Scalable Computing: Practice and Experience, ISSN 1895-1767, http://www.scpe.org
© 2024 SCPE. Volume 25, Issues 1, pp. 65–74, DOI 10.12694/scpe.v25i1.2254

ENHANCING INDUSTRIAL CONTROL NETWORK SECURITY THROUGH VULNERABILITY DETECTION AND ATTACK GRAPH ANALYSIS

YAN LIAO*

Abstract. Insufficient communication attack defense capabilities within industrial control networks is a serious problem that is addressed in this study. The author proposes a methodology that focuses on creating attack graphs to ease security and vulnerability studies in industrial control network systems in order to address this issue. The article provides thorough construction guidance and techniques for attack graphs, which are used for penetration testing and vulnerability analysis of networks for industrial control systems. On the created attack graph, experimental evaluations utilizing the "earthquake net" virus were carried out. The findings point to four main attack routes where the "Zhenwang" virus is most likely going to attack and cause the most damage. With a loss value of 12.2 and an attack success chance of 0.096, the first path involves cumulative attack stages. The second path consists of cumulative attack steps, with a loss value of 10.2 and an attack success probability of 0.072. The third path encompasses cumulative attack steps, with a loss value of 16.6 and an attack success probability of 0.063. The fourth path comprises cumulative attack steps, with a loss value of 18.6 and an attack success probability of 0.084.

Key words: Industrial control networks, Security vulnerability detection, Attack graph construction, Vulnerability analysis, Penetration testing, Network security

1. Introduction. The Internet has transformed people's lives significantly, facilitating global connectivity through its unique openness and data-sharing capabilities. Over nearly five decades of development, the Internet has saturated for all society, from finance, e-commerce, and industrial control to communication, transportation, healthcare, education, and beyond. It has become an essential infrastructure ensuring the stability of these critical domains. In the digital age, the Internet, with its core in cyberspace, is increasingly recognized as the "fifth space", closely intertwined with people's lives alongside land, sea, air, and sky [17].

Evolution of networking and informatization has introduced for security challenges in network security. These challenges apparent in the following ways: Explosion of Vulnerabilities: With the absence of remotely avoidable design flaws, the count of vulnerabilities halting from application software or operating system design and configuration continues to rise, maintaining elevated levels. These vulnerabilities frequently become targets for attackers, affecting an ongoing and significant threat to network security. The transformation in information carriers, transmission methods, and interconnection modes has furnished attackers with convenient avenues for launching network attacks. Furthermore, enhancing attackers' capabilities has led to more organized attack behaviours and specialized attack techniques, resulting in many new threats. Thus, vulnerabilities have evolved into a predictable security risk. According to data from the National Vulnerability Database (NVD) published by the National Institute of Standards and Technology (NIST), since 1997, the tally of known vulnerabilities has surged to 66,165. Over the years, the number of disclosed vulnerabilities has risen significantly [13].

Attack and defence represent the sides of network security. Without investigating the depths of attack theory and technology and comprehending our vulnerabilities and adversaries' tactics, we cannot effectively safeguard the security of network information systems. An integral aspect of research into network attacks centres on understanding and describing these attacks. The attack process encompasses a spectrum of distinct attack behaviours, each characterized by various stages and states. Given the complexity and diversity inherent to the attack process, deriving correlations and summarizing rules from known attack behaviours presents a formidable challenge [12].

The current theoretical foundations of attack detection technology remain incomplete. An approach rooted in attack-based analysis can furnish a structured and visual portrayal of the entire attack process. This

*Chongqing Technology and Business Institute, Chongqing, 400052 (liaoyan671@126.com)

approach is invaluable for separating and connecting the knowledge from existing research on attack behaviours. Furthermore, it enhances the usefulness of attack detection and security alerts [18].

The paper is organized into five main sections, including the introduction Section. The Literature review explores the existing body of knowledge and research in computer network security vulnerability detection and attack graph construction, as explained in Section 2. Section 3, the proposed method, outlines the novel approach and methodology proposed by the author, including the formulation of attack graphs and vulnerability detection techniques. Section 4, results and discussion, presents the empirical findings and engages in a detailed analysis and interpretation of the results obtained from experiments or simulations. Finally, in Section 5 summarizes the concluding remarks of the research.

