# Time to Toughen Up for IoT

The internet of things has wrought huge changes, not the least of which is in your security posture. Here's what you need to know, and do, now.

# Take Control of All Those 'Things'



**The threatening forecasts** have been with us from the start: The internet of things is coming for you, for your house, for your car, for your fridge. Before you know it, pundits say, the things will be in control and we humans just along for the ride.

Um, well—not yet. Maybe someday. Maybe not ever. But if there's one thing the internet of things *should* take over, it's the amount of time and attention IT teams spend on security. Whatever the list of IoT challenges you face, security needs to be at the top of it.

But of course the next logical question is: Then what? To answer that, we've compiled this three-part technical guide, pulling together three experts' views on how to address the security challenges that IoT presents. We open with a piece focused on the five steps you can take today to secure the interconnected devices already traversing your enterprise network or hauling around corporate data. Next we look at what you can do to harden those individual devices and minimize the chance of compromise. As with most things security-related, testing your defense posture is essential. So our final chapter zeroes in on how to conduct IoT security testing.

The pages ahead are loaded with actionable advice for IT professionals facing the new reality that the internet of things has wrought on enterprise security. We hope it will put those scary forecasts out of mind and be a useful aid to understanding and responding to IoT challenges. ■

Brenda L. Horrigan, Ph.D.
*Managing editor,*
*Security Media Group*

# Five Keys to IoT Security



THE INTERNET OF things brings both benefits and potential security vulnerabilities. Here are five key steps to securing IoT that enterprises should take to safely connect IoT devices to their networks.

The internet of things (IoT) is an evolution of networked computing devices that brings with it a variety of security issues. Many of these issues have existed for decades in IT systems. What's changed with IoT, though, is the large number of devices, their physical distribution, and their relatively limited computation and storage capabilities, all of which introduce additional factors that must be addressed to protect the integrity, availability and confidentiality of data and systems.

IoT devices can operate in a variety of interaction modes. They may act as data-collecting sensors sending information to a central service: An environmental sensor sending data on temperature, humidity and wind velocity is an example. This type of communication is primarily directed inward, toward the central service. In other cases, bidirectional communications may be employed. A smart power sensor in a home electrical system may send data about power consumption to a central service. After processing inputs, the central service can send instructions back to the smart sensor to adjust usage; for example, it might temporarily shut down some devices in the house to reduce electricity consumption.

Alternatively, devices may interact with other devices to employ localized, swarm intelligence algorithms to respond to local conditions without interaction with a centralized service. Devices on automobiles, for instance, can broadcast information about the vehicle speed, directions and acceleration to other vehicles in the area, which in turn can respond by adjusting their speed to avoid potential collisions.

## FIVE STEPS TO IoT DEVICE SECURITY

The modes of integration could be compromised without effective security controls on IoT devices. Here are five types of security controls that need to be in place to protect IoT operations:

**1.** IoT devices should be authenticated before being allowed to communicate with other IoT devices on the network or centralized services. This mitigates the risk of a malicious attacker spoofing an IoT device that appears to be a legitimate device on the network. Spoofed devices could be used to collect data from other IoT devices on the network or to transmit malicious data to other devices. This could be done either to corrupt data processing and analysis or to implement a denial-of-service attack on the IoT network.

**2.** Devices must be started securely. It is especially important to verify and authenticate the source of software running on the device. Unsigned software may be compromised, and the device would not be able to detect such tampering unless software is digitally signed by the software vendor.

**3.** Software patching must be done in a way that does not compromise the operation of the device. Software updates should only be accepted by authenticated sources. The patching process should be performed in a way that minimizes the risk of losing data or interfering with operations. For example, a device may be put into an update mode in which all local data is written to a central service, other devices are informed the updating device is going offline, and the update is performed and verified before returning to normal operating mode.

