Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 126 (2018) 441–450

Procedia Computer Science

www.elsevier.com/locate/procedia

22nd International Conference on Knowledge-Based and Intelligent Information & Engineering Systems

Towards Mapping the Security Challenges of the Internet of Things (IoT) Supply Chain

Tope Omitola[a,*], Gary Wills[b]

[a] *ECS, University of Southampton, Southampton, UK*
[b] *ECS, University of Southampton, Southampton, UK*

Abstract

The flow complexity in today's IoT supply chain is enormous. To produce an item in a global network of suppliers requires a delicate dance of people, assets, systems, information, companies, and even governments. The opportunities for security vulnerabilities abound. In this paper, we describe the security challenges facing an IoT supply chain. We first start by describing what an IoT endpoint is, their various types together with their concomitant security challenges. An IoT endpoint is an output of an IoT supply chain, and the enumeration of its security challenges is then used to describe what IoT attack surfaces are, together with the threats and vulnerabilities facing a typical IoT supply chain. We use the iPhone/Apple supply chain as an exemplar, creating a map, and using that map to depict likely vulnerabilities and attacks. We conclude by discussing the mitigations against potential vulnerabilities in such a supply chain.

Keywords: Cyberphysical systems;Internet of Things; IoT; IoT Supply Chain; IoT Security; Supply Chain security

1. The Security Challenges of the IoT

The Internet of Things (IoT) has been defined as "an infrastructure of interconnected objects, people, systems, and information resources together with the intelligent services to allow them to process information of the physical and the virtual world and react" [1]. It is interesting that no mention of the Internet has been made in this definition, but the idea of interconnection of objects does include some kind of inter-networking infrastructure. This inter-networking may be private, public or a mixture of the two, and from a security perspective, many of the issues are common, irrespective of the nature of the inter-networking. Many expect a growing number of devices and objects to be connected in ways that they have not been. For example, by 2020, the number of connected devices is expected to outnumber

[*] Corresponding author.
E-mail address: t.omitola@ecs.soton.ac.uk

10.1016/j.procs.2018.07.278

the number of connected people by a ratio of 6:1, and 26 billion devices are projected to be connected [2]. Figure 1 shows some IoT application domains. There are different kinds of endpoints in an inter-networking infrastructure.

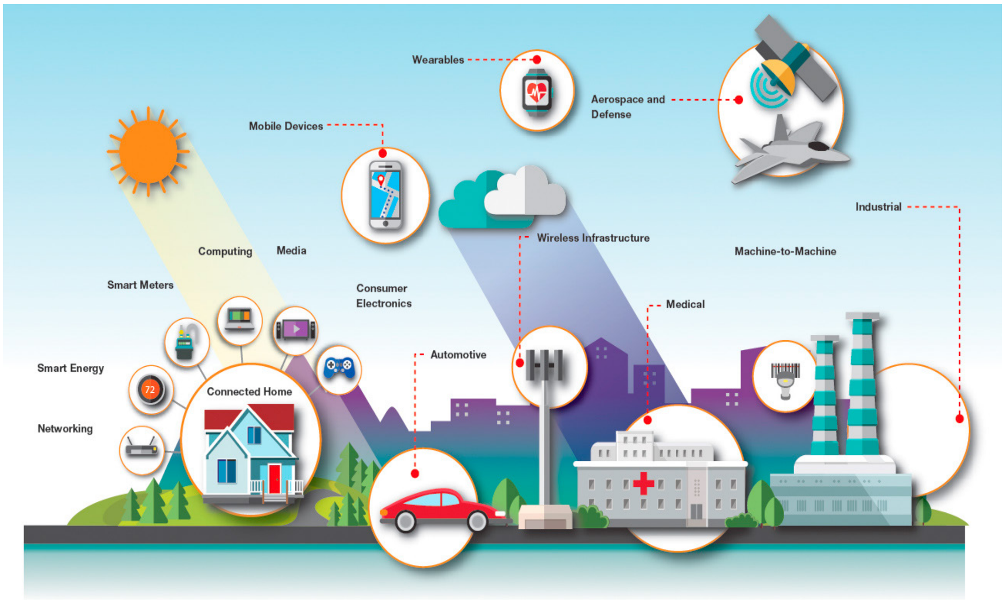

Fig. 1. Internet of Things application domains. From [3]

An **endpoint**, from an IoT perspective, is a physical computing device that performs a function or task as a part of an Internet connected product or service. Endpoints cover the entire spectrum of IoT devices including simple sensors, programmable logic controllers (PLC) and massive cloud servers with significant computing capabilities. An endpoint may be part of a control network, a concentrator between multiple communications streams, or routing traffic between other endpoints inside of the cloud infrastructure, a wearable fitness device, an industrial control system, an automotive telematics unit or even a drone unit. The endpoints may be on dedicated hardware or shared or virtualised hardware. The characterisation of these IoT endpoints will be very useful when it comes to investigating their security challenges.

