Threat-based Security Analysis for the Internet of Things

Ahmad W. Atamli
Department of Computer Science
University of Oxford
Oxford, UK
ahmad.atamli@cs.ox.ac.uk

Andrew Martin
Department of Computer Science
University of Oxford
Oxford, UK
andrew.martin@cs.ox.ac.uk

***Abstract*—The *Internet of Things* (IoT) is an emerging paradigm focusing on the inter-connection of things or devices to each other and to the users. This technology is anticipated to become an integral milestone in the development of smart homes and smart cities. For any technology to be successful and achieve widespread use, it needs to gain the trust of users by providing adequate security and privacy assurance. Despite the growing interest of the research community in IoT, and the emergence of several surveys and papers addressing its architecture and its elements, we are still lacking a thorough analysis of the security and privacy properties that are required for a system where the constituent devices vary in their capabilities. In this paper we provide a threat model based on use-cases of IoT, which can be used to determine where efforts should be invested in order to secure these systems. We conclude by recommending measures that will help in providing security and assuring privacy when using IoT.**

***Keywords*-Security; Internet of Things; Threats;**

I. Introduction

In the last few years the world has experienced rapid advancement in technology, the likes of which has had a significant impact on our daily lives. The rise of technologies - smartphones, tablets, laptops and PCs - has engendered an increase in interconnectedness through time and across the spatial dimension. Contemporary technology has moved beyond fostering only connections between humans, and now facilitates both the linkage of people to things and indeed, things to one another, to achieve a common goal; this being termed The *Internet of Things* (IoT). IoT is believed to be the next milestone in the technological evolution of the world, it having an expansion rate 270 percent higher than mobile devices in less than six years [1]. Based on this prediction, many governments and large corporations have earmarked substantial funding for research on IoT.

IoT is going to have a substantial role in shaping the future of smart cities. From the private user's perspective it manifests itself in the application of domestic tools at work; for example, systems such as the smart thermostat, smart car, and smart community. Moreover, with regard to the corporate environment, IoT will enable automation of work, the provision of smarter environments for employees, and the management of power consumption with the aim of reducing expenses [2]. IoT is able to achieve the aforementioned through utilisation of other technologies [3], [4] - for instance, sensors, Radio Frequency IDentifiers (RFIDs), actuators, and smart meters. These devices are linked together to create a new emergent behaviour where each *thing* contributes to achieving the desired functionality. A particularly salient example of such an application is a thermostat system that *senses* the temperature and adjusts itself by *learning* the behaviour patterns of its users [5].

The value of IoT could not possibly be overestimated, however it is obligatory that a thorough consideration be given to all aspects of security and privacy. Indeed, tackling such facts, whilst a challenge, is all the more imperative. As IoT, being the amalgam of a great many individual technologies, many of which may well have flaws with respect to security and privacy, could conceivably be instrumentalised in a sinister and far more threatening manner if there is a failure to afford sufficient attention to the subject matter of this paper.

The complex nature of security in IoT revolves around the fact that, while in itself connecting several technologies together is a great challenge, the system attempts to securely connect devices that are limited in computation, power, and storage. Some of the devices used by IoT can accommodate only very basic security mechanisms, the likes of which are incapable of maintaining the integrity and confidentiality of the users' data. Moreover, these devices - for instance, sensors, and RFIDs - lack a simple user interface, like an ON/OFF button or status indicator, thus presenting a visual psychological limitation for people when it comes to trusting these devices.

Nowadays, privacy concerns have become a hurdle; slowing the advancement of many technologies[6]. Furthermore, it has been shown that trust in a technology diminishes when the latter slanders or exposes the individual [7], [8], [9], and, recently, many technologies have failed to provide adequate security and privacy mechanisms, thereby causing pain and suffering to those afflicted [10]. In order to gain the trust of the public in the Internet of Things, we need to ensure the same failures with respect to privacy and security do not come to pass with this system, by ensuring the appropriate mechanisms to guarantee such things exist from the onset.