**4.** Access controls are fundamental measures for securing IoT and the organization as a whole. Users and roles are typically assigned

**IoT encompasses many aspects of IT security, but the new architectures and design patterns present new potential vulnerabilities as well.**

privileges to perform operations in IT systems. In the case of securing IoT, roles should be designated for querying the state of IoT devices, updating software on devices and changing configuration of devices. As with other IT systems, it is important to employ the principle of least privilege and grant users and roles only the minimal set of privileges needed to perform their business and technical function. This can help limit the damage done in the event a user's credentials are compromised.

**5.** Design IoT software analytics with an eye on anomaly detection. In many cases, baseline behaviors may be well established, and variation from those baselines can indicate problems. For example, higher-than-expected traffic from a set of IoT devices could indicate the devices have been compromised and are being used in a denial-of-service attack. Consider how to respond to anomalous behavior, perhaps by shutting down problematic devices or removing them from the network.

Internet of things security encompasses many aspects of IT security in general, but the new architectures and design patterns seen with IoT networks present new potential vulnerabilities as well as additional opportunities for securing IoT and improving enterprise security overall. —*Dan Sullivan*

# Toughening Up Your IoT Devices



ASK ANY ENTERPRISE security practitioner and they'll tell you that IoT device security, like any new technology, is a big challenge. One area where the internet of things presents a particular security challenge, though, is in understanding and dealing with the *scope* of the challenge: the variety of use cases, situations and devices included under its broader umbrella. Specifically, keep in mind that IoT device security potentially can include anything from the IP-connected television in your conference room to intelligent sensors used on the production floor to operational technology (like industrial control systems at a utility) or clinical devices (such as imaging devices or biomedical devices) for a healthcare provider.

## TIME TO GET TOUGH

As you might imagine, each of the above-listed situations can have a potential impact on your organization's security: The television could be an entry point to your internal network; the shop floor's sensors and other equipment could contain information of value to a competitor; the industrial control system could have a cyberwarfare implication (such as an attack on critical infrastructure); and the clinical devices could have patient health and safety impact. Ensuring that those devices are fielded according to a secure configuration is important—and it's equally important that they stay that way over time.

Obviously, device manufacturers can and should ultimately play a critical role in this: as technology matures, as standardization emerges, and as regulators and policy-makers evaluate their role, there is potential for increased maturity down the road. As a practical matter in the meantime, though, security pros in the enterprise need to ensure their organizations stay protected.

This can be a tough nut to crack for a few reasons. First, unlike hardening a general-purpose operating system (such as services, desktops or even BYOD devices), the specific configuration of a given IoT device may be less directly modifiable by an end user. Moreover, even where configuration options do exist that influence the IoT device security, a security professional may not be organizationally equipped to make sure this is done. For example, there may not be a clear delineation of responsibility for who specifically is responsible for the security configuration. Lastly, because of the diversity of potential devices, "one size fits all" guidance can only go so far. For example, the specific configuration changes or security countermeasures you'd employ on a television will be vastly different than those you might employ for a humidity sensor used in agricultural applications. This means that the decisions you make about hardening IoT devices must of necessity be done on a case-by-case, device-by-device basis. There are a few things that organizations can do to help develop and enforce a hardened configuration for the IoT devices they field.

## THREE KEY STEPS TO IoT DEVICE SECURITY

The following simple steps can provide significant value from a security standpoint to help ensure a robust configuration over time.

The first step is to establish a process to identify new devices coming into the organization. There are two components to this:

1. Identification/discovery/inventorying of new devices

2. Integration of devices into a broader asset management approach

For the first, the discovery side of the equation, adopt a "belt and suspenders" approach. Specifically, use existing data sources, such as vulnerability assessment information, to help discover devices on the network that you might not expect or already know about. At the same time, build relationships with business and other teams to identify initiatives that involve bringing in specialized devices, business automation scenarios and other use cases that would necessitate special-purpose devices that you might wish to protect.

