THE DANGERS OF IoT DEVICES

Vlad RUSU

TI-231, Faculty of Computers, Informatics and Microelectronics, Technical University of Moldova,
Chisinau, Republic of Moldova

Corresponding author: Vlad Rusu, vlad.rusu@isa.utm.md

Tutor/coordinator: **Ala ŞIŞIANU**, univ. assist.

Abstract. *The technological advancements and economic growth of the 21st century have created a necessity for more specialized approaches to computers and computing, which arrived fruitfully in the form of IoT devices. Although an indispensable part of society nowadays, the sheer speed of their expansion gave birth to a plethora of other problems with regards to security, business practices, political controversies, and health hazards. This article intends to shed light on the dangers associated with embracing this IoT and make a call for help to the community with ways to amend the current situation.*

.

Keywords: *IoT, Internet of Things, security, exploitation, smart devices, vulnerability*

Introduction

The Internet of Things or IoT for short is a blanket term that covers a realm of computing with non-standard devices, usually considered dumb devices, that equipped with internet connectivity can extend their control and supervision to computers for achieving a specialized task [1]. These can range from simple devices like thermostats, smart speakers, fridges to medical equipment and even autonomous and internet enabled assembly robots.

They're extremely versatile devices that are tailored to the field of work intended for and nowadays, most households and businesses have at a bare minimum a single IoT device in function. One cannot imagine not having internet in their house, which is provided graciously by the ISP Router. On a similar note, the luxury of having a morning routine set up in the home assistant for every morning to have the boiler kicking in function at exactly 6AM whilst there's a coffee brewing is, for some people now, the only reason they're not late to work.

Although they're useful, this fast-growing and very demanding industry has led to the appearance of unhealthy business and security practices. Who's to say that every device is guaranteed to be completely safe and who's guaranteeing the safety of one's possession, especially when there's the possibility that a device has been rushed on the market without the necessary testing due. I've taken upon the task of bringing awareness to the masses of the terrifying results of these questions.

Household security or the puppet of those in power

The company Ring first appeared in 2013 through a crowdfunded startup that raised $364,000. It promised a revolutionary home security system that could protect one's property from criminals before an actual crime happened [2]. Though a succession of investments, the company was acquired in 2018 by Amazon as one of its first tech subsidiaries. Since then, it has become one of the most prosperous security system providers in the world.

One cannot deny the appeal of owning and controlling a home security system. Ring covers everything, from indoor and outdoor cameras to camera equipped doorbells, movement sensors and even home automation like smart lights and internet-controlled power sockets [3]. Everything is tightly integrated in the Ring and Amazon ecosystem that utilizes the principles of IoT integration to unify everything for the comfort of the owner.

Not very far back though, Ring has been caught in a controversy where they allowed law enforcement to request video footage from ring doorbells through their Neighbors watch app. This allowed the police to obtain surveillance materials from doorbell owners without guardrails around the legality of the usage of said materials. As such, nobody had any say in what law enforcement could do with the footage attained. The feature has been officially removed by Amazon as of 2020, stating that such requests can only be legally made with a subpoena [4].

Whilst commendable, their work is farfetched as a series of vulnerabilities have been discovered in Ring doorbells [5] allowing bad actors and hackers to spy on proud owners of their products. The Federal Trade Commission of the US had sanctioned Amazon on this case for failing to provide its customers with basic security needs and had to pay $5.8M in refunds for the damage.

Unfortunately, this is only one of multiple cases since the existence of IoT, which proves the hazardous nature these appliances could possess. Even a multi-trillion dollar company with all the resources on hand can fail miserably on matters of security and underhanded business practices.

IoT Pacemakers. A health necessity and weapon in the wrong hands

Abbot Laboratories, formerly called Saint Jude Medical, has created several reputable pacemakers. Pacemakers are medical devices that get implanted in the human body to keep the rhythm of the heart or keep the heart from dropping its beat rate. These are usually supposed to be programmed with a docking station close to the heart. Abbot Laboratories has created pacemakers that can be controlled with a phone, making it an IoT device. Unfortunately, security researchers have found vulnerabilities in the implantable cardiac pacemakers and cardiac resynchronization therapy pacemaker "(CRT-P) devices", including "Accent", "Anthem", "Accent MRI", "Accent ST", "Assurity", and "Allure" devices. Fortunately, implantable cardiac defibrillators and cardiac resynchronization devices were not affected.

The vulnerabilities in question are "CVE-2017-12712 – Improper Authentication", allowing a bad actor to call upon commands without the interaction of the patient, "CVE-2017-12714 - Improper Restriction of Power Consumption", allowing an attacker to issue commands with unrestricted power draw effectively draining the device of battery and "CVE-2017-12716 - Missing Encryption of Sensitive Data", referring to the ability of the device to share patient information without the data being encrypted, this being an actively used function of the device [6].

