Managing the Risk of IoT

Regulations, Frameworks, Security, Risk and Analytics

Também disponível em português
www.isaca.org/currentissue

Does the recent distributed denial of service (DDoS) attack on Dyn[1] officially mark the passing of the Internet of Things (IoT) fear, uncertainty and doubt (FUD) stage, or is this still the beginning of the stage? IoT FUD pertains to IoT vulnerabilities leading to loss of data, service and possibly life. Traditionally, FUD about a security breach or regulatory noncompliance is the primary driver for management to invest in information security. The same FUD applies to IoT security, although it involves multiple variables that need to be considered. The resolve to address IoT device security at various levels—hardware and software, government and enterprise, consumers and services—is widespread. This soaring resolve is primarily due to the sheer quantity of IoT devices that are available and the ease with which these devices can be compromised and converted into thingbots. Thingbots are botnets of infected IoT devices that can be used to launch attacks that are like the Dyn attack, which affected more than one million devices, of which about 96 percent were IoT devices.[2, 3]

The primary issue is with IoT device hardware, which is manufactured mostly outside of the United States and needs to be regulated.[4] The retail industry sector has been the leading adopter of IoT technology because it reaches out directly to numerous customer bases, unlike the health care sector, which does not have benefits that are transparent immediately to the end user and has higher risk.

IoT Security—The Game Plan

The game plan for IoT security provides an overview of the IoT ecosystem and addresses standards, frameworks and regulatory proposals that have developed recently. **Figure 1** depicts an IoT ecosystem in which information security forms an integral part.

IoT Standards and Framework Developments
A positive repercussion of the Dyn DDoS attack was the US Department of Homeland Security (DHS) release, in 2016, of principles and guidelines for securing the IoT.[5, 6] These guidelines are not legally mandatory, but are definitely a sign of a good start toward IoT device security. Some of these guidelines are well-known mantras to most security professionals in the game:

- Leverage security from the feasibility phase.
- Apply security updates, patching and vulnerability management.
- Follow proven security practices.
- Prioritize controls based on the magnitude or impact.
- Provide oversight and proper governance of the IoT.
- Plug in the device off of the network if there is no absolute business need.

Also in 2016, exemptions to the US Copyright Law were approved that allow independent researchers to be able to hack almost any IoT device.[7] Although numerous limitations apply to the exemptions, they were granted for two years. This will help researchers unlock software for their research

Figure 1—IoT Ecosystem

Source: I. Atluri. 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.

Indrajit Atluri, CRISC, CISM, CEH, CISSP, CSSLP, HCISPP, ITILv3
Is a cyber security professional with expertise in IT governance, risk management and compliance. His current focus areas include security of emerging technologies, such as the Internet of Things, big data and security analytics, and their implications on information risk and privacy. Atluri is associated with the information security firm Secur80. He can be reached at iatluri@secur80.com.

without any legal implications. The intentions are right, but the impact of this change, positive or negative, is yet to be seen.

The Industrial Internet Consortium, primarily comprised of IoT-related enterprises, rolled out the Industrial Internet Security Framework (IISF), which outlines best practices to assist developers and end users with gauging IoT risk and possibly defending against this risk.[8] In early 2017, the US Federal Trade Commission (FTC) announced that it is granting prize money to anyone who develops an innovative tool that detects and protects home devices from software vulnerabilities.[9]

"If there is not a profit or cost benefit for the manufacturer to patch a less frequently replaced product, there is no drive for the manufacturer to patch it regularly; hence, it should be regulated."

Another recent development in IoT security is the Sigma Designs S2 security framework, which will be part of every Z-Wave-certified IoT device that is manufactured after March 2017 and is backward-compatible on existing Z-Wave IoT chipsets, making the devices more secure.[10]

Regulatory Proposals

Cyber security researcher and Harvard University lecturer Bruce Scheiner recently proposed a more regulated IoT industry in a meeting with two US House of Representatives' subcommittees—the Subcommittee on Communications and Technology and the Subcommittee on Commerce, Manufacturing and Trade.[11] He presented the comparison of the cost versus the incentive and drive for IoT device manufacturers to patch vulnerabilities periodically. Scheiner pointed out that most IoT devices provide lower profits and that the more frequently replaced devices, such as smartphones, are patched more often, compared to devices that are seldom replaced, such as thermostats and refrigerators. Smart cars and Blu-ray players fall in between. IoT thermostats and refrigerators that are not likely to be replaced are at a higher risk, if they are not patched. If there is not a profit or cost benefit for the manufacturer to patch a less frequently replaced product, there is no drive for the manufacturer to patch it regularly; hence, it should be regulated. The other side of this argument is that regulation of the IoT industry would stunt the growth of innovation.

