Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Special Issue 4, April : 2024

CYBER SUPPLY CHAIN THREAT ANALYSIS AND PREDICTION USING MACHINE LEARNING

[1]Anumalla Charan Raj, [2]Eravathni Karthik, [3]K.Amruta Vani, [4]Siddoju Abhinav Thrivarna,[5]P.Doopi Srilakshmi

[1,2,3,4] UG Scholar, Department of CSE (AI&ML)

[5]Assistant Professor, Department of CSE (AI&ML)

CMR Institute of Technology, Hyderabad, Telangana, India-501401

ABSTARCT: Cyber Supply Chain (CSC) security requires a secure integrated network among the sub-systems of the inbound and outbound chains. Adversaries are deploying various penetration and manipulation attacks on an CSC integrated network's node. The different levels of integrations and inherent system complexities pose potential vulnerabilities and attacks that may cascade to other parts of the supply chain system. Thus, it has become imperative to implement systematic threats analyses and predication within the CSC domain to improve the overall security posture. This paper presents a unique approach that advances the current state of the art on CSC threat analysis and prediction by combining work from three areas: Cyber Threat Intelligence (CTI), Ontologies, and Machine Learning (ML). The outcome of our work shows that the conceptualization of cybersecurity using ontological theory provides clear mechanisms for understanding the correlation between the CSC security domain and enables the mapping of the ML prediction with 80% accuracy of potential cyberattacks and possible countermeasures

INTRODUCTION Cyber Supply Chain (CSC) security nowadays is more challenging due to the inherent system complexity and vulnerabilities among various system components and their cascading effect. Cybersecurity risks in CSC have increased exponentially leading to major security breaches in most organizations [1, 2]. The recent high profile cyberattacks such as Ukraine 2015 and Saudi Aramco 2017 smart grid attacks have brought diverse challenges, different threat landscape and unexpected challenges with unpredictable consequences [3]. Therefore, it has become imperative to have a comprehensive understanding of the CSC

threat landscape. However, threat analysis in CSC is challenging due to a lack of understanding of the evolving threat landscape which often hinders the ability of organizations to analyze and effectively predict threats [1, 2]. This paper presents a novel threat analysis and prediction approach that uniquely combines work from Cyber Threat Intelligence (CTI), Ontology, and Machine Learning. In particular, this paper provides three main contributions. Firstly, we analyze CSC threats using CTI and ontological theory. Ontologies provide semantic mapping and explicit knowledge necessary for threat analysis. Secondly, we present a systematic process to analyse and predicate cyber threats. The process includes activities related to cyber threat intelligence and machine learning techniques such as Random Forest (RF) and GBoost algorithms for threat analysis and prediction. ML is considered for mapping the relationships between cyberattack, cyber threat propagations and their cascading impact on the various supplier chain nodes. Thirdly, we integrate knowledge from datasets from the Microsoft Malware Prediction to support threat prediction [5]. The results show that the ontological approach provides mechanisms for understanding the correlation between the CSC security domain. Both RF and GBoost algorithms provide accuracy around 80%.

RELATED WORK

Cyber supply chain (CSC) security provides secure integrated networks for various organizations. CSC attacks have increased exponentially, and its cascading impact is unquantifiable, causing collateral damage to organizations. Threat actors are using sophisticated attacks including advanced persistent threats (ATP) and command and control (C&C) methods to penetrate, manipulate and obfuscate in the supply inbound and outbound chains [8, 9]. Cyber Threat Intelligence (CTI) provides technical indicators, context, and actionable advice relating to existing and emerging threat [9]. Pokorny 2018 proposed a CTI lifecycle approach required to identify intelligence goals [10]. Friedman & Buchanan, proposed a CTI approach based on organizational requirements, gathering information, analysis and dissemination to protect assets and documents [11]. Miller proposed a cyber supplier chain framework and attack pattern that provides a comprehensive view of supply chain attacks of malicious insertions across a full question life cycle

