I. Stellios, P. Kotzanikolaou, M. Psarakis and C. Alcaraz, "Risk Assessment for IoT-Enabled Cyber-Physical Systems", *Advances in Core Computer Science-Based Technologies*, pp. 157-173, 2021.
http://doi.org/10.1007/978-3-030-41196-1_8
NICS Lab. Publications: https://www.nics.uma.es/publications

Risk assessment for IoT-enabled Cyber-Physical Systems

Ioannis Stellios, Panayiotis Kotzanikolaou,
Mihalis Psarakis, and Cristina Alcaraz

University of Piraeus, 85 Karaoli & Dimitriou, GR-18534, Piraeus, Greece
{jstellios, pkotzani, mpsarak}@unipi
Computer Science Department, University of Malaga,
Campus de Teatinos s/n, 29071, Malaga, Spain
alcaraz@uma.es

Abstract

Internet of Things (IoT) technologies have enabled Cyber-Physical Systems (CPS) to become fully interconnected. This connectivity however has radically changed their threat landscape. Existing risk assessment methodologies often fail to identify various attack paths that stem from the new connectivity/functionality features of IoT-enabled CPS. Even worse, due to their inherent characteristics, IoT systems are usually the weakest link in the security chain and thus many attacks utilize IoT technologies as their key enabler. In this paper we review risk assessment methodologies for IoT-enabled CPS. In addition, based on our previous work [47] on modeling IoT-enabled cyberattacks, we present a high-level risk assessment approach, specifically suited for IoT-enabled CPS. The mail goal is to enable an assessor to identify and assess *non-obvious* (indirect or subliminal) attack paths introduced by IoT technologies, that usually target mission critical components of an CPS.

Keywords: Internet of Things (IoT), Cyber Physical Systems (CPS), Risk Assessment, Attack paths, Critical Infrastructures.

1 Introduction

Cyber physical systems consist of large-scale interconnected cyber and physical components, interacting with each other through various connectivity technologies. There are a multitude of devices and applications being deployed to serve critical functions as well as everyday operations, like smart grids, Supervisory Control and Data Acquisition (SCADA) systems, smart healthcare devices, wearables, Intelligent Transportation Systems (ITS) and vehicles, smart cities and many more.

A typical example of CPS are Industrial Control Systems (ICS), which are formed in hierarchical model. Field devices, such as Programmable Logical Controllers (PLC) and Remote Terminal Units (RTU) to Intelligent Electronics Devices (IED) which, in turn, they are managed through Human-Machine-Interfaces (HMI) from Command and Control (C&C) centers.

Although traditional ICS used to be, more or less, "closed" and isolated systems, the evolution of the IoT has also affected modern CPS. IoT technologies and protocols, used both in industrial and non-industrial environments (*e.g.* 6LoWPAN [45], CoAP [6]), allow even large-scale and mission critical industrial equipment to connect directly to the Internet (*e.g.* industrial robots, wind turbines, solar panel systems etc.). These new IoT technologies enable ICSs to become more flexible and interpolatable. They allow for remote monitoring and control (*e.g.* interconnected PLCs, Industrial robots), thus reducing management, surveillance and maintenance costs as well as increase the expected lifetime of old, yet very expensive ICSs, like those supporting Critical Infrastructures and services.

Traditional CPS used proprietary technologies, were isolated from the Internet and were built to be reliable and robust. Besides physical security concerns, no security mechanisms for older SCADA devices where present, since, they were physically and logically isolated, *air-gaped* systems. Their main line of defense was that were installed in highly secure areas with a much smaller attack surface than traditional IT infrastructure, and with dedicated *off-the-grid* communication channels.

While IoT enabling technologies have created new opportunities for the global economy, this unprecedented explosion in inter-connectivity and inter-dependency between billions of unsecured, energy constrained devices have raised a number of security issues and challenges.

Since modern CPS highly depend on computer functionality, network inter-connectivity and machine-to-machine interaction in order to properly operate, an attack or disruption on a single component of a complex, large-scale CPS may concurrently affect the entire production line. The operating environment has evolved in a such a way that depends to a large extent on Internet connected/interconnected supply chains, networks and systems and thus reduces the ability to estimate inter/outer dependencies of such increased complexity.

To complicate things even more, latest policies in companies, like *Bring Your Own Devices* (BYOD), have enabled end-user devices such as smartphones, gadgets and laptops to connect and interact to corporate networks. On the other hand, concerns of privacy violations as well as a totally new set of attacks against mission critical IT systems and services, that can be launched from Internet using low-cost equipment and basic technical skills make the headlines more often. These kind of attacks not only are usually underestimated and in some cases hard to identify.

Assessing the risk of CPS systems and their related infrastructures has been the study of several research approaches [3, 7, 11, 29, 30, 35, 38] in the recent past. Moreover, several risk assessment methodologies [1, 4, 10, 12, 27, 33, 21] have been developed for the CPS systems focusing on IoT-enabled attack scenarios. In addition, security researchers [2, 16, 22, 51] proposed methodologies some of which incorporate Common Vulnerability Scoring System (CVSS) [13] in its latest version (3.0) for vulnerability assessment and complex access/attack path discovery.

Despite this extensive research detecting hidden/subliminal attack paths enabled by vulnerable IoT subsystems remains an hard task for an assessor, especially in facilities where IoT and mission critical systems coexist in close proximity. Our proposed a high-level risk assessment methodology focuses on identifying the risk that is introduced from subliminal access/attack paths by utilizing well established standards, such as ISO/IEC 7005:2011 [20], NIST SP800-30 [42] and SP800-39 [41] combined with newly introduced methodologies ([2, 16, 22, 51]). Its main contribution is that, by modeling characteristics of the device/technology as well as the applicable in each case access and attack paths (see Figure 1), it can be used as a guide to assess the risk that IoT devices may introduce in their related CPS. The discovered attack paths include both scenarios where the IoT enabling technology is the actual target and the ones where an adversary utilizes the IoT device in order to attack other mission-critical equipment.

