Volume 13, Issue 1, Page 26-34, 2024 https://doi.org/10.46810/tdfd.1273507 Research Article

BİNGÖL UNIVERSITY

Türk Doğa ve Fen Dergisi
Turkish Journal of Nature and Science
www.dergipark.gov.tr/tdfd

Deceptive Patch Solutions for Protecting Industrial Control Systems Based on Discovered Vulnerabilities

Özlem BATUR DİNLER[1*]

[1] Siirt University, Engineering Faculty, Computer Enginnering Department, Siirt, Türkiye
Özlem BATUR DİNLER ORCID No: 0000-0002-2955-6761

**Corresponding author: o.b.dinler@siirt.edu.tr*

(Received: 30.03.2023, Accepted: 15.01.2024, Online Publication: 26.03.2024)

Keywords
Cybersecurity,
Industrial control system,
Patch management,
Software vulnerability prediction

Abstract: An increase has been observed in concerns about cybersecurity threats in smart energy management on a global scale. Industrial Control Systems, or simply ICSs, are frequently present in industries and essential infrastructures, such as water treatment facilities, nuclear and thermal plants, heavy industries, power production, and distribution systems. ICS devices are high-risk targets for attacks and exploitation with significant security difficulties for ICS vendors and asset owners. Like many consumer electronics, industrial systems are susceptible to a bevy of vulnerabilities that hackers can exploit to launch cyber attacks. Extensive use of ICSs in Critical Infrastructures (CI) increases the vulnerability of CI to cyber attacks and makes their protection a critical subject. This study first contributes to a novel line of research considering how deception can be used by defenders in strategic terms with the objective of introducing uncertainty into an adversary's perception of a system patch management process in order to protect ICSs. Thus, we explore deceptive patch management models for the purpose of providing better insight into developing future cybersecurity techniques for ICS attacks.

Keşfedilen Güvenlik Açıklarına Dayalı Endüstriyel Kontrol Sistemlerini Korumaya Yönelik Yanıltıcı Yama Çözümleri

Anahtar Kelimeler
Siber güvenlik,
Endüstriyel kontrol sistemi,
Yama yönetimi,
Yazılım güvenlik açığı tahmini

Öz: Küresel ölçekte akıllı enerji yönetiminde siber güvenlik tehditlerine yönelik endişelerde artış gözleniyor. Endüstriyel Kontrol Sistemleri veya kısaca EKS'ler, su arıtma tesisleri, nükleer ve termik santraller, ağır sanayiler, enerji üretimi ve dağıtım sistemleri gibi endüstrilerde ve temel altyapılarda sıklıkla bulunur. EKS cihazları, EKS satıcıları ve varlık sahipleri için önemli güvenlik güçlükleri içeren saldırılar ve istismar için yüksek riskli hedeflerdir. Pek çok tüketici elektroniği gibi, endüstriyel sistemler de bilgisayar korsanlarının siber saldırılar başlatmak için yararlanabilecekleri bir dizi güvenlik açığına karşı hassastır. EKS'lerin Kritik Altyapılarda (KA) yoğun kullanımı, KA'ların siber saldırılara karşı savunmasızlığını artırmakta ve bunların korunmasını kritik bir konu haline getirmektedir. Bu çalışma ilk olarak, EKS'leri korumak için bir düşmanın bir sistem yama yönetimi sürecine ilişkin algısına belirsizliği sokmak amacıyla, aldatmanın savunucular tarafından stratejik terimlerle nasıl kullanılabileceğini ele alan yeni bir araştırma hattına katkıda bulunuyor. Bu nedenle, EKS saldırılarına yönelik gelecekteki siber güvenlik tekniklerinin geliştirilmesine ilişkin daha iyi bir anlayış sağlamak amacıyla aldatıcı yama yönetimi modellerini araştırıyoruz.

1. INTRODUCTION

An Industrial Control Systems (ICS) represents a range of individual control systems and other hardware that operate together with the vulnerability of automating or conducting industrial processes. The ICS domain has suggested automated tools and environments that are capable of simulating real control system hardware and software behaviors and ensuring a virtualized environment for the purpose of modeling a single type of ICS, such as Programmable Logic Controllers (PLCs), Distributed Control Systems (ICS), and Supervisory Control and Data Acquisition (CI).

It is vital to enhance the vulnerability of both enterprise networks and ICSs by strengthening cyber security across all points of ICSs. A vulnerability in a computer system represents a weak point, that a hacker can exploit and attack the system. It is possible to categorize the vulnerabilities exploited in the following way: Type 0 indicates zero-day vulnerabilities; Type 1 refers to known vulnerabilities; Type 2 denotes vulnerabilities that originate from protocols, services, and tools that are inherently insecure by nature; Type 3 indicates vulnerabilities related to the insecure configuration of equipment and networks; Type 4 refers to social engineering.