2. Literature Review. With an increasingly intricate network security landscape and growing cyberattack threats, many organizations and institutions recognize the limitations of solely relying on detection-based defence for post-attack responses. It has become evident that a proactive and preemptive defence mechanism is needed to address security challenges fundamentally. This demand has encouraged a growing interest in risk assessment within the security [8].

Given the complexity of attacks, researchers are exploring using attack models to dissect and understand these threats. In the initial phases of assessing network system vulnerabilities, researchers primarily distilled their experiences from practical use. Then, these insights are applied to test a broader spectrum of network systems. This process effectively transitions from rule extraction to rule matching. The primary research focus revolves around generating more precise and comprehensive rulesets. Presently, mature network vulnerability scanning technologies exemplify this method. Nevertheless, rule-based vulnerability analysis methods exhibit inherent limitations. Consequently, some researchers have used formal theoretical tools like attack trees, graphs, and Petri nets to develop more holistic vulnerability analysis methodologies [19].

For instance, an information security method is proposed that quantifies the energy level associated with each attack. This assessment relies on the energy level increment of the attack and its impact on the Common Vulnerability (CV). To demonstrate the effectiveness of their proposed countermeasures, they compared CV and energy consumption across different types of attacks. These countermeasures leverage network-related security algorithms to safeguard large data communication and Distributed Critical Infrastructure Applications (DCAV), effectively mitigating CV and large data leaks during data transmission [1].

The State Grid's software, hardware, and network layers are identified as the most vulnerable points. Subsequently, the contributors investigated the threats these systems faced based on their vulnerabilities. Finally, the authors aimed to offer insights into the most productive defence solutions currently available and the imperative need for developing new defence mechanisms [11].

The researchers presented a technique for creating intelligent Production Planning and Control (PPC) systems. To improve PPC procedures, these intelligent PPC systems make use of cutting-edge technology such as the Internet of Things, big data analytic tools, and machine learning. These systems enable dynamic and near-real-time responses to changes in the production system by gaining insights from various data sources inside the production system, taking into account the expertise of production planners, and applying analytics and machine learning. The important issues and difficulties that production managers may run into when applying the suggested strategy are shown through a case study [10].

The author introduces a novel approach wherein a node's weight is defined based on three key factors: the system loss resulting from various vulnerability exploitation methods, the likelihood of attack success, and the progression of attack steps. Simultaneously, this method employs these weightings to analyze the optimal attack target within the industrial control network. Subsequently, it identifies the corresponding attack path to target this vulnerability. This approach employs an attack graph generation technology that emphasizes repairing vulnerable links. Experimental validation demonstrates the effectiveness of this technology, underscoring its substantial importance in enhancing industrial control networks' communication attack defence capabilities [3].

3. Research Methods.

3.1. Generation algorithm of attack graph for industrial control network. The security of industrial control networks is enhanced by introducing an innovative algorithm. The algorithm takes indications from the four key elements inherent to these networks: components, connections, control authority, and com-

Table 2.1: Comparison of proposed and existing approaches in industrial control network security

Aspect	Proposed Approach	Existing Methods
Methodology	Focuses on attack graph generation for analysis.	Relies on IDS, firewalls, access controls, and more.
Focus	Emphasizes visualizing attack paths and vulnerabilities.	Prioritizes preventive measures and signature-based detection.
Risk Assessment	Quantitative risk assessment with values and probabilities.	Often uses qualitative risk assessment.
Proactive vs. Reactive	Proactive, identifying vulnerabilities before exploitation.	Reactive, responding to security incidents as they occur.
Complexity	Provides a structured and visual portrayal of attacks.	May lack a comprehensive view of potential attack paths.

Table 3.1: List of utilization methods

Description	Abbreviation
Modify control parameters	ModConPa
Modify measurement parameters	ModMeasPa
Modification control procedure	ModContPr
Get permission or a password	GetPriv

munication permissions. It aims to systematically evaluate network vulnerabilities and identify potential attack routes. By conducting a thorough analysis of these elements and effectively implementing the algorithm, the research endeavors to reinforce the defense mechanisms against communication attacks within industrial control networks, thereby strengthening their overall flexibility against cyber threats.

(a) Four Elements of Industrial Control Network

The first element is the industrial control component, represented by h_i for a single component and H for a set of industrial control components. It has the following four parameters: using *host_id* represents the address of a single component; Use service to represent the control service provided by the component; Use vul_i to indicate the vulnerability number of components available for remote or local use; $value_i$ represents the value of the component.

