IoT Needs Better Security

También disponível em português
www.isaca.org/currentissue

The Internet of Things (IoT) is an ecosystem of connected things (stationary or mobile devices). A 2016 *Business Insider* report stated that there will be 34 billion devices connected to the Internet by 2020, up from 10 billion in 2015. Further, IoT devices will account for 24 billion of them, while traditional computing devices (e.g., smartphones, tablets, smartwatches) will comprise 10 billion. And, nearly US $6 trillion will be spent on IoT solutions over the next five years.[1]

Why Do We Need IoT Security?

Industry is changing fast and new IoT use cases are maturing. More and more functionality is being added to IoT systems for first-to-market advantages and functional benefits, while security of IoT system devices is often ignored during design. This is evident from recent hacks:

- The US Food and Drug Administration issued safety advice for cardiac devices over hacking threat, and St. Jude Children's Research Hospital patched vulnerable medical IoT devices.[2]
- Hackers demonstrated a wireless attack on the Tesla Model S automobile.[3]
- Researchers hacked Vizio Smart TVs to access a home network.[4]

Other sources of missed security opportunities occur during IoT installation and post-installation configuration. A ForeScout IoT security survey stated that "Respondents, who initially thought they had no IoT devices on their networks, actually had eight IoT device types (when asked to choose from a list of devices) and only 44 percent of respondents had a known security policy for IoT."[5] Only 30 percent are confident they really know what IoT devices are on their network.[6]

These hacks and the implications of the ForeScout survey results indicate that IoT security needs to be implemented holistically. This requires understanding IoT architecture.

IoT Architecture

The Zachman Framework[7] answers why, how, what, who, where and when questions around "IoT. The why question around IoT security has already been addressed herein. Answers to how and what questions are explained in the four "layers of architecture. **Figure 1** depicts "IoT security architecture explained through "questions to be answered through the Zachman Framework approach.

Figure 1—Zachman Framework Contextual Architecture for IoT Security

Questions	IoT Security
Why?	Examples of security breaches, threat modeling
How?	Device configuration and integration, standards, processes
What?	List of components and their relationships
Who?	User, administrator, vendor, industry bodies
Where?	At every layer and component in the architecture
When?	Design, configuration/implementation and operations

Source: H. Patel. Reprinted with permission.

Do you have something to say about this article?
Visit the *Journal* pages of the ISACA® website *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

Hemant Patel, CISM, ITIL, PMP, TOGAF
Is a principal advisor at Computer Sciences Corporation, SC, as a part of the US Chief Technology Officer team. His expertise includes IT enterprise architecture, information security, portfolio planning, big data, web and e-commerce, analytics, enterprise resource planning and customer relationship management systems. His global experience includes working in the defense, manufacturing, health care, utilities, banking and insurance industries. Patel can be contacted at hpatel63@csc.com or mr.hemant.patel@hotmail.com.

Enjoying this article?

- Read *Internet of Things: Risk and Value Consideration.* *www.isaca.org/internet-of-things*
- Learn more about, discuss and collaborate on security policies and procedures in the Knowledge Center. *www.isaca.org/information-security-policies-and-procedures*

A high-level conceptual understanding of IoT needs to exist in order to understand IoT security requirements. Information flows from the edge layer (i.e., IoT devices, assemblies/machines) to the data layer to the business intelligence (BI) layer to the operations and strategy (OpS) layer, as shown in **figure 2**. A local network or a wide area network connects devices and layers. Often, many devices are grouped to support an assembly of components or a machine. Interdevice communication may or may not be present in an assembly or a machine. Devices and assemblies connect to a hub or a gateway to encapsulate unique device features and for better standardization and management.

A holistic security approach includes security for every layer and communications security between the layers. Layers other than the edge layer may be hosted on premises or in the cloud. It is important to understand the security requirements in each of the layers.