1.1. Characterisation of IoT Endpoint Types

Most IoT endpoints can be characterised into three [16], although some of these may straddle two or even all three endpoint types:

- **The Simple Endpoint**. This is typically a sensor or simple physical device, such as light switch or a door lock with very functions. Its goal is to serve a singular physical purpose (or a defined set of purposes), and to provide feedback to the IoT service ecosystem or to the user. Simple IoT Endpoints are typically connected to the service ecosystem via Service Gateways. Other examples include wearables, smart watches, smart doors, etc. Due to their low cost and constrained environments, the security technologies available to Simple Endpoints are quite minimal. However, they can draw on trust anchors to implement robust security framework.
  Wearables and smartwatches are examples of IoT endpoints that straddle more than one endpoint type. Some wearables and smartwatches have simple functionality and form function and, therefore, can be characterised as a simple endpoint. But many brands of smartwatches and wearables are strictly not simple endpoints, in that they connect directly to the Internet without the use of a gateway, and permit many services to be done on and through them, e.g. a smartwatch has the affordances of the ability to permit payments from credit cards and bank accounts, etc.

- **Medium-sized Endpoint**. This IoT endpoint model typically has a persistent connection to a back-end server over a long-distance communications link. They are capable of running a more robust processor and either directly connected to an alternating current (AC) power source or contain a battery and have regular access to a battery recharging system. Some examples of medium-sized endpoints are SCADA systems and IoT-enabled refrigerators or washing machines. Many of these devices have different types of affordances, for example, the failure of a refrigerator to display information may be of much less significant issue than the failure of a SCADA system doing its work
- **The Gateway Endpoint**. The gateway is a device, typically connected to a dedicated power source, that manages the communication between Simple Endpoints and the back-end systems that drive them. The gateway accepts commands from the back-end systems of the service ecosystem, translating them to messages that the Simple Endpoints understand. The gateway is sometimes also responsible for device discovery, service ecosystem management functionality, system runtime monitoring, authentication, security, etc. Because of their complexity, gateways are usually not managed by the end-user but by the IoT Service Provider or Network Operator.

  This is also applicable in the home context, where an internet connected smart TV can act as a Gateway Endpoint, connecting simple devices such as light bulbs, etc., to the control infrastructure.

In order to better understand the challenges of securing an IoT ecosystem, and supply chain, it is useful to characterise the types of IoT Lifecycles.

1.2. IoT Lifecycles

There are different kinds of entities' lifecycles engaged in the IoT. These are:

- The IoT device/product/service lifecycle. The lifecycle of the IoT device or service.
- The Stakeholders' lifecycle. This involves enumerating the stakeholders engaged in an IoT device or product or service within a relevant IoT ecosystem, including the parties accountable for the part(s) of the ecosystem.
- Contextual life cycle. In what context is a device/product used, as what persona is a stakeholder involved? In what context is the data used in an IoT ecosystem, what if the context changes, who is accountable in what context? All these questions help to delineate the contextual lifecycle of the IoT device or service.
- Data lifecycle. What data is collected or created? Who controls the data, for what purposes?
- Trust relationship lifecycle. What are the trust dynamics between the user of an IoT endpoint and that endpoint? This trust dynamic could be ephemeral, long-lived, semi-permanent, permanent, or persistent.

Each lifecycle contains possibly many different lifecycle stages.

