Chapter 1
IoT: Is It a Digital Highway to Security Attacks?

Edna Conway

1.1 Introduction to a Methodology to Secure the IoT Ecosystem

It used to be that we would imagine a world where things talk to, listen to, and observe all of us, so we could better understand ourselves and others, where biometric data about us might be compiled in real time as we eat, sleep, and go about our lives in order to provide us with better health outcomes—a world where devices could talk to other devices at speeds beyond human comprehension to improve the performance of auto and air travel, factory floor production, or even just the email on our phones. With today's Internet of Things (IoT) we are already roaring down that very digital highway! Our challenge is how to reap the benefits of that connected world while also ensuring security with every IoT connection we make.

For purposes of this discussion, let us agree that IoT, at its core, is what the Institute of Electrical and Electronics Engineers (IEEE) concluded in 2015 for low complexity systems. IoT is "a network that connects uniquely identifiable 'Things' to the Internet. The 'Things' have sensing/actuation and potential programmability capabilities. Through the exploitation of unique identification and sensing, information about the 'Thing' can be collected and the state of the 'Thing' can be changed from anywhere, anytime, by anything [1]."

200 billion [2]. 200 billion is the number of devices that are predicted to be digitally connected by 2020, that is, more than 22 devices for every one of us who will be on planet earth by then. Who and what are making, operating, and accessing these connected devices?

E. Conway (✉)
Merrimack, NH, USA
e-mail: ednaconway@gmail.com

F. D. Hudson (ed.), *Women Securing the Future with TIPPSS for IoT*, Women in Engineering and Science, https://doi.org/10.1007/978-3-030-15705-0_1

Table 1.1 IoT application areas

IoT application area	Description
Connected vehicles	IoT enabling vehicles and transportation infrastructure (e.g., roadway, traffic lights, cameras) to communicate.
Consumer IoT	IoT in the home and wearable and mobile connected devices.
Health IoT	IoT which processes data derived from sources such as electronic health records and patient generated health data.
Smart buildings	IoT such as energy usage monitoring systems, physical access control security systems, and lighting/temperature control systems.
Connected factories	IoT integrating real-time operations data, facilitating equipment function and monitoring, quality control, and failure analysis.

What will these 200 billion connected devices be doing? They will be sharing information and controlling operations across a spectrum we could not have imagined even 5 years ago. This convergence of Information Technology (IT) and Operational Technology (OT) has been sweeping global industries, including sectors such as energy, heavy equipment, and transportation. IoT has also expanded into all aspects of daily living and government, exacerbating the need for ever more vigilance and security across and through the IoT environment.

Before outlining a methodology to drive security across the IoT environment, it is helpful to categorize a few key IoT technology application areas. The United States National Institute of Standards & Technology (NIST) has identified five such areas in its Draft Interagency Report 8200 [3], which seeks to identify and list the many international cybersecurity standards that are applicable to IoT. Application Area descriptions follow in Table 1.1.

While we look to the future promise of exponential IoT growth, we must be prepared for the corollary security challenge. Of the utmost concern is this hidden and often overlooked reality: *as we digitize we are expanding the ecosystem of third parties who will inevitably impact us*, who will be "touching our stuff" along the Internet highway. For better, or for worse, the more we connect—the more transparent and collaborative we are—the more we are allowing others to observe and possibly control us.

As participants in digital transformation, whether individually or at an enterprise level, we must be aware of who and what is digitally and physically touching our information and devices. I call this the "third-party ecosystem[1]."

An interpretation of *Ponemon Institute's March 2018 Second Annual Study on IoT* [4] revealed a glaring reality regarding the security risk from the exponential growth of devices provided by the third-party ecosystem. The risk of the unknown is prevalent. Respondents can only fully identify less than 10% of devices connected to their networks. What is unknown cannot be secured (Fig. 1.1).

[1] Throughout this chapter, all references to the third-party ecosystem or ecosystem, by definition, include a community of third parties who are part of the Internet of Things (IoT).