In this paper, we discuss the Internet of Things from

978-1-4799-7907-3/14 $31.00 © 2014 IEEE
DOI 10.1109/SIoT.2014.10

IEEE computer society

a use-cases perspective. The following section provides a general overview of the work done in the field; section 3 details several interesting scenarios which are relevant to today's world; section 4 discusses a threat model; section 5 provides a security analysis to the IoT devices based on these use-cases respectively; section 6 lists security and privacy properties desirable in IoT systems; whilst finally, in section 7 we give a glimpse of the future work we plan to do in this field. In particular, our main contributions are:

- Defining several use-cases for the Internet of Things.
- Establishing threat modelling as a method for analysing the use-cases defined.
- Formulating a set of desirable security and privacy properties for IoT.

II. Related Work

Due to the rising interest in the Internet of Things, there have been numerous publications on security and privacy in this context. There are currently a myriad of descriptions of IoT visions, applications, and enabling technologies [11], [12], [13], [14] that briefly address some security and privacy aspects. Atzori et al. [11] has discussed the importance of security in IoT context and focused on the security aspects of the elements. In this survey it was pointed out that due to the limitation of the devices composing the IoT, and the properties of the current communication protocols, it is very challenging to employ complex security mechanisms. Some devices might not be able to have access control for different users, support sufficient authentication schemes, or even use secure communication channels between devices. However, it is important to keep in mind that the required security measures are application dependent. For instance, in Near Field Communication (NFC), physical proximity is vital for establishing the connection, which makes this technology useful for various applications. Therefore, due to this property, some applications using NFC might not require a complex security scheme such as encrypted channel. For example, in some instances the users might not care about other people seeing the exchanged data in their presence. For instance, in a domestic use for IoT, in order to prevent children from watching TV without adult supervision, the user might not need complex communication protocols and it would suffice to only use access control mechanisms to access the device, or symmetric encryption rather than asymmetric for communication.

Due to its heterogeneous nature, the Internet of Things poses many security and privacy challenges[15]. Different research groups have adopted diverse directions for addressing these issues. Roman et al. [16] presented several technologies in IoT context, discussed current technologies and their feasibility for some IoT devices, and provided a set of security requirements for IoT devices. In a subsequent study, the same group [17] compared the centralised and distributed architecture of IoT and their implication on security aspects. Moreover, Kozlov et al. [18] discussed security and privacy threats in IoT architecture, using a systematic approach to analyse the threats at different levels of the architecture.

Threat models to IoT have been presented by Babar et al. [19], who gave a general threat model that is not IoT specific, however, can be reflected on it. Nonetheless, the field still lacks a clear reference to the actual threats encountered in IoT, and in what applications security is more crucial. Abie et al.[20] focused on a risk-based adaptive security in a Healthcare application by taking risk management approach that adopts game theory theme to develop an adaptive security decision-making model. Similarly, Gan et al. [21] focused on security analysis of the network points and suggested solutions to some problems.

Even though IoT has been out for many years, it did not get the sufficient attention it deserves. According to Whitmore et al.[22] not much work has been done on security and privacy in IoT context, and most research was focused on the devices as individual entities rather than being part of an IoT system. Despite the various attempts to deal with security and privacy issues in IoT, a holistic analysis and risk assessment is still lacking. Due to the incompleteness of the security and privacy requirements, IoT still needs to overcome this obstacle that may prevent it from becoming widely adopted.

We argue that in order to be able to understand the security and privacy risks behind IoT we should relate them to a specific application, as each scenario bares its own concerns, thus providing us with a clear definition of the threats behind each use-cases. In this paper we describe the vision of IoT by providing several use-cases, and use threat-based security analysis method to help us formulating the security and privacy recommendations to overcome some major challenges in IoT.

III. Internet of Things use-cases

In this section, we present three representative IoT use-cases that have a high likelihood of being integrated into our daily routines now and in the near future. We describe how IoT elements, such as sensors, actuator, RFIDs, Internet, Network, and Near Field Communication, can support different applications, and help increase IoT adoption. Analysing the functionality of IoT elements in different scenarios is a method that allows us to perform case-based security analysis, and formulate the security and privacy properties that will support the use of IoT by many users.

A. Power Management

One of the most prominent uses for an IoT based smart system is managing power consumption both in the private and industry sectors. In a world where the resources of energy are becoming scarce, it is essential to have such a smart system that will contribute to maintaining these resources.The strength of the power management system is in the ability to manage the execution of different devices while keeping power consumption within allowed boundaries. This can be done by using a smart meter[23] that supplies the system with real time data to enable scheduling the devices' operation. For example, the user can sync between two devices, when one device pauses the other resumes execution.

