Vulnerabilities in the Distributed and Autonomous Internet of Things

Tom Strassner

tomstrassner@gmail.com

12/12/2014

Abstract

We are living in a time when computers are rapidly becoming cheaper and smaller, with no sacrifice in computing power. Furthermore, humankind has now become highly comfortable with the Internet, and the instantaneous connection it provides all of us to each other and to knowledge has become ingrained our daily lives. It is second nature to those who have been using it for more than a few years. The combination of this rapid advancement in computing technology and this major shift in how people interact with the Internet is leading to many objects in our lives other than computers to be connected to the Internet. These items have become known as the Internet of Things (IoT). The IoT is a large, autonomous network of devices that connect to the Internet with embedded systems. It is these characteristics that give it its power, but are also the root of many security vulnerabilities: "The internet-of-things holds great promise for enabling control of all the gadgets that we use on a daily basis… It also holds great promise for cyber criminals who can use our homes' routers, televisions, refrigerators and other internet-connected devices to launch large and distributed attacks." [5]. This paper will introduce the IoT, its distributed structure, and some of its important implications. Then it will establish why there are security vulnerabilities related to its distribution, how they could be exploited, and how the common user can defend against those exploits. Finally, it will end with a brief conclusion of my personal thoughts of how it should be handled.

Introduction

The term Internet of Things (IoT) is an emerging concept. It is a broad term that refers to the collection of objects that connect to the Internet, typically via embedded computing devices. The term especially refers to things other than computers, servers, and other devices that people more commonly used to connect to the Internet. As the hardware necessary to build a device with significant computing power is exponentially decreasing in size and cost, engineers and product designers are increasingly capable of putting this technology into objects that they never could before. Here are some examples of such common devices today, and how they are being used to leverage the added functionality of Internet connection: toasters that can burn a weather icon into your toast, refrigerators that scan the RFIDs of its contents, coffee machines and thermostats that you can control remotely from your smart phone, and watches that provide GPS and full internet browsing capabilities. These current technologies and many more are already making profound improvements on the convenience of our daily lives, and the future possibilities are virtually endless. Cars could communicate with roads to make driving safer and more efficient, refrigerators could order more milk for you when you run out, dumpsters could notify waste management companies when they are full [2]. Any object you can think of could conceivably use time and location awareness to improve its efficiency and utility. When enough things in the world can connect to the internet, the future could be one in which we have a "smart planet", where people interact with their surroundings in a completely new way, and global systems such as the economy could be entirely revolutionized [1]. While these grand possibilities are exciting, however, there are many hurdles we must get past in order to get to achieve such a deeply integrated world

Why this topic

Currently, one of the most significant problems with the IoT is security. In a world where so much effort has been put into computer security (encryption of data, authentication, etc.), why is it being largely overlooked in the IoT? Much of the world operates in a free market, where consumer demands dictate what goods and services are provided. When many users of a website experience dissatisfaction with a product due to its lack of security (e.g. if their passwords are detected by attackers), then the company can allocate resources to solve that problem (e.g. switch to a secure protocol, or improve user authentication measures). However, the IoT in its current state works on a slightly different paradigm: With the exception of devices with extensive capabilities and user interfaces such as smart watches, most of the things in the IoT perform their communication through the Internet with little to no direct interaction with the human user. This is in fact a major draw for users to own items in the IoT, as they integrate into people's lives so subtly that users are not always cognizant of the fact that the device is connecting to the Internet at all. For example, your toaster burns clouds and a raindrop into your toast without the user directly manipulating it to do so. Your thermostat turns on the heater because it has detected that you are on the way home; when you arrive your house it is a comfortable temperature and you may not even think about the thermostat at all. Even if it does cross your mind that Internet access is what is facilitating moments such as these, it is even less likely that the average consumer will really think about what data is being transferred, and whether or not it is secure. For these reasons, there is not much consumer desire for these devices to be secure, and in turn there is less incentive for companies to invest in security measures [5].