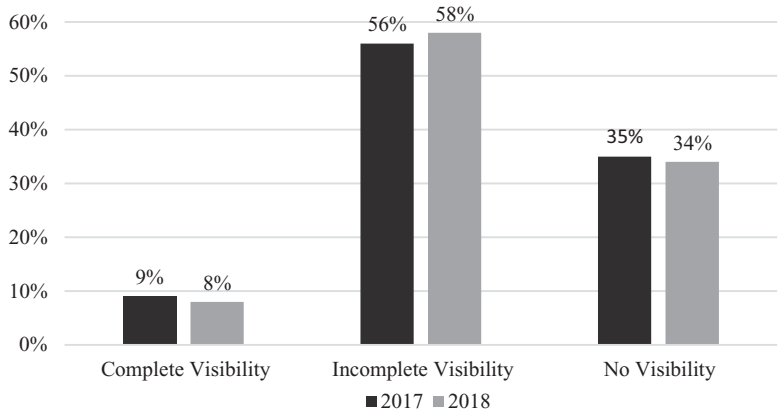

Fig. 1.1 Data answering the question "Are you aware of the network of physical objects that are connected?" Ponemon Institute's Second Annual Study on IoT, March 2018 [4]

Successful navigation of the digital super highway requires three key steps:

- Understand the security threats and their impact.
- Identify who is doing what within the connected ecosystem.
- Deploy a set of pervasive security techniques and processes across that ecosystem.

1.2 Threats and Related Exposures in the Connected Ecosystem

The connected ecosystem is increasingly the source of attacks. Disruption and disclosure of confidential information by third parties with whom we are connected, knowingly or unknowingly, continues to expand, as shown in Fig. 1.2.

Beyond reported attacks, research across global enterprises offers richer insight into the third-party impact. All third-party impact is significant. The data demands a call to action: 75% of the time incidents can be attributed to third parties (Fig. 1.3).

Third-party IoT devices are expanding overall third party risk. As the deployment of IoT devices expands, the related third-party security risk of data loss and cyberattacks from those devices will only rise. While some certainty of causation exists today, data shows a level of uncertainty that will increase the risk of unprotected IoT devices (Fig. 1.4).

Clearly the third-party ecosystem security risk is poised to grow. Sixty percent of respondents to the *Ponemon Institute's Second Annual Study on the IoT*, indicated their enterprises have a third-party risk management program. Forty-two percent of these respondents said the program is part of their companies' enterprise risk management program, but only 29% of respondents said their enterprises actively monitor the risk of IoT devices used by third parties [4].