A system that employs a sensor and an actuator can save energy and manage power consumption by analysing environmental data it obtains using the sensor and responding according to a pre-determined power saving plan through the operation of the actuator. For example, in a smart house a domestic thermostat system is an essential component to set and control the temperature. It uses a *temperature sensor*, that can monitor the room's temperature with reliance to desired properties and send feedback to an actuator to initiate a change when it detects any divergence from these values. This would include setting the temperature to a certain range defined by the user. The thermostat would then adjust its activity to maintain the room temperature within the configured range. It can also turn off once an energy usage ceiling has been reached or can be turned on only when certain environmental conditions are present, e.g. indoor temperature.

The employment of a *network* further improves the control of the user and enables managing the thermostat remotely and thus preparing the room temperature for his arrival; by the time the user gets to the house the room is set to a convenient temperature. The system can benefit from a *location device* that is connected to the user's smartphone and can send signals to turn on/off the system according to the distance from the location device. Another device with even finer control is a *movement sensor* that identifies the movement and responds accordingly by turning off to improve power consumption when the user is not present in a certain room for a prolonged period of time. In a matter of days the system *learns* the user's habits and automates its usage, for example, when waking up in the morning it turns the system on and when going to bed it turns it off.

B. Smart Car

In an automated world, people will no longer need to sit behind a wheel and suffer from driving for hours, by the year 2020 it is believed that people will be able to enjoy a new technology of automatic-driver [24]. In the modern world, smartphones will be used as an access control to unlock the car[25], [26], replacing conventional keys, thus solving the scalability problem of having a key for each user. The *Near Field Communication* is a perfect candidate for this feature due to its short communication range that gives assurance of the user's physical presence.

Once an authorised user unlocks the car, it can surf the *Internet* in order to download road maps, connect to the city's infrastructure to get live updates on traffic, signals from traffic lights, and even report status to contribute to a bigger system like Vehicular Network [27]. The car will use this information in order to plan its route to arrive at the destination in the fastest and most economic way. By knowing the time of change in the traffic light, it can adjust its speed so that less fuel is being consumed, and report a more accurate time estimate for arrival.The car will also communicate with the surrounding cars in order to coordinate driving in the street. For example, when a car wants to pass another car it will communicate with its system and arrange the passing in a safe way.

In addition, the reported increase in unfortunate incidents where children were forgotten in cars; according to Safe Kids Worldwide: every 10 days a child dies from heatstroke in vehicles[28], thus encouraging the adoption of alert mechanisms such as a *movement sensors* to identify if a child or an animal was left in a locked car and report to the relevant parties. Finally, in order to make the travelling experience more convenient for the users, they can connect to TV channels at home and watch their favourite shows while travelling.

A smarter car can contribute to a more secure world; it can prevent unauthorised users from driving/using the car, hence, it can protect against theft. Only authorised users who belong to a ”white list” are allowed to drive a car. Similarly, it would prevent reckless teenagers without a driving license or elderly people from using the car causing damage and loss of lives.

The adoption of smart cars will pass several phases before making an appearance on the streets. A prototype of this system adopted in an airport context where vehicles move between unpopulated buildings will be greatly beneficial to automate the airport's functionality.

C. Smart Healthcare System

As life span increases and new chronic diseases develop, there is a need to provide medical attention to a growing population where certain patients require constant monitoring. However, the current facilities at hospitals and clinics are very limited and cannot accommodate many individuals. Therefore, it is essential to develop the capability to follow the health condition of patients either at home or in the hospital when applicable. This can be achieved by using *sensors* to monitor the patient's condition and send the report back through the *Internet* to a system that analyses the obtained data and alerts the suitable staff member, thus allowing the health care system to identify health issues earlier, and respond faster to emergencies. In recent years, similar remote treatments have been introduced in the form of devices like insulin pumps and heart-pace units that are attached to the patient, providing an automated and rapid response when needed.

In a smart hospital, *RFIDs* can be used to identify patients, items, and doctors easily and rapidly, e.g in a case when an anonymous person gets in an accident and it is critical to obtain the relevant medical records without any delay. It will also allow the staff to keep track of the doctors' location to allow for better response time during emergencies. Connecting RFID tags is not limited to people, one of the main issues in many hospitals these days is a loss of medications and unauthorised use of expensive medical instruments[29]. Hence, tracking things with RFIDs can reduce these losses and help to track them.