The second element is the connection of the industrial control network, which is represented by C, and has three parameters in total, H_{From} is used to represent the starting component of the connection; Use *Pro* protocol to represent the connection protocol; Use H_{To} to represent the connected components [2].

The third element is the vulnerability of a single component, which is represented by vul_i, it has three parameters, namely *host_id* indicates the address of the component where the vulnerability is located; Use *Type* to indicate the utilization way of the vulnerability; Use *Att_Patt* indicates the utilization mode of the vulnerability, and various utilization modes are shown in Table 3.1.

The fourth element defines user permissions on an individual component. It employs three distinct categories: “access” signifies the browsing permissions granted to regular users, “user” represents the standard operational permissions for regular users, and “root” denotes the comprehensive operational authority employed by the system administrator user over the information resources of the component.

(b) Derivation of algorithm

After a successful attack, the industrial control network changes from network state S_i to the next network state S_{i+1}, it is called state migration. If the industrial control system network needs to undergo a state transition, the following four conditions must be met simultaneously:

① When the industrial control network is in the initial state S_0, the network attacker must have sufficient authority on the attack-initiating component and can use the controlled component to attack other components

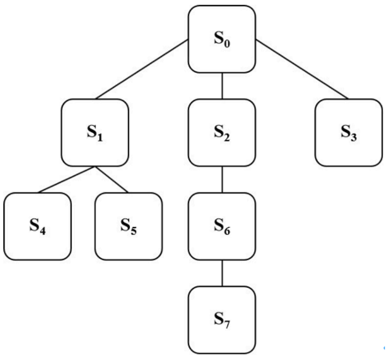

Fig. 3.1: Specific implementation process of algorithm

in the industrial control network. Use H_{victim} to indicate the components that have been successfully controlled by the attacker, and use H_{goal} to indicate the components that the attacker plans to control, namely the target components;

② There should be a relationship between H_{victim} and H_{goal} to ensure the smooth migration of network status as expressed in Equation (3.1);

$$C = (H_{victim}, Protocol, H_{goal}) \neq \emptyset \tag{3.1}$$

③ The target component H_{goal} needs to satisfy Equation (3.2), that is, it has a vulnerability so that attackers can use its vulnerability to migrate the network state;

$$Vul = (H_{goal}, Type, Att\_patts) \neq \emptyset \tag{3.2}$$

④ An attacker must obtain at least the minimum operation permission on the target component H_{goal}, and at least the minimum attack permission on the controlled component H_{victim}, to take advantage of its vulnerability to realize the migration of network state.

(c) Basic idea of algorithm

As shown in Figure 3.1, starting from the initial state S_0 of the network, use the above four rules to determine the possible state of the attacker in turn, after judgment, S_1, S_2 and S_3 meet the conditions for state migration. According to the principle of width first search, S_1, S_2 and S_3 are judged on the condition of state transition in turn, it can predict the state the attacker can reach. The attack target function H_{goal} whose S_3 state meets the above attack conditions indicates that S_3 state is a suitable attack target, so there is no need to judge its state transition conditions; Continue to judge S_1, where S_4 and S_5 are the nodes that meet the state migration conditions, and then judge S_2, and S_6 is the node that meets the migration conditions; Then continue to judge the state transition conditions of nodes S_4, S_5 and S_6 on the next layer, where S_5 state meets the state transition conditions and is a target of the attacker, therefore, it is not necessary to judge the condition of state transition; Continue to judge the state transition conditions of S_4 and S_6, when judging S_4, it is found that it can neither reach any new state node nor meet the attack target function, and it should be the last layer; When judging S_6, S_7 is the node that meets the migration conditions, and then judge the state migration conditions of node S_7, if it is found that the node can neither reach any new state node nor meet the attack target function, then S_7 is also the last layer, and the complete state migration process has been completed [4].

(d) Implementation of algorithm

Commencing from the initial state of the industrial control network, assess all potential network states based on the four state transition criteria mentioned earlier and incorporate the assessment outcomes into the state queue. The step-by-step procedure is visually depicted in Figure 3.2.

