Internet of Things – A Study on the Security Challenges

Rajendra Billure, Varun M Tayur, Mahesh V
Department of Computer Science and Engineering
Jain University
Bangalore, India
email: {rajendrabillure, varuntayur, mahesh92411}@gmail.com

***Abstract*—The vision of Internet of Things (IoT) is to enable devices to collaborate with each other on the Internet. Multiple devices collaborating with each other have opened up various opportunities in multitude of areas. It has presented unique set of challenges in scaling the Internet, techniques for identification of the devices, power efficient algorithms and communication protocols. Always connected devices have access to private sensitive information and any breach in them is a huge security risk. The IoT environment is composed of the hardware, software and middleware components making it a complex system to manage and secure. The objective of this paper is to present the challenges in IoT related to security, its challenges and recent developments through a comprehensive review of the literature.**

***Index Terms*—Internet of Things; security in IOT**

I. Introduction

The Internet is a global system of interconnected computer networks, which has evolved over decades. The Internet at the start was mostly defined by the World Wide Web which was a collection of linked HTML documents and was mostly static. An interactive social version called the Web 2.0 enabled user participation and collaboration leading to a massive generation of user generated content. The user generated data is largely unstructured, so work on a semantic Web – termed as Web 3.0 is emerging to make the data understandable by machines so that they can be intelligent.

Tiny embedded sensors have evolved and become more intelligent. Such collaborating devices require them to be uniquely identifiable when they collaborate on mainstream Internet because of the critical data they have with them. Along with sensor networks, RFID and NFC are becoming prevalent with the advent of ambient smart homes and smart-phones.

The central concept of the IoT is the enablement of everyday "things" like coffee machines, refrigerators, Smartphone and medical equipment to talk to each other. The hardware and software technologies have to act in harmony to enable the notion of such connected "things" to be successful. Hardware technologies are powered by RFID, NFC, sensor networks and Bluetooth low energy. Software is characterized by frameworks for middleware, data query, data storage retrieval and exchange. Specialized architectures provide the necessary framework based on which the hardware and software operate in unison to provide the desired service.

The widespread adoption of IoT will bring in a lot of visible changes to a wide range of users both on the personal and business purposes. Assisted living, smart homes, smart cars, etc. are areas where IoT helps an individual while businesses can benefit by more production, superior quality and better services. Rest of the paper is organized into the following sections. Section II presents the analysis by reviewing current literatures related to security in IoT. Section III presents an account of Exploits and Attacks in the IoT space, followed by Section IV which deals with the importance of security in IoT. Section V discusses the mitigation plans, which is followed by a conclusion.

II. Background of work

IoT is characterized by the presence of hardware, software and middleware components collaborating with each other. Each of the components in the IoT model has sensitive data which can be breached that poses a security risk.

A. Hardware

IoT hardware infrastructure is primarily provided by Radio Frequency Identification (RFID), Near Field Communication (NFC), Wireless Sensor Networks and Bluetooth Low Energy. RFID operates in the request-response mode, with the reader querying for the information stored in the tags. Most popular application of RFID is in the Electronic Product Code (EPC). An EPC is a universal unique identifier for an object. Exposing such data remotely can have wide implications in various applications.

NFC is relatively a newer technology that builds on the RFID standard. NFC is a short-range communication standard where devices are able to engage in radio communication with one another when touched together or brought into close proximity to one another. The main selling point for NFC was the ability to have bi-directional communication. NFC has become very popular with end-user devices especially Smartphone's enabling them to communicate with each other when brought close to each other. Similar to RFID tags, NFC tags contain a Unique Identification (UID). One common use for NFC is in smart posters. Smart posters contain readable NFC tags that transmit data to the user's Smartphone which reads the data from the tag.

978-1-4799-8047-5/15/$31.00 ©2015 IEEE

Sensor networks are systems encompassing multiple sensors that monitor characteristics of the environment or other objects such as temperature, humidity, movement, and quantity. Multiple such sensors are used together and their interaction as a system is referred to as a Wireless Sensor Network (WSN). Actuators can affect the environment by emitting sound, light, radio waves or even smells. These capabilities are one way that IoT objects can communicate with people. One example of the use of actuators in such a network is the use of a sensor to detect the presence of a vehicle on a zebra crossing and the use of an actuator to produce a loud noise alerting the offending person to move back. The combination of sensors and actuators enables objects to simultaneously be aware of their environment and interact with people more intelligently.

