Technical and Economical Evaluation of IOT Attacks and their Corresponding Vulnerabilities

Stefan NICULA, Răzvan-Daniel ZOTA
Bucharest University of Economic Studies
niculastefan13@stud.ase.ro, zota@ase.ro

An increase in popularity and adoption of IoT products encountered a direct proportionate interest in attacks and exploits on such solutions, having a measurable economic impact on the business industry and the IoT customers. The research analysis conducted on various IoT devices revealed security issues with patterns that are strongly related to high-risk vulnerabilities used in common exploit chains and malware campaigns. This includes vulnerabilities such as weak or default credentials, usage of outdated and vulnerable software, sensitive data exposure and missing security best practices and standards. This paper tackles multiple vectors of attack that are threatening the privacy and security integrity level of IoT devices in order to discover potential entry points and post-exploitation techniques that are often used on IoT attacks. The research perspective covers the malware incident aspect, vulnerabilities that are affecting different components and the overall security level provided by the products, with a focus on the economic impact delivered by such outcomes. Malware outbreaks are studied along with the impact of publicly known vulnerabilities, the attack surface of an IoT device and the mitigation enforced by some vendors. The security evaluation methodology was based on Penetration Testing practices, targeting all the components exposed by the IoT devices that were studied. This included the network capabilities, web and mobile applications and targeted the physical attack vectors as well. The recent IoT attacks were studied in order to draw conclusions and create potential recommendations and improvements to the IoT landscape.

Keywords: *IoT, Security, Vulnerabilities, Malware, Economic Impact*
DOI: 10.24818/issn14531305/25.1.2021.03

1 Introduction

The paper aims to reveal, categorize and interpret vulnerabilities and privacy concerns across a series of studied IoT devices. The study has been conducted on a number of research projects across a multi-purposes area design for IoT devices in order to understand and link the results with various public IoT attacks that have surfaced in the recent period. The outcome was analyzed in contrast with published research papers and popular attacks on IoT products.

The IoT security analysis was executed from a Penetration Testing perspective in order to conduct various research exercises to obtain metrics which can later be used as base references for the conclusions [1].

Such projects often had complex architecture designs because the intended purpose of the tested IoT solutions was to provide an automated and independent solution to publicly known problems. Based on these principles, the tested IoT products had multiple components that needed to be analyzed. Following the business logic of the tested products, the scope of the project included different technical components such as web applications, mobile applications and hardware physical devices that were involved in the Penetration Testing engagement and were taken as part of the main scope [2].

From previous past experiences, these systems defined as a single IoT product, have unique vulnerabilities that can affect the studied IoT product in different ways. However, these vulnerabilities can be noticed across the entire spectrum covered by the IoT product in their business area.

Another base research was targeted towards analyzing publicly known attacks and malware incidents that affected the IoT products from past years. By analyzing key elements from the exploit chain such as initial reconnaissance efforts, the entry points, potential exploits leveraged and lateral movements, we can draw specific conclusions that will help us decide on recommendations and improvements. This research methodology helped us identify deficient areas of IoT products in terms of security implementations and protection mechanisms.

With and increasingly larger number of IoT products coming into market each year, the risk of targeted attacks and exploits on such solutions is directly proportionate. So far, trends revealed that products with a bigger customer base are more prone to advanced threats, however, the security maturity level is definitely higher. Still, concerns of data privacy are revealed, and public key exploits have a larger impact across the clients in case of a breach.

2 The research base

The first aspect of the research was focused on testing and evaluating a list of available IoT products in order to reveal and understand a trend in vulnerabilities that might affect them. The following list contains the most important IoT products in terms of relevance that were tested as part of this research:

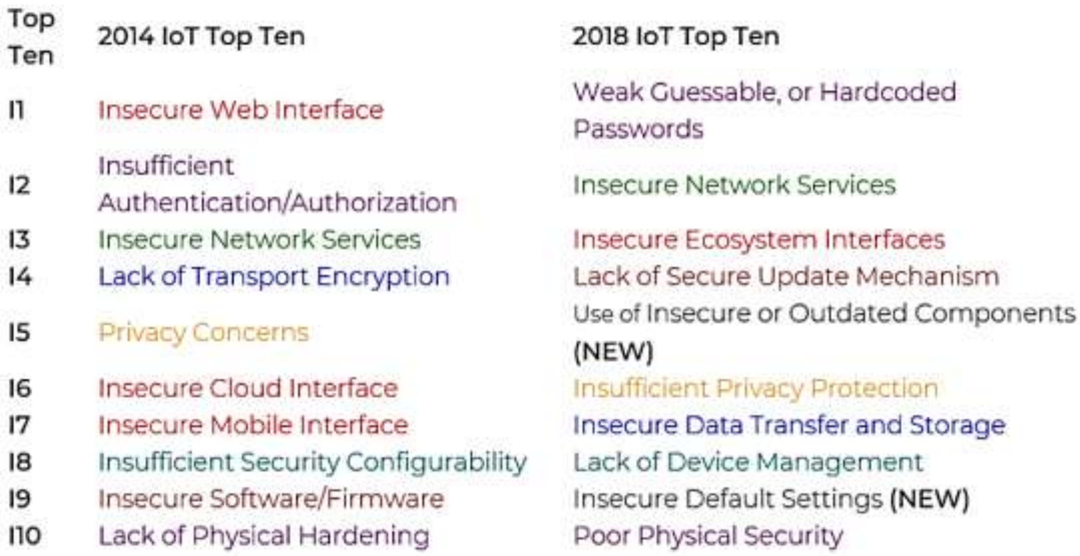
1. Robot device with camera, Wi-Fi capabilities and speakers (an IoT product containing a robot made from hardware pieces, a mobile application that can be linked with the robot via direct Wi-Fi connection, a web application hosted on the robot motherboard and exposed via port 80, a terminal CLI port exposed by the robot and a desktop application that communicates via a predefined port number) [3];
2. Smart gas station (tested a gas station that implements smart payment systems connected locally to multiple servers, the scope also included a card reader, a payment terminal and a point of sale machine defined as a sandbox touch-screen display hosting a Windows system);
3. Fingerprint payment solution (the scope was defined as a set of fingerprint readers implemented in conjunction with a retail payment terminal, a web application linked all the fingerprints and made all the connections);
4. Tire pressure monitoring system (a smart pressure valve inserted inside tires from vendors, using Bluetooth connection to communicate with a custom mobile application);
5. ATM machines (tested multiple ATM machines as part of stand-alone system and payment terminals; testing included lock-picking, security case tests, operating system tests and physical components test like keyboard, touchscreen and hard-drive);
6. Various routers (analyzed internet routers from multiple vendors).

From the provided research projects, some of the most common vulnerabilities that were identified can be categorized into:

1. Missing authorization and authentication (one of the most common and high-risk vulnerabilities identified across the products studied is the lack of authorization for important and critical functionalities such as administration interfaces; cases of default credentials have been identified and exploited, multiple important functionalities such as CLI terminals accessible without any authentication in-place);
2. Injection types of attacks (vulnerabilities such as Cross-Site Scripting, SQL Injection, Remote Code Execution and others have been identified, specifically for products that have embedded web application such as routers and IoT robots; these vulnerabilities are being reproduced due to missing user supplied-input validation and sanitization for many of the inputs exposed by the web applications);
3. Business logic flaws (even though adequate security controls were implemented for web applications, mobile interfaces and other components, the business flow could be exploited in order to cause a high impact on the affected functionalities);

4. Sensitive information disclosure (identifying cases of sensitive information disclosure such as payment details, personal identification information, card details, personal health details, all of them accessible in an unauthenticated or unauthorized manner);
5. Android and iOS mobile applications lacking security best practices (no root detection implemented, missing SSL Pinning mechanisms, source code not obfuscated, exported interfaces without proper external interaction validation; all these practices that were not implemented made room for attack vectors to be identified due to the ease of analyzing the mobile application and its internals);

The methodology for testing the presented IoT products was that of a Penetration Testing engagement, targeting all the components from the network layer perspective, to application layer and included the physical aspect as well.



Top Ten	2014 IoT Top Ten	2018 IoT Top Ten
I1	Insecure Web Interface	Weak Guessable, or Hardcoded Passwords
I2	Insufficient Authentication/Authorization	Insecure Network Services
I3	Insecure Network Services	Insecure Ecosystem Interfaces
I4	Lack of Transport Encryption	Lack of Secure Update Mechanism
I5	Privacy Concerns	Use of Insecure or Outdated Components **(NEW)**
I6	Insecure Cloud Interface	Insufficient Privacy Protection
I7	Insecure Mobile Interface	Insecure Data Transfer and Storage
I8	Insufficient Security Configurability	Lack of Device Management
I9	Insecure Software/Firmware	Insecure Default Settings **(NEW)**
I10	Lack of Physical Hardening	Poor Physical Security

Fig. 1. OWASP Top 10 IoT comparison between latest 2 versions

In Figure 1 we may see the OWASP common standard awareness document for the top 10 threats affecting the IoT products according to the open community of the OWASP foundation. This document represents a baseline of reference and a broad consensus about the most critical security risks of specific IT areas. The last two tops for the IoT area are the 2014 and 2018 versions. In both versions we may notice key differences, common points and an evolution of the risks associated with the IoT field. On the most recent 2018 version, the first risk is represented by the weak or hard-coded credentials used by the systems. This issue is strongly related to what the recent public IoT attacks are showing, with an increase in the brute-force attacks targeted towards authentication mechanisms as ways to compromise the products. [13] The same top threats can be mapped on our previously found issues as well, with the most critical ones being present in the majority of situations.