Abbot has issued firmware updates for all devices affected by these vulnerabilities. Said updates can be applied by healthcare providers using the specialized "Merlin PCS Programmer" [7]. This could have turned into a tragic situation for hundreds of thousands of patients and raises the question of whether IoT should be embraced in so many domains, especially when the IoT device in question is responsible for the life and health of a person.

The state of a Huawei ISP routers in Moldova

Internet Service Providers in Moldova have been in recent years, ubiquitous for issuing Huawei gateway routers to their customers. As of January 10th, 2024, I've received in my possession a Huawei HG255 Enterprise grade gateway router from a popular internet provider in Moldova. This was a device procured with a business contract for my friend's home.

While working on this article, I've engaged in the analysis of the security of said router. Unfortunately, I've found that this specific device had a vulnerability in 2017 classified as "CVE-2017-17309" which is a directory traversal vulnerability that allows an attacker to inspect files on an external storage device connected to the router. The HG255 can run as a NAS server (Network Attached Storage), which broadcasts the server's address on a local network for everyone's usage. This is an extremely useful feature, especially in an enterprise setting, where it enables easy sharing of files (possibly classified documents) throughout a network [8]. A proof of concept detection utility is also now part of the Metasploit module library which is an extremely popular pen testing utility used by security researchers worldwide. This vulnerability was fixed shortly after by Huawei after a security notice released on their website [9].

After booting up the device and checking the firmware version, it turned out that the currently flashed firmware was an older revision than the one stated in the CVE report, effectively making this device a possible target for this vulnerability and also other undisclosed ones. These gateway routers are not user updateable, meaning only the manufacturer and the ISP can update the device, all done remotely. To be fair, this can all be ruled out to be a misconfiguration on the provider's part. Personally, I haven't seen such a problem in other routers from said ISP and others in Moldova.

The risk is still there even if the probability is low. Considering that this router was a part of an enterprise issued contract to be used in a business environment and that there was always a chance that a bad actor could access the device, given enough knowledge in this domain, with an interest in this specific business, could have proven fatal to the owner. Routers are an essential part of everyone's household nowadays and should be completely secured and act as the first line of protection for anyone's network.

Conclusions

To sum up everything stated, IoT device are indeed extremely versatile, but the huge boom in popularity has increased the level of demand from customers, making even huge companies with enough monetary resources to rush up on devices and features to satisfy the market. Checkups and research before buying an IoT device should be mandatory to anyone interested in making such a purchase. Nobody should assume that an IoT device is completely secure if it comes from a resourceful company or if it's designed to ensure someone's health. These are all stereotypes that have been easily proved to be wrong in the examples above. The industry should prioritize security over quantity in the IoT space and engage in the active reduction of currently available vulnerabilities.

Acknowledgments:

I would like to thank my dear friend Petru Cojocaru for donating to me the router used for this article's research, while at the same time enhancing the security of his household by removing this hazard. It has been put to good use and truly helped me paint a clearer picture of the security dangers of consumer and enterprise routers in our country.

I would also like to thank miss Şişianu Ala for facilitating the research in this article and supporting my cause.

References:

[1] Alexander S. Gillis, Brien Posey, Sharon Shea, "IoT devices (internet of things devices)", August 2023 [Online] Available: https://www.techtarget.com/iotagenda/definition/IoT-device

[2] Wikipedia "Ring (company)" [Online] Available: https://en.wikipedia.org/wiki/Ring_(company)

[3] Ring store [Online] Available: https://ring.com/ .

[4] Annie Palmer, CNBC, "Amazon's Ring will stop allowing police to request doorbell video footage from users", [Online] Available: https://www.cnbc.com/2024/01/24/amazons-ring-will-stop-letting-police-request-doorbell-video-footage.html

[5] CVE Details, Public tracker of vulnerabilities [Online] Available: https://www.cvedetails.com/vulnerability-list/vendor_id-12126/year-2019/Amazon.html

[6] Ionut Arghire, "St. Jude Medical Recalls 465,000 Pacemakers Over Security Vulnerabilities" [Online] Available: https://www.securityweek.com/st-jude-medical-recalls-465000-pacemakers-over-security-vulnerabilities/

[7] NHS Online, "Abbott Laboratories Pacemaker Vulnerabilities", [Online] Available: https://digital.nhs.uk/cyber-alerts/2017/cc-1616

[8] CVEDetails, "CVE-2017-17309", [Online] Available: https://www.cvedetails.com/cve/CVE-2017-17309/

[9] Huawei, "Security Notice - Statement about the Directory Ttraversal Vulnerability in Huawei HG255s Products", [Online] Available: https://www.huawei.com/en/psirt/security-notices/huawei-sn-20170911-01-hg255s-en