Global Scientific JOURNALS

GSJ: Volume 12, Issue 5, May 2024, Online: ISSN 2320-9186
www.globalscientificjournal.com

IoT Hacking: Cyber Security Point of View

Ricardo Martins, Hugo Barbosa

Ricardo Martins is currently pursuing degree program in informatics engineering in University Lusofona, Portugal. a22001974@alunos.ulht.pt
Hugo Barbosa, Assistant Professor, Department of Computer Engineering and Information Systems, University Lusofona, Portugal. hugo.barbosa@ulusofona.pt

KeyWords

Intrusion, Detection Systems, IoT, Security, Attacks, Risk, Solucions, Future Prospect.

ABSTRACT

IoT is a very complex thing but very common in our lives. This paper aims to understand what the IoT is and to thoroughly investigate security in IoT devices and networks, going through the most common attacks, the risks and consequences of a successful attack, how to prepare so as not to al-low attacks to succeed, and to predict a future path for security in this area. The IoT is constantly growing and the subject of security is very important to address because leaving it insecure opens the way for malicious people, and hackers, to take advantage of vulnerabilities to steal data and information, which can lead to a great deal of damage, especially for companies that often only care about this topic when an incident occurs. Looking to the future of security is also an im portant point, as predicting and improving IoT techniques and approaches prevents future incidents from happening.

Introduction

The Internet of Things (IoT) has emerged as a revolutionary extension of internet technology, introducing an interconnected network of systems that aim to enable realtime interactions between physical objects, machines and human beings through advanced technologies. Since its first mention in the early 2000s, the term IoT has been widely used in numerous scientific articles, reflecting its growing importance [3]. As IoT expands its reach, security becomes a central concern. This paper analyses common hacking techniques on IoT devices, including man-in-the-middle attacks, malware, distributed denial of service (DDoS), eavesdropping and physical attacks. Understanding these threats is essential to mitigating risks and protecting the integrity of IoT systems. When assessing the impact of successful attacks, the significant influence on companies, both financially and organisationally, is highlighted. The drop in market value, repercussions on operational performance and changes in corporate policies are examined. However, this work goes beyond exposing risks, presenting a comprehensive analysis of defence techniques against cyber attacks targeting the IoT. The implementation of techniques such as network segmentation, secure password practices, regular firmware updates, real-time monitoring and encryption solutions emerges as an effective set of strategies for strengthening IoT security.

Looking to the future, the paper highlights crucial research and development areas, such as the large-scale detection of compromised IoT devices, the incorporation of perception features for security-related applications, the maturity of standardisation and reactive protocol defence frameworks, and the need for robust procedures for the secure development of IoT applications.

This paper is a systematic review and utilizes the Preferred Reporting Items for Systematic reviews and Meta-Analyses (PRISMA) methodology and provides a comprehensive overview of the IoT, from its definition to defence challenges and strategies. Recognising the critical importance of security from the outset of implementation, it seeks to shape a future where intelligent connectivity and reliability coexist, providing a truly effective and secure IoT ecosystem.

Methodology

In this paper it was used as the Preferred Reporting Items for Systematic reviews and Meta-Analyses (PRISMA). PRISMA was first published in 2009, and later updated in 2020. This framework provides guidance for the reporting process of research, rational methods, and findings. Systematic research is important for synthesizing knowledge, addressing complex questions, identifying important research elements, and generating or testing hypotheses they apply. Transparent and accurate reporting is essential to ensure that systematic reviews are useful to a variety of users. Recognizing the developments in systematic review methodology and terminology over the past decade, the revised 2020 PRISMA methodology replaced the 2009 version, as already mentioned, and includes new reporting guidelines on transparency. [12] Compared to the initial version, the checklist now includes sub-items for greater clarity, emphasising transparency by requiring full disclosure of search strategies, the number of results obtained and full citations of included and excluded studies. Thus, the PRISMA 2020 checklist contains seven sections (title, abstract, introduction, methods, results, discussion and further information) with a total of twenty-seven items, some of which include sub-items. [13]

IoT

The term Internet of Things (IoT) first appeared in the early 2000s to describe the concept of the evolution of internet technology and has since been used thousands of times in published scientific articles. [1] The IoT is a network of systems based on the Internet and its aim is to achieve real-time interaction between things, machines and humans through various advanced technologies. A market study found that the global IoT market reached 1.9 billion dollars in 2018 and is expected to reach more than 11 billion dollars by 2026. [2] According to Ben-Daya, Hassini and Bahroun (2019), the internet of things is "... a network of physical objects that are digitally connected to sense, monitor, and interact within a company and between the company and its supply chain enabling agility, visibility, tracking, and information sharing to facilitate timely planning, control, and coordination of the supply chain processes." [3]

