© 2017 IJSRSET | Volume 3 | Issue 8 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section : Engineering and Technology

Security Issues in IoT

Afreen Fatima Mohammed
Assistant Professor, Department of IT, Stanley College of Engineering & Technology, Hyderabad, Telangana, India

ABSTRACT

The Internet of things (IoT) is the network of various interconnected physical devices, vehicles, and other items embedded with electronics, software, sensors, actuators, and network connectivity which enable these objects to collect and exchange data. It connects devices embedded in various systems to the internet. When devices/objects can represent themselves digitally, they can be controlled or accessed from anywhere. The connectivity then helps to capture more data from more places, ensuring more ways of increasing efficiency and improving safety and IoT security. Data privacy, confidentiality, data integrity is at potential risk when these devices are connected. As more and more IoT devices are coming in the market, securing IoT systems represents a number of challenges. This paper discusses about various vulnerabilities and threats against IoT and what actions could be taken to provide a more secure IoT.

Keywords: *Malware attacks, Sniffing, Spoofing, Cross-site scripting, Botnet enslaving, Encryption, Data Leakage*

I. INTRODUCTION

The Internet of Things (IoT) refers to an area where everyday objects, places and environments are interconnected with one another via the Internet and these objects are referred as ”things”.According to [2], Industry experts usually define an IoT device as any object connected to the Internet (or to a Local Area Connection, in some cases). Examples include: Smart TVs, Internet connected cars,Wi-Fi routers,Smart cameras,Smart locks (including ones with Bluetooth),Some medical devices,Voice assistants, like Amazon Echo,Smart lights and Fitness bands.

It provides a different way of accessing and controlling these things, which were previously accessible on physical level. One of the common example of a simple IoT object is a thermostat which can determine when people occupy certain rooms it alters level of heating, lighting and other functions in the house accordingly. The emergence of Cloud computing has created the application and device management backbone needed to scale to and support billions of connected objects. Various consumers, governmental and business organisations are trending towards the usage of IoT. Numerous IOT devices are coming in the market and their accessibly may get increased in the next 10 years. But the security of these devices is a major concern. For instance, the Homeowners have to make sure that their home security systems are not accessible by any thieves. In regards to education, schools must make sure that student’s personal information remains private. Businesses must make sure that any device connected to the internet is safe from anyone accessing the company’s database. These are just a few cases of potential security breaches.

II. LITERARTURE SURVEY

The Internet of Things (IoT) is turning out to be an emerging discussion in the field of research and practical implementation in the recent years[3]. As the broadband Internet is now generally accessible and its cost of connectivity is also reduced, more gadgets and sensors are getting connected to it [4]. Hardware consists of sensors and actuators, the Middleware provides storage and computing tools and the presentation provides the interpretation tools accessible on different platforms. In secure systems the confidentiality of the data is maintained and it is made sure that during the process of message exchange the data retains its originality and no alteration is unseen by the system. The IoT is composed of many small devices such as RFIDs which remain unattended for extended times, it is easier for the adversary to access the data stored in the memory[5]. The application of IoT is at in an early stage,but it is going to be evolve rapidly.

IoT is vulnerable to various types of security threats, if necessary security measures are not taken there will be a threat of information leakage. IoT is extremely open to attacks [6], [7], for the reasons that there is a fair chance of physical attack on its components as they remain unsupervised for long time. Secondly, due to the wireless communication medium, the eavesdropping is extremely simple. Lastly the constituents of IoT bear low competency in terms of energy with which they are operated and also in terms of computational capability. The implementation of conventional computationally expensive security algorithms will result in the hindrance on the performance of the energy constrained devices.

