Critical Infrastructure Security: Penetration Testing and Exploit Development Perspectives

Papa Kobina Orleans-Bosomtwe

School of Computer Science, University of Guelph, Ontario, Canada

July 25, 2024

Abstract

Critical infrastructure refers to essential physical and cyber systems vital to the functioning and stability of societies and economies. These systems include key sectors such as healthcare, energy, and water supply, which are crucial for societal and economic stability and are increasingly becoming prime targets for malicious actors, including state-sponsored hackers, seeking to disrupt national security and economic stability. This paper reviews literature on critical infrastructure security, focusing on penetration testing and exploit development. It explores four main questions: the characteristics of critical infrastructure, the role and challenges of penetration testing, methodologies of exploit development, and the contribution of these practices to security and resilience. The findings of this paper reveal inherent vulnerabilities in critical infrastructure and sophisticated threats posed by cyber adversaries. Penetration testing is highlighted as a vital tool for identifying and addressing security weaknesses, allowing organizations to fortify their defenses. Additionally, understanding exploit development helps anticipate and mitigate potential threats, leading to more robust security measures. The review underscores the necessity of continuous and proactive security assessments, advocating for integrating penetration testing and exploit development into regular security protocols. By doing so, organizations can preemptively identify and mitigate risks, enhancing the overall resilience of critical infrastructure. The paper concludes by emphasizing the need for ongoing research and collaboration between the public and private sectors to develop innovative solutions for the evolving cyber threat landscape. This comprehensive review aims to provide a foundational understanding of critical infrastructure security and guide future research and practices.

Keywords: Cybersecurity, penetration testing, exploit development, critical infrastructure.

1 Introduction

Critical infrastructure includes the physical and cyber systems and assets essential for the uninterrupted functioning of a nation's society and economy [1, 2]. This includes healthcare, public health, energy, and information technology sectors. Over the years, advances in technology and information technology systems have improved many essential systems, making life

easier for relevant users and operators. It is not shocking to discover critical infrastructure firms' assimilation and adoption of newer technological systems to improve efficiency and output. The threats to technology increased with the progress and advancements over the years. Technological threats have become as sophisticated (sometimes more refined) as their counterparts. These threats can then be transferred to technologies used in critical infrastructure systems. Cyber attackers, who pose said threats to technological systems, utilize various means to cause harm to systems. A survey in 2023 was conducted to find the primary cause of cyber-attacks Figure 1 encountered by companies in the United States, which showed unpatched vulnerabilities, attributing to 23% of these causes. Penetration testing is basically an analysis of some aspects of a system [3, 4], with the discoveries used to improve the security and resilience of tested systems and networks by crafting new exploits or using existing ones to test systems further. Figure 2 shows the number of common IT security vulnerabilities and exposures worldwide (CVEs) from 2009 to 2024. This paper aims to assess the existing security and resilience of critical infrastructure using penetration testing and exploit development by answering 4 main research questions. These research questions are "What is critical infrastructure?", "What is penetration testing?", "What is exploit development?", and "How can penetration testing and exploit development improve critical infrastructure security and resilience?". These questions are being posed due to the information and understanding they can provide to readers of this paper. Answering these questions in the order they have been asked will help readers understand what critical infrastructure is, how important it is, and how the remaining concepts

which are penetration testing, and exploit development tie in in the security of critical infrastructure. These questions will be answered by reviewing pre-existent studies around these key areas: critical infrastructure, penetration testing, and exploit development.
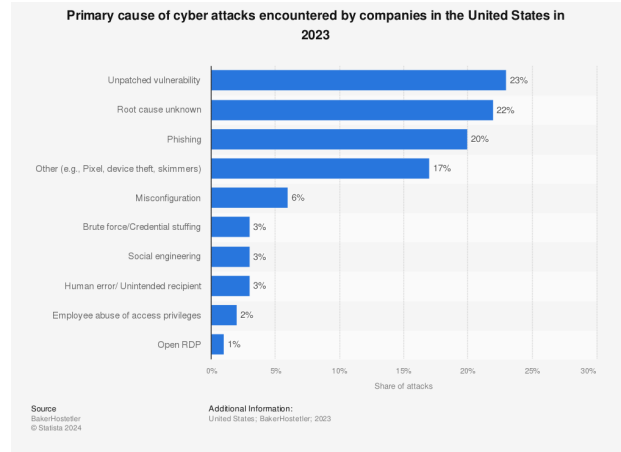