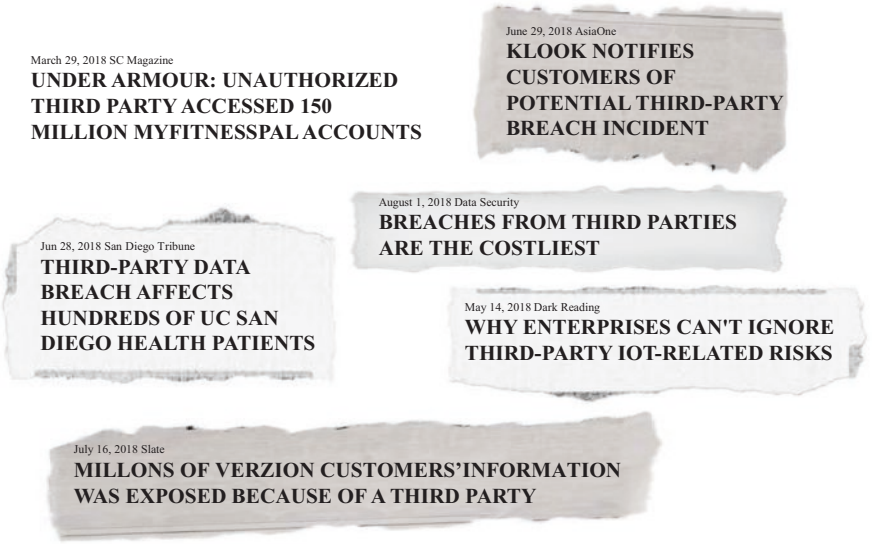

Fig. 1.2 News abounds with risks linked to third parties

Fig. 1.3 Third parties—a critical source of security risk

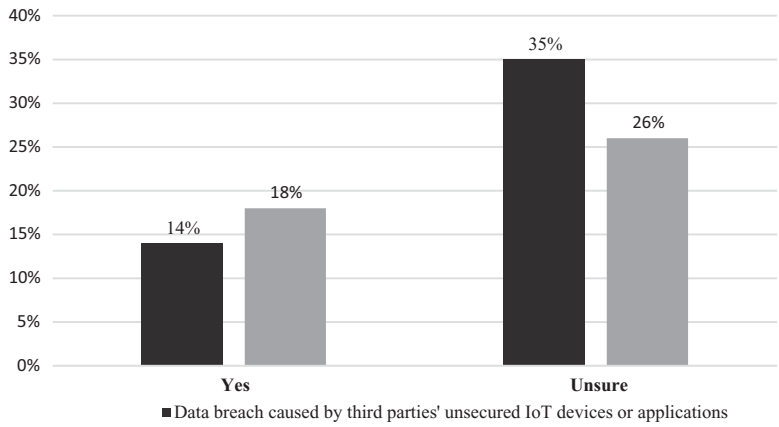

Fig. 1.4 Data answering the question "Has your company experienced a data breach or cyber attack caused by a third party's unsecured IoT devices?" Ponemon Institute LLC Second Annual Study on IoT, Publication Date: March 2018 [4]

To meaningfully address this inevitability, let us step back and examine the problem by defining it in terms of threats and threat impacts.

1.2.1 The Threats

Manipulation—The alteration of technology that allows unintended control or observation. Such an alteration of an IoT device and its resultant security vulnerabilities can have a host of ramifications. Ramifications that include a failure of the IoT device itself or control of the Information Technology (IT) systems to which it connects, including a denial of service. Ramifications can also manifest in the Operational Technology (OT) that has converged with these affected IT systems, including outright failures or reconfigured operational settings.

Espionage—The observation of confidential information at any point in the new ecosystem of digitally and operationally converged technology. Espionage is not just the prerogative of nation states anymore.

Disruption—Whether the most draconian level of a full denial of service or precise surgical alterations that allow data and operational processes to be changed.

1.2.2 The Threat Impacts

Tainted Solutions—Whether hardware, software or cloud-based services, the threats identified above lead to the risk of taint. Something that no longer functions as its designer or user intended. Taint can have far-reaching consequences.

Counterfeit Solutions—Functional integrity and quality are compromised when deceptively "real" looking and functioning technology is put into operation.

Intellectual Property Misuse—The lifeblood of innovation, intellectual property (IP), when disclosed in whole or in part, can be effectively leveraged by bad actors to manipulate, falsify, and create tainted and counterfeit solutions.

1.3 Understand Who and What Comprises the Third-Party Ecosystem

Having identified the threats and exposures, the next step to successfully navigating the connected ecosystem is to (1) identify the key players in your third-party ecosystem and (2) understand what those third parties deliver to you.

The Information and Communications Technology (ICT) third-party ecosystem is core to the digital convergence of IT and OT. Moreover, it serves as an illustrative example of both the sheer vastness and diversity of that ecosystem. Members of that ICT third-party ecosystem are depicted in Fig. 1.5 below.

Open Source Software	Software Licensors	HW Component Suppliers	Cloud Service Providers
Logistics Partners	OEMs/ODMs	IoT Devices	Manufacturing Partners
Channel/Distribution	Repair/Refurbishment Partners	Scrap Partners	Recycling Partners

Fig. 1.5 Members of the ICT third-party ecosystem

1.3.1 Drive Pervasive Security Across the Third-Party Ecosystem

The diversity of the third parties who participate in the life cycle of ICT solutions makes one thing clear. Pervasive security, namely the right security in the right way at the right time, can only be achieved if we coordinate meaningfully with those third parties.