Main areas of research in IoT is ongoing to improve the energy efficiency as energy is the scarcest resource in IoT and to improve scalability as the number of nodes connected will continue to increase. Research is also ongoing to improve reliability as IoT devices may be used in critical devices like urgent alarm events etc and to improve robustness as sensor nodes are likely to be subject to failures for several reasons [3].

Most of the wireless sensor networks are based on the IEEE 802.15.4 standard. It just defines the physical and Medium Access Control (MAC) layers for Wireless Personal Area Networks (WPAN). A main characteristic of the devices in Wireless Personal Area Networks is low-power and low bit rate communications [4]. IEEE 802.15.4 does not include specifications how to seamlessly integrate the sensor nodes into the Internet. The difficultly in it is:

- Sensor networks consist of a very large number of nodes. All the nodes connecting to the Internet will have issues with unique addressability with IPv4, the adoptability of IPv6 is on-going but at a very slow pace [2].
- The data packet payload size in wireless sensor nodes is too less when compared to the typical IP packet size. The largest physical layer packet in IEEE 802.15.4 has 127 bytes compared to a 60 byte payload header.
- A contrasting requirement of sensor networks is that most of the sensors are “sleeping” while they are awaiting events as against a constantly chattering IP based networks.

Bluetooth low energy is a wireless personal area network targeted at healthcare, fitness, security and home entertainment needs. The advantages of this technology is its low power requirement, operating capability for months or years on small button cell, small size and low cost of hardware and existing compatibility with large number of mobile phones, tablets and computers. A Bluetooth smart protocol named Cambridge Silicon Radio (CSR) mesh was introduced recently (2014) with an aim to support Internet of Things. This technology made possible to control groups of switches using QR Codes. Several profiles based on low energy application profiles or Generic Attribute Profile (GATT), are defined by the Bluetooth specification targeting healthcare, sports, fitness, proximity sensing and alerting [2].

B. Software

Software uses hardware and forms a crucial component in the IoT system. Some of the challenges are related to handling the generation of data at a fast pace by multitude of devices without a particular standard makes integration and interoperability a major challenge. The data generated is heterogenic introduced by different kinds of devices. The possible solution is to introduce good amount of abstraction to hide all the complexity details and ensure adoption of IoT in a bigger scale which is possible with software.

IoT still in its infancy relies on the hardware infrastructure to provide the necessary services with minimal support from software. The nature of data generation in IoT will be largely mobile and dynamic generating massive amounts of frequently changing information. A software framework to identify smart objects, discover them and techniques to interact with those objects is given in [8]. An IoT search engine that is capable of searching the rapidly changing information generated by IoT-enabled objects is discussed in [9] and a multi-tier data processing model is discussed in [5].

C. Middleware

Middleware is an abstraction layer between the hardware and the applications that drive it. It enables hiding the details of different technologies exempting the programmer from concentrating on development of a solution to a particular issue enabled by the IoT infrastructure. The middleware layer is very important because of the need to interoperate with new and existing legacy infrastructure. Among the various models proposed on IoT by various researchers, Semantic middleware and Service Oriented Architecture (SOA)[4] oriented middleware seem to be the most popular. The Semantic middleware based technologies are based on the Extensible Markup Language (XML) metadata exchange [6] for interoperability while the SOA and Representational State Transfer (REST) based [7] systems are more popular in the enterprise environment because of the advantage that it offers is that, it addresses both semantic and technical interoperability problems.

Distributed, heterogeneous nature of the IoT requires hardware, software, and processes to work in complete harmony to ensure the desired quality of service. Since IoT devices have specialized needs suitable adaptation layers have been provided. SOA based middleware’s for IoT is discussed in [4]. This model proposes to model IoT devices along the lines of a traditional service oriented broker. Focus on the security aspects of devices is not evident as the onus of the communication is put on the device which is seen as a service. Various specialized architectures that handle media traffic, clock synchronization, security systems, QoS are discussed in [5] and [10]. Focus on the secure communication is apparently absent as most legacy systems were never intended to be connected to the Internet. Other architectures such as [5] propose a model which is based on the separation of concerns; each of the layers is built on off-the-shelf technologies so the onus on the secure communication is left to the device being used. Service-Oriented Internet of Things is proposed in [1],

where the device is exposed as a service with decision making processing at each layer in the stack - application layer, network layer and perception layer.

