IoT Security

Christin Wilson
cwils28@clemson.edu

***Abstract*—Over the past decade, Internet of things has gained a lot of popularity and is rapidly developing. It has had an impact on all the domains ranging from tiny wearable devices to smart cars. IoT interconnects physical everyday objects by converging various technologies. But with this rapid growth, there have been uncertainties rising about its security and privacy. These enormous number of devices are potentially vulnerable and impose several security risks and thus it is a threat to the sustainable development of IoT. This paper is a survey about the various challenges for IoT in terms of security and their countermeasures.**

I. Introduction

IoT is the ubiquitous interconnection of physical computing devices, which are being used in place of common everyday objects, that enables the free flow of information amongst the devices through the internet. Kevin Ashton first proposed the term Internet of Things in 1999[1].

Over the years, IoT has found applications in almost every domain. This is due to its ability to provide advanced skills to various systems and devices. It has also garnered the development of advanced interaction between humans and everyday objects by creating a virtual environment. Thus the concepts such as smart devices, smart cars, smart homes have seen a rapid increase in interest from users and research communities. Over the years, devices like watches, TVs, heaters, refrigerators and cars have been updated to collect and send data to the connected devices by accessing the internet with the help of technological advances and are able to perform automated actions based on this. As shown in figure 1, the internet of things is made up of sections like communication, processing, sensors, actuators, storage etc.

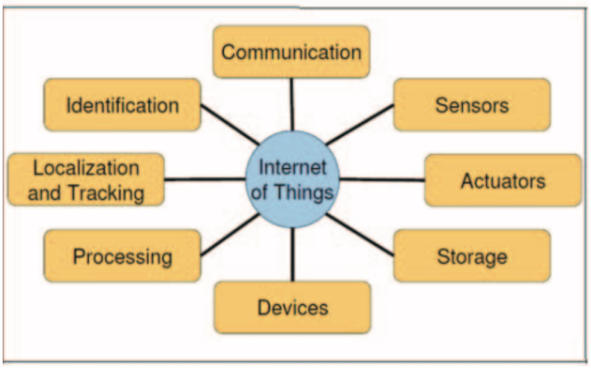

Fig. 1. Topics make up the Internet of Things

All kinds of devices are now able to be used as a smart and communicating device rather than as an isolated device. This is made possible by adding sensors, storage and computing capabilities to the device. These devices are being computerized and added with systems that equip them to connect to the network. Extensive research and development are being performed in this area. This has resulted in the rapid growth in the number of devices being added to this network.

IoT is thus opening up a large market for opportunities. But on the flip side, with this large sudden increase in the number of the connected objects, a lot of risks and threats have risen. Since every device is connected to the internet and is sharing information, the risk of private information and data that should not be shared might be shared through the internet. This can result in loss of private and thus pose a severe security threat.

The IoT applications thus must meet the communication standards such as confidentiality, authenticity, availability, integrity, privacy for users, access control and well-defined security and privacy policies. When these standards are not met, attackers can access the shared data violating the user's privacy. To achieve basic IoT security requirements, the device must be secured, the application interface must be secured and also ensure that the data transfer between the devices is secured.

II. Overview

This paper will discuss the various security threats to IoT. In section III, the generic architecture of IoT will be discussed. This will show the various layers where security can be compromised. Section IV will discuss the security in IoT and the various conditions that a developer has to consider while developing for IoT. Section V will discuss the various challenges that IoT will face in terms of security and privacy. Section VI will propose the various countermeasures that have to be taken for the several challenges posed on IoT. The paper will conclude with Section VII discussing the conclusion to the survey conducted.

III. Generic architecture of IoT

Generic architecture The generic architecture of IoT can be classified into four layers:

1) Perception Layer: The data sensors, actuators and other sensor networks make up this layer. The basic purpose of this layer is to collect data from the real world with the sensors and to deal with this collected data.

2) Network Layer: The basic purpose of the network layer is to transport the data that is being collected by the perception layer to the processing system through the internet or any

other kind of reliable network.