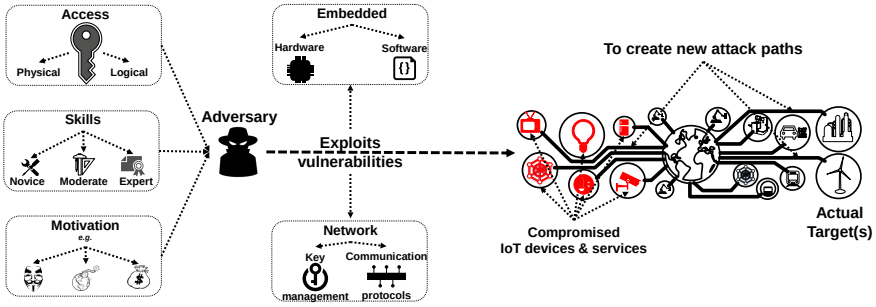

Figure 1: High level representation of IoT-enabled attacks against CPS.

IoT enabled attack scenarios. The FBI issued in 2012 an intelligence bulletin that reported an extensive fraud concerning thousands of smart meters in Puerto Rico [24]. The report states that even individuals with moderate technical skills, low cost tools and software that is available on the the Internet, may successfully alter the readings of the smart meters. According to the FBI the adversaries were company's employees that exploited the smart meters using an optical converter device which in turn enables the smart meter to communicate with a computer. Then using software that can be downloaded from the Internet, they managed to alter the settings for recording power consumption. The annual economical impact to the company is estimated to be over 400 million dollars. Clearly this case is a typical example of a direct attack path.

In 2017 security researchers [28, 37] were able to locate approximately 84.000 industrial robots, exposed to the Internet through FTP server (direct attack path) or through industrial routers (indirect path); 5.000 of these, did not even require any type of authentication. Among the vulnerabilities found were outdated software (application libraries, OS kernels), insecure web interfaces, publicly available firmware images, as well as wireless access to remote service facilities. In this attack scenario a "black hat" hacker may target a plethora of industrial robots so as to alter the robot state and force robots to produce defect products, install ransomware and/or injure the operators.

In December of 2015 and 2016 Ukrainian energy companies suffered from cyber attacks that targeted the smart grid. Utilizing spear-phishing techniques and sophisticated

exploitation methods adversaries managed to take over interconnected field devices, such as circuit brakers, and inflict a massive blackouts that lasted for several hours and affected over 200,000 people (2015) [17, 26].

In another proof-of-concept attack scenario researchers proved that is possible to exfiltrate sensitive information which is stored in a air-gaped data center inside a highly secure facility. As described in [39, 40], an adversary manages to bypass proximity checks of a smart lighting system and by utilizing wardriving/warflying techniques (a drone equipped with off-the-shelf communication equipment), and take over smart lighting systems from a large distance (aprox. 150 meters). Then, by extending the functionality of the light bulbs, she manages to control light flickering in a way that the human eye cannot perceive thus creating a covert channel to extract the information.

Paper Contribution. In this paper, we extend our previous work on modeling IoT-enabled attacks [47], and we present a targeted, high-level risk based approach that may be used to identify and assess IoT-enabled CPS. Such a methodology may assist a risk assessor to identify and assess *non-obvious* attack paths introduced by IoT technologies, such as indirect or subliminal attack paths against the critical components of a cyber-physical system.

Paper structure. In Section 2 we review the related work on risk assessment methodologies, from general purpose ones, to more targeted methodologies for IoT and CPS. In Section 3 we propose a high-level risk-based approach to model and assess IoT-enabled attacks. Finally, Section 4 concludes this paper.

2 Related work

Most existing security risk and threat assessment methodologies examine a series of factors such as: (i) the assets that need to be protected, (ii) the threats and vulnerabilities that correspond to these assets, (iii) their value to the organization under assessment, (iv) the consequences (or impact) in case of security violations against the identified assets and (v) security controls that can reduce/eliminate the potential damage. The main goal of a risk assessment methodology is to provide guidance to an organization in order to minimize the risk and maximize the level of confidentiality, integrity and availability. The procedure of implementing the necessary security measures must be done in respect of the organization's needs in order to achieve the desired levels of confidentiality, integrity and availability and, at the same time, guarantee a satisfactory level of functionality.

IoT-specific risk assessment methodologies have been developed in the last few years in order to describe the ever growing risk that stems from the IoT systems and services. Atamli and Martin [4] present use cases of IoT enabled attack scenarios (power management, smart car and healthcare) so as to identify potential threats sources, classes of attack vectors and impact assessment applicable in devices such as Radio Frequency Identifiers (RFIDs), actuators, sensors as well as networking technologies. They also propose specific countermeasures that can reduce the risks evolved mainly in security and privacy.

In [12] Dorsemaine *et al.* access the risks introduced to a legacy Information Sys-

tem (IS) due to the integration of an IoT infrastructure. A practical example is then presented with the integration of a smart lighting system in a company's IT systems. The authors divide the IS into local environment, transportation, storage, mining and provision sectors. Then, they define security properties for the IoT systems of each IS sector, by focusing mainly on aspects such as confidentiality, integrity, availability, usability and auditability while also introduce additional properties for IoT components including energy, communication, functional attributes, local user interface and hardware/software resources. Finally they present the potential threats and the impact in all of the aforementioned attributes for an IS and IoT infrastructure.

