Internet of Things: Security Challenges and Solutions

By **Paulo Cardoso**

Abstract

The purpose of this report is to study in depth the internet of things, the way in which it has been introduced into our daily lives and its weaknesses; The different types of threats that can jeopardise its correct functioning and ways to protect from them. What are the challenges in terms of ensuring the security and privacy of users and how we can solve them are some of the questions this report intends to answer.

1. Introduction

The Internet of Things is a network that connects real-world objects to the Internet in a self-configuring and adaptive way. This allows for a whole new plethora of services and actions that can be performed remotely via an Internet connection (Rahmani, AM. et al., 2017).

The IoT is supported by the idea of a world unified by devices connected by the Internet Protocol. This vision of the future projects an Internet with billions of intelligent devices with means of action and communication connected to each other, and it is a futuristic idea that becomes more and more a reality as year after year the Internet undergoes drastic improvements given the evolution of the hardware and cloud services (Cirani, S. et al., 2019.). This revolution has taken place exponentially and generated a boom in devices connected to the Internet, increasingly materializing the idea of the Internet of Things.

After having watched this phenomenon with our computers and mobile phones, we can see that new technologies are developed daily that allow the most diverse objects to enjoy an internet connection, bringing new dynamics to the way we use all these objects. It is a matter of time that we will be able to program a heater so that it detects rises and falls in temperature and can be turned off if necessary, or an irrigation system that only activates on days without rain or with high temperatures. These are only small examples of objects that are being incorporated into Internet of Things so it can improve our daily lives and preserve natural resources by increasing its efficiency (Hersent, O. et al., 2011.).

1.1. Historical Advancements

The concept of connecting devices to the Internet and thus enabling remote monitoring of the same first emerged in 1982 by a group of university students at Carnegie Mellon University when they were able to establish an internet connection with a coke machine,

although the term only emerged in 1999 at the Massachusetts Institute of Technology Auto-ID Center when it was given by Kevin Ashton.

Over the years, new technologies with the most varied functions have been developed, such as environment detection and remote action and communication, and at the same time new computing devices were becoming smaller and cheaper to produce but carrying the same power comparatively. This fed an interest in applying IoT to major aspect in society, like Intelligent cities, houses, and healthcare services. (Rahmani, AM. et al., 2017).

Nowadays, from technologists to society in general, IoT keeps everyone amazed. No wonder why that happens; Ideas and possible implementations that where decades-old are only possible now and new implementations made them a topic with large interest, often discussed and promoted. We have already billions of devices that make part of the IoT, and build-it detection and control techniques will continue to evolve with the goal of helping smooth the vehicle traffic flow, control natural resources usage more effectively and give individual health monitoring with the aim to improve society's quality of life, between others (Martonosi, M., 2016).

2. Technical Depth

As we started to have wearable devices, smart cars, and domestic systems, we needed to develop a scalable architecture capable of maintaining those devices without compromising their quality. In addition, IoT devices are constrained by their lack of computing resources such as power, storage capacity, computing and bandwidth. This means that the IoT architecture has been adapting and shaping itself according to all these restrictions that limit its possible implementation scenarios. (Rahmani, AM. et al., 2017).

Being so, implementing IoT involves a long list of prerequisites. It needs to operate over open environments with an integrated architecture of interoperable platforms, and connected to intelligent objects augmented with microcontrollers, sensors, actuators and transceivers so they can analyze and collect data from their surroundings, giving them a real-world interface. Some of this IoT implementations came out to be considered unfeasible due to the way they where projected into reality.

The introduction of more computational resources into the edge nodes of access networks is a way to mitigate this unfeasibility, improving IoT scenarios of implementation as it reduces the latency, gives access to real-time resources and better context over the situation. They can be used as an interface that streams all the data originating from the devices connected In the IoT and uses this raw data can be stored and processed using different techniques as Machine and Deep Learning, which can Improve the way data is processed so it can be sent to relevant users or devices and can be regarded as useful information (Cirani, S. et al. 2019.). This creates a need for the IoT to be general and adaptable in order to connect and send signals with the most constrained objects, associated with limited memory and subject to stringent low-cost requirements.

3.1 Industrial Applications

The IIoT (Industrial Internet of Things) was the result of the junction between the digital connection created by the Internet and all the machinery used at industrial level using advanced IT platforms that improve manufacturing processes and efficiency. The

intersection of the cyber world with the industrial world has created economic and social opportunities that have forever changed the way Industries operate to develop new products. Operations are now managed and supervised remotely, can be stopped at any time in the event of a critical failure and reconfigured to resume after. The management of Big data remotely has also made possible the constant supervision of product stock, the provision of online services and the management of workplaces in different parts of the world (Bhattacharjee, S. 2018.).