It is predicted that substantial amount of data is expected to be generated while IoT is used for monitoring purposes and it is vital to preserve unification of data [8]. Precisely, data integrity and authentication are the matters of concern. From a high level perspective, IoT is composed of three components namely, Hardware, Middleware and Presentation [9]. Hardware consists of sensors and actuators, the Middleware provides storage and computing tools and the presentation provides the interpretation tools accessible on different platforms. It is not feasible to process the data collected from billions of sensors, context-aware Middleware solutions are proposed to help a sensor decide the most important data for processing [10]. Inherently the architecture of IoT does not offer sufficient margin to accomplish the necessary actions involved in the process of authentication and data integrity. The devices in the IoT such as RFID are questionable to achieve the fundamental requirements of authentication process that includes constant communication with the servers and exchange messages with nodes.

Cryptography is the use of codes and ciphers to protect private communication and keep it private from everyone except the intended recipients[11]. The proper use of cryptography through cryptographic ICs is therefore essential to securing all IoT devices, as well as many other electronic products. Any key can theoretically be broken using a brute-force attack with sufficient computing power. The practical approach of modern cryptography is to use a key of sufficient enough length that it can’t be broken without an extraordinary amount of computing power that would be significantly in excess of the value of the contents that the cryptography protects.

III. SECURITY ISSUES

One of the security weakness of IoT is that it increases the number of devices behind network’s firewall. As Based on the review in [1], ten years ago, there was a major concern about protecting computers, five years ago, the concern was about protecting smartphones. Now we have to worry about protecting our car, our home appliances, our wearables, and many other IoT devices. Computers also have security problems but with automatic and easier updates have helped alleviate this problem. But in case of IoT devices, manufacturers are pressured to get their devices in the market , there by ending up on compromising the security. Even if they may offer firmware upgrades for a time, they often stop when they focus on constructing the next device, leaving customers with slightly outdated hardware that can become a security risk.

IoT devices have security concerns, as these devices can easily get attacked by hackers, the data will be hacked and these devices may get controlled or accessed by the hackers. The point is that we have to think about what a hacker could do with a device if he can break through its security. A strong cryptographic algorithms are required to secure IoT devices and to provide secure channel. The following lists different kinds of attacks which have been observed recently and discussed in [2].

3.1 DDoS attacks

In 2016, the Mirai botnet launched one of the biggest DDoS attacks ever recorded. More than 1 terabyte per second flooded the network of Dyn, a major DNS provider, and brought down sites such as Reddit and Airnbnb. But what made this attack so special was that it was the first to be carried out with IoT devices**.** Nearly 150,000 compromised smart cameras, routers and other devices all enslaved into a single botnet, focused on a single target.

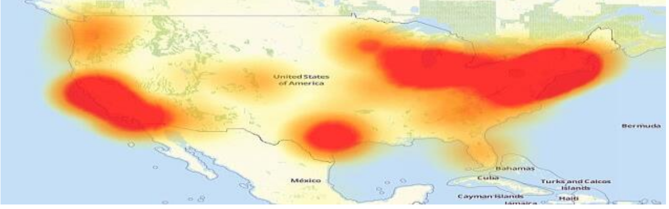


Figure 1. Intensity of DDOS attack done though IoT Devices

The above figure shows the intensity of the attack, done through IoT devices.

Manufacturers usually use a handful of default password and usernames to protect an IoT device. So there will be a few hundreds/thousands of password combinations to protect tens of millions of smart devices. All it took were a few simple lines of code, designed to test each of those default passwords. A device could be hacked and enslaved within a few seconds, so long as the user didn't change the standard login information.

3.2 Unsecure car apps

As Internet connected cars are coming around, it has been observed that hackers are trying to take control of the onboard software , trying to access and open the car locks. Unsecure car apps can allow malicious hackers to control one's car.

IV. INTERNET OF THINGS SECURITY VULNERABILITIES

There are certain IoT's security vulnerabilities, which are discussed in the following sections ,are studied from [2].

4.1 Simplicity and ease of use

Simplicity and ease of use are crucial principles in the IT and electronics industry. Every software and device out there is designed to be as easy to use as possible, so as to not confuse consumers and discourage them from using the product. Unfortunately, this often means that some products cut corners, and don't implement security features .

