International Journal of Computer (IJC)
ISSN 2307-4523 (Print & Online)

http://ijcjournal.org/

Responding to and Preventing Threats to Cybersecurity When Utilizing the Internet of Things

Jaipratap Singh Grewal*

University of Toronto, 27 Kings College Circle, Toronto M5S 1A1, Ontario, Canada
Email: jp.grewal@mail.utoronto.ca

Abstract

The Internet of Things has the potential to connect billions of devices and is developing at a tremendous rate. Billions of people will be able to connect through it. However, this system increases the vulnerability of each device, as a breach in the security of a single connected device will compromise the rest of the system's safety. A hacker or virus may be able to get access to multiple connected devices by targeting just one of the many devices online. Therefore, such attacks will have a much larger reach compared to the attacks on individual systems. Preventing or being able to react to this issue is important, as the safety and privacy of people must be protected. Society needs a proper protocol that can protect these connected devices from cyber-attacks. This paper aims to propose solutions that will either prevent or respond to these cyberattacks, thus making systems more secure.

Keywords: Device Security; Sensors and Devices for IoT; Security and Privacy; Social impacts; Device-to-Device Communication; Machine-to-Machine Communications; Cyber-Physical Systems.

1. Introduction

We live in a world with constantly changing technologies. One of the newer technologies is the Internet of Things (IoT), which is a system of everyday objects that are connected throughout the Internet. These objects are able to "communicate" with each other by sending and receiving data constantly. A simple example of such a device is a smart air conditioner - one that switches on with one command from your mobile device. The prominence of the aforementioned topic in the tech world is demonstrated by the projected forecast of over a 100 billion IoT connections by 2025, thus showing the large reach this system will have in the coming future.

---

* Corresponding author.

The following paper is based on a personal investigation of a Distributed Denial of Service (DDoS) attack on the website, "Krebs on Security", and the solutions thus found have been presented in a general light [1-14]

2. Threats

As is the case with every interconnected system, the IoT also provides many nodes for threats to enter through. On top of this, utilizing the IoT means that human communications lessen, becoming more and more indirect. This gives rise to a huge number of security problems [4, 13].

2.1. Security Vulnerability

Attacks can exploit any one weakness in the secure network and thus obtain credentials needed to compromise a part of if not the entire IoT device, and may also enable a pathway to secure, private information. Such compromises in security may even lead to cases of physical danger – as was the case when a JEEP Cherokee's dashboard connectivity system was hacked, and the engine, brakes, and steering were compromised [8, 9, 15-19].

2.2. Sleep Deprivation

Sleep deprivation attacks, targeting the susceptibility of batteries in devices to drainage, may be launched by attackers [20].

2.3. System Network Layer

The most widely known security risk involves targeting the system's network layer and achieving access to the other devices connected to that pertinent device using the internet, thus leading to the probability of a small-scale attack escalating into a large-scale one [21].

2.4. Phishing

- Fraudsters may gain access to the secure protocol by impersonating legitimate entities, thus tricking users into providing access or secure information.
- Attackers may use malware (viruses, worms, trojans) to delete/corrupt data, monitor user activity, disrupt important system operations or steal one's secure private information (SINs, SSNs etc.) [16, 17, 20, 22-24].

2.5. Concern

Threats are often overlooked, and users usually believe that their privacy is automatically protected (without taking any additional measures to strengthen their security). With the large number of devices that will potentially be connected in the future, the effect of a security breach will be amplified. The concept of the Internet of Things is built on connected devices, so if one becomes corrupted, the other connected devices would

be susceptible to corruption as well, thus making the security of the network as a whole and that of individual devices a topic of prime importance [15].

3. Measures and solutions to respond to and/or prevent and/or nullify attacks and risks

3.1. Intrusion Detection and Prevention System (IDPS)

An IDPS monitors the computer system and the network to which it is attached, detecting, blocking and reporting any suspicious-looking activity [25].

3.2. Strong Authentication

Strong authentication methods including firewalls, randomly generated passwords (like the ones one's browser may provide for a website), secure token-based authentication, and biometric authentication-based certificate (including the green lock you see beside a website link in your browser) etc. act as gatekeepers, keeping away unwanted traffic thus lessening the chances of an attack on one's secure network [25-27].

3.3. Device-Management Agent Integration

Integration of a device-management agent into products allows them to share information with a security management system. Such a setup keeps track of failed attempts at accessing your system and launching denial-of-service (DoS) attacks [25, 28, 29].

