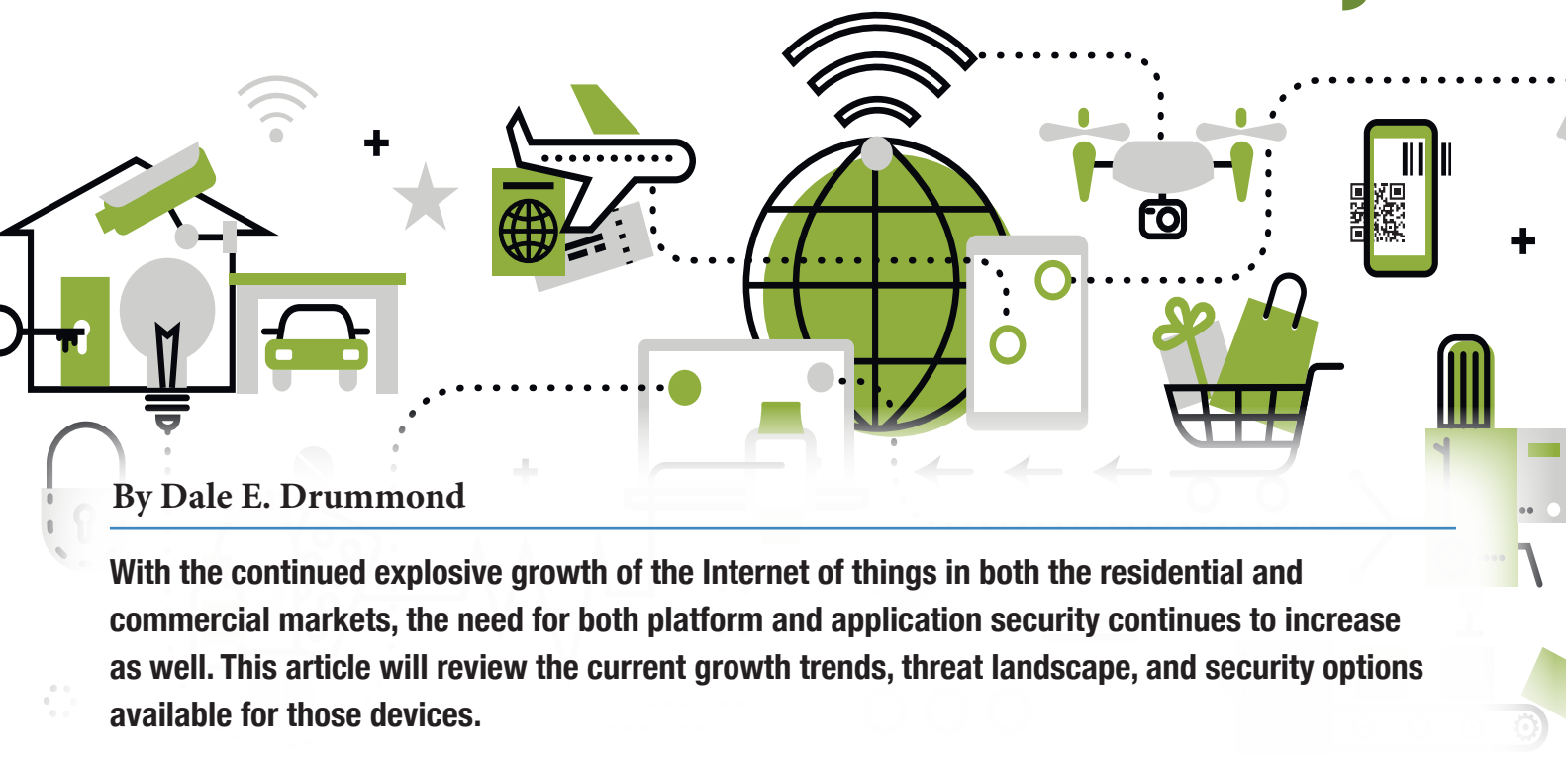
# Managing IoT Platforms with a Focus on Security



By Dale E. Drummond

**With the continued explosive growth of the Internet of things in both the residential and commercial markets, the need for both platform and application security continues to increase as well. This article will review the current growth trends, threat landscape, and security options available for those devices.**