Three main events (discovery, disclosure, and patch) mark a vulnerability's lifecycle. The discovery of a vulnerability by a vendor, third-party institutions, or hackers indicates the lifecycle's beginning. Its public disclosure by the vendor, third-party institutions, or security researchers represents the following event. Black risk refers to the time period between discovery and disclosure. In the said period, the existence of the vulnerability is known only to a closed group of individuals. The patch release by the vendor represents the following event. Gray risk represents the time between the vulnerability disclosure and the patch release date. Nevertheless, the patch will not be installed instantly by all users when it is released by the vendor. White risk denotes the period between the patch date and the date of its installation by all users. A vulnerability's lifecycle comes to an end at the moment of installing the patch by all users.

Patches ensure a direct understanding of the said vulnerabilities in unpatched systems. Conventional patches are capable of weakening systems due to leaking information to an attacker concerning the condition of the system. The patches in question present defects to attackers, which they can use for the purpose of acquiring increased privileges, stealing data, and/or performing malicious unauthorized acts. Deceptive patches impact the decision of an attacker.

The major cybersecurity attacks on ICS infrastructures carried out in the last 20 years represent the most prominent ones with regard to the economic loss described [1]. We investigated them by suggesting possible solutions to prevent such attacks. In Asghar et al. [2], we primarily, examined a number of available studies suggesting several security evaluations, guidelines, and metrics, which might be beneficial for network administrators in predicting the possible risk and guiding them in finding the best solution to protect the ICS from attacks or deliberate assaults. In Upadhyay et al. [3], we presented a timeline analysis of the effect of deceptive patches and ultimately analyzed a formal model of deceptive patches, examining the theoretical security of deceptive patches with a game-theoretic approach. In Mughaid et al. [4], we utilized the world rank of news websites as the primary factor of news accuracy by employing two common and trusted website rankings. The findings demonstrate that the suggested method yields promising results in comparison to other comparative methods in identifying the accuracy of the news. In Mughaid et al. [5], a methodology for wireless cyber attack detection in 5G networks on the basis of implementing K-Nearest Neighborhood (KNN), Decision Trees (DTs), multi-class Decision Forest (DF), multi-class Decision Jungles, and multi-class Neural Network (NN) techniques. A superior performance was obtained as a result of the experiments carried out, with a 99% accuracy for the KNN algorithm and 93% for DF and NN. The difficulties of implementing traditional security measures for ICS with the objective of addressing security ICS concerning security requirements were highlighted in [6]. Yantz [7] assessed patch management, compliance, and risk management in the business world from the perspective of Operating System (OS vendors and employee productivity. Hassani [8] provided a strong foundation for the process that could be improved in the future with novel applications, better solutions, and methods for patch management. This research indicated that security patch management is essential in vulnerability management due to its functioning as a remediation plan in vulnerability management. Moreover, a risk-based approach to vulnerability management was presented on a solid basis in [9]. A data set of the gas pipeline control system, one of the essential infrastructures, was employed in [10].

Since reliability and safety represent essential components for an ICS, it is mandatory to understand the attack vectors and threat landscape, involving the resulting threats, to ensure the continued safety and security of control systems. This study contributed to the cybersecurity knowledge by providing patch management solutions for targeted cyber attacks with vulnerabilities of ICSs.

This study contributed to the knowledge of cybersecurity by providing a patch management model of the targeted cyber attacks with vulnerabilities of ICSs. An efficient cybersecurity strategy for an ICS must implement defense-in-depth, which represents a method of layering security mechanisms in order to minimize the failure of a mechanism to a minimum. A vulnerability can be removed by a patch. However, a patch may also present a higher risk from a production or safety perspective. Patch management should be applied as a systematic, documented, and accountable ICS patch management process to manage exposure to vulnerabilities.

The main contributions of the current work are listed below:

- The current study represents the first model defining software security patches and applying deceptive principles to ICSs, making the said methodology a new approach toward efficient analysis and proposing security vulnerability solutions for ICSs.
- The current work presents the novel feasibility of the model based on the basis of deceptive patch models. The most common attacks chosen are used, showing

the possibility of applying deception to patching security vulnerabilities in ICSs.

- We exploit a novel ICS patch management process to capture solutions for the targeted cyber attacks with vulnerabilities of ICSs.
- We investigate how to utilize compensating deception patch-based solutions for security vulnerabilities to reliably secure their control systems.

The organization of the rest of the current article is presented below. Section 2 introduces the overview of the background. Section 3 presents the proposed model. Finally, Section 4 ends with the conclusions and outlines future work.

