Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks

Mohamed Abomhara and Geir M. Køien

Department of Information and Communication Technology,
University of Agder, Norway
Corresponding Authors: {Mohamed.abomhara; geir.koien}@uia.no

Received 14 September 2014; Accepted 17 April 2015;
Publication 22 May 2015

Abstract

Internet of Things (IoT) devices are rapidly becoming ubiquitous while IoT services are becoming pervasive. Their success has not gone unnoticed and the number of threats and attacks against IoT devices and services are on the increase as well. Cyber-attacks are not new to IoT, but as IoT will be deeply interwoven in our lives and societies, it is becoming necessary to step up and take cyber defense seriously. Hence, there is a real need to secure IoT, which has consequently resulted in a need to comprehensively understand the threats and attacks on IoT infrastructure. This paper is an attempt to classify threat types, besides analyze and characterize intruders and attacks facing IoT devices and services.

Keywords: Internet of Things, Cyber-attack, Security threats.

1 Introduction

The recent rapid development of the Internet of Things (IoT) [1, 2] and its ability to offer different types of services have made it the fastest growing technology, with huge impact on social life and business environments. IoT has

Journal of Cyber Security, Vol. 4, 65–88.
doi: 10.13052/jcsm2245-1439.414

gradually permeated all aspects of modern human life, such as education, healthcare, and business, involving the storage of sensitive information about individuals and companies, financial data transactions, product development and marketing.

The vast diffusion of connected devices in the IoT has created enormous demand for robust security in response to the growing demand of millions or perhaps billions of connected devices and services worldwide [3–5].

The number of threats is rising daily, and attacks have been on the increase in both number and complexity. Not only is the number of potential attackers along with the size of networks growing, but the tools available to potential attackers are also becoming more sophisticated, efficient and effective [6, 7]. Therefore, for IoT to achieve fullest potential, it needs protection against threats and vulnerabilities [8].

Security has been defined as a process to protect an object against physical damage, unauthorized access, theft, or loss, by maintaining high confidentiality and integrity of information about the object and making information about that object available whenever needed [7, 9]. According to Kizza [7] there is no thing as the secure state of any object, tangible or not, because no such object can ever be in a perfectly secure state and still be useful. An object is secure if the process can maintain its maximum intrinsic value under different conditions. Security requirements in the IoT environment are not different from any other ICT systems. Therefore, ensuring IoT security requires maintaining the highest intrinsic value of both tangible objects (devices) and intangible ones (services, information and data).

This paper seeks to contribute to a better understanding of threats and their attributes (motivation and capabilities) originating from various intruders like organizations and intelligence. The process of identifying threats to systems and system vulnerabilities is necessary for specifying a robust, complete set of security requirements and also helps determine if the security solution is secure against malicious attacks [10]. As well as users, governments and IoT developers must ultimately understand the threats and have answers to the following questions:

1. What are the assets?
2. Who are the principal entities?
3. What are the threats?
4. Who are the threat actors?
5. What capability and resource levels do threat actors have?
6. Which threats can affect what assets?

7. Is the current design protected against threats?
8. What security mechanisms could be used against threats?

The remainder of this paper is organized as follows. Section 2 provides a background, definitions, and the primary security and privacy goals. Section 3 identifies some attacker motivations and capabilities, and provides an outline of various sorts of threat actors. Finally, the paper concludes with Section 4.

2 Background

The IoT [1, 2, 11] is an extension of the Internet into the physical world for interaction with physical entities from the surroundings. Entities, devices and services [12] are key concepts within the IoT domain, as depicted in Figure 1 [13]. They have different meanings and definitions among various projects. Therefore, it is necessary to have a good understanding of what IoT entities, devices and services are (discussed in detail in Section 2.1).

An entity in the IoT could be a human, animal, car, logistic chain item, electronic appliance or a closed or open environment [14]. Interaction among

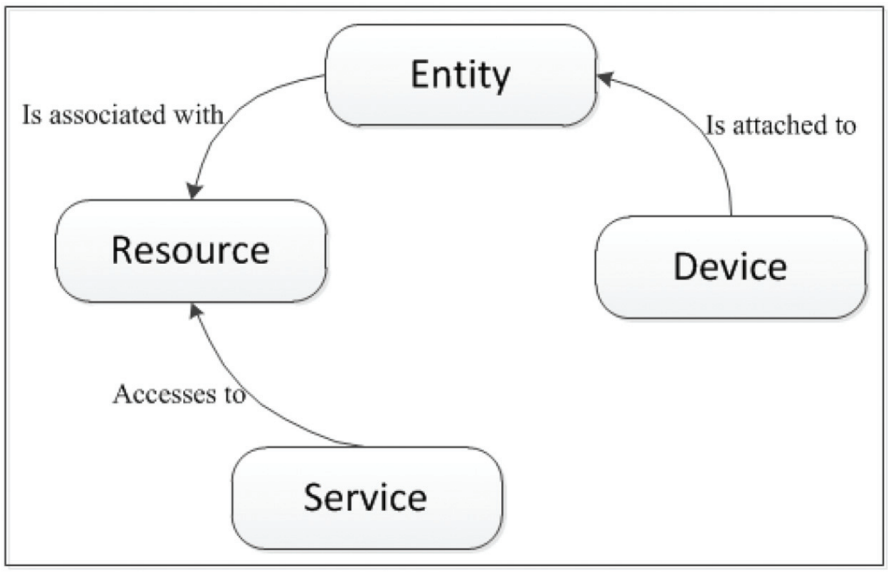

Figure 1 IoT model: key concepts and interactions.

entities is made possible by hardware components called devices [12] such as mobile phones, sensors, actuators or RFID tags, which allow the entities to connect to the digital world [15].

