International Journal of Latest Research in Engineering and Technology (IJLRET)
ISSN: 2454-5031
www.ijlret.com || Volume 09 - Issue 04 || April 2023 || PP. 01-05

Kill chain model based Advanced Persistent Threat in Power System

Xiao Ziyang[1], Wang Xingjian[2], Qiu Rixuan[1], Li Dingding[3], Li Shuai[3]
[1](*Information and Communication Branch of State Grid Jiangxi Electric Power Co., Ltd., China)*
[2](*Nanjing University of Posts and Telecommunications, China)*
[3](*Information and Communication Branch of State Grid Henan Electric Power Co., Ltd. (Data Center), China)*

Abstract: Based on the ATT&CK knowledge base, a kill chain model for APT attacks on power systems is established. Traditional methods have difficulty in dividing APT attack techniques into kill chain attack stages, which makes it difficult for security personnel to make defense decisions quickly. To address this issue, a method based on the kill chain model is proposed for dividing APT attack techniques into their respective stages. The method uses the Bert model for semantic analysis of technical texts to automatically classify attack techniques into their respective stages. Experimental results show that this method achieves better performance than existing models.

Keywords: power system; advanced persistent threat; ATT&CK; attack modeling; Bert; natural language processing; text classification

I. INTRODUCTION

Modern power systems are more dynamic and complex than traditional ones, and they have more security vulnerabilities as well. They are also critical national infrastructure that APT attacks often target. Thus, it is urgent to model APT attacks on new power systems.

This paper proposes an APT attack kill chain model based on the ATT&CK knowledge base and a method to classify APT attack techniques into stages using this model. The main contributions are:

(1) We use the ATT&CK framework to model APT attacks and apply a network kill chain model to analyze the APT attack process and proactively identify the cyber security situation.

(2) We use the Bert model to train the attack technique text and automatically assign it to the corresponding attack chain stage, because ATT&CK organizes techniques by strategy rather than by attack stages, which is not suitable for responding to real-world network attacks [13-20].

II. RESEARCH BACKGROUND

Modern power systems with new energy as the main body are the new development direction of the power industry[1-5]. Modern power systems will reduce traditional energy sources and integrate more new energy sources into the grid, which means that the future power system will have a more diversified energy structure, more complex power allocation and storage, and a large number of digital and intelligent devices will be used in modern power systems. Due to the introduction of more new digital technologies, modern power systems are more complex and have more vulnerabilities in each link. The proportion of new energy sources and diversified load forms has increased significantly.

Large enterprises, sovereign states or their controlled organizations often launch Advanced Persistent Threats (APT) for political or economic interests, targeting a specific organization or institution[6-12]. APT attacks have long activity cycles, high steal thiness and high destructiveness, as they aim to penetrate the whole system rather than achieve short-term gains. Many victims of APT attacks remain unaware of them even after they happen. APT attacks mostly target transnational enterprises, international organizations or government departments. Power and energy facilities are one of the key targets of APT attacks, as they are important national infrastructure that is crucial for military and civil affairs.

III. APT ATTACK MODEL

ATT&CK proposes 14 tactics for describing the process of a cyber attack, each containing dozens of techniques and sub-techniques. However, these tactics and techniques can be overwhelming and hard to understand for analyzing specific attacks due to the large amount of textual data. Moreover, ATT&CK organizes APT attack techniques by strategy rather than by attack stages, which can complicate the analysis of the attack process. The network kill chain model simplifies APT attacks into stages, making it easier to extract, analyze, identify, and perceive potential risks and take timely measures to block the attack chain and prevent the attack. Therefore, this paper proposes an APT attack model based on ATT&CK by analyzing multiple APT attack organizations and their attack processes and selecting, summarizing, and merging attack strategies. Furthermore,

this paper presents a BERT-based algorithm to classify APT attack techniques into the various stages of the kill chain model, as traditional machine learning algorithms struggle to obtain the semantic information contained within the natural language text of APT attacks.

Traditional network attack models, such as tree and graph models, are insufficient for dealing with increasingly complex attacks. The network attack chain model offers a detailed account of the attack lifecycle, and can be used for intrusion detection and analysis. APT attacks often progress through different stages of the kill chain model, and employing defensive measures at each stage can help stop the entire attack. This article introduces an APT attack chain model that comprises of eight stages:

Reconnaissance Stage:

At this stage, attackers scrutinize the target, collect information about the target, evaluate the target's defense mechanisms, and assess the target's attack value. They use technical means, such as eavesdropping, to gather intelligence and decide on the attack method to be used.