**Abstract**

With the continued explosive growth of the Internet of things in both the residential and commercial markets, the need for both platform and application security continues to increase as well. This article will review current growth trends, threat landscape, and security options available for those devices. Consumer IoT devices are most often treated much like traditional plug-and-play devices: installed and configured by users then not thought about until the devices stop operating. For the end-users of those devices, security is often not considered at all. Commercial operators of IoT devices may include a security review as part of their deployment model; however, those devices often need to be secured using methods different than traditional computing platforms. Manufactures of IoT products, consumers, and commercial businesses using IoT platforms all must have a sharper focus on security to prevent malicious use of IoT devices after deploying them in the field.

The Internet of things (IoT) is continuing to grow at a record pace. In 2019 the number of IoT devices installed was projected at 8.3 billion, but the actual number of connected IoT devices was 9.5 billion [11]. This number of devices does not include "bring your own device" (BYOD) equipment such as laptops, tablets, and phones. Updated projections for 2025 place the IoT installed base at 28 billion devices [11]. Some of the technologies driving the increased growth for IoT are smart home technologies, wearables, and edge computing [12]. With the increase in the use of IoT platforms, there needs to be a sharper focus on securing these devices from attack. Microsoft published a report on IoT devices in 2019 that shows in 2017, 60 percent of the IoT devices tested stalled at the security phase of testing. In 2019, that percentage decreased to 30 percent [3]. While that decrease in the number of devices failing the security test is good news overall, having thirty percent of devices still failing to pass the security portion of the test suite is cause for continued concern. In addition to the above information, 84 percent of companies using IoT devices have reported a security event related to those devices [5]. These security events include firmware compromises, inadvertent listening due to a zero-day flaw, equipment being disabled by malicious code, and data leakage via a Bluetooth protocol defect [14]. That high percentage shows that a high volume of sensitive data is potentially vulnerable to attack, depending on the severity of the security incidents reported.

For consumer products such as smart thermostats, smart lights, and smart security cameras, once the device is sold to the end-user and deployed, it is up to the end-user to man-

age the updates for applications used to control the device. The manufacture may make updates available to be installed; however, it is the responsibility of the user to install those updates. These updates, targeted at the application software, usually do not include device firmware or platform operating system updates. Those application-focused updates can allow hardware and operating system vulnerabilities to go unaddressed.

IoT devices used by businesses often have similar management issues as the consumer products mentioned above. The organization managing the devices relies on the manufacturer for security, firmware, and application updates. Another, and in some situations more significant, challenge to maintaining updates on IoT devices is that all the devices operated by the business may not be local to the business itself. Devices located at a remote location still require management. Yet, at sites that the business does not own, restrictions limiting access to those devices by security personnel of the device's installed location are common. The time it takes to schedule access to the site and travel time to get to the site must be taken into account when determining the cost of maintenance for the remote IoT devices.

Additionally, the challenge of remotely managing IoT devices is the need to secure the communications channel between the device and the backend systems used to transmit data back to a central location for processing or used to send commands to make the device perform operations. All traffic between the IoT device and backend system should be reviewed, understood, and the appropriate security measures put in place to prevent unauthorized access to the data or command traffic.

This article will examine common security risks and management challenges associated with IoT devices. It will look at the existing frameworks available for securing and managing those devices and make suggestions on what methods are available to improve the security posture and management capabilities of devices.

## IoT security risks

Security exploits of IoT devices and their management systems have been in the news frequently over the past several years. The most recent exploit to effect IoT devices while not being a vulnerability on the devices themselves is the Garmin ransomware attack that occurred on July 23, 2020, which resulted in Garmin's internal network and several production systems becoming unavailable. This exploit prevented all of Garmin's IoT devices from transmitting data from the device to the backend system. It also took Garmin's help desk systems and call center offline, so the company was unable to respond to its customer inquiries or put out a notice of impact until some of the systems were restored [6]. This attack shows the importance of securing the management systems that communicate with the end-user IoT devices as well as the devices themselves.