In the current state of technology, Machine-to-Machine (M2M) is the most popular application form of IoT. M2M is now widely employed in power, transportation, retail, public service management, health, water, oil and other industries to monitor and control the user, machinery and production processes in the global industry and so on [5, 16, 17]. According to estimates M2M applications will reach 12 billion connections by 2020 and generate approximately 714 billion euros in revenues [2].

Besides all the IoT application benefits, several security threats are observed [17–19]. The connected devices or machines are extremely valuable to cyber-attackers for several reasons:

1. Most IoT devices operate unattended by humans, thus it is easy for an attacker to physically gain access to them.
2. Most IoT components communicate over wireless networks where an attacker could obtain confidential information by eavesdropping.
3. Most IoT components cannot support complex security schemes due to low power and computing resource capabilities.

In addition, cyber threats could be launched against any IoT assets and facilities, potentially causing damage or disabling system operation, endangering the general populace or causing severe economic damage to owners and users [20, 21]. Examples include attacks on home automation systems and taking control of heating systems, air conditioning, lighting and physical security systems. The information collected from sensors embedded in heating or lighting systems could inform the intruder when somebody is at home or out. Among other things, cyber-attacks could be launched against any public infrastructure like utility systems (power systems or water treatment plants) [22] to stop water or electricity supply to inhabitants.

Security and privacy issues are a growing concern for users and suppliers in their shift towards the IoT [23]. It is certainly easy to imagine the amount of damage caused if any connected devices were attacked or corrupted. It is well-recognized that adopting any IoT technology within our homes, work, or business environments opens doors to new security problems. Users and suppliers must consider and be cautious with such security and privacy concerns.

2.1 Understanding IoT Devices and Services

In this section, the main IoT domain concepts that are important from a business process perspective are defined and classified, and the relationships between IoT components (IoT devices and IoT services) are described.

2.1.1 IoT device

This is a hardware component that allows the entity to be a part of the digital world [12]. It is also referred to as a smart thing, which can be a home appliance, healthcare device, vehicle, building, factory and almost anything networked and fitted with sensors providing information about the physical environment (e.g., temperature, humidity, presence detectors, and pollution), actuators (e.g., light switches, displays, motor-assisted shutters, or any other action that a device can perform) and embedded computers [24, 25].

An IoT device is capable of communicating with other IoT devices and ICT systems. These devices communicate via different means including cellular (3G or LTE), WLAN, wireless or other technologies [8]. IoT device classification depends on size, i.e., small or normal; mobility, i.e., mobile or fixed; external or internal power source; whether they are connected intermittently or always-on; automated or non-automated; logical or physical objects; and lastly, whether they are IP-enabled objects or non IP objects.

The characteristics of IoT devices are their ability to actuate and/or sense, the capability of limiting power/energy, connection to the physical world, intermittent connectivity and mobility [23]. Some must be fast and reliable and provide credible security and privacy, while others might not [9]. A number of these devices have physical protection whereas others are unattended.

In fact, in IoT environments, devices should be protected against any threats that can affect their functionality. However, most IoT devices are vulnerable to external and internal attacks due to their characteristics [16]. It is challenging to implement and use a strong security mechanism due to resource constraints in terms of IoT computational capabilities, memory, and battery power [26].

2.1.2 IoT services

IoT services facilitate the easy integration of IoT entities into the service-oriented architecture (SOA) world as well as service science [27]. According to Thoma [28], an IoT service is a transaction between two parties: the service provider and service consumer. It causes a prescribed function, enabling

interaction with the physical world by measuring the state of entities or by initiating actions that will initiate a change to the entities.

A service provides a well-defined and standardized interface, offering all necessary functionalities for interacting with entities and related processes. The services expose the functionality of a device by accessing its hosted resources [12].

2.1.3 Security in IoT devices and services

Ensuring the security entails protecting both IoT devices and services from unauthorized access from within the devices and externally. Security should protect the services, hardware resources, information and data, both in transition and storage. In this section, we identified three key problems with IoT devices and services: data confidentiality, privacy and trust.

Data confidentiality represents a fundamental problem in IoT devices and services [27]. In IoT context not only user may access to data but also authorized object. This requires addressing two important aspects: first, access control and authorization mechanism and second authentication and identity management (IdM) mechanism. The IoT device needs to be able to verify that the entity (person or other device) is authorized to access the service. Authorization helps determine if upon identification, the person or device is permitted to receive a service. Access control entails controlling access to resources by granting or denying means using a wide array of criteria. Authorization and access control are important to establishing a secure connection between a number of devices and services. The main issue to be dealt with in this scenario is making access control rules easier to create, understand and manipulate. Another aspect that should be consider when dealing with confidentiality is authentication and identity management. In fact this issue is critical in IoT, because multiple users, object/things and devices need to authenticate each other through trustable services. The problem is to find solution for handling the identity of user, things/objects and devices in a secure manner.

Privacy is an important issue in IoT devices and service on account of the ubiquitous character of the IoT environment. Entities are connected, and data is communicated and exchanged over the internet, rendering user privacy a sensitive subject in many research works. Privacy in data collection, as well as data sharing and management, and data security matters remain open research issues to be fulfilled.