4.2 Insecure default login credentials

In practice, manufacturers might hide the "Change password/Username" options deep in the UI, out of sight for most users. If each Internet of Things device had a randomized username and password, Mirai might not have happened in the first place.

4.3 Poor software updates

Many Internet of Things manufacturers don't even patch or update the software that came on their devices. If a device has software vulnerability, there's little one can done to prevent an attacker from exploiting it without help from the manufacturer.

4.4 The communication isn't encrypted

Many IoT devices lack basic encryption to hide the data sent between the device and the central server. This can potentially expose the user's personal information, if a malicious hacker can snoop in on his personal information.

Another thing that Internet of Things devices do, is that some of them ask for more permissions than they need to.One time, numerous Amazon Echo users were surprised to see their device ordering dollhouses after a TV anchor said the phrase "Alexa ordered me a dollhouse".In that case, the device had permission to do a purchase all by itself. Each extra permission in an IoT device adds another vulnerability layer which can be exploited**.** The fewer permissions, the more secure your device is.

4.5 Insecure user interface

A device's user interface is usually the first thing a malicious hacker will look into for any vulnerabilities. For instance, he might try to manipulate the "I forgot my password", in order to reset it or at least find out your username or email.

A properly designed device should also lock out a user from attempting to login too many times. This stops dictionary and brute force attacks that target passwords, and greatly secures your device credentials.

In other cases, the password might be sent from the device to the central server in plain text, meaning it isn't encrypted.

4.6 Poor privacy protection

Internet connected devices are data-hungry beasts, but some of them have a greater appetite than others. The less information they have on you, the better, since it limits how much a cybercriminal can learn about you if he hacks the device. As a rule, try to look into what type of data a device will store about you. Be critical of those that harvest data they don't need, such as coffee machines storing user's location information.

V. THE MAIN TYPES OF ATTACKS AGAINST IOT DEVICES

As discussed in [6], smart devices can be hacked in a number of ways, depending on the type of vulnerability the attacker decides to exploit.

5.1 Vulnerability exploitation

Every software has its vulnerabilities.:

Buffer overflows.:This happens when a device tries to store too much data into a temporary storage space. This excess data then spills over into other parts of the memory space, overwriting it. If malware is hidden in that data, it can end rewriting the code of the device itself.

Code injection: By exploiting a vulnerability in the software, the attacker is able to inject code into the device. Most often, this code is malicious in nature, and it can do a multitude of tasks, such as shutting down or taking control of the device.

Cross Site Scripting:These work with IoT devices that interact with a web-based interface. Basically, the attacker infects the legitimate page with malware or malicious code, and then the page itself will infect the IoT device.

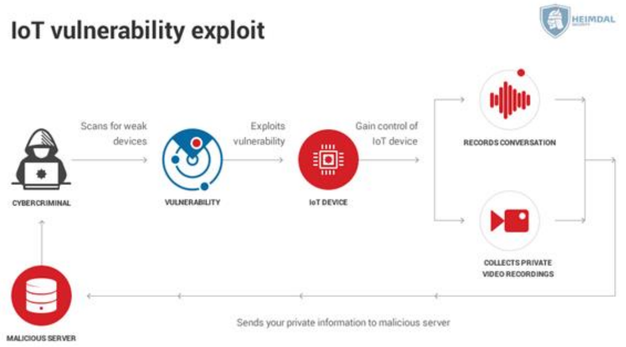

IoT vulnerability exploit
HEIMDAL
Scans for weak devices
Exploits vulnerability
Gain control of IoT device
CYBERCRIMINAL
VULNERABILITY
IoT DEVICE
RECORDS CONVERSATION
COLLECTS PRIVATE VIDEO RECORDINGS
MALICIOUS SERVER
Sends your private information to malicious server

Figure 2.1. Vulnerability exploitation

5.2 Malware attacks

The most frequent and well known malware attacks on PCs target a device’s login credentials. But recently, other types of malware such as ransomware have made their way onto IoT devices.

