CYBERSECURITY RISKS IN INTERNET OF THINGS SYSTEMS

Eduard SMELOV[1*], Bogdan CORNIEVSCHI[1], Nichita POPOV[1]

[1]Department of Software Engineering and Automation, gr. FAF-222, Faculty of Computers Informatics, and Microelectronics, Technical University of Moldova, Chisinau, Republic of Moldova

*Corresponding author: Eduard Smelov, eduard.smelov@isa.utm.md

Abstract. *New cybersecurity risks have emerged with the growing prevalence of Internet of Things (IoT) systems. These risks stem from insufficient authentication and authorization, encryption that is not strong enough, and vulnerabilities in software. Cybercriminals can exploit these vulnerabilities to access important data, interfere with infrastructure, and even cause physical damage. To address these risks, organizations must adopt a cybersecurity strategy that is based on risk assessment, implement comprehensive security measures such as network segmentation and intrusion detection, and regularly update their software and firmware.*

Keywords*: authentication, encryption, firmware security, software vulnerabilities, network segmentation, risk assessment.*

Introduction

IoT or the Internet of Things pertains to a group of interconnected devices that communicate with each other and share data. Although IoT has significantly impacted our way of living and working, it has also introduced security threats that require attention. Cybercriminals are attracted to exploit the network's vulnerabilities due to the fast expansion of IoT devices and systems.

The risks associated with IoT systems' security are varied and intricate, ranging from DDoS attacks to data breaches. Cybersecurity risks commonly found in IoT systems include inadequate authentication and authorization, insufficient firmware security, and weak encryption. Attackers can also compromise IoT devices by exploiting software, hardware, and communication protocol vulnerabilities.

The general position in the world in cybersecurity in IoT

As the Internet of Things (IoT) technology advances and becomes more widespread, it is crucial to tackling the security challenges that come with it. The potential dangers and repercussions of cyberattacks on IoT networks are substantial, making it imperative to give priority to the deployment of strong security measures. Therefore, it is vital to comprehend the types of security risks that IoT poses and utilize suitable tactics to reduce them because the aftermath of cyberattacks on IoT systems can be detrimental, including theft of sensitive information, disruption of critical infrastructure, and physical harm. The main threads of IoT and the possible ways of solving them are represented below.

Vulnerability to hacking:

The use of IoT gadgets is on the rise and is anticipated to surpass 75 billion by 2025. Sadly, these contraptions often focus on performance more than safety, leaving them exposed to hacking. This can lead to the stealing of confidential data, or the devices being utilized for malevolent purposes like initiating cyber-assaults on other gadgets or systems. (Figure 1)

One example of this vulnerability is the Mirai malware which was discovered in 2016 and infected and took control of IoT devices such as security cameras and routers. This malware was used to launch serious Distributed Denial of Service (DDoS) attacks, creating widespread destruction and highlighting the possible damage that can be caused by hacking into IoT devices. To counter these threats, producers must guarantee their IoT devices have strong security features, like encryption, firewalls, and secure firmware updates.

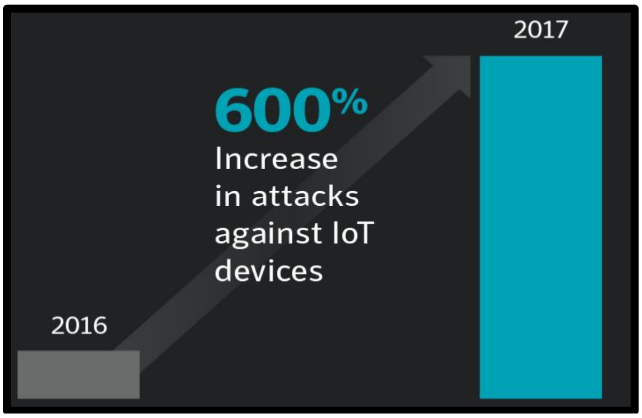


Figure 1. Percentage ratio of cyber attacks

Another example, is a report by the cybersecurity firm Symantec, it was found that IoT devices are attacked every two minutes, and the average IoT device is attacked more than 5,000 times per month [1].