To achieve the necessary level of coordination, we must develop a common taxonomy, as we did with the three threats and impacts mentioned earlier. Beyond that, a flexible architecture that can effectively be deployed across and through this diverse third-party ecosystem is essential.

1.3.2 A Flexible Security Architecture

A good approach is to establish key security architecture domains that can be deployed across the ICT third-party ecosystem. Most importantly, these domains should be agreed upon by all and be flexible enough to be adapted to fit the needs of all ICT third parties.

Brief descriptions and examples of Core Domains are listed in Table 1.2.

Leveraging an architecture touching upon these domains can allow third parties to effectively collaborate and drive comprehensive security. The domains can also serve as an approach to embedding security (including cybersecurity) into procurement [5].

It cannot be said too often: Security is a Team Sport. While the overarching architecture addresses all third parties, it must be flexible enough to allow variability. This variability allows for customized goals based on the nature of the products or services received from each specific third party (e.g., printed circuit board Gerber files or integrated circuit masks).

A key to success is to establish flexible security goals within each relevant domain, rather than setting forth specific requirements. In other words, keep security non-prescriptive to the optimum extent possible. Only by collaborating to understand the rich variety of third-party business models can we enable security

Table 1.2 Examples of core domains and descriptions

	Domain	Description
1	Security Governance	The security governance domain details requirements for an overall governance strategy to manage value chain security and compliance related risks by establishing requisite policies, standards, and procedures.
2	Security in Manufacturing and Operations	The security in manufacturing and operations domain details requirements for manufacturing and operating procedures in order to protect material assets, intellectual property, and information.
3	Asset Management	The asset management domain details requirements for securing IT and manufacturing assets throughout their life cycle.
4	Security Incident Management	The security incident management domain details requirements to establish a robust incident management process that should be followed for activities such as logging, recording, and resolving security incidents and anomalies.
5	Security Service Management	The service management domain details requirements: (a) for the delivery of services in accordance with agreed upon delivery timeframes, quality and security levels (b) for establishing a business continuity plan/program in the event of service disruption
6	Security in Logistics and Storage	The security in logistics and storage domain details security requirements that should be followed during storage and distribution of raw materials, inventory, and finished goods.
7	Physical and Environmental Security	The physical and environmental security domain details requirements that value chain members must design and implement to control access to facilities, equipment and resources, and to protect personnel and property from damage, harm, or unauthorized alteration.
8	Personnel Security	The personnel security domain details requirements to ensure that all value chain personnel who have access to any proprietary items, intellectual property and confidential information have the required authorizations, training, and contractual agreements including appropriate clearances, if required.
9	Information Protection	The information protection domain details requirements for protection of proprietary data through its life cycle, such as data classification, handling, cryptographic controls, and disposal. It also lists the requirements to be implemented on information systems that store or process intellectual property.
10	Security Engineering and Architecture	The security engineering and architecture domain details requirements to be followed during design, development, testing, and rollout of products (tangible and intangible) and services.
11	3rd Tier Partner Security	The third-tier partner security domain details requirements focused on information security controls that must be implemented at downstream value chain members (fourth parties, e.g., cloud service providers) in relation to procurement of goods and services.

that is embedded in the tools, processes, and people of the ecosystem. Flexible goals enable greater third-party adoption and swifter deployment.

For example, a prescriptive requirement addressing passwords might look like this:

Supplier must implement access controls on Information Systems via strong passwords and unique individual identifiers that are not shared among multiple users. Passwords must contain:

- At least eight alphanumeric characters;
- Both upper and lower case letters;
- At least one number (e.g., 0–9); and
- At least one special character (e.g., !$%^&*()_+|~-=\`{}[]:";'<>?,/).