3 Vulnerabilities and Malware Incidents

An attack chain for a compromised IoT device can usually be linked to patterns that have similar root causes. Often times, we see attacks that gain initial access using low-hanging fruits such as default passwords, exposed administrative console or any of the vulnerabilities discovered and mentioned in the previous section number 2. The term low-hanging fruits is most of the times associated with vulnerabilities that are easy to find and easy to exploit. The category can start from missing access controls to injection types of attacks and exposed control ports.

Using the initial foothold obtained, the attackers are leveraging vulnerabilities to elevate the privileges obtained inside the system. Sometimes, attackers do not even require a system level access in order to abuse the device. This is the case of botnets or spywares where IoT products are "incorporated" into the attacker's network of infected products and used, for example, as DDoS machines, as a pivot system inside a local network or a proxy server.

Some common features regarding IoT products such as routers are related to vulnerable VPN tunneling. This is an important aspect as VPN solutions are usually safe, especially the ones that have strong implementations of open source, up to date, mature VPN solutions. However, outdated software do have vulnerabilities that are publicly known and exploited in the wild. As such, these solutions deployed on specific IoT devices can expose an entire product range [4].

There is also the risk of a product being affected by a publicly available vulnerability [5]. In this case the risk is greater as mass-scanning can be launched across the internet in order to find exposed devices. There are also online services that are active as databases for quickly identifying ports exposed on the internet [6].

By studying popular malware outbreaks, we can make a direct correlation between important, wide-spread CVEs disclosed for popular brands and malware campaigns [7].

An important aspect regarding IoT malware campaigns is the initial payload delivery method. Comparing that with a first stage malware chain for Windows victims, the IoT product requires the attacker's direct contact with the device. Most of the times, the victim will not have direct access to the IoT product compared to the access of a Windows operating system. Attacks such as phishing or accidental malware execution, like Trojans, are not applicable.

There are also concerns regarding data privacy and manipulation or the threat of a backdoor in the product. These concerns are very dependent on the devices' capability of collecting, storing and processing sensitive data. Even though they are not the topic covered in this article, it's worth mentioning that such security flaws can sometimes be exploited by other malicious actors as well. If backdoors are uncovered and exposed or certain privacy risks are being made public, the affected products can become a high-value target to attackers, increasing the risk of being compromised [8].

In terms of research and responsible vulnerability disclosure, we can identify some patterns that are similar to web application development in the early stages of public disclosures. Due to the initial stages of the IoT products, there are but a small number of mature vendors that are enlisting as publicly available for research and testing. This is a big step for a company, as public enrolling can bring great benefits to the overall coverage, but it also requires a certain level of maturity and development. Big companies are always having a bigger advancement level in terms of security and this can be correlated with the allocated budget as well [9].

4 Comparison between IoT, Web and Mobile

The discrepancy between the IoT and other areas such as web development and mobile can be linked with the lack of frameworks, regulations and technology-stack patterns that are currently missing from the IoT area or are underdeveloped. We can compare web development or mobile development in this regard. Currently, there are very mature solutions for webservers, backend and client-side frameworks. We can see a lot of workarounds and limitations when it comes to IoT products. The technologies implemented are relatively primitive to other counterparts in the same area, like webservers deployed on IoT devices and on internet-facing servers.

However, those limitations or workarounds that are implemented are related, on a strong proportion, to hardware specifications. Robust and mature frameworks or operating systems do require more computing power in order to be used at full capacity. This is often an important limitation in an IoT product although we can see improvements in terms of hardware specifications as well [10]. As technology evolves, so are the IoT devices. With more computing power, storage and improvements related to memory, there is also a bigger security level enforced on the devices.

