Secure IoT: An Improbable Reality

Nayana Mannilthodi and Jinesh M. Kannimoola
Amrita Center for Cybersecurity Systems & Networks, Amrita School of Engineering, Amritapuri, India
Amrita Vishwa Vidyapeetham, Amrita University, Kollam, Kerala, India

Keywords: Internet of Things (IoT), Security, Attacks, Privacy, Vulnerability.

Abstract: Internet of Things(IoT) has been the buzzword for the past decade. Apart from its hype over opportunities, the security implications of IoT are unsolvable with current technologies. There is a wide range of security challenges in each layer of IoT conceptual model. We discuss the security challenges caused by the complex structures and integration of different techniques from diverse domains. By analysing attacks at the various layers we argue that the current standards are not enough to provide a secure framework for IoT. The economical and practical reasons make it impossible to puzzle out the various security challenges in IoT stack. From this perspective, we should think twice before connecting a device to the network of things.

1 INTRODUCTION

Internet of things (IoT) is an expansion of Internet to the real world which interconnects the physical devices to the virtual world. The term IoT was first proposed by Kevin Ashton in 1999 at MIT labs (Ashton, 2009) with a vision for a smarter planet. The vital part of IoT stack are the sensors, which collects data from the environment and shares with computing cloud through the Internet (Sathyadevan et al., 2014).

The concept of IoT is revolutionary, which changes the way people live, work, entertain, and travel, as well as how governments and businesses interact with the world (Insider, 2016). Everything around us from daily life appliances such as washing machines, refrigerators, mobile phones to cars, buildings and traffic cameras would gather data and then stream it to concerned computing platform autonomously. The analysis of this data can trigger the automated action using actuators. In other words, machines would start to replace human decision-making. Gartner has predicted that there will be 25 billion IoT devices by the year 2020 (Gartner, 2014).

IoT opens new security challenges to the world due to the wide use of sensors and smart devices. As the model is tightly coupled with the real world in real time, its security flaws cause more drastic results than the Internet security flaws. The sensors, gateways and repositories with full of interesting information are attractive targets for hackers. A network of the poorly secured device affects the security and resilience of the IoT globally. In this paper, we will look into various security implications of IoT and its reasons. The security challenges of IoT is never ending. There are many more attacks, which are beyond the scope of this paper. IoT can never be secure even in the future. New vulnerabilities are being invented and fixing it each time is not economically and practically feasible. This is because of the diversity of IoT. Bringing IoT to our daily activities is an invasion of our privacy and leaves us more exposed to the attackers.

The remainder of this paper is organised as follows. Section 2 discusses conceptual layers in IoT framework, and sections 3 and 4 describe the security challenges and current standards with their limitations respectively; section 5 describes why it is impossible to solve IoT challenges; section 6 outlines the related works and section 7 presents the conclusion.

2 CONCEPTUAL MODEL

ITU recommends(Kurakova, 2013) a five layer conceptual model for Internet of Things. It offers a modular structure to IoT stack by separating the responsibilities between different layers as described in Figure 1. We can summarise each layer in the conceptual model as follows.

- *Perception Layer:* This layer is responsible for collecting the information about the things which include sensors data, building parameters, location etc. It also provides this information to the

Mannilthodi, N. and Kannimoola, J.
Secure IoT: An Improbable Reality.
DOI: 10.5220/0006352903380343
In *Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security (IoTBDS 2017)*, pages 338-343
ISBN: 978-989-758-245-5

upper layer for transmission over the Internet.

- *Access Layer:* This layer enables the communication and information exchange through Internet by various networks such as WiFi, mobile networks, satellites.
- *Internet Layer:* It defines the connection establishment and the infrastructure for the upper layers along with the management and analysis of data.
- *Service Management Layer:* This layer is responsible for providing the data models and interoperability of different IoT services.
- *Application Layer:* The application layer takes the information and uses it for the different applications such as traffic signals, health care appliances and disaster monitors.