For one, many base their operating system on Android, so the malware is mostly interoperable, requiring only minor modifications.

Smart TVs and other similar gizmos are most exposed to this kind of threat, since users might accidentally click on malicious links or download infected apps.

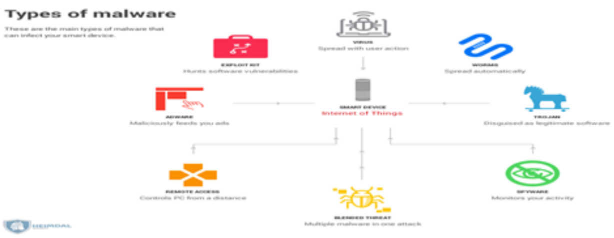

Types of malware
These are the main types of malware that can infect your smart device.
EXPLOIT KIT
Hunts software vulnerabilities
VIRUS
Spread with user action
WORMS
Spread automatically
ADWARE
Maliciously feeds you ads
SMART DEVICE
Internet of Things
TROJAN
Disguised as legitimate software
REMOTE ACCESS
Controls PC from a distance
BLENDED THREAT
Multiple malware in one attack
SPYWARE
Monitors your activity
HEIMDAL

Figure 2.2 Malware Attacks

5.3 Password attacks

Password attacks such as dictionary or brute force target a device’s login information by bombarding it with countless password and username variations until it finds the right one.

Since most people use a simple password these attacks are fairly successful. Not only that, but according to one study, nearly 60% of users reuse the same password. So if an attacker gets access to one device, they get access to all devices.

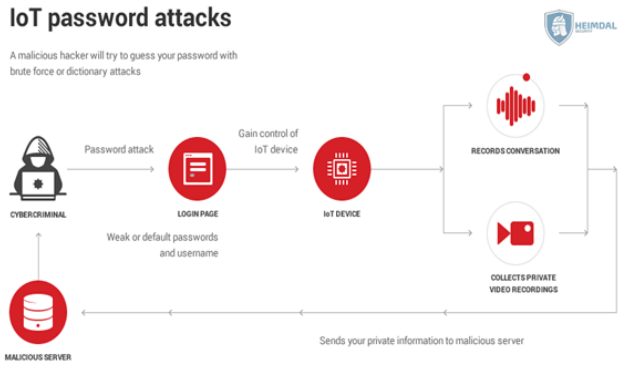

IoT password attacks
HEIMDAL
A malicious hacker will try to guess your password with brute force or dictionary attacks
Password attack
Gain control of IoT device
CYBERCRIMINAL
LOGIN PAGE
IoT DEVICE
RECORDS CONVERSATION
COLLECTS PRIVATE VIDEO RECORDINGS
Weak or default passwords and username
MALICIOUS SERVER
Sends your private information to malicious server

Figure 2.3. Password Attacks

5.4 Sniffing / Man-in-the-middle attacks

In this attack, a malicious hacker intercepts the Internet traffic that goes into and out of a smart device.The preferred target is a Wi-Fi router, since it contains all the of the traffic data sent of the network, and can then be used to control each device connected to it, even PCs or smartphones.

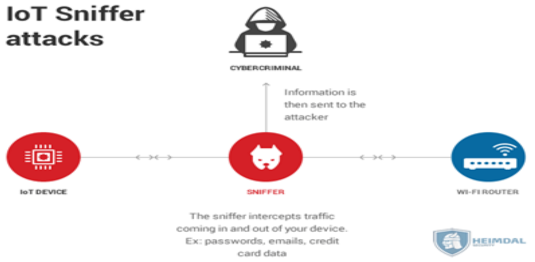

IoT Sniffer attacks
CYBERCRIMINAL
Information is then sent to the attacker
IoT DEVICE
SNIFFER
WI-FI ROUTER
The sniffer intercepts traffic coming in and out of your device. Ex: passwords, emails, credit card data
HEIMDAL

Figure 2.4. Sniffing/Main-in-the middle attack

5.5 Spoofing

Spoofing works by disguising device A to look like device B. If device B has access to a wireless network, then a disguised device A will trick the router into allowing it on the network. Now that the disguised device A can communicate with the router, it can inject malware into. This malware then spreads to all other devices on the network.

