Security and Privacy for Internet of Things

Aditya Vishnu Garg
School of Computer Science and Statistics
Trinity College Dublin
ADGARG@TCD.IE

***Abstract*—To reach the full potential of IoT, one of the challenges is the complex problem of ensuring information security in a wide range of intruder threats, and various issues related to standards, security, ecosystem building architecture, and device connection protocols, need to resolve.**

As we progress forward, more and more IoT devices would keep adding and would lead to huge amounts of data generation which might contain confidential user information such as user habits, personality traits and patterns, user's likes and dislikes, and so forth. To be able to safeguard such confidential and sensitive data, it is the need of the hour to look at how the existing practices and policies put forward in the IoT community tackling the issues and what can be further done to improve the current situation.

***Index Terms*—Internet of Things, Security, Privacy**

I. Introduction

Internet of Things (IoT) is a wide mesh or network of devices that might contain sensors and the software transmission technology to send the data collected to the cloud application for further processing of the data. The device itself can be controlled remotely and might also have an actuator connected with it, which is controlled on the basis of the data processed on the device itself or as per the instructions sent to the IoT device from the cloud. IoT mainly makes the interconnection between things and people smart and easy.

The IoT devices that are evolving exponentially will definitely become intelligent by each day and will eventually become equal participants in the network world like humans. But the existing communication network architecture of telecommunications operators can hardly support the access of billions of IoT devices, and the main reasons for the difficulty of providing information security on a network level - the diverse nature of the structure (variety of things, different network technologies) and a large number of objects. IoT receives information from a wide range of devices, collects large data in different formats from multiple sources with different characteristics, and each unique IoT project has its own risk and threat model, which makes it almost impossible to provide a single uniform security system that can be used in all areas of IoT. This results in DoS (Denial of Service) failures due to network congestion and software errors due to the complexity of debugging in real-time using an external load simulator.

Since IoT smart devices mainly adopt SSDP (Simple Service Discovery Protocol), hence for interaction, the IoT device has the characteristics of high bandwidth, low monitoring level, and all-weather online. Therefore, its reflection attacks have a broader device foundation than other types of attacks.

Manufacturers and developers of IoT devices are not paying sufficient attention to ensure security, as they are in a rush to get the product first to the market and to make sure it is as cheap as possible for them. With the development of cyber-attacks, attack vectors are becoming more sophisticated and aiming at several elements of architecture at the same time. IoT architecture typically includes millions of connected objects and devices that store and exchange confidential information. Most IoT devices use the public web to exchange data, making it vulnerable to cyberattacks. Modern information security approaches often offer solutions to individual problems when tiered approaches offer enhanced resistance to cyberattacks.

The paper is set out as follows. Section II reviews the past major cases of cyberattacks in IoT. Section III highlights the core security vulnerabilities in the architecture. Section IV reviews how various research studies have tried to solve the issues of security and privacy in IoT. Section V talks about the possible solutions, and Section VI discusses the future of IoT security challenges. Finally, Section VII concludes the paper.

II. Past Cases of Security Attacks

The following cases addresses the various major IoT attacks which have had a wider impact in the past:

A. Mirai Botnet

The IoT botnet virus ”Mirai” is a large-scale distributed DDOS attacks. The malware successfully checks IoT network equipment and infects embedded IoT systems that have factory keys or weak passwords. The firewall can not adequately stop the virus from reaching and spreading, and it unknowingly corrupts the IoT portion and becomes a part of the botnet. Attackers can use this breached system to basically dominate the entire network or to try to replicate this vulnerability to other components on the network to increase the range of the attack [1].

B. Reaper Trojan

The IoT Reaper Trojan (also known as the IoTroop) is a new type of IoT Trojan discovered in October 2017. This trojan shares some commonalities with Mirai botnet, but it is more powerful than Mirai. IoTroop uses vulnerabilities to achieve cross-platform IoT device access. As opposed to guessing passwords in Mirai, IoTroop uses the IoT device vulnerabilities for implantation. Currently, about 2 million IoT computers are vulnerable worldwide and can launch larger DDoS attacks than Mirai did. The root IP addresses of these attacks are spread [2].

C. Memcached DDoS reflection attack

Memcached is a high-performance distributed cache program for objects in the memory. It is primarily used to increase the scalability of web applications and can solve the big data caching problem effectively. It is currently widely used in ”cloud computing” and Infrastructure as a Service (IaaS), owing to its simple structure and easy implementation. Memcached stores small data fragments depending on the memory key-value and uses this data to complete page rendering. It is simple and efficient, but the initial design did not give too much thought to protection and sturdiness, leaving a lot of safety risks.

For example, in February 2018, a global Memcached DDoS attack broke out, with peak traffic up to 1.7 Tbit / s. The traceability results show that the Memcached server distributed in China in this attack ranked second, accounting for 12.7%, so the protection against such attacks also needs urgent attention [3].

III. Core Security Issues In IoT

From the above actual cases, it can be seen that the research and security deployment of Internet of Things security issues are not waiting. The majority of the problems security issue seems to be originating in the terminal issues, network issues and operator platform issues.