The importance of the Internet of Things (IoT) is defined by the advantages it brings to systems and their users. The IoT has revolutionised professional and personal systems, allowing for more control and efficiency in some day-to-day tasks. At a business level, IoT plays a fundamental role as it allows companies to streamline operations more efficiently and at lower cost, automates processes, increasing productivity, and helps minimise waste, for sustainable and ecological practices. As well as being important for companies, it's also important for the customer, who has a better experience. IoT makes it possible to monitor and analyse data in real time to create personalised and more efficient services, which also results in effective management. In short, IoT allows companies to be more profitable and perform better, leading to greater customer satisfaction. [4]

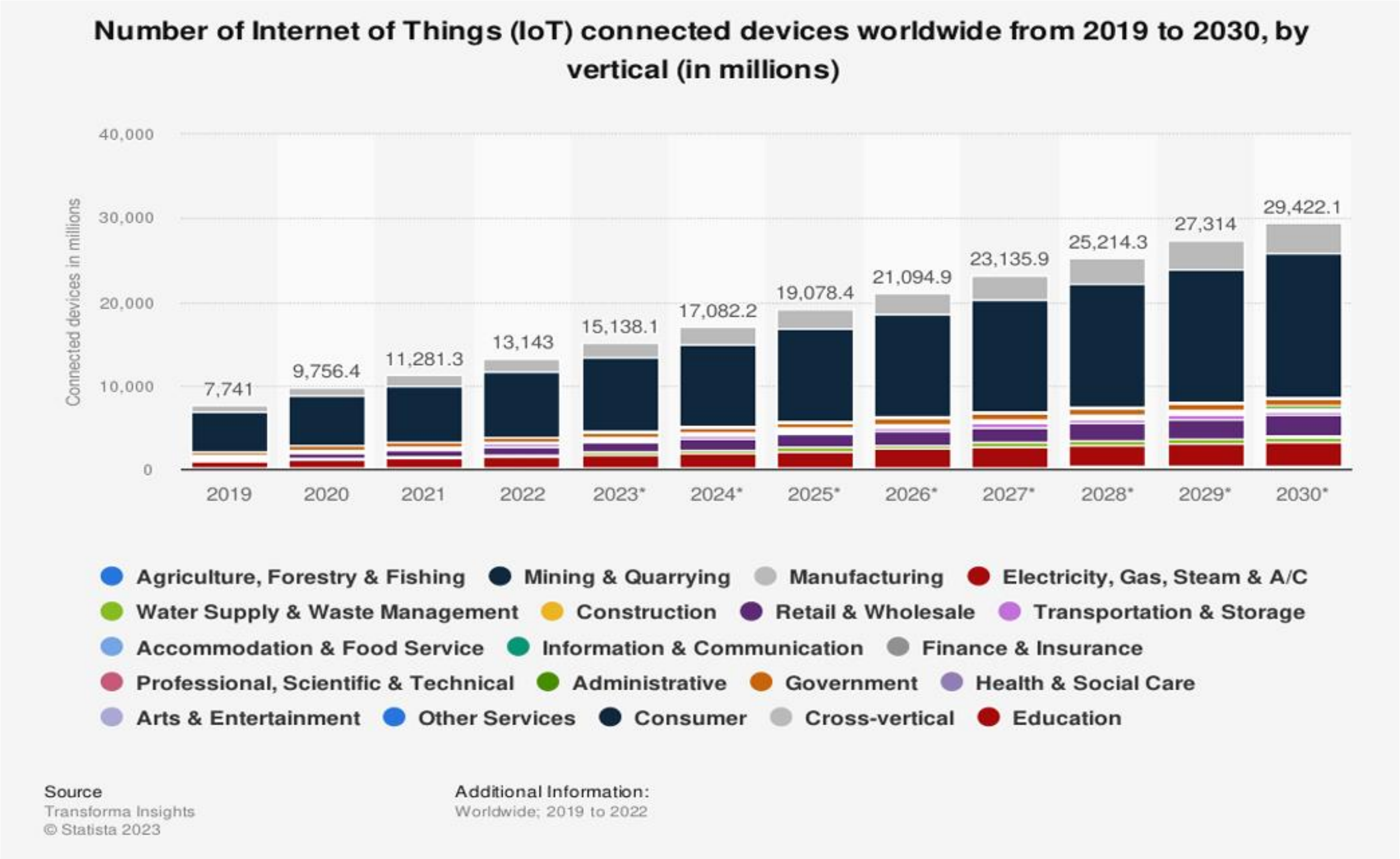

Figure 1. Number of IoT connected devices worldwide from 2019 to 2030. Source: Statista, 2024