III. Exploits and Attacks

The main threats relating to the IoT stack are presented in the following sections. [27]

A. Attacks to the Physical Layer

1) Jamming: Emission of radio signals with the goal of disturbing and/or disrupting the communication constitutes jamming. Wireless interference is unintentional, jamming is intentional and focuses on a specific target [27]. An attacker with a powerful jamming source can disrupt the entire communications of a victim network. Also, an attacker could make quickly drain the battery of target devices by intentionally disrupting their data transmission and make them repeatedly retransmit. Jamming could also lead to denial of service. (DoS) [28]

2) Tampering:

a) Injection Attacks: Disbursal of malicious software through the debugging interface of the device thereby disrupting the entire network and spreading the code across is a typical characteristic of injection attacks. Alternatively, an attacker may obtain all private information in the home network by injecting malicious software which will later transmit all information outside of the protected network.

b) Extraction of Security Information: Sensitive information such as pre-installed encryption keys can be extracted from devices by stealing the actual driver or connecting to a device. For example, we can copy the keys by extracting the firmware of a smart meter using a debugging cable. [27]

c) Duplication of a Device: An exact duplicate of the features of a genuine device including hardware, software and configurations with malicious software can manipulate a genuine device or degrade the functionalities of other devices. There are cases where an iPhone has been exploited by the use of a malicious duplicate charger which installed a Trojan into the device software.

B. Attacks to the Data Link Layer

The most vulnerable algorithms in the communication stack are represented by the data link layer

1) KillerBee: Killerbee provides a set of tools for exploiting vulnerabilities in ZigBee and IEEE 802.15.4. This has simplified injecting traffic, sniffing, packet decoding and manipulation. Numerous attacks can be carried out using KillerBee such as PANId conflict, replay attack, packet capturing, and network key sniffing. [29]

*2) Guaranteed Time Slot (GTS) Attack:*GTS attack is based on the characteristics of the IEEE 802.15.4 super frame organization in beacon-enabled operational mode. The GTS slots create a week point which can let adversary to catch hold of the frames and later initiate an attack to disrupt the communication between a device and its coordinator gateway. The attacks can cause interference which results in corruption and collision of the data packets between devices, and make target nodes to retransmit data packet repeatedly.

3) Back-off Manipulation: A malicious device constantly chooses a small back-off interval for contention using the Distributed Coordination Function (DCF), not giving chances for medium access to a genuine device. These attacks are common in CSMA/CA based networks such as IEEE 802.11 and IEEE 802.15.4 networks.

4) ACK Attack: By eavesdropping on the wireless channel, ACK attack can be launched by an adversary who may block the receiver device from picking the transmitted packet. It can then mislead the sender device by sending a fake ACK that comes from the receiver device.

C. Attacks to Network Layer

Different types of attacks such as flooding, spoofing, network sniffing, data capturing and modification, DoS are common due to the numerous protocols in use. Attack on the RPL networking protocol used for IoT networks are described in [27]

1) Black Hole Attack on RPL: The RPL implementation of ContikiOS is challenged in this attack, wherein a black hole which drops all the packets routed through it is introduced into the network causing disruptions in the data flow. The main challenge with this attack is that the black hole attack is effectively disguised and the attacked network behaves very similar to a healthy network [27].

D. Attacks to the Transport Layer

General well-known attacks to the transport layer are flooding and de-synchronization [27] – not many attacks have been documented with respect to IoT in this regard.

E. Attacks in Application Layer

XMPPloit, is a command-line exploit tool to attack XMPP connections exploiting vulnerabilities at the client and server side running the XMPP protocol. This attack can force clients not to encrypt its communications, so that an attacker may read and modify them while they are transmitting.

IV. Importance of Security in IoT

Protection of data has been an important issue ever since the beginning of the communication networks. With the modernization and commercialization of the Internet, security worries expanded to cover personal privacy, financial transactions, and the risk of cyber-theft. In IoT, security is inseparable from safety. Whether accidental or mischievous, interference with the controls of a car, pacemaker, or a nuclear reactor poses a risk to human life. Security must be addressed throughout the lifecycle of the device, from the initial design to the operational environment at all levels as discussed below

A. Hardware/ Physical Level

Devices need to be secure. The main security issues include physical security of sensing devices and the security of information collection. Due to the diversity, simple, energy

limited and weak protective capability of sensing node, and mostly deployed in unmanned harsh environment without a special standard, the IoT cannot provide a unified security protection system and is vulnerable to the invasion and attack.