Let us have a slight comparison between the web development and the IoT area in terms of security. In the initial stages of web development, a lot of (easy to find) vulnerabilities were found and reported or

.

abused in the wild. The level of difficulty required to identify and exploit one was exponentially lower compared to today's practice. This can also be seen in the annual reports of public bug bounty platforms [11] and the increased number of targets versus the reported vulnerabilities overall. Of course, when speaking of payment per vulnerability reported, the revenue is also much bigger than previous years but that reflects the level of maturity that the web area has improved in terms of security

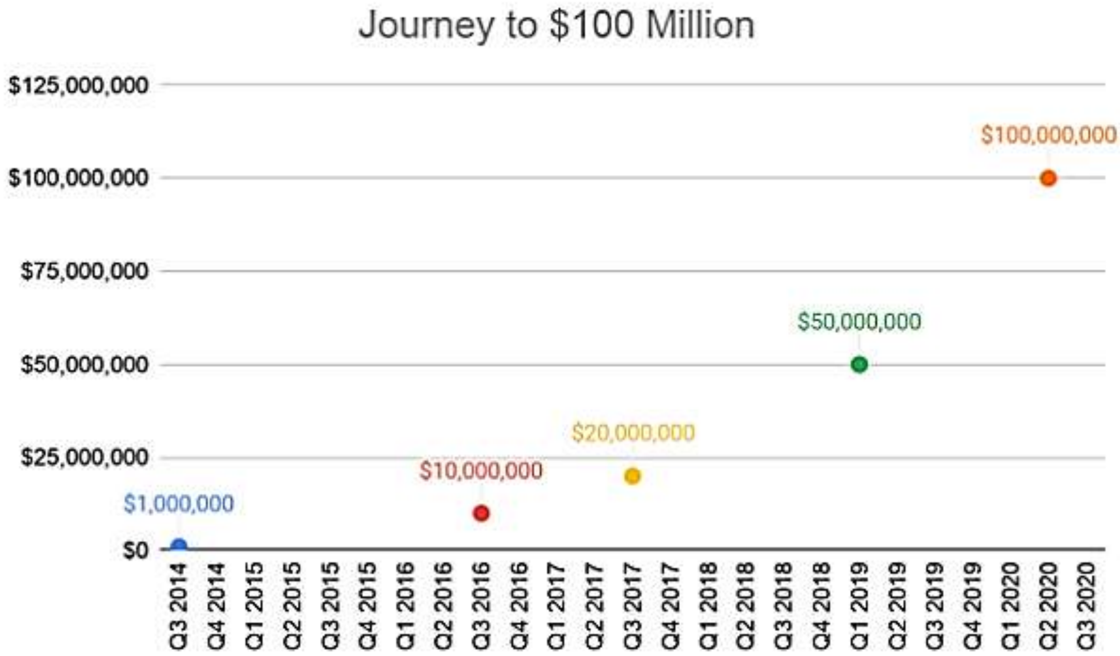


Fig. 2. HackerOne total bug bounty awards 2014-2020

We can expect this from the IoT perspective as well in the next years as the trend was translated in the mobile area too although this can be argued because the mobile area has major big companies that are regulating or controlling important aspects security-related like the development platform, application deployment, operating systems and privacy restrictions.

Some vendors have already started to implement local third-party software to embed inside their products for an increased resistance against outside threat [12]. Antivirus solutions are offering a great protection in terms of malware. Although they don't act like an IPS or IDS network monitoring tool, they do provide protection against publicly known threats, identify malware, malicious behavior and determine potentially compromised devices. This alternative has benefits in terms of size and computing power for the third-party software that is deployed on the IoT device. It is not meant to offer the same protection as dedicated security devices placed on the network level, but it offers a protection alternative installed directly on the IoT device that is adapted to the product's hardware limitations.

5 A Study on IoT Attacks and the Economic Impact

An analysis on some of the most impactful IoT attacks can help in evaluating and estimating the risk and impact of such campaigns, especially from the point of botnet transition and evolution, persistence, anti-detection modules and coverage.

In a case of an IoT complex attack that targets a larger surface of clients, some key aspects regarding the campaign development can be noted. The initial entry vector can be represented by high-risk issues such as default credentials of key services like FTP or SSH, weak passwords or outdated and vulnerable software with publicly known exploits. The initial vector will provide direct access to the device's inner capabilities, allowing an attacker to leverage the foothold in order to pivot inside an internal network, reach other potential IoT devices or directly communicated with a victim's personal or work devices. The persistence is the result of a successful device hijacking scenario, whereby the attacker will obtain long-term access to the device using backdoors, administrative accounts or by other means. Finally, the connection to a command and control server helps an attacker to control and use the newly compromised device for malicious purposes.