Further, the following practices must also be adhered to, at a minimum:

- Passwords must be changed at least every 180 days.
- After five failed login attempts a system alert must be created.
- Information Systems must prevent the reuse of the last ten passwords.
- Passwords must not be shared.

Alternatively, a flexible goal-based approach might state that access control must be implemented via a combination of multifactor authentication techniques. Such authentication can be any of the following:

- Biometric, mobility, or human behavioral based (e.g., fingerprint or swiping motion) and
- Incorporate traditional strong alphanumeric-character passwords of unlimited length or passphrases without duplicated words (aka "memorized secret message" according to NIST [6]) or randomly generated passwords.

Let's explore exactly how such an architecture might work with regard to IoT. To do that we can use cryptography as a discussion point around Domain 9, Information Protection, as defined in Table 1.2. Examples of Core Domains and Descriptions.

1.3.2.1 A Cryptography Example of Domain 9 (Information Protection)

In the truly digitized environment that we are racing toward, encryption is a building block of security. We are aware of the risks of intentionally altered or improperly implemented encryption. Public–private effects have focused on validating the accuracy of the algorithm implementing the encryption.

NIST spearheaded a program designed to address validation of cryptographic modules (Fig. 1.6).

Applying the concept of driving the right security at the right time requires an understanding of what the "right way" might look like. Leveraging and validating encryption in the IoT environment requires us to think through the unique function and operational parameters of the device itself, where it is located and what its purpose is. Of unique value is applying open protocols for Automated Validation of Encryption (Fig. 1.7).

Implementing encryption in an IoT environment in the same manner encryption is implemented in large capacity compute environments is a ticket to failure.

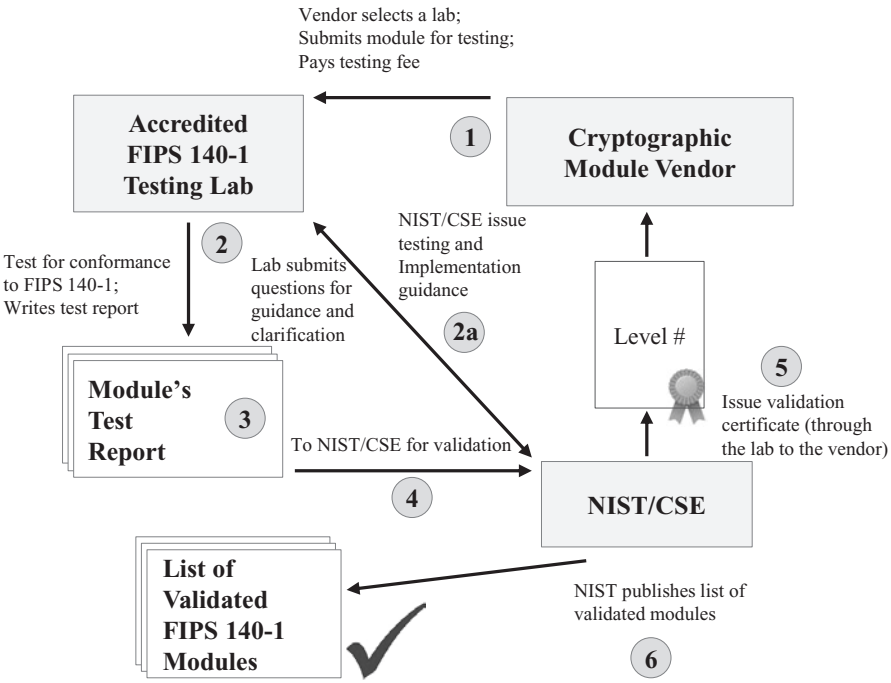

Fig. 1.6 Cryptographic Module Validation Process (Courtesy of NIST [7])