IV. Threat Model

A. Sources of Threats

After discussing the features of IoT and how can they be employed in several scenarios in a smart world, it is now feasible to identify the potential threats they are subject to in the context of the use-cases presented in the previous section. There are three main entities that pose risks to the security and privacy in IoT:

1) **Malicious User:** Is the owner of the IoT device with potential to perform attacks to learn the secrets of the manufacturer, and gain access to restricted functionality. By uncovering the flaws in the system the malicious user is able to obtain information, sell secrets to third parties, or even attack similar systems.

2) **Bad Manufacturer:** Is the producer of the device with the ability to exploit the technology to gain information about the users, or other IoT devices. Such a manufacturer can deliberately introduce security holes in its design to be exploited in the future for accessing the user's data and exposing it to third parties. Equally, the production of poorly secured goods results in compromising the users privacy. In addition, in IoT context where different objects connect to each other, a manufacturer can attack other competitors' devices to harm their reputation.

3) **External Adversary:** Is an outside entity that is not part of the system and has no authorised access to it. An adversary would try to gain information about the user of the system for malicious purposes such as causing financial damage and undermining the user's credibility. Also, causing malfunction to the system by manipulating the sensing data such as transmitting electromagnetic signals to inject fake data.

B. Classes of Attacks Vectors

Classifying the attacks on a system is essential for understanding the risks. We choose to address several categories to identify threats[30], [31]. These threats will be considered in more detail in the security analysis of the use-cases presented in section III.

1) **Device Tampering:** IoT devices are tiny devices integrated in other systems such as cars, light switches, TVs, ovens, and others. Some of the IoT devices spend most of the time unattended, thus, they can be easily stolen without being noticed. Once a device falls into the wrong hands, various sets of attacks can be performed such as secret stealing, software manipulation, and hardware tampering. It is important to mention that an adversary can tamper with the device and use it to insert impostor to the system, use the device maliciously or out of its intended functionality.

2) **Information Disclosure:** is the act of revealing information to an entity which does not have permission to see it. This includes accidental exposure, targeted attack, and inference or correlation. An attacker can obtain information by eavesdropping on the network channel, physical access to the device, or through accessing the device over the network.

3) **Privacy Breach:** unlike Information Disclosure, an adversary does not necessarily need to have access to confidential information to learn about the user. The adversary can infer private information from other sources such as meta data and traffic analysis.

4) **Denial-of-Service:** refers to the property of being inaccessible when requested by an authorised user. The system must have the ability to continue operating even when some undesired action is being performed by malicious users. This class of attacks can be performed by stealing the device, manipulating its software, or disrupting the communication channel.

5) **Spoofing:** refers to using credentials belonging to others in order to gain access to otherwise inaccessible service. The credentials can be obtained directly from a device, eavesdropping on the communication channel, or phishing.

6) **Elevation of Privilege:** is when an unprivileged user gains privileged access to a device/service. This

can be achieved by installing an impostor in the system that pretends to be another device, which has privileged access in the system.

7) **Signal Injection:** is when an attacker injects fake data to the system to change the sensed data, such as transmitting electromagnetic signals to a sensor.

8) **Side-Channel:** based on information such as timing analysis of the execution, power consumption, traffic analysis, fault analysis, and electromagnetic analysis of the device, private and confidential data can be inferred.

V. Attacks Impact

In order to make recommendations on how to secure IoT and to appreciate the severity of the threats it is subject to, it is not satisfactory to list the potential hazards without thorough consideration of their actual impact and likelihood, which will be context dependent. The majority of previous works focus only on the technical aspects of IoT devices and hardly give any attention to security in their application, we identified a gap in the literature which we try to fill through a different approach for analysing security and privacy requirements in IoT. In this section, we provide an attack analysis and address the security and privacy concerns for each device using the use-cases from section 3, giving a better overview of where more stringent security measures should be implemented.

A. Actuators

The actuator function in IoT context is equivalent to the write operation in PCs. In a world of things, an actuator can be operated by the user over the network, by receiving signals from other devices, or by being physically triggered by the user.

