31st National Conference with International Participation "Telecom 2023", November 16 - 17, 2023, Sofia, Bulgaria

CyberAttacks and robotics

Grozdan Hristov
Computer systems dept.
Technical University of
Sofia Sofia, Bulgaria
grozdan.hristov@dir.bg

Ivan Stankov
Cybersecurity dept.
Technical University of
Sofia Sofia, Bulgaria
istankov@tu-sofia.bg

Dayana Mladenova
Computer systems dept.
Technical University of Sofia
Sofia, Bulgaria
dayanamladenova97@gmail.com

2023 31st National Conference with International Participation (TELECOM) | 979-8-3503-0329-2/23/$31.00 ©2023 IEEE | DOI: 10.1109/TELECOM59629.2023.10409708

Abstract — As artificial intelligence and robotics continue to be integrated into our daily lives, there is a growing concern over potential vulnerabilities and their exploitation. The threats that arise from cyberattacks on robots and AI systems can lead to significant damage to both the system and the user. This article aims to explore the possible connections, threats, and implications for the fields of artificial intelligence, robotics, and cyberattacks. It provides an overview of common forms of cyberattacks, defines robots and artificial intelligence, and examines some of their various applications.

Keywords — cyberattacks, artificial intelligence, robots, robotics, cybersecurity, machine learning

I. Introduction

In today's society, technology is becoming increasingly intertwined with human activity and is relied upon more heavily than ever before. Over the past decade or so, there has been a significant and rapid rise in the use of technology for a wide variety of tasks, including facilitating communication, automating work processes, and simplifying household chores. According to a May 2018 survey conducted by Intel on 1,000 adults in the United States, approximately 53% of respondents stated that they heavily depend on technology to stay connected with their loved ones, while about 46% reported the same level of dependence when it comes to paying their bills. This trend is expected to continue increasing in the coming years [1].

As the trend towards increased reliance on technology continues, particularly in the fields of information technology and computer science, it is likely that artificial intelligence (AI) and robotics will become even more prevalent in the lives of everyday people. While this will create numerous opportunities and make life more convenient, it will also give rise to new challenges, such as higher incidence of cyberattacks and an increased likelihood of the misuse of high-tech solutions for purposes other than direct cyberattacks.

II. CYBERATTACKS – DEFINITION AND TYPES

A. Definition

According to the Cambridge dictionary, a cyberattack is defined as an unlawful effort to undermine a computer system or the data it holds via the internet [2]. IBM, a leading technology company, characterizes a cyber-intrusion as an undesired endeavor to pilfer, unveil, modify, incapacitate, or obliterate information through unauthorized access to computer systems [3]. The Computer Security Resource Center (CSRC) of the National Institute of Standards and Technology (NIST), an agency within the US Department of Commerce, provides three different definitions of a cyberattack, including an attack targeting a company's use of cyberspace, with the intent of disabling, disrupting, or maliciously manipulating the computing environment/infrastructure, compromising data integrity, or purloining controlled information [4]. As can be seen, there is no single, agreed-upon definition of what constitutes a cyberattack, but the basic premise is that it refers to any hostile behavior directed towards information systems or data via cyberspace.

B. Types

The numerous forms of cyberattacks can be categorized according to their activity, objective, actor, etc. One of the most popular categories is separating system-based from web-based intrusions. Cyberattacks can also be classified as either active or passive, based on their activity. An active attack aims to alter the system resources of the target in a specific way or disrupt their operation, while a passive attack seeks to gather information from the target without altering its resources.

When a cyberattack targets a substantial entity like an institution or a nation, it becomes possible to trace its origin. An internal breach is instigated by an entity or entity within the security boundaries that possess legitimate access to the target's information system resources. Conversely, an external breach is orchestrated by an unauthorized user situated beyond the security confines. These perpetrators may encompass novice hackers or even antagonistic government entities. [5].

1) System-based cyberattacks

System-based cyberattacks, unlike web-based attacks that target hosts, target applications. Malware programs such as viruses, worms, and Trojans are used for these types of attacks. Malware is a type of software designed to inflict damage on a system or a part of a system. System-based cyberattacks have the potential to incapacitate the target or provide the attacker with administrative privileges, facilitating remote control. A computer virus shares similarities with biological viruses as it is engineered to propagate across systems, aiming to replicate itself and assume control or inflict harm. Replication transpires as the virus embeds its code instructions into a host program, with these viral directives assuming precedence during program execution. It is important to note that a computer virus always requires a host program to achieve its programmed goal [8].

