International Research Journal of Computer Science (IRJCS)
Issue 12, Volume 3 (December 2016)
ISSN: 2393-9842
www.irjcs.com

Internet Security Threats types and Its Prevention in Internet of things

Johnbee

Abstract-- The "Internet of Things", commonly referred to as the "IoT", is a phrase that loosely describes the growing body of Internet-connected devices, gadgets, and other items that do not fit the traditional concept of a "computer". Examples of IoT device types include wearable technology (e.g., health monitors), networked home appliances, IP security cameras, connected vehicles, environmental controls, smart watches, and even smart light bulbs. Homes and offices now frequently have an array of different devices and device types simultaneously communicating with and exchanging data over the Internet. Because the Internet is so easily accessible to anyone, it can be a dangerous place. Know who you're dealing with or what you're getting into. Predators, cyber criminals, bullies, and corrupt businesses will try to take advantage of the unwary visitor. This paper deals with different types of threats and its prevention methods in IoT.

INTRODUCTION

TYPES OF INTERNET SECURITY THREATS AND ITS PREVENTION

1. VIRUSES:

A computer program developed intentionally to corrupt the files, applications, data, etc. of a computer. It gets from storage devices, internet, USB etc. Without the knowledge of the user, and exploits the system mercilessly.

PREVENTION:

1. *Beware of downloading applications, files mp3, mp4, gif, etc., from the sites and also from the attachments of the e-mails.*
2. *Use/buy certified and secured products from the vendors.*
3. *Keep a habit of regularly scanning the system also keeps updating the virus scanning tools/software.*

2. HACKERS:

An intruder or probably an enemy of a particular entity with malicious intentions creates and injects malicious content to steal sensitive information or money or sometimes to destroy some part of data or applications.

PREVENTION:

1. Initiate strong encryption technology on the website.
2. Secure your websites with digital SSL certificates.
3. Avoid exposure to unauthenticated access, unnecessary access to employees or users.
4. Install tools like anti malware, anti-phishing for scanning to detect vulnerabilities.

3. PHISHING THREATS:

Phishing means, when any website impersonates itself as a trustworthy and well established brand most probably to steal the information as well as money by misleading the online users. DNS farming attack, another type of phishing attack corrupts the DNS server because of which the client is automatically transferred to an imposter website (an illegal website having the look and feel of the original website).

Prevention:

1. Install updated version of antivirus tool.
2. Do not click blindly on the hyperlinks appearing in the e-mail that came from the unknown sources.
3. Secure your website with anti-spam and phishing detection tools.
4. Always look for the “https:” before trusting the website especially, before providing credit card information and personal information.
5. Guard the walls of the server with updated firewalls.
6. Website owners should establish trust & reduce risk of Phishing Attack by implementing EV Certificate.

4. INFECTED WEBSITES:

Be it in emails or ads on the websites or the normal looking website, you might never know what it is stored in it. These can be the sources of viruses, Trojans and malwares; by clicking on the link you install them in your system.

PREVENTION:

Avoid visiting to the suspicious websites specially those, which are not secured with digital certificates, install appropriate antivirus, anti- malware, anti-phishing tools.

5. SPYWARES, ADWARE, TROJANS:

Spywares, as the name suggests itself, are software that secretly tracks one's online behavior, and installs malicious software without user's concern. Adware's, Trojans also interpret the same behaviour. Downloaded applications, corrupted CDs can be counted as their sources. They may display loads of disturbing ads and in turn slowing down one's internet, they can pass one's information to others.

PREVENTION:

1. Present your website with Symantec SSL certificates that come with Norton Secured Seal (available separately) that scans regularly your website against viruses, spyware, Trojan horses, worms, adware or other malicious programs and will notify you by email.
2. Careful before downloading any content from the suspicious or even from the unsecured website.
3. Ignore clicking on the ad links as these behaviours are marked by the spywares and further leads to unknown threats.

6. INSECURE WIRELESS ACCESS POINTS:

Connecting to a wireless network like say connecting to a broadband router is not that safe. Devices like, laptop, PDA and mobile those connect with wireless connections are prone to get affected by several threats. Most common attacks when exposed to insecure wireless access points are: accidental association, malicious association, ad-hoc networks, identity theft, man-in-the-middle-attack, Denial of Service (DOS), network injection and cafe latte attack.