Trust plays an important role in establishing secure communication when a number of things communicate in an uncertain IoT environment. Two dimensions of trust should be considered in IoT: trust in the interactions between entities, and trust in the system from the users perspective [29] According to Køien [9] the trustworthiness of an IoT device depends on the device components including the hardware, such as processor, memory, sensors and actuators, software resources like hardware-based software, operating system, drivers and applications, and the power source. In order to gain user/services trust, there should be an effective mechanism of defining trust in a dynamic and collaborative IoT environment.

2.2 Security Threats, Attacks, and Vulnerabilities

Before addressing security threats, the system assets (system components) that make up the IoT must first be identified. It is important to understand the asset inventory, including all IoT components, devices and services.

An asset is an economic resource, something valuable and sensitive owned by an entity. The principal assets of any IoT system are the system hardware (include buildings, machinery, etc.) [11], software, services and data offered by the services [30].

2.2.1 Vulnerability

Vulnerabilities are weaknesses in a system or its design that allow an intruder to execute commands, access unauthorized data, and/or conduct denial-of-service attacks [31, 32]. Vulnerabilities can be found in variety of areas in the IoT systems. In particular, they can be weaknesses in system hardware or software, weaknesses in policies and procedures used in the systems and weaknesses of the system users themselves [7].

IoT systems are based on two main components; system hardware and system software, and both have design flaws quite often. Hardware vulnerabilities are very difficult to identify and also difficult to fix even if the vulnerability were identified due to hardware compatibility and interoperability and also the effort it take to be fixed. Software vulnerabilities can be found in operating systems, application software, and control software like communication protocols and devices drives. There are a number of factors that lead to software design flaws, including human factors and software complexity. Technical vulnerabilities usually happen due to human weaknesses. Results of not understanding the requirements comprise starting

the project without a plan, poor communication between developers and users, a lack of resources, skills, and knowledge, and failing to manage and control the system [7].

2.2.2 Exposure

Exposure is a problem or mistake in the system configuration that allows an attacker to conduct information gathering activities. One of the most challenging issues in IoT is resiliency against exposure to physical attacks. In the most of IoT applications, devices may be left unattended and likely to be placed in location easily accessible to attackers. Such exposure raises the possibility that an attacker might capture the device, extract cryptographic secrets, modify their programming, or replace them with malicious device under the control of the attacker [33].

2.2.3 Threats

A threat is an action that takes advantage of security weaknesses in a system and has a negative impact on it [34]. Threats can originate from two primary sources: humans and nature [35, 36]. Natural threats, such as earthquakes, hurricanes, floods, and fire could cause severe damage to computer systems. Few safeguards can be implemented against natural disasters, and nobody can prevent them from happening. Disaster recovery plans like backup and contingency plans are the best approaches to secure systems against natural threats. Human threats are those caused by people, such as malicious threats consisting of internal [37] (someone has authorized access) or external threats [38] (individuals or organizations working outside the network) looking to harm and disrupt a system. Human threats are categorized into the following:

- Unstructured threats consisting of mostly inexperienced individuals who use easily available hacking tools.
- Structured threats as people know system vulnerabilities and can understand, develop and exploit codes and scripts. An example of a structured threat is Advanced Persistent Threats (APT) [39]. APT is a sophisticated network attack targeted at high-value information in business and government organizations, such as manufacturing, financial industries and national defense, to steal data [40].

As IoT become a reality, a growing number of ubiquitous devices has raise the number of the security threats with implication for the general public. Unfortunately, IoT comes with new set of security threat. There are

a growing awareness that the new generation of smart-phone, computers and other devices could be targeted with malware and vulnerable to attack.

2.2.4 Attacks

Attacks are actions taken to harm a system or disrupt normal operations by exploiting vulnerabilities using various techniques and tools. Attackers launch attacks to achieve goals either for personal satisfaction or recompense. The measurement of the effort to be expended by an attacker, expressed in terms of their expertise, resources and motivation is called attack cost [32]. Attack actors are people who are a threat to the digital world [6]. They could be hackers, criminals, or even governments [7]. Additional details are discussed in Section 3.

An attack itself may come in many forms, including active network attacks to monitor unencrypted traffic in search of sensitive information; passive attacks such as monitoring unprotected network communications to decrypt weakly encrypted traffic and getting authentication information; close-in attacks; exploitation by insiders, and so on. Common cyber-attack types are:

(a) Physical attacks: This sort of attack tampers with hardware components. Due to the unattended and distributed nature of the IoT, most devices typically operate in outdoor environments, which are highly susceptible to physical attacks.
(b) Reconnaissance attacks – unauthorized discovery and mapping of systems, services, or vulnerabilities. Examples of reconnaissance attacks are scanning network ports [41], packet sniffers [42], traffic analysis, and sending queries about IP address information.
(c) Denial-of-service (DoS): This kind of attack is an attempt to make a machine or network resource unavailable to its intended users. Due to low memory capabilities and limited computation resources, the majority of devices in IoT are vulnerable to resource enervation attacks.
(d) Access attacks – unauthorized persons gain access to networks or devices to which they have no right to access. There are two different types of access attack: the first is physical access, whereby the intruder can gain access to a physical device. The second is remote access, which is done to IP-connected devices.
(e) Attacks on privacy: Privacy protection in IoT has become increasingly challenging due to large volumes of information easily available

through remote access mechanisms. The most common attacks on user privacy are:

- Data mining: enables attackers to discover information that is not anticipated in certain databases.
- Cyber espionage: using cracking techniques and malicious software to spy or obtain secret information of individuals, organizations or the government.
- Eavesdropping: listening to a conversation between two parties [43].
- Tracking: a users movements can be tracked by the devices unique identification number (UID). Tracking a users location facilitates identifying them in situations in which they wish to remain anonymous.
- Password-based attacks: attempts are made by intruders to duplicate a valid user password. This attempt can be made in two different ways: 1) dictionary attack – trying possible combinations of letters and numbers to guess user passwords; 2) brute force attacks – using cracking tools to try all possible combinations of passwords to uncover valid passwords.