What makes the IoT more vulnerable than pre-IoT devices

Individual devices in the IoT serve many different purposes, and many new ones will certainly be invented. Each of these different devices with different purposes have the potential to open the door for any number of security vulnerabilities, based off their functionality, what services they connect to, what data they transfer, and what network protocols they conform to. For these reasons, it would be impossible to enumerate all of the potential issues. However, there is one characteristic of the IoT as a whole that differentiates it from the pre-IoT Internet: It is extraordinarily distributed, and most of the devices are unmanned while they communicate with the network. The pre-IoT Internet was highly distributed as well, with hosts connecting from all corners of the globe, however the IoT takes it to a whole new level, as predictions for the number of devices within the IoT in 2020 range from about 26 billion to 200 billion [2][6][7]. Even conservative estimates will vastly eclipse the number of conventional devices (such as personal computers and servers) connected to the Internet. Furthermore, there is a human physically operating a personal computer most of the time it is connected to the Internet. Servers are usually not manned, but a multitude of software exists for the purpose of automating that process by parsing network traffic and server logs for malicious and problematic activity. As it stands, most IoT devices perform their interaction with the Internet autonomously, and have no means of detecting, let alone handling, malicious activity.

The autonomous nature of the IoT opens doors for innovation. For example, the thermostat mentioned above needs no command from a human to turn off the heat when you leave and turn it back on when you are on the way home. Uses such as this can make daily life simpler in many different ways. This functionality in turn facilitates a highly distributed network, because devices no longer have to physically be with a human in order to serve its purpose. This

is undoubtedly a major advantage to the IoT, but these same characteristics can be very problematic as well. For example, it opens the door for the possibility of a black hat hacker to assign an arbitrary task to a large number of devices. Despite the infancy of the IoT, this sort of attack has already been proved to have happened once. In January 2014, Proofpoint, a security as a service vendor, discovered that someone had launched an attack that entailed 750,000 phishing and spam emails from over 100,000 devices. These devices mainly consisted of household electronics, such as televisions and refrigerators [6]. Since the messages came from so many different devices, it was impossible to track the origin of the attack. Furthermore, it is not difficult to imagine how this sort of attack could be slightly altered to be even more sinister. For instance, the task assigned to each of the 100,000 devices could have been to SYN flood a certain vulnerable server with the goal of causing a DoS (Denial of Service). Since the packets originate from such a large number of sources, this is what is commonly referred to as a DDoS (Distributed Denial of Service) attack. The massive and rapidly increasing population of the IoT gives the malicious hacker a brand new ocean of potential bots to leverage for this sort of activity.

There is yet another characteristic of many devices in the IoT that creates the potential for new threats: The embedded systems on these devices usually use ARM, PPC, MIPS and MIPSEL chip architectures, as opposed to the Intel x86 architecture that is on most servers and personal computers today [7]. This may not seem inherently like a problem, but a separate set of architectures opens up a whole new set of potential hacks. Indeed, many of these hacks are positive, as they are what has enabled such small devices to connect to the Internet and have such elaborate computing capabilities. However, it is a double-edged sword, as any architecture will have its own set of vulnerabilities for malicious hacks as well. For example, Kaoru Hayashi, an

investigator at Symantec, a well-known security firm, discovered a worm that could take advantage of devices with those older architectures, as well as the distributed nature of the IoT. The worm in question, called Linux.Darlloz, targets machines with the x86 architecture and exploits a well-documented PHP vulnerability (CVE-2012-1823, CVE-2012-2311, CVE-2012-2335, CVE-2012-2336) that has been patched for on most computers. Since it has been patched, it seems relatively innocuous, however when Hayashi found the server with the original worm, he discovered that there were versions of the same exact worm but targeting the ARM, PPC, MIPS and MIPSEL chip architectures [8]. It has not been confirmed whether or not those versions of the worm have been deployed or caused any damage, but it is concerning nonetheless, as many machines in the IoT with older architectures would not have the proper patch. The dated architecture on the IoT devices could allow for the successful penetration of the worm, or others like it, and the wide and distributed network of the IoT could allow for effective replication and distribution of the worm to infect many different machines.