Tool Preparation Stage:

Attackers design and create Trojan viruses and malicious code based on the selected attack method and victim characteristics. They insert malicious programs into the system through 0day vulnerabilities, spear-phishing, or mobile storage devices. This stage also encompasses other preparations for the attack, such as setting up servers, registering attack accounts, purchasing domains, stealing code development certificates, and purchasing web services.

Payload Delivery Stage:

Attackers try to insert the malicious code created in the previous stage into the system. APT attacks frequently use email as an attack carrier and use techniques such as watering hole attacks and spear-phishing to trick victims into clicking on phishing emails to obtain user account passwords and other information, thus proceeding to the next stage of the attack.

Exploitation Stage:

After gaining adequate system operating privileges, attackers run their controlled malicious code along with other attack strategies to gain access to user accounts and passwords, understand system details, steal or manipulate required data, control the system, disrupt the system's normal operation, and communicate with other nodes based on this device or node to spread the attack.

Installation Implantation Stage:

To gain further access to and control over the system, attackers establish a foothold for the attack by installing backdoor programs and other control software in the system, replacing or hijacking legitimate code, or adding startup code. Afterwards, to further explore the network, attackers may use system configuration errors or vulnerabilities or use forged tokens to modify the registry, thereby elevating their own attack privileges.

Exploration and Collection Stage:

To expand the attack further, attackers observe the network and system, potentially stealing account names and passwords, using these legitimate credentials to access the system, and creating more accounts to assist in achieving their goal. After that, attackers explore the environment around their attack points and the units they can manipulate. Finally, by understanding the environment, they penetrate the environment, spread the attack across various systems and accounts, or steal data.

Command and Control Stage:

Attackers try to communicate with infected systems and use communication between network protocols to establish different levels of stealthy command and control based on the victim's network structure and defense, thereby controlling the target system's operation.

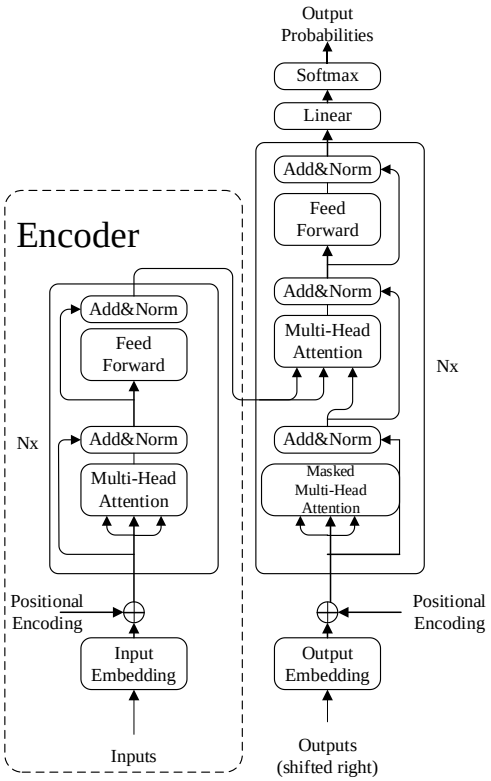
Objectives Achieved Stage:

Attackers launch attacks based on their targets, usually bundling stolen data. The technology used to obtain data from the target network usually transmits data through their command and control channel or backup channel, and may also include size restrictions on the transmission to extract data from the system. The goal of the destructive attack is to stop and interfere with the normal operation of the system, often using deletion or tampering of critical files, modifying user permissions, or interrupting network traffic.

IV. METHOD OF APT ATTACK TECHNIQUE STAGE DIVISION BASED ON BERT

We proposes a workflow for dividing the APT attack technique stages based on the process described in the previous section. Given an attack technique text, we first use Bert to convert it into word vector representation using pre-trained word vectors from a large-scale training dataset. We then feed the word vector representation to the encoder, where xi denotes the i-th word vector in the sentence. The encoder layer consists of two sub-layers: a multi-head self-attention mechanism layer and a fully connected feed-forward network layer. The attention layer computes the weight coefficients and generates attention values by weighting and summing the value elements. The Add & Norm layer performs residual connection and layer normalization, followed by the feed-forward layer that applies two linear transformations and ReLU activation function, and finally another Add & Norm layer. Before training the model, we initialize the required parameters. We vectorize the text through the embedding layer first. Then, we use the multi-head attention layer to analyze the similarity between the elements and calculate their weight coefficients. We obtain their corresponding output through a fully connected layer, calculate its loss value, and update its model parameters backwards for further training. The model returns its final result as an APT attack technique classified into one of kill chain stages.