Since its inception, the IoT has shown constant growth every year, as shown in a study published on the Statista platform. It evaluates the number (in millions) of IoT devices connected worldwide from 2019 to 2022 and also forecasts this number until 2030. The study vertically separates the different areas in which these devices are used. By 2030 there is expected to be a 123.9 per cent increase in the number of connected devices compared to 2022. Manufacturing, consumer and education are the three largest areas, with the consumer's share significantly larger than the rest. [5]

Common hacking techniques in IoT devices

Description of common hacking techniques in IoT devices: There are various types of attacks that can be carried out on IoT devices, including man-in-the-middle attacks, malware attacks, distributed denial of services (DDOS), eavesdropping attacks and physical attacks.

Man-in-the-middle attack (MITM): This attack consists of, as the name suggests, the hacker positioning himself in the "middle" of communications and intercepting them, accessing their contents and even modifying them.

MITM consists of 5 steps:

- Initialisation: The hacker chooses the target and positions his attack device between the target and the receiver.
- Interception: Decodes data by intercepting communication

- Modification: Changes the intercepted data by adding malicious code or simply modifying the communication.
- Redirection: The data manipulated by the hacker is redirected to the recipient who has no idea that it has been stolen and altered.
- Execution: A successful MITM attack occurs when the recipient executes the malicious code or accesses the modified data. [6]

Malware attack: A malicious software attack, or more commonly known as a malware attack, is carried out by infecting an IoT device giving them access to the device where they can access private and sensitive data, giving the attacker the chance to do whatever they want with it. The most commonly used malware is ransomware, which is nothing more than malicious software that accesses the data on the infected device and encrypts it, leaving the owner of the data without access to it. After this attack, the hackers ask for a sum of money to decrypt it again. [6]

Distributed denial of services (DDOS): This type of attack serves to overload the attacked system and make it inaccessible to legitimate users. The attack consists of sending excessive traffic until the system is shut down. These attacks can cause great damage to the organisations being attacked and the lack of security mechanisms opens the door to a DDOS attack.

DDOS has three stages:

- The attacker gains control of the network and IoT devices with the help of malware.
- The hacker remotely controls each device and directs them to the target's IP address, which causes a port or server overflow due to the hundreds of commands sent in a short space of time.
- The service is closed down because it can't cope with so many requests. [6]

Eavesdropping Attack: The aim of an Eavesdropping attack is to access confidential data without the data owner knowing. The most common way to carry out an Eavesdropping Attack is via wireless communication and threatens the privacy and security of an IoT device. As well as taking confidential data that the device contains, an Eavesdropping attack can also obtain user data that can compromise privacy and security. [6]

Physical attack: A physical attack on an IoT device requires the hacker to be physically near or inside the IoT system. One possible scenario is for an attacker to access a smart home with smart locks and surveillance cameras and use this to gain access to the network and steal private data. [6]

Impact of successful attacks

Attacks can have various impacts on companies, both financially and organisationally. Starting with the impact on the stock market, i.e. on the value of the affected company. According to the study "WHAT IS THE IMPACT OF SUCCESSFUL CYBERATTACKS ON TARGET FIRMS?", published in the National Bureau of Economic Research (NBER) by Shinichi Kamiya, Jun-Koo Kang, Jungmin Kim, Andreas Milidonis and René M. Stulz, cyberattacks, especially those involving the loss of financial data, have a significant and lasting impact on the value of the companies affected. In the same study, they also refer to the impacts on company performance, risk management and corporate policies, concluding that the impact on operational performance is severe. There is no major impact on ROA (A financial acronym for “Return on assets”. ROA it's a profitability ratio that measures how efficiently a company is using its assets to generate earnings. It can be calculated by dividing its net income by its total assets.), ROE (A financial acronym for “Return on equity”. ROE is used to assess a company's profitability, specifically in relation to shareholders' equity. It can be cal culated by dividing its net income by its Shareholders’ equity.) and cash flow metrics, but there is a negative impact on sales growth. With regard to the impact on companies' financial health, cyberattacks have a negative and lasting effect on this sector, since even after 3 years, the S&P credit rating continues to fall. In addition, they also find that companies' investment decreases in the years after the attack, there is more focus on risk management at corporate level and they change remuneration policies in order to reduce incentives to take risks. [7]

In conclusion, companies are affected on several levels after suffering an attack, which makes them rethink their organisation and future decisions.