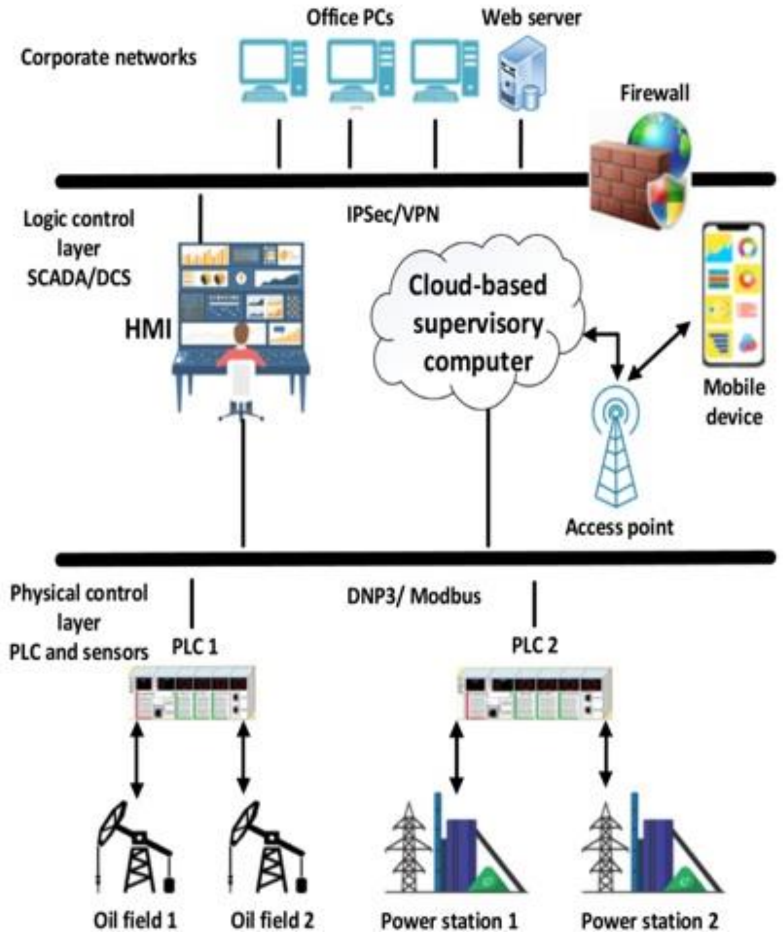
2. BACKGROUND

2.1. ICS Security Management

Security standards, among the ICS security issues, indicate the need for securing the ICS environment in an explicit way. The standards comprise security concepts, policies, risk management approaches, and security safeguards. The guidelines present suggestions for the measures that should be taken in case of attack detection. Moreover, they suggest the best practices and present an overview of the most essential security measures that all users can comprehend. It is possible to utilize the different metrics defined in the guidelines for the purpose of assessing cybersecurity strategies.

ICS standard protocols perform the collection and measurement of the system's status, utilize control-layer protocols with the objective of configuring the automation controller, send novel logic, and update the code. Nevertheless, the control layer protocols are predominantly vendor-specific protocols.

Figure 1 shows an overview of the ICS system. It is possible to divide a complete ICS infrastructure into three layers. In the corporate network layer, a supervisory computer or a Human Machine Interface (HMI) can be accessed remotely by managers in a remote way. In the logic control layer (in other words, SCADA/DCSs), an HMI or a cloud-based supervisory computer is utilized by system administrators to monitor the purpose of monitoring the status and sending the command for updating the control sequence. Additionally, all control devices (e.g., PLCs and sensors), protocols (e.g. Distributed Network Protocol version 3 (DNP3)/Modbus, and production sites are categorized as physical control layers.



Possible weaknesses in corporate networks
- Virus (anti-virus software not installed, anti-virus detection signatures not updated).
- Social engineering attacks (phishing, rogue access point).

Possible weaknesses in SCADA/DCS
- Configuration vulnerabilities (default system configurations are used, critical configurations are not stored or backed up, and OS and application security patches are not maintained).
- Weaknesses in security architectures (firewall, intrusion detection system are not installed).
- Software vulnerabilities (buffer overflow attacks, DoS attacks).

Possible weaknesses in production environments
- Communication vulnerabilities (use of insecure industry-wide ICS protocols, DNP3 or Modbus).
- Hardware vulnerabilities (insecure remote access of ICS components, inadequate physical protection of critical systems, and unauthorized personnel have physical access to the equipment).

Figure 1. Illustration of overview of the ICS system cyber security [2]

2.2. Patch Management in ICS

Software patch usually represents a piece of code utilized with the objective of fixing, altering, or updating anything in the software. It is necessary not to confuse patches with updates or upgrades since patches are generally employed to deal with single problems, while updates frequently involve a number of patches and improvements, and upgrades usually present novel versions and characteristics.

The deceptive patch types are presented below:

Diverse Patch: Patch diversity deals with the mono-culture issue caused by the available patching practices and may adversely influence resources utilized for development and exploitation. Due to the possibility of releasing multiple patches for a vulnerability, attackers should develop many exploits for every version of a patch to owe the potential for a widespread attack.

Faux Patch: A faux patch comprises fake patches for vulnerabilities not existing in the same sense, whereas a traditional patch comprises legitimate patches for existing vulnerabilities. A ghost patch is created by a faux patch when combined with a traditional patch. A faux patch is implemented in the best way to input validation vulnerabilities. In this way, we utilize deception to benefit from this frequently employed technique for the purpose of fixing the vulnerability type in question. Fake patches are similar to decoy passwords and decoy documents.