Figure 1: Primary causes of cyber-attacks in the US in 2023

2 Literature Review

Upon the first search of related artifacts, it was discovered that some articles related to critical infrastructure security from a cybersecurity standpoint. Dating to as recently as 2021, Makrakis et al. [1] note the growing integration of modern information technology by critical infrastructure and industrial organizations into their existing operational technology (OT) architectures. They point out that the ever-increasing attack surfaces of these new modern technology integrations provide malicious attackers, owing to their complexity and modernity, which, in turn, also handicap the defenders of these sys-
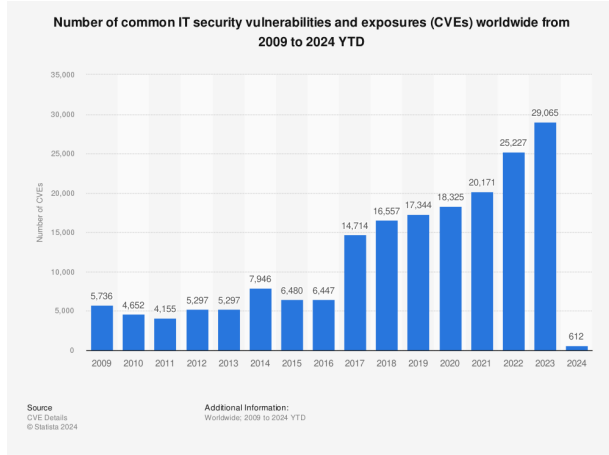
Figure 2: Number of common IT security vulnerabilities and exposures worldwide (CVEs) from 2009 to 2024

tems. This paper then follows up with a survey of the most prevalent threats against industrial control systems and critical infrastructures at the time, exposing vulnerabilities in specific operational technology (OT) network protocols and devices. The authors also explore some malicious software (malware) that has targeted critical infrastructure in the past, highlighting how social engineering has been a significant attack vector for adversaries. 2021 also saw Malatji et al. [5] reviewing critical infrastructure and cybersecurity in general, focusing on the growing interconnectivity between Enterprise Information Technology (IT) and Industrial Control Systems (ICS). The authors note that this growing connectivity also poses increasing dangers to operators and organizations regarding the new attack surfaces they present to malicious attackers. The paper also discusses the cybersecurity framework proposed by the National Institute of Standards and Technology (NIST) for critical infrastructure, noting its customization potential

and inclusion of cloud capabilities and security in the modern world. A paper by Ghafir et al. [6] in 2018 points out threats to critical infrastructure, focusing on humans, classified as "non-computer experts." The authors acknowledge current security awareness training platforms and tools and highlight their shortcomings. Using prior research, the authors note that the knowledge retention rate after completing a security awareness training session or campaign was low. Their paper proposes a "context-aware education tool" for security awareness, where training is related to the current business environment, with platform administrators able to monitor and track users' progress. The studies mentioned above all note the growing cybersecurity risks facing Critical Infrastructure (CI) ICS as they get updated and integrated with modern IT systems and networks. They do not, however, explore penetration testing and exploit development perspectives in improving the security of CI and ensuring their resilience. This paper aims to review further work done in this capacity to be a guide for future research activities [7].

3   Research Goals

This paper aims to review existing studies on critical infrastructure security, penetration testing, and exploit development, and the utilization of penetration testing and exploit development to enhance critical infrastructure security and resilience.

- A total of 32 different articles and studies were discovered relating to critical infrastructure, its security, and penetration testing and exploit development.

- After further review, 13 of the previous 32

Research Questions	Description
RQ1: What is critical infrastructure?	A brief overview of critical infrastructure and what differentiated it from other structures put up to make it vital to a government and its population.
RQ2: What is penetration testing?	An explanation of penetration testing, types of penetration testing, phases involved, common tools, and its challenges and limitations.
RQ3: What is exploit development?	This question aims to explore exploit development in its entirety, including types of exploits, some tools and techniques used, and ethics to be considered when developing exploits.
RQ4: How can penetration testing and exploit development improve critical infrastructure security and resilience	A combination of all research questions above to finally understand critical infrastructure security from a penetration testing and exploit development standpoint.

Table 1: Research Questions

articles and studies were selected for this paper. The selected 13 papers are carefully and comprehensively reviewed to carry out the purposes of this paper.

The paper continues with a research methodology indicating how the selected journals and articles were found. The paper then presents all findings from the selected journals and discusses these findings. A conclusion will be made, and suggestions for possible future research efforts will be made.

4   Research Methodology

4.1   Inclusion Criteria

Studies to be selected for this paper had to meet pre-defined criteria. This criterion includes an in-depth explanation and analysis of critical infrastructure security, penetration testing, exploit development, and relevant supporting background research. The studies must also be written within the last ten years and in English. All discovered studies on Google Scholar and other sources listed above were compared against the criteria defined in this section and Table 2.