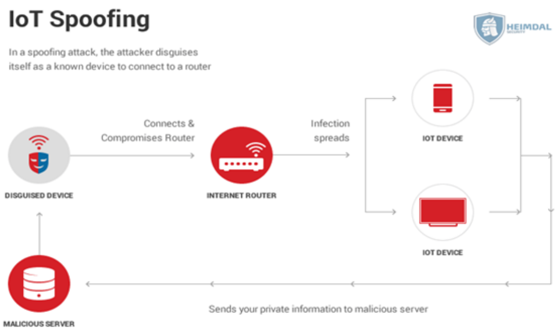

IoT Spoofing
In a spoofing attack, the attacker disguises itself as a known device to connect to a router
HEIMDAL
Connects & Compromises Router
Infection spreads
DISGUISED DEVICE
INTERNET ROUTER
IOT DEVICE
IOT DEVICE
MALICIOUS SERVER
Sends your private information to malicious server

Figure 2.5. Spoofing

5.6 Botnet enslaving

Internet of Things devices are prime candidates for a botnet. They are both easier to hack, and harder to diagnose if they are compromised. Once your device is enslaved, it can be used for a wide variety of cybercriminal activities, such as DDoS attacks, sending spam emails, performing click fraud (basically using the enslaved device to click an ad), and Bitcoin mining. Mirai is the biggest IoT botnet we know about, and it was built on the backs of default passwords and usernames.

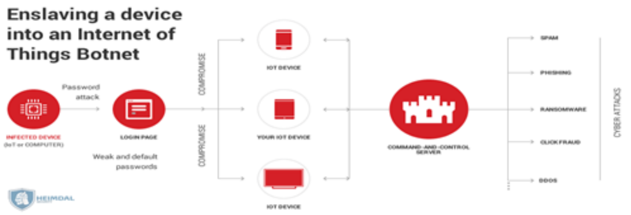

Enslaving a device into an Internet of Things Botnet
Password attack
INFECTED DEVICE (IoT or COMPUTER)
LOGIN PAGE
Weak and default passwords
COMPROMISE
COMPROMISE
IOT DEVICE
YOUR IOT DEVICE
IOT DEVICE
COMMAND-AND-CONTROL SERVER
SPAM
PHISHING
RANSOMWARE
CLICK FRAUD
DDOS
CYBER ATTACKS
HEIMDAL

Figure 2.6. Botnet Ensalving

5.7 Remote access

Taking control of an IoT device does not sound so menacing at first glance. After all, it's not as if a malicious hacker could poison you if he hacked your coffee maker.

But things will quickly get serious if the attacker takes control of your car as you're driving it. This isn't even hypothetical situation, it's actually been done, albeit by cybersecurity researchers. In that example, the whitehat hackers were able to hack into the car's braking system and acceleration.

Some people now use smart locks to secure their homes, but ultimately they're just software on hardware. At DEF CON 2016 (the biggest hacker conference in the world), researchers tested out 16 smart locks, and proved how many of them used very simple security features such as plain text passwords. Others were vulnerable to device spoofing or replay attacks.

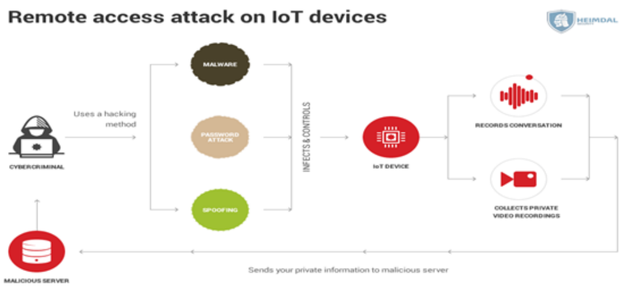


Figure 2.7. Remote access attack

5.8 Data leakage

Smart devices process a lot of personal information, such as:

- ✓ medical data
- ✓ location data
- ✓ usage patterns
- ✓ search history
- ✓ financial information, etc.