The spread of a generic malware campaign can have many parallel vectors such as emails, through some form of web delivery or via a direct channel such as network access to the system. In case of IoT malware attacks, social engineering methods and malevolent emails with payloads have a lower risk for a direct spread since the malware has a low probability of being directly downloaded or executed on and IoT device. However, the likely case of an entry point is through direct access via the compromised host, be it a desktop or a mobile device. A malware might be downloaded by an unknown victim on the desktop host and that particular malware will scan the internal network for any IoT device. An internet facing IoT device will be prone to direct exploitation attempts.

A remote communication and control channel is also used in order to sync the botnet as many IoT attacks are targeting devices for botnet inclusion. Each botnet requires a C&C mechanism in order to be used by the attacker.

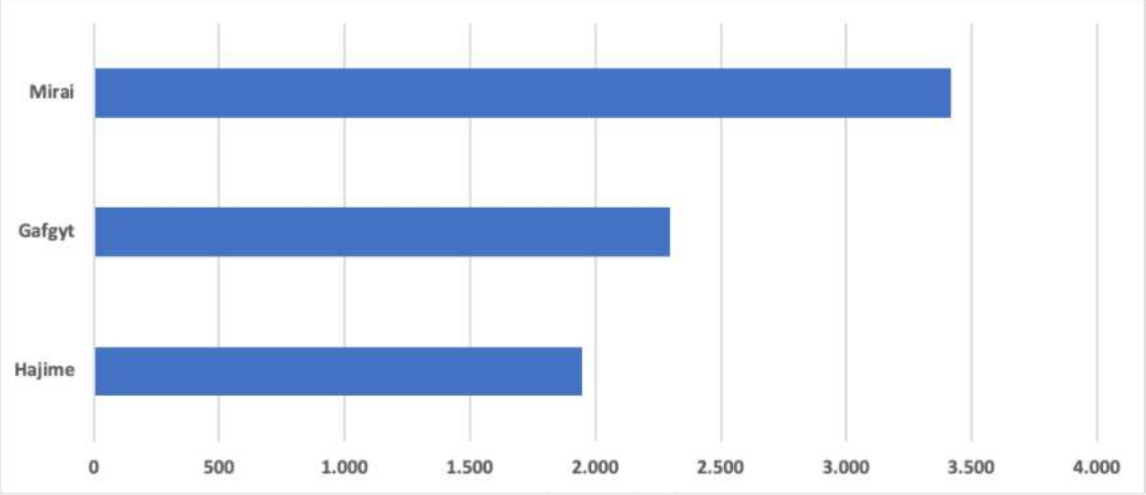
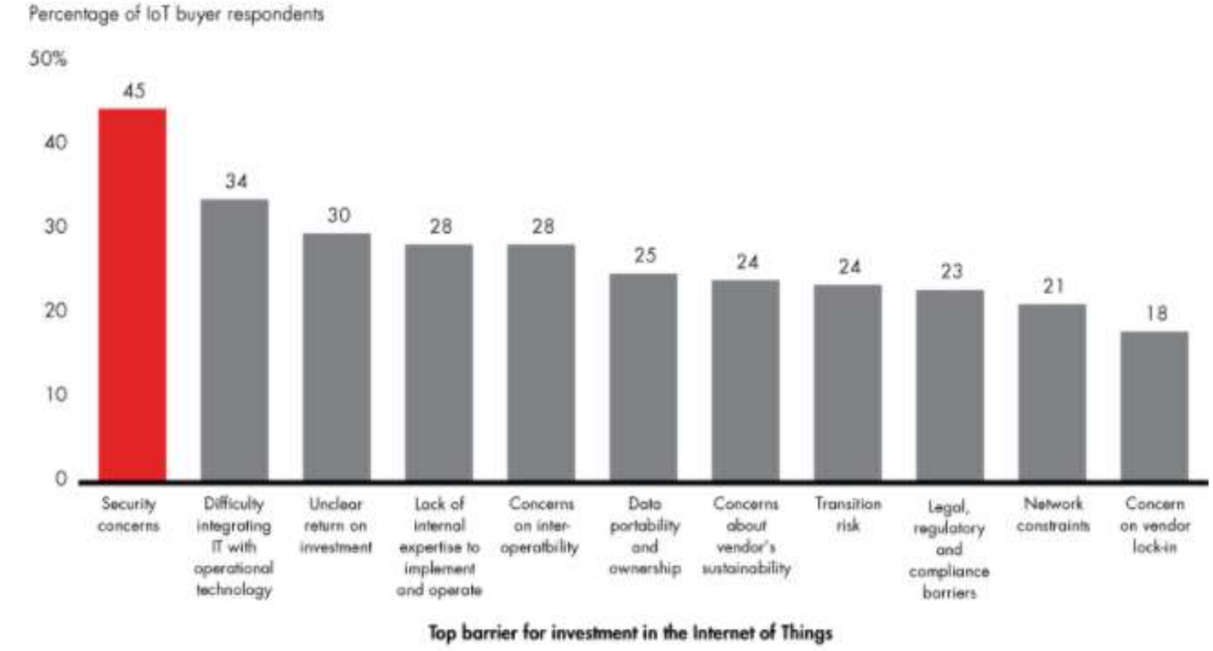