4.2   Selection Results

The initial keyword searches yielded numerous results that had to be filtered through based on the inclusion criteria. This initial title/abstract screening yielded thirty studies relevant to the purposes of this paper. The thirty shortlisted studies subsequently underwent another screening phase (full text), closely following the inclusion criteria. Of the thirty initially found, only 13 papers were selected for final review in this paper.

Inclusion Criteria	Exclusion Criteria
The paper must be written in English.	Paper not written in English.
The paper must discuss one, or more of the relevant topics.	Paper does not discuss critical infrastructure in a cybersecurity context.

Table 2: Inclusion and Exclusion Criteria

4.3 Data Extraction

After going through the first and second screening steps, the papers that were finally selected had their data extracted. This data was extracted to evaluate the accuracy of information provided in the chosen texts. The data extraction process was first carried out on 3 out of the final 13 papers and was then applied to the remaining ten papers, with the data then getting categorized and stored for later use. The categories gained from the extracted data are as follows:

- **Context data:** This includes all information about the purpose of the study.

- **Qualitative data:** This includes the findings, proposals, and conclusions proposed by the studies' authors.

4.4 Significant Keyword Counts

In addition to the keywords utilized in searching for these papers, various other keywords were discovered in the selected texts. These keywords have been listed and compiled, with their given counts in Table 3. The aim of Table 3 is to accumulate the number of times selected keywords appeared in the 13 studies selected. Observing the keyword counts in Table 3, it can be noted that the prevailing theme across the selected studies is "cybersecurity," with a count of 375.

5 Findings

After carefully reading selected primary texts, relevant information related to this paper was extracted, including contextual and qualitative data. From the percentages in Figure 4, it can be determined that 27% of the selected studies were concerned with cybersecurity. The next most prevalent themes in the selected studies were critical infrastructure and penetration testing, each with a 15% distribution. Critical infrastructure being our main focus of this conversation and penetration testing being an aid in discovering some misconfigurations within critical infrastructure systems. At 14%, the keyword "exploits" comes in as the fourth most discussed theme in the selected texts. Supervisory Control and Data Acquisition (SCADA) systems, which are typically used in industrial control devices and systems had a 13% rate of discussion within the selected texts. Threats, mostly digital and within the cyber space have a 10% discussion in the selected studies. Threats are the dangers that industrial control systems and critical infrastructure face. Industrial control systems usually found being used in Critical infrastructure had a 6% distribution within the selected discussion papers. The selected studies all discussed the topics intended to meet their intended capacities. These studies were chosen because they sufficiently described and explained the relevant topics in this paper which are critical in-

Keywords	Count
critical infrastructure.	213
industrial control system	80
penetration testing/tests	208
cybersecurity	375
power system control	6
SCADA	176
exploit	189
threats	145

Table 3: Significant Keyword Counts

frastructure, penetration testing, exploit development, and cybersecurity. A number of studies highlight the services and systems (IT) that are used in critical infrastructure and their gross misconfigurations. The importance of critical infrastructure penetration testing is also discussed, with some studies diving deeper into the importance of penetration testing and cybersecurity in critical infrastructure[8, 9].
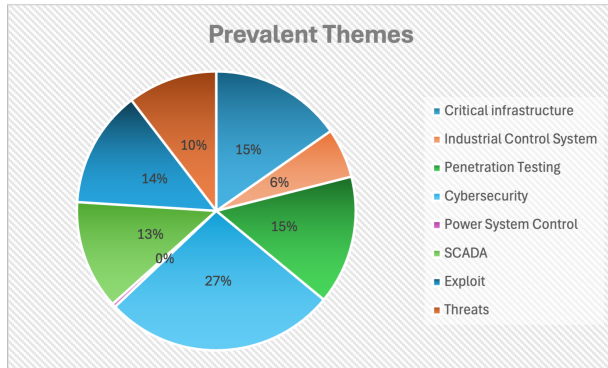

Figure 3: Distribution of Prevalent Themes

6 Discussion

The keyword searches conducted on the selected papers show a relevant interest in critical infrastructure security, penetration testing, and exploit development. The significance of critical infrastructure is well established in several of these studies, with a significant number also recognizing the growing risks these infrastructures face as they modernize their IT systems and other control systems. The papers have significant qualitative data regarding the chosen topics but need more practical solutions. Some valuable solutions offered are revisions of currently existing methodologies with some improvements. About penetration testing in these studies, the act is defined and well explained, with light also shed on the different types of penetration tests. Penetration testing tools were discussed, and a combination of these tools and other platforms was explored to simplify penetration testing. Addressing the critical infrastructure, a number of papers attempt to define CI and industrial control systems. The papers note that ICS were initially believed to be safe and free from possible cyberattacks but increasing attacks on CI and ICS have changed this belief. IT and cybersecurity