The security challenges with Internet of things devices, according to *eForensics* magazine [17], are :

1. **The pace of deployment of Internet of things devices.** The concern isn't with the number of devices deployed but rather that the devices used are insecure with no easy way to improve the security of the device once implemented.
2. **Shadow devices deployed on the network.** Many companies are unable to detect when a new device connects to their network. This administrative blind spot allows for malicious devices to connect to the network with no oversight. It is possible to prevent shadow devices; however, there is a significant amount of system administration that must

happen to do so. Methods to avert shadow devices are dynamic host control protocol (DHCP), reservations tied to specific media access control (MAC) addresses, administratively disabling unused ports on networking equipment, and securing wireless networks using enterprise authentication that requires a username and password.

3. **Default or insecure passwords.** Manufacturers still use default passwords today. There are sites where you can look up what default passwords are for various protocols for different vendors [16].
4. **Limited effort for security testing by manufacturers.** The first-to-market mentality causes manufacturers to cut items from their development and testing plans. Often security is one of the first things cut since it is complicated, difficult to test, and expensive to do correctly.
5. **Increase in the number of attacks.** The more devices are connected combined with the success of previous attacks leads to a higher number of attackers, "trying things out" to see if they can also compromise a device or build a botnet.
6. **Data privacy and security.** The amount of data generated by IoT devices is predicted at 79.4 zettabytes by the year 2025 [8]. This data is critical to businesses operating effectively and efficiently. Protecting the information on the device, in transit, and on the aggregating systems is essential to ensuring companies can operate.
7. **Securing the communications infrastructure.** IoT devices are usually resource-limited. These limitations make it difficult to implement complex encryption algorithms on the devices [1]. There is still a need to secure communications in some way either through an increase in the resources available on the device, the use of more efficient encryption algorithms, or sacrificing some application performance for improved security.
8. **Botnets.** Increasingly large botnets, like the Mirai malware botnet in 2016 [13], continue to thrive on the Internet today. The rise in the value of crypto-currency led to an increase of botnets created to focus on blockchain development applications and blockchain IoT devices specifically.
9. **IoT automation.** The vast number of IoT devices and the data they generate require a large amount of system administration. The increase in deployed devices requires system administrators to rely on tooling and workflow automation for successful management.
10. **Home network access.** Home users may not have the technical knowledge to deploy their home network and connected devices in a secure manner. This insecurity leads to attackers placing shadow devices on a user's network or to the compromise of the user's equipment. More devices used in the home are "smart" or IoT devices, and due to their insecure nature tend to be ripe for inclusion into a botnet or to access other equipment on the home network.

The IoT security challenges listed above provide excellent examples of the reasons securing IoT devices, communications channels, and backend infrastructure should be top-of-mind for security professionals and operators alike.

## IoT management

Lopez et al. [10] examined IoT platforms and found that managing them have their own set of challenges:

1. Lack of detailed documentation of existing management frameworks
2. Number of programming languages and libraries available to control the platforms
3. Limited resources available on the devices
4. Each device can use multiple communications protocols

These challenges leave the task of determining how to manage the IoT device up to the person operating it. The lack of a unified company-wide IoT management strategy can lead to multiple management frameworks being available internally and possibly externally if they are published. Still, it also has the potential to lead to differing management frameworks deployed together in the same organization, with one operator developing one system and another operator developing another. This ships-in-the-night development effort leads to more work for the organization overall. It has the potential to create security issues if the company's information security group doesn't vet each framework.

## Existing IoT management frameworks

There is little unification on IoT management frameworks today. Each vendor implements its own management infrastructure for the devices they produce. The few management frameworks that operate on devices from multiple vendors are developed mainly for the consumer IoT market. This focus on the consumer market is due to manufactures hoping that the easy to use management framework will allow more users to adopt their hardware.

Some of the most popular IoT management frameworks for consumer IoT devices are:

### Closed Source

- Google Home Hub
- Apple Home kit
- Amazon Echo
- Wink Hub 2

### Open Source

- openHAB
- Home Assistant
- ioBroker
- Ubidots

The above-listed frameworks are primarily used for simplifying the integration of smart home automation devices like

smart lights, smart outlets, smart thermostats, and security cameras and designed with ease of use in mind. For consumer IoT products, the framework manages how the devices interact with the environment and other devices; however, each type of device uses the manufacturer's application to update the software and firmware on the devices in the event an update is needed.