In contrast, a worm operates independently and doesn't rely on a host program. A computer worm consists of a program or code fragments that can exist autonomously, with its primary objective being the complete destruction of the host system. Upon infiltrating a new environment, a computer worm typically initiates a network scan to identify opportunities for further propagation before initiating harm to the host system. Unlike viruses, which often corrupt or

979-8-3503-0329-2/23/$31.00 ©2023 IEEE

alter files on the target machine, worms invariably impose some form of impact, even if it's merely by consuming network bandwidth [8]. It's worth noting that certain worms are designed solely to pass through a system without attempting alterations, yet they can still disrupt network communication or cause other undesired consequences.

A Trojan or Trojan horse is a type of malware that disguises itself as a legitimate program, deceiving users and systems about its true intentions. The name comes from the ancient story of the Trojan wooden horse that ultimately led to the fall and capture of the city of Troy. Unlike viruses and worms, Trojan horses do not have the ability to replicate themselves and use other methods to spread, often relying on social engineering tactics. [9].

2) Web-based cyberattacks

The discussion will begin with the initial category of web-based cyberattacks, which is the injection attack, specifically focusing on Structured Query Language (SQL) injection. In a broader context, an injection attack empowers an actor to make queries or install malicious software on a system with the intention of executing remote commands, introducing code instructions into a program (process injection), or a combination of both [6]. In the context of web-based attacks, the primary objective typically involves gaining access to and/or altering a database hosted on a server or seizing control of a website.

In the context of an SQL injection attack, the assailant inserts harmful SQL commands into a system or application with the intention of illicitly accessing the database in use. Once this unauthorized access is achieved, the attacker gains the ability to view, modify, or manipulate stored data as they see fit, potentially resulting in data theft and the compromise of confidential or critical information. SQL injections can also serve as a means to establish a hidden entry point in the compromised system, paving the way for subsequent unauthorized access and malicious activities. The overarching goal of this form of attack is to circumvent the authentication process and obtain unrestricted access to the data stored within the compromised system. [7].

DNS spoofing, also recognized as DNS cache poisoning, is a method employed to compromise computer security by introducing inaccurate Domain Name System (DNS) information into the cache of a DNS resolver. This manipulation leads the name server to return erroneous result records, such as an IP address, redirecting traffic towards the attacker's system or an alternative location. An illustration of spoofing can be observed in email correspondence, where a sender may employ someone else's email address to transmit malicious content. DNS spoofing has the capability to implant corrupted DNS data and alter the source IP address, rendering it advantageous for executing a man-in-the-middle (MiTM) attack. In a MiTM, or adversary-in-the-middle (AiTM), attack scenario, the attacker intercepts, relays, and potentially modifies communication between two or more parties who believe they are engaging in a direct and secure communication channel. Eavesdropping serves as a fundamental example of a MiTM attack, where a third party establishes separate connections with the victims and relays information between them, all the while the victims perceive the connection as direct and secure.

III. ARTIFICIAL INTELLIGENCE – DEFINITION AND APPICATIONS

Intelligence can be broadly defined as the capacity for logic, abstraction, critical thinking, creativity, and problem-solving. Human intelligence refers to the mental quality that includes the ability to learn from experience, adapt to new situations, comprehend and manage intellectual ideas, and apply knowledge to influence one's environment. Effective adaptation requires a variety of cognitive functions, such as perception, learning, memory, reasoning, and problem-solving. Therefore, the focus of a definition of intelligence is not on a single cognitive or mental function, but on a deliberate blend of various activities that are intentionally directed towards successful adaptation [10].

The concept of artificial intelligence (AI) involves modeling or creating intelligence in objects that are typically viewed as inanimate, such as computers. The focus of AI research is on finding ways that computers can simulate intelligent thinking. A significant milestone in the development of AI is Alan Turing's theory, which he presented in "Computing Machinery and Intelligence." In this work, Turing examined the problem of determining whether something is intelligent. He proposed a solution in the form of an imitation game, now known as the Turing test. The test involves a person trying to identify the sex of two other individuals (referred to only as X and Y) without any visual contact, but with the ability to ask questions. Turing suggested that the answers should be written to minimize any influence from voice tonality. If a machine can successfully pass the test and is not identified as a machine, it is considered to be intelligent. [11]

In his book “Introduction to AI robotics” R.R. Murphy explains that an agent that is physically placed and has the ability to perceive and respond to its surroundings is a robot. He goes on defining an intelligent robot as a combination of the aforementioned and an intelligent agent that has the capacity to see and take action to increase its chances of success. So as there wouldn’t be any confusion for the purpose of the paper software agents, also known as software AI, are examined as computer programs that represent users or other programs in a relationship of agency. The term agency comes from the Latin agere (to do), which refers to an agreement to act on behalf of another. Now since a robot has a physical aspect logically the question about what are its component arises. In a wider sense the perception, effectors, communications, control, and power are the five general categories of parts found in robots. These components roughly correspond to the animal's arms and legs, five senses, central nervous system, capacity for producing and understanding sounds, gestures, and social cues, and digestive system [12].