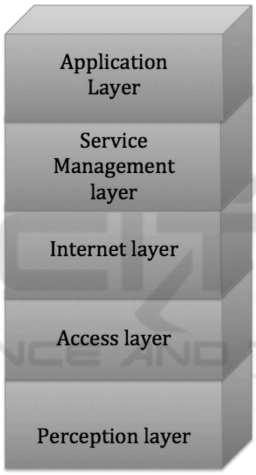

Figure 1: Conceptual Layers of IoT.

3 SECURITY CHALLENGES

IoT devices interact very closely with human lives. The security challenges of IoT devices has severe effects because it is the safety critical systems that are connected to the Internet and these devices can perform machine to machine communication (Suo et al., 2012; Sathyadevan et al., 2015). Securing IoT means securing all the sensor data, access points, the network infrastructure, the cloud, and the storage. Internet of things is a collection of various technologies, devices, and standards, thus ensuring security in this diverse environment is one of the biggest challenges. Few security challenges on each layer are mentioned below.

3.1 Perception Layer

The perception layer mainly consists of sensor nodes which have low computational power and are operated by battery. Most sensors would be disposable so applying a software update is a tedious task and would not be cost effective.

Illegal access: The tags in the sensors use RFID which does not use any authentication mechanisms (Uttarkar and Kulkarni, 2014). An attacker can hack into the sensors just by following the steps of an authorised user and gather the information. The attacker can modify or access the sensor data without much difficulty.

Unauthorised tag cloning: An attacker can easily get the tag identity and conduct integrity attacks by manipulating tag information. This vulnerability can be exploited to overcome counterfeit protection in passports and drug labels. This vulnerability also questions the verification step which uses the RFID tags for security procedures (Burmester and De Medeiros, 2007).

Unauthorised tag tracking: The attacker can trace and track the tags then find its activity and location. These are privacy attacks, which can also be exploited by hackers or adversarial organisations.

Relay attacks: RFID is used as a contact-less identification card due to its read at a distance feature. But the RFID identification information can be hacked by the attacker. In this attack, the attacker borrows the victims card information without his/her knowledge or any physical access. This attack exploits the tags response to a rogue readers challenge to impersonate the tag (Hancke, 2005).

Eavesdropping: Eavesdropping attacks are one of the most prominent risks of RFID devices. It is very easy to sniff the information flow from reader to tag or tag to reader (Hancke et al., 2008). The majority of the communication use radio frequency spectrum. The signals that are broadcasted can be simply intercepted with a receiver tuned to the same frequency.

Spoofing: Spoofing is a variant of cloning that does not require RFID tag to be physically replicated. The attackers impersonate a valid RFID tag or broadcast fake information to the RFID (Mitrokotsa et al., 2010).

Active jamming: An attacker can exploit the fact that RFID tags listen to all radio signals in its range, he can conduct a DoS attack by creating signals in the same range that node uses to communicate with the reader (Li, 2012).

3.2 Network and Access Layer

Network layer consists of the Wireless Sensor Network (WSN), WiFi capabilities, mobile networks, satellites, access points, gateways and all other network infrastructure. The function of this layer is to reliably transmit information between the perception layer and service management layer. The network layer has the challenges inherited from the Internet and the additional ones from the specific features of IoT (Patton et al., 2014).

Sybil attack: Sybil attack is a type of attack in which a node illegitimately claims multiple identities. The system can be compromised by this attack and the information from the perception layer would be misinterpreted. The attack can alter too many important functions of the sensor network such as routing, resource allocation, misbehaviour detection (Messai, 2014).

Sinkhole attack: Sinkhole is an attack in which an attacker makes a node the most attractive one for the other nodes to transfer the data. Thereby all the data traffic will be diverted to this particular node which can be rerouted to an attacker or made to drop the packets to cause a DoS attack (Kibirige and Sanga, 2015).