1.2.1. Lifecycle Stages

These lifecycle stages can be described thus:

- Concept. This is the idea stage, when the entity, e.g. service, device, or product, is first conceived
- Development. This is when development of the idea gathers steam
- Production. This is the stage at which the entity starts being produced
- Deployment. This is the stage when the entity starts being deployed in the intended market or domain
- Utilisation. This is the stage when the entity starts being used by consumers. At this stage, utilisation can be monitored, by interested and relevant stakeholders, to provide help for the next stage, Support
- Support. Users, in the marketplace (or internal to the organisation developing the system), may need help and support with utilisation
- Retirement, Sunsetting or Decommissioning. This is when the decision is taken to retire or decommission this entity (which may be a service, device or product). With some devices or products, decommissioning is not the end of the product or device. Sometimes, a decommissioned product may be requisitioned somewhere else, which starts the next stage, Re-commissioning

- Re-commissioning. This is the stage when an already retired product or service may be put into service, probably to serve a similar or totally different need from the original need the service was conceived for.

Since an IoT endpoint is one of the outputs of the supply chain, understanding the security challenges of an IoT endpoint will help to map the security challenges of the supply chain that produces it.

1.3. The IoT Endpoint Security Challenge

The security challenge of an IoT endpoint is related to the specific characteristics of that endpoint. Many IoT endpoints have the following characteristics which have particular security challenges associated with them:

- Low Energy Consumption. Low energy consumption endpoint may be required to achieve long battery life (some lasting several years) for a remote inaccessible endpoint without a permanent power supply. Therefore, if the mechanism employed for security is via cryptography, such low energy consumption endpoints may only be able to participate in computationally simple cryptographic operations, such as defined within ISO/IEC 29192. The low energy consumption may also significantly limit the available communication bandwidth, which may have an effect on the security challenge.
- Low Cost. The business case for many IoT services and systems demands the cost of an IoT endpoint be kept low. This often results in the device containing low processing capability, small amounts of memory and constrained operating system.
- Long Lived. Many IoT endpoints, especially those used for city, home and industrial applications (e.g. a smart electric meter) must be long lived (sometimes over several years). This presents a challenge because the security mechanism choices made when the device is designed, manufactured and deployed will have to be robust for the lifetime of the device. Management of long-lived devices is also a challenge particularly if a security vulnerability is found that cannot be patched within that IoT endpoint.
- Physically Accessible. Many IoT endpoints are physically accessible to the Attacker, as many of the endpoints are out in the open. They are running in cities, hospitals, etc. All hardware components and interfaces on these endpoints are therefore potentially subject to attack.

As technology improves, the cost of endpoints tends lower. For a cheap easily accessible device connected to thousands of other devices, it is economically feasible to destroy several devices in the course of reverse engineering their security. Therefore, having good security engineering in place is important.

Good security engineering requires four things to come together [4]: (1) Policy, i.e. what the system is supposed to achieve, (2) Mechanism, i.e. how is the security policy implemented, e.g. ciphers, access controls, certification revocation lists, hardware tamper-resistance, etc. are examples of implementing a security policy; (3) Assurance: the amount of reliance the principals can place on each particular mechanism; and (4) Incentive: the motive that the people guarding and maintaining the system have to do their job properly, and also the motive that the attackers have to try to defeat the security policy. Incentives do matter and should not be overlooked. Many security system failures were not due to technical errors but to wrong incentives that were put in place. If people do not want to, or are not incentivise to, protect a system, it is hard to make them secure. Some of these incentives fall outside the formal assurance process but are critical to the environment within which a security policy has to be defined. All these four things interact.

Since all these four things interact, engineers need to understand the proportions of these interactions in a typical IoT ecosystem in order to properly secure the ecosystem and the IoT supply chain.

2. IoT and its Supply Chain

The supply chain is the sequence of processes involved in the production of components, software and parts that together make up a system, and their integration, spanning many organisations, including suppliers, vendors and multiple tiers of outsourcing. It is a complex, geographically diverse, globally distributed system of interconnected networks, covering a broad surface area.

2.1. IoT and the Expanding Attack Surface

We define an **attack surface** to be the total of all exposures of a system to sources (trusted and untrusted). It can also be defined to include, not only all the systems and networks in an organisation but also, exposure to third parties. This includes everyone in that organisation's enterprise 'ecosystem' including major customers, vendors, and perhaps government agencies. As more organisations are finding efficiencies from being more connected, and are connecting more of their systems, people and processes, this leads to an attack surface getting very large. This raises the risk of organisations being breached through one of their vendors. Organisations have many vendors, several of which in turn have multiple large corporate and government clients, therefore mapping this cyber-ecosystem of connections of surfaces will be very difficult, as it may involve these other organisations to divulge sensitive information regarding their relationships with other companies (which they may be reluctant to do due to contractual or legal reasons). Supply chain vulnerabilities can be inserted or discovered throughout the lifecycle of a system, and at any point of the attack surface.

