives and levels of sophistication, which in turn helps define the threats and determine what potential attacks to expect. For example, unsophisticated attackers like script kiddies may not employ complex attacks, but since knowledge spreads quickly on the Internet, high levels of attack sophistication should be assumed.

The expected strength of those threats also influences how security measures will be implemented. Persistent and well-funded attackers pose the highest risk to device security, so a conservative assumption when considering potential attacks is the best approach. Since security is a war of escalation, it may be only a matter of time before a device will be compromised. Making a device as strong as economically feasible is always prudent.

## PROTECT AND DETECT

Once potential threats are identified, manufacturers can start development of specific device security measures to meet expected threats.

### Implement Security Measures

To implement IoT security measures, well-known cybersecurity tactics can be leveraged by device manufacturers. For example, if the device employs an information security policy, measures and techniques should be considered that implement confidentiality, integrity, and availability (known as the CIA triad). What specifically gets implemented depends on the expected threats, but the catalog of measures includes these techniques:

- Using secure architecture design and processes from the start of development
- Ensuring the use of a secure boot process to establish a root of trust (e.g., using digital signatures of binary images)—for integrity
- Providing mechanisms for system and software attestation at boot time and periodically during run time—for integrity and availability
- Securing data-at-rest and data-in-motion, and providing sanitization of resources—for confidentiality and integrity
- Securing device communications with secure technologies and protocols (e.g., HTTPS, TLS), and using firewalls for both wired and wireless connections—for confidentiality and integrity
- Providing secure encryption key management (key generation, key distribution, key storage) with periodic key updates—for confidentiality and integrity
- Providing authentication, authorization, and accounting (AAA) services on devices for applications as well as users—for integrity
- Utilizing whitelisting for applications on the device with periodic whitelist updates—for availability
- Implementing intrusion prevention and intrusion detection with periodic updates of these mechanisms—for availability
- Securing the supply chain from chipmaker to original equipment manufacturer (OEM) to application provider so that components can be trusted—for integrity
- Providing secure patch and update management—for availability

Additionally, regular updating is required to ensure these techniques remain effective in keeping pace with the development of new attacks.

### Defense-in-Depth: Many Silver Bullets Are Better Than One

One concept security architects need to employ in IoT device security is the defense-in-depth methodology, involving the use of multiple layers of security techniques. A DHS paper[17] on recommended practices for industrial control cybersecurity states there is no silver-bullet solution for security, stating "A single countermeasure cannot be depended on to mitigate all security issues." The report continues: "In order to effectively protect industrial control systems from cyber-attacks, multiple countermeasures are needed that will disseminate risk over an aggregate of security mitigation techniques. The strategy of implementing multiple layers of defense to combat multiple security issues is commonly referred to as defense-in-depth."

The use of defense-in-depth dates to medieval times, when castles were built to protect a kingdom's assets. A castle's moat, drawbridge, portcullis, parapets and crenels, machicolations in thick stone walls, multiple layers of those walls, inner keeps, bowmen and swordsmen atop every wall and tower—none of these defense mechanisms alone would suffice to repel an attack, but layering these complementary countermeasures would slow attackers, thin the attacking horde, or even deter the attack altogether.

### Adapting Cybersecurity for IoT Security

IoT device manufacturers should adapt traditional cybersecurity practices with device-specific techniques to help mitigate the added vulnerabilities introduced by IoT. Such techniques include:

- Designing security into both a device's hardware and software
- Protecting the physical packaging of the device by providing anti-tamper—for availability
- Leveraging hardware-based security where possible, such as encryption engines and the Trusted Platform Module (TPM)[18]—for confidentiality, integrity, and availability
- Securing the applications on the device (e.g., requiring users to change default passwords and to use strong passwords when doing so)—for availability
- Ensuring the secure provisioning of devices to manage deployment, lifecycle updates and upgrades, and eventual decommissioning—for integrity and availability

**Incorporating Device-Specific Security**

Finally, IoT device manufacturers should use additional device-specific techniques to help mitigate the threats unique to IoT devices. Such techniques include:

- Locking any software debug interface (e.g., using a secure shell with usernames and passwords)—for availability
- Using bi-directional identification and authentication of devices and servers to ensure that each entity engaged in IoT communications knows exactly with whom it is communicating—for integrity and confidentiality
- Incorporating a secure, runtime, monitor application on the device to oversee communications and overall device behavior, and to detect anomalies such as denial-of-service attacks or other security breaches (e.g., noticing abnormally high network traffic or detecting anomalous communication paths, such as the in-dash infotainment system commanding the anti-lock brakes)—for availability
- Incorporating a security management application on the device to manage provisioning, device configuration, security measure configurations, security policies, security event monitoring and responses, and ongoing software and patch management—for confidentiality, integrity, and availability

## RESPOND AND RECOVER

Using defense-in-depth and security techniques, IoT devices will be able to protect themselves against known attacks and also detect attacks in real time. But to be truly effective, IoT security needs to do more than just detect attacks—it needs to be able to respond quickly. The high-level security policies will dictate the actions that need to be taken for each type of detected security event. Response actions can include:

- Locking out administrator access (such as if the wrong username and password combination is presented *n* times)
- Shutting down an aberrant or misbehaving application
- Reloading a compromised application's image and restarting it
- Updating the device's firmware or other software
- Shutting down the device completely to avoid further potential data loss or attacker incursion

The appropriate response depends, of course, on the nature of the attack and the perceived threat.

Beyond the immediate attack response, other recovery actions should be taken to help improve the security posture of the device. For example, attack event records should be securely logged for subsequent retrieval and analysis. Post-event analysis can lead to remedial design activity and potential future device software updates or upgrades, helping devices continually adapt to an ever-changing threat environment.

## CONCLUSION

To help secure the IoT and reduce barriers to adoption, IoT security design should start with traditional cybersecurity techniques, adapt them to the unique aspects of IoT devices and environments, and finally incorporate additional defense mechanisms to defend against the increasingly broad range and vulnerable nature of IoT devices. Following standard security processes can ensure a thorough review of areas of concern, which can then be followed by leveraging advanced cybersecurity and device-specific techniques, including a layered, defense-in-depth approach to security.

Wind River® can help with IoT device development and can ensure implementation of the latest best practices. Wind River Professional Services has a practice for IoT security, an overview of which is provided in the whitepaper "A Survey of Information Security Implementations for the Internet of Things" (available on request; please contact Wind River[19] or your Wind River account manager). By properly designing security into IoT devices, financial damage, reputational damage, and potential risk to human life can be avoided.

## REFERENCES


1. www.latimes.com/business/la-fi-mh-anthem-is-warning-consumers-20150306-column.html
2. money.cnn.com/2014/09/08/technology/security/home-depot-breach
3. www.lawfareblog.com/why-opm-hack-far-worse-you-imagine
4. fortune.com/sony-hack-part-1
5. money.cnn.com/2013/12/22/news/companies/target-credit-card-hack
6. www.theaustralian.com.au/national-affairs/defence/france-launches-investigation-into-massive-submarine-data-leak/news-story/a94aadaac52508ca79f385a234e50583
7. money.cnn.com/2015/04/14/technology/security/cyber-attack-hacks-security
8. www.wired.com/2015/07/hackers-remotely-kill-jeep-highway
9. www.cnbc.com/2015/08/03/citing-hacking-risk-fda-says-hospira-pump-shouldnt-be-used.html
10. fusion.net/story/192189/internet-connected-baby-monitors-trivial-to-hack
11. www.bbc.com/news/technology-36903274
12. www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf
13. csrc.nist.gov/groups/SMA/fisma/framework.html
14. nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-183.pdf
15. U.S. Code Section 3542 - Definitions
16. blogs.mcafee.com/consumer/family-safety/7-types-of-hacker-motivations
17. https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/Defense_in_Depth_Oct09.pdf
18. www.trustedcomputinggroup.org/work-groups/trusted-platform-module/
19. windriver.com/company/contact/request.html


WIND

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.