In [27] Liu *et al.* propose a dynamical risk assessment method for complicated and constant changing IoT environments adopting features from an *Artificial Immune System* such as the distributed and parallel treatment, diversity, self-organization, self-adaptation, robustness etc. Through packet inspection from agents that are deployed in IoT systems, the proposed method locates abnormal behavior and responds by adapting appropriately the risk value.

A management framework for IoT devices, called Model-based Security Toolkit (SecKit), used to evaluate security policies that protect user's privacy, is presented in [33]. Seckit has been integrated in a framework, proposed by the *iCore* project, which enables usage control and protection of user data. Then a case study is presented in a smart home scenario.

Abie and Balasingham [1] propose a risk-based adaptive security framework for IoT enabled e-Health CP systems that estimates risk damages and future benefits using game theory and machine learning techniques. This enables the security mechanisms to adjust their security decisions accordingly.

A recent approach [10] about Medical Internet of Things (MIoT) points out difficulties that traditional risk assessment methodologies face when used in non-stable environments, such as the MIoT, where devices maybe added, removed or changed in their configuration. For assessing and managing threats the researchers adopt HMG IS1 and ISO/IEC 27033 standards and an existing threat analysis from the Technology Integrated Health Management (TIHM) project. They taxonomize threats according to the severity level ranging from *very low* to *very high*, as well as the risk that emerges from IoT devices against other MIoT devices. In addition, for each MIoT device connected to the hub a multicheck process is proposed,

A survey [21] focusing mainly on cyber security management in industrial control systems depicts the current standards and future challenges that ICS face in the ever evolving threat landscape. Hot topics for future research, among others, considered to be the need for maintenance of security of ICS components throughout their lifetimes, interdependencies between large CPS, as well as real-time risk assessment.

In [22] Kott *et al.* describe Mission Impact Assessments (MIAs) in an effort to bridge the gap between operational decision makers and cyberdefenders . They managed to set a testbed (*Panoptesec*) that emulated cyber physical systems of an Italian water and energy distribution company as well as a prototype simulation platform named *Analyzing Mission Impacts of Cyber Actions (AMICA)* that simulate a military's air operations center they managed to discover high number of hidden network dependencies that weren't identified by human operators, unnecessary large volume communications between Human-Machine Interfaces (HMIs) and field devices and attacks against spe-

cific nodes of the network that, when used in a timely manner could lead to devastating results. The researchers proposed an abstractive threat modeling (*e.g.* [23]), for both adversaries and defenders, and emphasized on the challenges involved when modeling large scale, diverse and complex networks.

Agadakos *et al.* [2] proposed a methodology for modeling cyber-physical attack paths in IoT. In particular, they developed a framework that allowed the identification of IoT device types, interaction channels, as well as security and proximity features. Using the proposed framework they managed to simulate a home network that consisted of several home IoT devices. In particular, by using techniques such as passive sniffing for host discovery, they managed to discover attack scenarios that utilized hidden connectivity/interaction paths, security degradation (*e.g.* from authenticated to unauthenticated communication channels) and violations of transitions and states. According to the authors limitations of this work are considered to be the fact that the model may introduce false positives, since it does not filters unrealistic attacks and it is not easy to implement in large scale networks with mission critical systems.

Researchers in [5] propose a risk-based access control model for IoT technologies. Real-time data from IoT devices are utilized to dynamically estimate security risks through an risk estimation algorithm. The proposed model monitors and analyzes user behavior in order to detect abnormal action from authorized users

Recent methodologies that utilize the CVSS 3.0 have been also proposed by similar group of researchers [16, 51]. In [16], a framework for modeling and assessing the security of the IoT ecosystem based on previous work is proposed. The framework consists of five phases: (1) Data processing, (2) security model generation, (3) security visualization, (4) security analysis, and (5) model updates. In phase one system information and security metrics are introduced in order to construct the IoT network which is then used (phase two) to construct the extended Hierarchical Attack Representation Model (HARM) [19] and calculate all possible attack paths in the IoT network. In phase three attack graphs (in low, upper and middle layer) are utilized to visualize the IoT network whereas in four a security analysis, that takes into consideration *e.g.* nodes or vulnerabilities, is constructed and fed into an analytic modeling and evaluation tool (*Symbolic Hierarchical Automated Reliability and Performance Evaluator - SHARPE* [43]) for further security analysis. Finally in phase five proper defense strategies are decided. The researchers present scenarios such as a Sinkhole attack [32] in a smart home environment, wearable healthcare and environmental monitoring. According to the researcher the limitations in presented attack scenarios include the difficulty to depict all diverse connectivity paths, no-connectivity attack scenarios (*e.g.* Distributed-Denial-of-Service - DDoS) heterogeneity on communication protocols and static network topology.

3 Modeling Security Risks in IoT-enabled CPS

In order to identify and assess the risks against CPS that derive from related IoT technologies, we will adopt and extend our modeling approach for IoT-enabled attacks, initially presented in [47]. From a high-level view, the adversary's access capabilities to the IoT device will be combined with the connectivity level of the IoT device with the

target CPS, in order to identify and assess the attack paths against the target system that are enabled by the IoT device (see Figure 2).

Note that such an approach can be combined with generic risk assessment methodologies, such as ISO27005 [20] and NIST800-30 [42]. The characteristics of the adversary will be used to assess the threat level of an attack whereas hardware, software and network vulnerabilities will be used to assess the vulnerability level. Finally, characteristics similar to ones of the aforementioned reviewed methodologies (*e.g.* [16, 2]) can also be incorporated.