2.2. Threats, Vulnerabilities, and Vulnerability Classes

Threats refer to specific opportunities by identified adversaries to defeat security goals, while a **vulnerability** is a weakness in an information system, such as an IoT (eco) system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. A **vulnerability class** is a grouping of common vulnerabilities.

The four classes of potential vulnerabilities that can make such an IoT ecosystem vulnerable are [5] are:

- People, Policy and Procedure Vulnerabilities. Policies and procedures are the documented mechanisms by which an organisation operates, and people are trained to follow them. Policies and procedures lay the groundwork for how the organisation will operate; adequate training ensures that people understand their role/responsibility in implementing the policy and procedures. Policy, procedures and adequately trained people are not effective without each other, and not advisable to be implemented as discrete elements. A failure in, lack of, or deficiency in policies and procedures can lead to security risks for any information ecosystem. Inadequately trained and/or not well-incentivised staff is also another vulnerability, and therefore constitute a threat.
- Platform Software/Firmware Vulnerabilities. Software and firmware are the programmable components of a computing environment. Errors or oversights in software and firmware commissioning, design, development, deployment, decommissioning may result in unintended functionality that allows adversaries or other conditions to affect, via programmatic means, the security of the technology platform.
- Network Vulnerabilities. Networks are the connections between multiple locations or organisational units and are composed of many differing devices using similar protocols and procedures to facilitate a secure exchange of information. Vulnerabilities and risks occur between and within IoT networks when policy management and procedures do not conform to required standards and compliance policies as they relate to the data exchanged.
- Gateway Vulnerabilities. Any gateway that the subsystems in the IoT ecosystem and its supply chain is also vulnerable.

These vulnerabilities open opportunities for different types of malicious attacks.

2.3. Types of Malicious Attacks

Supply chain attacks can arise from three principal causes:

- Malicious insertion of defect or malware,
- Exploitation of latent vulnerabilities, and
- Non-cyber attacks, such as surreptitiously reducing the accuracy of physical sensors and actuators.

Insertion of a malicious vulnerability via the supply chain can occur at any time during the lifecycle of a system, device or service. Parts, including physical and cyber components, may be deliberately subverted at design time, during fabrication, during transport, or while actually operating in a system via malicious insertion. This is a multi-step process: the attacker must first gather detailed information on the target system and its suppliers to identify opportunities for access and means to achieve effects through the insertion. With this knowledge, the attacker creates malicious hardware or software (or both) and performs insertion. Finally, the malicious insertion operates to achieve the attacker's desired effect. When done effectively, malicious insertion will not be detectable until actuated and it may be present as a design flaw when ultimately observed. For example, the existence of counterfeit electronics in the supply chain demonstrates the potential for such attacks. Instances of exploitation via malicious insertion have been confirmed in the commercial sector. Examples include Volkswagen's insertion of a "defeat device" to thwart emissions testing [6] and insertion of embedded code into Juniper routers [7].

Looking at a concrete example of an IoT device will help us observe likely vulnerabilities and potential threats on a typical IoT supply chain. One of the most popular IoT devices is today's smartphone, and the second biggest selling smartphone is the iPhone [8].

2.4. The iPhone Supply Chain - An IoT Supply Chain Exemplar

Looking at the supply chain of the making of the iPhone will show us some of the threats faced when securing the supply chain of an IoT device. Table 1 shows a list of some of the components and their manufacturer or supplier. Many of these manufacturers are household names in themselves, and many of them subcontract components' fabrication to other manufacturers, potentially expanding the attack surface. Table 2 shows the list of locations and the number of Apple suppliers per country.