Lack of encryption:

Manufacturers also need to regularly assess their devices for vulnerabilities and provide guidelines for securing them to keep up with changing security demands. Consumers can take steps to protect themselves by changing default passwords and enabling encryption. Consumers should be vigilant and knowledgeable about the most recent cybersecurity threats and best practices to mitigate them. This can potentially impact sensitive information, such as personal data and financial information. A hacker who intercepts unencrypted data transmitted by a smart home device may be able to access sensitive data or even control it as shown in Figure 2.

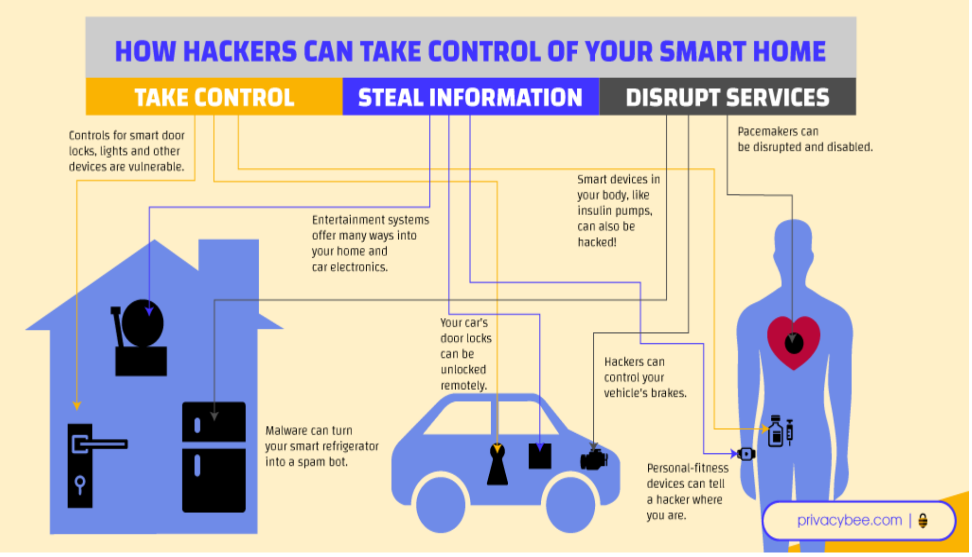

HOW HACKERS CAN TAKE CONTROL OF YOUR SMART HOME
TAKE CONTROL
STEAL INFORMATION
DISRUPT SERVICES
Controls for smart door locks, lights and other devices are vulnerable.
Pacemakers can be disrupted and disabled.
Smart devices in your body, like insulin pumps, can also be hacked!
Entertainment systems offer many ways into your home and car electronics.
Your car's door locks can be unlocked remotely.
Hackers can control your vehicle's brakes.
Malware can turn your smart refrigerator into a spam bot.
Personal-fitness devices can tell a hacker where you are.
privacybee.com

Figure 2. How hackers can take control of your smart home [2]