teams are now attempting to quantify the cyber risks CI and ICS are exposed to and are finding it difficult to do so. Multiple ICS and OT network environments have been discovered to be misconfigured and are easy to exploit. Penetration testing and red teaming activities have been shown to help discover said misconfigurations. Other researchers also propose using testbeds to discover cybersecurity vulnerabilities within ICS. Some authors of the selected studies attempt to develop penetration system specific to large networks found in CI by simulating complex human or automated attacks. Solutions proposed by authors include the integration of artificial intelligence and machine learning algorithms to detect and prevent potential cyber-attacks against ICS found within CI. The research also discovered that some definitions of Critical Infrastructure were inadequate, which could lead to some gaps in security as networks and systems for critical infrastructure were not properly categorized. CI must be well-defined, and assets, including systems and other products, must be correctly identified and labeled. The identified assets must be protected at all costs throughout their entire lifecycle. The remaining discoveries are tabulated in Figures 4-7 below.

6.1 RQ1. What is Critical Infrastructure?

Critical infrastructure can be defined as complex physical and cyber-based systems that form the lifeline of a modern society [10, 11]. Some sectors in Critical Infrastructure include transport, energy, food, water, finance, and health [12]. For various functions, industrial control systems are widely used in CI and are typically used to control different infrastructures like manufacturing [13]. The ICS architecture found in

Selected Study	Key Findings
[13]	Social engineering attacks are typically used by attackers in this paper to carry out majority of their attacks. Upon successful breach of an IT network, attackers are more than likely able to breach OT environments as well. A lot of server and network misconfigurations also leave systems exposed to attack. This paper also points out a difficulty in quantifying cyber risk posture in ICS and CI. The paper also highlights other ICS device vulnerabilities such as control logic injection, and unauthorized access.
[14]	This paper brings to knowledge the fact that ICS were initially not perceived to be vulnerable to cyber threats, which has otherwise been proven wrong. It then provides a customizable CI cybersecurity framework to ensure and improve CI resilience, where general IT cybersecurity frameworks do not apply to CI.
[18]	Proposes more research to be done on the Receiver Autonomous Integrity Monitoring (RAIM) framework especially considering online risk monitoring algorithms, and advanced modeling that accounts for impacts such as load loss. The paper also proposes periodic vulnerability assessment for CI through test-bed development. Reduction of system vulnerabilities within budgetary limits should also be considered for future research purposes.
[16]	This paper acknowledges growing cyber threats and the need for cyber resilience in

Figure 4: Key Findings

CI typically consists of 6 levels. These levels range from sensors providing sensing capabilities to a system, to manufacturing operations systems used to manage production at any CI site [1, 14]. The sentence before was added to paint a picture of just how complex ICS and CI can get and how all the systems found within the ICS archcitecture require security on varying levels to protect them from cyber attacks.

6.2 RQ2. What is Penetration Testing?

Penetration testing is a structured process to test an organization's computing base, which includes hardware, software, and people [15]. The adopted frameworks differ in the number of penetration testing phases they offer. For example,

7

	critical power grid infrastructure. The potential of artificial intelligence, machine learning, and advanced analytics are recognized as potential solutions to an ever-evolving threat landscape. Partnerships among industry stakeholders, governments, and cybersecurity experts are noted as crucial to ensure resilient power grid infrastructures.
[15]	This paper has its researchers using testbeds to discover cybersecurity vulnerabilities within ICS. Commercial hardware and software devices were experimented on and demonstrate physical properties of controlled processes being used to detect incorrect variations in process measurements.
[4]	Since the discovery of Stuxnet in 2010, an increasing number of other cyber-attacks were discovered to have targeted critical infrastructure. A holistic, resilient approach is to be considered which considers supply chain to the management of the system for the ICS of critical infrastructure. Considerations for the protection of the entire lifecycle of the product. Some challenges to this approach included asset and inventory management, and the difficulty to entirely monitor the product lifecycle.
[3]	Critical failures in CI protocol configuration and design were discovered through cyber red-teaming operations. Information from these operations led to a proposal of regular execution of said cyber red-team procedures to address critical CI protocol configurations. A proposal was also made to further target and explore the IEC 61850 protocol stack.
[5]	This paper aims to use machine learning algorithms to detect malicious URLs and test them using scripts and payloads, to classify the type of vulnerability. The random forest algorithm was the most efficient in carrying out their exercise goals. With their focus only on the Open Worldwide Application Security Project (OWASP) top 10 vulnerabilities, future work could focus on all other types of web vulnerabilities. Future work could also delve around the automatic development of exploits for the remaining web vulnerabilities.