Obfuscated Patch: A legitimate vulnerability is fixed by an obfuscated patch, which is ideally designed to be infeasible for the purpose of reversing engineer and uncovering the underlying defect. The mentioned patches increase the effort required for the adversary to define the vulnerability being fixed by the patch. Since the said patches fix legitimate vulnerabilities, they change the program’s semantics. The objective of the patches in question is to confuse attackers as they perform exploit development by burying the actual vulnerable code in layers of the obfuscated patch code.

Active: An active response patch fixes the underlying vulnerability but responds to adversarial interaction as if the vulnerability is still present. In the interaction with an active response patch, attackers must, in ideal, be unable to find whether the remote system is patched or vulnerable. The primary aim of the mentioned patches is to impact attackers to make them believe in the success of their exploit, which will ensure that defenders monitor the actions of the adversary during their attack.

A security patch refers to a change in an asset to correct a weakness induced by a vulnerability. The objective of a security patch is preventing exploitation and mitigating threats to an asset. Hackers continuously develop novel techniques with the aim of breaking software and exploiting defects for the penetration of security measures.

Vulnerabilities and bugs in ICS software modules may lead to severe results. However, frequent patching of the said systems can cause mission-CI to be intolerably unavailable. The vulnerability trends in software considerably influence the process of discovery and subsequently trigger a patch deployment for suppressing the potential possibility of a breach.

A patch management program is centered on safe procurement, testing, and implementing the trusted patches to keep ICS more secure. It ensures that the ICS is up-to-date and safeguarded against malware and hackers. It is applicable to all hardware and software components of ICS, in both Information Technology (IT) and OT. Patches are required to assist in resolving security vulnerabilities and addressing functional problems. Table 1 represents Industrial Control System attacks.

Table 1. Industrial Control System Attack

Attack Ref	SRA	PM	CM	NS	SRP	OTD	EAS	ANHSF	SCM	A&T
Slammer [11]		•		•					•	•
Stuxnet [12]			•		•	•	•	•		
VPN Filter [13]		•				•				•
Black Energy [14]	•		•		•	•	•	•		•
NotPetya [15]		•	•	•	•	•	•	•		
Industroyer [16]					•	•	•	•		•
Steel Mill [17]										•
Triton [18]				•	•	•	•	•	•	
Shamoon [19]			•		•	•	•	•		•

SRA: Secure Remote Access, PM: Patch Management, CM: Credential Management, NS: Network Segmentation, SRP: Software Restriction Policies, OTD: Outbound Traffic Detection, EAS: Execution of Explicitly Allowed Software, ANHSF: Audit Network Hosts for Suspicious Files, SCM: Secure Configuration Management, A&T: Awareness and Training

3. PROPOSED MODEL

This study presents novel research, considering the possibility of strategic use of deception by defenders with the aim of introducing uncertainty into the adversary's perception of a system. In the current research, we concentrate on deceptive patches, in which standard software patches are designed for the purpose of limiting the knowledge that an adversary can acquire about the underlying vulnerability.

This study demonstrates the feasibility of applying deception, in the form of fake patches, to ICS attacks. We believe that the approach in question, either as a stand-alone technique or in combination with other deceptive and detection methods, can cause an exponential increase in program analysis, making exploit generation on the basis of patches a costly procedure while increasing the program runtime only at a minimal level.

3.1. Deceptive Patch Solutions for ICS Attacks

With the persistence of observed trends in ICS environments, attackers have scant motivation to adjust a set of Tactics, Techniques, and Procedures (TTPs) from currently successful behavior types. What is more important is that security suggestions and guidance should be expanded to involve fundamental detection and monitoring strategies, which are capable of identifying (or blocking) fundamental behaviors related to available adversary TTPs. Policymakers and defenders should seek avenues with the aim of enhancing defense and response acrooss the whole chain of events constituting and intrusion scenario. In this way, the response is provided at earlier stages, which minimize effects and protect crucial services. In this way, the response is provided at earlier stages, which minimizes effects and protects crucial services. Figure 2-3 demonstrates an attack on corporate information system hosts.