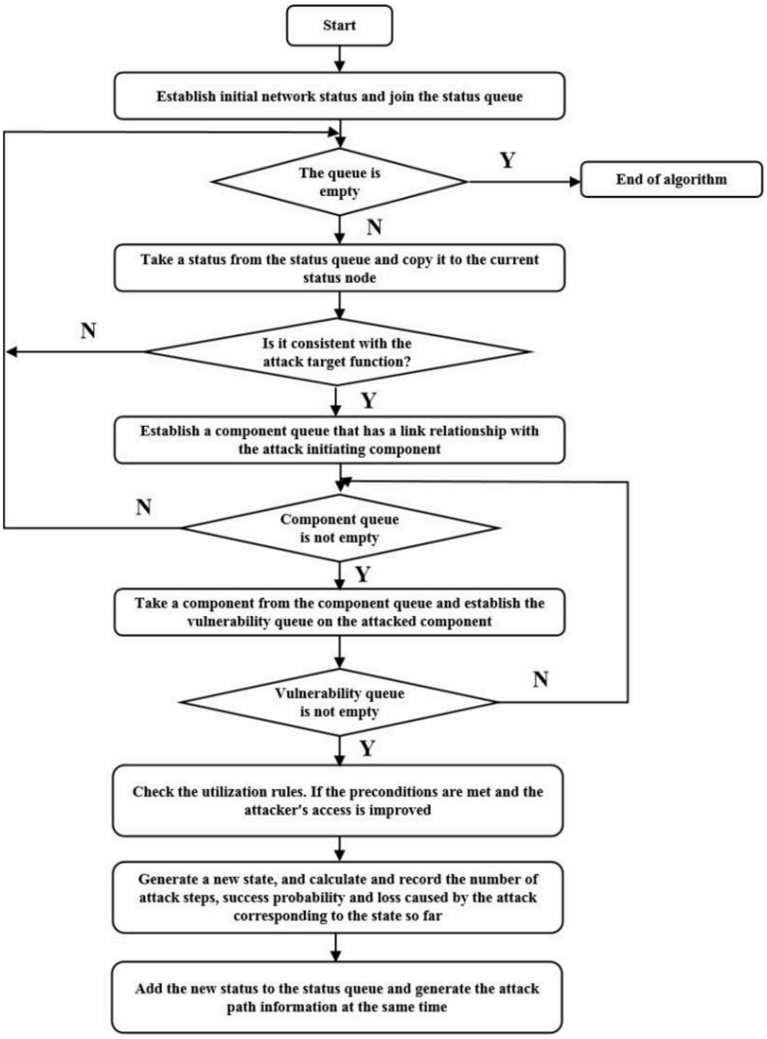
Start
Establish initial network status and join the status queue
The queue is empty
Y
End of algorithm
N
Take a status from the status queue and copy it to the current status node
N
Is it consistent with the attack target function?
Y
Establish a component queue that has a link relationship with the attack initiating component
N
Component queue is not empty
Y
Take a component from the component queue and establish the vulnerability queue on the attacked component
N
Vulnerability queue is not empty
Y
Check the utilization rules. If the preconditions are met and the attacker's access is improved
Generate a new state, and calculate and record the number of attack steps, success probability and loss caused by the attack corresponding to the state so far
Add the new status to the status queue and generate the attack path information at the same time

Fig. 3.2: Flow chart of the proposed vulnerability detection and attack graph algorithm

3.2. Comprehensive analysis and modeling of network vulnerabilities and attacks. A multilayered strategy for network security, encompassing three pivotal stages is introduced. Initially, it conducts a careful examination of network vulnerabilities to pinpoint potential vulnerabilities. Subsequently, the training focuses on crafting a strong attack prototype, serving as the groundwork for simulating and comprehending potential cyber threats. Finally, the research employs a systematic methodology to deduce attack sequences, providing deeper insights into prospective security breaches. The overarching objective is to fortify network defenses and strengthen against evolving cyber threats.

(1) Analyze network vulnerabilities

A data mining technique known as the association rule mining algorithm is employed to divide the attributes of vulnerability exploitation behaviour. This algorithm can uncover patterns of shared characteristics within comparable instances of vulnerable intrusion behaviours. However, the extraction process necessitates combining environmental factors with the recognized characteristics of vulnerability exploitation behaviour.

(2) Establish attack prototype

To execute an atomic attack, an attacker must fulfil specific prerequisites, including identifying vulnerabilities within industrial control components, establishing a requisite connection, and attaining a predetermined level of control authority. Upon successfully infiltrating a component, the attacker can elevate their control authority, augmenting the network's loss value. This process forms a continuous cycle where each concluding atomic attack covers the way for the subsequent one, ultimately culminating in reaching the attack target and accomplishing the intended attack objective.