(f) Cyber-crimes: The Internet and smart objects are used to exploit users and data for materialistic gain, such as intellectual property theft, identity theft, brand theft, and fraud [6, 7, 44].

(g) Destructive attacks: Space is used to create large-scale disruption and destruction of life and property. Examples of destructive attacks are terrorism and revenge attacks.

(h) Supervisory Control and Data Acquisition (SCADA) Attacks: As any other TCP/IP systems, the SCADA [45] system is vulnerable to many cyber attacks [46, 47]. The system can be attacked in any of the following ways:

i. Using denial-of-service to shut down the system.
ii. Using Trojans or viruses to take control of the system. For instance, in 2008 an attack launched on an Iranian nuclear facility in Natanz using a virus named Stuxnet [48].

2.3 Primary Security and Privacy Goals

To succeed with the implementation of efficient IoT security, we must be aware of the primary security goals as follows:

2.3.1 Confidentiality

Confidentiality is an important security feature in IoT, but it may not be mandatory in some scenarios where data is presented publicly [18]. However, in most situations and scenarios sensitive data must not be disclosed or read by unauthorized entities. For instance patient data, private business data, and/or military data as well as security credentials and secret keys, must be hidden from unauthorized entities.

2.3.2 Integrity

To provide reliable services to IoT users, integrity is a mandatory security property in most cases. Different systems in IoT have various integrity requirements [49]. For instance, a remote patient monitoring system will have high integrity checking against random errors due to information sensitivities. Loss or manipulation of data may occur due to communication, potentially causing loss of human lives [6].

2.3.3 Authentication and authorization

Ubiquitous connectivity of the IoT aggravates the problem of authentication because of the nature of IoT environments, where possible communication would take place between device to device (M2M), human to device, and/or human to human. Different authentication requirements necessitate different solutions in different systems. Some solutions must be strong, for example authentication of bank cards or bank systems. On the other hand, most will have to be international, e.g., ePassport, while others have to be local [6]. The authorization property allows only authorized entities (any authenticated entity) to perform certain operations in the network.

2.3.4 Availability

A user of a device (or the device itself) must be capable of accessing services anytime, whenever needed. Different hardware and software components in IoT devices must be robust so as to provide services even in the presence of malicious entities or adverse situations. Various systems have different availability requirements. For instance, fire monitoring or healthcare monitoring systems would likely have higher availability requirements than roadside pollution sensors.

2.3.5 Accountability

When developing security techniques to be used in a secure network, accountability adds redundancy and responsibility of certain actions, duties and

planning of the implementation of network security policies. Accountability itself cannot stop attacks but is helpful in ensuring the other security techniques are working properly. Core security issues like integrity and confidentiality may be useless if not subjected to accountability. Also, in case of a repudiation incident, an entity would be traced for its actions through an accountability process that could be useful for checking the inside story of what happened and who was actually responsible for the incident.

2.3.6 Auditing

A security audit is a systematic evaluation of the security of a device or service by measuring how well it conforms to a set of established criteria. Due to many bugs and vulnerabilities in most systems, security auditing plays an important role in determining any exploitable weaknesses that put the data at risk. In IoT, a systems need for auditing depends on the application and its value.

2.3.7 Non-repudiation

The property of non-repudiation produces certain evidence in cases where the user or device cannot deny an action. Non-repudiation is not considered an important security property for most of IoT. It may be applicable in certain contexts, for instance, payment systems where users or providers cannot deny a payment action.

2.3.8 Privacy goals

Privacy is an entitys right to determine the degree to which it will interact with its environment and to what extent the entity is willing to share information about itself with others. The main privacy goals in IoT are:

- Privacy in devices – depends on physical and commutation privacy. Sensitive information may be leaked out of the device in cases of device theft or loss and resilience to side channel attacks.
- Privacy during communication – depends on the availability of a device, and device integrity and reliability. IoT devices should communicate only when there is need, to derogate the disclosure of data privacy during communication.
- Privacy in storage – to protect the privacy of data stored in devices, the following two things should be considered:
    - Possible amounts of data needed should be stored in devices.

  - Regulation must be extended to provide protection of user data after end-of-device life (deletion of the device data (Wipe) if the device is stolen, lost or not in use).
- Privacy in processing – depends on device and communication integrity [50]. Data should be disclosed to or retained from third parties without the knowledge of the data owner.
- Identity privacy – the identity of any device should only discovered by authorized entity (human/device).
- location privacy – the geographical position of relevant device should only discovered by authorized entity (human/device) [51].

3 Intruders, Motivations and Capabilities

Intruders have different motives and objectives, for instance, financial gain, influencing public opinion, and espionage, among many others. The motives and goals of intruders vary from individual attackers to sophisticated organized-crime organizations.