Figure 1 Transformer



V. EXPERIMENT

This paper uses the MITRE ATT&CK knowledge base as its dataset. This knowledge base covers network attack activities from both tactical and technical perspectives and organizes the actors and incidents involved in network attacks. It provides a common framework to describe the different phases of the attack lifecycle and gives detailed information about the attack methods and the malicious code/software employed. Due to its open source nature and frequent updates, this knowledge base has been widely adopted in the field of APT attacks.

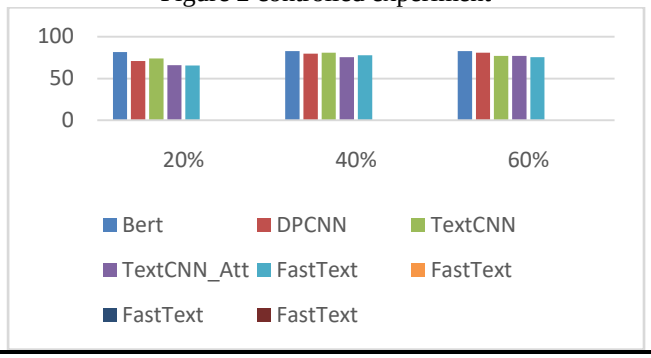
To validate the feasibility of the proposed attack technique phase division method in this paper, we compared it with other relevant research in the field of network security, as shown in Figure 2.

As can be seen from the figure, the method proposed in this paper outperforms the comparative models in all indicators. Text CNN and DPCNN models achieve good results in feature extraction by using convolutional neural networks when dealing with large datasets. However, RNNs tend to suffer from gradient vanishing when dealing with longer text data, making it difficult to capture information that is far apart in the text, resulting in poor accuracy, only 57.73%. Text RNN_Att, on the other hand, improves RNN by using BiLSTM to train the data from both forward and backward directions, capturing the semantic dependencies

between words and effectively solving the aforementioned problem. The addition of an attention mechanism also improves the model's effectiveness.

Although the Fast text model uses a shallow network and has poorer training accuracy, it takes much less time than deep networks. Bert, on the other hand, greatly improves the understanding of contextual information and semantic relationships between words by using pre-trained word vectors. By training with a bidirectional transformer network structure, the results show that Bert's method outperforms other methods by 4-6% in all indicators.

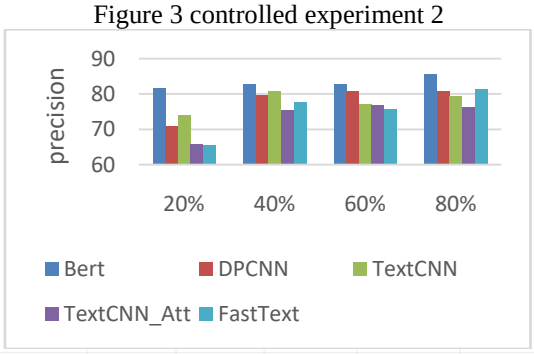
Figure 2 controlled experiment



	Bert	transformer	Text CNN	Text RCNN	Fast Text	DPCNN	Text RNN	Text RNN_Att
P	85.72	80.06	78.99	80.72	78.81	82.32	57.26	81.03
R	86.29	80.68	81.02	79.09	80.04	80.87	63.55	80.22
F1	85.89	79.81	80.26	78.94	77.29	81.16	57.92	79.74

To evaluate the algorithm's performance, we conduct experiments on the sample dataset by varying the proportions of the training set, validation set, and test set while keeping other parameters fixed. This allows us to observe how the model behaves under small or insufficient sample conditions. We use different percentages of data as the training set and split the remaining half equally into the validation set and test set. We use precision as the metric and report the results in Figure 3：

Figure 3 controlled experiment 2



precision	Bert	DPCNN	TextCNN	TextCNN_Att	FastText
20%	81.67	70.85	74.01	65.83	65.49
40%	82.76	79.68	80.87	75.42	77.69
60%	82.92	80.79	77.13	76.84	75.55
80%	85.68	80.95	79.33	76.34	81.45

Figure 3 shows that the precision of each model drops to different extents when the training data is relatively scarce. However, the Bert model, which leverages a pre-trained model that has been trained on a large amount of data for various tasks, significantly enhances its text comprehension ability. This enables it to effectively capture the contextual semantic information and the relationships between sentences. Therefore, it still performs well even with insufficient training data.

VI. CONCLUSION

This paper introduces a kill chain model for APT attacks on power systems and proposes a BERT-based attack technique matching algorithm. This algorithm can effectively capture the dependency relationship

between contextual semantic information and technical texts, and thus automatically assign the technical texts in the ATT&CK knowledge base to the corresponding stages of the kill chain model. Experimental results demonstrate that the proposed algorithm outperforms other related algorithms in the field of network security and enhances the effectiveness of mapping APT attack techniques to the kill chain. We use the MITRE knowledge base dataset to validate our approach.