The US Food and Drug Administration (FDA) has been providing some guidance to manufacturers on the best practices to build security into medical devices since October 2014. In December 2016, the FDA added a guide that lists the best ways to secure medical devices after they enter the consumer's hand, primarily to prevent any harm to patients. The guide also states that the IoT device manufacturers need to report to the FDA if the use of a device had resulted, or can result, in any kind of serious harm or the death of a person. Reporting to the FDA is waived only if customers and device users are notified about the vulnerability in the device within 30 days, the device is fixed within 60 days, and this information is shared with the Information Sharing and Analysis Organization (ISAO).[12, 13] The premise is somewhat similar to the optical character recognition (OCR) sanctions on US Health Insurance Portability and Accountability Act (HIPAA) violations, but the difference is that the FDA guides are just recommendations and are not legally binding. It is believed that these guides will eventually lead to legislation, as in the case of HIPAA.

More recently, the US Senate Commerce Committee approved the Developing Innovation and Growing the Internet of Things (DIGIT) Act. It is currently waiting on approval from the full senate. The DIGIT Act creates a working group that would focus on the security, privacy and other issues relating to IoT.[14]

The Game of IoT Security

The number of connected IoT devices is estimated to reach 200 billion by 2020.[15] Similarly, it is estimated that approximately 4 billion people will be online by 2020.[16] The online exposure increases multifold by 2020 for the simple reason that human-to-machine (H2M) interactions increase along with the machine-to-machine (M2M) interactions.

The IoT Arena

Figure 2 shows a conceptual IoT architecture. The IoT devices fall generally into one of two categories—one type of device interacts with a gateway and the other has a gateway built into the

device. The second category of devices includes mostly devices that need to be in constant motion, e.g., smart cars and fitness wearables.

Defense

Defense starts at the chip or hardware level. The hardware on which the IoT device is built forms the basis for a robust and secure IoT device. This is like laying a strong foundation for a house to ensure a stable and sustainable end product.