For commercial IoT devices such as telemetry gathering devices, environmental monitoring, and Internet-attached control equipment, there is no unifying framework for defining how heterogeneous devices interact with the environment or other IoT devices. Each operating organization must decide the best way to manage the devices, based on the communication protocols each device supports, preferably under the umbrella of a well-developed, company-wide IoT security policy.

Some of the most popular frameworks for commercial IoT devices are:

- IFTTT
- Carriots
- Xively
- SmartThings

Each of the above frameworks will work for both commercial and consumer IoT devices. The extensibility of the above-listed frameworks for commercial IoT allows the user or team to develop the IoT management platform and add devices that may not be officially supported by the framework. To the extent each framework can be adapted to support new hardware independently of a new release of the framework, the software is dependent on each framework and how extensible it is.

Several researchers have proposed new IoT management frameworks to help companies develop their IoT management plan. The most common theme from the proposed frameworks is developing an architectural standard for device setup, configuration, deployment, data transmittal, and hardware and software updates. This standard architecture would allow the rapid addition of new IoT devices to an existing management platform and would not prohibitively increase the administrative overhead on the operations personnel.

## Proposed IoT management frameworks

There are many proposed management frameworks being published. Currently, there is no front runner as to which one will get adopted first. They all present unique solutions to the challenge of managing IoT devices.

### ManIoT — A 2-tier platform for IoT management

ManIoT breaks the control of IoT devices into local and global scope [2]. The local scope is the location where the IoT devices reside. In that scope there is a device known as a local manager with which the IoT devices register. The global scope is operated in the cloud, whether that is the operator's central office or a cloud service provider like Amazon AWS, Microsoft Azure, or Google Cloud Platform. The global manager is responsible for providing the high-level policies to the local managers, which in turn provide individual policies to the devices. The global manager can manage many local managers. A significant benefit of the 2-tier management is that it allows the management platform to be upscaled and downscaled easily as the demands of the locally installed devices change.

ManIoT is also extensible to allow for the addition of new devices, supports many different types of IoT devices, and has a focus on security and privacy. This framework is currently a prototype framework.

### RestThing — A restful web service infrastructure for mash-up physical and web resources

RestThing allows for the configuration of IoT devices using the representational state transfer (REST) method [15]. Using standard REST architecture enables the decoupling of specific device options from the handling of resources. Using RestThing, the configuration of a device is achieved through the standard HTTP verbs GET, POST, PUT, and DELETE. Using standard HTTP actions addresses potential compatibility issues with communications. The only requirement is that the

IoT device supports a webserver so the commands can be received and processed. For those devices that do not support transmission control protocol/Internet protocol (TCP/IP) communications, an adaptation layer would be needed to process the REST command and execute the configuration commands sent.

RestThing is extensible, allowing for the addition of new devices, and using adaptation layers can even support new sensors that only operate over radio or Bluetooth. This framework is currently a prototype framework.

### Things management protocol

The things management protocol isn't a full-blown management framework but rather a protocol that can be used by other frameworks and devices to facilitate integration between devices [7]. Similarly to RestThing, it allows for the creation of an adaptation layer for those devices that do not support TCP/IP communications. These adaptation layers create the opportunity to include many more sensor types into the IoT management platform. Using the Internet protocol (IP) layer, standard encryption methods are available to secure the traffic while in transit. The creators also defined the complete things management protocol (TMP) protocol datagram unit (PDU). This protocol is currently a theoretical implementation.

### Open Balena — A complete IoT management framework and application

The company that created it, Balena, released a version as an open-source project [4]. Open Balena is installed on the device as the operating system, and the individual applications run in containers on that operating system (OS). This base image allows for the application and operating system to be independently updated. There is a communications channel that allows the devices to communicate to the main controller at a central location.

Open Balena allows for remote upgrade of the operating system by partitioning the disk and upgrading the new image into the second partition, then setting a watchdog to trigger a reversion to the original OS if the device doesn't come online with the new OS within the watchdog time limit. It also communicates using standard encryption methods.

Open Balena is currently available for download and test. There is also a commercial version available from Balena.