Security: An attack on this device can cause damage to the user in different domains. In the power management scenario, unauthorised triggering of the actuator can result in financial loss due to excessive power consumption. The damage can be even more severe in the smart car scenario where a malfunction in the breaks' actuator can result in loss of lives[32]. In the smart healthcare system, an actuator can be the trigger for injecting medication to a patient monitored at home, and any mistake or malfunction in this context can result in a wrong dosage of medication which can have fatal impact.

B. Sensors

The sensors collect data that is transferred to other components in the system to be analysed and result in a certain response or activity.

Security: The collected data can be a source of an attack[33], such as when data is fabricated due to a physical attack, resulting in an unexpected behaviour of other entities in the system. In the power management use-case, fake data from the sensors result in a different behaviour by the actuator, thus activating the thermostat at wrong time which will be manifested in financial loss to the user. However, in this system it is unlikely to learn substantial secrets about the user from the sensed data. In the healthcare system, fake data can result in wrong prognosis of the patient, administration of wrong medication that can result in allergic response or even life-risk[34], [35]. It could also send fake alerts and cause financial loss, for instance by sending a medical team to the wrong patient.

Privacy: The data collected from these devices can reveal information about the user's habits, even though it might not reveal secrets about the user. For instance, in the power management use-case the attacker can learn from basic analysis of the movement sensor data when the user leaves the house, goes to sleep, or wakes up in the morning. In the healthcare system, the signals from the sensors used to report the patient's conditions can reveal the medical function of the device, thus reveal private information about the holder.

C. RFID tags

The RFIDs involve the use of a reader device to identify a tag. These devices became popular due to their low cost, while maintaining the ability to track and identify objects. However, this technology raises many security and privacy concerns[36], [37].

Security: The limitation in hardware and power of these elements prevent the adoption of sufficient security mechanisms[38], [39]. For instance, holders of RFID tags must not be identified by an attacker with a tag reader, thus, scanty access control mechanisms might lead to information disclosure[37]. In the smart car example, an attacker within a close range of the user might be able to intercept the signals when accessing the vehicle, in which some of these signals can be the credentials of the user. An attacker can use these credentials to steal a car.

Privacy: A main feature of RFIDs is the ability to track. Therefore, this can pose a huge privacy concern, when it is exploited maliciously [40]. In the Health care scenario, privacy is the main concern for employees when using this technology, since they can be tracked constantly. Also, an attacker can learn about the health condition of patients by standing close and intercepting the signals from the RFID tags[20] that are used to monitor them.

D. Network,NFC and the Internet

IoT devices communicate with each other via a network connection. The communication protocols vary according to their function, thus vary in their security and privacy levels. Here we briefly mention the security and privacy behind the communication, and leave more detailed analysis of communication protocols for future work.

Security: Due to the heterogeneous environment of IoT, different communication protocols are adopted with different security levels[41]. It is most likely that IoT devices will communicate with each other via wireless channels, that will increase the system's vulnerability to eavesdropping and mask attacks[42]. An attacker can exploit the communication channel to gather information about the user such as location, credentials, and operation. A typical attack in the Smart car use case can be performed when one car tries to negotiate passing another car with the surroundings, however, receives erroneous information that can lead to chaos, accidents and loss of life. Also, an adversary can modify signals transmitted from devices to cause an unexpected or opposite response of other devices in the system, such as turning on a device instead of turning it off.

Privacy: The network is the main means of communication between IoT devices, thus posing critical point for information disclosure. For instance, when a smart car accesses a local node to download maps or updated traffic information, an attacker can learn about the destination of the driver. Furthermore, since automobiles can easily access the wide network, and have many elements such as stereo, microphone, and connection to the Internet. Bad manufacturers can use their technology to learn things about the users.

VI. Desirable Security and Privacy Properties

In this section, we integrate the hazards and security analysis from previous sections in order to formulate the security and privacy properties for an IoT system. Including the following properties when developing a framework for IoT is essential to furnish a reliable, appealing, and secure system to many users.

A. Security Properties

The ultimate goal is to keep the confidentiality and integrity of the system. For each breach point a different measure should be applied, we link between the security properties to the attacks vectors in section IV-B [IV.B.*].