Figure 5: Key Findings continued

[17]	This study provides an overview of penetration testing and penetration testing process, its benefits, and tools used to conduct these tests. Vulnerability assessments and penetration tests conforming to international standards like ISO 27001 are also assessed. The competencies required to carry out a penetration test including the upholding of ethics is also pointed out in this paper.
[2]	Discusses penetration tests, knowledge available to malicious attackers and the resources at their disposal. The applications of penetration tests and the ethical issues involved in penetration testing are also discussed. It is also noted that penetration tests cannot find all vulnerabilities and the failure to find any vulnerabilities does not also guarantee absolute security of a system.
[9]	This study simply compares various definitions of critical infrastructure and analyzes the weaknesses of these definitions. Significant consequences of weak definitions of critical infrastructure with respect to weak security policies that do not adequately capture critical infrastructure. This can lead to glaring gaps in the security of CI. A proposal for CI from an attacker's viewpoint is believed to be the best definition, allowing a clearer view of what should actually be classified as critical infrastructure.
[11]	The study aims to develop a system for the penetration testing of large networks such as those found in CI by imitating complex human or automated attacks. It does this by evaluating attack node command system used in the Blackboard Architecture-based command system. Proposals for the addition of supplementary tools to make attack preparation easier. An expansion of the scope of influence of attack nodes is also proposed. Lastly, a demonstration of the newly distributed attack capability combined with the broader system is to be considered for future related works.

Figure 6: Key Findings continued

the National Institute of Standards and Technology Special Publication (NIST SP) 800-115 has four stages, whereas the penetration testing execution standard (PTES) has seven. A penetration test's primary objectives are identifying vulnerabilities, reducing risks, and guaranteeing compliance by figuring out how a malevolent actor may enter the target environment, navigate it, and steal data from it. In penetration testing, three main testing methods are typically used, the first being black box. In black box testing, the team has no information about the tested target [15]. White box testing has testers provided with all information about the test target, while gray box testing has testers provided with partial information [15]. Several tools like Nmap, Metasploit, and Nessus are used in various stages of the penetration testing process.

6.3 RQ3. What is Exploit Development?

Exploit development involves identifying vulnerabilities in applications and software and de-

[8]	This paper puts forth a platform to carry out security and vulnerability analysis of CIs in factories by utilizing hybrid and distributed simulation techniques by adopting an Infrastructure-as-a-Service (IaaS) paradigm. This proposed solution can be used to carry out penetration tests of CI networks.

Figure 7: Key Findings continued

termining how to gain control of a system [16]. When discussing exploit development, there are two broad categories under which all exploits fall: known and unknown (zero-day) exploits [16]. Both malicious actors and security teams can exploit developments to their advantage. Security team members or researchers can use exploit development to learn more about security flaws within systems or networks, including possible critical failures and the consequences of attackers exploiting these vulnerabilities. The information obtained from this exercise can help security team members adequately patch or fix the discovered vulnerabilities to prevent facing the consequences. This information can also be shared with relevant parties to ensure more systems affected by these vulnerabilities are secured.

While the traditional methods of exploit development are critical, recent advancements in automated exploit generation tools and machine learning techniques have significantly enhanced the speed and efficacy of this process. Automated exploit generation tools, such as those leveraging symbolic execution and fuzz testing, allow for rapid identification and exploitation of vulnerabilities. These tools can systematically explore numerous execution paths in software to uncover hidden bugs and security flaws that might be missed by manual testing [17].

Recent advancements in automated exploit generation have significantly enhanced the speed and effectiveness of exploit development. Automated exploit generation typically involves automatically discovering paths in a program that trigger vulnerabilities, thereby creating exploits [18]. Tools like AAHEG exemplify the integration of automation in this field. AAHEG utilizes symbolic execution to analyze and detect potential heap-related vulnerabilities in sourcee code, develops an exploit abstract syntax tree, then selects exploitable methods. These methods are then tested and the final exploit is produced.

Incorporating these technologies into exploit development can provide security teams with powerful tools to proactively identify and address vulnerabilities before malicious actors can exploit them. This proactive approach is essential for maintaining robust security measures against the continuously evolving cyber threat landscape.

6.4 RQ4. How can penetration testing and exploit development improve critical infrastructure security and resilience?

The general issue with critical infrastructure security and resilience is that cybersecurity is primarily perceived in the context of enterprise IT systems. Industrial Control Systems (ICS) were mistakenly considered impervious to cyberattacks [5]. Other issues relating to critical infrastructure include the old age of the systems and technologies used. Legacy systems and older components typically found in critical infrastructure system architectures pose significant problems for CI security teams [19]. These older systems typically lack modern security features to detect or counter contemporary cyber threats and attacks. Penetration testing and exploit development, when correctly carried out, especially

9

on networks by the relevant parties, can expose vulnerabilities and possible threats to critical infrastructure.

