2015 IEEE World Congress on Services

Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things

Md. Mahmud Hossain, Maziar Fotouhi, and Ragib Hasan
{mahmud, maziar, ragib}@cis.uab.edu
Department of Computer and Information Sciences
University of Alabama at Birmingham
Birmingham, AL 35294-1170

***Abstract*—The Internet of Things (IoT) devices have become popular in diverse domains such as e-Health, e-Home, e-Commerce, and e-Trafficking, etc. With increased deployment of IoT devices in the real world, they can be, and in some cases, already are subject to malicious attacks to compromise the security and privacy of the IoT devices. While a number of researchers have explored such security challenges and open problems in IoT, there is an unfortunate lack of a systematic study of the security challenges in the IoT landscape. In this paper, we aim at bridging this gap by conducting a thorough analysis of IoT security challenges and problems. We present a detailed analysis of IoT attack surfaces, threat models, security issues, requirements, forensics, and challenges. We also provide a set of open problems in IoT security and privacy to guide the attention of researchers into solving the most critical problems.**

***Keywords*-Internet of Things; Security Requirements; Security Challenges; Attack Surfaces; Threat Model; Attack Taxonomy; IoT Forensics;**

I. Introduction

The Internet of Things (IoT) paradigm has gained popularity in recent years. At a conceptual level, IoT refers to the inter connectivity among our everyday devices, along with device autonomy, sensing capability, and contextual awareness. IoT devices include personal computers, laptops, tablets, smart phones, PDAs, and other hand-held embedded devices. Devices now communicate smartly to each other or to us. Connected devices equipped with sensors and/or actuators perceive their surroundings, understand what is going on and perform accordingly [1] [2]. This is achieved by processing the sensed data at a node, device hub, or in a cloud. Devices are also enabled to take decisions autonomously or may propagate information to users, so that users can make the best decisions [2].

The interconnected device networks can lead to a large number of intelligent and autonomous applications and services that can bring significant personal, professional, and economic benefits [3], resulting in the emergence of more more data-centric businesses. IoT devices have to make their data accessible to interested parties, which can be web services, smart phone, cloud resource, etc. Making these data available through the Internet is one thing, doing this in a controlled way, not exposing data to the whole world, is another thing. Therefore, the more objects get linked via the Internet of Things, the greater becomes the possibility of digital mischief or mayhem.

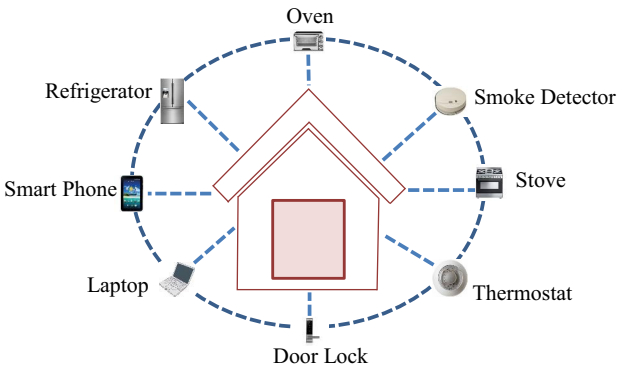

Fig. 1: Smart-Home with inter-linked Things

We present a scenario in which we show that, a single compromised smart object among a set of interconnected network objects is sometimes able to provide unauthorized access to other smart objects. Let us consider a smart home (see Figure 1), where the refrigerator is linked to the oven, the oven is linked to the stove, and so on. Here, the attacker can use the compromised refrigerator and eventually get access to the home door lock. The same is true and even more severe for e-health Internet of Things applications, services, and devices. For instance, using a compromised smart pacemaker, an adversary may send its user into cardiac arrest.

The world of IoT includes a wide variety of devices and diverse applications which call for different deployment scenarios and requirements. Most of these devices and applications are not primarily designed with security and/or privacy issues in mind. Therefore, new security and privacy problems arise, e.g., secrecy, confidentiality, data integrity, authentication, access control, etc. We must examine the security implications of IoT devices carefully and include such considerations into the design of IoT devices, systems, and protocols.

A. Contributions

In this article, we present an overview of Internet of Things architecture and interconnected networks' interoperability. We also illustrate a systematic analysis of the critical security problems and mitigation strategies. The contributions of this paper are as follows:

978-1-4673-7275-6/15 $31.00 © 2015 IEEE
DOI 10.1109/SERVICES.2015.12

1) We analyze the security aspects of the Internet of Things with a three dimensional framework to indicate the intricacy of IoT security domain.
2) We provide a systematic summary of the IoT security requirements and challenges
3) We identify attack surfaces, threats, and tentative measures towards securing IoT devices.
4) Finally, we enumerate research issues and provide directions for each of them.