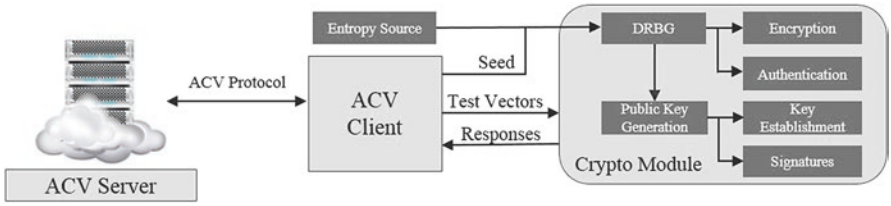

Fig. 1.7 Implementing encryption in an IoT environment. *ACV* = Automated Cryptographic Validation, Courtesy of Cisco Systems, Inc. [9]

Understanding the third-party device and its limitations and constraints is essential. Applying an Automated Cryptographic Validation Protocol can enhance efficiency and secure operation. However, we must evaluate the unique environment.

Recognizing the benefits of encryption in constrained environments such as automotive systems, sensor networks, healthcare, distributed control systems, the Internet of Things (IoT), cyber-physical systems, and the smart grid, NIST put forth an informational report on Lightweight Cryptography [8].

"Constrained environments cannot always use all the commonly accepted crypto algorithms available because of their constrained nature. A battery operated sensor, for example, cannot use 3072-bit RSA because it would deplete its battery faster and because of the processing load [9]."

Introducing Advanced Cryptographic Validation in Lightweight Encryption for constrained environments, such as IoT, is a glaring example of a flexible security architectural approach. An example of such an Advanced Cryptographic Validation Protocol that operates for lightweight crypto can be found at https://github.com/sigmaJ/ncsu-wolfssl. Applying security practices, modified for the IoT environment, delivers higher integrity overall while retaining the operational efficiency of IoT devices.

This kind of architectural approach can serve to further enhance the security posture of IoT.

1.4 Deploy the Security Architecture Using a Layered Approach

Thus far on the journey the following steps have been addressed:

- Establishing a taxonomy of threats and related exposures in the connected ecosystem.
- Understanding who and what comprises the third-party ecosystem—using the ICT ecosystem as an example.
- Developing a process to drive pervasive security across the third-party ecosystem:
  - Establishing a flexible security architecture.

A flexible architecture alone is not enough. Deployment of the architecture using a layered approach is highly recommend. Layering techniques in each of the following areas should be considered:

Physical Security: Deployed from components-to-finished product. Examples include: traceability, real-time transport tracking, security checkpoints, biometric access gates, segregation of high-value materials, tamper resistant labeling and packaging, and role-based access control to all physical locations.

Logical (Operational) Security: Implement rules-based access and leave no device unprotected, from security cameras to personal phones. Examples include: requiring all product development to follow strict Secure Development Lifecycle (SDL) protocol, encrypt data transmissions, conduct material reconciliation, and carefully manage all data destruction and scrap handling processes.

Security Technology: Utilize applicable security technology through the stages of the IoT life cycle. Examples include: deploying next generation encryption, anti-

counterfeiting chips, insertion of immutable identity during test, secure device boot and deploying obfuscation techniques at the integrated circuit level.

Behavioral Security: Embrace pervasive security cultural behaviors. For example, raise and maintain awareness around phishing campaigns, encourage employee participation in "see something say something" programs, adhere to "carrot vs. stick" management.

Network Security: Approach IoT as a part of the IT network, even if simply an OT sensing device. Examples include: network segmentation for IoT information input, controlled IoT device linking, encrypting IoT device transmission, and vetting security of clouds storing or transmitting IoT device data.

1.5 A Coordinated Deployment Plan

To make driving pervasive security a reality, an enterprise-wide coordinated deployment plan is key. The third-party ecosystem is commercially managed from multiple functions within an enterprise. Imagine, for example, the risk to successful deployment of your architecture without the governance risk and controls/compliance organization or the development of quality teams. Engage EVERYONE across your enterprise, whether your enterprise is commercial, educational or governmental.