Sleep deprivation attack: The ability of the wireless node to sleep when the battery is down can be exploited by an adversary. An attacker can exploit the clustering algorithm to drain the node's energy savings and make it sleep. There are two varieties of such attack one is sleep deprivation attack and the other is barrage attack (Pirretti, 2006). Barrage attack is noticeable as it aggressively bombards the node. Whereas in the sleep deprivation attack the adversary sends packets with an interval by which adversary can keep the victim awake (Pirretti, 2006).

Location disclosure attacks: An attacker can get the node location, structure of the network, a route map by analysing the traffic. Thus the attacker can figure out the identities, learn from the network traffic and track changes in the traffic pattern (Miller and Valasek, 2015).

Other common network attacks: As mentioned before the IoT also has the inherited vulnerabilities from the Internet. Attackers can poison the routing tables, control the traffic flow, flood the network, drop the packets by interfering the network. An attacker can inject malicious code into the network by compromising a node; by doing so, he can take down the entire network or get full control over the network (Farooq et al., 2015).

3.3 Service Management Layer

Insider attack: This attack is very common in cloud infrastructure where an attacker is someone who is inside the system and has access to cloud data. An attacker can tamper the data on the cloud for personal or third party benefits.

Weak authentication: In a test conducted by Symantec on cloud services on IoT, it was found that most of the IoT cloud services allow users to choose weak passwords. In some other services, users are prevented from using complex passwords. For example, one service was found with password restriction of a PIN code with maximum four digits. Even after many failed login attempts, many services do not lock the users out of their accounts. Also, none of the tested back-end cloud services provides two-factor authentication.

3.4 Application Layer

The application layer is also vulnerable to security attacks. The application contains lots of user data. The protocols used in application layer such as HTTP, SMTP, FTP have known vulnerabilities and are entry points for attackers.

Malware attacks: Malware such as virus, spyware and Trojan horses can steal the user information and do malicious activities.

Code injection: The vulnerabilities in the applications due to the mixing up of code and data can be exploited by hackers. An attacker can inject malicious code into the system and steal user data (Barcena and Wueest, 2015).

3.5 Multi-layer Attacks

Some attacks are done by exploiting the vulnerabilities that are evolved from integrating multiple layers.
Botnets: Botnet is a network of nodes remotely controlled by an adversary to perform DDoS attacks, to distribute malware, to steal private data and to sent spam or phishing emails. Thingbots are botnets of connected objects. These botnets have a variety of connected devices. Wireless routers and modems are the main targets for Thingbots due to their ubiquity and direct connectivity to the Internet. Other devices such as network cameras, network storage system, and all the smart devices that have Internet connectivity and are able to transfer data are also targets of Thingbots (Sabanal, 2016).

Man in middle attack: This is one of the old attack concepts in the network where an attacker tries

to interrupt and breach communication between two nodes. As the attacker has the original communication, they can trick the recipient into thinking that they are still getting a legitimate message.

Data and identity theft: Data available from the Internet, social media, smart devices that the person owns, the smart meters and much more can provide an overview of the person's identity, location and other personal information. These data can be utilised for commercial purpose or to create personalised attacks.

Denial of service (DoS) attack: A DoS attack can be initiated from different layers. At the physical layer, an attacker can jam the signals. At link layer, the attacker can do a capture effect. At the network layer, the attacker can do selective dropping, routing table poisoning, table overflow. At transport and session layer, the attacker can hijack the session, or do a SYN flood. At the application layer, there are malware to do DoS attack (Messai, 2014).

4 CURRENT STANDARDS AND THEIR LIMITATIONS

The core need of IoT is to have a full interoperability among IoT devices. Practically a full interoperability is very complex. The concept of connecting any IoT object to the Internet is one of the biggest standardisation challenges. An IoT device needs to communicate with any other IoT device or IoT infrastructure from various layers of communication protocols at different degrees (Rose et al., 2015).