Intruders also have different levels of resources, skill, access and risk tolerance leading to the portability level of an attack occurring [52]. An insider has more access to a system than outsiders. Some intruders are well-funded and others work on a small budget or none. Every attacker chooses an attack that is affordable, an attack with good return on the investment based on budget, resources and experience [6]. In this section, intruders are categorized according to characteristics, motives and objectives, capabilities and resources.

3.1 Purpose and Motivation of Attack

Government websites, financial systems, news and media websites, military networks, as well as public infrastructure systems are the main targets for cyber-attacks. The value of these targets is difficult to estimate, and estimation often varies between attacker and defender. Attack motives range from identity theft, intellectual property theft, and financial fraud, to critical infrastructure attacks. It is quite difficult to list what motivates hackers to attack systems. For instance, stealing credit card information has become a hackers hobby nowadays, and electronic terrorism organizations attack government systems in order to make politics, religion interest.

3.2 Classification of Possible Intruders

A Dolev-Yao (DY) type of intruder shall generally be assumed [53, 54]. That is, an intruder which is in effect the network and which may intercept all or any message ever transmitted between IoT devices and hubs. The DY intruder is extremely capable but its capabilities are slightly unrealistic. Thus, safety will be much stronger if our IoT infrastructure is designed to be DY intruder resilient. However, the DY intruder lacks one capability that ordinary intruders may have, namely, physical compromise. Thus, tamper-proof devices are also greatly desirable. This goal is of course unattainable, but physical tamper resistance is nevertheless a very important goal, which, together with tamper detection capabilities (tamper evident) may be a sufficient first-line defense.

In the literature intruders are classified into two main types: internal and external. Internal intruders are users with privileges or authorized access to a system with either an account on a server or physical access to the network [21, 37]. External intruders are people who do not belong to the network domain. All intruders, whether internal or external, can be organized in many ways and involve individual attackers to spy agencies working for a country. The impact of an intrusion depends on the goals to be achieved. An individual attacker could have small objectives while spy agencies could have larger motives [55]. The various types of intruders will be discussed hereby based on their numbers, motives and objectives.

3.2.1 Individuals

Individual hackers are professionals who work alone and only target systems with low security [55]. They lack resources or expertise of professional hacking teams, organizations or spy agencies. Individual hacker targets are relatively small in size or diversity and the attacks launched have relatively lower impact than ones launched by organized groups (discussed in 3.2.2). Social engineering techniques are most commonly used by individual attackers, as they have to obtain basic information about a target system like the address, password, port information, etc. Public and social media websites are the most common places where general users can be deceived by hackers. Moreover, operating systems used on laptops, PCs, and mobile phones have common and known vulnerabilities exploitable by individual attackers.

Financial institutions such as banks are also major targets for individual attackers as they know that such types of networks carry financial transactions that can be hacked, and thus attackers can manipulate the information in

their interest. Credit card information theft has a long history with individual hackers. With the growth of e-commerce, it is easier to use stolen credit card information to buy goods and services.

Individual hackers use tools such as viruses, worms and sniffers to exploit a system. They plan attacks based on equipment availability, internet access availability, the network environment and system security.

One of the individual hacker categories is the insider [21, 37]. Insiders are authorized individuals working against a system using insider knowledge or privileges. Insiders could provide critical information for outsider attackers (third party) to exploit vulnerabilities that can enable an attack. They know the weak points in the system and how the system works. Personal gain, revenge, and financial gain can motivate an insider. They can tolerate risk ranging from low to high depending on their motivation.

3.2.2 Organized groups

Criminal groups are becoming more familiar with ongoing communications and IoT technology. In addition, as they become more comfortable with technological applications, these groups can be more aware of opportunities offered by the infrastructure routing information of different networks. The motivations of these groups are quite diverse; their targets typically include particular organizations for revenge, theft of trade secrets, economic espionage, and targeting the national information infrastructure. They also involve selling personal information, such as financial data, to other criminal organizations, terrorists, and even governments.

They are very capable in terms of financial funding, expertise and resources. Criminal groups capabilities in terms of methods and techniques are moderate to high depending on what the goals are. They are very skillful at creating botnets and malicious software (e.g., computer viruses and scareware) and denial-of-service attack methods [44]. Organized criminals are likely to have access to funds, meaning they can hire skilled hackers if necessary, or purchase point-and-click attack tools from the underground economy with which to attack any systems [46]. Such criminals can tolerate higher risk than individual hackers and are willing to invest in profitable attacks.

Cyber terrorism [21, 56] is a form of cyber-attack that targets military systems, banks, and specific facilities such as satellites, and telecommunication systems associated with the national information infrastructure based on religious and political interests. Terrorist organizations depend on the internet to spread propaganda, raise funds, gather information, and communicate

with co-conspirators in all parts of the world. Another prevalent group of criminal organization entails hacktivists. Hacktivists are groups of hackers who engage in activities such as denial-of-service, fraud, and/or identity theft. Also, some of these groups have political motivations, like the Syrian Electronic Army (SEA) [57], Iranian Cyber Army and Chinese cyber-warfare units [58].

3.2.3 Intelligence agency

Intelligence agencies from different countries are persistent in their efforts to probe the military systems of other countries for specific purposes, for example industrial espionage, and political and military espionage. To accomplish their objectives, the agencies require a large number of experts, infrastructure ranging from research and development entities to provide technologies and methodologies (hardware, software, and facilities) besides financial and human resources.

