International Journal of Scientific Engineering and Applied Science (IJSEAS) – Volume-2, Issue-3, March 2016
ISSN: 2395-3470
www.ijseas.com

ADDRESSING SECURITY CHALLENGES IN INTERNET OF THINGS

Mrs. B. Rajeswari, Asst. Prof. (IT), MERI New Delhi, India

Abstract

We are in the era of the Internet of Things (IoT), where digitally connected devices are encroaching on every aspect of our lives, including our homes, offices, cars, etc. More connected devices mean more attack vectors and more possibilities for hackers to target us. It is high time that we address this rising security concern. This paper explains some of the security challenges posed by this growing technology of Internet of Things, which, if not meted out, can be disastrous. It also proposes possible measures to address them.

Keywords: NAT, reverse tunneling, vulnerable, access control, device authentication

I. Introduction

Protection of data has been an issue ever since the first two computers were connected to each other. With the commercialization of the Internet, security concerns have expanded to cover personal privacy, financial transactions, and the threat of cybertheft.

What is IoT?

The definition of Internet of Things (IoT) evolves around the central concept: “a world-wide network of interconnected objects”, where objects can be addressable through unique identity, accessible through Internet and are self organized and repairable. Internet of Things actually implies Machine to Machine (M2M) communication which can be described as “a world of intelligent, adaptive, self organized sensors, actuators, other devices and systems that use various network technologies to connect each and every object of physical world to web of world”.

IoT has become possible with the wide deployment of Wi-Fi networks and the advent of IPv6. It is growing at an alarmingly fast pace and researchers estimate that by 2020, the number of active wireless connected devices will exceed 40 billion. We should realize that it is also becoming an increasingly attractive target for cybercriminals.

II. Security Challenges in IoT

The emerging IoT applications pose severe security challenges some of which are listed below:

1. Addition of Wi-fi enabled devices to local area networks (LANs) without proper security:

This is the biggest threat to IoT security. When TCP/IP-based endpoints are allowed on a LAN without enterprise-level security protocols in place, there is a great deal of risk involved. They may want to exploit every network they can get their hands on. The problem is that firewalls and NATs (Network Address Translation boxes) are a network’s first line of defense against direct host attacks. If suddenly we add a Wi-Fi enabled device inside our LAN, it’s already behind the

firewall. Once this device is installed, it can reach out and connect to malicious servers. This process is known as "reverse tunneling," because the device inside the firewall can make an outbound connection through the firewall, and open a socket connection more easily than an inbound connection. Firewalls do not block most outbound requests, since it would be hard to use most applications otherwise.

2. Absence of effective channels for delivering upgradations and patches for IoT endpoints:

Effective patch deployment is a big problem for IoT. With IoT devices, it is up to the companies that sold them to have a mechanism in place for any kind of patch related security vulnerabilities. The problem is, that may or may not ever happen. Some security breaches may go unnoticed, but others may be discovered and consumers will demand a solution. Even if a patch is issued, there is not an effective channel to reach the majority of devices in a timely fashion.

3. Existence of vulnerable points - Protecting physical access:

Every single device and sensor in the IoT represents a potential risk. Vulnerabilities including poor encryption and backdoors that could allow unauthorized access have been found. With any physical device, there's a chance that a hacker could manipulate it and get into exposed USB ports or a debugger interface. If someone is able to successfully hack at the embedded level into an IoT device's memory and can read the encryption key, every device that is or has been shipped becomes vulnerable. The network is only as strong as its weakest link.

4. Increasing pressure on developers:

When time is of the essence, and all efforts are centered around a quick deployment, security can become secondary. When pressure mounts, IoT devices can enter into market with poor encryption, unpatched operating systems, etc. Thus in the IoT, security capability doesn't exist in many of the devices that suddenly become connected.

5. Lack of trust in hardware

As devices with improper security (not fully tested for loopholes) or low quality are released into the market, people may soon lose trust in devices that enter the market.

III. Dealing with Security Challenges

Security controls have evolved in parallel to network evolution, from the packet-filtering firewalls to more sophisticated systems like intrusion detection and prevention systems (IDS/IPS).These controls attempted to keep malicious activity off of networks and detect them if they did gain access. Moreover, various access control systems were developed to authenticate both the devices and the users sitting behind them, and to authorize those users and devices for specific actions.

More recently, various software verification and attestation techniques often referred to as trusted or measured boot have also been developed. The confidentiality of data always remains a primary concern. Controls such as virtual private networks (VPN) or physical media encryption,

such as 802.11i (WPA2) or 802.1AE (MACsec), are in place to ensure the security of data in motion.

A few points have been suggested to address the security challenges of IoT. They are as given below:

1. The more things that are added to a LAN, the greater the security concerns. The industry will have to create some kind of standard around the expectations of security patches for IoT devices.

2. Security from day one and regular updates have to be emphasized. This is required especially when dealing with immature technologies and underdeveloped markets. In the rush to bring new products and services to market, we always end up with millions of unpatched and insecure computers and mobile devices. Secure IoT devices must be secure by design and impervious from the start. They should also receive vital updates throughout their lifecycle.

3. Access control and device authentication - The principle of least privilege dictates that only the minimal access required to perform a function should be authorized in order to minimize the effectiveness of any breach of security. When the device is plugged into the network, it should authenticate itself prior to receiving or transmitting data. Just as user authentication allows a user to access a corporate network based on user name and password, machine authentication allows a device to access a network based on a similar set of credentials stored in a secure storage area. Creating access controls, and authentication methods that can be implemented on cheap and compact IoT devices without compromising the user experience would be preferred.

4. Be proactive – study the threat

It is vital to study threats and potential attackers before tackling IoT security. The threat level is not the same for all devices. It is necessary to reduce data risk, keep as much personal data as possible from IoT devices and properly secure necessary data transfers.

5. Be prepared for security breaches and create awareness

Always have an exit strategy, a way of securing as much data as possible and rendering compromised data useless without wrecking the IoT infrastructure. It is also necessary to educate customers, employees and everyone else involved in the process about the risks of such breaches.

IV. Conclusion

We are truly in a brave new world that promises many exciting opportunities. Trust is the foundation of the IoT and that needs to be underpinned by security and privacy. As the IoT has become an important part of our lives, its security is one of the major issues that must be addressed so that we live in a secure and safe world of connected things.

V. References

1. Nitesh Dhanjani, “Abusing the Internet of Things- Blackouts, Freakouts, and Stakeouts”, O'Reilly Media, 2015
2. https://en.wikipedia.org/wiki/Internet_of_Things
3. RH Weber, R Weber, “ Internet of Things”, Springer, 2010