Integration of devices into your broader asset management approach, the second component, involves clearly demarking and establishing areas of accountability and responsibility for keeping devices protected, configured appropriately and in their optimal configuration from a security standpoint. In other words, ensure that it is someone's job to verify that these critical steps happen. In some cases, it might best be a job for the IT organization, but in other cases, the business teams or even third-party-vendor support personnel might best be suited for this task. Whatever is decided, assigning a point of responsibility will ensure that appropriate action is taken. It is also helpful to marry this information with the inventory information that you are capturing in the first step. This means that circumstances might dictate on a device-by-device basis who the responsible party is; ensure that this information is retained and tied to inventory.

The next key step is to do the legwork to understand the model for the IoT device security. Include mechanisms such as security configuration parameters that the organization can set. Again, this will be a device-by-device exercise. Since it's conceivable that the responsibility for ensuring the security of the devices in scope is distributed among different teams, it's helpful to document expectations and objectives about security goals. The scope of

**Integrating devices into your broader asset management approach means clearly establishing accountability and responsibility.**

this documentation can be both technical guidance to teams that have responsibility for oversight of securing certain devices, and the documentation can also address areas of security-related considerations to include in procurement activities, cases in which the security team might be only tangentially involved. For example, guidance can address requirements or guidelines for application testing techniques the device manufacturer uses, use of a trusted execution environment, requirements for encryption (including data in transit and also

data at rest) and so on.

The final suggested step to hardening IoT devices may sound trite, but keep in mind that the value of protection mechanisms addressing the rest of the network increases in value in light of IoT. This means that an essential step in limiting possible attacks on IoT devices is to get the rest of the house in order. Ideally, the savvy security practitioner will be doing this anyway, but IoT can provide additional impetus to do this well. Putting your security house in order includes testing activities such as vulnerability assessment, penetration testing and application security testing. It also includes "detective" controls (e.g., IDS), enhanced authentication and the like.

In short, the final step in hardening IoT devices is to use all the normative countermeasures in your toolbox for ensuring an overall robust security posture. —*Ed Moyle*

# Testing for IoT Security: Cover All Your Bases



THE INTERNET OF things has been a buzz term for the past several years. However, as the technology slowly trickles into our everyday lives, people are becoming more and more concerned with the security of these devices and the systems that run them. From cars to refrigerators, IoT is making its way into many households—and the backlash against IoT security is not unfounded. The importance of IoT security testing is increasing, and for good reason.

## IoT SECURITY UNVEILED

Last year, ethical hackers started showing off what they could do with networked automobiles. Fiat Chrysler recalled 1.4 million vehicles after two security researchers demonstrated they could remotely disengage the brakes and transmission of a 2014 Jeep Cherokee. The Tesla Model S was a topic of conversation at the DEF CON hacking conference when it was shown the car could be started using a laptop connected to the driver-side dashboard.

Medical devices are also potential targets for hackers. A group of students at the University of Alabama hacked the pacemaker inside a medical training robot using the device's Wi-Fi capabilities. Similarly, security expert Billy Rios found vulnerabilities in the drug infusion pumps used at a hospital after receiving surgery there. He claims the vulnerabilities could allow a hacker to remotely change the dosage of drugs administered with the pumps.

While these are all extreme situations with life-threatening consequences, organizations must be expected to properly secure their devices.

## TESTING IS A MUST-DO

Security is not an add-on feature; it must be built into the foundation of any given device.

The level of security held by a device is derived from both the architecture and coding choices made by developers. This is particularly important to keep in mind when working in IoT as a lot of security choices need to be made with the platform in mind. Commonly used security techniques, such as encryption, may be challenging for devices with little processing power. Although it is a challenge to create a secure IoT fleet, attention needs to be paid to data confidentiality and integrity, as well as the availability of IoT services.

A good way to start is by following the security practices defined by the Open Web Application Security Project (OWASP). OWASP guidelines include information about secure coding and firewall use in addition to application interface best practices. When securing your IoT fleet, the first order of business is to test the security of the device itself.