ICS used in CI consist of various levels and are very complex. This requires that security operators have deep understandings of the multiple tiers within ICS. Penetration testing, therefore, plays a critical role in ensuring the security and resilience of these systems by addressing vulnerabilities at each level [1] of the architecture:

- **Level 0 - Sensors, motors, and instruments:** Penetration testing at this level involves assessing the security of devices that provide sensing capabilities to the ICS. These components are often targeted because they are fundamental to the physical operation of industrial processes. Penetration tests should check for vulnerabilities such as weak authentication mechanisms, insecure communication protocols, and potential physical tampering points [20].

- **Level 1 - Devices including PLCs:** Programmable Logic Controllers (PLCs) are critical as they provide sensory and monitoring control over physical processes. Comprehensive penetration tests should focus on identifying flaws in PLC firmware, misconfigurations, and unsecured connections that could be exploited to disrupt operations or cause physical damage.

- **Level 2 - Control systems:** This level includes Engineering Workstations that supervise physical processes. Penetration testing here involves evaluating the security of control systems, ensuring that they are not vulnerable to attacks that could lead to unauthorized changes in operational settings or shutdowns [11].

- **Level 3 - Plant-wide production workflow systems:** Systems at this level, such as file servers and Microsoft Active Directory, are tested for vulnerabilities that could allow attackers to gain control over the workflow management systems. This includes examining network security, access controls, and potential insider threats.

- **Level 4 - IT-related activity systems:** Systems like application servers and ERP systems are crucial for overseeing IT-related activities. Comprehensive penetration tests will assess these systems for vulnerabilities in web applications, databases, and network interfaces, ensuring they are robust against exploits that could impact the broader enterprise operations.

- **Level 5 - Enterprise network:** The enterprise network encompasses both internal and external networks of the organization, used for production and resource data exchange. Penetration testing should focus on identifying and mitigating risks associated with network perimeter security, remote access vulnerabilities, and potential data breaches that could propagate to lower levels [**5h**, 21].

Emphasis should be placed on network penetration testing because numerous incidents attest that attackers can easily penetrate Operational Technology (OT) environments after breaking into IT networks [1]. A comprehensive penetration testing strategy that addresses each layer of the ICS architecture ensures that vulnerabilities are identified and mitigated across the entire system, thereby improving the security and resilience of critical infrastructure.

Recent advancements in exploit development, particularly in automated exploit generation (AEG), can significantly enhance penetration testing and overall security of CI and ICS. Automated tools like AAHEG (Automatic Advanced Heap Exploit Generation) leverage symbolic execution and abstract syntax trees to automatically identify and exploit heap-related vulnerabilities without requiring source code, effectively bypassing various protection mechanisms [18].

Integrating these advanced technologies into penetration testing enables quicker and more efficient identification and mitigation of vulnerabilities, ensuring that security measures are robust and up-to-date against evolving cyber threats. This proactive approach is crucial for maintaining the security and resilience of critical infrastructure and industrial control systems.

7 Conclusion and Future Work

Critical Infrastructure is vital to the daily operation and working of a society; any disruptions or outages to the services they provide cannot be afforded. Owing to their importance, critical infrastructure security should be taken seriously, especially in cyberspace. The growing attraction of cyber attackers to critical infrastructure is undeniable, and action should be taken. Penetration testing to discover the vulnerabilities in essential systems of critical infrastructure, coupled with exploit development to understand the criticality of these vulnerabilities, will spur security teams into immediate action to fix and patch these vulnerabilities and corresponding systems to prevent exploitation by malicious attackers. The research has shown the benefits of penetration testing and exploit development and pointed out, as earlier stated, how necessary critical infrastructure is. For future research, I propose that researchers investigate social engineering and securing the human part of any IT system. Social engineering is currently the most common way of committing cybercrimes through the intrusion and infection of computer systems [22]. Hypothetically speaking, even if the systems and network of critical infrastructure manage to be perfectly configured with no potential breach avenues, the one remaining threat will remain the human aspect of these systems. Another risk aspect of the human part of any IT system is insider threats. Insider threats are malicious acts carried out by authorized persons, which may cause detrimental implications for the digital and physical assets of an organization [23]. More research should be conducted in this respect for mitigation strategies and the role penetration testing can play. The final area of suggestion for future research will be artificial intelligence and machine learning. Machine learning and artificial intelligence could play essential roles in automated penetration testing and exploit development to benefit the cybersecurity of critical infrastructure systems.