Device-Manufacturer Level

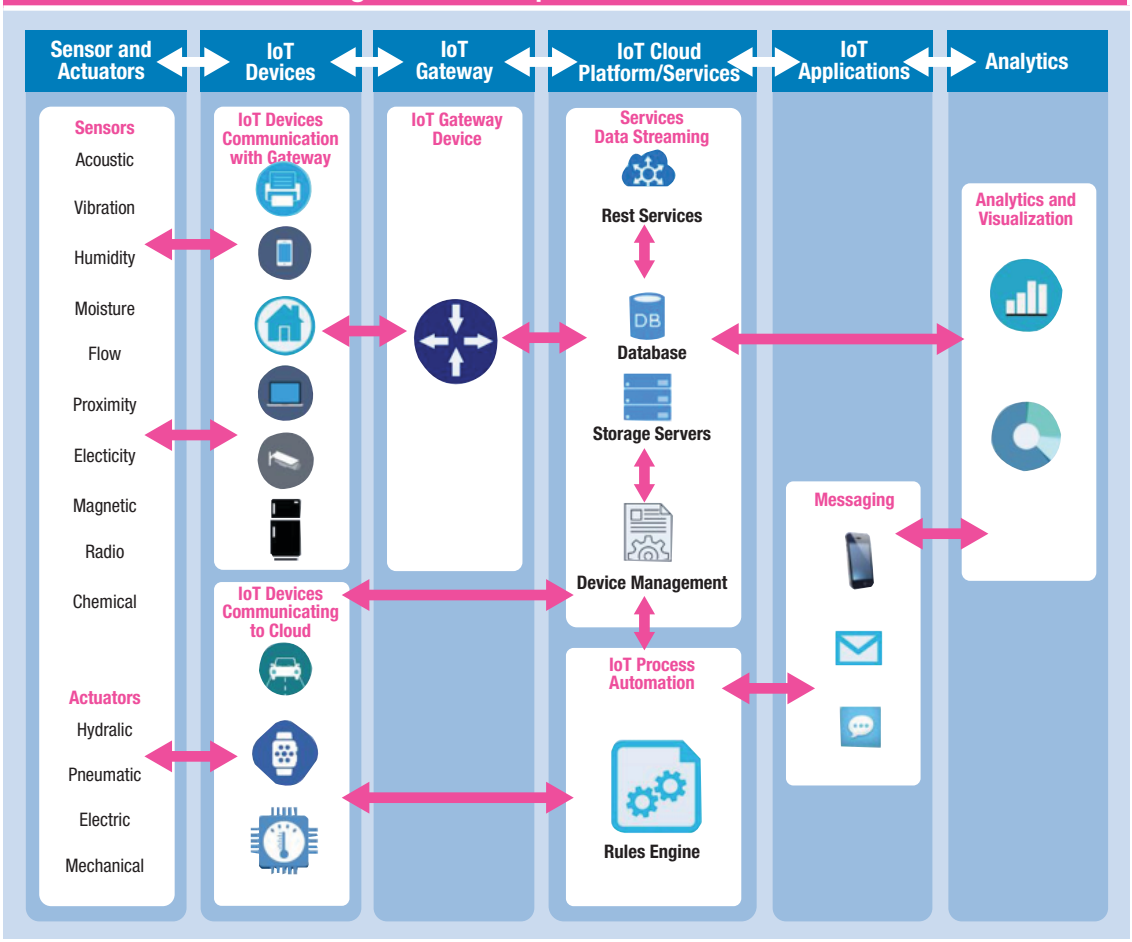
As shown in **figure 1**, the chip and hardware of the IoT device is where the life cycle of an IoT device starts and is also the right time to steer the process in the right path.

Hardware

Primary threats to an IoT device at the hardware level are that it can be stolen, physically modified, replaced and cloned. Hardware vulnerability examples include prebuilt weak default passwords or hard-coded credentials and counterfeit integrated circuits.

The nonprofit Internet of Things Security Foundation (IoTSF) aids all IoT manufacturers, vendors and end users to help secure IoT devices.[17] Nevertheless, the best countermeasure to combat the hardware vulnerabilities is to regulate the process of manufacturing an IoT device. The manufacturers of IoT devices need to be accountable for not adhering to the appropriate IoT regulatory standards (there are not any standards at the time of this writing), industrial standards and/or guidelines. Today, there are no legal implications for not following the standards, but there can be a pushback at the enterprise level in adopting a substandard IoT device from a manufacturer. This pushback can prevent most hardware vulnerabilities

Figure 2—Conceptual IoT Architecture



Source: I. Atluri. Reprinted with permission.

Enjoying this article?

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

and software weaknesses that may be inherently available in IoT devices. If hardware vulnerabilities are not mitigated, the rest of the controls, methodologies, frameworks, time, resources and investment to make IoT devices secure cannot be effective. Some of the regulations and pushback need to be driven by the respective governments, with assistance from the security community.

"Today, there are no legal implications for not following the standards, but there can be a pushback at the enterprise level in adopting a substandard IoT device from a manufacturer."

Software

Major threats to the software or firmware on IoT devices are that the software can be modified or decompiled to extract credentials and leveraged to perform the DDoS attacks. The vulnerabilities at the software level are:

- Insecure code
- Hard-coded default passwords
- Improper software testing leading to backdoors
- Absence of strong authentication during M2M,

H2M and machine-to-human (M2H) interactions

The Open Web Application Security Project (OWASP) helps IoT manufacturers build secure IoT software and periodically categorizes the top 10 IoT software vulnerabilities.