Calculating the risk involved among complex cyber physical systems that operate in a environment with IoT devices and related technologies can be a quite a challenging task during a risk assessment. The proposed algorithm takes into consideration the available inputs/outputs, functions, network and software characteristics of each IoT device, the potential attack vectors (access paths) to the IoT device and the attack paths that originate from the IoT device. Then, by utilizing state-of-the-art methodologies, the vulnerability, threat and impact level are calculated. Finally, using the aforementioned calculated metrics the risk level for each attack path scenario is defined. Depending on the attack path, the IoT device may be used either as a target or as an amplifier of an attack.

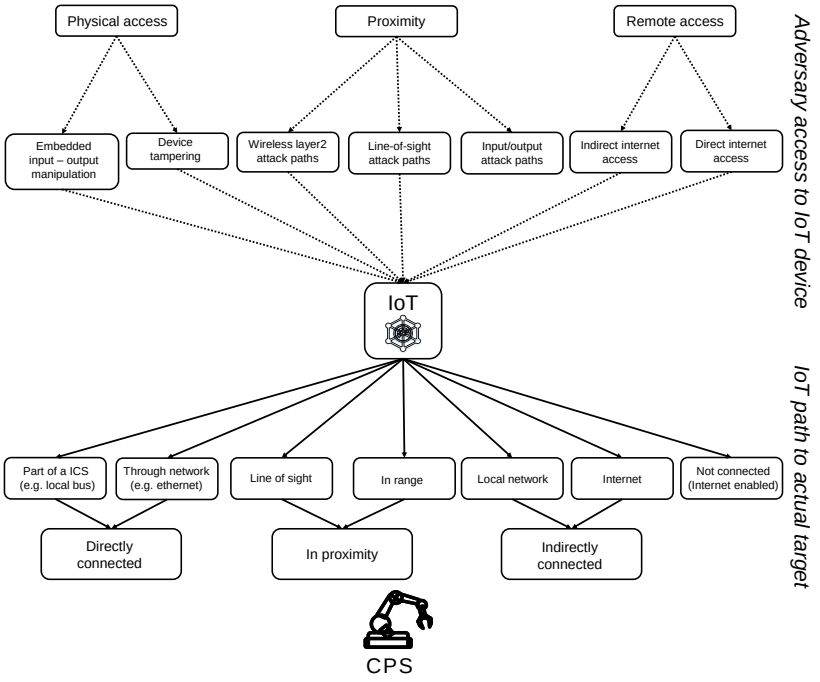

Figure 2: An overview of the components of the proposed risk assessment methodology

3.1 Attack vectors: Modeling the adversary

To assess the access level, one must consider three key factors: Physical, proximity and network access. Listing the device's physical characteristics such as network and input/output interfaces as well as location is essential in order to determine all possible direct machine-to-machine and human-to-device interactions that can take place. It is also a key factor in order to reduce the amount of the potential access paths per device thus eliminating impractical attack vectors (*e.g.* a layer-2-enabled temperature sensor cannot be directly accessed via layer-3 network).

3.1.1 Physical access

Physical access mainly describes the ability of an actor (malicious or not) to access sensitive inputs/outputs and/or modify/replace the IoT device thus affecting the threat level. For example, if physical tampering of the IoT device is required for an attack, then this attack will be less likely to happen, in comparison with one than can be triggered remotely (*e.g.* through the Internet). On the other hand, a susceptible to tampering IoT device, placed in a public area with no physical access security controls enforced (*e.g.* a IP-enabled security camera outside a factory's premises), can be used as a point of entry to the company's internal mission critical systems, with severe consequences.

3.1.2 Proximity

Proximity attack vectors and paths can be hard to identify and may include bidirectional machine-to-machine and human-to-machine interactions. In [2] authors present an approach that can potentially depict all machine-to-machine interactions under the assumption that all activity may take place among devices in proximity through all available input/output channels and network interfaces in their predefined range. Furthermore, subliminal attack paths may also occur when the range for input/output and network interfaces can be extended and functionality characteristics can be manipulated in unpredictable ways, so as to server an adversary's needs, as various researched have recently been demonstrated [39, 40].

For example, several IoT enabling technologies utilize devices that include unsecured and vulnerable inputs/outputs (*e.g.* sensing systems, Light Emitting Diode (LED) lights). A typical example is the LIght Detection and Ranging (LIDAR), that researchers proved that can be manipulated from up to a certain distance [36, 50]. Wireless layer-2 network interfaces (*e.g.* Bluetooth, Zigbee) can also be used by adversaries to remotely adjust and even replace the legitimate system software.

3.1.3 Remote access

If an attack can be triggered remotely by Internet adversaries, *e.g.* by abusing the connectivity features of the IoT, then such an attack has a high likelihood. The need for constant monitoring, remote management and control, cost reduction and increased productivity creates complex attack vectors that adversaries can use to their advantage. Since more and more IoT devices are Internet enabled attacks on such IoT systems are likely to increase in the near future. Recent real cyber attacks in Ukraine's smart grid [17,

26] considered to be the most prominent indirect connectivity attack scenarios: Through spear-phishing campaigns the adversaries manage to penetrate the corporate network and attack the remote controlled circuit brakers thus causing large-scale disruptions in the electricity network.

3.2 Impact level: Identifying attack paths

In some cases, the IoT device itself is the actual target of an attack. Unfortunately, the manufacturers of IoT devices do not usually consider security as the top priority, at least in the case of consumer IoT products. Even for IoT devices that are used in sensitive cyber-physical operations, characteristics like the reliability of the device are usually favored instead of security, for example in the case of implantable medical devices or SCADA field IoT devices.