The security problems faced in this layer include nodes physical capture, capture gateway node, sensing information leakage (the location of the reader and user, the user information and other information), integrity attacks, energy depletion attacks, congestion attack, unfair attacks, denial of service attacks, replay attacks, tampering and man-in-the-middle attacks, forward attack and node replication attacks. For M2M terminal equipment, the risk is mainly due to the deployment before connecting and unattended M2M devices leading to theft, damage and subscription information attack [12]. The need is to have intelligent network which identifies any node gone bad and self-organizes the network without breaking the network.

B. Software/Communication/ Protocols Level

Communication framework in IOT is easily attacked by the intruders. The risks in existing IoT communication network include illegal access, data eavesdropping, confidentiality, integrity, destruction, denial of service attacks, man-in-the middle attacks, virus attack [12]. Loss of privacy in IoT devices collecting personal information is another threat. Most of the communication is wireless which makes snooping very easy. Authentication is also challenging as it requires suitable authentication infrastructures which are generally missing in IoT. IoT devices have scarce resources as compared to present computing and communication devices [11].

The major problem is that the keys cannot be formed as they need the support of end hosts, and end hosts are inadequate in IOT devices due to the characteristics of limited energy, storage, network bandwidth and communication abilities. [13] The possible solutions is to use low power encryption methods.

C. Storage of the Data Level/Application Layer

Data stored should be secure and encrypted. Since the IoT sensing a large number of devices, a variety of formats of the data collected, and the data information has a massive, multi-source and heterogeneous characteristics, Therefore, in the network layer it will also bring other more complex aspects of network security issues, such as large data transfer requirements due to large number of nodes in IoT leading to network congestion and thus resulting in denial of service attack [14]. The possible solution is to introduce IoT applications to use cloud computing, data mining, data storage, data backup, data management and authentication mechanisms.

V. Security Mitigation Approaches

IoT has three basic characteristics: comprehensive awareness, reliable transmission and intelligent processing [15]. Awareness is realized mainly with RFID, sensors and M2M terminal to get the information of the object anywhere and anytime. Reliable transmission goal is realized with high accuracy and by real-time encryption, routing, communication and network security protocols. Intelligent processing depends on cloud computing, intelligent computing technology to analyze and hand mass information and pick up meaningful data to meet the different users. It depends on the secure way of storing the data collected by IoT devices.

A. Hardware/ Physical Level

Self-healing networks is the new research area in the IoT. If any node stops functioning or is lost or stolen, the network should be able to self-heal and should not get broken up. Any addition or removal of nodes should be effortless and should not break the network.

The second is the authentication security mechanism, mature cryptosystem to meet the security authentication protocol for RFID systems, such as hash-lock protocol, randomized hash-lock agreement, hash-chain protocol, and interactive authentication protocol [12]. But there is a tradeoff between security and cost.

M2M devices should have a strong anti-radiation, high temperature resistance, resistance to physical damage, and provide reliable execution environment for M2M. One option is to integrate the machine and card in a single cell, carrying USIM (Universal Subscriber Identity Module) or UICC (Universal Integrated Circuit Card) such that it cannot be removed or will be removed and disabled permanently. It is generally accepted that the UICC is tamper proof and the master key in the UICC is fairly resistant to any types of physical and network attacks to disclose secret keys. In the continuing sense, we must assume that the master secret key in the core network, particularly in the HSS, is also immune to any physical and network attacks [17]. If MCIM (M2M Communications, Identity Module) in the form of software directly bound to the M2M device, we need a special trusted environment M2M device to safely store and execute MCIM, such as remote attestation mechanism in the trusted computing technology.

Fingerprinting techniques [18] can be used to identify nearby base stations or access points. Fingerprinting can be done at the physical communication layer by extracting unique signatures from wireless signals by looking amplitude, frequency, delays, and phases. For devices in close proximity can use signal characteristics for pairing [19] [20]. Their solutions use characteristics of radio signals to verify that devices are in close proximity to each other. Two devices first measure reciprocal signal characteristics, which are identical only for pair-wisely communicating devices and accepted pairing if measurements are identical.

B. Software/Communication/ Protocols Level

Connecting networked nodes with restricted user-interaction capabilities and interfaces securely to Internet services is challenging. Current Internet and software methods are highly modular, highly distributed (cloud) and loosely coupled. In today's systems, every unit comes from a different source and they all still must snap together [21]. This requires open, rapid and safe protocol methods.