Actuators, Sensors, and RFIDs

SP1: The device should be *tamper resistant* against unauthorised re-programing and passive secret stealing. The device must maintain its security properties, this includes keeping the integrity and confidentiality of the user's data and the device[IV.B.2][IV.B.4] when a physical attack[IV.B.1] is launched, and prevent denial of service[IV.B.4]. However, it should be possible for the user to update the firmware on the device.
SP2: The IoT device must have a *protected storage* by keeping the data encrypted to keep the confidentiality of the user information on the device[IV.B.2][IV.B.8], e.g. using security features of the hardware such as ARM TrustZone [43].
SP3: An *access control* mechanisms is needed in each device in order to prevent unauthorised access from compromising the entire system. The adoption of complex access control mechanisms is harder in some of the IoT devices such as sensors and actuator due to the limited storage. However, in some applications access control is a must since compromising one device can compromise the entire system, leading to information disclosure[IV.B.5], stealing credentials[IV.B.2][IV.B.8], and denial of service[IV.B.4].

Internet,Network, and NFC

SP4: The *data exchanged* between the user and the IoT should be secured to keep the integrity and confidentiality of the user [IV.B.2]. If the integrity of the data is compromised, the system's normal operation is interrupted and can result in both financial and personal damage to the user.
SP5: *Identification and authorisation* mechanisms should be employed. Only authorised entities can access the IoT device with different permissions to read and write [IV.B.4]. The IoT device needs to identify the devices in the system and be able to identify any impostors[IV.B.6].

Actuators, Sensors, RFIDs, Network

SP6: The system must be *available* within normal parameters and adapt when some undesired action is performed by a malicious user such as physical damage to a device[IV.B.4], also the damage reflected from the adversary must have minimal impact on the system.

B. Privacy Properties

The privacy properties counter the privacy breaches from section IV-B, where a malicious entity can learn personal information about the user.
PP1: The data exchanged between a user and the IoT devices should be protected so that an attacker eavesdropping on the communication can't infer information about the user.

An attacker shouldn't be able to infer the time when the user is present or absent, the user's identity or any other sensitive information.

PP2: The messages exchanged between IoT devices must not reveal Personal Information Identity (PII) of the user.

PP3: Signals from a device must be sent in a privacy preserving manner so as not to reveal the device's function since this can reveal information about the user.

PP4: The IoT devices should keep a record of personal user information only when absolutely necessary, and in such a case it should be for a limited time only.

PP5: Only data that doesn't reveal the personal information of the user can be collected such as aggregated data, e.g keeping a record of the number of people in a building, but not data relating to their identity like name, ID, and visual image.

PP6: The user should be made aware what and when data is being captured.

PP7: The user must be able to securely erase all private data from a device, e.g. if the device is to be resold.

VII. Future work

Security should not be redesigned for every system, we would like to identify groups of use-cases and requirement frameworks that will lead to architecture, middleware, and libraries. In our future work we aim to build on the security analysis we have performed here and on the features of the different devices in an IoT system in order to develop a security package that can be used by designers for any use-case. The objective of developing this package is to offer the users a generalised and complete package that includes a variety of security mechanisms suitable for different devices and different security levels. The designers will then be able to make their personalised combinations of these measures according to the desired application and can even assess the risk level in their design.

As we have discussed earlier, the IoT system encompasses devices with distinct features and limitations. Small devices such as RFIDs, sensors, and embedded devices, suffer from limitations in storage, power, and computation logic. On the other hand, powerful devices like laptops, PCs, and servers are less limited in the applicability of complex security measures. Our package will include the minimal set of functionalities to ensure the basic security mechanism compatible with the limited devices as well as much more sophisticated ones to be employed with the most powerful ones. In addition, intermediate mechanisms can be included to be used at the expense of increasing the costs or power requirement when high level security is required from the more limited devices. It is not a trivial question as to whether such a package is feasible and we aim to explore this further in the near future, where it will be interesting to investigate whether we will need to include a huge leap in the mechanisms employed in order to cover the full range of devices at a variety of security levels.