A coordinated plan can include the following:

- Building compliance to security architecture into performance management, that is, scorecards and metrics for third parties.
- Active sharing of security best practices and information in public–private partnerships.
- Serving as a liaison to governmental agencies writing or enforcing laws and regulations as they address the challenge of pervasive security across a vast third-party ecosystem.
- Incorporating security parameters into the development life cycle, operational tools, and manufacturing processes.
- Developing processes to effectively evaluate the security maturity of third parties into the onboarding and procurement process for your enterprise.
- Publishing internally all enterprise functions success/failure in ensuring that the third parties they manage are adhering to the security architecture.

After all, security is a highly collaborative team effort and measuring the collective enterprise as a whole can afford more meaningful visibility and security integrity.

1.6 Conclusion: Safely Merging onto the IoT Super Highway

The IoT Super Highway is the path to our hyperconnected world. To ensure our security in this environment, we must keep in mind that at the foundation of IoT lies the network. After all, it is the "Internet" of things. Securing IoT devices and their foundation—the network itself—will ensure true digital transformation.

Application of IoT has the infinite potential to transform business, society and the global economy. We can achieve that potential only by also delivering security at every step along the digital journey.

Leveraging the pitstops and charging stations along the IoT super highway, as outlined in this chapter, will enable pervasive security. Perhaps most importantly, it must be remembered that the steps, summarized below, can only be successful if taken together across the third-party ecosystem:

1. Establish the common set of security threats.
2. Rally around clear goals that can only be achieved collectively.
3. Understand the unique business aspects of key third parties.
4. Openly, and without retribution, reveal challenges.
5. Share technical security strategies, practices and successes.

The extraordinary opportunity to reap life-altering benefits from the burgeoning growth of IoT is ours as we roar down today's digital highway.

References

1. Minerva R, Biru A, Rotondi D (2015) Towards a definition of the Internet of Things (IoT) Revision1. The Institute of Electrical and Electronics Engineers (IEEE), Piscataway, NJ
2. Intel Corporation [Internet]. Santa Clara: The Corporation; c.2014 [cited 2018 Aug 3]. "Intel IoT Gateway." Available from: https://www.intel.com/content/dam/www/public/us/en/documents/product-briefs/gateway-solutions-iot-brief.pdf
3. National Institute of Standards and Technology (NIST) (2018) Interagency report on status of international cybersecurity standardization for the Internet of Things (IoT). National Institute of Standards and Technology (NIST), Gaithersburg, MD
4. Ponemon Institute and The Santa Fe Group (2018) Second annual study on The Internet of Things (IoT): a new era of third-party risk. Ponemon Institute and The Santa Fe Group, Traverse City, MI. Sponsored by the Shared Assessments Program
5. See NIST 2015 Case Study for more information on the Cisco Value Chain Security Architecture: National Institute of Standards and Technology (NIST) (2015) Best Practices in Cyber Supply Chain Management. Cisco: Managing Supply Chain Risks End to End. National Institute of Standards and Technology (NIST), Gaithersburg, MD
6. National Institute of Standards and Technology (NIST) (2017) Special Publication 800-63, Revision 3: Digital Identity Guidelines. National Institute of Standards and Technology (NIST), Gaithersburg, MD
7. National Institute of Standards and Technology (NIST) (2014) NIST ITL Bulletin for November 2014: Cryptographic Module Validation Program (CMVP). National Institute of Standards and Technology (NIST), Gaithersburg, MD

8. National Institute of Standards and Technology (NIST) (2018) Internal Report 8114: Report on Lightweight Cryptography. National Institute of Standards and Technology (NIST), Gaithersburg, MD
9. Kampanakis P (2017) Collaborating with NCSU to promote lightweight crypto validation and assessment. [cited 2018 Aug 3]. In: Cisco Blogs [Internet]. Cisco Systems, Inc., San Jose, CA. Available from: https://blogs.cisco.com/security/collaborating-with-ncsu-to-promote-lightweight-crypto-validation-and-assessment