However, due to their increased connectivity features, IoT devices may also be used as a means to attack other CPS that are *indirectly* connected with the IoT device. For example, consider a car infotainment system that may be indirectly connected to critical control systems of the vehicle.

Another category of subliminal attack paths, are those that involve vulnerable IoT technologies, whose functionality is *misused* or *extended* by an adversary, in an unpredictable way. For example, smart lights that are abused to create a covert channel for data exfiltration or even to attack patients and cause epileptic seizures [40]). IoT devices can be exploited so as to create, novel and hard-to-identify attack paths against other interconnected systems.

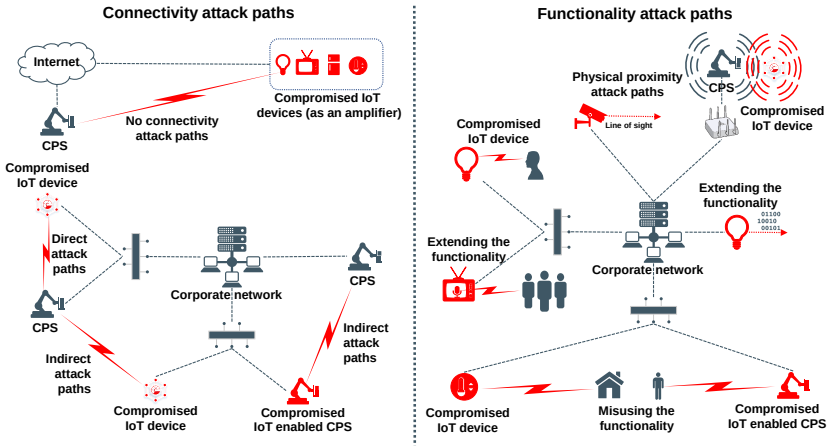

Figure 3: On the left side of the figure are shown IoT-enabled attack paths that are based on direct, indirect and no connectivity features whereas on the right side are presented potential attacks paths that may occur in case of misuse/abuse/extend the functionality of the IoT device/service. In both connectivity/functionality attack paths the aforementioned characteristics induce risk that is not easy to identify and assess.

Figure 3 presents typical examples of such attack paths, which are explained bellow.

3.2.1 Connectivity attack paths

These may be realized due to the physical and/or logical connectivity of vulnerable IoT devices with other critical CPS components.

- *Direct connectivity attack paths* The IoT device is part of a critical system, or has direct connection to it. In this case, the IoT device is usually the actual target of the attack, since in most cases, it is considered a crucial component of the CPS [24]. In addition, if network segmentation is not well implemented, the IoT device may be used as an amplifier in order to disrupt other systems or processes, as described in [46].
- *Indirect connectivity attack paths:* Such attack paths usually involve indirect attacks that are not always obvious (as in the previous case). For example, by using zero-day (or even known) exploits against an intermediate system connected to an already compromized IoT device in order to extend the attack towards a third system that is critical [31]. Vulnerable IoT devices may be used both as an amplifier [48, 44] or as the actual target of the attack [15, 25, 26]. Bring-Your-Own-Phone/Device (BYOP/D) policies may also cause indirect attack paths that may be hard to identify.

3.2.2 Attacks paths based on massive number of compromised IoT devices

Such attacks are usually based on the plethora of consumer IoT devices, such as smart home appliances and end-user devices. Although these devices are not connected (directly or indirectly) with critical CPS, they can still be used to create attack paths against critical systems (*e.g.* IoT-based botnets [9]). Compromised IoT devices in large numbers may cause Denial of Service (DoS attacks) against a critical system. A special case are concurrent Permanent DoS attacks that may target at the IoT devices themselves (*e.g.* ransomware attacks against consumer IoT devices). Although such devices are usually of low importance, a concurrent PDoS attack against thousands of devices may impose a high impact.

3.2.3 Functionality attack paths

Security researchers [40] and real incidents [49] have shown that it is possible to create subliminal attack paths by misusing or by extending the functionality of the IoT devices, to attack targets that are not connected (even indirectly) with the IoT device. Usually such attack are targeted against systems that are in some proximity with the vulnerable IoT device.

3.2.4 Physical proximity attack paths

IoT devices installed near critical CPS components may be used to create subliminal attack paths against them [18]. Proximity may imply close distance, or even line of sight proximity. These attacks exploit common characteristics of wireless technologies (*e.g.* IEEE 802.15.4x wireless network adapters for ZigBee and WirelessHART protocols all

use the same frequency for broadcasting). Such attacks are difficult to discover since they extend, alter or misuse the functionality of the IoT device in ways that cannot easily predicted [34]. Examples of such attacks include covert channels and data exfiltration attacks.

3.3 Calculating the vulnerability level

Since our methodology emphasizes on attacks against CPS that are IoT-enabled, and IoT technologies are usually the weakest link in the security chain due to their inherent limitations, identify the vulnerabilities of the IoT technologies involved. Vulnerability assessment should include at a minimum:

Embedded vulnerabilities on hardware (HW): IoT devices susceptible to physical tampering may allow an adversary to disable and/or extract sensitive hard-coded information, such as encryption keys and stored credentials, *e.g.* through the use of Correlation/ Differential Power Analysis (CPA/DPA) techniques [39].

Embedded vulnerabilities on software (SW): Untested, outdated software and vulnerable update services may enable an attacker to entirely compromise the device from distance. This includes, but is not limited to, publicly available and unsigned firmware update files, the use of outdated vulnerable operating systems and Application Programming Interfaces (APIs) that have not been security tested. Lack of security techniques and practices such as firmware signing, secure OS parameterization and input sanitation may allow an adversary to remotely exploit interconnected CPS, with minimal effort.