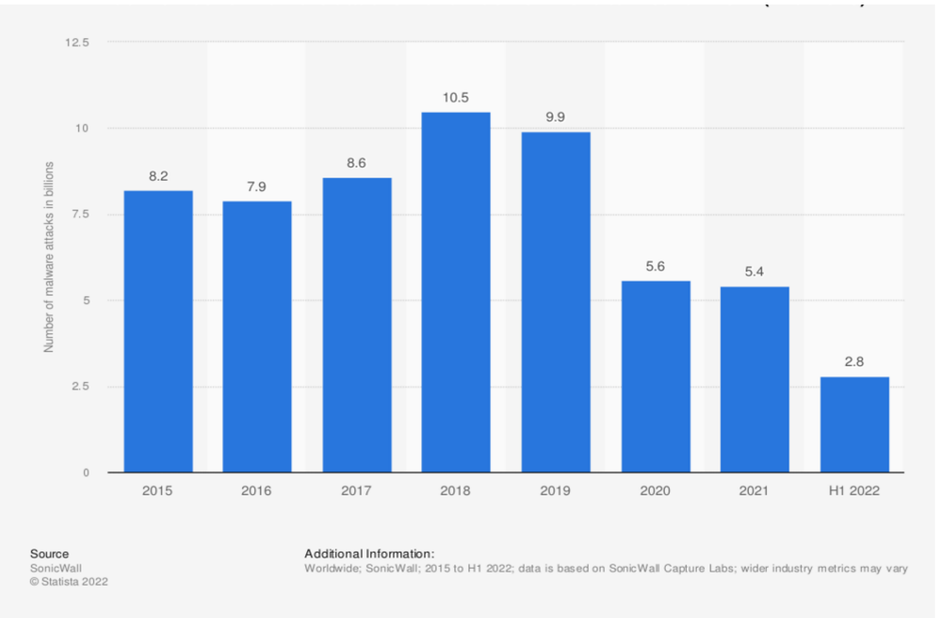
To reduce the chances of problems, producers should prioritize encryption in their items and give customers instructions for keeping their equipment safe. This involves encrypting information sent by the machine, keeping the encrypted data on the device as well as in the cloud, and offering secure methods for updating the firmware.

In addition, shoppers must take an active role in protecting their devices by following the manufacturer's guidelines, such as activating encryption and changing the default passwords. It is imperative to comprehend the potential outcomes of not encrypting data sent by IoT devices and to take the necessary steps to guard against them.

Spread of malware

The proliferation of malware represents a serious risk to connected Internet of Things (IoT) systems, as it can do damage to multiple devices and networks. For instance, a contaminated device can be used to perpetrate attacks on other gadgets or to steal confidential data. Therefore, it is essential to restrict the transmission of malware and guard against cyberattacks due to the integrated nature of IoT systems also including the fact that the number.

To reduce this hazard, producers must make sure their devices are equipped with solid security features to forestall infection from malware and restrict its transmission across IoT systems. This involves firewalls, anti-virus software, and secure firmware updates. They must also give customers instructions on how to protect their devices, such as installing software updates and utilizing anti-virus software. Although over the past 4.5 years, the number of attacks has steadily fallen but is still measured in billions (Figure 3):



Source
SonicWall
© Statista 2022

Additional Information:
Worldwide; SonicWall; 2015 to H1 2022; data is based on SonicWall Capture Labs; wider industry metrics may vary

Figure 3. Annual number of malware attacks worldwide from 2015 to first half 2022 (in billions) [3]

Additionally, customers should also avoid connecting to unsecured public Wi-Fi networks and using weak passwords for their accounts. It's crucial to use strong and unique passwords that include a mix of upper and lower case letters, numbers, and special characters. Furthermore, customers should be cautious when opening emails from unknown senders or clicking on links and attachments in those emails. They should also verify the authenticity of websites before providing any personal or financial information. By following these simple steps, customers can ensure the security of their devices and safeguard their personal information from cyber threats.In summary, it's the joint responsibility of both the manufacturers and customers to take all the necessary precautions to protect devices and personal information from cyber threats, and by following these guidelines, everyone can contribute towards creating a more secure online environment.

Economic impact

The fiscal repercussions of cyber-attacks on IoT systems can be tremendous, including expenses for victims' compensation and repair. Take, for instance, a cyber-attack on an IoT system that can cause data theft, theft of intellectual property, or other harm, leading to financial losses for the affected people or corporations. The financial effect of security issues with IoT systems can also reach out to the broader economy as IoT systems become increasingly important in multiple industries and supply chains. To minimize these risks, businesses must spend on cybersecurity initiatives to reduce the economic impact of cyber-attacks on IoT systems. This includes putting into place firewalls, anti-virus software, secure firmware updates, and conducting regular security evaluations.