[12]. The protection of the CSC is critical as it incorporates various embedded networks, software and computational algorithms for information flows and data structures in the live and mission-critical systemSecurity ontology from the CSC perspective describes organizational security concepts, properties relationships and their interdependencies in a formal and structured manner [14]. The goal of security ontology is to extract relevant attack instances and information from data to ensure consistency and accuracy in the CSC security concepts and for knowledge reuse in the threat intelligence domain. Mozzaquatro et al proposed a model driven ontology-based cybersecurity framework for the internet of things that considers design time and run time concepts for knowledge reasoning [4]. Gao et al., proposed an ontology-based model of network and computer attacks for security assessment and standards classifications that establishes relationships among network security services, threats, vulnerabilities and causes of failures [15]. Gyrard et al. proposed an ontology for attacks and countermeasures for capturing and presenting concepts of security requirements [16]. Machine Learning (ML) in cybersecurity uses various algorithms to learn and train datasets to determine their classifications and for threat predictions. ML algorithm is initially trained to allow the system to learn the data [17]. The purpose of using ML is to get the system to use past events to make an informed decision that can be used to predict future attacks

EXISTING SYSTEM

The CSC security provides a secure integrated platform for the inbound and outbound supply chains systems with third party service provider including suppliers, and distributors to achieve the organizational goal [10]. Cybersecurity from supply chain context involves various secure outsourcing of products and information between third party vendors, and suppliers [11]. This outsourcing includes the integration of operational technologies (OT) and Information technologies (IT) running on Cyber Physical Systems (CPS) infrastructures. However, there are threats, risks and vulnerabilities that are inherent in such systems that could be exploited by threat actors on the operational technologies and information technologies of the supply inbound and outbound chains systems. The outbound chain attacks include data manipulations, information tampering,

redirecting product delivery channels, and data theft. The IT risks include those attacks on the cyber physical and cyber digital system components such as distributed denial of service (DDoS) attacks, IP address spoofing, and Software errors [12]. Regarding CSC security, NIST SP800 [13] proposed a 4 tier framework approach for improving critical infrastructure cybersecurity that incorporates the cyber supply chain risk management framework into it as one of its core components. Tier 1 considers the organizations CSC risk requirement strategy. Tier 2 considers the supply chain associated risk identifications including products and services in the supply inbound and outbound chains. Tier 3 implementation considers the risk assessments, threats analyses, associated impacts and determine the baseline requirements for governance structure. Tier 4 consider realtime or near-time information to understand supply chain risk associated with each product and service. However, the approach and tiers considered risks management but did not emphasize on ML and threat prediction for future trends in the CSC domain. Additionally, [14] proposed a supply chain attack framework and attack patterns that structured and codifies supply chain attacks. The goal of the framework was to provide a comprehensive view of supply chain attacks of malicious insertion across the full acquisition lifecycle to determine the associated threat and vulnerability information.

DISADVANTAGES

- Existing works that consider CSC threats and risks but a lack of focus on threat intelligence properties for the overall cyber security improvement. Further, it I also essential to predict the cyberattack trends so that the organization can take the timely decision for it countermeasure.
- There is no technique called Inbound and Outbound Supply Chain to detect cyber threat.

PROPOSED SYSTEM

The proposed system aims to improve the cybersecurity of CSC by specifically focusing on integrating Cyber Threat Intelligence (CTI) and Machine Learning (ML) techniques to predicate cyberattack patterns on CSC systems and recommend suitable controls to tackle the attacks. The novelty of our work is threefold:

- Firstly, we consider Cyber Threat Intelligence(CTI) for systematic gathering and analysis of information about the threat actor and cyber-attack by using various concepts such as threat actor skill, motivation, IoC, TTP and incidents. The reason for considering CTI is that it provides evidence-based knowledge relating to the known attacks. This information is further used to discover unknown attacks so that threats can be well understood and mitigated. CTI provides intelligence information with the aim of preventing attacks as well as shorten time to discover new attacks.
- Secondly, we applied ML techniques and classification algorithms and mapped with the CTI propreteis to predict the attacks. We use several classification algorithms such as Logistic Regression (LG), Support Vector Machine (SVM), Random Forest (RF) and Decision Tree (DT) for this purpose. We follow CTI properties such as Indicator of Compromise (IoC) and Tactics, Techniques and Procedure (TTP) for the attack predication.
- Finally, we consider widely used cyberattack dataset to predict the potential attacks [6]. The predication focuses on determining threats relating to Advance Persistent Threat (APT), command and control and industrial espionage which are relevant for CSC [7] [8] [9]. The result shows the integration of CTI and ML techniques can effectively be used to predict cyberattacks and identification of CSC systems vulnerabilities. Furthermore, our prediction reveals a total accuracy of 85% for the TPR and FPR. The results also indicate that LG and SVM produced the highest accuracy in terms of threat predication.