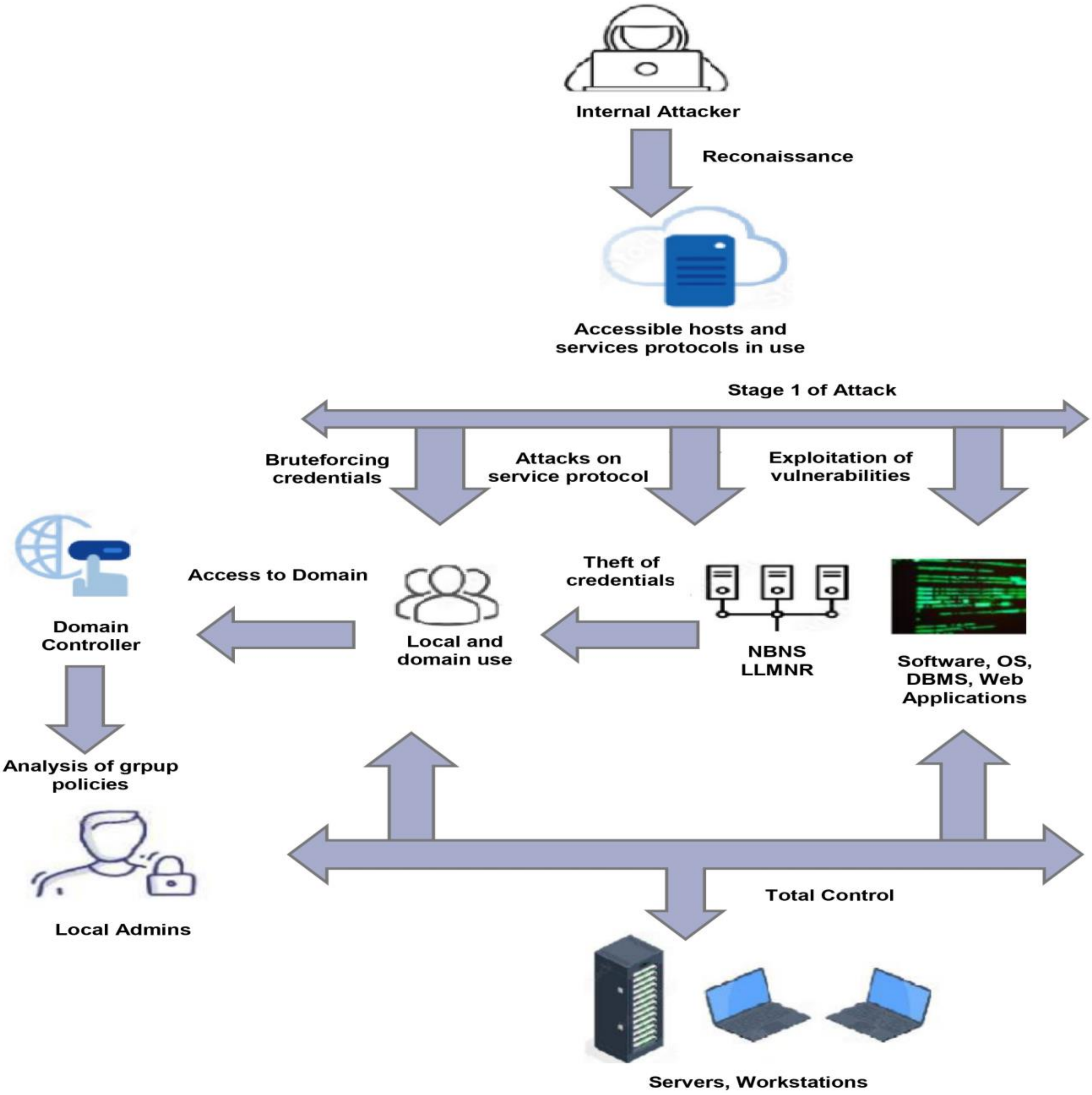


Figure 2. An attack on corporate information system hosts.

Deceptive patches have three general categories: faux patches that present a fix for a vulnerability not exist in reality, obfuscated patches that hide the vulnerability being dealt with, and active response patches that fix the vulnerability while trying to convince adversaries that the system remains unpatched. To analyze ICS attack-based security, we propose to present it based on all types of patch solutions.

In attack [11], a vulnerability in Microsoft SQL Server 2000 constituted the basis of the worm, which penetrated the network of the nuclear power plant through the laptop of a contractor connected to the facility’s business network. The worm could access the monitoring system by leveraging incorrect network isolation and made it inaccessible because of the large traffic created.

Remediate Vulnerability; It is necessary to keep ICS isolated from the corporate network utilizing firewalls. While it is understood that there is no possibility for complete ICS isolation, a solution is to limit the number of entry points into the ICS from the corporate network and keep them monitored. It is recommended to update and perform maintenance checks on servers on a regular basis with the objective of reducing the probability of attacks. Following the mentioned event, the update of all Microsoft SQL servers' software in the power plant was updated, and patches were installed.

In attack [12], Stuxnet physically delivered a number of its first infections physically, in other words, through a USB flash drive. Thus, it tried to spread to other workstations in the target network through numerous alternative zero-day vulnerabilities, such as a) USB flash drives, b) the Windows Print Spooler service, c) network shares or the Server Service, and d) local privilege escalation.

Remediate Vulnerability; The attackers employed a workaround method with the aim of bypassing such solutions by infecting the personal computers of individuals with legitimate physical access to the plant's system of the plant. It is also necessary to monitor the physical components of the plant for the purpose of detecting an unusual behavior of a component in order to detect any compromise of the ICS of the plant in the shortest time. It is necessary to authenticate the control loops among the mentioned entities in a proper way and verify the results of their feedback loops.