The impact that the IIoT implementations had on industry worldwide quickly made it clear that the success of this new 'industrial revolution' was directly related to the security and reliability that this digital connection could provide to companies.

3. Security Challenges

The IoT has evolved in order to provide greater comfort to its users by giving them the chance to connect and control all their smart objects. Nevertheless, the connection of all these devices to the Internet has raised concerns about the security of the information that is transmitted and that may be subject to interference by third parties. As the number of smart objects connected to the Internet increases, so does the risk of these same objects be the target of a malicious attack. As such, the need has arisen to develop ways of protecting users' information so that their privacy is not compromised with the development of IoT.

This requires the creation of mechanisms capable of providing information security without compromising the ability to connect, communicate and manage the data collected by the instances that make up the IoT.(Shandilya, SK. et al. 2018.). The way security works on the Internet and on IoT is different for a couple of reasons; although the principles of security are virtually the same, the same approach cannot be used as IoT work with LLN’s and sensors, both things restricted by their memory and processing power. This makes so things like public Key encryption impossible to use as a way to secure IoT (Alaba, F, A, et al, 2017.).

3.1. Cybercrime Impact on IIoT

The IIoT concept projects a fully connected factory with implementation of technology such as cloud computing, IoT, artificial intelligence, etc... With the aim of creating innovative solutions that include reducing production costs, increasing efficiency or producing operations remotely, among others. With the development of new IIoT implementations on the rise, new threats to companies' cybersecurity have emerged. Any type of breach that can be detected at an industrial level can be devastating, exposing the entire machine-to-machine communication environment. Connected industries are totally dependent on these M2M communication networks, which in turn are highly susceptible to attacks coming from the internet. The gigantic number of IoT and M2M devices connected at industrial level sharing the same weaknesses from the cyber security point of view leads to a general compromise of the company's information/assets. Control and security standards will have to be applied so that it is possible to assess the impact of the cyber threat on the stolen/manipulated information so that appropriate prevention techniques can be developed. (Dhirani, LL, et al, 2021)

3.2. Types of Cyber Attacks

Between various types of treats that can disrupt information if it is available on Internet, cyber attacks aimed to IoT networks tend to aim for physical devices and appliances connected to them, deteriorating the target, misusing the ongoing traffic, and sometimes halting the entire operation. Against some of those attacks there are some ways we can stop them at a router level. Intrusion prevention and detection systems, firewalls and access control lists are some examples of methods that can be applied to defend the IoT from these types of malwares. (Shandilya, S,K, 2018.).

Today DDoS attacks are presented as among the most damaging attacks because they have adapted to the emergence of IoT-based systems, using armies of computers to exhaust server resources and gain unauthorized access to it. (Snehi, M, et al, 2021.). This is compounded by the fact that nowadays, most of the IoT malwares to be able to compile on a wide range of architectures simultaneously.

These are some specific DDoS attacks that occurred in the last years in large scale and shaped the way we see and face those threats:

- Linux.Hydra: The first IoT malware to be registered, it was found as an open-source project for devices based on the MIPS architecture in 2008, but whose real goal was to infect devices to join a URC-based network and execute simple SYN flood attacks. Best known for being the malware that served as a mote for the next MIPS targeting malware.

- Psyb0t: Pretty much identical to its predecessor, it distinguishes itself by being able to perform UDP and ICMP floods in addition to Syn flood attacks. Despite this and the fact that the real code behind psyb0t is not known, it is thought to be an offspring of Linux.Hydra given the high number of similarities.

- Chuck Norris: Was discovered in 2010 and is believed to have emerged as an alternative to Psyb0t after it was taken offline; it has the same traits as Psyb0t but sacrifices the ability to perform ICMP floods to perform ACK Flood attacks.

- Tsunami/Kaiten: Easily the strongest of Linux.Hydra iterations, it combines Chuck Norris malware with the DDoS KaitenTrojan. This makes the botnet preforms a set of more complex DDoS attack as HTTP Layer 7 Flood and TCP XMAS attack in addition to the more traditional attacks.

- Aidra/LightAidra/Zendran: Three identical malwares that can compile multiple architectures as MIPS, ARM and PPC, making them more complex than Linux.Hydra malware types. It creates an IRC-based botnet that send simple attacks like SYN Flood and ACK Flood.

- Spike/Dofloo: This type of malware was first developed after the Linux.Hydra family decayed and is part of a large group of malwares that had Agent Handler as its botnet architecture. It could resist a reboot by modifying the /etc/rc.local file and

control the amount of computing power being used by each infected computer during a DDos attack, all new implementations to avoid its cease and detection.