Cyber-attack defence techniques for the IoT

As concluded above, IoT attacks can cause major damage, especially to companies. It was also seen that companies treat security as an afterthought, i.e. they act only after incidents happen instead of preparing for them so that they don't happen. [8] So what can you do to minimise the risk of a successful attack? There are various techniques that can be implemented in an IoT system to make it more secure.

To implement network segmentation, VLANs and firewall policies are configured to isolate IoT devices, protecting the network from lateral attacks and offering more control over communication between devices. By dividing the network into smaller segments, the attack surface is reduced and the IoT network becomes more secure. [9]

Most IoT devices are shipped with a default password, which opens the door for an attack to be exploited by a hacker. Default passwords should be changed and the company should create a password policy to maintain the security of the system, all because weak passwords are a common vulnerability in IoT systems and are therefore widely exploited by hackers. Guaranteeing unique and secure passwords is crucial for IoT security. [9]

Many IoT devices do not receive regular updates, which can cause problems for the system as non-updated versions can contain vulnerabilities that hackers can take advantage of. Paches and updates should be checked whenever new devices are installed and the latest updates should be applied regularly to ensure the greatest possible security for the IoT network. [9]

Monitoring, reporting and alerting in real time is essential for efficient risk management. This work done in real time enables the integration of next-generation firewalls, taking better advantage of their capabilities and making the IoT system more secure. [9]

Trust in IoT devices allows the full potential of IoT to be utilised. That's why an effort must be made to build an ecosystem of trust from the outset. Security must be applied by computer security experts, using the necessary tools and appropriate mechanisms for each layer in the IoT network. [9]

It's important to understand the risks involved in building an IoT. A general network assessment should be carried out to analyse vulnerabilities and implement the necessary security measures. When using different IoT devices, personalised security measures may be required, so it is necessary to pay attention to every detail of the network to avoid leaving vulnerabilities unresolved. [9]

There are some IoT devices that present a greater risk to the network than others, such as smart speakers. It is necessary to deactivate some features and isolate these devices in separate network segments to ensure greater security. [9]

Encryption can be implemented in various ways and on various different devices, even on devices that have limited resources. Lightweight cryptography is used for the latter. There is also key cryptography (symmetric and asymmetric), which are algorithms that use keys to encrypt and decrypt data. When implementing key cryptography, it is important to define a key management policy to guarantee availability, integrity, confidentiality, authentication and non-repudiation. [10]

Future prospect

In this section, we describe a variety of research and organisational issues and acknowledge some proposals for future work, both technological and non-technical, that we consider worthy of undertaking in this crucial area of IoT security. [11]

The creation and implementation of Internet-scale strategies to solve the problem of security in IoT devices is one of the most critical priorities for future work. Detecting maliciousness, given the widespread implementation of IoT in various private environments, inhibits the disclosure of IoT-related security incidents, making it difficult to properly review this data. Creating methods to collect critical data quickly is a major obstacle for such approaches. The first advantage is that this analysis is non-intrusive, as it does not require support from the IoT network or hardware. The second is related to the compila tion of adequate knowledge, currently inaccessible, to produce IoT-centred malicious signatures. [11]

The secure analytics of IoT devices and information is now addressed by challenges. While gaining access to smart sensors by using default passwords or exploiting vulnerabilities is still an undeniable primary attack, we found that while the necessary strategy is to change the default passwords, many legacy smart sensors still work. While standard password-based access methods are still widely used, the IoT is actively seeking alternatives based on environmental sensing methods however we found a lack of systematic reviews providing a comprehensive understanding of the advantages and disadvantages of these strategies. They should discuss ways and means to increase consumer understanding of the impact of future IoT risks and other technical and non-technical solutions to mitigate the likelihood of exposure. It seems that the testing community needs more thought on ways to implement new certificates and perform regular firmware updates considering the perceived risk of authentication mechanisms, technology interoperability, and IoT a combined use can result from such methods. [11]

While several research efforts consider standardising the IoT protocol, it is clear that they need potential improvements to overcome limitations. The convergence of developments in technology and robust regulatory mechanisms are problems that are still worth addressing in the future. [11]

In order to achieve adequate security in IoT products, an appropriate and timely approach should be applied to the identified vulnerabilities. Static code in IoT systems is another critical issue. IoT systems focus on customized software applications that can be vulnerable in specific ways. Diagnostic tests should be conducted to identify IoT vulnerabilities as long as patches are developed and eventually applied to the IoT computers involved This will also enhance the implementation of risk management in the IoT model and to improve, especially system deployment flexibility -To identify dependencies between suppliers, technologies , system models, and deployment environments for poor programming practices for IoT device deployments in system (CPS) environments will enable a more consistent choice of software providers, while empowering suppliers to develop more complex code needs to be distributed and should develop IoT Self-assessment tools to test various applications, thus further contributing to the security and sustainability of the IoT. [11]