B. Organization

The rest of the paper is organized as follows: Section II describes the motivation for secure Internet of Things. The interoperability among various IoT components (smart devices, gateway, service provider, etc.) is presented in section III. Requirements and challenges towards secure IoT are detailed in section IV. Security landscape, attack surfaces, and its vulnerability are discussed in section V. The analysis of threat model with different security risks and attacks are identified in section VI. The top-notch security research issues are enumerated in section VII. Finally, we conclude in Section VIII.

II. Motivation

To understand the importance of exploring security and privacy issues in the domain of IoT, we first take a look at the existing state of the IoT device deployments in the world. A 2014 study by Hewlett-Packard [4] on commercialized IoT deployments found that 80% of such devices violate privacy of personal information (e.g., name, date-of-birth, etc.), 80% failed to require passwords of sufficient complexity and length, 70% did not encrypt communications, and 60% had security vulnerabilities in their user interfaces.

Attacks on IoT devices are simple and easy to conduct. There are several cases where researchers showed the successful take-over of smart things [5], [6], [7]. The common attack strategy is to compromise one device in the IoT network and perform fraudulent acts towards another connected object, impersonating the real one.

Attackers have used household "smart" appliances to launch an IoT based cyberattack, where everyday consumer gadgets such as home-networking routers, connected multi-media centers, televisions, and refrigerators had been compromised and used as a platform to send thousand of phishing and spam emails [5]. Silvio et al. [8] showed that an adversary can compromise a home alarm system by eavesdropping on the RF signal used for enabling and disabling the alarm system. Researchers from IOActive Labs showed attack on traffic control systems. Magnetic sensors use in the streets (to collect and disseminate data) are compromised using professional transmitters or antennas from a couple of miles away, as there are few security protocols in place [6] . Oren et al. [7] have found in their research that a smart TV could be compromised using a cheap antenna and through broadcasting messages, as it relies on an insecure Hybrid Broadcast-Broadband Television Standard (HbbTV).

We argue that the above incidents coupled with the insecure deployments of IoT device systems show a significant threat to the success of the emerging IoT ecosystem. Therefore, it is important to examine and understand the critical security issues in IoT. In this paper, we take the first step towards motivating and educating researchers about the various security threats.

III. Background

To understand IoT security issues, we first need to examine the components of the IoT information network (native network and global network) and the interoperability among them [9], [10]. The IoT ecosystem has five major components: IoT devices, Coordinator, Sensor Bridge, IoT services, and Controller. Figure 2 presents an overview of the inter component operational model of the IoT ecosystem. The properties and functions of these components are described as follows .

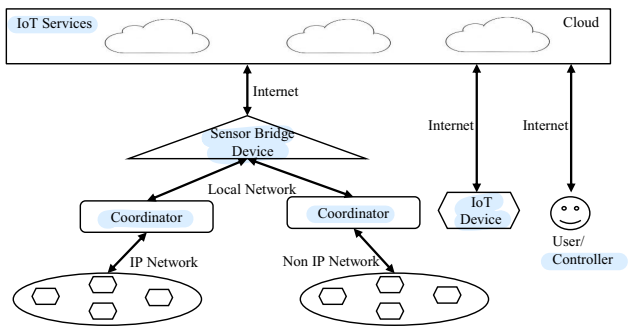

Fig. 2: IoT Device Interoperability

IoT device. An IoT device consists of sensors, actuators, communication interface, operating systems, system software, preloaded applications and lightweight services. The main responsibility of a smart thing is to collect contextual information using sensors and to perform actions using actuators. For example, a smart thermostat perceives room temperature and humidity, and adjusts the air conditioner's temperate accordingly.

Coordinator. A coordinator device acts as a device manager. One or more smart things operate under a single coordinator. The primary responsibility of a coordinator is to monitor health and activities of the smart things. It also sends an aggregated report of their actions and events to the IoT service provider. Let us consider a smart home, where a motion sensor camera and a smart door lock operate under the same coordinator. Whenever the motion sensor camera detects human activities, it sends lock/unlock command to smart door lock. First, the smart camera sends the perceived information along with the appropriate command (lock/ unlock) to its coordinator. Next, the Coordinator forwards the command to the smart door lock. Later, the coordinator prepares a report aggregating the information about this event and sends to the IoT service provider.

Sensor bridge. It is also termed as a multi-protocol device/IoT gateway. It acts as a hub between the local IoT network and IoT cloud services. Sensor bridge also performs as a connector between uneven local IoT networks. For instance, a Sensor

Bridge device enables ZigBee IoT devices to talk with Z-Wave IoT devices.

IoT services. Usually, IoT services are hosted on cloud so that users can access IoT objects anytime, anywhere. The responsibilities of these services include IoT process automation, device management, decision making, etc.

Controllers. IoT devices are controlled using the controllers (e.g. Smart phone, Tablet). For example, an user might use his mobile phone to issue commands to smart home appliances either from home or remotely.

IV. Security Constraints and Requirements

A. *Security Constraints*

IoT devices are inherently resource-constrained. Therefore, employing the conventional security mechanisms directly in the smart things is not straightforward. The major security constraints of IoT devices are as follows:

Limitations based on hardware.