Table 1. Some major components of the iPhone and their Manufacturer. From [9]

Component	Manufacturer's Name
System-on-Chip	TSMC
Baseband	Intel
RF Front End (Antenna Switch Module)	TDK Corp.
Envelope Tracking	Qorvo Inc.
FEM	Broadcom Ltd.
PAM	Skyworks
Battery	Huizhou Desay
BT / WLAN	Universal Scientific
GNSS	Broadcom Ltd.
NAND Memory	SK Hynix
SDRAM	Samsung Semiconductor
PMIC Main (Power Management)	Dialog Semiconductor
PMIC RF	Intel
NFC	NXP

Apple orders many of these components from its global suppliers, selling these en-masse, to some of its major contract manufacturers around the world. One of these is Foxconn [11]. In a typical manufacturing site, such as the one in Zhengzhou, it takes about four hundred steps to assemble an iPhone [12]. After assembly, packs of iPhone are placed in wooden pallets, wheeled out to trucks and distributed locally in China or taken to customs from where they find their ways to Apple affiliates around the world, and from where they get on to the hands of private individuals.

From Table 1 and especially from Table 2, one can see that the potential attack surface area for a malicious insertion is very large, and shows the amount of work to do in order to mitigate potential attacks. From the iPhone supply chain, one can discern a map of the IoT supply chain.

2.5. A Map of the IoT Supply Chain

Figure 2 depicts the web of actors and their interdependencies supporting a typical IoT supply chain. Understanding these web of actors will help characterise the susceptibility of the supply chain to attacks.

Table 2. Number of Suppliers to the Apple Supply Chain Per Country. From [10]

Num. of Apple Suppliers in the Country	Country
349	China
139	Japan
60	USA
42	Taiwan
32	South Korea
21	Malaysia
24	Philippines
21	Thailand
17	Singapore
13	Germany
11	Vietnam
7	Mexico
6	Indonesia
6	Israel
5	France
5	Czech Republic
3	Belgium
3	Italy
3	Ireland
3	UK
2	Brazil
2	Costa Rica
2	Austria
2	Netherlands
1	Canada
1	Portugal
1	Spain
1	Morocco
1	Puerto Rico
1	Malta
1	Hungary

The main actors are the Design and Development groups, the major Components' suppliers, Contract Manufacturers, and the major Distribution and Sales networks. These first level of actors would normally have been carefully chosen by the IoT device producer (e.g. in this case, Apple). As a result of this careful choice, there will be a high level of monitoring for likely attacks and vulnerabilities, due to the adverse publicity and potential loss of business if attacks were to happen at this level. These major component suppliers may subcontract some of these items to the global commercial supply chain. It is at this secondary level that parts' provenance is harder to trace, and since some of these business relationships are fluid, the potential of malicious insertions and attacks is highly likely and are difficult to track.

There is a strategy normally followed by a supply chain attacker.

2.6. Supply Chain Attacker Strategy

No matter where an attack occurs in the lifecycle, and the lifecycle stage, of the system, an attacker seeking to exploit a maliciously inserted vulnerability will need to execute each step in the 'attacker's chain', and these are [13]

- Intelligence and Planning. Gathering information of the target system and suppliers to develop supply chain vector
- Design and Create: Develop the malicious vulnerability to insert into the target supply chain. This may be done in an attacker-owned facility or by an insider in a legitimate facility
- Insert: incorporate malicious vulnerability into the target system through its supply chain