Network vulnerabilities on communication protocols: Vulnerable encryption algorithms used at the network layer, may reveal sensitive information. With most of the IoT communication protocols based on inherently insecure wireless network protocols (*e.g.* WirelessHART, ZigBee, MiWi, WiFi) an adversary can remotely eavesdrop, inject and modify network messages in order to accomplish an attack. In addition, constraints of the IoT devices, such as energy and computational power, make them susceptible to inadequate key management schemes. The lack of support for Public Key Cryptography (PKC), the use of weak encryption algorithms (*e.g.* WEP encryption over WiFi), the use of a single embedded network key (such as in the ZigBee Light Link - ZLL protocol) or the absence of encryption mechanisms, may be exploited in order to disrupt highly sophisticated and critical systems.

3.4 Calculating the risk

Based on the threat model described above, we describe a targeted, high-level risk assessment methodology, whose goal is to identify and assess *hidden risks* in CPS that stem from the IoT interaction. Following the RA standards, the calculation of the risks will be based on three basic phases: threat, vulnerability and impact assessment. Finally, the security risk of each identified attack path will be assessed. In the proposed methodology, one can use of typical Likert scales, to define the threat, vulnerability, impact and risk scales. This is common to most general purpose RA methodologies (*e.g.* [14, 42]), although each methodology may define a different scales for each risk factor.

By combining all the factors assessed in the previous phase, the risk of all possible IoT-enabled attack paths will be assessed in this phase. Essentially, during this process

all the steps performed in the previous phases will be combined to methodologically output all the related risks. Also, it is crucial, when defining the IoT devices/technologies, to take into consideration mobile devices such as smartphones and laptops (BYOD), since, they are equipped with multiple inputs, outputs and wireless network interfaces, can be directly/indirectly (via the corporate network) connected to the Internet, and sometimes are in proximity of mission critical systems.The basic steps of this process are as follows:

1. Identify all IoT devices and enabling technologies.
2. Repeat for each of IoT device (say device *i*):
   - 2.1. **Access paths:** Identify all applicable access paths (physical, proximity, remote) to the IoT device/enabling technology:
     - 2.1.1. If the device can be physically accessed define all of embedded device's input, output and wired network interfaces (*e.g.* USB, Ethernet & Serial ports, sensors, speakers)
     - 2.1.2. Proximity access paths: Define all of input, output and wireless network interfaces characteristics (frequency active range etc.) (*e.g.* ZigBee, Bluetooth, WiFi, Z-Wave, microphone range and sensitivity etc.).
     - 2.1.3. Remote access paths: Define all enabled layer-3 network interfaces. Then for each network interface define all possible access paths (directly, indirectly), especially the ones that lead to Internet connectivity (*e.g.* Ethernet $\rightarrow$ Control Room $\rightarrow$ Corporate network $\rightarrow$ Web server).
   - 2.2. **Attack paths:** Identify all possible attack paths against any affected CPS:
     - 2.2.1. *Direct connectivity attack paths:* Identify all direct attack paths between the IoT device and any other system.
     - 2.2.2. *Indirect connectivity attack paths:* Identify all systems that are indirectly connected to the IoT using any network interfaces (wired or wireless).
     - 2.2.3. Identify attack paths against any affected CPS, related with IoT *extended/misused functionality*:
       - 2.2.3.1. *Physical proximity:* Identify systems that are in physical proximity in respect with the IoT device's wireless network interfaces (*e.g.* protocols that use the same bandwidth, devices that are in line of sight etc [34]).
       - 2.2.3.2. *Potential covert channels:* Examine devices for possible ways to create hidden covert channels (*e.g.* smart lamp systems have used as a covert exfiltration channels [40]; smart TVs/cameras for espionage [49]).
       - 2.2.3.3. *Other potential misuse:* Examine devices for any other possible misuse against other CPS. Examples of such misuse include abusing smart lamp systems installed in hospitals to cause epileptic seizures [40]; alter the functionality of IoT-enabled industrial

robots to affect the production line [28, 8]; manipulate the functionality of thermostats to disrupt the operations of the data center [18]).

2.3. **Calculate risk:** For each identified attack path k (with target system j):

2.3.1. For each corresponding access path (attack vector):

2.3.1.1. Assess the threat level of the relative attack vector, denoted as T_{ijk}.

2.3.1.2. Assess the vulnerability of the IoT device, for the examined attack, denoted as V_{ijk}.

2.3.1.3. Assess the impact of the *actual target system* of the attack path, denoted as I_{ijk}.

2.3.1.4. Assess the risk of each examined attack path k that is triggered by IoT device i against the target system j as follows:

$$R_{ijk} = T_{ijk} V_{ijk} I_{ijk} \tag{1}$$

As a final step we propose the construction of a table with the calculated risk values of all IoT devices/enabling technologies in respect of the affected systems for all applicable paths. Metrics such as total risk ($R_{i_{total}}$) and Maximum Risk ($R_{i_{max j}}$) per affected system, can be used in order to assess the criticality of each IoT device/technology i, and help prioritize the implementation of the appropriate security controls, so as to effectively reduce the organization's risk levels under a desirable threshold.

4 Conclusions

Insecure off-the-shelf IoT devices and relative technologies that may be connected to critical cyber-physical systems, or even nearby such systems, may enable an adversary to discover attack paths against CPS and cause severe damage to such systems. Assessing the risk introduced from IoT ecosystem in CPS is a very challenging task. In our work we present a high-level risk assessment approach that mainly focuses on the identification of subliminal access/attack paths. In order to do so, we examine all applicable access paths (physical, proximity, remote) to the IoT device/technology. Then we estimate all paths from the IoT device to other CPSs based on direct or indirect connectivity and dependency, or on the proximity of the IoT device to the target CPS. As a future work, we will extend the proposed high-level risk assessment approach to develop a detailed risk assessment methodology. We also plan to develop a tool that can be used to automate the identification and assessment of hidden and subliminal attack paths of IoT technologies against critical components of CPS.