A. *Preliminary Risk Assessment*

The risk assessment is what will most likely determine the security level for many systems. We provide a preliminary risk assessment for each one of the use-cases from section 3, based on the attack analysis presented in the previous sections. The risk assessment takes into account the severity of the attack as well as the likeliness of its occurrence. We have divided it into three categories from low to high risk. We appreciate that there are other factors such as "who" is the attacker that affect these number. Table 1 summarises the different risk levels for each threat in the context of the use-cases. These are directly deduced from analysing the security properties of the devices. Here we assume a benign user and limit this preliminary investigation to be based on external adversary only. Based on the risk assessment, different security mechanisms should be adopted using a scenario based approach. The risk assessment will play a critical role in designing IoT systems, however, more extensive study is needed and will be covered in subsequent work.

Attacks Vector	Power Management	Smart Car	Healthcare
Physical Threat	1	2	3
Information Disclosure	2	3	2
Denial-of-Service	1	3	2
Spoofing	1	2	2
Elevation of Privilege	1	2	3

Table I: Risk Assessment
3 - High Risk, 2 - Medium Risk, 1 - Low Risk

VIII. Conclusion

The Internet of things has finally stepped out of its infancy and is gaining more attention from researchers and industrial communities. In this paper, we discuss a vision for the Internet of Things and relate it to previous work on security and privacy in IoT context. In particular, we present the different approaches that have been taken by many researchers when addressing security and privacy. While many researchers focused on the security and privacy of the devices constituting IoT, few papers addressed threat models, security, and privacy analysis of the system as a whole. In our paper, we adopted a threat analysis based approach to present a threat model as a method to analyse the impact of threats in different applications. From the threat model we deduced the security and privacy properties. This assessment will guide future work as to where more substantial efforts should be invested in developing security mechanisms for IoT.

IX. Acknowledgement

The authors would like to thank David Rogers and Andrew Paverd for the discussions and fruitful comments on this manuscript.

References

[1] Y. Montcheuil, “How to make the most of the Internet of Things,” *http://www.itproportal.com/2014/04/25/how-to-make-the-most-of-the-internet-of-things/*.

[2] C. Buckl, S. Sommer, A. Scholz, A. Knoll, A. Kemper, J. Heuer, and A. Schmitt, “Services to the Field: An Approach for Resource Constrained Sensor/Actor Networks,” in *2009 International Conference on Advanced Information Networking and Applications Workshops*. IEEE, May 2009, pp. 476–481.

[3] G. Kortuem, F. Kawsar, D. Fitton, and V. Sundramoorthy, “Smart objects as building blocks for the Internet of things,” *IEEE Internet Computing*, vol. 14, no. 1, pp. 44–51, Jan. 2010.

[4] A. Serbanati, C. M. Medaglia, and U. B. Ceipidor, “Building blocks of the internet of things: State of the art and beyond,” *Deploying RFID-Challenges, Solutions, and Open Issues, C. Turcu, Ed., InTech*, 2011.

[5] Nest labs, “Nest, Smart thermostat system,” 2014.

[6] H. Xu, T. Dinev, J. Smith, and P. Hart, “Information privacy concerns: linking individual perceptions with institutional privacy assurances,” in *Journal of the Association for Information Systems*. Citeseer, 2011.

[7] University of Oxford, “How internet affects young people at risk of self-harm, suicide – ScienceDaily.”

[8] A. Hawks, “Leaked cell phone photos Archives - starcasm.net.”

[9] J. Best, “Man HACKS into 10-month-old’s baby monitor and shouts at sleeping infant - Mirror Online.”

[10] S. Hinduja and J. Patchin, “Bullying, cyberbullying, and suicide,” *Archives of Suicide Research*, 2010.

[11] L. Atzori, A. Iera, and G. Morabito, “The internet of things: A survey,” *Computer networks*, 2010.

[12] Cisco, “CISCO: The Internet of Things: How the next Evolution of the Internet is changing everything from http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf,” Tech. Rep.

[13] 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, Sep. 2012.

[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] R. H. Weber, “Internet of Things New security and privacy challenges,” *Computer Law & Security Review*, vol. 26, no. 1, pp. 23–30, Jan. 2010.

[16] R. Roman, P. Najera, and J. Lopez, “Securing the Internet of Things,” *Computer*, vol. 44, no. 9, pp. 51–58, Sep. 2011.

[17] 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, Jul. 2013.

[18] D. Kozlov, J. Veijalainen, and Y. Ali, “Security and privacy threats in iot architectures,” in *Proceedings of the 7th International Conference on Body Area Networks*, ser. BodyNets ’12. ICST, Brussels, Belgium, Belgium: ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2012, pp. 256–262.