- BASHLITE: A malware that performed the same set of traditional DDoS, but this time used a lightweight version of IRC fully modified to be Agent-Handler based. It was designed to easily cross-compile to various computer architectures and it can infect even SPARC devices.

- Elknot/BillGates: This malware targets mostly SOHO devices, attacks MIPS and ARM architectures and produces several types of DDoS attacks such as HTTP Layer 7 Flood and TCP Floods. It was famous for being used extensively by Chinese Hackers, hence the family name China ELF. Given its origin, it is extremely difficult to detail this malware without access to the Source Code.

- XOR.DDoS.: Probably another malware of Asian origin, this time a malware capable of launching large-scale attacks of various complexity, from attacks such as SYN Flood, UDP Flood, DNS Flood, and more complex TCP Flood. Its name derives from the high use of XOR encryption that is used in its composition and the way it deals with communication.

- LUABOT: It is a trojan malware completely coded in Lua language that due to its atypical nature was especially difficult to understand its purpose. From what it is known it can perform HTTP Layer7 Flood attacks and it has a Javascript engine embedded that bypasses DDoS protections given by some well-known companies.

- Remaiten: It uses the main traits from Tsunami and BASHLITE, borrowing the Tsunami type of DDoS attacks using telnet scanning capabilities. It is capable of preform group of malicious tasks as launching DDoS, downloading more malware and even scan and remove other bots that can be present in the system competing for computing resources.

- Mirai: It is regarded as the most dangerous DDoS-capable IoT malware created and that is because it was capable of tracking and infecting thousands of weak IoT devices and join them in a huge Agent-Handler botnet. It uses a dictionary attack that targets small IoT devices and takes advantage of their lack of security to hijack them to be part of the botnet. As it was designed to target specifically IoT devices poorly protected with, this raised big concerns about the way IoT devices should be implemented. To make matters even worst, the source code of Mirai was made available on the internet, giving chance to more and more sophisticated versions of Mirai to be developed.

- NewAidra/Linux.IRCTelnet: A more recent malware that combines Aidra root code, Kaiten IRC-based protocol, BASHLITE scanning/injection, and Mirai dictionary attack, NewAidra can compromise any device based on a traditional architecture and it is capable of launching the most varied types of DDoS attacks. NewAidra presents itself today as the most powerful IoT malware since the appearance of Mirai and the only one that competes in terms of damage and danger.

4. Possible solutions

Although software implementations were used to mitigate possible attacks against the IoT, due to the limited resources that compound the IoT they are not viable. Lightweight cryptography was presented as an option, but it didn't fix the problem that information can be stolen and manipulated before it's encryption.

LUKS(Linux Unified Key Setup), are seeing as a good hardware alternative as Embedded LUKS(E-LUKS) adds integrity and authentication methods to the LUKS and uses last gen encryption algorithms. E-LUKS are already being implemented in modern chips, about 10 % the size of previous LUKS implementations, making it a great solution to provide Full Disk Encryption to different IoT devices(Cano-Quiveu, G, et al, 2021.).

5. Conclusion/ Critical Reflection

It is safe to say that IoT behaves as an entity in constant evolution and that creates a setup for innovation, comfort and life quality improvements. Unfortunately, at the same time its constant evolution means that it is developing new ways of being exploited. In this way, DDoS attack will be evolving and will become even more threatening than before. This creates a constant need for the IoT to update and protect against Specialized threats such as Mirai or NewAidra, an idea that currently will still be a bit precocious given the potential destruction of these large-scale attacks compared to general IoT security.

IoT is a recent concept; its appeal is more than justified given the impact it can have on a personal and professional level, capable of shaping the world around us, making it almost futuristic. However, it is only recently that effective ways to protect IoT connected objects have been developed and it is still necessary for these technologies to be applied on a large scale to see their real impact on IoT security in the long term.

For now, the use of E-LUKS presents itself as the most viable and effective solution for a secure IoT implementation, and it will only be exploited to its exponential extent when its security is ensured.

References

Cirani, S, Ferrari, G, Picone, M, & Veltri, L, 2018, Internet of Things: Architectures, Protocols and Standards, John Wiley & Sons, Incorporated, Newark.

Hersent, O, Boswarthick, D, & Elloumi, O, 2011, The Internet of Things: Key Applications and Protocols, Wiley, Somerset.

Rahmani, AM, Liljeberg, P, Preden, J, & Jantsch, A (eds) 2017, Fog Computing in the Internet of Things: Intelligence at the Edge, Springer International Publishing AG, Cham.

I. Ghafir, M. Husak and V. Prenosil, “A Survey on Intrusion Detection and Prevention Systems,” IEEE/UREL conference, Zvule, Czech Republic, pp. 10-14, 2014.