1) **Computational and energy constraint:** Most of the time, IoT devices are battery driven and devices are using low-power CPUs having low clock rate. Therefore, computationally expensive cryptographic algorithms – algorithms that require fast computation – cannot be ported directly to such low powered devices
2) **Memory constraint:** IoT devices are built with limited RAM and Flash memory compared to the traditional digital system (e.g. PC, Laptop, etc.), and use Real Time Operating System (RTOS) or lightweight version of General Purpose Operating System (GPOS). They also run system software and proprietary services. Therefore, security schemes should be memory efficient. However, traditional security algorithms are not designed specifically considering the memory efficiency, because the traditional digital system uses spacious RAM and hard drive. Those security schemes might not get enough space in memory after booting up the operating system and system software. Therefore, conventional security algorithms cannot be used directly for securing IoT devices.
3) **Tamper resistant packaging:** IoT devices might be deployed in the remote regions and are left unattended. An attacker might tamper with the IoT devices by device capture. Later, they can extract the cryptographic secrets, modify programs, or replace them with malicious nodes. Tamper resistant packaging is one way to defend against these attacks.

Limitations based on software.

1) **Embedded software constraint:** IoT operating systems, which are embedded with the IoT devices, have thin network protocol stacks and might lack enough security modules. Therefore, the security module designed for the protocol stack should be thin, but robust and fault tolerant.
2) **Dynamic security patch:** Installing a dynamic security patch on the IoT devices and mitigating the potential vulnerabilities is not a straightforward task. Remote reprogramming might not be possible for the IoT devices, as the operating system or protocol stack might not have the ability receiving and integrating new code or library.

Limitations based on network.

1) **Mobility:** Mobility is one of the prominent attributes of the IoT devices, where the devices join a proximal network without prior configuration. This mobility nature raises the need to develop mobility resilient security algorithms for the IoT devices.
2) **Scalability:** The number of IoT devices is growing everyday and more devices are getting connected with the global information network. Current security schemes lack of the scalability property; therefore, such schemes are not suitable for IoT devices.
3) **Multiplicity of devices:** Diversity of the IoT devices within the IoT network ranges from the full fledged PCs to low-end RFID tags. Therefore, it is hard to find a single security scheme that accommodate even the simplest of devices.
4) **Multiplicity of communication medium:** IoT devices connect to the local and public network via a wide range of wireless links. Therefore, it is difficult to find a comprehensive security protocol considering both the wired and wireless medium properties.
5) **Multi-Protocol Networking:** IoT devices might use a proprietary network protocol (e.g., non IP protocol) for communication in proximal networks. At the same time, it might communicate with an IoT service provider over the IP networking. These multi protocol communication characteristics make traditional security schemes unsuitable for IoT devices.
6) **Dynamic network topology:** An IoT devices might join or leave a network at anytime from anywhere. The temporal and spatial device adding and exiting characteristic make a network topology dynamic. Existing security model for the digital systems does not cope with this types of sudden network topological changes. Hence, such a model does not fit with the smart devices security.

B. *Security Requirements*

There are several factors which need to be taken care of while devising a security solution for the IoT devices. The Security requirements that are expected to be met by the IoT security schemes are as follows.

Information security requirements.

1) **Integrity:** An adversary can change the data and compromise the integrity of an IoT system. Thus, integrity ensures that any received data has not been altered in transit.
2) **Information protection:** The Secrecy and confidentiality of the on-air and stored information should be strictly preserved. It refers to limiting the information access and disclosure to the authorized IoT node, and preventing access by or disclosure to unauthorized ones. For instance, an IoT network should not reveal the sensor readings to its neighbours (if it is configured not to do so).
3) **Anonymity:** Anonymity hides the source of the data. This security service helps with the data confidentiality and privacy.

4) **Non-repudiation:** Non repudiation is the assurance that someone cannot deny something. An IoT node cannot deny sending a message it has previously sent.
5) **Freshness:** It is required to ensure the freshness of each message. Freshness guarantees that the data is very much recent and no old messages have been replayed.

Access level security requirements.

1) **Authentication:** Authentication enables an IoT device to ensure the identity of the peer with which it communicates (e.g. receiver verifies whether received data originated from the correct source or not). It also requires to ensure that valid users get access to the IoT devices and networks for administrative tasks: remote reprogramming or controlling of the IoT devices and networks.
2) **Authorization**: It ensures that only the authorized devices and the users get access to the network services or resources.
3) **Access control:** Access control is the act of ensuring that an authenticated IoT node accesses only what it is authorized to, and nothing else.

Functional security requirements.