3.4. Virtual Private Networks (VPNs)

VPNs work by using hackers' techniques back on them. A VPN connects one's server to a proxy server before one starts using the internet and in this way one's information is saved even from companies which utilize it for commercial purposes [30-32].

3.5. Access Control Lists (ACLs)

ACL is a computer filing system that identifies the users logging on to a system and grants them access. ACLs also permit what can be done on networking systems.

- By identifying the people logging onto a system, it will prevent unauthorized people from obtaining access.
- Another important thing to recognize about ACL systems is that they control what activity can be done on a system. This helps prevent suspicious activity that may harm the system.
- For e.g. Connecting to one's school's Wi-Fi may prevent access to certain websites etc. [33-35].

3.6. Encryption

Encryptions are codes that can be ciphered by authorized people only. Having encryptions will really make sure that the right people are entering a network. Many times, cyber-attacks consist of people hacking into accounts.

Thus, we need to make sure that authorized people are granted access, and that not just anyone gets into closed off areas. Without these codes, we are risking the chance of potentially letting dangerous people into systems [17, 33, 36].

3.7. Log Monitoring

Log monitoring means keeping track of events that take place on a network.

- If a cyberattack is ever to occur, this process can help detect where it happened or how. This also helps detect suspicious activity, which is something that people do not catch when detecting cyber security issues.
- This connects back to the ACL system where only certain activity is allowed on a network. With these two ideas combined the security is improved. This way, there will only be certain activity allowed on a network and all such activities will be recorded. All this helps prevent hackings etc. and in the case one occurs helps enhance hacker and malware recognition. [17, 33, 37].

3.8. Complications Relating to Software Use

A common problem relating to firewalls, anti-viruses and other risk averting programs is that these take up a lot of valuable disk space and require a lot of processing power to run. A solution to this problem is to utilize security protocols and systems which are specifically built to protect the system from the threats it is most vulnerable to (based on its software and architecture) [25, 38, 39].

4. Bringing out the True Power of the Internet of Things

To bring out the true power of IoT, physical security solutions need to be programmed to work together with cyber solutions. This is because

- coordinating information amongst security systems proffers a more comprehensive view of activities all around the network.
- Machine-to-machine (M2M) communications cut short the response time, thus preventing loss on a larger scale if any.
- For e.g. If the ACL system detects the utilization of a stolen badge, automated actions may include cutting off access to resources, alerting security, and last but not the least using a nearby security camera for identification of the suspect [38].

5. Conclusion

Though the Internet of Things makes life easier, it can also make things difficult security wise. The Internet of Things adds complications to security due to the additional risk of billions of potential attack vectors, but it still strengthens security due to its far better intelligence gathering and automation of responses based on policy. Using smart solutions and paying attention to even the smallest of details can help make a difference. Tech side

of things aside, making people morally strong rather than passwords gives society a much better chance of prevailing over attacks on privacy and secure information.

Thus, with an all-inclusive approach to security, organizations can make the most of the IoT to improve upon finance, economics, safety and every other field imaginable in remarkable ways [40, 41].

Acknowledgements

I am thankful to Yale University and the Yale Young Global Scholars (YYGS) Program for introducing me to the field of the Internet of Things and for giving me the opportunity to conduct research on the same. I am also thankful to Olivier Trottier and Analea Cuevas-Ferraras for guiding me on the topic during my two-week stint at the YYGS 2017 Program.

References

[1] Karen Rose, Scott Eldridge, and Lyman Chapin. "The Internet of Things: An Overview." Internet: https://www.internetsociety.org/wpcontent/uploads/2017/08/ISOC-IoT-Overview-20151221-en.pdf, Oct. 2015.

[2] Huawei Technologies Co., Ltd. "Harnessing the Power of Connectivity." Internet: https://www.huawei.com/minisite/gci/files/gci_2017_whitepaper_en.pdf, 2017.

[3] Chuck Leddy. "IOT SECURITY: HUGE PROBLEMS AND POTENTIAL SOLUTIONS". Internet: https://www.cintas.com/ready/healthy-safety/iot-security-huge-problems-and-potential-solutions/, Jun. 26, 2016.