The proposed deceptive patch solution is an active response patch. An active response patch fixes the underlying vulnerability and responds to adversarial interaction as if the vulnerability no longer exists (and possibly issues an intrusion notification). This type of patch presents deceptive data to attackers in real-time. In other words, data is statically or dynamically produced and introduced to attackers to impact their decision-making process. According to the non-interfering feature, faux patches must not change the program's semantics; the verify step will reveal that fake patches do not change the behavior of the program. In the interaction with an active response patch, attackers must, in ideal, be unable to find whether the remote system is patched or vulnerable. The exploitation of a vulnerability by active response patches, which respond to exploits using the same response as an unpatched program. The said masking will increase the resources required for dynamic analysis tools to recognize unpatched systems.

Attack [14] equipped adversaries with the toolset for the purpose of performing reconnaissance in IT and accessing software, including VPN and remote access tools. With the above-mentioned access type, attackers can connect to the OT in a direct way and realize their malicious acts.

Remediate Vulnerability; In case of infecting the system with malware, there is a possibility of using decrypting tools to decrypt the Master File Table (MFT) with the aim of recovering files impacted by the attack. Performing the system's regular backups represents another good practice. If damage to the OS cannot be repaired, it is a possibility of reverting back to the version that has been previously saved version in a safe manner. It is possible to employ sandboxing technology for testing emails and documents entering the network and deploy proxy systems for the control of inbound and outbound communication paths. Strong authentication and encrypted communication are needed during remote access to ensure that attackers do not access ICS remotely.

Attack [15] represents a cryptoworm attack against MS Windows-basedhosts. A defect in the company's patch update policies ensured that the attackers compromised certain servers. The modification of the malware was performed to utilize an open-source credential dumping tool, showing that user passwords are stored in the memory of the computer for the purpose of spreading across the network. It could be limited by performing frequent updates of the OS and establishing antimalware and antivirus utilities.

Remediate Vulnerability: In case of infecting the system by the malware, there is a possibility of using decrypting tools to decrypt the MFT with the aim of recovering files impacted by the attack. Performing the system's regular backups represents another good practice. If damage to the OS cannot be repaired, it is a possibility of reverting back to the version that has been previously saved version in a safe manner.

The proposed deceptive patch solution is a faux patch. A ghost patch is created by a faux patch when combined with a traditional patch. A faux patch is implemented in the best way to input validation vulnerabilities. In this way, we utilize deception to benefit from this frequently employed technique for the purpose of fixing the vulnerability type in question. Fake patches are similar to decoy passwords and decoy documents. Adding conditional and/or assertion statements to the code, which is capable of detecting invalid input, represents the conventional way to fix the said vulnerability type.