Whitehat researchers proved it was able to hack into a smart speaker and analyze data from its sensors to figure out if you are home or not. This would be extremely useful for a burglar seeking empty homes to steal from.

In a high profile case, the German government banned a children's doll because it recorded so much information, it was labeled as a "spying tool".

Devices which leak information from inside the privacy of a house are dangerous for a wide variety of reasons. Recordings of sensitive conversations and intimate acts can then be used as blackmail tools against a person or outright publicized to damage a person's image.

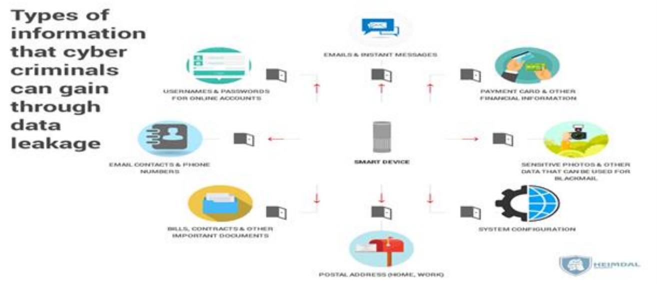

Types of information that cyber criminals can gain through data leakage
EMAILS & INSTANT MESSAGES
USERNAMES & PASSWORDS FOR ONLINE ACCOUNTS
PAYMENT CARD & OTHER FINANCIAL INFORMATION
EMAIL CONTACTS & PHONE NUMBERS
SMART DEVICE
SENSITIVE PHOTOS & OTHER DATA THAT CAN BE USED FOR BLACKMAIL
BILLS, CONTRACTS & OTHER IMPORTANT DOCUMENTS
SYSTEM CONFIGURATION
POSTAL ADDRESS (HOME, WORK)
HEIMDAL

Figure 2.8. Data Leakage

A more worrying scenario is the possibility of hacking IoT devices used in the healthcare industry. In theory, a cybercriminal could hack a pacemaker or an insulin pump, and then demand a ransom from the victim in order to keep the devices working properly.

But sometimes it's the central server that leaks information. Sometimes, companies are the ones that leak information, and not the devices. Such was the case of a teddy bear that spilled recordings from nearly 2 million kids and parents.

This kind of information goes into the company's cloud. If that's compromised, chances are each one of its consumers are also hacked.

One major weakness of Internet of Things devices is that is that many of them send data over unsecured ports. In other words, you can actually see the data live, without requiring a password and username. All it takes to view this data is a paid account at Shodan, and you're set.Another possible way to limit the damage caused by Internet of Things devices is to filter out some of the bad traffic sent over the wider Internet.

ISPs could theoretically identify and filter out any malicious traffic they see on their network. But the process wouldn't be foolproof, and false positives would be a likely possibility.

Another possibility would be for traffic filtering to be applied at a user level. Smart and secure traffic filtering hardware such as Bitdefender Box or Luma Wi-Fi System are making their way onto the market, with more to come. Unfortunately, they are expensive and it remains to be seen if users will consider them as worthwhile investments.

VI. PLAN OF ACTION

In this section the techniques for improving the security of IoT is discussed, as mentioned in [2].

6.1 Change your default passwords and usernames

The Mirai malware is still out there, actively seeking out more IoT devices to enslave into the botnet. Fortunately, it's a fairly simple malware, and can be easily countered by setting up a strong and secure password and changing your default username.