References

[1] Abie, H., Balasingham, I.: Risk-based adaptive security for smart iot in ehealth. In: Proceedings of the 7th International Conference on Body Area Networks, pp. 269–275. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering) (2012)

[2] Agadakos, I., Chen, C.Y., Campanelli, M., Anantharaman, P., Hasan, M., Copos, B., Lepoint, T., Locasto, M., Ciocarlie, G.F., Lindqvist, U.: Jumping the air gap: Modeling cyber-physical attack paths in the internet-of-things. In: Proceedings of the 2017 Workshop on Cyber-Physical Systems Security and PrivaCy, pp. 37–48. ACM (2017)

[3] Amin, S., Schwartz, G.A., Hussain, A.: In quest of benchmarking security risks to cyber-physical systems. IEEE Network **27**(1), 19–24 (2013)

[4] Atamli, A.W., Martin, A.: Threat-based security analysis for the internet of things. In: Secure Internet of Things (SIoT), 2014 International Workshop on, pp. 35–43. IEEE (2014)

[5] Atlam, H.F., Alenezi, A., Walters, R.J., Wills, G.B., Daniel, J.: Developing an adaptive risk-based access control model for the internet of things. In: 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), pp. 655–661 (2017)

[6] Bormann, C., Castellani, A.P., Shelby, Z.: CoAP: An application protocol for billions of tiny Internet nodes. IEEE Internet Computing **16**(2), 62 (2012)

[7] Cárdenas, A.A., Amin, S., Lin, Z.S., Huang, Y.L., Huang, C.Y., Sastry, S.: Attacks against process control systems: risk assessment, detection, and response. In: Proceedings of the 6th ACM symposium on information, computer and communications security, pp. 355–366. ACM (2011)

[8] Cesar, C., Lucas, A.: Hacking robots before Skynet (IOActive) (2017). URL `https://ioactive.com/pdfs/Hacking-Robots-Before-Skynet.pdf`

[9] Cobb, S.: 10 things to know about the October 21 IoT DDoS attacks (2016). URL `http://www.welivesecurity.com/2016/10/24/10-things-know-october-21-iot-ddos-attacks/`

[10] Darwish, S., Nouretdinov, I., Wolthusen, S.D.: Towards composable threat assessment for medical iot (miot). Procedia Computer Science **113**, 627–632 (2017)

[11] Depoy, J., Phelan, J., Sholander, P., Smith, B., Varnado, G., Wyss, G.: Risk assessment for physical and cyber attacks on critical infrastructures. In: Military Communications Conference, 2005. MILCOM 2005. IEEE, pp. 1961–1969. IEEE (2005)

[12] Dorsemaine, B., Gaulier, J.P., Wary, J.P., Kheir, N., Urien, P.: A new threat assessment method for integrating an iot infrastructure in an information system. In: Distributed Computing Systems Workshops (ICDCSW), 2017 IEEE 37th International Conference on, pp. 105–112. IEEE (2017)

[13] Erdősi, P.M.: The common vulnerability scoring system (cvss) generations–usefulness and deficiencies

[14] Evans, D., Bond, P., Bement, A.: Fips pub 199 standards for security categorization of federal information and information systems. The National Institute of Standards and Technology (NIST) (2004)

[15] Falliere, N., Murchu, L.O., Chien, E.: W32. stuxnet dossier. White paper, Symantec Corp., Security Response **5**(6) (2011)

[16] Ge, M., Hong, J.B., Guttmann, W., Kim, D.S.: A framework for automating security analysis of the internet of things. Journal of Network and Computer Applications **83**, 12–27 (2017)

[17] Goodin, D.: Hackers trigger yet another power outage in Ukraine (2017). URL `https://arstechnica.com/security/2017/01/the-new-normal-yet-another-hacker-caused-power-outage-hits-ukraine/`

[18] Hernandez, G., Arias, O., Buentello, D., Jin, Y.: Smart nest thermostat: A smart spy in your home. Black Hat USA (2014)

[19] Hong, J., Kim, D.S.: Harms: Hierarchical attack representation models for network security analysis (2012)

[20] ISO: ISO/IEC 27005:2011 Information technology – Security techniques – information security risk management. Tech. rep., International Standardization Organization (2011)

[21] Knowles, W., Prince, D., Hutchison, D., Disso, J.F.P., Jones, K.: A survey of cyber security management in industrial control systems. International journal of critical infrastructure protection **9**, 52–80 (2015)

[22] Kott, A., Ludwig, J., Lange, M.: Assessing mission impact of cyberattacks: toward a model-driven paradigm. IEEE Security & Privacy (5), 65–74 (2017)

[23] Kott, A., Wang, C., Erbacher, R.F.: Cyber defense and situational awareness, vol. 62. Springer (2015)

[24] KrebsonSecurity: Fbi: Smart meter hacks likely to spread (2012). URL `https://krebsonsecurity.com/2012/04/fbi-smart-meter-hacks-likely-to-spread/`

[25] Kushner, D.: The real story of Stuxnet. IEEE Spectrum **50**(3), 48–53 (2013)

[26] Lee, R.M., Assante, M.J., Conway, T.: Analysis of the cyber attack on the Ukrainian power grid. SANS Industrial Control Systems (2016)