A. Terminal and Device Vulnerabilities

An IoT terminal is a software interface that allows the data collected on the IoT device to be transmitted back and forth to the cloud easily and usually have low price and low intelligence, which in turn can be a security issue threatening the entire network of IoT or the network layer.

Most of these IoT solutions are designed to have high efficiency and low costs, which is one of the major problems, as the cost of the project and its economic efficiency become evident, the companies usually underestimate the cyberisks. But even the simplest intelligent device (environmental control systems, irrigation systems, fire detection, leak detection, etc.) must be provided with maximum protection. For example, an ordinary IoT thermostat that was once installed in a casino aquarium contributed to a cyber security catastrophe when the hackers were able to gain access to the thermostat and then breached the institution’s internal network, stealing the sensitive casino data [4].

As a solution, it is advised that users set strong passwords on the device, and to install anti-virus software and upgrade regularly. Subsequently, it is recommended to install a malicious code monitoring system in the IoT, which collects incoming port traffic, conduct deep packet inspection (DPI), identify malicious code characteristics by capturing packets, which then alerts the officials.

B. Cybersecurity Risk Issues

At present, common IoT attacks are similar to traditional Internet attacks. One of the basic steps to maintain network performance is the prevention of giant traffic assaults culminating in network blockage, and diminished network capacity.

In the face of such a massive traffic attack, operators must first prepare corresponding security plan templates at the backbone network level. They can set up whitelists and other means to achieve fast response and one-click blocking. At the same time, each autonomous domain needs to perform security flow control on its connected peer to prevent it from attacks from botnets so that it is able to discard abnormal traffic packets. At the core network level, organizations can deploy firewalls, IPS, and other security equipment at the node exit location, periodically perform vulnerability scans and weak password verification of core network equipment, strengthen its robustness.

The security plan should follow a 3 steps approach:

1) First analyze whether the IP address under attack is the IoT device address.
2) Tracking the scope of devices infected by the new IoT botnet.
3) Associate detection of new indications of outgoing traffic for IoT addresses for further traffic suppression.

C. Authentication Issues

There is a lack of shared norm for identity and authentication, which makes it challenging for IoT systems to develop trust. Adding new devices or their modules to the IoT environment will increase the risk of intruders breaching critical systems (industrial, governmental, water, etc.) with the resulting cessation of operations, because there are no guidelines.

Similarly, you must be able to safely manage IoT computer user accounts and the programs themselves. Account data is often kept freely, even in large technology companies, which is inappropriate.

D. Privacy Concerns

Consumers demand great, life-simplifying products that work well, pushing software engineers and device manufacturers to work hard in short time cycles to create beautiful, creative devices. This market driven rush basically leads to bad tech, which is published with a minimum security audit at best. There are machines that do not have protection over the network. Printers, routers, coffee machines, webcams, thermostats, and even electronic kettles are amongst others. Consequently, if any of these items are in a home, you need to consider possible safety risks.

For example, Smart TVs were one of the first applications IoT, but later received criticism because of privacy concerns as manufacturer are often tasked with compromising on consumers ' preferences by sending info to advertisers further, which can reveal the users ' interaction habits and also the IP addresses.

IV. Literature Review

Garg et al. (2019) proposed a middleware architecture solution for IoT devices to connect to the network grid. Traditionally, IoT devices use the Internet Protocol (IP) but it is very power expensive. In the new solution proposed, no IoT device is directly connected to the internet, and instead, all the devices are made to connect to a middle gateway, which is further connected to the internet. This solution is better than the traditional approach because no individual device is directly exposed, thus reducing the security vulnerability, and also making sure that the data is only exposed to only relevant stakeholders.

To be able to combat future Mirai DDoS attacks, Yoon et al. (2017) study looked into a new improved secured server for processing the IoT devices data. It consists of variety of security features like the privacy feature which redacts any personally identifiable data, an authentication feature which gives temporary read rights to a specific resource in the architecture, which gets expired after a certain time, this ensures that no unnecessary resource is allowed to have access to any more data then it is required for its functioning. A secured data transmission pipeline is used based on Datagram Transport Layer Security (DTLS) which ensures that no third party can corrupt the data during the transmission, thus making sure that data integrity is maintained. Yoon's server for IoT also has a “security policy” feature which define the various protocols such as firmware upgradation and read/write control for each device in the network and makes sure all the devices are updated.

Blythe et al. (2018) aimed to tackle the security awareness issue amongst the consumers by building a rating index of how secure the device is. This research work was built on Loi et al.(2017) work and improved it by defining the methodology on how to define a security index and also allowing the researchers to get inputs on their work.

In the year 2018, Shah et al. tried to solve the authentication vulnerability issues in IoT by introducing a concept of ”Secure Vaults”.