Such agencies have organized structures and sophisticated resources to accomplish their intrusion goals. This sort of agencies are the biggest threat to networks and necessitate tight surveillance and monitoring approaches to safeguard against threats to the information systems of prime importance for any country and military establishment.

4 Discussion and Conclusions

4.1 Discussion

The exponential growth of the IoT has led to greater security and privacy risks. Many such risks are attributable to device vulnerabilities that arise from cybercrime by hackers and improper use of system resources. The IoT needs to be built in such a way as to ensure easy and safe usage control. Consumers need confidence to fully embrace the IoT in order to enjoy its benefits and avoid security and privacy risks.

The majority of IoT devices and services are exposed to a number of common threats as discussed earlier, like viruses and denial-of-service attacks. Taking simple steps to avoid such threats and dealing with system vulnerabilities is not sufficient; thus, ensuring a smooth policy implementation process supported by strong procedures is needed.

The security development process requires thorough understanding of a systems assets, followed by identifying different vulnerabilities and threats that can exist. It is necessary to identify what the system assets are and what

the assets should be protected against. In this paper, assets were defined as all valuable things in the system, tangible and intangible, which require protection. Some general, IoT assets include system hardware, software, data and information, as well as assets related to services, e.g. service reputation. It has been shown that it is crucial to comprehend the threats and system weaknesses in order to allocate better system mitigation. In addition, understanding potential attacks allows system developers to better determine where funds should be spent. Most commonly known threats have been described as DoS, physical attacks and attacks on privacy.

Three different types of intruders were discussed in this paper, namely individual attacks, organized groups, and intelligence agencies. Each attacker type has different skill levels, funding resources, motivation, and risk tolerance. It is very important to study the various types of attack actors and determine which are most likely to attack a system. Upon describing and documenting all threats and respective actors, it is easier to perceive which threat could exploit what weakness in the system. Generally, it is assumed that IoT intruder has full DY intruder capabilities in addition to some limited physical compromise power. We will presume that physical compromise attacks do not scale, and they will therefore only at-worst affect a limited population of the total number of IoT devices. IoT architecture must consequently be designed to cope with compromised devices and be competent in detecting such incidents. It is concluded that attackers employ various methods, tools, and techniques to exploit vulnerabilities in a system to achieve their goals or objectives. Understanding attackers motives and capabilities is important for an organization to prevent potential damage. To reduce both potential threats and their consequences, more research is needed to fill the gaps in knowledge regarding threats and cybercrime and provide the necessary steps to mitigate probable attacks.

5 Conclusions

IoT faces a number of threats that must be recognized for protective action to be taken. In this paper, security challenges and security threats to IoT were introduced. The overall goal was to identify assets and document potential threats, attacks and vulnerabilities faced by the IoT.

An overview of the most important IoT security problems was provided, with particular focus on security challenges surrounding IoT devices and services. Security challenges, such as confidentiality, privacy and entity trust were identified. We showed that in order to establish more secure and

readily available IoT devices and services, security and privacy challenges need to be addressed. The discussion also focused upon the cyber threats comprising actors, motivation, and capability fuelled by the unique characteristics of cyberspace. It was demonstrated that threats from intelligence agencies and criminal groups are likely to be more difficult to defeat than those from individual hackers. The reason is that their targets may be much less predictable while the impact of an individual attack is expected to be less severe.

It was concluded that much work remains to be done in the area of IoT security, by both vendors and end-users. It is important for upcoming standards to address the shortcomings of current IoT security mechanisms. As future work, the aim is to gain deeper understanding of the threats facing IoT infrastructure as well as identify the likelihood and consequences of threats against IoT. Definitions of suitable security mechanisms for access control, authentication, identity management, and a flexible trust management framework should be considered early in product development. We hope this survey will be useful to researchers in the security field by helping identify the major issues in IoT security and providing better understanding of the threats and their attributes originating from various intruders like organizations and intelligence agencies.

References

[1] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," *Computer networks*, vol. 54, no. 15, pp. 2787–2805, 2010.

[2] S. Andreev and Y. Koucheryavy, "Internet of things, smart spaces, and next generation networking," *Springer, LNCS*, vol. 7469, p. 464, 2012.

[3] J. S. Kumar and D. R. Patel, "A survey on internet of things: Security and privacy issues," *International Journal of Computer Applications*, vol. 90, no. 11, pp. 20–26, March 2014, published by Foundation of Computer Science, New York, USA.

[4] A. Stango, N. R. Prasad, and D. M. Kyriazanos, "A threat analysis methodology for security evaluation and enhancement planning," in *Emerging Security Information, Systems and Technologies, 2009. SECURWARE'09. Third International Conference on*. IEEE, 2009, pp. 262–267.

[5] D. Jiang and C. ShiWei, "A study of information security for m2m of iot," in *Advanced Computer Theory and Engineering (ICACTE), 2010 3rd International Conference on*, vol. 3. IEEE, 2010, pp. V3–576.