Defining a resource policy is pointless unless it can be implemented throughout the organisation. One of the most important aspects of any IoT platform is figuring out the best way to combine the platform's features with existing procedures to maximise policy compliance during use. The user's governance needs, the size and type of IoT network, and how the IoT is reflected in the cloud subscription architecture are the main elements in deciding the extent of policy enforcement activities. An increase in the scope of policy enforcement can be justified by an increase in network size or a greater need to centrally supervise policy enforcement. All of these attributes must be considered when addressing resource requirements for the IoT network. [11]

Conclusion

In summary, given a comprehensive understanding of the concepts, applications and challenges associated with the Internet of Things (IoT), establishing security practices in our networks from day one of implementation is essential. The adoption of security policies, as detailed throughout this paper, not only strengthens the resilience of IoT networks, but creates key elements such as performance, availability, integrity, and privacy also protect These pillars are necessary to maintain the optimal operation of the IoT network and enable safe and reliable ownership can fulfill the objective In a highly connected environment, trust in device integrity and network security is a top priority By implementing security measures from the beginning, we are not preventing interference not only a variety of possibilities, but we promote an environment for continued innovation and secure IoT expansion. In this way, by recognizing the critical importance of security in the IoT, we can shape a future where intelligent connectivity and reliability and robustness coexist in harmony, paving the way for an IoT ecosystem really effective and safe.

References

[1] M. Dachyar, Teuku Yuri M. Zagloel, L. Ranjaliba Saragih, Knowledge growth nd development: internet of things (IoT) research, 2006–2018, Heli yon, Volume 5, Issue 8, 2019, e02264, ISSN 2405-8440

[2] Jianxin Wang, Ming K. Lim, Chao Wang, Ming-Lang Tseng, The evolution of the Internet of Things (IoT) over the past 20 years, Computers & Industri al Engineering, Volume 155, 2021, 107174

[3] Alex Koohang, Carol Springer Sargent, Jeretta Horn Nord, Joanna Pal iszkiewicz, Internet of Things (IoT): From awareness to continued use, In ternational Journal of Information Management, Volume 62, 2022, 102442, ISSN 0268-4012

[4] https://internationalsecurityjournal.com/why-iot-is-important/

[5] https://www.statista.com/statistics/1194682/iot-connected-devices-vertically/

[6] https://wjarr.com/content/review-hacking-techniques-iot-systems-and-future trends-hacking-iot-environment

[7] Shinichi Kamiya, Jun-Koo Kang, Jungmin Kim, Andreas Milidonis & René M. Stulz, What is the Impact of Successful Cyberattacks on Target Firms?, NBER, 2018, DOI 10.3386/w24409

[8] Phillip Williams, Indira Kaylan Dutta, Hisham Daoud, Magdy Bayoumi, A survey on security in internet of things with a focus on the impact of emerg ing technologies, Internet of Things, Volume 19, 2022, 100564, ISSN 2542 6605

[9] Tan, Jek. (2023). Improving Security for IoT Devices: Safeguarding Against Hacking and Pen Testing.

[10] Phillip Williams, Indira Kaylan Dutta, Hisham Daoud, Magdy Bayoumi, A survey on security in internet of things with a focus on the impact of emerging technologies, Internet of Things, Volume 19, 2022, 100564, ISSN 2542-6605

[11] Tariq Ahamed Ahanger, Abdullah Aljumah, Mohammed Atiquzzaman, State-of-the-art survey of artificial intelligent techniques for IoT security, Computer Networks, Volume 206, 2022, 108771, ISSN 1389-1286

[12] Page MJ, McKenzie JE, Bossuyt PM, Boutron I, Hoffmann TC, Mulrow CD, et al., 2021 The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. PLoS Med 18(3): e1003583. https://doi.org/10.1371/journal.pmed.1003583

[13] http://www.prismastatement.org/PRISMAStatement/PRISMAStatement.as px

[14] J. Gonçalves, H. Barbosa, A Survey of Cyber Security Systems: Approaches for Attack Detection, Prediction and Prevention, Proceedings of the Digital Privacy and Security Conference 2020, pp. 21-32, Porto - Portugal, January 2020 | eoi: 10.11228/dpsc.02.01.002

[15] R. Azevedo, H. Barbosa, Cyber Threats to Mobile Technology Services, International Journal for Research & Development in Technology (IJRDT), Volume-18, Issue-6, pp. 11-26, December 2022, ISSN 2349-3585