Edge Layer Security

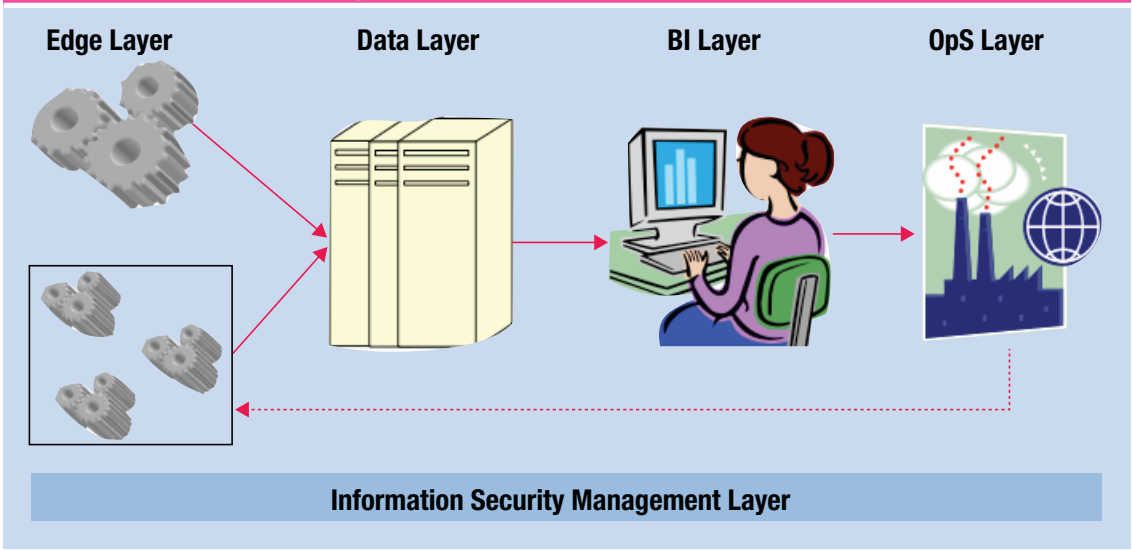
IoT security should be part of the broader topic of information security. Edge layer devices/sensors produce data that are processed by upstream components of the IoT architecture. The volume of data is much more than, and unlike, the volume of data produced by Internet user activity.

There is significant competition in the device-based security and IoT hub/gateway management software space, and there is a plethora of standards. Organizations such as Microsoft, IBM and Allegro have done good work in wrapping device-based security in higher-level application programming interfaces (APIs) and tools. The basic building blocks of the edge layer security architecture are depicted in **figure 3**. The hub, or the gateway, supports security administration, storage management and communications components related to IoT security.

> **"A holistic security approach includes security for every layer and communications security between the layers."**

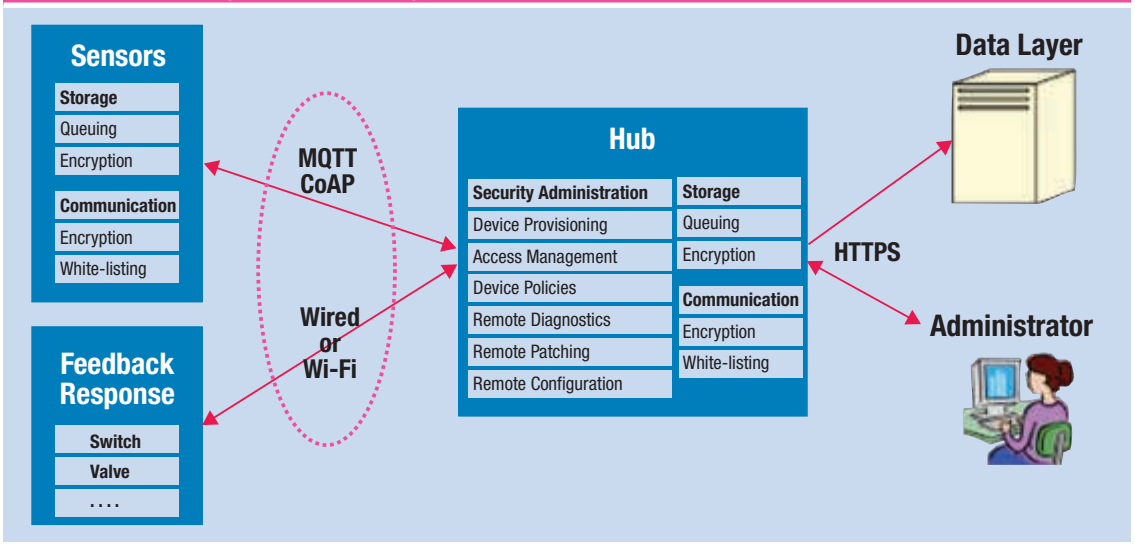
Devices may interconnect or communicate with hubs, and such communication software needs a smaller footprint with queuing capabilities. Transmission Control Protocol (TCP) socket-based, peer-to-peer communication was used earlier, which was then followed by better protocols, including:

Figure 2—IoT Conceptual Architecture



Source: H. Patel. Reprinted with permission.

Figure 3—IoT Edge Layer Security Conceptual Architecture



Source: H. Patel. Reprinted with permission.

- **Message Queuing Telemetry Transport (MQTT)**—A TCP-based protocol supporting device authentication, Secure Sockets Layer (SSL)/Transport Layer Security (TLS) encryption, queuing and publish-subscribe capabilities
- **Constrained Application Protocol (CoAP)**—A User Datagram Protocol (UDP)-based transport, supports microdevices and has a much smaller footprint than HTTP. It supports Advanced Encryption Standard (AES) encryption.[8]

A wireless local area network (WLAN) is used in many sectors with WPA2 security. Wi-Fi security is most commonly hacked due to inadequate security configuration and poor choice of passwords. A gateway may connect to multiple hubs and provide higher-level data transfer protocols such as HTTPS, which supports TLS encryption and Representational State Transfer (REST)-Simple Object Access Protocol (SOAP) messaging.

Device and hub vendors need to support security protocols and management, as described herein, and this support can get complicated due to multiple protocols and supporting authentication through the protocols.

Another issue to monitor is IoT device malfunction. A malfunction can occur due to a security breach or for other reasons. A malfunction can result in a device retrying to access data and, without a proper configuration limiting the number of retries, there can be an infinite number of retries. When each retry sends an error message back to the hub, the hub can end up getting infinite error messages (similar to a distributed denial-of-service [DDoS] attack) and the IoT hub can become nonoperational due to excessive load, thus affecting availability of the hub.

A malfunction may stop an IoT device from generating data. This results in the hub not receiving any data, which affects the integrity of the hub. Thus, a device malfunction can affect the availability and integrity (basic qualities of information security) of IoT security.

Data Layer Security

The data layer includes activities such as data ingestion, data engineering and data transformation using Structured Query Language (SQL) or NoSQL technologies with traditional databases/warehouses or big data technologies. SQL-based databases offer row-column-and cell-level securities. Earlier big data technologies offered only file or operating system (OS)-level security, but now offer lower-level security, for example, Apache Sentry[9] with role-based authorization.

Security sublayers in this layer include network security, authentication and authorization, masking and/or industry standard encryption of data storage and data management. Data management commands a separate discussion, but includes enterprise data architecture, data

lineage, auditing and governance. A bad data architecture and/or poor management of data lineage could compromise data consistency and availability.

Confidentiality needs to be maintained by adhering to various industry standards such as the US Health Insurance Portability and Accountability Act (HIPAA) and the Payment Card Industry Data Security Standard (PCI DSS) governing storage, access and transmission of data. A previous *ISACA® Journal* article, "Back to the Future in Device Security: Leveraging FIPPs to Proactively Manage IoT Privacy and Security Risk,"[10] explains designing privacy considerations in processing data generated from IoT components.