Enterprise/Network Level

Like other network devices, the most common IoT device threats at the enterprise/network level are eavesdropping, man-in-the-middle (MiTM) attacks and bandwidth theft. The suggested three steps to protect against these threats are:[18]

1. Identify and inventory the IoT devices in the enterprise and make sure they are integrated into the enterprise asset management program.
2. Define standards and baselines for the IoT device security based on enterprise policies and standards.
3. Implement the necessary security controls to mitigate IoT risk.

Segmentation of all of the IoT devices onto a separate network zone is recommended, which makes it easier to quarantine the entire IoT zone in the case of a breach.[19] The rest of IT can continue its operations without any major impact.

If segmentation and zoning are not feasible, adopting a software-defined networking (SDN) model that not only improves IoT security, but also helps with identifying the location of the breach is suggested.[20]

Other commonplace controls that need to be implemented for IoT devices are the same controls that apply to most of the IT infrastructure today. They are two-factor authentication, stronger passwords or key-based authentication.

It is of paramount importance to realize that the key to having these defense methodologies work as expected is to secure the IoT devices and the network from the day that they are introduced into the network. If not, the possibility is high that these IoT devices are hackable forever and they will not be able to be patched and secured. If such a rogue IoT device is detected, it should be replaced immediately.[21]

IoT devices need to be able to carry out a multifactor authentication, e.g., phone the human user/owner of the IoT device, before the user/owner performs the security update.

Public key infrastructure (PKI) authentication for communication between IoT devices and gateways is a recommended countermeasure to prevent an IoT device from being jailbroken to install unauthorized software. Only certified software should be permitted to be installed during upgrades and patching.

Frameworks are being introduced that can help to implement a robust security model for IoT devices. The KeyScaler 5.0 product from Device Authority offers certificate and key provisioning specifically for IoT devices during the registration process.[22]

Offense

The best defense always starts with a good offense. Early detection and preventing attacks in real time is the priority for security teams and has become the new mantra. Many recent breaches happened months ago or in some instances years ago (e.g., the Yahoo breach), before they were detected and the response processes began.[23]

Testing

Quality testing of the IoT software is altogether different from traditional software testing. Autonomy, connectivity and momentum are the three factors that make IoT software-quality testing different from traditional software testing.[24] The concept that security is a process and not an add-on feature is well known. The IoT software testing for weaker passwords, buffer overflow vulnerabilities, etc., must follow the OWASP best practices. IoT devices should also be tested on universal serial bus (USB) ports for vulnerabilities. The key is to reduce the attack surface of the IoT device to the maximum extent possible. Additionally, like any other IT system that is close to the Internet, one should store, transmit and process only the minimum amount of sensitive information.[25]

IoT Risk Management

Forescout categorizes IoT devices into three levels:

- **Disastrous**—IP-connected devices that are hooked directly to the Internet are at high risk. They can cause damage to the enterprise by gaining access to sensitive information or cause critical infrastructure impairment.
- **Disruptive**—Interconnected systems, such as the voice over Internet protocol (VoIP) phones and printers, can result in disruption in business operations.
- **Damaging**—Devices such as smart bulbs and refrigerators can be used to snoop around the enterprise network to possibly gain access to metadata about the network.[26]

FDA guidance recommends that device manufacturers form or join an information sharing and analysis organization (ISAO), which is similar to the information sharing and analysis centers that exist today. An ISAO can help participating organizations by sharing looming security threats and risk in real time and devising appropriate responses in a timely manner.

> **"The key to having these defense methodologies work as expected is to secure the IoT devices and the network from the day that they are introduced into the network."**

Analytics and Detection

Recent advancements in data analytics improvises the actionable intelligence metric for security. Products such as Adaptive Defense not only provide security teams with information on the executables that enter the network, but also proactively confirm an incident, rather than just alerting for all suspicious events.[27] PatternEx combines artificial intelligence (AI) with analyst intuition to offer a threat prediction platform that detects current and emerging threats in real time across the enterprise. This will and should be the trend going forward, especially with the limited resources and analysts, continuous monitoring, security budgets, and more devices being added to the network creating still more ways to get hacked. Determining the point at which an intrusion actually happened after detecting that it happened is the key. AI can, hopefully, reduce the time and resources that are needed to detect an intrusion soon.