IoT security testing must be performed for common web application vulnerabilities such as cross-site scripting and cross-site request forgery, make use of public encryption algorithms when possible, and try to make the most out of firewall protection as certain devices may not support it. On the software side, make sure patches and updates can be digitally signed to prove legitimacy to the device. Devices should not assume all patching attempts are legitimate; an apparent patch could be a piece of malicious code.

In general, authentication should be as strong as possible. Test for weak passwords and mandate two-factor authentication for sensitive operations, such as setting changes. Use fuzz testing to send a wide variety of inputs to a device to probe for potential vulnerabilities related to buffer overflows or other unhandled exceptions. Also be sure to complete IoT security testing on port devices such as USBs to detect vulnerabilities. Minimizing the use of physical ports altogether will decrease the overall attack surface of your IoT device and reduce the chances of an attack. In the event that a breach does occur, it is important to enable security event logging for later analyses.

## EXTEND THE TESTING RANGE

Next comes the securing of the network interacting with your devices. First look at how data

is transmitted to the back end for processing; all communications should be encrypted. Protection of cloud services is also vital to the security of an IoT fleet, and some practices from securing the devices carry over to this. Use two-factor authentication and avoid weak passwords for cloud services, and test cloud interfaces for common web interface vulnerabilities.

It is also important to only collect and store data relevant to business operations. While a data breach on personal medical records is bad enough, if the same organization is also holding financial information it would make the attack much worse. Only store information that is relevant to business operations and customer care; this can help minimize the amount of confidential and sensitive information transmitted and stored off the device, which in turn reduces the amount of data that could be compromised in a data breach.

Building a secure IoT infrastructure and completing routine IoT security testing means covering all your bases; it includes both securing the devices themselves and the networks or cloud services they are connected to. Organizations looking to use IoT technology need to think in terms of securing the device, communications and the data collected all at the same time. The internet of things can be a powerful tool, but, much like superheroes in the movies, its greatest strength can be its greatest weakness.

*—Dan Sullivan and James Sullivan*

**ED MOYLE** *is director of emerging business and technology at ISACA. Moyle previously worked as a senior security strategist for Savvis Inc. and a senior manager with CTG. Prior to that, Moyle served as a vice president and information security officer at Merrill Lynch Investment Managers.*

**DAN SULLIVAN** *is an author, systems architect and consultant with over 20 years of IT experience with engagements in advanced analytics, systems architecture, database design, enterprise security and business intelligence.*

**JAMES SULLIVAN** *is a technology writer with concentrations in cloud database services, IoT and security. He is based out of Portland, Ore.*

**STAY CONNECTED!**

**Follow @SearchSecurity today.**

TechTarget

*Time to Toughen Up for IoT* is a SearchSecurity.com e-publication.

**Robert Richardson** | *Editorial Director*

**Kara Gattine** | *Executive Managing Editor*

**Brenda L. Horrigan** | *Associate Managing Editor*

**Robert Wright** | *Site Editor*

**Linda Koury** | *Director of Online Design*

**Jacquelyn Howard** | *Senior Director, Editorial Production*

**Doug Olender** | *Senior Vice President/Group Publisher*
dolender@techtarget.com

**TechTarget**
275 Grove Street, Newton, MA 02466
www.techtarget.com

© 2016 TechTarget Inc. No part of this publication may be transmitted or reproduced in any form or by any means without written permission from the publisher. TechTarget reprints are available through The YGS Group.

**About TechTarget:** TechTarget publishes media for information technology professionals. More than 100 focused websites enable quick access to a deep store of news, advice and analysis about the technologies, products and processes crucial to your job. Our live and virtual events give you direct access to independent expert commentary and advice. At IT Knowledge Exchange, our social community, you can get advice and share solutions with peers and experts.

COVER: FOTOLIA