1) **Exception handling:** Exception handling confirms that an IoT network is alive and continues serving even in the anomalous situations: node compromise, node destruction, malfunctioning hardware, software glitches, dislocation environmental hazards, etc. Thus it assures robustness.
2) **Availability:** Availability ensures the survivability of IoT services to authorized parties when needed despite denial-of-service attacks. It also ensures that it has the capability to provide a minimum level of services in the presence of power loss, failures.
3) **Resiliency**: In case a few inter connected IoT devices are compromised, a security scheme should still protect against the attack.
4) **Self organization:** An IoT device may fail or run out of energy. The remaining device or collaborator devices should have the ability to be reorganized to maintain a set level of security.

V. Security Vulnerability

A. Security Landscape

Billions of smart things perform heterogeneous responsibilities residing in the heterogeneous networks and communicate with each other through heterogeneous communication protocols. For example, devices for the smart home solutions might be using one network protocol for home network communication (device-to-gateway) and another for public network communication (gateway-to-cloud). In addition, a lightweight cryptography might be used because of their low computational capabilities. Therefore, finding a right combination of security schemes for them is much more difficult comparing to the typical digital systems. Parameters that make the security task complex could be plotted in a 3-D framework (see Figure 3). The security complexity varies with the variation of any parameters in any dimension. For this reason, it is required to consider device specification, networking, and application objective, while dealing with the IoT security issues and countermeasures.

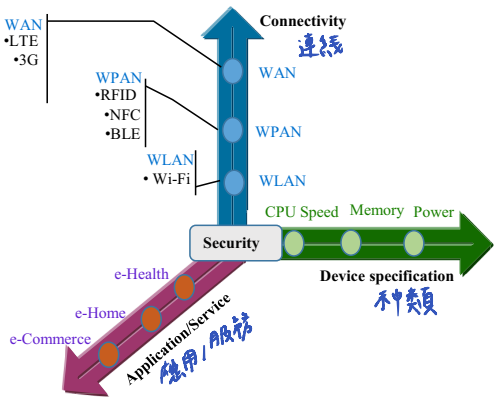

Fig. 3: Security Landscape

B. Attack Surfaces

The attack surface increases in many folds in IoT. The increased population (number of IoT devices), complexity, heterogeneity, interoperability, mobility, and distribution of entities (smart objects, controller, user, and services) expand the attack surfaces in the interconnected things' networks [11]. This expansion also contributes to the expansion of new security issues. We consider two branches of the IoT network. One is proximal networks (local, private, or home network) where the entities are IoT controller, IoT gateway, IoT coordinator, and smart objects. Another one is public networks which consist of IoT controller, IoT services, IoT gateway, and Cloud. A subset of these attack surfaces are inherited from the cloud computing paradigm [12] because of the IoT cloud services. We present the attack surfaces in Figure 4 and identify the potential vulnerabilities associated with these attack in the following section.

Network	Attack Surface
Local Network	*Device* ⇔ *Device* . e.g. Communication between TV and Refrigerator.
	Device ⇔ *Coordinator* e.g. Interface between Thermostat and Sensor hub.
	Coordinator ⇔ *Gateway.* e.g. Medium between Sensor hub & Sensor gateway
	Device ⇔ *Controller* e.g. Interface between Smart TV and Smart Phone
Public Network	*Controller* ⇔ *IoT Service Provider* e.g. Smart phone to control home devices remotely.
	Service ⇔ *Service* e.g. Medical IoT service consumes Payment service

Fig. 4: Internet of Things Attack Surface

C. Surface Associated Vulnerabilities

The *Open web application security project for IoT* identifies ten critical security vulnerabilities in the Internet of Things

[13]. Later, HP [4] found 50% of the commercialized IoT suffers from critical security weakness. We present some of the prominent aspects of security here [14].

◎ **End device security:** We consider three aspects of security vulnerability associated with the end-devices.

1) **Insecurity due to device category and capability**: The IoT devices equipped with sensors will act as collectors and the ones embedded with actuators will act as performers. Device having both the sensors and actuator will perceive and perform. In addition, device can also be formed with hybrid configuration of collector, performer, and controller. This multifaceted responsibilities make the IoT devices susceptible to identity theft security risks. Therefore, it becomes easy for the malicious entities pretending to be an innocent and justified end-device.
2) **Software and firmware security:** If not updated properly and regularly, security risks are associated with pre-installed software and firmware. The patches and updates should be applied in a secure manner and the attacker should not be able to discover sensitive information (i.e. cryptographic credential and updated software configuration) during the update process.
3) **Storage security:** IoT enables data to be stored both in physical devices and cloud storages. Personal data and security credentials might be kept within an IoT device. Therefore, poor physical security makes the storage medium and any data stored on that medium susceptible to intrusion.