3)Middle-ware Layer: This is the layer comprising of the information processing system which is connected by the network layer. These take automated actions based on the data collected and links to the database for storage purposes of this data.

4)Application Layer: This is the layer where the actual practical application of the IoT devices happens. The actions will be performed as needed by the users.

IV. Security in IoT

IoT still relies on traditional frameworks for development and thus is more susceptible to a security threat. Existing researches in IoT security are focused on problems such as RFID tag security, wireless security, network transmission security, privacy protection, information processing security etc. [2] The security threats raised by the connected objects increase with the growth of IoT. Several new policies and protocols have been published to ensure the security of critical and sensitive data. The backbone of IoT systems are the various wireless communication technologies that are being used for connectivity between the devices and the applications. The various technologies that are commonly used are NFC, RFID, Bluetooth, Wi-Fi, ZigBee WirelessHART, 6LowPAN, WiMAX and mobile communication.

The CIA triad model for the development of security mechanisms must be implemented to ensure the security of the IoT system. To make a device secure, the developer has to ensure that the following conditions are met.

Authentication: The device should follow better practices to authenticate the user. instead of using traditional approaches for authentication, new technologies like multi-factor authentication must be made use of. Users can be prompted to authenticate themselves by making use of any other device like their mobiles or their wristwatches that they carry all the time in addition to the traditional authentication method like a password or biometric identification.

Confidentiality: It is very easy to intercept an IoT message by using the latest technology that can result in sensitive or critical data to reach the hands of third parties. If a user connects an IoT device to a certain network and uses it, it is very easy for someone in the same network to access this content. Therefore, confidentiality should be maintained and the messages that are being passed should be encrypted and hidden from unauthorized entities and can be accessed by permitted users only.

Data integrity: It refers to the protection of data from cyber criminals or external interference and ensuring that the data transferred by the source reaches the destination as such and is not tampered with during the transfer. If tampering happens the system must be able to identify it. Data integrity is even more important than privacy or availability in the case of IoT because if the devices which are used for medical purposes or the smart cars are not secure and is exploited, it might result in the loss of life. Keyless Signature Infrastructure, complemented with public key infrastructure can be used as an integrity proof.

Access Control: Unlike traditional systems where access control is targeted only to closed systems, those in IoT should target both open and closed systems since unknown parties should be given proper control of the system.

Availability: This is ensuring that data is available to users, whenever they need them. The system should be made secure from Denial of service attacks which can deny the availability of data and resources to authentic users when they need them. Proper steps must be taken to ensure reliability and availability of data even during system failure by using redundancy and failover backup methods.

V. Security Issues and Privacy concerns

Even though IoT has immense potential, due to the flawed infrastructure in terms of the security standpoint, it faces a large chance of threats in terms of privacy to the end user. The challenges that are discussed in the following sections can result in sensitive information being stolen, unauthorized access to personal details, confidential information and also compromise the integrity of all the interconnected devices in the system. The devices can also be susceptible to malware due to its reliance on the internet.

A. Research challenges

Several research challenges have been identified for IoT security which has to be considered. These surveys will act as a guideline to researchers to work on the various challenges and come up with advancements. Thorough analysis has been done by different surveys and authors on the various technologies and protocols used for security in IoT. The secured collection of huge amounts of data and storing it safely will be the major challenge that IoT will face in the future. New advanced technologies have to be developed and incorporated into these devices to achieve this. To ensure a minimum level of privacy, industry standards must be set for all developers. Research must be carried out to ensure that sensitive data and private data is secure from attack.

B. Communication Layers

Researches have classified the security protocols for different layers. Widely used protocols are available for IoT as well. Security can be provided to the communication process by using these standardized security mechanisms.CoAP is the application layer protocol whereas the IEEE 802.15.4 is a the Data-link layer. Figure 2 shows a table with the respective security protocols for different layers in IoT.

C. Perception Layer challenges

The layer consists of the sensors which actually collects the data from the real world, so challenges faced in this layer is related to the different sensor technologies like RFID.