Fig. 3. Top three IoT malware families in 2020 [21]

One of the best scenarios that exemplifies the aforementioned techniques is the *Mirai IoT Botnet*, which is still one of the most prevalent malwares for smart devices, as shown in Figure 3. The Mirai malware is probably one of the most popular attacks on IoT devices that resulted in numerous campaigns including a massive DDoS attack in 2016 (the Dyn Attack) across multiple popular internet targets. The initial Mirai malware is very different compared to the current state whereby attackers are creating variants and new Mirai evolutions with relative ease, since the source code has been made publicly available. Initial access on early stages mostly relied on default credentials for exposed cameras and DVR players, a total number of 61 combinations of username and password were used during the lateral movement phase of the malware. An undetermined number of targets were exposed to this attack. At its peak, the DDoS attacks reached around 620 Gbit/s to 1 Tbit/s in terms of network traffic potency, using only a portion of the entire botnet. This attack was based on the usage of 24,000 compromised IoT devices. In time, the malware developed multiple capabilities and functionalities such as usage of zero-days found in routers, including the exploitation of CVE-2014–8361 and CVE-2017–17215 [14]. The full reach of the attack is still undetermined however, a rough estimation would be around 600,000 of hijacked routers. In this specific attack, there was also a estimation of more than $300,000 of total cost for the device owners that got were unknowingly part of the botnet, owning at least one of the compromised devices. [15] The total number in terms of losses created by the Mirai botnet was estimated to be a seven-figure number, the downtime and the DDoS protection were part the assumption as well. This is no surprise as the attacks on IoT products continue to grow and the real consumer costs are still elusive [16].



Source: Bain 2018 IoT customer survey (n=521)

Fig. 4. Top barrier for investment in IoT showing security first [18]

Attackers are seeing IoT devices as low-hanging fruits and the attacks are increasing each year. The vast majority of IoT based attacks are still falling in the DDoS category, with a 75% of these attacks having a compromised infected router as source, followed by connected cameras with 15%. [17]. The security concern still remains a leading barrier for IoT adoption in the market.

6 Discussion

The series of attacks that affected IoT devices from past years brought an attention to the technical and regulatory challenges of securing and managing the IoT systems. A short comparison between the IoT area versus the general desktop/server and mobile side reveal key differences such as a baseline of general frameworks and operating systems like Windows, Android, iOS, macOS that offer a confident level of security maturity and development and lay the foundation for software development in a more controlled manner in terms of security and compliance to standards. In the IoT field, we see a lot more diversification in terms of general software usage and the technology stack frame used [19]. From a security perspective, these differences are considerable and a similarity to early days of desktop malware can be interpreted. Solutions are still young in their development lifecycle and the adoption of more general baseline software is still pending.

One of the important aspects is the general security hardening of the devices. Default or weak credentials, unprotected login forms or weak password policies are still an increasing threat and latest attacks and malware campaigns are showing that clearly. From honeypots placed in the wild, we notice extensive brute-forcing attempts on remote access protocols such as FTP and SSH for IoT related devices. In terms of network protocol usage, in current state, the majority of IoT devices have fully opened ports exposed by the systems allowing for an easier external communication. Instead, a closed-port and network restriction policy should be implemented in order to limit the unintended client interaction and restrict network level access.

Automatic updates require modular software architecture and a secure trusted update mechanism that can be reliable to offer secure firmware upgrades and updates in case of a zero-day patching or code replacement. Desktop and mobile operating system already offer this feature which has been developed and hardened to ensure that developers are able to quickly patch important issues. Automatic updates are not a trivial task to implement but IoT developers must provide a secure mechanism that is able to patch and correct any vulnerability or zero-day. [20]

Notifications and restrictions represent the client-developer communication in terms of attacks or known issue and security concerns. The major difference in the variety of device ownership creates a complicated situation whereby bulletins or public alerting systems cannot easily pin-point or communicate security breaches affecting a specific set of IoT devices. Communication with the client is always an important aspect to take into consideration in case of attacks and IoT developers can help by providing a clear breach notification channel along with a secure automatic update flow in order to mitigate any vulnerability as soon as possible. Sometimes, a reactive action from the consumer, such as changing the default password, will be required. This action falls, again, in the same category of notifying and enforcing secure policies across the entire IoT ecosystem. Optional notifications about incoming or successful connections to different ports and services should also be considered, as a logging mechanism designed for the user to be aware of the device's external network interactions.