Network segmentation and intrusion detection in IoT systems:

The act of dividing a network into smaller, separate subnetworks is known as network segmentation. This practice is useful in reducing the risk of attack and stopping compromised devices from affecting other parts of the network. VLANs, DMZs, and micro-segmentation are all types of network segmentation that offer varying levels of security and isolation. Intrusion detection is the process of monitoring network traffic to detect signs of unauthorized access, malicious activity, or other security threats. In IoT systems, intrusion detection can help identify abnormal behavior which may indicate a potential threat, including unexpected data transfers or unusual communication patterns [1]. Two primary types of intrusion detection exist signature-based and behavior-based, each with its own benefits and drawbacks.

The table below contains the key definitions of theme Network Segmentation. In addition, this information can serve as a summary of this topic. Moreover, for a better understanding of the chapter, it is recommended to get familiar with data from *Table 1.*

Table 1

Key Information on Network Segmentation

Topic	**Crucial information**
Network Segmentation	The practice of dividing a network into smaller, isolated subnetworks
Types of Network Segmentation	VLANs, DMZs, and micro-segmentation
Benefits of Network Segmentation	Reduces attack surface, prevents compromised devices from affecting other parts of the network
Intrusion Detection	The process of monitoring network traffic for signs of unauthorized access, malicious activity, or other security threats
Types of Intrusion Detection	Signature-based and behavior-based
Benefits of Intrusion Detection	Helps to identify anomalous behavior that may indicate a threat
Challenges	Complexity of implementation, maintaining visibility and control over network traffic and devices, ensuring compatibility with legacy systems or devices

Therefore, the presented table provides great value for readers who are not into IoT theme, giving a chance to get familiar with the main definitions of the topic.

Authentication and authorization challenges in IoT systems:

The security of IoT systems is dependent on two crucial factors, namely authentication, and authorization. Authentication involves verifying the identity of the user, device, or application seeking to access the network or data. Authorization, on the other hand, determines whether the user, device, or application has the required permissions to access particular data or resources.

In IoT systems, authentication and authorization can be challenging due to a large number of devices and the complexity of managing access control. Here are some of the key challenges[2]:

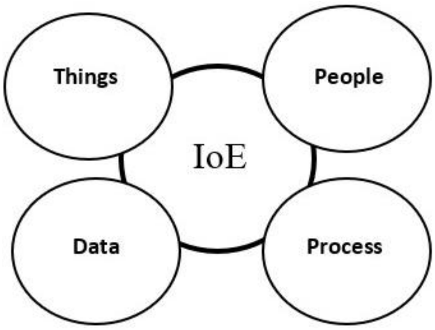
1. Device Diversity: IoT systems typically consist of a wide variety of devices from different vendors, with different operating systems, firmware, and security capabilities. This can make it difficult to establish a standardized authentication and authorization process across the entire system.

2. Limited Resources: Many IoT devices have limited processing power, memory, and battery life, which can make it difficult to implement strong authentication and authorization mechanisms.

3. Legacy Devices: Many IoT systems include legacy devices that may not support modern security protocols or may have known vulnerabilities that can be exploited by attackers.

4. Scalability: IoT systems can involve thousands or even millions of devices, which makes it challenging to manage and update authentication credentials and authorization policies on a large scale.

Authentication and authorization are crucial elements in ensuring the security of IoT systems. The former involves verifying the identity of the user, device, or application trying to access the network or data, while the latter involves determining if the user, device, or application has the necessary permissions to access specific data or resources [4]. The complexity of managing access control and a large number of devices pose significant challenges in IoT systems (Figure 4). The diversity of devices from various vendors, operating systems, firmware, and security capabilities makes it difficult to establish a standardized authentication and authorization process across the entire system.