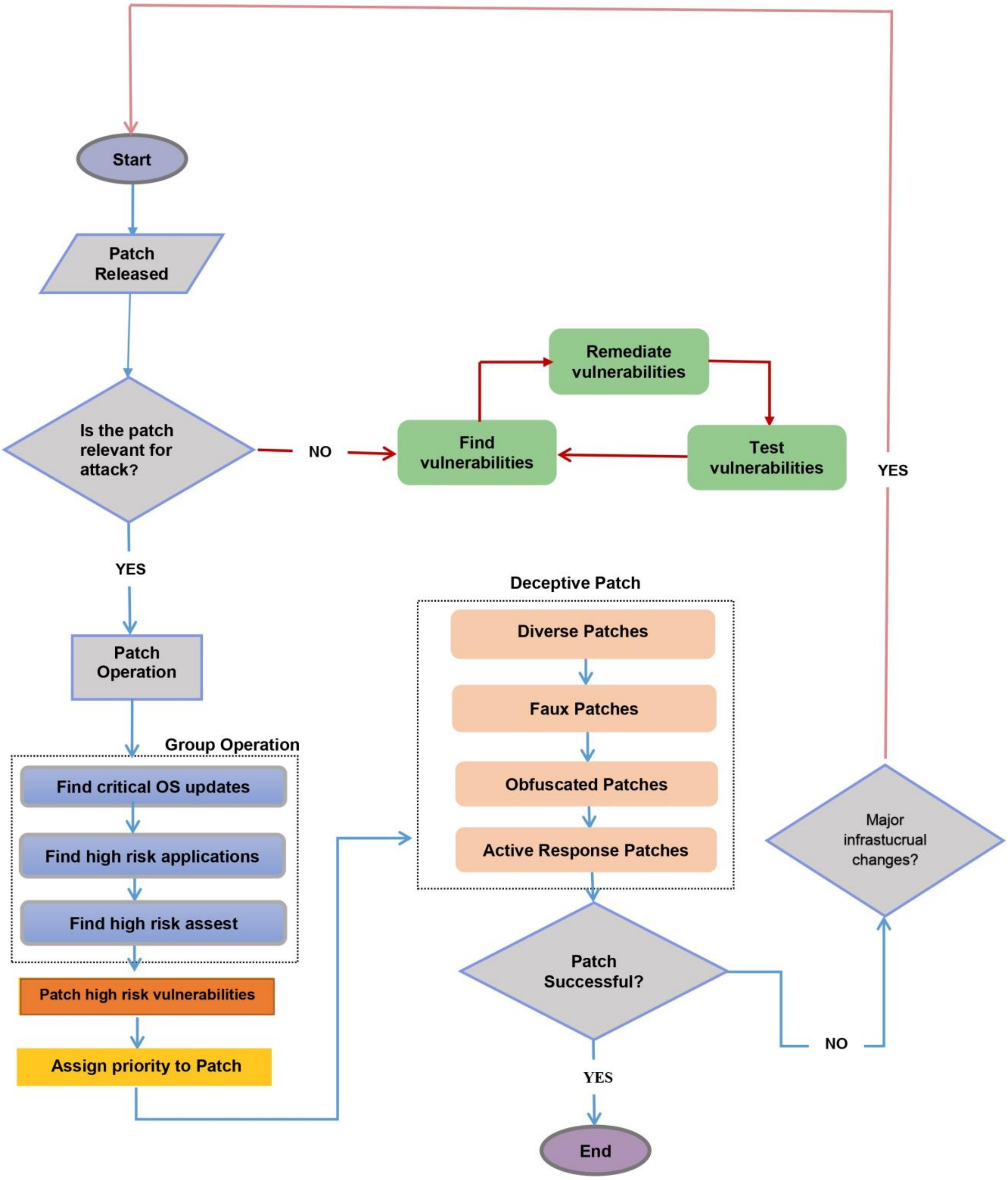


Figure 3. An attack on corporate information system hosts.

In attack [16], the attackers utilized a misconfiguration providing bidirectional data flow, with the objective of gaining a foothold on the ICS network. Industroyer performs scanning and prepares lists of all the OPC servers that the software provides. Moreover, it tries to alter the state of devices that are connected to the said OPC servers. The attackers exploited vulnerabilities targeting the devices of grid operations and network communications, infecting them via spear-phishing campaigns and the fundamental lack of security mechanisms for ICS protocols.

The proposed solution is a diverse patch. Patch diversity deals with the mono-culture issue caused by available patching practices and may adversely affect resources utilized for development and exploitation. Due to the possibility of releasing multiple patches for a vulnerability, attackers should develop many exploits for every version of a patch to owe the potential for a widespread attack. Implementing software diversity in patch development, using deceptive language in patch notifications, and re-releasing the said patches as novel updates may impact attackers by leading to uncertainty in the reconnaissance phase of their attack.

In attack [17], spear-phishing and social engineering tactics were employed by the attackers with the objective of accessing the business network. Thus, they established access to the OT network and could connect to individual control systems.

Remediate Vulnerability; Tools such as defense systems and firewalls must be utilized to protect interconnections between the OT network and the corporate network for the purpose of safeguarding against the above-mentioned intrusions. Additionally, it is necessary to minimize the number of connection interfaces between the corporate network and the OT network. In attack [18], the goal of the malware was to breach the controllers' safety mechanisms in the target facility. Pieces of evidence show that the attackers may have acquired access to the OT network almost a year prior to the incident. Due to a misconfigured firewall, the attackers gained a foothold on the target controller by utilizing a custom-made TRITON attack framework. Attack [19] represents malware aiming to render the computers in the target organizations unusable as a result of wiping their hard drives. The malware could carry out its acts because of the interconnected computers in the business network, stolen credentials, and the usage of a legitimate driver. Because the exchanged data between the OT and IT are utilized for the purpose of determining the requirements and procedures of the business, such terrible attacks on the IT network can deprive the ICS of high-level site operations, supporting the process of production in the OT.

The proposed deceptive patch solution is an obfuscated patch. Implementing polymorphic patches represents a solution to it. Randomization can be employed by ghost patches to create polymorphic patches, which can be distributed based on the basis of various heuristics (such as on the basis of region, OS version, or staggered by time). The non-deterministic characteristics of a polymorphic ghost patch can make exploit development more difficult since the same patch will not be implemented on every end system. In the above-mentioned situation, it will also be necessary to change the conventional patch for every patch instance for the purpose of preventing attackers using multiple instances of a patch to expose the legitimate vulnerability.

4. CONCLUSION

Industrial computer networks have recently been constantly exposed to cyberattacks. The detection and patch philosophy constitute the basis for numerous security solutions in the said area. A systematic approach toward managing and employing software patches may assist organizations in enhancing the general security of their IT systems in an inexpensive way. This study presented the first map for formally modeling the security of the suggested deceptive defense techniques for ICS. The proposed patch methodology is the first work on solutions for ICS software vulnerabilities using deceptive patch types in most common ICS attacks. This paper provided evidence indicating that the applied deceptive patch methodologies keep ICSs more secure. Investigating and implementing deep learning to deception is a future research field that may have an enormous effect on the way of our defense.

