Security in internet of things

Trends and challenges

Pedersen, Jens Myrup; Kidmose, Egon

Published in:
CEUR Workshop Proceedings

Publication date:
2018

Document Version
Publisher's PDF, also known as Version of record

Security in Internet of Things: Trends and Challenges

Jens Myrup Pedersen[1] and Egon Kidmose[1]

[1] Aalborg University, Department of Electronic Systems, Aalborg, Denmark
jens@es.aau.dk, egk@es.aau.dk

Abstract. Internet of Things describes an Internet consisting not only of computers, but a large variety of smaller and larger devices including sensors, devices in industrial settings and the many smart appliances that surrounds us – from smart watches to washing machines and surveillance cameras. However, this development also brings new and increasing security challenges. Among other factors, this is driven by the facts that even if each of the devices have limited capabilities, the huge numbers together represent significant computational and network resources, that the devices are often poorly protected and not properly updated/patched, and that they to an increasing extend are implemented in critical applications such as in industrial control settings. In this paper we analyze a number of attacks and based on this analysis derive some of the trends and challenges in Internet of Things. We also discuss how these can be handled. The examples show that while there is a trend of more sophisticated attacks, especially for the very targeted attacks, many of the attacks we see today are still simple and reflects the poor security level of the devices. In the future we might see more attacks based on artificial intelligence. It is important that the security challenges are handled, and that time is considered critical for both prevention and detection.

Keywords: Internet of Things, Security.

1 Introduction

The first large-scale cyberattack involving Internet of Things (IoT) is often said to be the Mirai Botnet, which in late 2016 was used to launch powerful DDoS attacks against DYN, an important DNS infrastructure provider. In this way, attackers managed to take down a number of prominent websites such as Spotify, Twitter and GitHub. While the attack itself was rather sophisticated, the way the Mirai Botnet took over the devices – estimated to be at least 100.000 and likely several millions – was rather simple: Brute-forcing through 62 combinations of default usernames and passwords [1-4]. A well-known example of a very different and much more sophisticated attack was the attack on the Ukrainian power distribution infrastructure that took place in December 2015 and left around 230.000 residents without power for several hours. Expected to be a nation-sponsored attack that had been prepared for almost a year, the hackers had worked their way into the SCADA system through several segments and layers of firewalls, from a first foothold achieved with a spear-

phishing attack. Eventually the hackers wrote malicious firmware for controllers in the grid [5]. These examples and many more are well known and analyzed, and together with a number of other attacks described in e.g. [6]. The problem with devices not being patched, or even sold with already known vulnerabilities is also previously described in the literature [7]. In this paper we search to update the threat picture by analyzing a few of the more recent attacks and based on this spot recent trends in threats and challenges. This is relevant to both practitioners and researchers who need to stay up to date with the current developments in the area of IoT security. The rest of the paper is structured as follows: Section 2 describes four attacks or attack groups, and for each we derive some of their characteristics. Section 3 discusses the results, and Section 4 concludes the paper.

2 Recent Attacks

The Reaper Botnet

The Reaper Botnet takes on many similarities with the previously mentioned Mirai Botnet as the main idea is the same: To take over control of a large number of devices, remotely controlled through a botnet infrastructure. Once the control is established a botnet can in principle be used for a variety of malicious activities including abuse of processing capabilities (e.g. for cryptocurrency mining), data theft (e.g. stealing pictures from video cameras), storage of illegal material, and DDoS attacks. However, Reaper is much more sophisticated in its capabilities to take over devices as it goes beyond simple password cracking and makes use of nine different approaches to exploit known vulnerabilities in devices by a number of prominent manufacturers. It is still unclear who is behind it, and how it is intended to be used, but according to the research by CheckPoint it contains a software platform that makes it possible to upload new code modules to the infected devices, giving much more flexibility in how the infected devices can be (ab)used [8-9]. However, so far it seems that only a limited number of devices have been infected. According to [10] only 28.000 devices were infected in February 2018, but based on the weaknesses that the botnet can exploit around 2.000.000 devices are vulnerable to being attacked.

In short, the Reaper Botnet shows that malware targeting IoT devices is becoming more sophisticated. To summarize, it can be said to demonstrate two important trends, which are well in line with the development of “classical” botnets targeting computers:

- More sophisticated means of conducting attacks, i.e. the capability to abuse several different vulnerabilities.
- More sophisticated control of the infected devices, e.g. capabilities to upload new software modules so the usage can be adapted over time.

Industrial Control Systems

More and more devices to industrial production are being connected, either in internal networks, or through the Internet. This is an important enabler for "Smart Production" and "Industry 4.0", but it does also come with security risks. Last year we demonstrated an attack against a state-of-the-art production line, where we could basically take over the production including adding/changing orders, stealing data, and wiping important data that would leave the system crippled [11].

Before moving on with another recent example, one important point is how easy it is to find vulnerable IoT (including Industrial IoT) devices using search engines specifically developed for this purpose such as Shodan [12]. [13] provides a good insight to Shodan's capabilities, but also discuss how it is actually a strong tool for network administrators to identify vulnerable systems and devices so they can be properly secured.