Figiure 4. Security and privacy challenges in the internet of everything (IOE) [4]

Man-in-the-middle(MITM):

Man-in-the-middle (MITM) attacks are a major concern for IoT security. Such attacks occur when hackers intercept the communication between an IoT device and its connected network, thereby obtaining access to confidential data. This data can include sensitive information such as login credentials, financial details, and personal data.

There are various ways in which hackers can carry out such attacks, with one popular method being the creation of a fake Wi-Fi hotspot that appears authentic but is controlled by the hacker [5]. Once an IoT device connects to this fake hotspot, the hacker can gain access to and manipulate the transmitted data. The attacker can exploit vulnerabilities in the communication protocol, sniff network traffic, or perform DNS spoofing to redirect traffic to a fake website. In a MITM attack, the attacker can steal sensitive information, such as login credentials, financial data, or personal information. The attacker can also perform session hijacking to take over an ongoing session and perform unauthorized actions on behalf of the user.To prevent MITM attacks, it's essential to use secure communication protocols, such as HTTPS, and avoid using public Wi-Fi networks or untrusted devices. Users can also use Virtual Private Networks (VPNs) to encrypt their traffic and protect their communication from interception.

Here is a simplified view of how it works (Figure 5):

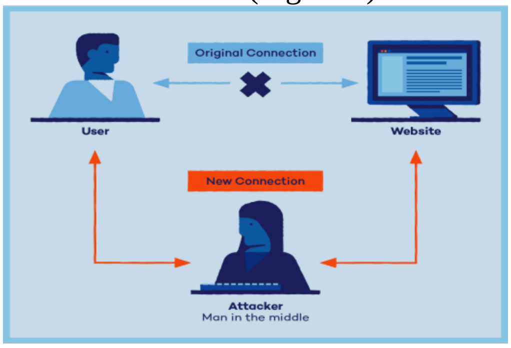


Figure 5. Implementation process of MITM [6]

In order to prevent man-in-the-middle attacks, it is crucial to utilize robust encryption and authentication protocols. Additionally, it is imperative to frequently maintain and repair IoT devices to fix any security weaknesses. Lastly, organizations must adopt a proactive security strategy by continuously monitoring their networks for any suspicious activities. By making security a top priority, we can effectively safeguard against man-in-the-middle attacks and other potential security risks to IoT devices.

Botnets:

Moreover, botnet attacks are becoming more sophisticated as hackers create new strains of malware that are difficult to detect and remove. These malware strains can remain undetected for months, even years, causing significant damage to networks and devices. Additionally, botnets can also be rented out on the dark web to other cybercriminals, enabling them to launch attacks without having to build their botnet from scratch. This makes it even more challenging to track down the origin of an attack.

As IoT devices become more prevalent in homes and businesses, the risk of botnet attacks continues to grow. Many of these devices lack basic security features, making them easy targets for hackers. Even devices with security features can be compromised if users fail to change default passwords or neglect to install security patches.

To combat botnet attacks, it's essential to have robust security measures in place, such as firewalls, intrusion detection systems, and antivirus software. Regularly updating firmware and software on all devices is also critical, as is changing default passwords and disabling unnecessary services. IoT device manufacturers must also take responsibility for the security of their products by implementing robust security protocols and providing regular security updates.

Governments around the world are also taking steps to combat botnet attacks, such as enacting legislation requiring IoT device manufacturers to implement basic security features and providing funding for research into botnet prevention and mitigation.

It's worth noting that end-users must also play their part in preventing botnet attacks by practicing safe internet habits, such as avoiding suspicious websites, downloading files only from trusted sources, and being cautious when opening emails from unknown senders. Moreover, it's crucial to create backups of critical data to minimize the damage caused by a botnet attack. By creating regular backups, users can restore their data quickly in case of a security breach. Finally, it's essential to have an incident response plan in place to address botnet attacks promptly. An incident response plan can help minimize the damage caused by an attack and help organizations recover more quickly (Figure 6).

