FRI-2G.302-1-CCT2-07

A REVIEW ON THE PRESENT-DAY CYBERSECURITY TRENDS, CHALLENGES AND THREATS [20]

Prof. Plamen Zahariev, PhD
Department of Telecommunications,
"Angel Kanchev" University of Ruse
Tel.: +359 82 888 663
E-mail: pzahariev@uni-ruse.bg

Prof. Georgi Hristov, PhD
Department of Telecommunications,
"Angel Kanchev" University of Ruse
Tel.: +359 82 888 663
E-mail: ghristov@uni-ruse.bg

Assist. Prof. Georgi Georgiev
Department of Telecommunications,
"Angel Kanchev" University of Ruse
Tel.: +359 82 888 353
E-mail: gdgeorgiev@uni-ruse.bg

Assist. Prof. Diyana Kinaneva, PhD
Department of Telecommunications,
"Angel Kanchev" University of Ruse
Tel.: +359 82 888 353
E-mail: dkyuchukova@uni-ruse.bg

Abstract: *This paper reviews the present trends, challenges, and threats in the cybersecurity domain. The new generation of attacks in the local, wireless, and global networks are presented and discussed in detail. The commonly used security standards are also analyzed and discussed, as well as the concepts of quantum cryptography.*

Keywords: *Information and Communication Technologies, Cyberattacks, Cybersecurity, Emerging Trends.*

INTRODUCTION

The present-day cybersecurity domain is organized as a complex structure that encompasses many different methodologies, technologies, approaches and solutions. The aim of the modern cybersecurity is focused not only on the data integrity, the network security processes and the user authentication, accessibility or accounting, but also on more complex paradigms, like application security, risk assessment, threat intelligence and the different means for providing effective physical security. All of this is the result of the rapidly increasing number of cybercrimes, which are becoming more diverse, increasingly complex and are causing damage that is estimated to be in the range of several trillions of dollars worldwide, as presented by Fig. 1 (Petrosyan, A., 2023).

The widespread of newer types of threats and attacks in the modern digital world is presenting the need of the modern societies for reliable and secured means and technologies for information processing, data storage and network transfer. These solutions have to be conformable with the advancements in the different industrial domains, as even more and more manufacturers are looking to integrate the most recent technologies in their products. Unfortunately, in many cases these integration efforts are not made according to the best practices and the widely available security

[20] Докладът е представен на научната сесия на 27.10.2023 в секция „Комуникационна и компютърна техника" с оригинално заглавие на български език: ПРЕГЛЕД НА СЪВРЕМЕННИТЕ ТЕНДЕНЦИИ, ПРЕДИЗВИКАТЕЛСТВА И ЗАПЛАХИ В КИБЕРСИГУРНОСТТА

standards and recommendations, which is resulting into numerous software and hardware vulnerabilities and is making the products susceptible to attacks from the hacker armies worldwide.

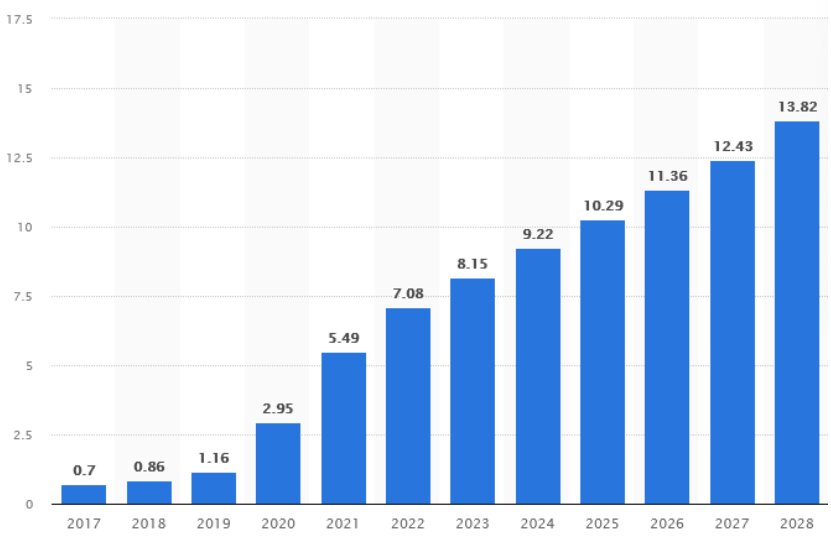

Fig. 1. Estimated (expected) costs of cybercrime in trillion of U.S. dollars (Petrosyan, A., 2023)

PRESENT-DAY CYBERSECURITY CHALLENGES AND THREATS

According to several studies (Babu, F. & Kishore, S., 2018), (Kaur, J. & Ramkumar, K.R., (2022), cyberattacks are occurring more than once every minute and more than eight hundred thousand people are affected annually by different cybercrimes. While some of these attacks are based on well-known and widely studied and analysed methods and scripts, others are novel and are targeted against never before attacked services or devices. In the following list, we have categorized and grouped some of the most recent types of emerging attacks, which we consider to be presenting the trend in the cybersecurity domain:

- **Automotive hacking –** as vehicles get "smarter", their attack surfaces grow. Attacks against the vehicles and the use of vehicles to eavesdrop data or initiate attacks against other devices and the surrounding infrastructure are among the new cybersecurity trends (Fig. 2).
- **Artificial Intelligence (AI) –** AI has evolved to help developers write code. Unfortunately, the hackers are using this opportunity as a tool to develop AI-generated malware and viruses.
- **Deepfakes –** a term that describes the extensive use of synthetic media, which was digitally manipulated using AI to replace or add audio and video content with the aim to commit frauds and to influence the public opinion. These types of attacks are on the rise and can target all levels of the society, including celebrities and government representatives (Fig. 2).
- **Attacks on mobile devices –** our mobile devices contain many photos, emails, messages, financial information, health data, etc. Malware and viruses that target the mobile devices are expected to become the most significant cybersecurity threat in the upcoming 5 years.
- **Could exploitation –** cloud configuration errors can lead to direct exploitation, insertion of malicious software and data breaches.
- **IoT and 5G attacks –** the connectivity between multiple devices opens them to vulnerabilities, exploits and attacks. Reduced levels of security in the IoT architectures and the mobile networks are making them attractive for hackers.
- **Vulnerable libraries and components –** complex websites and apps are very hard to safeguard, as they rely on third-party libraries, which are full of vulnerabilities.
- **Dual-payment ransomware –** a new generation of ransomware is becoming very popular lately. It demands for one payment for the decryption of the stolen information and then analyses the user data and demands another payment to prevent the disclosure of this data.
- **State-sponsored cyberattacks –** high-profile data breaches targeted against political, governmental or industrial organizations and activities are entering the Top-5 of cyber threats.

- **Insider threats –** 1/3 of the attacks are directly or indirectly made by employees and the trend is going up.

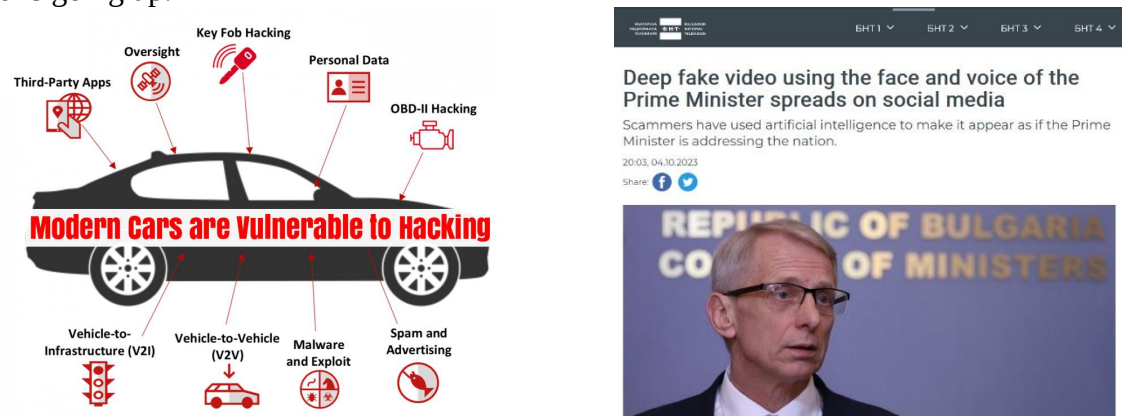

Fig. 2. Vulnerabilities in the modern cars (left), which are used in some of the trending automotive hacking attacks (Li, Y. & Liu, Q., 2021) and a public media announcement for a deepfake video with the Bulgarian Prime Minister, Acad. Nikolay Denkov (right) (BNT, 2023)

EMERGING CYBERSECURITY TECHNOLOGIES

To answer the challenges that are presented by the emerging cyberattacks and threats, the scientific, cryptographic and engineering communities are constantly improving the existing security technologies and are developing new solutions. The trending cybersecurity mechanisms and technologies are presented below:

- **Improved wireless security standards** – in response to the many new attacks against WPA and WPA2 networks, as well as specifically to solve the problems with the KRACK attack, the Wi-Fi Alliance has announced the WPA3 mechanism as a replacement for WPA2.
- **AI for cybersecurity –** AI-powered cybersecurity systems excel in detecting and analysing possible threats. The AI systems can reveal strange patterns or behaviours suggestive of assaults by continually tracking network operations and analysing massive volumes of data. This allows for faster and more precise danger detection, which reduces response times and potential harm (Du, D., Zhu, M., Li, X., Fei, M., Bu, S., Wu, L. & Li, K., 2023).
- **Biometric cybersecurity –** the modern cybersecurity is focused on reducing the risks presented by the traditional passwords, as they have long been a point of weakness for security systems. The Biometric security aims to answer these issues by linking proof-of-identity to our bodies and behaviour patterns.
- **Zero trust cybersecurity –** also known as zero trust architecture (ZTA) or perimeter-less security is an approach to plan, design and implement IT systems. The main concept behind the zero trust security model is “never trust, always verify”, which means that users and devices should not be trusted by default, even if they are connected to a permissioned network, such as a corporate LAN and even if they were previously verified.
- **Blockchain security –** blockchain security is a comprehensive risk management system for the blockchain network, using cybersecurity frameworks, assurance services and best practices to reduce risks against attacks and frauds. The blockchain technology enables decentralization through the participation of the members across the distributed network. There is no single point of failure and a single user cannot change the record of transactions. However, blockchain technologies differ in some critical security aspects (Ribas Monteiro, L.F., Rodrigues, Y.R. & Zambroni de Souza, A.C., 2023).
- **Cloud and IoT Security –** the set of tools and strategies that protect devices connected to the cloud and the network they use to connect to each other. The main goals of the cloud and the IoT security are to keep the user data safe, to stop the cyberattacks and to keep the numerous network devices running smoothly.
- **Quantum cryptography** – one of the most recent additions to the cybersecurity technologies that represents a method for data encryption and decryption that uses the naturally