Node Tapping: There is no proper authentication mechanism for many RFID systems. This results in unauthorized persons accessing these tags. These can result in the data being deleted

IoT Layer	IoT Protocol	Security Protocol
Application	CoAP, MQTT	User defined
Transport	UDP	DTLS
Network	IPv6, RPL	IPsec, RPL security
6LoWPAN	6LoWPAN	None
Data-link	IEEE 802.15.4	802.15.4 security

Fig. 2. IoT stack with Security Protocol

or manipulated by the attacker.

Tag Cloning: The tags are visible on certain objects and these can be easily obtained and attackers can create an indistinguishable replica of this tag. This will result in the attacker accessing the data and modifying or deleting it by making use of the compromised tag without the reader knowing.

Eavesdropping: Since the RFID has wireless characteristics it is very easy for an attacker to sniff the information being shared between the user and the tag. If the data being shared is sensitive or critical, this can pose a vulnerability to the system as it breaks the privacy of the user and the users' data can be used in despicable ways.

RF Jamming: Launching a DoS attack can result in the jamming of the RFID tags because of the large number of communications happening that will disrupt the RF signals.

Spoofing: Attackers can inject fake data to the RFID system by posing as the original user which can result in the attacker to even get full access to the system.

Besides these attacks like Reverse engineering, Viruses, killing tag approaches can also be performed on this layer.

D. Network Layer Challenges

These challenges arise during the transmission of data from the perception layer to the information processing systems. The challenges are:

Sinkhole Attack: In this attack a particular node that is an adversary looks attractive to the other nodes and reroutes traffic to it and the data packets that are being sent to this node is dropped and the source node is fooled to think that the transmission is completed and data has been received on the other side.

Sleep deprivation Attack: This attack deprives the various nodes of sleeping. since the nodes are being powered with batteries these sleeps are necessary for the devices to last longer. By depriving them of this, the batteries in these nodes run out of power and these nodes are forced to shut down.

Denial of Service Attack: The network is flooded with a lot of fake and useless traffic by the attacker to launch this attack. This will result in the network becoming unavailable for the legitimate processes to occur.

Acknowledgement flooding: Fake acknowledgements are spoofed by attackers providing false information to nodes transmitting data.

Malicious Code injection: In this attack, the attacker compromises a node and inserts some malicious code into the network which will result in compromising the network and can lead to the shutdown or gaining full access to the network.

man-in-the-middle attack: In this attack, the attacker monitors and controls the communication happening by eavesdropping.

De-synchronization: In this attack fake messages are sent to source nodes transmitting data to re transmit the data thus resulting in the power loss of the node for a non-existent error.

E. Middle-ware Layer Challenges

This layer connects to the network layer and contains data storage options. The challenges faced in this layer are:

Unauthorized access: An unauthorized access to the system can result in the attacker destroying existing data from the database and forbidding acmes to the various services of the system which will compromise the system.

Denial of service attack: This will result in making the system unavailable to the authorized users and deprive them of their legitimate services.

Malicious Insider: This attack occurs when a person on the inside manipulates the data from his own purposes or for others. Since it is an inside guy, the data can be obtained easily.

F. Application Layer Challenges

This is the layer where the actual services are offered. The challenges faced here are:

Malicious Code injection: Some malicious code can be inserted by the user that will be injected to the system to compromise it and obtain data from the system.

Sniffing Attack: Sniffing can be performed by an attacker on the IoT system to gain network information to compromise it.

Spear-Phishing Attack: This attack involves sending an email to a high ranked victim who has access to the network which on opening will give the attacker the credentials of the person with which the attacker can access the network.

VI. CounterMeasures

A. Adding security to the Link layer

Roman et al. [2011] proposed a key management system for sensor network.[3] This is a security system for the link layer. Also while adding security to the link layer, it must be made sure that the outlined approach is not enough to ensure that the hot system is secured completely. In order to achieve end to end security, every node in the network must be made secure and trusted. A suitable key exchange mechanism must be mad use of like the SSL to establish a session key between the server and the client with respect to the internet of things. This will provide authenticity, integrity and confidentiality. But SSL uses TLS instead of TCP which is a drawback since it is not the preferred option for this kind of communication.