There have been many industrial and academic attempts to standardise IoT environment and to create a secure architecture for IoT. CISCO proposed a secure framework for securing different layers of IoT(CISCO, 2013). Ning et al. (Ning et al., 2012) proposed a secure framework called IPM considering the informational, physical and management models. Another example for a secure framework is PubNub which consist of a secure global Data Stream Network and APIs that are easy to use for customers(PubNub, 2015). The Internet Engineering Task Force (IETF) is currently leading the standardisation process of communication protocols for resource constrained devices, being developed. There are other Internet protocols such as Routing Protocols for Low Power and Lossy Networks (RPL) and Constrained Application Protocol (CoAP) (Group, 2016). From the available standards choosing the best framework is not easy. There is no accepted reference architecture among vendors. As a solution for this many vendors build their IoT platform from the start. They customise and design services according to their platform. However, this approach ends up with more non-interoperable IoT systems. Such independent development of IoT platforms leads to less secure choices, gaps in the standards and lack of an agreed-upon methods(Group, 2016).

5 WHY IT IS IMPOSSIBLE TO SOLVE IOT CHALLENGES

The technological shift promised by IoT is very exciting; at the same time, the security vulnerabilities are worse than what the Internet currently faces. A study by HP Security unit found that 70 percentage of IoT devices are hackable (HP, 2014). An IoT device like smart fridge is as vulnerable as laptops and mobiles.

Users ignorance: Most of the consumers do not know or do not care to know how IoT devices operate. Even for a tech savvy person interested in the security of device is unable to find more about device's operations. Most of the 'things' do not provide access to system information such as its operating system or the software version, hardware configuration or any details about its last update. A person is unable to manually update, in case he discovers vulnerabilities in his device. Unlike the laptop and mobile phones, there is little documentation and tools publicly available to the check the device security.

Productions: One of the most important question to solve is, who makes the 'things'. In a study conducted by Jay Schulman, (Spring, 2016), in search of an activity tracker on Amazon, he found that there are thousands of brand names on Amazon. Also, there were the things that are high rated and perfect products from unknown producers. Later on the investigation, it was found that these were products from producers not much concerned about the security of the IoT things. Most of the producers are concerned only about customer service and satisfaction. Many products today are produced by a third party and shipped to customers.

Unknown vulnerability: Integrating many complex technologies together bring new unknown vulnerabilities. The common man being excited about the possibilities of IoT use the smart appliances knowing nothing about the security implications. In recent, researchers could show that Samsung's smart fridge RF28HMELBSR can be exploited by Man in Middle attack and could access house owners social media credentials through the fridges touch screen display (Schulman, 2016). Hack on Jeep Cherokee well explains the possibility of a remote attack (Zunnurhain,

2016). The hackers Charlie Miller and Chris Valasek could remotely control the entire car systems like air-conditioning, radio, and windshield wipers, accelerator and even brakes.

Cost of production and Patch: Most of the RFID tags in detecting and identifying 'things' are disposable. It is economically infeasible to call back all the RFID tags on finding a security flaw and to fix it. On the other hand some devices have vulnerabilities that could not be fixed because they did not have the ability to be updated. Industries also do not provide long-term support and a patching solution for Internet-connected devices that have to be updated and patched from the upcoming security bugs in the future.

Architecture: IoT has to be secure by design, but unfortunately, security has turned out to be an add-on feature for IoT (Zunnurhain, 2016). In the current state of IoT, the developers are trying to solve the problem by adding patches. This can only increase the complexity of the system. There are different organisations striving to make a secure architecture for IoT. But these attempts are not going together to have a common standard.

Limited capability of devices: Most IoT devices have limited computational power and run on batteries. There is only limited space available in the devices for additional codes and data. A security researcher Maxim Rupp found a vulnerability on ESCs 8832 Data Controller, and it was mentioned that the device had no available code space to add the security patch according to ICS-CERT 2016.