[19] N. Meghanathan, S. Boumerdassi, N. Chaki, and D. Nagamalai, Eds., *Recent Trends in Network Security and Applications*, ser. Communications in Computer and Information Science. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, vol. 89.

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

[21] G. Gan, Z. Lu, and J. Jiang, “Internet of Things Security Analysis,” in *2011 International Conference on Internet Technology and Applications*. IEEE, Aug. 2011, pp. 1–4.

[22] A. Whitmore, A. Agarwal, and L. Xu, “The Internet of ThingsA survey of topics and trends,” *Information Systems Frontiers*, Mar. 2014.

[23] M. Venables, “Smart meters make smart consumers,” *Engineering & Technology*, vol. 2, no. 4, pp. 23–23, Apr. 2007.

[24] S. Rosenblatt, “Google’s self-driving car turns out to be a very smart ride,” 2014.

[25] S. Clark, “Orange and Valeo demonstrate NFC car key concept,” 2010.

[26] Telekom, “Intelligent car key in a cell phone.”

[27] H. Moustafa and Y. Zhang, *Vehicular Networks: Techniques, Standards, and Applications*, 1st ed. Boston, MA, USA: Auerbach Publications, 2009.

[28] J. Null, “Fact Sheet - Heatstroke Deaths of Children in Vehicles.”

[29] Arup Laboratories, “Using RFID to track Equipment and Patients,” 2011.

[30] S. Myagmar, A. J. Lee, and W. Yurcik, “Threat modeling as a basis for security requirements,” in *Symposium on requirements engineering for information security (SREIS)*, vol. 2005, 2005, pp. 1–8.

[31] S. Babar, A. Stango, N. Prasad, J. Sen, and R. Prasad, "Proposed embedded security framework for internet of things (iot)," in *Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE), 2011 2nd International Conference on*. IEEE, 2011, pp. 1–5.

[32] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, and S. Savage, "Experimental Security Analysis of a Modern Automobile," in *2010 IEEE Symposium on Security and Privacy*. IEEE, 2010, pp. 447–462.

[33] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," in *Proceedings of the 9th ACM conference on Computer and communications security - CCS '02*. New York, New York, USA: ACM Press, Nov. 2002, p. 41.

[34] A. Parmar, "Hacker shows off vulnerabilities of wireless insulin pumps."

[35] W. Alexander, "Barnaby Jack Could Hack Your Pacemaker and Make Your Heart Explode — VICE Canada."

[36] D. Molnar and D. Wagner, "Privacy and security in library RFID: issues, practices, and architectures," *. . . on Computer and communications security*, 2004.

[37] M. O. Lehtonen, F. Michahelles, and E. Fleisch, "Trust and Security in RFID-Based Product Authentication Systems," *IEEE Systems Journal*, vol. 1, no. 2, pp. 129–144, Dec. 2007.

[38] S. A. Weis, S. E. Sarma, R. L. Rivest, and D. W. Engels, "Security and privacy aspects of low-cost radio frequency identification systems," in *Security in pervasive computing*. Springer, 2004, pp. 201–212.

[39] P. Rotter, "A Framework for Assessing RFID System Security and Privacy Risks," *IEEE Pervasive Computing*, vol. 7, no. 2, pp. 70–77, Apr. 2008.

[40] I. Gudymenko, K. Borcea-Pfitzmann, and K. Tietze, "Privacy implications of the internet of things," in *Constructing Ambient Intelligence*. Springer, 2012, pp. 280–286.

[41] W. Hu, H. Tan, P. Corke, W. C. Shih, and S. Jha, "Toward trusted wireless sensor networks," *ACM Transactions on Sensor Networks*, vol. 7, no. 1, pp. 1–25, Aug. 2010.

[42] I. Cha, Y. Shah, A. Schmidt, A. Leicher, and M. Meyerstein, "Trust in M2M communication," *IEEE Vehicular Technology Magazine*, vol. 4, no. 3, pp. 69–75, Sep. 2009.

[43] C. Namiluko, A. J. Paverd, and T. De Souza, "Towards Enhancing Web Application Security Using Trusted Execution," in *Workshop on Web Applications and Secure Hardware - WASH'13*, 2013.