References

[1] Georgios Makrakis et al. "Industrial and Critical Infrastructure Security: Technical Analysis of Real-Life Security Incidents". In: *IEEE Access* 9 (2021), pp. 165295–165325. DOI: 10 . 1109 / access . 2021 . 3133348.

[2] Abbas Yazdinejad et al. "An energy-efficient SDN controller architecture for IoT networks with blockchain-based secu-

rity". In: *IEEE Transactions on Services Computing* 13.4 (2020), pp. 625–638.

[3] Matt Bishop. "About Penetration Testing". In: *IEEE Security & Privacy Magazine* 5.6 (Nov. 2007), pp. 84–87. DOI: 10.1109/msp.2007.159.

[4] Abbas Yazdinejad et al. "Enabling drones in the internet of things with decentralized blockchain-based security". In: *IEEE Internet of Things Journal* 8.8 (2020), pp. 6406–6415.

[5] Masike Malatji, Annlizé Marnewick, and Suné Von Solms. "Cybersecurity capabilities for critical infrastructure resilience". In: *Information & Computer Security* 30.2 (Oct. 2021), pp. 255–279. DOI: 10.1108/ics-06-2021-0091.

[6] Ibrahim Ghafir et al. "Security threats to critical infrastructure: The human factor". In: *The Journal of Supercomputing* 74.10 (Mar. 2018), pp. 4986–5002. DOI: 10.1007/s11227-018-2337-2.

[7] Jacob Sakhnini et al. "A generalizable deep neural network method for detecting attacks in industrial cyber-physical systems". In: *IEEE Systems Journal* 17.4 (2023), pp. 5152–5160.

[8] Danyal Namakshenas et al. "Federated quantum-based privacy-preserving threat detection model for consumer internet of things". In: *IEEE Transactions on Consumer Electronics* (2024).

[9] Behrouz Zolfaghari et al. "The dichotomy of cloud and iot: Cloud-assisted iot from a security perspective". In: *arXiv preprint arXiv:2207.01590* (2022).

[10] Chee-Wooi Ten, Govindarasu Manimaran, and Chen-Ching Liu. "Cybersecurity for Critical Infrastructures: Attack and Defense Modeling". In: *IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans* 40.4 (July 2010), pp. 853–865. DOI: 10.1109/tsmca.2010.2048028.

[11] Abbas Yazdinejad et al. "An ensemble deep learning model for cyber threat hunting in industrial internet of things". In: *Digital Communications and Networks* 9.1 (2023), pp. 101–110.

[12] Massimo Ficco, Michał Choraś, and Rafał Kozik. "Simulation platform for cybersecurity and vulnerability analysis of critical infrastructures". In: *Journal of Computational Science* 22 (Sept. 2017), pp. 179–186. DOI: 10.1016/j.jocs.2017.03.025.

[13] Sandro Bologna, Alessandro Fasani, and Maurizio Martellini. "Cyber Security and Resilience of Industrial Control Systems and Critical Infrastructures". In: *Cyber Security*. Ed. by M. Martellini. Springer International Publishing, 2013, pp. 57–72. DOI: 10.1007/978-3-319-02279-6_6.

[14] Abbas Yazdinejad et al. "Accurate threat hunting in industrial internet of things edge devices". In: *Digital Communications and Networks* 9.5 (2023), pp. 1123–1130.

[15] Hessa Shebli and Babak Beheshti. "A study on penetration testing process and tools". In: *2018 IEEE Long Island Systems, Applications and Technology Conference (LISAT)*. IEEE, May 2018, pp. 1–7. DOI: 10.1109/lisat.2018.8378035.

[16] Rosy Chadha et al. "A Study on Exploit Development". In: *2022 7th International Conference on Computing, Communication and Security (ICCCS)*. IEEE, Nov. 2022, pp. 1–7. DOI: 10.1109/icccs55188.2022.10079387.

[17] Thanassis Avgerinos et al. "Automatic exploit generation". In: *Communications of the ACM* 57.2 (2014), pp. 74–84. DOI: 10.1145/2560217.2560219.

[18] Yu Wang, Yipeng Zhang, and Zhoujun Li. "AAHEG: Automatic Advanced Heap Exploit Generation Based on Abstract Syntax Tree". In: *Symmetry* 15.12 (2023), Article 12. DOI: 10.3390/sym15122197.

[19] S Parshivlyuk and K Panchenko. "Cyber Threats and Resilience in Power Grid Infrastructures: Assessing Vulnerabilities and Countermeasures". In: *Eduzone: International Peer Reviewed/Refereed Multidisciplinary Journal* 13.1 (2024), p. 1.