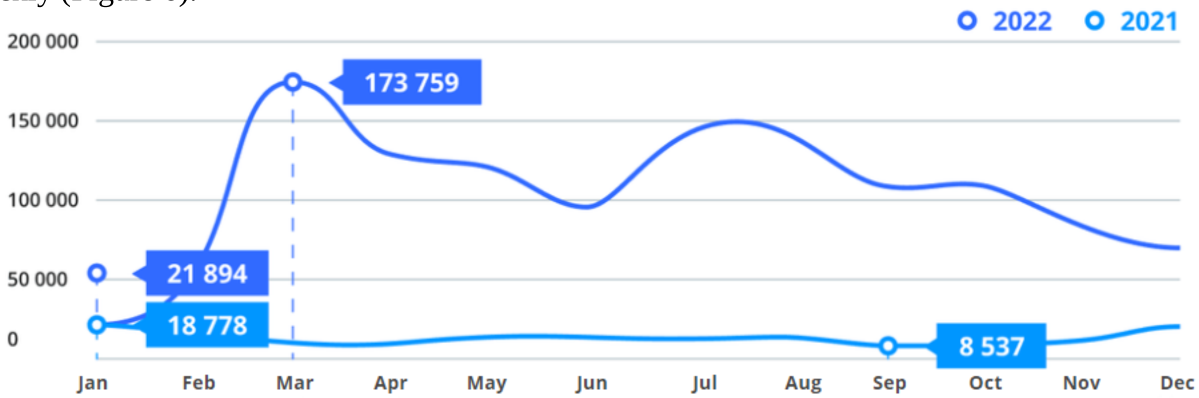


Figure 6. Analytical report DDoS-Guard for 2022 [7]

To prevent botnet attacks, it is crucial to ensure that all IoT devices have strong passwords and up-to-date firmware. Additionally, it is essential to monitor IoT devices for any unusual activity, such as traffic surges or anomalous connections, on a regular basis.

Conclusions

To summarize, while the emergence of IoT systems has resulted in substantial advantages, it has also brought forth intricate cybersecurity threats. To avoid any potential vulnerabilities, businesses that depend on IoT devices need to take a proactive stance toward cybersecurity. This can be achieved by incorporating strong security protocols, regularly evaluating and revising their IoT systems, and minimizing the chances of cyberattacks to safeguard essential data, infrastructure, and people. In the end, prioritizing cybersecurity during the creation and implementation of IoT systems is paramount to ensure their durability and endurance.

References:

1. Acola: Cyber Security Risks in IoT Systems and Techniques for their Mitigation [online][accessed 24.02.23] Available: https://acola.org/wp-content/uploads/2021/02/acola-iot-input-paper_cyber-security-risks-in-IoT-systems_varadharajan.pdf
2. TechTarget: IoT security (internet of things security) [online][accessed 05.03.23] Available: https://www.techtarget.com/iotagenda/definition/IoT-security-Internet-of-Things-security
3. Statista: Annual number of malware attacks worldwide from 2015 to first half 2022 (in billions)[online][accessed 05.03.23] Available: https://www.statista.com/statistics/873097/malware-attacks-per-year-worldwide/
4. Suresh Gyan Vihar University: Security and privacy challenges in the internet of everything (IOE) [online][accessed 06.03.23] Available: https://www.gyanvihar.org/journals/index.php/2021/01/29/security-and-privacy-challenges-in-internet-of-everything-ioe-with-security-requirements/
5. Trendmicro: The IoT Attack Surface: Threats and Security Solutions [online][accessed 09.03.23] Available: https://www.trendmicro.com/vinfo/mx/security/news/internet-of-things/the-iot-attack-surface-threats-and-security-solutions
6. PandaSecurity: What is MITM attack? [online][accessed 09.03.23] Available: https://www.pandasecurity.com/en/mediacenter/security/man-in-the-middle-attack/
7. DDoS-Guard: DDoS Attack Trends in 2022 [online][accessed 06.03.23] Available: https://ddos-guard.net/en/blog/ddos-attack-trends-2022