Having numerous proposed frameworks and protocols allows for users, manufacturers, and companies to pick and choose the one that integrates the best with their products. A strong focus on open standards is required when evaluating a framework for managing IoT devices. This focus on standards will allow for the seamless integration of future devices that support open standards while allowing for existing devices to operate cohesively with future devices.

## IoT management security

Whatever framework is selected to manage the IoT devices deployed, it must have a strong focus on security. The section on IoT security risks shows that securing IoT devices should be a top priority for both manufacturers and users. Basic security practices like using secure HTTP via TLS [18] is a big step toward providing secure communications between IoT devices and the systems with which they communicate. Restricting access to the device by limiting the sources and destinations that the device can communicate with and configuring authentication, authorization, and accounting to define who can access the device, execute specific commands on the device, and generate a log of executed commands on the device are best common practices [18].

In 2017 researchers sent a survey to a broad set of industries querying them on the security incidents experienced related to IoT and the decision-making process behind their security posture. The researchers concluded that few companies spent money on securing IoT infrastructure based on best practices information available to them. Instead, management executed decisions made on financial or time constraints [9]. They recommend understanding the applicable laws required for security, if they exist, and implementing the required security measures based on the law and a thorough review of the security risk by the manufacturer's security personnel.

Lopez et al. [10] examined ten IoT major platforms to determine which met their defined IoT security criteria of authentication, authorization, accounting, encrypted information management, and anomaly detection. For the ten platforms analyzed only two, Amazon IoT and IBM Watson IoT, met all the criteria. After their analysis, they concluded that while IoT is changing the world, choosing the IoT platform to deploy must have security as a must-have requirement in the selection process. They also state that choosing the right IoT platform will have a significant impact on the success of the IoT deployment.

## Conclusion

Reviewed in this paper were the top security risks to IoT devices in 2020, IoT management frameworks, both consumer and commercially focused, and some of the more popular existing and proposed IoT management frameworks available today. Also reviewed was research into IoT management security. We can conclude after reviewing the research that making security a mandatory requirement for both your Internet of things devices and the management platform chosen to manage them is critical to a successful IoT deployment. Selecting devices that support robust security protocols and modern management methods will allow a company to operate securely while minimizing the risk of a compromise in their IoT network. The conclusions in this article are not specific to businesses that are deploying IoT devices. Home users deploying smart home devices are just as well served by taking the recommendations for security and management into consideration when choosing home automation devices.

### References

1. Abuagoub, A. M. A., "IoT Security Evolution: Challenges and Countermeasures Review," *International Journal*

# 4 COMMON CYBERSECURITY ASSET MANAGEMENT CHALLENGES & HOW TO SOLVE THEM.

By Nathan Burke, CMO, Axonius

If you're responsible for managing, securing, tracking, or even monitoring assets, you've probably come across a fair share of challenges. When talking with customers, we hear the same four challenges come up time after time.

## 1. AGGREGATING DATA

To have accurate, comprehensive visibility of your environment, you need to pull data about your assets from every possible source. That's easier said than done – but this essential step is foundational for solving every other challenge discussed below.

***Solving It***

When it comes to aggregating data, almost every tool that knows about an asset has an API. Whether you decide to use a product or go it alone, APIs are available for almost any tool that knows about assets.

## 2. FINDING UNMANAGED DEVICES

We're defining unmanaged devices as those unknown to a management system and without a security agent installed. An unmanaged device can be as innocuous as a webcam, or as significant as an unpatched Raspberry Pi connected to a production network.

***Solving It***

To discover unmanaged devices, gather data from the network (solutions like network management consoles and VA scanners) and data from agent-based solutions. This will help you understand which devices are network-connected and which are covered by agents. Then you can identify the devices that are present, but not managed.

## 3. INVENTORYING AT SCALE

It's the culmination of the first two cybersecurity asset management challenges: you need to pull data on all managed and unmanaged devices. While this can be done, it takes a really long time. We're talking 80+ man-hours – and it gets out of date quickly.

***Solving It***

To address issues of scale, it's important to have customizable data aggregation frequency per data source. For example, asking Active Directory to give real-time updates will negatively impact performance. But getting asset data from a public cloud provider should be as close to real-time as possible. Ultimately, scaling an asset inventory must accommodate the downstream impact of the source.