VII. ACKNOWLEDGEMENTS

This work was supported by the State Grid Jiangxi Electric Power Corporation Science and Technology Project "Research on Active Defense Technology for Advanced Sustainable Network Attacks Based on Dynamic Obfuscation" under Grant 521835220003.

REFERENCES

[1]. HAN Xueyuan,et al: Runtime Provenance-Based Detector for Advanced Persistent Threats [EB/OL]. https://doi.org/10.48550/arXiv.2001.01525,2020-01-06/2022-08-20.
[2]. KARANTZAS G, PATSAKIS C. An Empirical Assessment of Endpoint Detection and Response Systems against Advanced Persistent Threats Widely Used Attack Vectors [J]. Cybersecur. Priv. 2021, 1: 387–421.
[3]. LIU J, et al. A New Realistic Benchmark for Advanced Persistent Threats in Network Traffic [J]. IEEE Networking Letters, 2022: 1-1.
[4]. HOFER-SCHMITZ K, KLEB U, STO-JANOVIC B. The Influences of Feature Sets on the Detection of Advanced Persistent Threats [J]. Electronics, 2021, 10:704.
[5]. SIDAHMED B, GHITA B, JAMES C, PETKO V. A Rule Mining-Based Advanced Persistent Threats Detection System [EB/OL]. https://doi.org/10.48550/arXiv.2105.10053,2021-05-20/2022/07/28.
[6]. DONG Jun, et al. Key Issues and Technical Applications in the Study of Power Markets as the System Adapts to the New Power System in China [J]. Sustainability, 2021, 13(23):13409.
[7]. MENG Zijie, et al. Study on the Influence of Extreme Weather on Power Grid Operation under New Power System[C]. 2021 4th International Conference on Algorithms, Computing and Artificial Intelligence, 2021:1-6.
[8]. YOON K. Convolutional Neural Networks for Sentence Classification [EB/OL]. https://arxiv.org/abs/1408.5882,2020-08/2022-08.
[9]. LIU Pengfei, QIU Xipeng, HUANG Xuanjing. Recurrent Neural Network for Text Classification with Multi-Task Learning[EB/OL].https://doi.org/10.48550/arXiv.1605.05101,2016-05-17/2022-08-21.
[10]. MILAJERDI S M, GJOMEMO R, ESHETE B, et al. HOLMES: Real-Time APT Detection through Correlation of Suspicious Information Flows[C]. 2019 IEEE Symposium on Security and Privacy, 2019:1137-1152.
[11]. TOUNSI W, RAIS H. A Survey on Technical Threat Intelligence in the Age of Sophisticated Cyber Attacks [J]. Computers & Security, 2018, 72: 212-233.
[12]. DAISUKE M. MITRE ATT&CK Based Evaluation on In-Network Deception Technology for Modernized Electrical Substation Systems [J]. Sustainability, 14(3):1256
[13]. XIONG Wenjun, et al. Cyber security threat modeling based on the MITRE Enterprise ATT&CK Matrix [J]. Software and Systems Modeling, 2021, 21:157-177.
[14]. KIM Kyoungmin, et al. Automatically Attributing Mobile Threat Actors by Vectorized ATT&CK Matrix and Paired Indicator [J]. Sensors, 2021, 21(19):6522.
[15]. GEORGIADOU A, MOUZAKITIS S, ASKOUNIS D. Assessing MITRE ATT&CK Risk Using a Cyber-Security Culture Framework[J]. Sensors, 2021, 21(9):3267.
[16]. SANS INSTITUTE. SANS Institute Provides Guidance on Improving Cyber Defense Using the MITRE ATT&CK Framework [J]. Computers, Networks & Communications, 2020.
[17]. BENÍTEZANDRADES J A, et al. Traditional Machine Learning Models and Bidirectional Encoder Representations From Transformer (BERT)-Based Automatic Classification of Tweets About Eating Disorders: Algorithm Development and Validation Study [J]. JMIR medical Informatics, 2022, 10(2):e34492.
[18]. LI Jing, ZHANG Dezheng, WULAMU Aziguli. Chinese Text Classification Based on ERNIE-RNN [J]. JMIR Medical Informatics, 2022, 10(2):e34492.
[19]. LIU Shuaiqi, et al. Key phrase aware transformer for abstractive summarization [J]. Information Processing and Management, 2022, 59(3):102913.
[20]. LI Hongwei, MAO Hongyan, WANG Jingzi. Part-of-Speech Tagging with Rule-Based Data Preprocessing and Transformer. Electronics, 2021, 11(1):56.