Establishing an attack prototype relies on two primary inputs: network topology and network vulnerability analysis, both of which furnish specific details about network vulnerabilities. In this context, the network topology contributes information encompassing the control network connection (C), control components (H), and control authority associated with each control component—comprising the quartet of elements characterizing the industrial control network. Concurrently, the network vulnerability analysis segment offers insights into the connection status and component vulnerabilities (Vul) within the real industrial network. Subsequently, the Attacker model, proposed in the attack graph algorithm, serves as the attack source. At the same time, the Attack_Rule rules are employed to convert all network vulnerabilities into sets of atomic attacks, thereby constituting the attack prototypes [16].

(3) Reasoning attack sequence

The process of deducing the attack sequence involves the application of pre-established attack prototypes to the real industrial control network. This application aids in ascertaining the attacker's actions and their impact on the overall network.

The term "Atom" is employed to denote an autonomous attack prototype comprising two essential parameters: the edge (referred to as "edge") and the node (designated as "point") within the attack graph. The dynamic progression of these edges and nodes within the attack graph interlinks individual attack prototypes, thereby composing the attacker's sequence of actions. To deduce the comprehensive attack sequence, inferring the transition conditions between these atomic prototypes is imperative. To establish whether two atoms are capable of transitioning, the following specific steps are undertaken:

① Determine whether the two components are connected;

② To establish the permission utilization relationship among various attack prototypes (referred to as "atoms"), the attacker's operational authorization gained from the target component in one attack prototype (atom1) must surpass the access permissions employed by the attacker on the target component of another attack prototype (atom2). Only under these conditions can the continuous transformation of atoms be sustained, ensuring the uninterrupted progression of the attack.

Attackers can be categorized into two primary types: direct and indirect. A direct attack involves the attacker directly targeting a specific component, and this type of attack occurs exclusively between two attack prototypes, referred to as "atoms". Conversely, an indirect attack occurs when the attacker targets a component through an intermediate "springboard" component. In the case of an indirect attack, the attack can transition between multiple attack prototypes of atoms.

Once the attack sequence has been deduced through the reasoning process, it becomes possible to ascertain all attack routes from the initial attack state to the ultimate attack target. These routes collectively form the basis for constructing an attack graph. In this construction, the current network state serves as the initial node, while each step in the attack sequence contributes to creating edges within the graph. These edges are defined by the associated attack behaviour, attack success probability, and component loss value at each step.

3.3. Penetration test analysis based on attack graph. The penetration test diagram is a composite representation that incorporates the four fundamental components of the traditional penetration testing process into the attack diagram. These components include test items, test objectives, test constraints, and test cases. Within this diagram, test items, test objectives, and test constraints of the penetration test are depicted as vertices, while the test cases are depicted as connecting arcs. The process of testing based on this model is as follows:

Initially, within the real industrial control network, certain security safeguards are often implemented to safeguard potential attack routes. This precautionary measure may fail to attain the intended objectives when executing corresponding test cases. Consequently, the penetration test chart obtained after a successful test may diverge from the initial penetration test chart. Therefore, adjusting the penetration test chart before initiating the test becomes imperative, ensuring that it aligns with the testing objectives and requirements.

The second step involves a comprehensive analysis of the penetration test chart after the Conclusion of the penetration test. Initially, this analysis entails comparing the penetration test chart following the test and the vertex configuration before the test. This comparison yields the final results for the test project. Subsequently, a search is conducted based on these test results to identify the successful attack path. Finally, leveraging the weight values associated with each edge within the penetration test graph, the success probability of the attack, the resulting loss value, and the cumulative number of attack steps up to that point in the algorithm are determined. This information is then used to calculate the weight of an attack sequence, ultimately quantifying the network attack's impact on the network's security [5, 15].

3.4. Vulnerability risk assessment based on attack graph. To assess the risk associated with each vulnerability and prioritize the defence of the most difficult vulnerabilities and attack paths, a vulnerability's risk value is employed to gauge the harm it can cause. To ascertain the risk value of a vulnerability, the initial steps involve determining the vulnerability's overall probability of exploitation and the global degree of harm it can inflict. The following are the specific implementation steps for this process:

(a) Global Probability Assessment: Initially, calculate the global likelihood of the vulnerability being exploited across the entire system or network.