[6] B. Schneier, *Secrets and lies: digital security in a networked world*. John Wiley & Sons, 2011.
[7] J. M. Kizza, *Guide to Computer Network Security*. Springer, 2013.
[8] M. Taneja, "An analytics framework to detect compromised iot devices using mobility behavior," in *ICT Convergence (ICTC), 2013 International Conference on*. IEEE, 2013, pp. 38–43.
[9] G. M. Koien and V. A. Oleshchuk, *Aspects of Personal Privacy in Communications-Problems, Technology and Solutions*. River Publishers, 2013.
[10] N. R. Prasad, "Threat model framework and methodology for personal networks (pns)," in *Communication Systems Software and Middleware, 2007. COMSWARE 2007. 2nd International Conference on*. IEEE, 2007, pp. 1–6.
[11] O. Vermesan, P. Friess, P. Guillemin, S. Gusmeroli, H. Sundmaeker, A. Bassi, I. S. Jubert, M. Mazura, M. Harrison, M. Eisenhauer *et al.* "Internet of things strategic research roadmap," *Internet of Things-Global Technological and Societal Trends*, pp. 9–52, 2011.
[12] S. De, P. Barnaghi, M. Bauer, and S. Meissner, "Service modelling for the internet of things," in *Computer Science and Information Systems (FedCSIS), 2011 Federated Conference on*. IEEE, 2011, pp. 949–955.
[13] G. Xiao, J. Guo, L. Xu, and Z. Gong, "User interoperability with heterogeneous iot devices through transformation," 2014.
[14] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of things (iot): A vision, architectural elements, and future directions," *Future Generation Computer Systems*, vol. 29, no. 7, pp. 1645–1660, 2013.
[15] M. Zorzi, A. Gluhak, S. Lange, and A. Bassi, "From today's intranet of things to a future internet of things: a wireless-and mobility-related view," *Wireless Communications, IEEE*, vol. 17, no. 6, pp. 44–51, 2010.
[16] C. Hongsong, F. Zhongchuan, and Z. Dongyan, "Security and trust research in m2m system," in *Vehicular Electronics and Safety (ICVES), 2011 IEEE International Conference on*. IEEE, 2011, pp. 286–290.
[17] I. Cha, Y. Shah, A. U. Schmidt, A. Leicher, and M. V. Meyerstein, "Trust in m2m communication," *Vehicular Technology Magazine, IEEE*, vol. 4, no. 3, pp. 69–75, 2009.
[18] J. Lopez, R. Roman, and C. Alcaraz, "Analysis of security threats, requirements, technologies and standards in wireless sensor networks,"

in *Foundations of Security Analysis and Design V.* Springer, 2009, pp. 289–338.

[19] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," *Computer Networks*, vol. 57, no. 10, pp. 2266–2279, 2013.

[20] Y. Cheng, M. Naslund, G. Selander, and E. Fogelstrom, "Privacy in machine-to-machine communications a state-of-the-art survey," in *Communication Systems (ICCS), 2012 IEEE International Conference on*. IEEE, 2012, pp. 75–79.

[21] M. Rudner, "Cyber-threats to critical national infrastructure: An intelligence challenge," *International Journal of Intelligence and CounterIntelligence*, vol. 26, no. 3, pp. 453–481, 2013.

[22] R. Kozik and M. Choras, "Current cyber security threats and challenges in critical infrastructures protection," in *Informatics and Applications (ICIA), 2013 Second International Conference on*. IEEE, 2013, pp. 93–97.

[23] P. N. Mahalle, N. R. Prasad, and R. Prasad, "Object classification based context management for identity management in internet of things," *International Journal of Computer Applications*, vol. 63, no. 12, pp. 1–6, 2013.

[24] A. Gluhak, S. Krco, M. Nati, D. Pfisterer, N. Mitton, and T. Razafindralambo, "A survey on facilities for experimental internet of things research," *Communications Magazine, IEEE*, vol. 49, no. 11, pp. 58–67, 2011.

[25] Y. Benazzouz, C. Munilla, O. Gunalp, M. Gallissot, and L. Gurgen, "Sharing user iot devices in the cloud," in *Internet of Things (WF-IoT), 2014 IEEE World Forum on*. IEEE, 2014, pp. 373–374.

[26] G. M. Køien, "Reflections on trust in devices: an informal survey of human trust in an internet-of-things context," *Wireless Personal Communications*, vol. 61, no. 3, pp. 495–510, 2011.

[27] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of things: Vision, applications and research challenges," *Ad Hoc Networks*, vol. 10, no. 7, pp. 1497–1516, 2012.

[28] M. Thoma, S. Meyer, K. Sperner, S. Meissner, and T. Braun, "On iot-services: Survey, classification and enterprise integration," in *Green Computing and Communications (GreenCom), 2012 IEEE International Conference on*. IEEE, 2012, pp. 257–260.

[29] M. Abomhara and G. Koien, "Security and privacy in the internet of things: Current status and open issues," in *PRISMS 2014 The 2nd*

International Conference on Privacy and Security in Mobile Systems (PRISMS 2014), Aalborg, Denmark, May 2014.

[30] D. Watts, "Security and vulnerability in electric power systems," in *35th North American power symposium*, vol. 2, 2003, pp. 559–566.

[31] D. L. Pipkin, *Information security*. Prentice Hall PTR, 2000.

[32] E. Bertino, L. D. Martino, F. Paci, and A. C. Squicciarini, "Web services threats, vulnerabilities, and countermeasures," in *Security for Web Services and Service-Oriented Architectures*. Springer, 2010, pp. 25–44.

[33] D. G. Padmavathi, M. Shanmugapriya *et al.*, "A survey of attacks, security mechanisms and challenges in wireless sensor networks," *arXiv preprint arXiv:0909.0576*, 2009.