Limitation of lightweight encryption: Lightweight encryption was suggested as a solution for security on IoT devices. Symmetric algorithms provide confidentiality, integrity. These algorithms have small keys and low complexity. But authentication and key distribution still pose a major problem. Some symmetric algorithms used for IoT are AES, which was found to have man in middle attack vulnerability (Drozhzhin, 2015). Another algorithm, High security and lightweight (HIGHT) that use basic operations such as addition mod 28 or XOR work for Feistel network was found to have saturation vulnerability (Luhach et al., 2016). PRESENT is lightweight encryption based on SPN and is used as an ultra lightweight algorithm for security, it is vulnerable to differential attack on 26 of 31 rounds (Derbez and Fouque, 2013). RC5 that work as a lightweight algorithm for wireless sensors are also vulnerable to differential attack. Tiny Encryption Algorithm (TEA) used in constrained environment are also found vulnerable to many attacks (Lee et al., 2010). The asymmetric algorithms have very large key sizes which make it more complex to be calculated on devices that have energy and computation constraints.

Convenience and Ease of usage: Since it is not just the laptops and mobiles connected to the Internet, users find it difficult to be concerned about security all the time. A user would think that a microwave connected to IoT is still a microwave but he does not realise that it can have same vulnerabilities as his laptop which is connected to the Internet. Daily things asking for security updates, permissions and passwords will take out the cool quotient of IoT.

Vertical integration: The integration of technologies are really complex. Small devices that have their own software, are integrated into one bigger device. For example, a car would have several devices from different manufactures. It will be more complicated when the device becomes more complex. Its a big challenge to make sure that all the sub-devices are secure. Even if the individual devices would be secure it would be difficult to say that its integrated version is secure.

Lack of standards: Some of the layers of IoT stack have no standards and on the other side, there are numerous standards from different organisations competing to win. Some of these standards are incompatible with each other. For example, in the connectivity there are Bluetooth, ZigBee, LTE category 0 standards. Even if agreed upon a common networking protocol, then there is an issue of software standards to contend with. These make the devices impossible to share a common security protocol. Gartner says that the divergent number of approaches to solve the problems will only create security gaps.

6 RELATED WORKS

The security of Internet of Thing has started to get attention in recent years. Kaspersky has regularly written about how unexpectedly vulnerable a connected device can be (Miller and Valasek, 2015). Allen Storey, Intercede has criticised IoT as "Theres nothing 'smart' about insecurely connected devices" in which he has mentioned about the possible cyber crimes through IoT (Storey, 2014). Mark et al. did a study on the vulnerable devices on Internet of Things and found vulnerability rates ranging from a low of 0.44% to a high of 40% at various IoT domains (Patton et al., 2014).

7 CONCLUSIONS

Though the Internet of things seems to be a revolutionary concept it can't come to reality without solving its security issues. The security challenges of IoT is so vast, and it cannot be solved by current technologies. Integration of multiple technologies will only make the system more complex and hence less secure. We explained various reasons why IoT cannot be secure practically. There are no satisfying solutions for the security issues of IoT. Even the suggested solutions like lightweight encryption and standardisations face many criticisms for its efficiency. Hence we conclude that IoT can never be secure.

REFERENCES

Ashton, K. (2009). That internet of things thing. *RFiD Journal*, 22:97–114.

Barcena, M. B. and Wueest, C. (2015). Insecurity in the internet of things. *Security Response, Symantec*.

Burmester, M. and De Medeiros, B. (2007). Rfid security: attacks, countermeasures and challenges. In *The RFID Journal*.

CISCO (2013). Securing the internet of things: A proposed framework. http://www.cisco.com/c/en/us/about/security-center/secure-iot-proposed-framework.html.

Derbez, P. and Fouque, P.-A. (2013). Exhausting demirciselçuk meet-in-the-middle attacks against reduced-round aes. In *International Workshop on Fast Software Encryption*, pages 541–560. Springer.

Drozhzhin, A. (2015). Internet of crappy things. https://kas.pr/at2F.

Farooq, M., Waseem, M., Khairi, A., and Mazhar, S. (2015). A critical analysis on the security concerns of internet of things (iot). *International Journal of Computer*.

Gartner, I. (2014). Gartner says 4.9 billion connected "things" will be in use in 2015. http://www.gartner.com/newsroom/id/2905717.