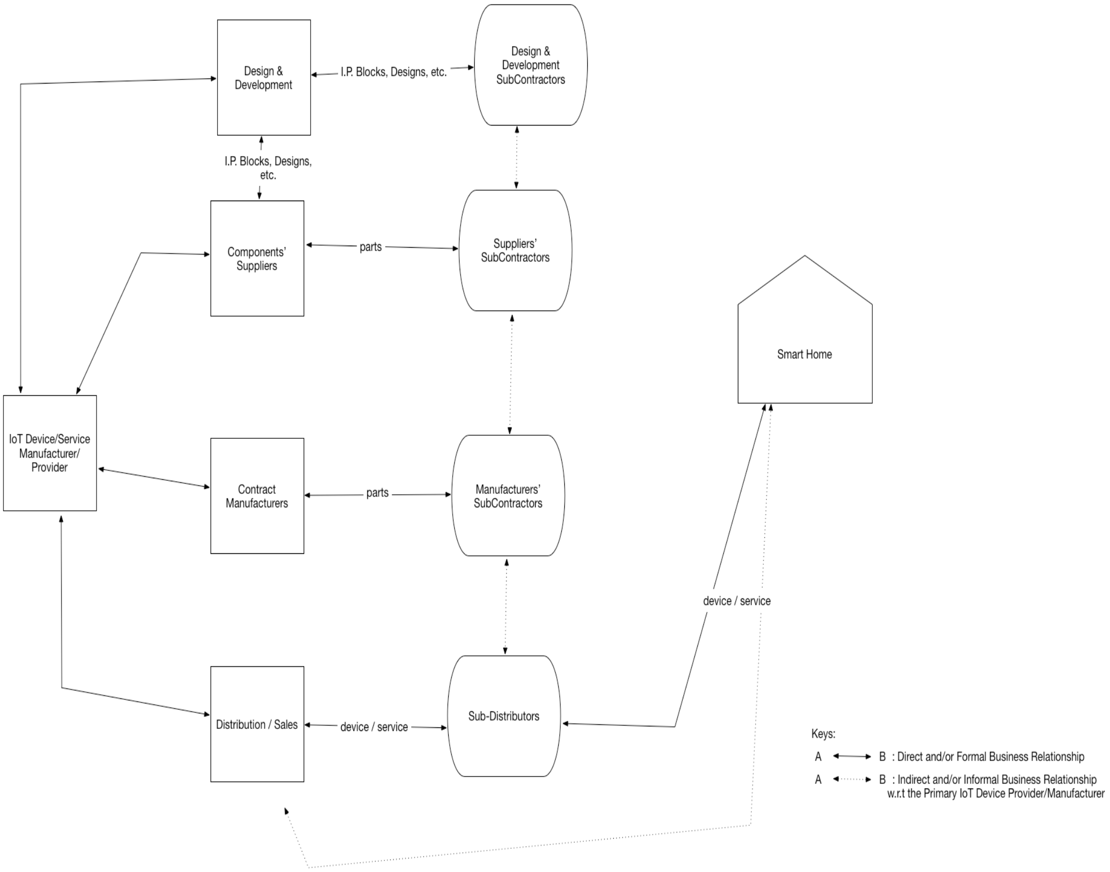
Design & Development
I.P. Blocks, Designs, etc.
Design & Development SubContractors
I.P. Blocks, Designs, etc.
Components' Suppliers
parts
Suppliers' SubContractors
Smart Home
IoT Device/Service Manufacturer/ Provider
Contract Manufacturers
parts
Manufacturers' SubContractors
device / service
Distribution / Sales
device / service
Sub-Distributors
Keys:
A B : Direct and/or Formal Business Relationship
A B : Indirect and/or Informal Business Relationship w.r.t the Primary IoT Device Provider/Manufacturer

Fig. 2. Map of an IoT Supply Chain

- Achieve Effect: actuating and operating malicious vulnerability (hardware or software) to achieve desired effect.

Since this is the pattern normally followed by a supply chain attacker, it is very important to develop strategies to disrupt this pattern and to mitigate potential vulnerabilities in the chain, itself.

3. Mitigating Potential Vulnerabilities in the Supply Chain

The procedures to use to mitigate potential vulnerabilities in the supply chain include:

- Protecting critical information and systems. Supply chain vulnerability can be reduced by protecting design and supplier information, protecting design, manufacturing, and distribution systems, and employing better assurance of parts provenance
- Detecting and Responding to Attacks on Supply Chains. Design strategies that provide built-in active monitoring to improve the ability to detect exploitation and response. Modular system architectures that isolate functions and provide fail-over capabilities can improve the ability to respond and fight through an attack.
- Recovering from Attacks. System architectures that provide for rapid upgrades can improve the ability to recover from an attack by eliminating the affected components, networks, or software.

4. Conclusion and Future Work

With the expected growth in the number of IoT devices, the number of participants and actors in the supply chain will increase too. The IoT endpoint is one of the outputs of the supply chain, characterised by low energy consumption, low cost, sometimes of long duration, and differing levels of physical accessibility. As these four things interact, it is important to understand the proportions of these interactions in a typical IoT ecosystem in order to properly secure the ecosystem and the IoT supply chain.

The supply chain is the sequence of processes that together make up a system, and their integration, spanning many organisations. We define an attack surface to be the total of all exposures of a system to sources both trusted and untrusted. Therefore, a supply chain spanning many organisations makes the attack surface potentially large. Threats refer to specific opportunities by adversaries to circumvent security goals, while a vulnerability is a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

This paper examined concrete example of the supply chain of an IoT device (iPhone) in order to observe likely vulnerabilities and potential threats on a typical IoT supply chain. From this concrete supply chain example, we describe a map of an IoT supply chain. Attackers seeking to exploit a maliciously inserted vulnerability will need to execute each step in the ‘attacker’s chain’, which are described in the paper. The paper concludes with describing procedures actors in the supply chain can use to disrupt the steps in the attacker’s chain and to mitigate potential vulnerabilities.