For the best results, password must be set for at least 10 characters long, and use at least 1 capitalized letter, 1 normalized one, 1 number and 1 special character, such as an * or a &. Set different passwords for each device, so that if one device gets hacked, then one can rely on the other ones.

6.2 Update to the latest software

The manufacturers of the best IoT devices release frequent updates to improve functionality and also patch security vulnerabilities. For this reason, try to make sure that the device receives these updates whenever they are available.

Unfortunately, not all manufacturers release updates on a regular basis. Many don't even bother to update them at all, and effectively abandon the customer to his own devices (pun intended).

While selecting a device, look into the update cycle of the product. If update cycles are not mentioned that means reviewers are openly lamenting the non-existent software updates, then chances are that company wants to cut costs. And frequently, that means cutting costs from customer support as well.

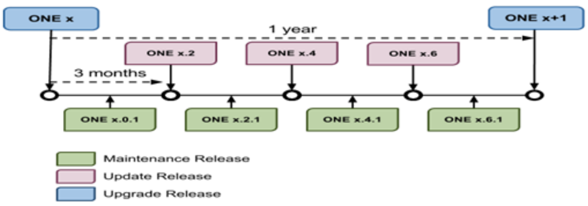
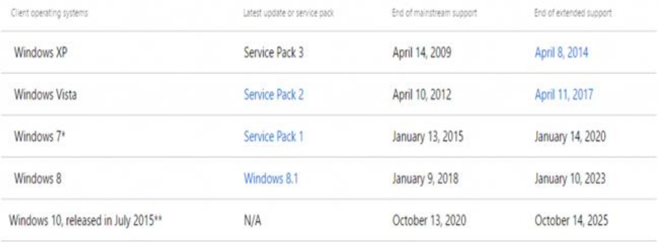


Figure 3.1. Update cycle for a software

This is the update policy for a software called Open Nebula. Not all developers are this thorough in their patching policy, but it should give user an idea as to what constitutes good practice.

On a more similar note, here’s a small sample of Microsoft’s update policy for various Windows software versions.



Client operating systems	Latest update or service pack	End of mainstream support	End of extended support
Windows XP	Service Pack 3	April 14, 2009	April 8, 2014
Windows Vista	Service Pack 2	April 10, 2012	April 11, 2017
Windows 7*	Service Pack 1	January 13, 2015	January 14, 2020
Windows 8	Windows 8.1	January 9, 2018	January 10, 2023
Windows 10, released in July 2015**	N/A	October 13, 2020	October 14, 2025

Figure 3.2. Sample of Microsoft Update Policy

6.3 Login lock settings

Even strong passwords and custom usernames can be vulnerable to a dictionary or brute force attack. These will bombard a login page with countless password combinations, until it hits the right one.iPhones for instance, have a setting which locks the PIN authentication after too many attempts. At the 10th attempt, it completely wipes the device. IoT devices with good built-in security should have a similar option, to ensure their login integrity.

6.4 Two-Factor Authentication

The Internet of Things has lagged behind other services in implementing two-factor authentication, but recently Nest announced it will roll out two-factor authentication to secure it’s thermostats and smart cameras. For the time being, most devices don’t have two-factor authentication, but as the industry matures, the feature will become more and more prevalent.

6.5 Physical weaknesses in IoT devices

Sometimes, all it takes to infect a PC is to introduce a USB stick in it and let Windows auto-run the USB, and by implication the malware. The same principles apply to smart devices. If it has a USB in it, then all a malicious hacker has to do is to plug it in, wait a bit, and that’s it.

6.6 Encryption

Most smart devices work by communicating with a central server, Internet network or smartphone. Unfortunately, the information isn’t properly encrypted in most cases. Either the devices are too small to carry a strong processor, or the manufacturer decided to cut costs (including security features).

Whenever available, it is strongly recommend you activate the option to encrypt the data it sends and receives.