BI Layer Security

Data masking, role-based authorization and single sign-on (SSO) provide security in this layer in addition to network security and firewalls. BI (predictive, prescriptive) model management is an information governance topic. Sufficient testing and validation are required for such models. Use of flawed intelligence can lead to ill-informed business decisions, which can ruin an organization's reputation and credibility.

Data loss prevention (DLP) and backup technologies need to be considered for additional security.

OpS Layer Security

A feedback loop may exist from operation applications/systems to the devices. Traditional network security and firewalls, role-based application access and authorizations, and SSO provide security in this layer.

DevOps tools minimize the risk of an incorrect build and/or misconfiguration, which could affect the availability of the system.

> **"A device malfunction can affect the availability and integrity (basic qualities of information security) of IoT security."**

A strategy may decide a course of action based on BI results. A strategy can be just monitoring data received from IoT devices, or it can include processing data received from IoT devices and altering the behavior of IoT devices based on acceptable limits of data readings from the devices. Both the strategy (requirement and design) and feedback loop (implementation) need to be validated/tested.

Threat Modeling and Risk Management

Figure 2 shows an optional feedback loop from the OpS layer to the edge layer. In cases when the feedback loop is missing and data from devices are deemed to be nonsensitive, data access and encryption security may be lowered in conformance with proper risk management.
Risk mitigation and response strategies may be based on the following questions:

- Can a compromised device compromise other devices or the hub?
- How quickly can a compromised device be detected and isolated?
- What is the impact of a compromised device?

> **"IoT security does not mean only device-level security; it should be applied to all components and layers of the IoT system."**

These questions are not comprehensive and should be used as initial guidance for risk management.

Conclusion

IoT security often lacks priority consideration when IoT systems are being designed and implemented. IoT security does not mean only device-level security; it should be applied to all components and layers of the IoT system. Security needs to be addressed at all stages of the IoT system life cycle, including the design, installation, configuration and operational stages.

Additionally, strong passwords and certificate keys, difficult-to-guess device or host names/identifiers, log monitoring and analysis, proactive user and device management, and adherence to industry guides and security recommendations from organizations such as the US National Institute of Standards and Technology and the International Organization for Standardization will complement the security of the IoT system.

Endnotes

1 BI Intelligence, "Here's How the Internet of Things Will Explode by 2020," *Business Insider*, 31 August 2016, *www.businessinsider.com/iot-ecosystem-internet-of-things-forecasts-and-business-opportunities-2016-2*

2 Bacon, M.; "St. Jude Medical Finally Patches Vulnerable Medical IoT Devices," *TechTarget*, 13 January 2017, *http://searchsecurity.techtarget.com/news/450410935/St-Jude-Medical-finally-patches-vulnerable-medical-IoT-devices*

3 Golson, J.; "Car Hackers Demonstrate Wireless Attack on Tesla Model S," *The Verge*, 19 September 2016, *www.theverge.com/2016/9/19/12985120/tesla-model-s-hack-vulnerability-keen-labs*

4 Zorz, Z.; "Researchers Hack Vizio Smart TVs to Access Home Network," *Help Net Security*, 12 November 2015, *https://www.helpnetsecurity.com/2015/11/12/researchers-hack-vizio-smart-tvs-to-access-home-network/*

5 ForeScout, IoT Security Survey Results, *https://www.forescout.com/iot-security-survey-results/*

6 *Ibid*.

7 Zachman, J.; "The Concise Definition of the Zachman Framework," Zachman International Enterprise Architecture, 2008, *https://www.zachman.com/about-the-zachman-framework*

8 Eclipse, MQTT and CoAP, IoT Protocols, *www.eclipse.org/community/eclipse_newsletter/2014/february/article2.php*

9 Sentry, Apache Sentry, *http://sentry.apache.org/*

10 Rotman, D.; C. Kypreos; S. Pipes; "Back to the Future in Device Security: Leveraging FIPPs to Proactively Manage IoT Privacy and Security Risk," *ISACA® Journal*, vol. 6, 2015, *https://www.isaca.org/Journal/archives*