## 4. TESTING COMPLIANCE

Without that comprehensive inventory, it's impossible to understand whether all assets adhere to or deviate from compliance requirements. And without the ability to constantly monitor and validate how dynamic changes to the environment relate to compliance, point-in-time compliance checks become obsolete.

***Solving It***

The only way to test adherence is by understanding each compliance requirement and seeing exactly how every device, user, and security control map to what's mandated. For example, companies with a heavy public cloud footprint may choose to use the CIS Benchmarks to evaluate whether all cloud instances match industry best practices for security. For end user devices, organizations might use the CIS 20, NIST, or industry-specific regulations like HIPAA, PCI, or others to determine whether assets are compliant.

*of Communication Networks and Information Security*, https://search.proquest.com/docview/2354296086?accountid=10639.

2. Antunes, J. B. et al., "ManIoT: A 2-Tier Management Platform for Heterogeneous IoT Devices and Applications," *International Journal of Network Management*, https://doi.org/10.1002/nem.2034.
3. Azure, "IoT Signals," Microsoft, https://go.microsoft.com/fwlink/?linkid=2099329.
4. Balena, "Open Source Software to Manage Connected IoT Devices," https://www.balena.io/open/.



5. Bera, A. "80 Insightful Internet of Things Statistics (Infographic)," Safe At Last, https://safeatlast.co/blog/iot-statistics/.
6. Cimpanu, C. " Garmin Services and Production Go Down after Ransomware Attack," ZD Net, https://www.zdnet.com/article/garmin-services-and-production-go-down-after-ransomware-attack/.
7. Dai, G., "Design and Implementation on a Things Management Protocol for Internet of Things," in Proceedings of the 32nd Chinese Control Conference, https://ieeexplore.ieee.org/document/6640733.
8. Horwitz, L. "Top IoT Trends to Watch in 2020," IoT World Today, https://www.iotworldtoday.com/2020/01/26/top-iot-trends-to-watch-in-2020-2/.
9. Koo, C. et al., "Enforcing High-Level Security Policies for Internet of Things," *The Journal of Supercomputing*, https://doi.org/10.1007/s11227-017-2201-9.
10. López, D. D. et al., "Developing Secure IoT Services: A Security-Oriented Review of IoT Platforms," *Symmetry*, http://dx.doi.org/10.3390/sym10120669.
11. Lueth, K. L. "IoT 2019 in Review: The 10 Most Relevant IoT Developments of the Year," IoT Analytics, https://iot-analytics.com/iot-2019-in-review/.
12. Lynkova, D. "IoT Statistics and Trends to Know in 2020," Leftronic, https://leftronic.com/internet-of-things-statistics/.
13. Maker.io, "5 Leading IoT Security Breaches and What We Can Learn from Them," Maker.io, https://www.digikey.com/en/maker/blogs/2019/5-leading-iot-security-breaches-and-what-we-can-learn-from-them.
14. Penta Security, "Top 5 Shocking IoT Security Breaches of 2019," https://www.pentasecurity.com/blog/top-5-shocking-iot-security-breaches-2019/.
15. Qin, W. et al., "RestThing: A Restful Web Service Infrastructure for Mash-Up Physical and Web Resources," https://dx.doi.org/10.1109/euc.2011.59.
16. Selmeczy, P. "Default Router Login Details," Pro Privacy, https://proprivacy.com/guides/default-router-login-details.
17. Trimidal, C. "Top 10 IoT Security Challenges to Expect in 2020," eForensics Magazine, https://eforensicsmag.com/top-10-iot-security-challenges-to-expect-in-2020-by-cathy-trimidal/.
18. Zúquete, A. et al., "Security-Oriented Architecture for Managing IoT Deployments," *Symmetry*, https://doi.org/10.3390/sym11101315.

## About the Author

*Dale E. Drummond is a graduate student at East Carolina University in the College of Engineering and Technology pursuing his Master of Science in network technology with a concentration in computer network management. He is also a team lead/sr. network management engineer at MCNC. He ma be reached at drummondd16@students.ecu.edu.*