◎ **Communication security:** There are three major factors in the communication security

1) **Security in multifarious connectivity**: In order to connect the diversified smart objects to the global interconnected network, IoT network spans through different types of network infrastructure comprising wireless, wired, private, and public networks. This cross protocol characteristic makes the IoT network vulnerable to various security problems like data integrity violation, inadequate quality-of-service (QoS), etc.
2) **Network service security:** Vulnerable network services may lead an IoT device towards dead state, where the device is inaccessible to users. This might be the case, when networks services are found susceptible to buffer overflow or DoS attack, as unnecessary ports are exposed and available.
3) **Cryptographic security**: Because of the low computational capability, IoT devices might avoid transport encryption or might use weak encryption. Therefore, communication becomes easy to discover and traceable by the malicious actors.

◎ **Service security.** It comprises of on-device service security, cloud service security and partner cloud service security.

1) **Native service security:** Different IoT services are available at the local network, which we denote as native service. We classify native services into three categories: in device service, coordinator service and gateway service. The web interface used by those local devices might have some vulnerabilities including account enumeration, insecure account credentials and lack of account suspension after a limited number of password guessing.
2) **Cloud service security:** IoT services are hosted on clouds, so that devices and applications can be access at anytime from anywhere. This eliminates boundaries for access, but incorporates security risks at the same time. For instance, security concerns raise for the data privacy and confidentiality.
3) **Partner cloud service security:** IoT cloud services and applications might use services and resources from the partner or enterprise cloud services. Lack of secure and seamless access to those services might make the consumers susceptible to different critical security risks.

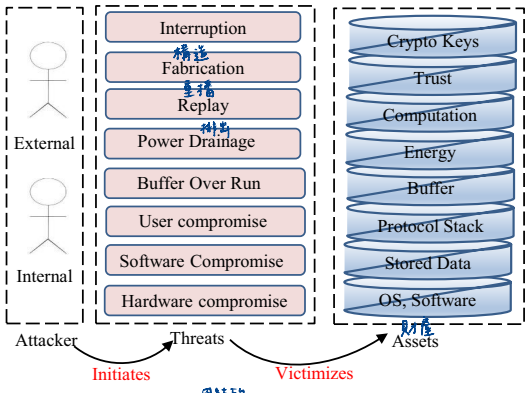

Fig. 5: Consolidated Threat Model

VI. Attack Taxonomy

The consolidated threat model representing different types of attacks is shown in Figure 5. This model consists of attackers, threats, and assets. The Attacker might reside within the IoT network or might be an outsider and has a great interest in assets: protocol stack, communication channels, etc. The attacker performs illicit acts such as jamming, message sniffing, node compromising, etc. in order to gain unauthorized access to the assets or to make the IoT services dysfunctional. The subsequent section describes different types of attacks targeting IoT assets.

A. Attacks Based on Device Property

Low-end device class attack: The Adversary can attack using IoT devices with similar capabilities and configurations to native network's IoT devices. For example, let us consider a smart home with interconnected smart things (smart TV, smart refrigerator, smart thermostat, etc.). An adversary with malicious wearable device (smart watch) – which contains malicious applications – might get unauthorized access to smart TV and launch different types of attacks which threatens communication, message integrity, privacy, etc. Here, capabilities of wearable device and smart home-devices are more or less similar.

High-end device class attack: Here, the attacker uses more powerful or full-fledge devices – personal-computer, laptop,

cloud PC (virtual machine) – to get to access to native IoT network and device from anywhere and launch severe attacks.

B. Attacks Based on Adversary Location

Internal attack: Here, the attacker resides in the close proximity of the IoT devices or within the same IoT network. Adversary either uses its own malicious device or compromises legitimate device in order to launch attacks.

External attack: Here, an attacker is deployed out of the native network – attacker might reside anywhere in the public network –, and gets unauthorized remote access to the native network entities (devices/ resources) or it compromises the native trusted device to initiate various attacks.

C. Attacks Based on Access Level

Active attacks: When the adversary performs illicit activities in order to disrupt the normal functionality of IoT device and/or networks , then those malicious activities are referred as active attacks. For example, jamming, denial of service (DoS), etc.

Passive attacks: In this case, the adversary is similar to the authorized IoT device and performs illegal activities to gather information from the trusted IoT devices and networks, however communication is not interrupted. This types of attacks are against the privacy of IoT. For example, monitoring , eavesdropping, traffic analysis, etc. of communication channel.

D. Attacks Based on Attack Strategy

Physical attacks: Attacks which cause physical damage or change in device properties and configurations are treated as physical attacks; for example, tampering with the IoT devices, malicious code injection.

Logical attacks: Without doing any physical damage an adversary might launch attacks to make the IoT devices dysfunctional; for example, attacks on communication channel.

E. Attacks Based on Information Damage Level

The adversaries are enthusiastic about the on-the-fly messages and their motive is to attack the floating data either disrupting communication or compromising information. A set of in-transit attacks are:

Interruption: Other than interruptions that may happen ordinarily like power outages or service shut downs, DoS attacks are used to cause resource exhaustion and hence make some services unavailable. Disaster recovery mechanisms are important to implement here [15], [16], [17].