PREVENTION:

1. Keep your Service Set Identifier ID hidden.
2. Block the non-approved MAC addresses so as to avoid sniffing of the MAC addresses and spoof the address.
3. Implementing regular WEP (Wired Equivalent Privacy) encryption, this is originally designed for securing wireless networks.
4. WPA (Wi-Fi Protected Access), a better technique than WEP provides stronger protection through encrypted passwords.
5. TKIP (Temporal Key Integrity Protocol) includes techniques like: per-packet key mixing along with the re-keying.
6. Use SSL for the end-to-end encryption.
7. Entertain network encryption through software's from trusted authorities like: Cisco's Secure Access Control Software, Microsoft's Internet Authentication Service and so on.

7. SOCIAL ENGINEERING:

Tricks like pretexting; quid pro quo, tailgating etc. are accomplished in social engineering. Where quid pro quo refers to the old method, in which users are trapped by bogus offers in return they have to provide their personal or bank account information whereas pretexting refers to the theft of the personal and other such sensitive info by impersonating oneself as a legal authority.

Prevention:

1. Implement strict measures against unauthorized access either from the user side or even from the employee side.
2. Educate your employees as well customers regarding various tricks and techniques of social engineering, and warn them to not providing any kind of personal information to irrelevant entity.

8. BACK DOORS:

Back doors just as the name suggests are the piece of code or programs that enters into the website without the knowledge of the website owner and that too by defeating the security restrictions.

PREVENTION:

1. Purchase products from the authorized vendors only that too after ensuring the certainty of the products.
2. After completing the applications or the software's, test thoroughly in case if back doors are added in to the code.

9. BRUTE FORCE:

Brute force attack also known as exhaustive key search attack, in which the encrypted data or messages are hacked, and then with the use of software they are broken down to acquire the messages, user IDs and passwords. Once a hacker is able to gain the access of the privileged authority, he/she can install a back door for future use even if the passwords or the user IDs keep changing.

PREVENTION:

1. To secure the passwords and the other sensitive data, implement unbreakable encryption technology and also preserve the keys safely.
2. Keep the passwords long and keep changing them from time to time.
3. Frequently scan or test the system to detect vulnerability.
4. Literate users about security precautions.

10. DENIAL OF SERVICE (DOS):

Denial of service is a very ancient type of attack, in which a web server is hanged up because of sending overwhelming number of requests. DOS attack has a sibling also called DDOS (distributed denial of service) in which the attacker simultaneously launches a dozen of requests to a number of servers until they are hanged up.

PREVENTION:

1. Keep a data backup and place them at a safer place.
2. Install tools that can test the capacity of your web server against the DOS or DDOS attacks.

11. EXPOSURE TO KNOWN VULNERABILITIES:

Sometimes an attacker may exploit the website to known vulnerabilities with the malicious intention of breaking down into the main access system. The sources of such vulnerabilities can be softwares, hardware, web servers or the firewalls. With exploiting the websites, a hacker can even change the contents of the web pages and so on.

PREVENTION:

1. Disable or uninstall the unused applications on the servers or on the firewalls.
2. Keep updating the software and patches.
3. Purchase software from the trusted vendors who keep the updated versions of the software.
4. To detect the bugs in the website that can be vulnerable to security breach like protocol flaws or bug in the coding, scan your website regularly.

12. PASSWORD GUESSING:

This is a very serious type of threat, in which the passwords are guessed to gain access to a system by trying all the possible combinations.

PREVENTION:

1. Make stronger the password policies.
2. Apply stringent access controls like disable the user ID after several failed login attempts.
3. Change the passwords on the sensitive network components.
4. Password must comprise of long & short alphabets, numerical and sensitive characters.

13. HIJACKING:

When attacker injects malware and takes control of the system and redirects user to another website or home page is called Hijacking. This attack massively takes place over the remote computers. There are mainly three types of hijacking and they are:

1. Network hijacking: Man-in-the-middle-attack can be counted as the network hijacking. In this attack, a perpetrator hijacks the connection of the two communicators, without their knowledge, intercepts their messages, and modifies the message and relay back to them. The two victims think that they are communicating with each other only but the actual scenario is totally different.

2. Browser hijacking: Also known as DNS hijacking, takes the requester to the adulterated site, when requested for the valid one. The attacker infects the DNS server itself, so that each time a user requests for the legitimate website, he/she ends up at the fake or disturbing site.