Group, I. W. (2016). Future-proofing the connected world: 13 steps to developing secure iot products.

Hancke, G. et al. (2008). Eavesdropping attacks on high-frequency rfid tokens. In *4th Workshop on RFID Security (RFIDSec)*, pages 100–113.

Hancke, G. P. (2005). A practical relay attack on iso 14443 proximity cards. *Technical report, University of Cambridge Computer Laboratory*, 59:382–385.

HP (2014). Hpe fortify and the internet of things. http://go.saas.hpe.com/fod/internet-of-things.

Insider, B. (2016). The master key to understanding the iot revolution. http://read.bi/29mOi16.

Kibirige, G. W. and Sanga, C. (2015). A survey on detection of sinkhole attack in wireless sensor network. *arXiv preprint arXiv:1505.01941*.

Kurakova, T. (2013). Overview of internet of things. *Proceedings of the Internet of things and its enablers (INTHITEN)*, pages 82–94.

Lee, J., Kapitanova, K., and Son, S. H. (2010). The price of security in wireless sensor networks. In *Computer Networks*. Elsevier.

Li, L. (2012). Study on security architecture in the internet of things. In *Measurement, Information and Control (MIC), 2012 Int. Conference on*, volume 1, pages 374–377. IEEE.

Luhach, A. K. et al. (2016). Analysis of lightweight cryptographic solutions for internet of things. *Indian Journal of Science and Technology*, 9.

Messai, M.-L. (2014). Classification of attacks in wireless sensor networks. *arXiv preprint arXiv:1406.4516*.

Miller, C. and Valasek, C. (2015). Remote exploitation of an unaltered passenger vehicle. *Black Hat USA*.

Mitrokotsa, A., Rieback, M. R., and Tanenbaum, A. S. (2010). Classifying rfid attacks and defenses. *Information Systems Frontiers*, 12(5):491–505.

Ning, H., Liu, H., et al. (2012). Cyber-physical-social based security architecture for future internet of things. *Advances in Internet of Things*.

Patton, M., Gross, E., Chinn, R., Forbis, S., Walker, L., and Chen, H. (2014). Uninvited connections: a study of vulnerable devices on the internet of things (iot). In *JISIC, 2014*, pages 232–235. IEEE.

Pirretti, M., Z. S. V. N. M. P. K. M. B. R. (2006). The sleep deprivation attack in sensor networks: Analysis and methods of defense. *International Journal of Distributed Sensor Networks*, 2.

PubNub (2015). A new approach to iot security.

Rose, K., Eldridge, S., and Chapin, L. (2015). The internet of things: An overview. *The Internet Society (ISOC)*, pages 1–50.

Sabanal, P. (2016). Thingbots: The future of botnets in the internet of things. *RSA Conference*.

Sathyadevan, S., Achuthan, K., and Poroor, J. (2014). Architectural recommendations in building a network based secure, scalable and interoperable internet of things middleware. In *Advances in Intelligent Systems and Computing*, volume 327, pages 429–439. Springer.

Sathyadevan, S., Kalarickal, B., and Jinesh, M. K. (2015). Security, trust and implementation limitations of prominent iot platforms. In *Advances in Intelligent Systems and Computing*, volume 328, pages 85–95. Springer.

Schulman, J. (2016). Why we will never secure the internet of things. *buildingacareerinsecurity.com*.

Spring, T. (2016). Iot insecurity pinpointing the problems.

Storey, A. (2014). There's nothing smartabout insecure connected devices. *Network Security*, pages 9–12.

Suo, H., Wan, J., Zou, C., and Liu, J. (2012). Security in the internet of things: a review. In *Computer Science and Electronics Engineering (ICCSEE), Int. Conference on*, volume 3, pages 648–651. IEEE.

Uttarkar, M. R. and Kulkarni, R. (2014). Internet of things: Architecture and security. *International Journal of Computer Application*, pages 12–19.

Zunnurhain, K. (2016). Vulnerabilities with internet of things. In *Proceedings of the Int. Conference on SAM*, page 83.