occurring properties of quantum mechanics to secure and transmitted data in a way that cannot be hacked (Fig. 3).

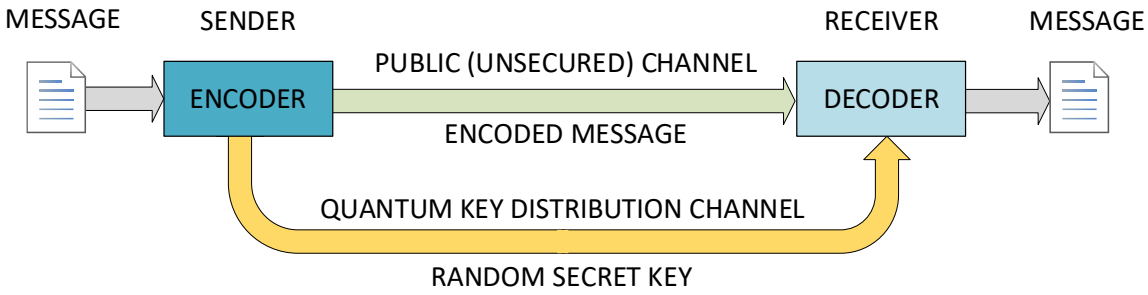

Fig. 3. The operational principles of the quantum cryptography

CONCLUSION

The modern cybersecurity focuses on the network security and the protection of the computers, programs, infrastructure and data from unintended or unauthorized access, destruction or change. The importance of cyber security cannot and should not be underestimated in the present digital world. Our personal information is stored online, critical infrastructure, such as power grids are controlled through computer systems, and even our physical safety can be affected by cyber threats targeting transportation systems or medical devices. All of this makes the cybersecurity one of the most important present-day research and application domains.

ACKNOWLEDGMENTS

The work presented in this publication is completed as partial fulfilment of Project BG05M2OP001-1.001-0004 UNITe, funded by the OP "Science and Education for Smart Growth", co-funded by the European Union.

This article was prepared with the support of Project 2023 – FEEA – 03, financed under the Scientific and Research Fund of the University of Ruse "Angel Kanchev".

REFERENCES

Babu, F. & Kishore, S. (2018). *A Review on Cybersecurity Threats and Statistical Models*, 2018 Conference Series: Materials Science and Engineering, Vol. 396, pp. 1-6, https://doi.org/10.1088/1757-899X/396/1/012029.

BNT. (2023). *Deep Fake Video Using the Face and Voice of the Prime Minister Spreads on Social Media*. BNT. 04.10.2023. URL: https://bnt.bg/news/deep-fake-video-using-the-face-and-voice-of-the-prime-minister-spreads-on-social-media-321680news.html (Accessed 30.11.2023).

Du, D., Zhu, M., Li, X., Fei, M., Bu, S., Wu, L. & Li, K. (2023). *A Review on Cybersecurity Analysis, Attack Detection, and Attack Defense Methods in Cyber-Physical Power Systems*. Journal of Modern Power Systems and Clean Energy, vol. 11, no. 3, pp. 727-743, May 2023, https://doi.org/10.35833/MPCE.2021.000604.

Kaur, J. & Ramkumar, K.R. (2022). *The Recent Trends in Cyber Security: A Review.* Journal of King Saud University – Computer and Information Sciences, Volume 34, Issue 8, Part B, pp. 5766-5781, ISSN 1319-1578, https://doi.org/10.1016/j.jksuci.2021.01.018.

Li, Y. & Liu, Q. (2021). *A Comprehensive Review Study of Cyber-Attacks and Cyber Security; Emerging Trends and Recent Developments.* Energy Reports, Volume 7, pp. 8176-8186, ISSN 2352-4847, https://doi.org/10.1016/j.egyr.2021.08.126.

Petrosyan, A. (2023). *Annual Cost of Cybercrime Worldwide 2017-2028.* Statista, URL: https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide (Accessed 30.11.2023).

Ribas Monteiro, L.F., Rodrigues, Y.R. & Zambroni de Souza, A.C. (2023). *Cybersecurity in Cyber–Physical Power Systems.* Energies, vol. 16, no. 12, https://doi.org/10.3390/en16124556.