Proactive vulnerability discovery and responsible security evaluation of products must be integrated in an organic SDLC workflow.

There is a lack of generalization for many key areas such as operating system layer protections, binary protections, network level port management, an uniform mechanism to identify firmware and model version. IoT manufacturers could start adopting a more uniform approach for a better third-party integration, a more secure general framework that can represent a backbone for development and strive for an alignment to market standards and procedures comparable to mobile and desktop.

Finally, certifications for product security compliance might be a solution to achieve a uniform way in which the IoT industry can adopt security best practices and standards.

7 Conclusions

The IoT security area represents the security of a larger spectrum of technologies combined into a standalone product. Hence, the attack surface can be significant in width while also limited in terms of architectural deepness and complexity. Hardware capabilities and their limitations play an important role in the product development maturity level. As multiple frameworks and technology stacks are emerging, so are the standards for security best practices and implementations. IoT devices are considered an area of interest for the attackers that are especially looking to compromise internal networks or hijacking devices for DDoS scenarios, although the number of DDoS attacks started to see a decline in recent quarters. Compromised IoT devices are acting as pivots and backdoors inside internal networks. Vulnerabilities affecting popular products are the primary drive when it comes to malware attacks on IoT devices, especially vulnerabilities that are affecting base software components. A majority of the IoT products are functioning offline or standalone however, important functionalities and features are usually linked to some form of connectivity to the internet or with other local devices. That inter-connectivity between endpoints can expose components and networks. There are also privacy concerns linked to IoT products that are non-related to attacks and exploits. Sensitive client data manipulation, third party processing and the general data protection play an important role when it comes to client's trust and security. Functionalities and capabilities are dictating, in this case, the sensitivity and the importance of product security and data privacy. Functionalities such as video and audio recording hold the biggest attention due to the nature of processed information. We see a significant increase in popularity, market value and share as IoT products are becoming a big part of our environment. This surge is directly linked with the number of threats that are showing an advance, pointing that security levels should be prioritized accordingly as the technology increases even further. The most impactful attacks on IoT systems have demonstrated us that in multiple cases, unsophisticated attacks such as dictionary brute-force for credentials could compromise hundreds of thousands of IoT devices and create significant monetary damage across the industry.

References

[1] A. Guzman and A. Gupta, IoT Penetration Testing Cookbook: Identify vulnerabilities and secure your smart devices. Packt, 2017.

[2] A. Gupta, The IoT Hacker's Handbook. Apress, 2019.

[3] S. Nicula, Robot hacking research, September 22, 2017. Accessed on: Sept. 22, 2017. [Online]. Available: https://securitycafe.ro/2017/09/22/robot-hacking-research/

[4] C. Cimpanu, New vulnerability lets attackers sniff or hijack VPN connections, December 05, 2019. Accessed on: March 10, 2020. [Online]. Available: https://www.zdnet.com/article/new-vulnerability-lets-attackers-sniff-or-hijack-vpn-connections/

[5] I. Adascalitei, "Smartphones and IoT Security," Informatica Economica Journal, vol. 23, no. 2/2019, pp. 63-74, 2019.

[6] Shodan, 2009. Accessed on: Jan. 15, 2020. [Online]. Available: https://www.shodan.io/

[7] D. Demeter, M. Preuss, Y. Shmelev, Iot: a malware story, October 15, 2019. Accessed on: Feb. 01, 2020. [Online]. Available: https://securelist.com/iot-a-malware-story/94451/

[8] C. Cimpanu, Researcher: Backdoor mechanism still active in many IoT products, February 04, 2020. Accessed on: Feb. 04, 2020. [Online]. Available: https://www.zdnet.com/article/researcher-backdoor-mechanism-still-active-in-many-iot-products/

[9] D. Bradbury, Why Successful IoT Bug Bounties Are So Rare, October 02, 2019. Accessed on: Dec. 21, 2019. [Online]. Available: https://www.infosecurity-magazine.com/infosec/why-successful-iot-bug-bounties/

[10] A. Clim, "Cyber Security Beyond the Industry 4.0 Era. A Short Review on a Few Technological Promises", Informatica Economica Journal, vol. 23, no. 2/2019, pp. 34-44, 2019.