Man-in-the-middle: The man-in-the middle attack intercepts a communication between two nodes. Two parties are tricked into thinking they are communicating securely with each other, while the attacker actually sits in between them, communicating with both. Alteration and Eavesdropping are two major branches of Man-in-the-middle attacks.

Eavesdropping: The attacker surreptitiously listens to the information carried through a private communication. RFID devices are one of the most susceptible kinds of IoT devices to this attack [18]. This kind of attack threatens message confidentiality.

Alteration: An adversary gains unauthorized access to data and tampers with information, which creates confusion and misleads innocent entities in an IoT network. Message integrity suffers severely in this attack. A well designed Intrusion Detection System (IDS) can be used to detect these kinds of situations [19].

Fabrication: An adversary generates additional data or activity that would normally not exist. This attack creates confusion among the parties involved in the communication. Fabrication threatens messages genuineness and can either be launched by an internal or external source [20].

Message Replay: The main purpose of this operation is to confuse or mislead the parties involved in the communication protocol that are not time-aware. This attack threatens message freshness. Efficient protocol to eliminate message replay is presented in [21], [22].

F. Host Based Attacks

Operating system and system software are embedded into the IoT devices. Most of them also contain sensitive information: private data, and cryptographic keys. Therefore, the IoT devices fall victim to attackers who are targeting those data.

User compromise: An adversary entraps the users to expose their security credentials such as keys or passwords through unsporting maneuver. Secure transfer of the credentials is a very important aspect in this part [23].

Software compromise: An adversary takes advantage of the vulnerabilities of operating systems or system softwares running on an IoT node. One common method is to push device in exhaustion state by means of resource buffer overflows [24].

Hardware compromise: An adversary extracts embedded credentials such as data, keys, or program code stored within an IoT device by tampering with the hardware. This kind of attack usually requires physical access to devices and includes micro-probing and reverse engineering to be performed on that particular device. However, a device may have a tamper resistant design and be immune to this kind of attack [25], [26], [27].

G. Protocol Based Attacks

Adversaries compromise stand protocols and threatens service availability. Protocol compromise attack has two perspectives.

Deviation from protocol: An attacker deviates from standard protocols (e.g. application protocols, networking protocols) becoming an insider and acts maliciously.

Protocol disruption: An attacker might be deployed inside or outside the network and perform illegal actions on standard protocols: key management protocol, data aggregation protocol, synchronization protocol, etc.

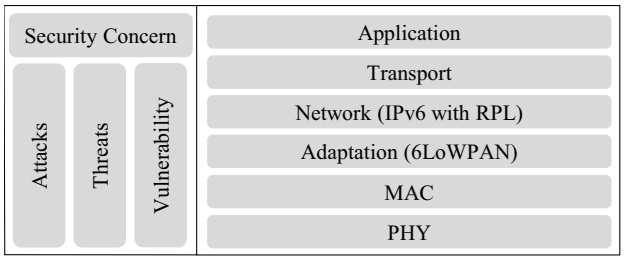

Fig. 6: Security and IETF LLN Protocol Stack

Layers	Attacks	Defences
Physical	Jamming	Channel surfing, spatial retreat, priority messages
	Radio Interference	Delayed disclosure of keys
	Tampering	Tamper-proofing, hiding
MAC	Collision	Error-correcting code
	Exhaustion	Rate limitation
	Unfairness	Small frames
Network	Sinkhole	Geo-routing protocol
	Worm/ Black hole	Authorization, monitoring, redundancy
	Homing	Encryption
	Misdirection	Egress filtering, authorization, monitoring
Transport	De-synchronization	Authentication
	Flooding	Client puzzles
Application	Overwhelm	Rate-limiting
	Reprogram	Authentication

TABLE I: LLN Protocol Stack Threats and Defense

H. *Communication Protocol Stack* Attacks

Security concerns for *Low Power and Lossy Network (LLN)* standard [28] are shown in figure 6 . The layer wise attacks [29], [30], [31] of the LLN protocol stack are shown in the Table I.

VII. Research Directions

Several IoT-centric critical security issues might be unnoticed or poorly addressed by the security researchers, as this paradigm is not full-fledged yet. Therefore, we organize this section with some of the prominent security issues.

Trust management: Depending on the level of interoperability in the network and the ability of dynamic expansion, an IoT device may have to decide which other entities in that network (or outside the network) are trustworthy. This decision requires the device to possess the ability to distinguish such a node. Implementing this concept in a network of devices with limited resources, can be quite challenging.

Governance: Governance is the amount of actual security control on the network of things. Wherever there is more control and monitoring, there is more safety. This also applies to IoT networks. If every interaction is monitored, then it would be much easier to track a malicious activity to the attacker. Thus, this security control can be a very positive aspect. However, if it exceeds some limit, it can turn into a nuisance as a high level of monitoring can be a threat for every user's privacy.