Team IoT Governance

The risk of an insecure IoT device is relative based on the domain in which it is operated and the jurisdiction in which it thrives. For example, privacy is at utmost risk when the device handles protected health information (PHI), compared to when it is in an industrial set up, in which the infrastructure or services are at risk. The geography of where the IoT device operates also matters because the legal and regulatory bindings can differ from place to place. The governance of IoT devices needs to be handled separately, but under the IT governance umbrella. The four critical success factors that contribute to an effective IoT project are an efficient IoT project management team, a project stakeholder who has the authority to drive the IoT project, data and telecommunication infrastructure to support IoT, and subject matter experts to maintain high data quality and integration issues.[28]

> **"The governance of IoT devices needs to be handled separately, but under the IT governance umbrella."**

At a project-management level, the eight steps[29] that can help enterprises to put in place a sustainable IoT security program are:

1. Identify information
2. Prioritize the devices
3. Evaluate data loss risk
4. Evaluate IoT access risk
5. Perform IoT incident response planning
6. Formulate a big data strategy to manage the vast amount of IoT data generated
7. Devise policies for privacy of sensor data
8. Protect IoT devices

Conclusion

The IoT footprint will vary in size based on the industry vertical. As enterprises move forward on the IoT bandwagon to be more profitable and to be able to reach out to an extended customer base, they need to have an IoT strategy that encompasses the entire IoT device life cycle (from procurement to end of life) in place. Enterprises need to build an IoT risk strategy that evaluates and manages risk. Consider IoT as part of the overall security and risk management portfolio and have a dedicated focus on continuously evaluating and monitoring IoT risk. Early adoption of security into the IoT device life cycle, at the hardware and software level, is the best practice.

The FUD factor mentioned earlier will continue to drive management to invest in information security and, more specifically, IoT security in the near future, at least until the risk of breaches reduces.

Endnotes

1 York, K.; "Dyn Statement on 10/21/2016 DDoS Attack," Oracle, 22 October 2016, *http://dyn.com/blog/dyn-statement-on-10212016-ddos-attack/*
2 *Ibid*.
3 Martin, C.; "U.S. to Issue IoT Principles After Internet Cyberattack," *MediaPost*, 26 October 2016, *www.mediapost.com/publications/article/287614/us-to-issue-iot-principles-after-internet-cybera.html*
4 Atluri, I.; "The Rewards and Risks of Our Smarter Future," *InfoSecurity Professional*, International Information Systems Security Certification Consortium, Inc. November/December 2014, *www.isc2.org/uploadedfiles/(isc)2_member_content/member_resources/infosecurity_professional_magazine/infosecurity-professional-magazine-nov-dec-2014.pdf*
5 *Op cit,* Martin
6 Martin, C.; "U.S. Issues Guidelines for IoT Security," *MediaPost*, 18 November 2016,

www.mediapost.com/publications/article/289288/us-issues-guidelines-for-iot-security.html

7 Armerding, T.; "Feds Provide Legal Loophole to Hacking IoT Devices," *CSO*, 28 November 2016, *www.csoonline.com/article/3144648/internet-of-things/feds-provide-legal-loophole-to-hacking-iot-devices.html*

8 Lawson, S.; "Industrial IoT Inches Toward Consensus on Security," *ComputerWorld*, 19 September 2016, *www.computerworld.com/article/3122244/internet-of-things/industrial-iot-inches-toward-consensus-on-security.html*

9 Federal Trade Commission, "FTC Announces Internet of Things Challenge to Combat Security Vulnerabilities in Home Devices," USA, 4 January 2017, *www.ftc.gov/news-events/press-releases/2017/01/ftc-announces-internet-things-challenge-combat-security*

10 Zurier, S.; "Z-Wave Alliance Ups IoT Security," *SC MEDIA*, 12 December 2016, *www.scmagazine.com/z-wave-alliance-ups-iot-security/article/578656/*

11 Gross, G.; "US Lawmakers Balk at Call for IoT Security Regulations," *CSO*, 16 November 2016, *www.csoonline.com/article/3141920/security/us-lawmakers-balk-at-call-for-iot-security-regulations.html*