Defenses

The IoT is still quite young, but it already has a substantial presence in society, is rapidly growing in size and reach, and has astronomical growth projections over the next five to ten years. For this reason, the earlier these questions of security can be solved, the brighter the future will be. The larger the network of devices, the more difficult it will be to fix things, especially due to the variety within the IoT. As a consumer and owner of such devices, there are some measures that you can and should take in order to improve security. The first step is to understand that there is no such thing as complete security, and there will always be threats and new hacks that people come up with. Improving your security is good, but forgetting about it due

to a false sense of security can be your downfall. As mentioned in the "Why this topic" section of this paper, it can be easy to forget that your devices connect to the Internet at all, particularly when they are common objects that previously never had internet connection, and they are made specifically to seamlessly integrate into your life. However, from a security standpoint, you should always be aware of what connects to the Internet, what data it sends and receives, and whether it sends that data encrypted or not. A smart move would be to look online and contact vendors in order to understand these details about your devices. Another mistake that people make with such devices is to skip configuration upon initial setup [5]. When this happens, devices are frequently left with the factory default password to gain access to them; factory default passwords are extremely easy to crack. A third crucial measure you must take to optimize the security of your IoT devices is to make sure that your software is always up to date. As with the patch of the PHP worm discussed above, software updates are not just for improved functionality for the user, but also for important bug fixes and vulnerability patches. The device may automatically update itself, but not always, so you may need to regularly check the manufacturer's website for updates you need to download [7].

Conclusion

This is undoubtedly an interesting time to live, as we will see a veritable explosion in the IoT over the next ten years. Today, the IoT is still in its infancy, and there have not yet been any known severe security breaches. However, I believe that it will surely be a heavily targeted vector of attack in the near future. The reasons for this prediction include but are not limited to: the massively distributed nature of the IoT, the fact that the devices tend to be always connected to the Internt and never physically manned, the dated and therefore vulnerable hardware and

software on the machines, and a largely computer-illiterate user base. While it is important for people to take security measures and be aware of the connectedness of their devices, I believe that it is far more important that manufacturers and vendors have these vulnerabilities I have described in mind, and that they put security as a top priority with their devices. Unfortunately, this may be a difficult goal to attain, because the majority of the user base does not value security, and therefore it is not an economic incentive for the producer.

BIBLIOGRAPHY

[1] Real-Time Systems
http://link.springer.com/chapter/10.1007/978-1-4419-8237-7_13

[2] A Simple Explanation Of 'The Internet Of Things'
http://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/

[3] An Analysis of DrDoS SNMP/NTP/CHARGEN Reflection Attacks
http://www.stateoftheinternet.com/downloads/pdfs/2013-state-of-the-internet-web-security-white-paper-drdos-snmp-ntp-chargen-attacks.pdf

[4] RFC 1157
https://www.ietf.org/rfc/rfc1157.txt

[5] Cyber attack launched through fridge as internet-of-things vulnerabilities become apparent
http://www.computing.co.uk/ctg/news/2323661/cyber-attack-launched-through-fridge-as-internet-of-things-vulnerabilities-become-apparent

[6] Proofpoint Uncovers Internet of Things (IoT) Cyberattack
http://www.proofpoint.com/about-us/press-releases/01162014.php

[7] The Internet of Things: New Threats Emerge in a Connected World
http://www.symantec.com/connect/blogs/internet-things-new-threats-emerge-connected-world

[8] Linux Worm Targeting Hidden Devices
http://www.symantec.com/connect/blogs/linux-worm-targeting-hidden-devices

[9] MITRE CVEs: CVE-2012-1823, CVE-2012-2311, CVE-2012-2335, CVE 2012-2336
http://cve.mitre.org/cve/cve.html