Acknowledgement
This manuscript does not contain any studies with human participants carried out by any of the authors.

REFERENCES

[1] Alladi T, Chamola V, Zeadally S. Industrial control systems: Cyberattack trends and countermeasures. Computer Communications. 2020; 155(22):1–9.

[2] Asghar MR, Hu Q, Zeadally S. Cybersecurity in industrial control systems: Issues, technologies, and challenges. Computer Networks. 2019; (165):1389-1286.

[3] Upadhyay D, Zaman M, Joshi R, Sampalli S. An efficient key management and multi-layered security framework for SCADA systems. IEEE Transactions on Network and Service Management.2021; 19 (1): 642–660.

[4] Mughaid A, Al-Zu'bi S, Al Arjan A, Al-Amrat R, Alajmi R, Zitar RA, et al. An intelligent cybersecurity system for detecting fake news on social media websites. Soft Computing. 2022; 26(12):5577–5591.

[5] Mughaid A, AlZu'bi S, Alnajjar A, AbuElsoud E, Salhi SE, et al. Improved dropping attacks in 5G networks using machine learning and deep learning approaches. Multimedia Tools and Applications. 2022: 82(1): 1–23.

[6] Idrissi OE, Mezrioui A, Belmekki A. Cybersecurity challenges and issues of industrial control systems–some security recommendations. IEEE International Smart Cities Conference (ISC2). Casablanca: April; 2019. p. 330-335.

[7] Yantz M. [Internet]. Importance of patch management to avoid business vulnerabilities; 2023 [cited 2023 March 13]. Available from:https://itsupportguys.com/importance-of-patch-management-to-avoid-business-vulnerabilities.

[8] Hassani P. Implementing patch management process [dissertation]. School of Technology Degree Programme in Information and Communication Technology; 2020.

[9] Koskenkorva H. The role of security patch management in vulnerability management [dissertation]. Finland: South-Eastern Finland University of Applied Sciences; 2021.

[10] Söğüt E, Erdem OA. Endüstriyel kontrol sistemlerine (SCADA) yönelik siber terör saldırı analizi. Politeknik Dergisi.2020;23(2):557-566.

[11] Holloway M. Slammer worm and David-Besse nuclear plant [Internet]; 2015 [cited 2022 April 12]. Available from: http://large.stanford.edu/courses/2015/ph241/holloway2/.

[12] Nourian A, Madnick S. A systems theoretic approach to the security threats in cyber-physical systems applied to Stuxnet. IEEE Transactions on

Dependable and Secure Computing. 2015;15 (1):2–13.

[13] Largent W [Internet]. New VPNFilter malware targets at least 500k networking devices worldwide; 2018. [cited 2022 Jun 6]. Available from: http://blog.talosintelligence.com/2018/05/ VPNFilter.html.

[14] Xiang Y, Wang L, Liu N. Coordinated attacks on electric power systems in a cyber-physical environment. Electric Power Systems Research. 2017;149(6): 156–168.

[15] Furnell S, Emm D. The ABC of ransomware protection, Computer Fraud & Security. 2017;(10):5–11.

[16] Cherepanov [Internet]. A new threat for industrial control systems; 2021 [cited 10 August 2023]. Available from: https://www.nae.edu/ File.aspx?id=266340.

[17] Lee RM, Assante MJ, Conway T. German steel mill cyber attack. Industrial Control Systems. 2014;1-15.

[18] Johnson B, Caban D, Krotofil M, Dan S, Brubaker N, Glyer C [Internet]. Attackers deploy new ics attack framework triton and cause operational disruption to critical infrastructure; 2023 [cited 2023 September 10]. Available from:https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html.

[19] Symantec [Internet]. The shamoon attacks. [cited 2022 March 6]. Available from: http://www.symantec.com/connect/blogs/shamoon-attacks.

[20] Panetta K. [Internet]. Gartner top 10 security projects for 2020-2021; 2021.[cited 2023 January 15]. Available from: https://www.gartner.com/smarterwithgartner/gartner-top-security-projects-for-2020-2021/

[21] Olswang A, Gonda T, Puzis R, Shani G, Shapira B, Tractinsky N. Prioritizing vulnerability patches in large networks. Expert Systems with Applications.2022; 116467.

[22] Corallo A, Lazoi M, Lezzi M, Luperto A. Cybersecurity awareness in the context of the Industrial Internet of Things: A systematic literature review. Computers in Industry. 2022; 137(4):1-16.

[23] Bristow M, Sans A [Internet]. A SANS 2021 Survey: OT/ICS Cybersecurity. Survey; 2021. [cited 2023 Januray 15]. Available from: https://www.sans.org/white-papers/SANS-2021-Survey-OTICS-Cybersecurity/

[24] Yang B, Zhang Y. Cybersecurity analysis of wind farm industrial control system based on hierarchical threat analysis model framework. International Conference on Computing, Communication, Perception, and Quantum Technology, CCPQT 2022. Xiamen: IEEE p. 6-13.