Intelligent robots can be deployed on land, in the air, or underwater. Instead of being referred to as robots when they operate outdoors, unmanned systems or vehicles are more generally used terms. In the air domain robots are termed unmanned aerial vehicles (UAV) or unmanned aerial system to emphasize that they are more than just a platform and that they are a human-robot system. There are various competing definitions for how to classify UAVs based on their size and form. Often they are divided into fixed wing aircraft, robot-craft or vertical take-off and landing platforms and small or micro UAV, but it will not be further discussed in this paper [12].

Apart from military use, robots and robotics can and are used in the education system, where relatively low cost but capable kits are used. The availability and popularity of kit platforms are high due to their affordability and widespread usage in educational and hobbyist settings. These robot kits typically require the addition of a separate processing unit, either a personal computer or a specialized robot controller, or are constructed using one of two types of robot microcontrollers: the Parallax Stamp/Propeller or the Arduino. For example, the Boe-Bot is a collection of robot kits that enable the creation of various types of robots such as wheeled, treaded, and walking robots. The Boe-Bot is designed to be used with Parallax processors such as Stamp and Propeller, but it can also be used with an Arduino controller [13].

Robots are also used in farming to automate tasks such as planting, harvesting, and monitoring crops. They can be equipped with sensors and cameras to collect data on plant growth and soil conditions. These robots can also be used for precision agriculture, which involves analyzing data on a per-plant or per-square-meter basis to optimize crop yields and reduce waste [14]. Additionally, robots can be used for tasks that are too dangerous or labor-intensive for humans, such as spraying pesticides or working in extreme weather conditions. Overall, robots have the potential to increase efficiency, reduce costs, and improve crop yields in the agricultural industry.

Robots are used in logistics to automate various processes, such as sorting, packing, and transportation of goods. Some examples of robots used in logistics include autonomous mobile robots (AMRs) that transport goods within warehouses, AGVs that move materials from one location to another, and robotic arms that are used to pick and place items onto pallets or conveyor belts [16]. These robots can help increase efficiency and accuracy, reduce labor costs, and improve safety by reducing the need for human workers to perform repetitive or physically demanding tasks.

In the hospitality industry, robots and robotics are being used in a variety of ways to enhance the guest experience and improve efficiency. For example, robots can be used to assist with check-in and check-out procedures, deliver room service and amenities, provide concierge services and answer guests' questions, and even clean hotel rooms. One specific example is the use of robotic assistants in hotels. These robots can be programmed to deliver items like towels, toiletries, and room service orders to guest rooms, freeing up hotel staff to focus on other tasks. They can also provide information about hotel amenities, nearby attractions, and transportation options. Robots are also being used in the food and beverage industry, particularly in fast food and quick service restaurants. Automated kiosks and self-service ordering systems allow customers to place orders without the need for human interaction, reducing wait times and improving order accuracy. Additionally, robots can be used to prepare and cook food, with some restaurants experimenting with robotic chefs to speed up the cooking process and ensure consistent quality [15].

IV. CYBERATTACKS AND ROBOTICS

As technology advances, cyberattacks are becoming increasingly common and sophisticated. In parallel, robots are becoming more prevalent in public spaces, providing benefits such as cleaning, delivery, security, and public information. With time, the list of benefits is expected to grow, leading to exciting possibilities for how robots will serve humanity in the future [16]. However, as society becomes more reliant on these cyber companions, there are also challenges to be faced.

Robotic systems are vulnerable to a number of flaws that may impair their connectivity, operations, productivity, and accuracy, some of which are: [17]

- Network vulnerability – robotic systems are subject to various wired and wireless communication and connection attacks, such as man-in-the-middle, eavesdropping, spoofing, etc. due to the absence of or adoption of basic security measures;

- Application vulnerability – the performance of the robotic system can also be impacted by apps that have not been thoroughly tested and checked for coding or compatibility issues. Therefore, additional testing is essentially necessary;

- Bad practice vulnerability – includes using the improper security measures and tools, as well as having poor coding abilities that may be readily changed to make mistakes or carry out the wrong duties.