[4] J. H. Ziegeldorf, O. Garcia Morchon, and K. Wehrle. (2013, June). "Privacy in the Internet of Things: threats and challenges." Security and Communication Networks. [Online]. Available: https://doi.org/10.1002/sec.795

[5] Irfan Saif, Sean Peasley, Arun Perinkolam. "Safeguarding the Internet of Things: Being secure, vigilant, and resilient in the connected age". 27 July 2015. Internet: https://www2.deloitte.com/insights/us/en/deloitte-review/issue-17/internet-of-things-data-security-and-privacy.html, Jul. 27, 2015.

[6] Deloitte Touche Tohmatsu Limited (US). "Data security and the Internet of Things". Internet: https://www.youtube.com/watch?v=HBCFUEGgQo8, Aug. 4, 2015

[7] Brian Krebs. "Krebs on Security". Internet: https://krebsonsecurity.com, Jul. 18, 2018.

[8] Paul Szoldra. "Akamai Kicked Journalist Brian Krebs' Site off Its Servers after He Was Hit by a 'record' Cyberattack.". Internet: https://www.businessinsider.in/Akamai-kickeda- journalists-site-off-its-servers-after-he-was-hit by-a-record-cyber-attack/articleshow/54473344.cms, Sep. 22, 2016.

[9] Paul Szoldra. “Here’s How the ’Internet of Things’ Is Being Used for Major Cyberattacks on the Enterprise.”. Internet: https://www.businessinsider.in/Hereshow-the-Internet-of-Things-is-being-used-for-major-cyberattackson-the-enterprise/articleshow/54987418.cms, Oct. 21, 2016.

[10] I. H. Lim, S. Hong, M. S. Choi, S. J. Lee, T. W. Kim, S. W. Lee, B. N. Ha. "Security Protocols Against Cyber Attacks in the Distribution Automation System". IEEE Transactions on Power Delivery, 30 Oct. 2009.

[11] Alec Scott. (2017, May) "8 ways the Internet of things will change the way we live and work". The Globe and Mail. [Online]. Available: https://www.theglobeandmail.com/report-on-business/rob-magazine/the-future-is-smart/article24586994/

[12] Benson Houghland. (2014, Dec.). "What is the Internet of Things? And why should you care?". TEDx. [Online]. Available: http://ed.ted.com/on/roPxRePe\#finally

[13] Ernst and Young Inc. (2015, Mar.). "Cybersecurity and the Internet of Things". EY. [Online]. Available: https://www.ey.com/Publication/vwLUAssets/EY-cybersecurity-and-the-internet-of-things/\%24FILE/EY-cybersecurity-and-the-internet-of-things.pdf

[14] Eyal Ronen, Colin O’Flynn, Adi Shamir and Achi-Or Weingarten. “IoT Goes Nuclear: Creating a ZigBee Chain Reaction”. [Online]. Available: http://iotworm.eyalro.net

[15] Chris Folk, Dan C., Wesley K. Kaplow, James F.X. Payne. “The Security Implications of the Internet of Things.” Internet: https://www.afcea.org/committees/cyber/documents/InternetofThingsFINAL.pdf, Feb. 2015.

[16] Kurt Thomas, Frank Li, Ali Zand, Jacob Barrett, Juri Ranieri, Luca Invernizzi, Yarik Markov, Oxana Comanescu, Vijay Eranti, Angelika Moscicki, Daniel Margolis, Vern Paxson, Elie Bursztein. "Data Breaches, Phishing, or Malware? Understanding the Risks of Stolen Credentials" in Proc. CCS'17, 2017.

[17] Teemu Väisänen, Lorena Trinberg, and Nikolaos Pissanidis. (2016). "I accidentally malware - whatshould I do... is this dangerous?: Overcoming inevitable risks of electronic communication". NATO Cooperative Cyber Defence Centre of Excellence. [Online]. Available: https://ccdcoe.org/sites/default/files/multimedia/pdf/I\%20acc-\\identally\%20malware.pdf

[18] Aaron M. Kessler. (205, Jul.). "Fiat Chrysler Issues Recall Over Hacking". The New York Times. [Online]. Available: https://www.nytimes.com/2015/07/25/business/fiat-chrysler-recalls-1-4-million-vehicles-to-fix-hacking-issue.html

[19] Bernie Woodall, Joseph Menn. (2015, Jul.) "Fiat Chrysler U.S. to recall vehicles to prevent hacking". Reuter. [Online]. Available: https://www.reuters.com/article/us-fiat-chrysler-recall/fiat-chrysler-u-s-to-

recall-vehicles-to-prevent-hacking-idUSKCN0PY1U920150724

[20] Tristan O' Gorman. "A Primer on IoT Security Risks." Internet: https://securityintelligence.com/a-primer-on-iot-security-risks/, Feb. 8, 2017.