End-to-end security: There are two major kinds of connection in the IoT, H2T (human to thing) and T2T (thing to thing). Over time, the majority of connections in IoT are shifting from H2T to T2T. Merging Internet and WSNs speeds this shifting process up as there are more things and less human activity involved. Providing security for these connections, which are likely to communicate sensitive information, is a very important matter which is referred to as End to End security.

Fault tolerance: The IoT objects must have certain defense mechanisms and use them when required to first repel the threat and after that, recover from any possible damage. These mechanisms may each have its own way to do these steps. For example, one mechanism may report any intrusion to a certain human being (system operator, owner, police department, etc.). Another one may just lock everything and shut down the whole system. In some cases other complex approaches may be more effective.

Identity management: It is most important for a smart device to know when it should or should not reveal its identity. Providing identity to an adversary can be a serious threat. However, we must obtain a system that, in the same time, provides device identity to other qualified devices. Devices that interact with users (humans) must know their identity and be able to distinguish them too. Authorization is also an issue that corresponds to identity management as authority will be granted to identities (device or human).

Energy efficient security: While there has been some research to reduce energy consumption of the sensor devices through utilizing more efficient cryptographic methods, no significant effort has been put to reduce the energy consumption of the security processes in an IoT device.

Key management: Lightweight key management systems are crucial in order to maintain a safe key and to distribute it between trusted nodes.

Data transparency: Data transparency enables the owner to know or even decide who is going to be able to access the data. That depends on the level of data transparency implementation in the system. Data transparency also lets the owner make sure of his data genuineness.

Group membership: Machine-to-machine (M2M), Radio Frequency Identification (RFID), context-aware computing, and ubiquitous computing all are considered to be seamlessly integrated into the IoT paradigm. This integration creates two other kinds of connections in the IoT, Ts2T (things to thing) and T2Ts (thing to things). These two refer to communication between groups of nodes and a single node in the IoT network. These groups have members and for their memberships, they will need specific certification. This certification can be in form of a shared key or any shared credentials for that matter. Managing and maintaining group memberships and also applying the same concepts that are applied to nodes, to these groups, can lead to some complexity and new issues that need to be addressed.

Security of handling IoT big data: All the devices working in an IoT network will generate some kind of data and will need some place to store it. Providing security for handling

this data, including transfers and maintenance, and syncing all the data from different devices without compromising any part of the system, requires great attention and effort.

IoT forensics: The definition of computer crime and cloud crime will be extended to the IoT crime, which represents any malicious activity that involves the IoT paradigm in the sense that the IoT devices, services or communication channels can be a subject, object, or tool related to the crimes. To investigate these type of cases, it is required to execute digital forensics procedures in the IoT to determine the facts about an incident. The definition of an efficient and exact IoT digital forensics procedure is still at its great demand.

VIII. Conclusion

In this paper, we have surveyed the most important security aspects of the Internet of Things with emphasis on what is being done and what are the issues that require further research. Our work explores the overall security architecture of IoT followed by security issues related to interoperability of heterogeneous objects. We also perform an exhaustive analysis of the vulnerabilities of the connected objects by taking consideration of their computational limitation, energy limitation, resource limitation, and lightweight cryptographic protocols. Additionally, we address real life situations where the lack of IoT security could pose various threats. Our work analyzes existing research problems and challenges and provides opportunities for future research work in this area. In conclusion, we believe this survey may provide an important contribution to the research community, by documenting the current security status of this very dynamic area of research and motivating researchers interested in developing new schemes to address security in the context of the Internet of Things.

Acknowledgements: This research was supported by the National Science Foundation CAREER Award CNS-1351038 and an Amazon AWS for Education Grant.

References

[1] Q. Zhou and J. Zhang, "Research prospect of Internet of Things geography," in *Proceedings of the 19th International Conference on Geoinformatics*. IEEE, 2011, pp. 1–5.

[2] Y. Yu, J. Wang, and G. Zhou, "The exploration in the education of professionals in applied Internet of Things engineering," in *Proceedings of the 4th International Conference on Distance Learning and Education (ICDLE)*. IEEE, 2010, pp. 74–77.

[3] J. Li, Z. Huang, and X. Wang, "Countermeasure research about developing Internet of Things economy: A case of hangzhou city," in *Proceedings of the International Conference on E-Business and E-Government (ICEE)*, 2011.

[4] "Internet of Things research study," 2014, accessed on 19-April-2014. [Online]. Available: http://www8.hp.com/h20195/V2/GetPDF.aspx/4AA5-4759ENW.pdf

[5] "Proofpoint uncovers Internet of Things cyberattack," 2014, accessed on 19-April-2015. [Online]. Available: http://investors.proofpoint.com/releasedetail.cfm?releaseid=819799

[6] C. Cerrudo, "Hacking us traffic control system." 2014, accessed on 12-April-2015. [Online]. Available: http://blog.ioactive.com/2014/04/hacking-us-and-uk-australia-france-etc.html

[7] Y. Oren and A. D. Keromytis, "From the aether to the ethernet–attacking the Internet using broadcast digital television," in *Proceedings of the 23rd USENIX Security Symposium, San Diego, CA, USA*, 2014, pp. 353–368.