[34] H. G. Brauch, "Concepts of security threats, challenges, vulnerabilities and risks," in *Coping with Global Environmental Change, Disasters and Security*. Springer, 2011, pp. 61–106.

[35] K. Dahbur, B. Mohammad, and A. B. Tarakji, "A survey of risks, threats and vulnerabilities in cloud computing," in *Proceedings of the 2011 International conference on intelligent semantic Web-services and applications*. ACM, 2011, p. 12.

[36] R. K. Rainer and C. G. Cegielski, *Introduction to information systems: Enabling and transforming business*. John Wiley & Sons, 2010.

[37] A. J. Duncan, S. Creese, and M. Goldsmith, "Insider attacks in cloud computing," in *Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on*. IEEE, 2012, pp. 857–862.

[38] P. Baybutt, "Assessing risks from threats to process plants: Threat and vulnerability analysis," *Process Safety Progress*, vol. 21, no. 4, pp. 269–275, 2002.

[39] C. Tankard, "Advanced persistent threats and how to monitor and deter them," *Network security*, vol. 2011, no. 8, pp. 16–19, 2011.

[40] F. Li, A. Lai, and D. Ddl, "Evidence of advanced persistent threat: A case study of malware for political espionage," in *Malicious and Unwanted Software (MALWARE), 2011 6th International Conference on*. IEEE, 2011, pp. 102–109.

[41] S. Ansari, S. Rajeev, and H. Chandrashekar, "Packet sniffing: a brief introduction," *Potentials, IEEE*, vol. 21, no. 5, pp. 17–19, 2002.

[42] M. De Vivo, E. Carrasco, G. Isern, and G. O. de Vivo, "A review of port scanning techniques," *ACM SIGCOMM Computer Communication Review*, vol. 29, no. 2, pp. 41–48, 1999.

[43] I. Naumann and G. Hogben, "Privacy features of european eid card specifications," *Network Security*, vol. 2008, no. 8, pp. 9–13, 2008.
[44] C. Wilson, "Botnets, cybercrime, and cyberterrorism: Vulnerabilities and policy issues for congress." DTIC Document, 2008.
[45] A. Daneels and W. Salter, "What is scada," in *International Conference on Accelerator and Large Experimental Physics Control Systems*, 1999, pp. 339–343.
[46] A. Nicholson, S. Webber, S. Dyer, T. Patel, and H. Janicke, "Scada security in the light of cyber-warfare," *Computers & Security*, vol. 31, no. 4, pp. 418–436, 2012.
[47] V. M. Igure, S. A. Laughter, and R. D. Williams, "Security issues in scada networks," *Computers & Security*, vol. 25, no. 7, pp. 498–506, 2006.
[48] M. Kelleye, "Business Insider. The Stuxnet attack on Irans Nuclear Plant was Far more Dangerous Than Previously Thought," http://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11/,2013, [Online; accessed 03-Sep-2014].
[49] B. Jung, I. Han, and S. Lee, "Security threats to internet: a korean multi-industry investigation," *Information & Management*, vol. 38, no. 8, pp. 487–498, 2001.
[50] C. P. Mayer, "Security and privacy challenges in the internet of things," *Electronic Communications of the EASST*, vol. 17, 2009.
[51] A. R. Beresford, "Location privacy in ubiquitous computing," *Computer Laboratory, University of Cambridge, Tech. Rep*, vol. 612, 2005.
[52] S. Pramanik, "Threat motivation," in *Emerging Technologies for a Smarter World (CEWIT), 2013 10th International Conference and Expo on*. IEEE, 2013, pp. 1–5.
[53] D. Dolev and A. C. Yao, "On the security of public key protocols," *Information Theory, IEEE Transactions on*, vol. 29, no. 2, pp. 198–208, 1983.
[54] I. Cervesato, "The dolev-yao intruder is the most powerful attacker," in *16th Annual Symposium on Logic in Computer ScienceLICS*, vol. 1. Citeseer, 2001.
[55] J. Sheldon, "State of the art: Attackers and targets in cyberspace," *Journal of Military and Strategic Studies*, vol. 14, no. 2, 2012.
[56] E. M. Archer, "Crossing the rubicon: Understanding cyber terrorism in the european context," *The European Legacy*, no. ahead-of-print, pp. 1–16, 2014.

[57] A. K. Al-Rawi, "Cyber warriors in the middle east: The case of the syrian electronic army," *Public Relations Review*, 2014.
[58] D. Ball, "Chinas cyber warfare capabilities," *Security Challenges*, vol. 7, no. 2, pp. 81–103, 2011.

Biographies

M. Abomhara is currently pursuing his PhD at University of Agder, Norway. His research work is in the area of computer security, information security, information system management, cyber-security, and Internet of things. He received a Master of Computer Science (Data Communication and Computer Network) from University of Malaya, Malaysia in 2011. He also received a Master of Business Administration (MBA, Information technology management) from Multimedia University, Malaysia in 2013 and a Bachelor of Computer Science from 7th October University, Libya in 2006.

G. M. Køien is an associate professor in security and privacy in ICT at the University of Agder, Norge. He has previously worked for Ericsson Norway, System Sikkerhet AS and Telenor R & D. During his time with Telenor R & D he was the Telenor delegate to the SA3 (3GPP) work group on security. He received his PhD for Aalborg University, Denmark in 2008.