[20] Abbas Yazdinejad et al. "A Robust Privacy-Preserving Federated Learning Model Against Model Poisoning Attacks". In: *IEEE Transactions on Information Forensics and Security* (2024).

[21] Florian Nelles et al. "A Federated Learning Approach for Multi-stage Threat Analysis in Advanced Persistent Threat Campaigns". In: *arXiv preprint arXiv:2406.13186* (2024).

[22] Nina Klimburg-Witjes and Alexander Wentland. "Hacking Humans? Social Engineering and the Construction of the "Deficient User" in Cybersecurity Discourses". In: *Science, Technology, & Human Values* 46.6 (Feb. 2021), pp. 1316–1339. DOI: 10.1177/0162243921992844.

[23] Rakan Alsowail and Taher Al-Shehari. "Techniques and countermeasures for preventing insider threats". In: *PeerJ Computer Science* 8 (Apr. 2022), e938. DOI: 10.7717/peerj-cs.938.

[24] A Chesne. "Indirect boundary force measurements in beam-like structures using a derivative estimator". In: *Journal of Sound and Vibration* 333.24 (June 2024), pp. 6438–6452. DOI: 10.1016/j.jsv.2014.07.026.

[25] Daniel Dalalana Bertoglio and Avelino Zorzo. "Overview and open issues on penetration test". In: *Journal of the Brazilian Computer Society* 23.1 (Feb. 2017). DOI: 10.1186/s13173-017-0051-1.

[26] Thomas Morris et al. "A control system testbed to validate critical infrastructure protection concepts". In: *International Journal of Critical Infrastructure Protection* 4.2 (Aug. 2011), pp. 88–103. DOI: 10.1016/j.ijcip.2011.06.005.

[27] Bernhards Blumbergs. "Remote Exploit Development for Cyber Red Team Computer Network Operations Targeting Industrial Control Systems". In: *Proceedings of the 5th International Conference on Information Systems Security and Privacy*. SCITEPRESS - Science and Technology Publications, 2019, pp. 88–99. DOI: 10.5220/0007310300880099.

[28] C Gallais and E Filiol. "Intrathecal administration of tetanus antitoxin and corticosteroids in treatment of tetanus". In: *The Journal of Trauma: Injury, Infection, and Critical Care* 17.11 (2017), p. 893. DOI: 10.1097/00005373-197711000-00029.

[29] Jack Hance et al. "Distributed Attack Deployment Capability for Modern Automated Penetration Testing". In: *Computers* 11.3 (Feb. 2022), p. 33. DOI: 10.3390/computers11030033.

[30] Abbas Yazdinejad et al. "P4-to-blockchain: A secure blockchain-enabled packet parser for software defined networking". In: *Computers & Security* 88 (2020), p. 101629.

[31] Abbas Yazdinejad et al. "Block hunter: Federated learning for cyber threat hunting in blockchain-based iiot networks". In: *IEEE Transactions on Industrial Informatics* 18.11 (2022), pp. 8356–8366.

[32] Abbas Yazdinejad et al. "Secure intelligent fuzzy blockchain framework: Effective threat detection in iot networks". In: *Computers in Industry* 144 (2023), p. 103801.

[33] Abbas Yazdinejad, Ali Bohlooli, and Kamal Jamshidi. "Efficient design and hardware implementation of the OpenFlow v1.3 Switch on the Virtex-6 FPGA ML605". In: *The Journal of Supercomputing* 74 (2018), pp. 1299–1320.

[34] Abbas Yazdinejad et al. "A high-performance framework for a network programmable packet processor using P4 and FPGA". In: *Journal of Network and Computer Applications* 156 (2020), p. 102564.

[35] Abbas Yazdinejad et al. "A machine learning-based sdn controller framework for drone management". In: *2021 IEEE Globecom Workshops (GC Wkshps)*. IEEE. 2021, pp. 1–6.

[36] Abbas Yazdinejad, Ali Dehghantanha, and Gautam Srivastava. "AP2FL: Auditable privacy-preserving federated learning framework for electronics in healthcare". In: *IEEE Transactions on Consumer Electronics* (2023).

[37] Abbas Yazdinejad et al. "Hybrid privacy preserving federated learning against irregular users in next-generation Internet of Things". In: *Journal of Systems Architecture* 148 (2024), p. 103088.

[38] Abbas Yazdinejad. "Secure and private ml-based cybersecurity framework for industrial internet of things (iiot)". PhD thesis. University of Guelph, 2024.

[39] Karthik Viswanathan and Abbas Yazdinejad. "Security considerations for virtual reality systems". In: *arXiv preprint arXiv:2201.02563* (2022).