6.7 Create a second network for IoT devices

A good way to secure your smart devices is to create a separate network for them to communicate in. This network isn’t connected to the Internet, and so there is minimal chance for malware to make its way on user devices.This system does come with a set of drawbacks however. If a user want to control smart devices from phone, switch must be made between Wi-Fi’s to control IoT network. In this case, user either have to learn to how automate everything, or use Z Wave switches to go between networks.

6.8 Secure home Wi-Fi

Wi-Fi router is one of the first attack points for a malicious hacker. To make sure it is secure, the following points are suggested:

- Use a strong and secure password.
- Change username, and make it non-recognizable. Don’t make it easy for an attacker to identify which Wi-Fi is yours.
- Set up a firewall to protect Wi-Fi. In most cases, the firewall will be software based, but some routers come with a hardware one preinstalled.
- Disable guest network access for your wireless network.
- A guest network is a second Wi-Fi created from a router, which limits access to user’s “core” network. In theory, it should offer extra security, by isolating guests on the separate network. However, most Wi-Fi routers set up an insecure guest network, which can act as a window to your core Wi-Fi.

6.9 Disconnect the device from the Internet when not in use

Devices such as Smart TVs don’t need to be permanently connected to the Internet. By keeping them off the Internet, user will limit the time interval in which a cybercriminal could attempt to break its security.

6.10 Read the device manual for any security tip you might find

Most people only use a device’s manual during installation, to figure out how to use it. But manuals often contain a lot of useful tips and tricks that can improve the performance of a device and make it more secure

6.11 Download security applications

Some smart devices such as TV's are powerful enough to run apps. Even simple, free versions of antivirus apps can significantly boost your security. For the best results, use the paid version of an antivirus app, since it will unlock its full functionality.

6.12 Use a hardware solution to secure IoT network from outside attacks

A dedicated security solution for IoT network can make all the difference between an infected or clean device. There are quite a few security solutions available, even if the market is not as developed as it is for desktop or mobile.

VII. CONCLUSION

In the near future Internet of Things will be an essential element of our daily lives. Numerous energy constrained devices and sensors will continuously be communicating with each other the security of which must not be compromised. Cryptographic algorithms can be applied. Choose an appropriate cryptographic algorithm which is best suitable to be adopted in IoT applications

VIII. REFERENCES

[1]. www.networkworld.com/article/3166106/internet-of-things/4-critical-security-challenges-facing-iot.html

[2]. https://heimdalsecurity.com/blog/internet-of-things-security/

[3]. Muhammad Usman , Irfan Ahmed† , M. Imran Aslam† , Shujaat Khan and Usman Ali Sha ,"SIT: A Lightweight Encryption Algorithm for Secure Internet of Things",IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 8, No. 1, 2017

[4]. R. Want and S. Dustdar, "Activating the internet of things [guest editors' introduction]," Computer, vol. 48, no. 9, pp. 16–20, 2015.

[5]. T. Karygiannis, B. Eydt, G. Barber, L. Bunn, and T. Phillips, "Guidelines for securing radio frequency identification (rfid) systems," NIST Special publication, vol. 80, pp. 1–154, 2007.

[6]. M. A. Simplicio Jr, M. V. Silva, R. C. Alves, and T. K. Shibata, "Lightweight and escrow-less authenticated key agreement for the internet of things," Computer Communications, 2016.

[7]. L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," Computer networks, vol. 54, no. 15, pp. 2787–2805, 2010.

[8]. F. Xie and H. Chen, "An efficient and robust data integrity verification algorithm based on context sensitive," way, vol. 10, no. 4, 2016.

[9]. J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of things (iot): A vision, architectural elements, and future directions," Future Generation Computer Systems, vol. 29, no. 7, pp. 1645–1660, 2013.

[10]. S. Wang, Z. Zhang, Z. Ye, X. Wang, X. Lin, and S. Chen, "Application of environmental internet of things on water quality management of urban scenic river," International Journal of Sustainable Development & World Ecology, vol. 20, no. 3, pp. 216–222, 2013.

[11]. http://iotdesign.embedded-computing.com