12 CNBC, "New Cybersecurity Guidelines for Medical Devices Tackle Evolving Threats," *The Verge*, 29 December 2016, *www.cnbc.com/2016/12/29/new-cybersecurity-guidelines-for-medical-devices-tackle-evolving-threats.html*

13 Food and Drug Administration, "Postmarket Management of Cybersecurity in Medical Devices: Guidance for Industry and Food and Drug Administration Staff," USA, 28 December 2016, *www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM482022.pdf*

14 Zurier, S.; "No Clear Policy," *SCMagazine*, March 2017, *https://media.scmagazine.com/documents/287/0317_digital_edition_71636.pdf*

15 Sun, L.; "IoT Stocks: What to Watch in 2017," *The Motley Fool*, 23 November 2016, *www.fool.com/investing/2016/11/23/iot-stocks-what-to-watch-in-2017.aspx*

16 Microsoft Secure Blog Staff, "The Emerging Era of Cyber Defense and Cybercrime," *Microsoft Secure Blog*, 27 January 2016, *http://blogs.microsoft.com/microsoftsecure/2016/01/27/the-emerging-era-of-cyber-defense-and-cybercrime/*

17 Dickson, B.; "Why IoT Security Is So Critical," *TechCrunch*, 24 October 2015, *https://techcrunch.com/2015/10/24/why-iot-security-is-so-critical/*

18 Moyle, E.; "Three Steps to Better Security in IoT Devices," *TechTarget*, July 2016, *http://internetofthingsagenda.techtarget.com/tip/Three-steps-to-better-IoT-device-security-in-the-enterprise*

19 Kerravala, Z.; "How Network Segmentation Provides a Path to IoT Security," *NetworkWorld*, 17 December 2015, *www.networkworld.com/article/3016565/security/how-network-segmentation-provides-a-path-to-iot-security.html*

20 D'Abreo, C.; "What CIOs Need to Know About IoT and Security Risks," Masergy Blog, 21 October 2015, *www.masergy.com/blog/what-cios-need-know-about-iot-and-security-risks*

21 SecureRF, "Why Dyn Suffered a DDoS Attack and How Consumer IoT Device Security Vulnerabilities Can Be Addressed," 23 October

2016, *www.securerf.com/dyn-suffered-ddos-attack-consumer-iot-device-vulnerabilities-can-addressed/*

22 Stephenson, P.; "Access Control," *SC Magazine*, 14 December 2016, w*ww.scmagazine.com/access-control/article/577086/2/*

23 Cross, K.; "This Is the New Reality for Cyber Security: Accept That Hackers Will Get In," *MarketWatch*, 10 December 2016, *www.marketwatch.com/story/this-is-the-new-reality-for-cyber-security-accept-that-hackers-will-get-in-2016-12-09*

24 Lawton, G.; C. McKenzie; S. Raman; "IoT Applications Pose New Problems for Developers," *TechTarget*, February 2016, *http://internetofthingsagenda.techtarget.com/ehandbook/IoT-applications-pose-new-problems-for-developers*

25 Sullivan, D.; J. Sullivan; "IoT Security Testing: Cover All Your Bases," *TechTarget*, May 2016, *http://internetofthingsagenda.techtarget.com/feature/IoT-security-testing-Cover-all-your-bases*

26 ForeScout Technologies, Inc., *How Hackable Is Your Smart Enterprise?*, USA, 2016, *https://www.forescout.com/wp-content/uploads/2016/10/iot-enterprise-risk-report.pdf*

27 Zurier, S.; "When It Comes to IoT, More Security Is Needed," *SC Magazine*, 12 December 2016, *https://www.scmagazine.com/when-it-comes-to-iot-more-security-is-needed/article/578654*

28 Schulz, Y.; "Critical Success Factors for IoT Projects," ITWorldCanada Blog, 25 June 2015, *www.itworldcanada.com/blog/critical-success-factors-for-iot-projects/375399*

29 O'Donnell, L.; "8 Strategic Steps for Long-Term IoT Security," ITbestofbreed.com, 20 March 2015, *www.itbestofbreed.com/slide-shows/8-strategic-steps-long-term-iot-security/page/0/2*