(b) Global Harm Assessment: Next, determine the extent of harm or damage the vulnerability can cause when exploited.

These following steps are essential in establishing the risk value attributed to each vulnerability, enabling a targeted strategy for prioritizing defence mechanisms.

(1) The breadth-first traversal algorithm is employed to compute the global utilization probability (denoted as 'P') of each node's successful utilization, calculated layer by layer starting from the initial node.

(2) Value is used to represent the value of each component, and $\emptyset$ is used to represent the independent harm degree of the vulnerability, so the loss caused by a single vulnerability to its component is $\emptyset x$ value; The letter Y represents the global hazard degree of a vulnerability, that is, the ratio of the associated hazard degree W of a single vulnerability to the sum of the value of all components in the industrial control network.

(3) 'R' signifies the risk value associated with vulnerability, calculated as the product of the global utilization probability of each node ('P') and the global hazard degree of the node ('Y') [14].

4. Result Analysis and Discussion. The "Zhennet" virus is employed as the attacker targeting the industrial control system in the experiment. The experimental process begins by establishing a network environment simulating the industrial control system. Subsequently, the attack graph is generated using the previously described method. Finally, the attack graph is the foundation for deriving the penetration test scheme and assessing vulnerability risks. The steps followed in the experimental process of the proposed method are as follows:

(1) Build network topology

It encompasses establishing an organized model for a computer or communication network. Network topology delineates the interconnections among devices and components within the network and elucidates the pathways through which data travels. It encompasses diverse configurations like star, bus, ring, mesh, and others, each with merits and drawbacks. Creating a network topology constitutes a pivotal phase in network design, facilitating streamlined data exchange and laying the groundwork for network administration and issue resolution.

(2) Generation algorithm parameter selection

Given that the "seismic network" attack gains entry into the industrial control network via a USB flash drive inserted into the operator station h_1, it designates the operator station h_1 as the initiating attack component. Table 4.1 illustrates the asset value assigned to each component within the industrial control network.

The impact coefficient of the vulnerability utilization mode is recorded as α_i, the disposable weight value of component assets is recorded as θ_i, and the component loss value is recorded as $Loss_i$, the loss value of each component after attack is shown in Table 4.2. The graphical analysis is shown in Figure 4.1.

(3) Generation of attack graph

According to the attack mentioned above graph generation method, the four paths that are most likely to attack and most harmful to the "Zhennet" virus are as follows:

① $h_1 \to h_1 \to h_3 \to h_2 \to h_5$ cumulative attack steps are 4, loss value is 12.2, and attack success probability is 0.096;

Table 4.1: Asset value table

Component No	Asset value	Component No	Asset value
h_1	2	h_4	1
h_2	3	h_5	3
h_3	4	h_6	5

Table 4.2: Calculation of loss value

Assembly	Vulnerability	$Value_i$	α_i	θ_i	$Loss_i$
h_1	vul_1	2	1	0.7	1.5
h_2	vul_2	4	1	1	4
h_3	vul_5	3	1	1	3
h_4	vul_6	1	1	1	1
h_5	vul_4	3	1.4	0.7	3.5
h_6	vul_4	5	2.4	0.7	10

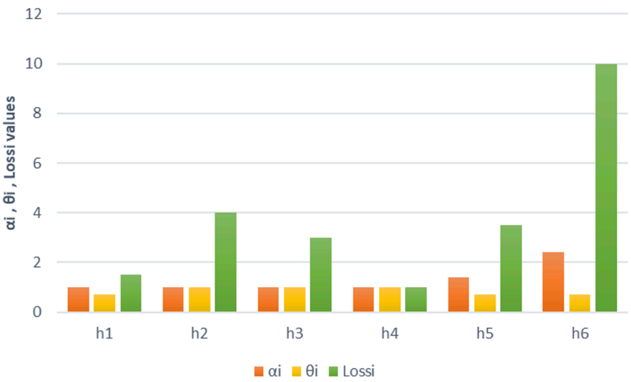

Fig. 4.1: Loss value analysis for various assembly

② $h_1 \rightarrow h_1 \rightarrow h_4 \rightarrow h_2 \rightarrow h_5$ cumulative attack steps are 4, loss value is 10.2, and attack success probability is 0.072;

③ $h_1 \rightarrow h_1 \rightarrow h_4 \rightarrow h_2 \rightarrow h_6$ cumulative attack steps are 4, loss value is 16.6, and attack success probability is 0.063;

④ $h_1 \rightarrow h_1 \rightarrow h_3 \rightarrow h_2 \rightarrow h_6$ cumulative attack steps are 4, loss value is 18.6, and attack success probability is 0.084.