[21] euronews Knowledge. "Internet if Things: Cyber crime on the rise". Internet: https://www.youtube.com/watch?v=z67DCxIE_6U, Feb. 3, 2016.

[22] Paul Szoldra. "Inside the 72-hour hacking contest to take over your 'smart' home.". Internet: https://www.businessinsider.in/Insidethe-72-hour-hacking-contest-to-take-over-your-smarthome/articleshow/54158477.cms, Sep. 8, 2016.

[23] John Markoff. (2016, Nov.). "Why Light Bulbs May Be the Next Hacker Target". The New York Times. [Online]. Available: https://www.nytimes.com/2016/11/03/technology/why-light-bulbs-may-be-the-next-hacker-target.html?_r\=0

[24] Eyal Ronen, Colin O'Flynn, Adi Shamir and Achi-Or Weingarten. "IoT Goes Nuclear: Creating a ZigBee Chain Reaction". [Online]. Available: http://iotworm.eyalro.net

[25] Alan Grau. "How to Build a Safer Internet of Things.", IEEE Spectrum: Technology, Engineering, and Science News. Internet: https://spectrum.ieee.org/telecom/security/how-to-build-a-safer-internet-of-things, Feb. 25, 2015.

[26] Margaret Rouse, "What Is digital signature?". Internet: https://searchsecurity.techtarget.com/definition/digital-signature

[27] Garrett Gross. "Botnet Detection and Removal: Methods and Best Practices". Internet: https://www.alienvault.com/blogs/security-essentials/botnet-detection-and-removal-methods-best-practices, Nov. 3, 2015.

[28] Steve Zurier. "5 Tips For Preventing IoT Hacks". Internet: http://www.darkreading.com/endpoint/5-tips-for-preventing-iot-hacks-------/d/d-id/1327270, Oct. 24, 2016.

[29] Sam Thielman. "Can we secure the internet of things in time to prevent another cyber-attack?". Internet: https://www.theguardian.com/technology/2016/oct/25/ddos-cyber-attack-dyn-internet-of-things, Oct. 25, 2016.

[30] Microsoft Corporation. "How VPN Works". Internet: https://technet.microsoft.com/pt-pt/library/cc779919(v=ws.10).aspx

[31] Larry Greenemeier. "Seeking Address: Why Cyber Attacks Are So Difficult to Trace Back to Hackers". Internet: https://www.scientificamerican.com/article/tracking-cyber-hackers/, Jun. 11, 2011.

[32] Business Insider. "IoT Cyber Security Hacking Problems". Internet: https://www.businessinsider.in/iot-cyber-security-hacking-problems-internet-of-things-2016-3?r=US&IR=T, Mar. 3, 2016.

[33] Ajit Jha and Sunil M. C. "Security Considerations for the Internet of Things". Internet: http://www.larsentoubro.com/media/30090/whitepaper_security-considerations-for-internet-of-things.pdf, 2014.

[34] Margaret Rouse. "What Is Access Control List (ACL)?". Internet: https://searchsoftwarequality.techtarget.com/definition/access-control-list

[35] Andy Greenberg and Kim Zetter. "HOW THE INTERNET OF THINGS GOT HACKED". Internet: https://www.wired.com/2015/12/2015-the-year-the-internet-of-things-got-hacked/, Dec. 28, 2015.

[36] Margaret Rouse. "What Is Encryption?". Internet: https://searchsecurity.techtarget.com/definition/encryption

[37] Margaret Rouse. "What Is Log Management?". Internet: https://searchitoperations.techtarget.com/definition/log-management

[38] Herb Segars. "Help! My Hard Drive Is Full!". Internet: http://www.gotosnapshot.com/myblog/help-my-hard-drive-is-full, Feb. 20, 2011.

[39] MacPaw Inc. "Slow Mac: Why Is My Mac Running Slow". Internet: https://macpaw.com/how-to/fix-mac-running-slow, Jun. 8, 2017.

[40] Cisco Systems, Inc. "The Internet of Things: Reduce Security Risks with Automated Policies". Internet: https://www.cisco.com/c/dam/en us/solutions/trends/iot/docs/security-risks.pdf, 2015.

[41] Cisco Systems, Inc. "Internet of Things". Internet: https://www.cisco.com/c/en/us/solutions/internet-of-things/overview.html