Existing legacy solutions for security pairing uses passwords, trusted certification authorities, or physical connection, but it is not feasible when devices have long distance and have no interfaces for inputting passwords or secret keys. Possible solution is out-of-band proximate pairing which can be applied in situations where the counter party is far away or has incompatible interfaces [16]. The devices may pair if they both have NFC interfaces, Bluetooth or if one can act as USB host's role and another in USB device's role. Short-string compare model based security protocols [22] [23], which allow the user to pair devices by comparing two displayed short strings or by entering the string on one device. However, embedded IoT devices without displays or keyboards are a challenge for security. Figure 1 shows an example of pairing and key exchange between a IoT device and Smartphone.

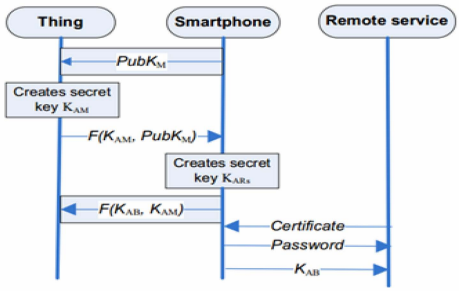

Fig. 1 Pairing between IOT Device and Remote Service Using Smartphone [16]

Figure 2 shows the key exchange between multiple devices [16] using context-aware security, allowing a device to perform particular actions or adjusting device's security level based on contextual information such as device location or time has been an active research area in the scope of short-range networks in IoT. For instance, proximity information proves that devices are physically close to each other at particular time has been used in security pairing by many researchers. Device location based pairing using GPS can be used provided the IOT devices are spread across distinct geographical regions. But GPS integration in the IOT devices can add to cost.

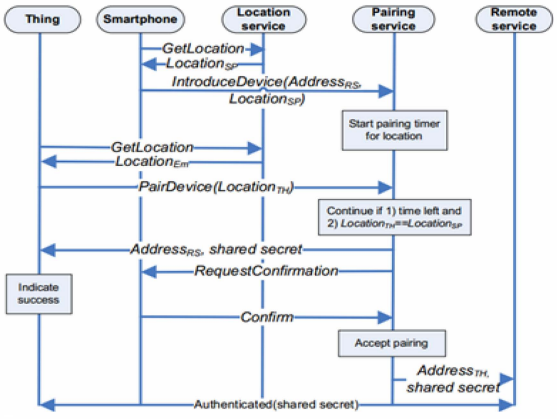

Figure 2: Pairing between IOT Device and Remote Service Using Smartphone [16]

Mobile network based location services are available for devices with mobile connectivity. A possible attack against network based location is the tunneling of signals to a distant base station with radio relays. A device communicating with a remote base station will seem to be in different location than the intended pair. Consequently, the attacker may create pairing with both devices and launch a man-in-the-middle attack.

Other unauthenticated pairing models such as Wi-Fi Push-button and Bluetooth JustConnect utilize proximity-information when making the pairing. But geographical limitation comes into picture when devices are not in proximity. Another approach is mediating devices can be used to establish a key for devices that cannot be directly connected. Touch-mediated Association Protocol (TAP) [24] is a solution where the end-user touches two devices with a third one in order to pair them. Tapping is based on forwarding secrets through a short-range wireless channel, which is assumed to be confidential.

Many applications in IoT networks are based on multicast communication model where single source sends common data to many receivers. In such scenario, it is possible to secure the multicast communications by leveraging on a common secret key shared by multiple users known as group key. In case of any membership change, the shared key should be refreshed through a suitable rekeying operation so that previous group member has no access to present communications and new member has no access to former communication [25] but it increases the computation overhead during frequent group membership changes caused by user's joining and leaving groups.

C. Storage of the Data Level/Application Layer

Prevention of unauthorized users from use and accessing the database by proper security management is a critical aspect. Database administrative privileges must be assigned to select users. The security itself must be provided at various layers importantly database encryption library should be used to encrypt outgoing data, encryption outside the library also needs to be in place to secure incoming communication. The hardware encryption takes the initiative to protect data, data protection security, data backup, remote disaster recovery and other means to achieve the active protection of the data[12][26]

VI. CONCLUSIONS

This article reported the current state of IoT security by examining the literature, identifying current trends in securing IoT environments, and open research challenges. The Internet has changed the world in many ways and with the advent of devices connecting to the Internet, a new dimension to the Internet has arisen. The interconnection of the devices helps in improving people's lives through both automation and augmentation. All the communication occurring on the public networks needs a secure communication channel as private data is exchanged.