(4) Penetration test based on attack graph

In penetration testing, parameters such as test objectives, test items, and test constraints are depicted as vertices, while test cases are represented as arcs within the penetration test diagram. These penetration test schemes are generated using the depth-first traversal method. Upon generating the penetration test chart, a comparison is made with the initial penetration test chart created at the outset of the test, and the results are found to be entirely consistent [6, 7].

(5) Vulnerability risk assessment based on attack graph

The risk value associated with each vulnerability is determined using a standard vulnerability scoring system and a vulnerability utilization diagram, as illustrated in Table 4.3 and Figure 4.2.

As shown in Table 4.3, the biggest vulnerability risk is vul_4, which is the DLL loading policy defect

Table 4.3: Specific risk value of each vulnerability

Vulnerability code	Component	Value quantity	Probability P	Overall hazard degree	Risk
vul_1	h_1	2	0.5	0.54	0.34
vul_2	h_2	4	0.7	0.74	0.6
vul_3	h_2	4	0.77	0.73	0.58
vul_4	h_5, h_6	8	0.90	0.8	0.82
vul_5	h_3	3	0.75	0.4	0.37
vul_6	h_4	1	0.4	0.4	0.2

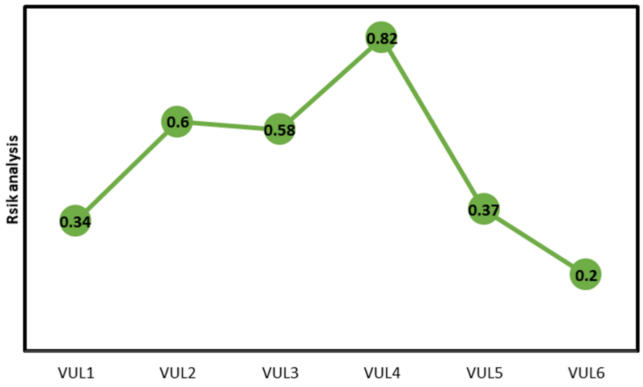

Fig. 4.2: Risk value of each vulnerability

in WINCC. It can be seen that the components installed with WINCC software are the most dangerous vulnerabilities to the system in the "seismic network" attack, which means that the attack path must be focused on defence [9]. The defence situation is the same, meaning the analysis results are correct. The penetration test analysis scheme is derived from the attack graph generated using the abovementioned method. The vulnerability risk values assessed through this penetration analysis scheme align with the actual scenario, demonstrating the feasibility and efficacy of the attack graph generation method.

5. Conclusion. The paper introduces a noteworthy approach to industrial control network security through an attack graph generation technology. The primary objective of this technology is to facilitate comprehensive security and vulnerability analyses within the industrial control network domain. The approach entails the development of a precise generation algorithm and explaining meticulous construction steps for the attack graph, which serves as a foundational tool for understanding network vulnerabilities and potential attack pathways. One key facet of this research is the empirical testing conducted using the "Zhennet" virus as the attacking agent. This practical application aims to validate the accuracy and effectiveness of the attack graph generation method proposed. The results obtained from these tests offer valuable insights into the practical utility of the approach. Notably, a degree of subjectivity is involved in calculating two critical parameters: the system loss value and the probability index of successful attacks. These calculations form pivotal components of the attack graph generation process, and their accuracy directly influences the reliability of the generated attack graph.

REFERENCES

[1] A. Algarni and V. Thayananthan, *Autonomous vehicles: The cybersecurity vulnerabilities and countermeasures for big data communication*, Symmetry, 14 (2022), p. 2494.

[2] O. Briones, R. Alarcón, A. J. Rojas, and D. Sbarbaro, *Tuning generalized predictive pi controllers for process control applications*, ISA Transactions, 119 (2022), pp. 184–195.

[3] B. Fan, C.-X. Zheng, L.-R. Tang, and R.-Z. Wu, *Critical nodes identification for vulnerability analysis of power communication networks*, IET Communications, 14 (2020), pp. 703–713.