Martonosi, M, 2016, Keynotes: Internet of Things: History and hype, technology and policy; 49th Annual IEEE/ACM International Symposium on Microarchitecture (MICRO).

I. Ghafir, J. Svoboda and V. Prenosil, “Tor-based malware and Tor connection detection,” International Conference on Frontiers of Communications, Networks and Applications. Kuala Lumpur, Malaysia, pp. 1-6, 2014.

Shandilya, SK, Chun, SA, Shandilya, S, & Weippl, E (eds) 2018, Internet of Things Security: Fundamentals, Techniques and Applications, River Publishers, Aalborg.

Bhattacharjee, S, 2018, Practical Industrial Internet of Things Security: A Practitioner's Guide to Securing Connected Industries, Packt Publishing, Limited, Birmingham.

I. Ghafir and V. Prenosil, “Advanced Persistent Threat Attack Detection: An Overview,” International Journal of Advances in Computer Networks and Its Security (IJCNS), vol. 4(4), pp. 50-54, 2014.

Dhirani, LL, Armstrong, E, Newe, T, 2021, Industrial IoT, Cyber Threats, and Standards Landscape: Evaluation and Roadmap. Sensors (Basel, Switzerland).

I. Ghafir and V. Prenosil, “Blacklist-based Malicious IP Traffic Detection,” Global Conference on Communication Technologies (GCCT). Thuckalay, India: pp. 229-233, 2015.

Shandilya, SK, Chun, SA, Shandilya, S, & Weippl, E (eds) 2018, Internet of Things Security: Fundamentals, Techniques and Applications, River Publishers, Aalborg.

De Donno, M, Dragoni, N, Giaretta, A, Spognardi, A, 2018, DDoS-capable IoT malwares: Comparative analysis and mirai investigation, Security and Communication Networks.

Snehi, M, Bhandari, A, 2021, Vulnerability retrospection of security solutions for software-defined Cyber–Physical System against DDoS and IoT-DDoS attacks, Computer science review.

Alaba, F, A, Othman, M, Hashem, I, A, T, & Alotaibi, F, 2017, Internet of Things security: A survey. Journal of Network and Computer Applications.

I. Ghafir and V. Prenosil, “Advanced Persistent Threat and Spear Phishing Emails.” International Conference Distance Learning, Simulation and Communication. Brno, Czech Republic, pp. 34-41, 2015.

Cano-Quiveu, G, Ruiz-de-clavijo-Vazquez, P, Bellido, M, J, Juan-Chico, J, Viejo-Cortes, J, Guerrero-Martos, D, Ostua-Aranguena, 2021, Embedded LUKS (E-LUKS): A Hardware Solution to IoT Security.

I. Ghafir and V. Prenosil, “DNS query failure and algorithmically generated domain-flux detection,” International Conference on Frontiers of Communications, Networks and Applications. Kuala Lumpur, Malaysia, pp. 1-5, 2014.

Khan, Minhaj, A, Khaled, S,2018, IoT Security: Review, Blockchain Solutions, and Open Challenges, Future Generation Computer Systems, vol. 82.

I. Ghafir, J. Svoboda, V. Prenosil, “A Survey on Botnet Command and Control Traffic Detection,” International Journal of Advances in Computer Networks and Its Security (IJCNS), vol. 5(2), pp. 75-80, 2015.

S. Eltanani and I. Ghafir, "Aerial Wireless Networks: Proposed Solution for Coverage Optimisation," IEEE Conference on Computer Communications Workshops”, IEEE, 2021.

M. Hammoudeh, I. Ghafir, A.Bounceur and T. Rawlinson, “Continuous Monitoring in Mission-Critical Applications Using the Internet of Things and Blockchain,” International Conference on Future Networks and Distributed Systems. Paris, France, 2019.

I. Ghafir and V. Prenosil, “DNS traffic analysis for malicious domains detection,” International Conference on Signal Processing and Integrated networks. Noida, India: pp. 613 - 618, 2015.

U. Raza, J. Lomax, I. Ghafir, R. Kharel and B. Whiteside, “An IoT and Business Processes Based Approach for the Monitoring and Control of High

Value-Added Manufacturing Processes," International Conference on Future Networks and Distributed Systems. Cambridge, United Kingdom, 2017.

I. Ghafir, V. Prenosil, M. Hammoudeh, F. J. Aparicio-Navarro, K. Rabie and A. Jabban, "Disguised Executable Files in Spear-Phishing Emails: Detecting the Point of Entry in Advanced Persistent Threat." International Conference on Future Networks and Distributed Systems. Amman, Jordan, 2018.