Techniques to ensure that authentication and data privacy must be made use of in this layer. Also a risk assessment must

be carried out regularly to prevent security breaches and to understand the best security strategies.

B. Securing the network layer

Granjal et al [2010] proposed and developed an implementation where a new compressed 6LoWPAN security headers was used. This could be used with the existing wireless nodes while at the same time provides secure integration WSNs. [4] Raza et al[2011] proposed an IPsec implementation and verified that communication between the sensor nodes and the hosts on the internet can be made secure using the compressed IPsec. [5] In addition, several transport layer protocols like TCP, UDP, HTTP and CoAp can be made use of by IPsec.
Techniques to ensure that authentication, routing Security and data privacy must be made use of in this layer.

C. Securing the Transport Layer

TLS has been made use of in IoT but as discussed earlier, it is not the preferred option over TCP, even though both of these protocols are based on the congestion control algorithm because of the constrained resource devices used in IoT. A new Protocol is proposed called Datagram Transport Layer Security (DTLS). This operates on UDP and thus works better on constrained environments while providing the same level of security.
Techniques to ensure that authentication, Intrusion detection, risk assessment and data security must be made use of in this layer.

D. Data Security

Security the data that is being collected by the devices is as important as securing the communication channel of these devices. Due to the small size of the IoT devices, they do not have enough constraints to secure them from hardware threats. To store the data proper techniques must be made use of to ensure its security. The transmitted data packets must be properly encrypted and authenticated before storing. Data format defined by Encapsulation Security Payload can be used for processing the data.

VII. Conclusion

The hurdle that IoT currently faces is the issues in security and privacy that they face. A thorough analysis of security protocols have been researched for IoT and mechanisms are available to protect the communication between the devices. Answers to the open questions posed by the researchers should be found and IoT should be made safe and secure. More work is expected to fill the gaps in IoT security. Researchers should focus on the development of customized security and privacy measures. Security must be designed in device thus reducing data theft and unauthorized access to prevent sensitive and critical data to be stolen. Proper security measures should be taken throughout the cycle. The solutions for the challenges raised in each layer must be added to the existing devices to ensure the stable development of the IoT technology.

References

[1] Shen, Guicheng, and Bingwu Liu. "The visions, technologies, applications and security issues of Internet of Things." E-Business and E-Government (ICEE), 2011 International Conference on. IEEE, 2011.

[2] Deshmukh, S., & Sonavane, S. S. (2017, March). Security protocols for Internet of Things: A survey. In Nextgen Electronic Technologies: Silicon to Software (ICNETS2), 2017 International Conference on (pp. 71-74). IEEE.

[3] Rodrigo Roman, Cristina Alcaraz, Javier Lopez, Nicolas Sklavos, Key Management Systems for Sensor Networks in the Context of the Internet of Things, Computers & ElectricalEngineering, vol. 37, pp. 147-159, 2011.

[4] Shahid Raza, Simon Duquennoy, Tony Chung, DoganYazar Thiemo Voigtand Utz Roedig, Securing Communication in 6LoWPAN with Compressed IPsec, 978-1-4577-0513- 7/11/2011 IEEE.

[5] Sain, M., Kang, Y. J., & Lee, H. J. (2017, February). Survey on security in Internet of Things: State of the art and challenges. In Advanced Communication Technology (ICACT), 2017 19th International Conference on (pp. 699-704). IEEE.

[6] Farooq, M. U., Waseem, M., Khairi, A., & Mazhar, S. (2015). A critical analysis on the security concerns of internet of things (IoT). International Journal of Computer Applications, 111(7).

[7] Borgohain, T., Kumar, U., & Sanyal, S. (2015). Survey of security and privacy issues of internet of things. arXiv preprint arXiv:1501.02211.