[4] Y. Feng, G. Sun, Z. Liu, C. Wu, X. Zhu, Z. Wang, and B. Wang, *Attack graph generation and visualization for industrial control network*, in Proceedings of the 39th Chinese Control Conference, Shenyang, China, 2020, IEEE, pp. 7655–7660.

[5] T. Gu, K. Liu, B. Dolan-Gavitt, and S. Garg, *Badnets: Evaluating backdooring attacks on deep neural networks*, IEEE Access, 7 (2019), pp. 47230–47244.

[6] I. Kotenko and M. Stepashkin, *Attack graph based evaluation of network security*, in Proceedings of the 10th IFIP TC-6 TC-11 International Conference, Heraklion, Crete, Greece, 2006, Springer, pp. 216–227.

[7] J. Luan, J. Wang, and M. Xue, *Automated vulnerability modeling and verification for penetration testing using petri nets*, in Proceedings of the Cloud Computing and Security: Second International Conference, Nanjing, China, 2016, Springer, pp. 71–82.

[8] S. Mubarak, M. H. Habaebi, M. R. Islam, A. Balla, M. Tahir, A. Elsheikh, and F. Suliman, *Industrial datasets with ics testbed and attack detection using machine learning techniques*, Intelligent Automation & Soft Computing, 31 (2022), pp. 1345–1360.

[9] E. Normanyo, F. Husinu, and O. R. Agyare, *Developing a human machine interface (hmi) for industrial automated systems using siemens simatic wincc flexible advanced software*, Journal of Emerging Trends in Computing and Information Sciences, 5 (2014), pp. 134–144.

[10] O. E. Oluyisola, S. Bhalla, F. Sgarbossa, and J. O. Strandhagen, *Designing and developing smart production planning and control systems in the industry 4.0 era: a methodology and case study*, Journal of Intelligent Manufacturing, 33 (2022), pp. 311–332.

[11] V. D. Savin, *Cybersecurity threats and vulnerabilities in energy transition to smart electricity grids*, in Navigating Through the Crisis: Business, Technological and Ethical Considerations: The 2020 Annual Griffiths School of Management and IT Conference (GSMAC) Vol 2 11, Springer, 2022, pp. 71–83.

[12] M. T. Siponen and H. Oinas-Kukkonen, *A review of information security issues and respective research contributions*, ACM SIGMIS Database: the DATABASE for Advances in Information Systems, 38 (2007), pp. 60–80.

[13] Y. Su, M. Zhao, C. Wei, and X. Chen, *Pt-todim method for probabilistic linguistic magdm and application to industrial control system security supplier selection*, International Journal of Fuzzy Systems, 24 (2022), pp. 1–14.

[14] R. Vishwakarma and A. K. Jain, *A survey of ddos attacking techniques and defence mechanisms in the iot network*, Telecommunication Systems, 73 (2020), pp. 3–25.

[15] B. Wang, Y. Yao, S. Shan, H. Li, B. Viswanath, H. Zheng, and B. Y. Zhao, *Neural cleanse: Identifying and mitigating backdoor attacks in neural networks*, in Proceedings of the IEEE Symposium on Security and Privacy, San Francisco, CA, USA, 2019, IEEE, pp. 707–723.

[16] S. Wang and Y. Gong, *Adversarial example detection based on saliency map features*, Applied Intelligence, (2022), pp. 1–14.

[17] W. Xia, R. Neware, S. D. Kumar, D. A. Karras, and A. Rizwan, *An optimization technique for intrusion detection of industrial control network vulnerabilities based on bp neural network*, International Journal of System Assurance Engineering and Management, 13 (2022), pp. 576–582.

[18] J.-P. A. Yaacoub, H. N. Noura, O. Salman, and A. Chehab, *Robotics cyber security: Vulnerabilities, attacks, countermeasures, and recommendations*, International Journal of Information Security, (2022), pp. 1–44.

[19] P. Zeng, G. Lin, L. Pan, Y. Tai, and J. Zhang, *Software vulnerability analysis and discovery using deep learning techniques: A survey*, IEEE Access, 8 (2020), pp. 197158–197172.

Edited by: Venkatesan C
Special issue on: Next Generation Pervasive Reconfigurable Computing for High Performance Real Time Applications
Received: May 4, 2023
Accepted: Sep 28, 2023