ADVANTAGES

- The system is more effective due to INTEGRATION OF CTI AND ML FOR THRAT ANALYSIS AND PREDICATION PROCESS
- The gives accurate results due to presence of Evaluating the Accuracy of the Threats.

MODULES

Service Provider

In this module, the Service Provider has to login by using valid user name and password. After login successful he can do some operations such asBrowse Cyber Security Data Sets and Train &Test, View Trained and Tested Accuracy in Bar Chart, View Trained and Tested Accuracy Results, View Prediction Of Cyber Threat Type, View Cyber Threat Type Ratio, Download Cyber Threat Predicted Data Sets, View Cyber Threat Type Ratio Results, View All Remote Users.

View and Authorize Users

In this module, the admin can view the list of users who all registered. In this, the admin can view the user's details such as, user name, email, address and admin authorizes the users.

Remote User

In this module, there are n numbers of users are present. User should register before doing any operations. Once user registers, their details will be stored to the database. After registration successful, he has to login by using authorized user name and password. Once Login is successful user will do some operations like REGISTER AND LOGIN, PREDICT CYBER THREAT TYPE, VIEW YOUR PROFILE

CONCLUSION

The integration of complex cyber physical infrastructures and applications in a CSC environment have brought economic, business, and societal impact for both national and global context in the areas of Transport, Energy, Healthcare, Manufacturing, and Communication. However, CPS security remains a challenge as vulnerability from any part of the system can pose risk within the overall supply chain context. This paper aims to improve CSC security by integrating CTI and ML for the threat analysis and predication. We considered the necessary concepts from CSC and CTI and a systematic process to analyse and predicate the threat. The experimental results showed that accuracies of the LG, DT, SVM, RF algorithms in Majority Voting and identified a list of predicated threats. We also observed that CTI is effective to extract threat information , which can integrate into the ML classifiers for the threat predication. This allows CSC organization to analyse the existing controls and determine additional controls for the improvement of overall cyber security. It is necessary to consider the full automation of the process and industrial case study to generalize our findings. Furthermore, we are

also planning to consider evaluating the existing controls and the necessary of future controls based on our prediction results.

REFERENCES

[1] National Cyber Security Centre. " Example of Supply Chain Attacks." NCSC. 2018. [Online] Available: https://www.ncsc.gov.uk/collection/supply-chain-security/supply-chain-attack-examples.

[2] A. Yeboah-Ofori, and S. Islam, "Cyber Security Threat Modelling for Supply Chain Organizational Environments." MDPI. Future Internet. 11, (3), 63, March 2019. doi: 10.3390/611030063.

[3] B. Woods, and A. Bochman, "Supply Chain in the Software Era" Scowcroft Center for Strategic and Security. Atlantic Council: Washington, DC, USA, May 2018.

[4] ENISA "Exploring the Opportunities and Limitations of Current Threat Intelligence Platforms" Version 1. December 2017. [online]

[5] C. Doerr, "Cyber Threat Intelligences Standards – A High Level Overview" TU Delft CTI Labs, 2018. [Online]. Available: https://www.enisa.europa.eu/events/2018-cti-eu-event/cti-eu-2018-presentations/cyber-threat-intelligence-standardization.pdf.

[6] Microsoft Malware Prediction, Research Prediction. 2019. [Online] Available: https://www.kaggle.com/c/microsoft-malware-prediction/data.

[7] A. Yeboah-Ofori, J. D. Abduli, F. Katsriku, "Cybercrime and Risks for Cyber Physical Systems" International Journal of Cyber Security and Digital Forensics. Vol.8 No1, pp 43-57. 2019.

[8] CAPEC-437, Supply Chain. Common Attack Pattern Enumeration and Classification: Domain of Attack. October 2018. [Online] Available: https://capec.mitre.org/data/definitions/437.html.

[9] Open Web Application Security Project (OWASP). The Ten Most Critical Application Security Risks. Creative Commons Attribution-Share Alike 4.0 International License. 2017. [Online] Available: https://owasp.org/www-pdf-archive/OWASP_Top_10-2017_%28en%29.pdf.pdf.

[10] US-Cert. "Building Security in Software & Supply Chain Assurance." 2020. [Online] Available: https://www.us-cert.gov/bsi/articles/knowledge/attack-patterns.