[8] S. Cesare, "Breaking the security of physical devices." 2014, accessed on 12-April-2015. [Online]. Available: http://regmedia.co.uk/2014/08/06/dfgvhbhjkui867ujk5ytghj.pdf

[9] P. Desai, A. Sheth, and P. Anantharam, "Semantic gateway as a service architecture for IoT interoperability," *arXiv preprint arXiv:1410.4977*, 2014.

[10] S. K. Datta, C. Bonnet, and N. Nikaein, "An IoT gateway centric architecture to provide novel m2m services," in *Proceedings of the World Forum on Internet of Things (WF-IoT)*. IEEE, 2014, pp. 514–519.

[11] M. Covington and R. Carskadden, "Threat implications of the Internet of Things," in *Proceedings of the 5th International Conference on Cyber Conflict (CyCon)*. IEEE, 2013, pp. 1–12.

[12] N. Gruschka and M. Jensen, "Attack surfaces: A taxonomy for attacks on cloud service," in *Proceedings of the IEEE 3rd International Conference on Cloud Computing (CLOUD)*, 2010, pp. 276–279.

[13] "Open web application security project for internet of things," accessed on 12-April-2015. [Online]. Available: https://www.owasp.org/index.php/OWASP_Internet_of_Things_Top_Ten_Project

[14] D. Lake, R. Milito, M. Morrow, and R. Vargheese, "Internet of Things: Architectural framework for ehealth security," *Journal of ICT Standardization, River Publishing*, vol. 1, 2014.

[15] H. Suo, J. Wan, C. Zou, and J. Liu, "Security in the Internet of Things: a review," in *Proceedings of the Computer Science and Electronics Engineering (ICCSEE)*, vol. 3. IEEE, 2012, pp. 648–651.

[16] T. Heer, O. Garcia-Morchon, R. Hummen, S. L. Keoh, S. S. Kumar, and K. Wehrle, "Security challenges in the ip-based internet of things," *Wireless Personal Communications*, vol. 61, no. 3, pp. 527–542, 2011.

[17] A. Wood and J. A. Stankovic, "Denial of service in sensor networks," *Computer*, vol. 35, no. 10, pp. 54–62, 2002.

[18] G. Hancke, "Eavesdropping attacks on high-frequency RFID tokens," in *Proceedings of the 4th Workshop on RFID Security (RFIDSec)*, 2008, pp. 100–113.

[19] Y. Zhang and W. Lee, "Intrusion detection in wireless ad-hoc networks," in *Proceedings of the 6th annual international conference on Mobile computing and networking*. ACM, 2000, pp. 275–283.

[20] T. Zia and A. Zomaya, "Security issues in wireless sensor networks," in *Proceedings of the International Conference on Systems and Networks Communications, ICSNC*, 2006.

[21] T. Dimitriou, "A lightweight rfid protocol to protect against traceability and cloning attacks," in *Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks*. IEEE, 2005, pp. 59–66.

[22] Y. Mo and B. Sinopoli, "Secure control against replay attacks," in *Proceedings of the Communication, Control, and Computing*. IEEE, 2009, pp. 911–918.

[23] A. Arsenault and S. Farrell, "Securely available credentials-requirements," RFC 3157, August, Tech. Rep., 2001.

[24] S. X. Xu and J. Z. Chen, "Analysis of buffer overflow exploits and prevention strategies," *Applied Mechanics and Materials*, vol. 513, pp. 1701–1704, 2014.

[25] S. Babar, P. Mahalle, A. Stango, N. Prasad, and R. Prasad, "Proposed security model and threat taxonomy for the Internet of Things," in *Proceedings of the Recent Trends in Network Security and Applications*. Springer, 2010, pp. 420–429.

[26] 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, 2012, pp. 269–275.

[27] A. Perrig, J. Stankovic, and D. Wagner, "Security in wireless sensor networks," *Communications of the ACM*, vol. 47, no. 6, pp. 53–57, 2004.

[28] J. Vasseur, "Terminology in low power and lossy networks." Online at https://tools.ietf.org/html/draft-ietf-roll-terminology-06, *Work in Progress, IETF Draft*, 2011.

[29] T. Kavitha and D. Sridharan, "Security vulnerabilities in wireless sensor networks: A survey," *Journal of information Assurance and Security*, vol. 5, no. 1, pp. 31–44, 2010.

[30] M. Panda, "Security threats at each layer of wireless sensor networks," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 3, pp. 50–56, 2013.

[31] A. S. Sastry, S. Sulthana, and S. Vagdevi, "Security threats in wireless sensor networks in each layer," *Int. J. Advanced Networking and Applications*, vol. 4, no. 04, pp. 1657–1661, 2013.