Robots, as all thing that are connected to network, are susceptible to web-based cyber-attacks. In [18] The authors present a scenario where Denial of Service (DoS) attacks are used against robots. They describe a situation where an attacker repeatedly manipulates the robot's controller during operation, leading to a DoS attack. In such a case, the robot would become stuck in a stop status.

Many robots have issues with authentication and authorization, use unsecured communications and weak encryption, and have weak default configurations. Additionally, many robots are built using open source frameworks and libraries. Some robots can be controlled using mobile apps or programmed using computer software, while others communicate through cloud-based services to receive updates and software applications. If the communication channels between these components are insecure and unencrypted, attackers can launch man-in-the-middle attacks and insert malicious software commands or updates that will be executed by the robots. As a result, robots can be vulnerable to cyberattacks that can cause significant damage [19]. The potential use of AI in offensive operations against other AIs or robots is an intriguing aspect of cyberattacks. The use of adversarial inputs, where malicious actors produce inputs that cause models to forecast erroneously in order to avoid being found, is one possible strategy. In [20] is presented the MalGAN technique, a generative adversarial network (GAN)-based tool for creating adversarial samples that successfully evade black-box machine learning-based detection models.

In simple terms, a model extraction attack works by creating a duplicate of the machine learning model that is being used to detect a particular behavior or pattern. The attacker can then manipulate the duplicated model to figure out how to bypass the original model's detection methods. This can be done by analyzing the input/output behavior of the model or by using other techniques like adversarial examples. The extracted model can then be used to launch attacks or to create new, more effective models. The research mentioned in [21] focuses on how to detect and prevent model extraction attacks. The authors expound on the fact that machine learning inherently involves a degree of memorization, even for arbitrary patterns, and it's widely acknowledged that the output of trained neural networks often strongly hints at the training data employed. Trained neural networks may, in some cases, inadvertently memorize irrelevant training data (out-of-distribution), and this unintentional memorization may be detectable by the network. Once data has been memorized, an algorithm can retrieve it. The experiment encompassed a range of diverse approaches, from relatively straightforward ones like brute force to more sophisticated techniques. Despite some drawbacks, such as time consumption, the attacks proved to be generally effective. It's essential to recognize such vulnerabilities because, by extracting both the model and training data, attackers can potentially streamline their development of successful AI and robotic exploitation strategies. Implementing data sanitization or stricter privacy constraints could mitigate this risk or at least raise the bar for potential attackers. However, even when these techniques are employed, there is no guarantee of absolute security. When opting for methods to enhance privacy and limit the disclosure of information, it's imperative to consider the inherent weaknesses of the chosen approach.

One type of attack that can be launched against training data involves poisoning it before it is fed into the algorithm, used by the robot. This type of attack can be especially dangerous in domains like spam filtering or virus analysis, as it can significantly reduce the accuracy of detection and open the door for further cyberattacks. To mitigate this risk, data normalization and additional integrity checks can be implemented.

V. CONCLUSION

The article examines the possible connections, threats and implementations for AI, robotics and cyberattacks. It was found that robotics and AI have become increasingly prevalent in various industries, from healthcare to agriculture, logistics, retail, and hospitality. These technologies offer numerous benefits such as increased efficiency, accuracy, and cost savings. However, they also come with various risks and vulnerabilities. As robots and AI become more advanced, so do the threats that come with them, and it is important to implement strong security measures to protect against cyberattacks. Cyberattacks' computational complexity necessitates the development of new strategies that are more reliable, scalable, and adaptable. It is also important to consider the ethical implications of these technologies and to ensure that they are used in a responsible and beneficial way.

ACKNOWLEDGMENT

The authors would like to thank the scientific research sector of the Technical University of Sofia for financial support for publishing the present paper.

REFERENCES

[1] Marketing Charts, Here’s How People Say Tech Fits Into Their Lives – And Will in the Future, Marketing Charts, 16.09.2018, https://www.marketingcharts.com/industries/technology-105678 (visited 03.04.2023)

[2] Cambridge Dictionary, Cambridge University Press & Assessment, https://dictionary.cambridge.org/dictionary/english/cyberattack (visited 03.04.2023)

[3] IBM, What is a cyberattack?, https://www.ibm.com/topics/cyber-attack (visited 03.04.2023)

[4] Computer security resource center, Glossary, National institute of standards and technology, https://csrc.nist.gov/glossary/term/Cyber_Attack (visited 03.04.2023)