The goal of security is not only to guard the physical network and prevent intrusions, which is threat focused, but also to ensure that critical functions and the services that the network and systems provide are maintained in the face of disruptions (both intentional and unintentional) [14]. This requires a more strategic and systematic approach. For future work, we will apply a systems-theoretical model, the System-Theoretic Process Analysis for Security (STPA-SEC) [15], to develop a systems-theoretic framework that participants of an IoT supply chain can use to mitigate vulnerabilities and prevent malicious attacks in the chain.

Acknowledgements

The first author will like to thank the UK’s IoT Security Foundation (IoTSF), and especially Dan Ng, for providing an intellectually stimulating and supportive environment while the work reported in this paper was being carried out.

References

[1] Information technology Internet of Things Reference Architecture (IoT RA). ISO/IEC CD 30141, at, https://www.w3.org/WoT/IG/wiki/images/9/9a/10N0536_CD_text_of_ISO_IEC_30141.pdf (23.03.2018)

[2] D. Evans. “The Internet of Things: How the Next Evolution of the Internet Is Changing Everything,” Cisco, April 2011. Quoted in Martin C. Libicki, Lillian Ablon, Tim Webb: “The Defender’s Dilemma. Charting a Course Toward Cybersecurity”. pub. RAND Corporation, 2015

[3] Internet of Things application domains, at http://www.skyworksinc.com/products_IoT.aspx

[4] R. J. Anderson. “Security Engineering: A Guide to Building Dependable Distributed Systems”. pub. Wiley, 2008

[5] Keith Stouffer, Victoria Pillitteri, Suzanne Lightman, Marshall Abrams, Adam Hahn: “Guide to Industrial Control Systems (ICS) Security”. pub. National Institute of Standards and Technology, 2015

[6] “Volkswagen to Pay $14.7 Billion to Settle Diesel Claims in U.S.”, at https://www.nytimes.com/2016/06/28/business/volkswagen-settlement-diesel-scandal.html (23.03.2018)

[7] “Secret code found in Juniper Networks”, at https://www.wired.com/2015/12/juniper-networks-hidden-backdoors-show-the-risk-of-government-backdoors/ (23.03.2018)

[8] “iPhone: 2^{nd} biggest selling phone in 2017”, at https://en.wikipedia.org/wiki/List_of_best-selling_mobile_phones#2017 (23.03.2018)

[9] “Apple’s Supply Chain Cost of Making the iPhone 7”, at https://www.supplychain247.com/article/apples_supply_chain_cost_of_making_the_iphone_7 (23.03.2018)

[10] “How & Where iPhone Is Made: Comparison Of Apple’s Manufacturing Process” http://comparecamp.com/how-where-iphone-is-made-comparison-of-apples-manufacturing-process/ (23.03.2018)

[11] “Foxconn, Apple and the partnership that changed the tech sector”, at https://asia.nikkei.com/magazine/20170713/On-the-Cover/Foxconn-Apple-and-the-partnership-that-changed-the-tech-sector (23.03.2018)

[12] “An iPhone’s Journey, From the Factory Floor to the Retail Store”, at https://www.nytimes.com/2016/12/29/technology/iphone-china-apple-stores.html (23.03.2018)

[13] Jon Boyens, Celia Paulsen, Rama Moorthy, Nadya Bartol. "Supply Chain Risk Management Practices for Federal Information Systems and Organizations". pub. National Institute of Standards and Technology, 2015

[14] William Young and Nancy G. Leveson: "An Integrated Approach to Safety and Security Based on Systems Theory", *COMMUNICATIONS OF THE ACM*, NO. 2, **VOL. 57**, FEBRUARY 2014

[15] William Young and Nancy Leveson: "Systems thinking for safety and security". *Proceedings of the 29th Annual Computer Security Applications Conference*, 2013

[16] Industrial Internet of Things Volume G4: Security Framework, pub. industrial internet CONSORTIUM, at www.iiconsortium.org