V. Proposed Solution for Security Issues

To be able to combat various security threats the following solutions are proposed:

- Early Planning: At the system design stage, an existing cyber security team of experts should be involved so that unforeseeable cyberattacks can be prevented. Experts will build a secure authentication system, communication channel encryption and an intrusion detection system.
- Track threats: It is beneficial to keep monitoring and timely respond to information security incidents, and to keep track that they are not getting spread to devices on the network. One way to monitor threats is to manage network traffic from IoT devices, which must go through attack prevention / detection systems.
- Selecting Security Certified Suppliers: Collaborating only with those companies which have adequate safety standards in place for their IoT devices, don't just care only on the functionality of the device and design.
- Provide end-to-end Secured Pipeline: Protecting only the IoT system itself is not enough, we need to talk about data security along the whole course of its lifespan: from creation and transmission to storage and processing. First, it is necessary to protect the sensor itself, then organize the secure transmission of data via an encrypted channel, protected from data modification. And at the storage and processing level-to secure the internal protection from DDoS and ransomware assaults.
- Prepare For Emergencies: Including IoT systems in disaster response strategies, building a safe and catastrophe-proof IoT systems database, ensuring malware can not corrupt data backups, and performing routine disaster recovery tests.

VI. Future of Security in IoT

The problems in the field of network security have been taken seriously by countries all over the world, and their importance can even rise to the level of national security. The future IoT architecture would be a different world where humans and machines co-exist together independently and safely.

In the medium term, the security operations of the Internet of Things will shift from conventional hardware distribution to full service production. Although security protection equipment is indispensable, professional security services, security assessment, security training, and security operations services will also become the focus of future security market development.

Only decentralized, regional autonomy, and flat network structure can meet the future development needs of IoT business. Various IoT devices can establish a highly encrypted, lightweight communication mechanism. Perhaps in the near future, this trust-less point-to-point communication protocol will evolve into a transport layer protocol that is more suitable for the Internet of Things than TCP/IP.

To be to make IoT more decentralized, use of ”Blockchain” can be incorporate. Blockchain technology is a natural decentralized protocol. It uses a distributed database as a carrier, and the rights and obligations between any nodes are equal. Without a central repository, all of the system's data blocks have management roles throughout the system.

Although the use of Blockchain technology has a promising business future in the defense of the Internet of Things, its use in the base network is still in its infancy. There are still many obstacles to be overcome in order to facilitate large-scale commercialisation. First, the IoT terminal needs to have the computing capabilities to encrypt and verify Blockchain transactions. Second, as the Blockchain grows, the demand for node storage space is also increases, and generating a single block requires multiple nodes in the system. Subsequently, recording and verifying communication will increase the delay.

VII. Conclusion

In every aspect of the IoT environment, the security model requires cooperation, communication, and synchronization. Terminals, networks, and systems need to function together and be connected together. For this ideal, IoT security model to be accomplished, each aspect of the IoT environment must be tested for its security in order to ensure reliability.

Review of publications and works clearly demonstrate how much unresolved issues shed light on safety research areas of IoT. There is still no unified concept regarding safety requirements and privacy in such a diverse environment that uses various technologies and different standards of communication. Appropriate solutions need to be developed and implemented. They must be independent of platforms, guarantee the privacy of users, reliable among devices, and adhere to certain security policies. This article will be useful in choosing further areas of research.

References

[1] C. Kolias, G. Kambourakis, A. Stavrou and J. Voas, "DDoS in the IoT: Mirai and Other Botnets," in Computer, vol. 50, no. 7, pp. 80-84, 2017.

[2] "IoTroop Botnet: The Full Investigation - Check Point Research", Check Point Research, 2017. [Online]. Available: https://research.checkpoint.com/2017/iotroop-botnet-full-investigation/. [Accessed: 09- Mar- 2020].

[3] K. Singh and A. Singh, "Memcached DDoS Exploits: Operations, Vulnerabilities, Preventions and Mitigations," 2018 IEEE 3rd International Conference on Computing, Communication and Security (ICCCS), Kathmandu, 2018, pp. 171-179.

[4] O. Grut, "Hackers once stole a casino's high-roller database through a thermometer in the lobby fish tank", Business Insider, 2018. [Online]. Available: https://www.businessinsider.com/hackers-stole-a-casinos-database-through-a-thermometer-in-the-lobby-fish-tank-2018-4.

[5] H. Garg and M. Dave, "Securing IoT Devices and SecurelyConnecting the Dots Using REST API and Middleware," 2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU), Ghaziabad, India, 2019, pp. 1-6.

[6] S. Yoon and J. Kim, "Remote security management server for IoT devices," 2017 International Conference on Information and Communication Technology Convergence (ICTC), Jeju, 2017, pp. 1162-1164.

[7] J. M. Blythe and S. D. Johnson, "The consumer security index for IoT: A protocol for developing an index to improve consumer decision making and to incentivize greater security provision in IoT devices," Living in the Internet of Things: Cybersecurity of the IoT - 2018, London, 2018, pp. 1-7.

[8] F. Loi, A. Sivanathan, H. Gharakheili, A. Radford and V. Sivaraman, "Systematically Evaluating Security and Privacy for Consumer IoT Devices", Proceedings of the 2017 Workshop on Internet of Things Security and Privacy - IoTSP '17, pp. 1-6, 2017.