3. Website hijacking: Here, the attacker only has to register a domain name almost similar to that of the actual one. Now, whenever a user types address of that website either by mistake he/she will be redirected to the corrupted site, in many of the cases to porn sites.

PREVENTION:

1. For remote access, strong authentication measures should be implemented. For sessions, periodic re-authentication should be enforced.
2. Firewalls should be installed as and when required.
3. Monitor the network traffic and vulnerable interruptions on a regular basis.
4. Scanning tools should be installed in order to prevent the on-going vulnerabilities.
5. For the most sensitive data, a strong end to end encryption should be implemented.

14. RANDOM DIALLING OR WAR DIALLING:

Random dialling or war dialling means dialling of phone numbers randomly, just to see that which one of them is a modem connected to the computer and is available to bypass the firewall and other security technologies.

Prevention:

1. Ensure that all the modems are secured and authenticated with strong encryption technology.
2. Modems should be protected by centralizing them at single physical location in order to prevent other network segments from being attacked.
3. Set the modem to the dial-back mode to prevent unauthorized third party.

15. SNIFFERS:

They are the software's that monitor the network to keep a track of keystrokes and the data eavesdropping over the networks.

Prevention:

1. Proper encryption technologies should be implemented.
2. Monitor your network traffic to avoid any kind of intrusions.
3. Use strong scanning tools to scan the vulnerabilities that may harm your website.
4. Enable strong end-to-end encryption techniques for protecting highly sensitive data and applications

16. SPOOFING:

It refers to a computer or a network that is impersonating as a legal network. Hence, corrupt other networks or computers by misleading the signals of the network. E-mail spoofing means the e-mail reader is misguided to irrelevant path other than that of the original destination, generally by spam e-mails with the help of SMTP and telnet protocols.

Prevention:

1. Ensure and enforce strong authentication as well as encryption techniques for securing the communications, messages transmitted, data and session.
2. Firewalls should be installed as and when required.
3. Keep a sharp eye on the network traffic. Regulate the traffic monitoring.

17. Trojan horses:

Trojan horses are similar to the normal programs but are slightly different in a way as they contain additional malicious and viral functions or piece of codes. These are installed with an intention of theft of the information, gaining control over the system and sometimes impersonating the login screens to get the entire user IDs and the passwords. Sources of the Trojans generally are e-mail attachments and back doors.

PREVENTION:

1. Strict security measures should be taken to avoid any kind of installation of the malware or Trojans. Thorough testing should be a compulsion before a product goes on the platform.
2. Programs used should be tested thoroughly.
3. Sensitive data should be protected through encryption and also the employees and other staff members should be educated regarding the avoidance of the Trojan horses in organization.
4. Customers should be warned about the common risks (like in opening an email from untrusted source, downloading, or purchasing a software product from unauthorized vendors.)
5. These were some of the threats that have caused a lot catastrophe to a number of businesses as well as to the customers/users. As internet is advancing day by day so are the threats.

CONCLUSION

Although there is an ever-growing tendency of cyber-attacks targeting IoT devices, based predominantly on plenty of warnings from distinguished security experts, most of the companies nowadays do not envisage adequate privacy and security safeguards for their Internet-enabled sensor products. Only 33% of surveyed executives express firm belief that their products are resilient enough to withstand persistent cyber-threats.

Reportedly, medical device manufacturers and home automation are among the most endangered industry segments, as far as cyber security is concerned. It is really worrying, given the anticipated sky-high demand for IoT products in these sectors—the expected growth is estimated to reach the astounding figure of over 19 million patients by 2018. A survey by Capgemini Consulting shows that 71% of consumers' choices for purchasing IoT products will be affected by security concerns. Firms in some areas, for example, industrial manufacturing and smart metering, will be affected to a greater extent than other segments like home automation and automobiles.

REFERENCES

1.http://study.com/academy/lesson/what-is-internet-security-privacy-protection-essentials.html.
2.https://www.linkedin.com/pulse/types-internet-security-threats-its-prevention-mr-ooppss.
3.http://www.kaspersky.com/au/internet-security-center/threats/viruses worms.http://resources.infosecinstitute.com/security-challenges-in-the-internet-of-things-iot/