In 2017, researchers from Trend Micro and Politecnico di Milano demonstrated how they were able to take over an Internet-connected industrial robot arm. This could be used for a variety of attacks: A heavy robot arm can cause significant harm to people, products and machinery, it can be used to stop the production, or to tamper with what is being produced, e.g. by introducing small production errors that would change the performance of the products. The researchers were able to perform a variety of attacks using different vulnerabilities such as open FTP servers connected to the robots and bad HTTP interfaces to inject unauthorized commands [14]. While the combination of these weaknesses and the use of Shodan is by itself scary, the wider use of IoT in the industry also opens up for more targeted, sophisticated and coordinated attacks – from espionage to efficient sabotage of infrastructure and production environments.

To summarize, there may not be much news to the analysis based on such attacks, but the increasing spread and usage of the technology while still fighting with "getting the basics" makes it even more important to start acting. So, to summarize the trends:

- More critical infrastructures and industrial systems are connected to the Internet.
- Vulnerabilities of Internet-exposed devices are easy to find using automatic tools and search engines.
- With more industrial systems being connected to the Internet, alone the connectivity of such devices and systems can lead to new vulnerabilities that can be exploited in targeted and sophisticated attacks.
- With more systems and devices being connected to the Internet (directly or indirectly) the potential consequences of such attacks increase.

Health Care Systems

There has been a number of reported cases where IoT devices used in the health sector were vulnerable to attacks. Among the most famous examples are probably the Merlin@Home transmitter, which is used for communication between implantable cardiac devices and hospitals – it can both transmit data and receive commands in

order to e.g. deliver paces/shocks. A number of vulnerabilities were discovered, and in January 2017 the U.S. Food and Drug Administration sent out an official warning stating that the vulnerabilities could be used for an unauthorized user to remotely access the Merlin@home transmitter, eventually enabling an attacker to modify programming commands and e.g. cause fast battery depletion and/or to alter the pacing/shocks [15]. However, it often appears that to successfully conduct a significant attack, the attacker must be physically very close to the victim such as for the pacemaker in [16]. The increasing use of IoT devices in health care should be seen in the light of the general threat picture against the health sector, which seems to be a good target for attackers whether for strategic or financial reasons. This is for example seen through the many ransomware attacks against the UK health sector, see e.g. [17]. Another problem with IoT in the health sector is that the devices used here seem to suffer from some of the same weaknesses as traditional IoT in terms of e.g. lack of updates and patches, especially as the age of devices increase. In a study from 2018, researchers from Kaspersky found 27.716 open entry points for hackers in the hospital sector, many of which were using out-of-date management software, including lightning systems, air condition systems and printers [18]. To sum up, the following trends are worth noting.

- More and more IoT devices are making their way into the health sector. Even if there are no known and serious attacks, there has previously been found vulnerabilities in some such devices.
- The threat picture should be seen in the light of hospitals being attractive targets for cyber criminals, as manifested in e.g. recent ransomware attacks.
- IoT devices used in the health sector suffers from some of the same weaknesses as general IoT devices in terms of e.g. lack of updates and patches. In this respect, it is worth noting that the automatic searches and search engines also here makes it easier to find and exploit vulnerable devices.

Attacks Based on Artificial Intelligence

In the last few years, Artificial Intelligence (AI) has gained increasing awareness in the cyber security community. Examples of this are as part of Intrusion Detection/Prevention Systems, such as various applications of IBM's Watson technology [19]. However, AI is not only interesting from the defensive side of things. Especially since 2016 a number of publicly known initiatives have started to explore the potentials on the attacker side (it is probably safe to assume that much has happened even before this time, behind closed doors). 2016 was the year where the first all-AI Capture The Flag took place, known as the Darpa Cyber Grand Challenge [20], and also the year where ZeroFox demonstrated that an AI was better in getting Twitter users to click on malicious links than skilled humans: In particular, humans were able to do 1,075 tweets per minute and catch 49 victims, whereas AI was able to do 6,75 tweets per minute and catch 275 victims [21]. Even if each tweet was a little less efficient, the fact that it was able to send out a much larger number led to a great increase in the number of victims.

It is our expectation that we have only seen the beginning of using AI here. In particular when it comes to an environment where many devices are connected at different layers, it seems viable that AI implementations can help malware to spread through infected devices, which through "local AI" is able to make decisions without always having to communicate with a central machine such as a botmaster. Moreover, such AI-based systems will be able to use data from successful and unsuccessful attacks to improve future attacks. It is worth noting that AI is not a matter of either/or, as it is easy to imagine how AI can be used to support attacks that are being carried out by humans.

To summarize: Even if AI is still at an early stage (at least based on publicly available information), it is a technology with a lot of potential as seen from an attacker point of view. While initially the technology might be used to increase the amount and size of automated attacks, smart use of data can very well lead to also more efficient and successful attacks. While devices still need to be vulnerable in order to be exploited, this can make it easier to find and carry out attacks – both simple and "broad" attacks, and attacks which are more targeted and sophisticated.