[5] R. Shirey, Internet Security Glossary Version 2, RFC 4949, August 2007, https://www.rfc-editor.org/rfc/pdfrfc/rfc4949.txt.pdf (visited 03.04.2023)

[6] IBM, IBM Security Network Intrusion Prevention System, 03.08.2021, https://www.ibm.com/docs/en/snips/4.6.0?topic=categories-injection-attacks (visited 03.04.2023)

[7] K. M. Sudar, P. Deepalakshmi, P. Nagaraj and V. Muneeswaran, "Analysis of Cyberattacks and its Detection Mechanisms," *2020 Fifth International Conference on Research in Computational Intelligence and Communication Networks (ICRCICN)*, Bangalore, India, 2020, pp. 12-16, doi: 10.1109/ICRCICN50933.2020.9296178

[8] G. A. Abdalrahman and H. Varol, "Defending Against Cyber-Attacks on the Internet of Things," *2019 7th International Symposium on Digital Forensics and Security (ISDFS)*, Barcelos, Portugal, 2019, pp. 1-6, doi: 10.1109/ISDFS.2019.8757478

[9] Symantec Security Center, Difference between viruses, worms, and trojans, Broadcom Inc, 05.06.2019, https://knowledge.broadcom.com/external/article?legacyId=tech98539 (visited 04.04.2023)

[10] Sternberg, Robert J., "Human intelligence", Encyclopedia Britannica, https://www.britannica.com/science/human-intelligence-psychology (visited 05.04.2023)

[11] Alan M. Turing., Computing Machinery and Intelligence, Mind vol. 59, 1950, 433–460

[12] Robin R. Murphy, Introduction to AI robotics, MIT press, 2019, https://books.google.bg/books?hl=bg&lr=&id=TmquDwAAQBAJ&oi=fnd&pg=PR7&dq=robotics+and+AI+&ots=RrAgovz8G6&sig=mtr4X1O0Q1JTZIH3JxTGzOoWDG0&redir_esc=y#v=onepage&q=robotics%20and%20AI&f=false (visited 03.05.2023)

[13] Miller, D.P., Nourbakhsh, I, Robotics for Education, Springer Handbook of Robotics. Springer Handbooks, Springer, 2016 https://link.springer.com/chapter/10.1007/978-3-319-32552-1_79 (visited 04.05.2023)

[14] Intel, Types of Robots: How Robotics Technologies Are Shaping Today’s World, Intel, https://www.intel.com/content/www/us/en/robotics/types-and-applications.html (visited 04.05.2023)

[15] Yang, L., Henthorne, T.L., George, B, Artificial Intelligence and Robotics Technology in the Hospitality Industry: Current Applications and Future Trends, Digital Transformation in Business and Society, 2020, https://link.springer.com/chapter/10.1007/978-3-030-08277-2_13 (visited 04.05.2023)

[16] Mintrom, M., Sumartojo, S., Kulić, D., Tian, L., Carreno-Medrano, P., & Allen, A, Robots in public spaces: implications for policy design, Policy Design and Practice, 5:2, 123-139, 2022, https://www.tandfonline.com/doi/full/10.1080/25741292.2021.1905342 (visited 02.05.2023)

[17] Yaacoub, JP.A., Noura, H.N., Salman, O. et al, Robotics cyber security: vulnerabilities, attacks, countermeasures, and recommendations, Int. J. Inf. Secur. 21, 115–158, 19.03.2021, https://link.springer.com/article/10.1007/s10207-021-00545-8 (visited 02.05.2023)

[18] Rueben, Matthew & Grimm, Cindy & Bernieri, Frank & Smart, William, "A Taxonomy of Privacy Constructs for Privacy-Sensitive Robotics" ResearchGate, 03.01.2017, https://www.researchgate.net/publication/312061072_A_Taxonomy_of_Privacy_Constructs_for_Privacy-Sensitive_Robotics (visited 02.05.2023)

[19] Lacava, Giovanni, et al, Cybsersecurity Issues in Robotics., J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl. 12.3, 2021, https://isyou.info/jowua/papers/jowua-v12n3-1.pdf (visited 02.05.2023)

[20] Hu, W.; Tan, Y, Generating adversarial malware examples for black-box attacks based on GAN, Data Mining and Big Data. DMBD 2022, https://arxiv.org/pdf/1702.05983.pdf (visited 06.04.2023)

[21] Carlini, Nicholas, et al, "The Secret Sharer: Evaluating and Testing Unintended Memorization in Neural Networks.", USENIX Security Symposium. Vol. 267, 2019, https://www.usenix.org/system/files/sec19-carlini.pdf