[1] National Cyber Security Centre. " Example of Supply Chain Attacks." NCSC. 2018. [Online] Available: https://www.ncsc.gov.uk/collection/supply-chain-security/supply-chain-attack-examples.

[2] A. Yeboah-Ofori, and S. Islam, "Cyber Security Threat Modelling for Supply Chain Organizational Environments." MDPI. Future Internet. 11, (3), 63, March 2019. doi: 10.3390/611030063.

[3] B. Woods, and A. Bochman, "Supply Chain in the Software Era" Scowcroft Center for Strategic and Security. Atlantic Council: Washington, DC, USA, May 2018.

[4] ENISA "Exploring the Opportunities and Limitations of Current Threat Intelligence Platforms" Version 1. December 2017. [online]

[5] C. Doerr, "Cyber Threat Intelligences Standards – A High Level Overview" TU Delft CTI Labs, 2018. [Online]. Available: https://www.enisa.europa.eu/events/2018-cti-eu-event/cti-eu-2018-presentations/cyber-threat-intelligence-standardization.pdf.

[6] Microsoft Malware Prediction, Research Prediction. 2019. [Online] Available: https://www.kaggle.com/c/microsoft-malware-prediction/data.

[7] A. Yeboah-Ofori, J. D. Abduli, F. Katsriku, "Cybercrime and Risks for Cyber Physical Systems" International Journal of Cyber Security and Digital Forensics. Vol.8 No1, pp 43-57. 2019.

[8] CAPEC-437, Supply Chain. Common Attack Pattern Enumeration and Classification: Domain of Attack. October 2018. [Online] Available: https://capec.mitre.org/data/definitions/437.html.

[9] Open Web Application Security Project (OWASP). The Ten Most Critical Application Security Risks. Creative Commons Attribution-Share Alike 4.0 International License. 2017. [Online] Available: https://owasp.org/www-pdf-archive/OWASP_Top_10-2017_%28en%29.pdf.pdf.

[10] US-Cert. "Building Security in Software & Supply Chain Assurance." 2020. [Online] Available: https://www.us-cert.gov/bsi/articles/knowledge/attack-patterns.

[11] S.Dhanalakshmi, T.Ravichandran, "Image Segmentation Using Thresholding and Genetic Algorithms", in International Journal of Advanced Innovative Research (IJAIR), Volume 1, Issue 3, ISSN: 2278-7844, August 2012,

PP 240-244

[12] S.Dhanalakshmi,, T.Ravichandran, "A Modified Approach for Image Segmentation in Information Bottleneck Method", in International Journal by Advanced Research in Computer Engineering and Technology (IJARCET), Volume 1, Issue 7, ISSN: 2278 – 1323, September 2012, PP 59-63

[13] S.Dhanalakshmi,, T.Ravichandran, "A New Method for Image Segmentation", in International Journal of Advanced Research in computer science and software engineering (IJARCSSE), Volume 2, Issue 9, ISSN: 2277 128X, September 2012, PP 293-299

S.Dhanalakshmi,, T.Ravichandran, "A Survey of Different Image Segmentation Process Using Genetic Algorithm Approach", in International Journal of Engineering Associates (IJEA), Volume 1, Issue 2, and ISSN: 2320-0804, December 2012, PP 12-18

1.Kumbala Pradeep Reddy; Sarangam Kodati; Thotakura Veeranna; G. Ravi, "6 Machine Learning-Based Intelligent Video Analytics Design Using Depth Intra Coding," in Big Data Management in Sensing: Applications in AI and IoT , River Publishers, 2021, pp.77-86.

2. G. Ravi; Kumbala Pradeep Reddy; M. Mohan Rao; Sarangam Kodati; J. Praveen Kumar, "10 Design a Novel IoT-Based Agriculture Automation Using Machine Learning," in Big Data Management in Sensing: Applications in AI and IoT , River Publishers, 2021, pp.149-158.

3.Reddy, Kumbala Pradeep, Sarangam Kodati, Madireddy Swetha, M. Parimala, and S. Velliangiri. "A hybrid neural network architecture for early detection of DDOS attacks using deep learning models." In *2021 2nd International Conference on Smart Electronics and Communication (ICOSEC)*, pp. 323-327. IEEE, 2021.