3 Discussion

In the previous section we looked at recent attacks and attack methods and derived some general points on trends and challenges in Security of IoT. In particular that:

- Attacks are generally becoming more sophisticated; This is valid both for the attack itself and for the following actions. On the other hand, simple attacks still exist.
- More and more devices are being connected to the Internet, including industrial systems, critical infrastructures, and health related devices. Both the numbers and the criticality of their usage makes for increasingly attractive targets.
- The fact that more and more devices are being connected to each other, and to the Internet, can lead to exposure of new vulnerabilities.
- Vulnerable and Internet-exposed devices are easy to find using automatic tools and search engines.
- Basic security problems in IoT-devices remain largely unsolved, with many vulnerable and unpatched devices still being around. A problem that will likely increase as more and more old devices will remain active and connected.

While this describes a development that certainly calls for action, it seems that the attack picture is evolving gradually rather than going through disruptions. Even if AI might be a joker than can significantly change the picture through faster, better, more efficient and automated attacks, it still seems that the classical recommendations hold, and are more important than ever: These include using unique usernames/passwords, segmentation, strong encryption, disabling unused ports/services, keep an overview of devices, establish procedures for patching, block Internet access unless needed, consider physical access, and consider an appropriate level of network security. Should we point to one factor, it would be that the increasing automation can decrease the

time span from a vulnerability is found until it is exploited, and also the speed of attacks. So, time becomes an increasingly important factor also from the defending side.

4 Conclusion

In this paper, we studied recent attacks and attack trends in the Internet of Things. While there are more advanced attacks, there are also still many simple attacks, which reflect the poor security level of the devices. In the future we might see more attacks based on artificial intelligence; all in all, this suggest that it becomes even more important to be aware of the potential threats when investing in Internet of Things, to follow the classical advices on security in such devices, and to be aware that attacks can happen fast so time is important in all aspects from patching to detection and mitigation.

References

1. DYN analysis summary of Friday October 21 attack. http://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack (last accessed 08-20-2018)
2. http://www.forbes.com/sites/leemathews/2016/11/03/someone-just-used-the-mirai-botnet-to-knock-an-entire-country-offline (last accessed 08-20-2018)
3. Krebs on Security blog. https://krebsonsecurity.com (last accessed 08-20-2018)
4. Symantec blog, https://www.symantec.com/connect/blogs/mirai-what-you-need-know-about-botnet-behind-recent-major-ddos-attacks (last accessed 08-20-2018)
5. https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid (last accessed 08-20-2018)
6. Kidmose, E., Pedersen, J. M., Security in Internet of Things, in Cybersecurity and Privacy: Bridging the Gap. River Publishers, 2017. s. 99-118.
7. Hastings, M., Fried, J., Heninger, N. "Weak Keys Remain Widespread in Network Devices", Proceedings of the 2016 ACM on Internet Measurement Conference, ACM, 2016.
8. https://www.ophtek.com/iot-reaper-botnet-predicts-grim-future/ (last accessed 08-20-2018)
9. https://research.checkpoint.com/new-iot-botnet-storm-coming/ (last accessed 08-20-2018)
10. https://www.secplicity.org/2018/02/20/iot-botnets-evolving-big-can-get/ (last accessed 08-20-2018)
11. Knudsen, A.H., Pedersen, J.M., Sørensen, M.A.M., Villumsen, T.D. Security in the Industrial Internet of Things, in Cybersecurity and Privacy: Bridging the Gap. River Publishers, 2017. s. 119-134
12. Shodan website. https://www.shodan.io (last accessed 08-20-2018)
13. Long, M. How Shodan is used to exploit vulnerable SCADA systems. http://www.cs.tufts.edu/comp/116/archive/fall2015/mlong.pdf (last accessed 08-20-2018)
14. https://www.wired.com/2017/05/watch-hackers-sabotage-factory-robot-arm-afar/ (last accessed 08-20-2018)
15. http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm535843.htm (last accessed 08-20-2018)
16. https://www.pcworld.com/article/143496/article.html (last accessed 08-20-2018)

17. https://www.theverge.com/2017/5/12/15630354/nhs-hospitals-ransomware-hack-wannacry-bitcoin (last-accessed 08-20-2018)
18. https://www.cnet.com/news/iot-attacks-hacker-kaspersky-are-getting-worse-and-no-one-is-listening/ (last accessed 08-20-2018)
19. https://www.ibm.com/blogs/watson/2017/08/ai-is-the-future-of-cybersecurity-how-watson-helps-detect-threats-faster-and-better-protect-your-organization/ (last accessed 08-20-2018)
20. https://www.wired.com/2016/08/security-bots-show-hacking-isnt-just-humans (last accessed 08-20-2018)
21. https://www.forbes.com/sites/thomasbrewster/2016/07/25/artificial-intelligence-phishing-twitter-bots/#172777a376e6 (last accessed 08-20-2018)