[27] Liu, C., Zhang, Y., Zeng, J., Peng, L., Chen, R.: Research on dynamical security risk assessment for the internet of things inspired by immunology. In: Natural Computation (ICNC), 2012 Eighth International Conference on, pp. 874–878. IEEE (2012)

[28] Maggi, F., Quarta, D., Pogliani, M., Polino, M., Zanchettin, A.M., Zanero, S.: Rogue robots: Testing the limits of an industrial robot's security. Tech. rep., Trend Micro, Politecnico di Milano (2017)

[29] Maglaras, L., Ferrag, M.A., Derhab, A., Mukherjee, M., Janicke, H., Rallis, S.: Threats, countermeasures and attribution of cyber attacks on critical infrastructures. Security and Safety **5**(16), 1–9 (2018). DOI 10.4108/eai.15-10-2018.155856

[30] Maglaras, L., Ferrag, M.A., Derhab, A., Mukherjee, M., Janicke, H., Rallis, S.: Threats, protection and attribution of cyber attacks on critical infrastructures. arXiv preprint arXiv:1901.03899 (2019)

[31] Marin, E., Singelée, D., Garcia, F.D., Chothia, T., Willems, R., Preneel, B.: On the (in) security of the latest generation implantable cardiac defibrillators and how to secure them. In: Proceedings of the 32nd Annual Conference on Computer Security Applications, pp. 226–236. ACM (2016)

[32] Martins, D., Guyennet, H.: Wireless sensor network attacks and security mechanisms: A short survey. In: Network-Based Information Systems (NBiS), 2010 13th International Conference on, pp. 313–320. IEEE (2010)

[33] Neisse, R., Steri, G., Fovino, I.N., Baldini, G.: Seckit: a model-based security toolkit for the internet of things. Computers & Security **54**, 60–76 (2015)

[34] O'Flynn, C.P.: Message denial and alteration on IEEE 802.15.4 low-power radio networks. In: New Technologies, Mobility and Security (NTMS), 2011 4th IFIP International Conference on, pp. 1–5. IEEE (2011)

[35] Peng, Y., Lu, T., Liu, J., Gao, Y., Guo, X., Xie, F.: Cyber-physical system risk assessment. In: Intelligent Information Hiding and Multimedia Signal Processing, 2013 Ninth International Conference on, pp. 442–447. IEEE (2013)

[36] Petit, J., Stottelaar, B., Feiri, M., Kargl, F.: Remote attacks on automated vehicles sensors: Experiments on camera and Lidar. Black Hat Europe **11**, 2015 (2015)

[37] Quarta, D., Pogliani, M., Polino, M., Maggi, F., Zanchettin, A.M., Zanero, S.: An experimental security analysis of an industrial robot controller. In: Security and Privacy (SP), 2017 IEEE Symposium on, pp. 268–286. IEEE (2017)

[38] Ralston, P.A., Graham, J.H., Hieb, J.L.: Cyber security risk assessment for scada and dcs networks. ISA transactions **46**(4), 583–594 (2007)

[39] Ronen, E., O'Flynn, C., Shamir, A., Weingarten, A.O.: IoT goes nuclear: Creating a zigbee chain reaction. IACR Cryptology ePrint Archive **2016**, 1047 (2016)

[40] Ronen, E., Shamir, A.: Extended functionality attacks on iot devices: The case of smart lights. In: 2016 IEEE European Symposium on Security and Privacy (EuroS&P), pp. 3–12. IEEE (2016)

[41] Ross, R.S.: NIST SP-800-39 Managing Information Security Risk–Organization, Mission, and Information System View. The National Institute of Standards and Technology (NIST), Gaithersburg (2011)

[42] Ross, R.S.: NIST SP-800-30rev1 Guide for conducting risk assessments. The National Institute of Standards and Technology (NIST), Gaithersburg (2012)

[43] Sahner, R.A., Trivedi, K., Puliafito, A.: Performance and reliability analysis of computer systems: an example-based approach using the SHARPE software package. Springer Science & Business Media (2012)

[44] Santamarta, R.: In flight hacking system (IOActive Research Labs) (2016). URL http://blog.ioactive.com/2016/12/in-flight-hacking-system.html

[45] Shelby, Z., Bormann, C.: 6LoWPAN: The wireless embedded Internet, vol. 43. John Wiley & Sons (2011)

[46] Spenneberg, R., Brüggemann, M., Schwartke, H.: PLC-blaster: A worm living solely in the PLC. Black Hat Asia, Marina Bay Sands, Singapore (2016)

[47] Stellios, I., Kotzanikolaou, P., Psarakis, M., Alcaraz, C., Lopez, J.: A survey of iot-enabled cyberattacks: Assessing attack paths to critical infrastructures and services. IEEE Communications Surveys & Tutorials **20**(4), 3453–3495 (2018)

[48] TrapX Research, Labs: Anatomy of Attack: MEDJACK.2 – Hospitals Under Siege. TrapX Investigative Report (2016)

[49] Wikileaks: Vault 7: CIA Hacking Tools Revealed - CIA malware targets iPhone, Android, smart TVs (2017). URL https://wikileaks.org/ciav7p1/

[50] Yan, C., Wenyuan, X., Liu, J.: Can you trust autonomous vehicles: Contactless attacks against sensors of self-driving vehicle. DEF CON (2016)

[51] Yusuf, S.E., Ge, M., Hong, J.B., Kim, H.K., Kim, P., Kim, D.S.: Security modelling and analysis of dynamic enterprise networks. In: Computer and Information Technology (CIT), 2016 IEEE International Conference on, pp. 249–256. IEEE (2016)