[11] HackerOne, 2019 Hacker Report. - HackerOne, August 21, 2019. Accessed on: Aug. 22, 2019. [Online]. Available: https://www.hackerone.com/sites/default/

files/2019-02/the-2019-hacker-report_3.pdf

[12] Avira, Avira and TP-Link Join Forces to Offer Wi-Fi Routers with IoT Security for the Smart Home, September 17, 2019. Acessed on: Sep. 17, 2019. [Online]. Available: https://www.avira.com/en/press/avira-and-tp-link-join-forces-to-offer-wi-fi-routers-with-iot-security-for-the-smart-home

[13] OWASP Internet of Things, Internet of Things (IoT) Top 10 2018, November 1, 2019. Accessed on: Novemeber 1, 2019. [Online]. Available: https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=IoT_Top_10

[14] Wikipedia contributors, Mirai (malware), Wikipedia, The Free Encyclopedia, December 12, 2020. Accessed on: January 5, 2021. [Online]. Available: https://en.wikipedia.org/w/index.php?title=Mirai_(malware)&oldid=993766835

[15] C. Osborne, Mirai DDoS attack against KrebsOnSecurity cost device owners $300,000, May 9, 2018. Accessed on: November 23, 2020. [Online]. Available: https://www.zdnet.com/article/mirai-botnet-attack-against-krebsonsecurity-cost-device-owners-300000/

[16] F., Kim H., Kurt Hepler, R. Raghavan and P. Rowland, “Quantifying Consumer Costs of Insecure Internet of Things Devices.”. [Online]. Available: https://www.semanticscholar.org/paper/Quantifying-Consumer-Costs-of-Insecure-Internet-of-Fong-Hepler/73968dfe4ab7c885ab5d7b51815d3b25d8d92640

[17] D. B. Davis, ISTR 2019: Internet of Things Cyber Attacks Grow More Diverse, April 4, 2019. Accessed on: December 12, 2020. [Online]. Available: https://symantec-enterprise-blogs.security.com/blogs/expert-perspectives/istr-2019-internet-things-cyber-attacks-grow-more-diverse

[18] S. Ali, A. Bosche and F. Ford, Cybersecurity Is the Key to Unlocking Demand in the Internet of Things, June 13, 2018. Accessed on: June 28, 2020. [Online]. Available: https://www.bain.com/insights/cybersecurity-is-the-key-to-unlocking-demand-in-the-internet-of-things/

[19] G. Attlee, "An impact review on Internet of Things attacks", International Conference on Emerging Trend in Networks and Computer communications, May 2015. Available: https://www.researchgate.net/publication/280385693_An_impact_review_on_Internet_of_Things_attacks

[20] V. Hurtoi, D. Avadanei, “IoT Project Management”, Informatica Economica Journal, vol. 24, no. 3/2020, pp. 75-80, 2020.

[21] Avira Protection Labs, Malware Threat Report: Q2 2020 Statistics and Trends, September 29, 2020. Accessed on: September 30, 2020. [Online]. Available: https://www.avira.com/en/blog/malware-threat-report-q2-2020-statistics-and-trends

Stefan NICULA graduated from the Faculty of Cybernetics, Statistics and Economic Informatics of the Bucharest University of Economic Studies in 2016 and followed a Master's degree in IT&C Security at the same university. He is a threat researcher and pentester with over 5 years of experience. His areas of expertise are in penetration testing, malware analysis, reverse engineering, and exploitation techniques, with a passion for Windows internals, vulnerability research, exploit development, and mitigation techniques. At present he is pursuing a PhD in Information Security at the Bucharest University of Economic Studies, focusing on heap memory exploits on browsers, Windows kernel vulnerabilities and fuzzing Windows API functions. Current publications and public presentations held by Stefan are covering areas such as IoT security evaluation and Windows binary exploitation, latest malware trends and recent developments in the exploit development field.

Răzvan Daniel ZOTA has graduated the Faculty of Mathematics – Computer Science Section at the University of Bucharest in 1992. He has also a Bachelor degree in Economics and a postgraduate degree in Management from SNSPA Bucharest, Romania. In 2000 he has received the PhD title from the Academy of Economic Studies in the field of Cybernetics and Economic Informatics. From 2010 he is supervising PhD thesis in the field of Economic Informatics, part of the Doctoral School of Economic Informatics in the Bucharest University of Economic Studies.