Proceedings of the 2023 International Conference on Machine Learning and Automation
DOI: 10.54254/2755-2721/30/20230089

Overview of cyber security situation awareness

Zheng Li

City University of Macau, Faculty of Data Science, Macau, 9990978, China

T20090105760@cityu.mo

Abstract. The rapid development of the network has made the network immersed in most people's lives, and even the degree of development of the network reflects the overall national strength of a country. Moreover, the control of the country is unable to leave the power of the network. All countries are becoming more and more urgent for the development of network, but in the face of more and more diverse attacks, people become overwhelmed. Network security is crucial to individuals, organizations and countries, and is related to the stability of the whole society and the security of the country. Therefore, network security has become a part of the network that cannot be ignored. In view of the current network security technology and the current network technology in the world, some network systems strengthen the application of network security situational awareness technology. This paper introduces the relevant concepts and technical fields of network security situational awareness technology, so that better understand and deepen the network security situational awareness technology.

Keywords: situation perception, concept analysis, data fusion technology, data mining technology

1. Introduction

With the continuous development of society in recent years, the use of the Internet is also growing. Moreover, under the impact of the COVID-19 pandemic in 2020, the Internet gradually began to have a place in various fields. It plays an increasingly important role, from the small to the individual, whether it is the electronic wallet needed for shopping, remote diagnosis in medical treatment, or online courses for students in education. As for the country, the publication of national plans, the management of various platforms, and the observation of people's movement tracks through big data during the epidemic are all inseparable from the Internet in life and work, which shows that the operation of the human society has been unable to leave the Internet altogether. In the network a large number of people rely on at the same time, the user's information is also being uploaded in succession, but also the formation of several database network security problems have become more and more urgent, especially in recent years: Trojan horses, worms and other viruses emerge in an endless stream, and even some criminals - "hackers" attack others' network security for benefits. These improper behaviors have brought considerable losses to relevant departments, personnel, and individuals [1]. Viruses typically manipulate data and run programs to damage entire systems. The Panda incense burning event in 2006 was to start the browser to download the virus independently through the running network file, which resulted in the loss of hundreds of millions of dollars. Therefore, the initial design based on the Internet is as follows: Firewall, vulnerability scanning, and other security technologies have been unable to curb the decline

DOI: 10.54254/2755-2721/30/20230089

of the security factor effectively, coupled with the popularity of the open development environment even if the software may also exist vulnerabilities, network security needs continuous improvement. The importance of network security situation awareness technology has also been gradually amplified and studied by various scholars, which has become the general trend.

2. Analysis of network security situation perception

2.1. Situation Awareness

The concept of situational awareness first appeared in the military and developed from perception, understanding, and prediction. It's a state and a tendency, and it all forms a whole, and it's not a situation if you just put out a single element or a single state [2]. In the situational awareness proposed by Endsley in 1988, "perceive elements in the environment within a certain time and space, understand their meaning, and predict their development trend and state shortly." There is too much situational awareness in our life. When crossing the road, we will slow down and stop at the side of the road when we see the red light. When the light is green, we will predict the car running the red light and subconsciously observe and cross the street. This is a primary situational awareness. The observation that the light turns red or green is the perception of the environment. The word that the light stops at the red light and walks at the green light is understanding the situation. However, it is impossible to fully predict all possible situational awareness by relying solely on situational awareness. Attention and working memory are the keys to situational awareness [3]. Therefore, there are many research directions, and the most prominent one is combining attention mechanisms with deep learning. This method is more extensive and effective in solving the most complex situation prediction and analysis judgments.

2.2. Network Security Situation Awareness

With the continuous development of the network, based on security big data, at the end of the 20th century [4], Bass proposed the concept of situational operation awareness in the network. Network situation awareness refers to using situation awareness technology in network management to achieve sufficient security of products. According to Bass, situational awareness needs to be "evaluated," "predicted," "visualized," and "interconnected." All of these are necessary. Similarly, situation awareness also requires analyzing unstructured data, just like the sights and smells collected by our brains. We can sort out the correlation between two different structures, so this is a vital role of situation awareness. Therefore, data mining and neural network-related technologies are needed to apply network security situation awareness to the network [5]. Bass proposed the concept, formed the theory, and then extended it till now. Quite a few scholars have also studied it [6]. Li Zhijian studied the prediction of network security situation awareness, integrated multiple attention mechanisms, and used BG-Trans network structure with BiGRRU dimension reduction to make more efficient and accurate predictions [7]. Wen Renyuan, Construction of security data analysis system based on big data [8]; Chang Liwei et al. established a network security situation awareness model based on the multi-source fusion of convolutional neural networks to improve the accuracy of attack identification. All levels of situational awareness are constantly being drilled.

3. Analysis of data processing

3.1. Data Fusion Technology

Situational awareness data comes from many platforms, where various security designs and content is supervised, so the data obtained may not be in the same format, which will form multiple sensor environments [3]. In this case, it is necessary to use relevant technologies to preprocess various information and carry out normalization and fusion. After data fusion is realized, data identity and location can be easily estimated, thus completing some real-time estimation of threats to the current state of the network. Data fusion technology is a key link in network security situation awareness. Its primary role is to integrate and process data of different types and sources better to identify security threats and

DOI: 10.54254/2755-2721/30/20230089

risks in the network. It combines and analyzes network traffic data, device log information, and security audit information to improve the ability to identify and predict network security risks.

Data fusion technologies can be divided into two categories: rule-based fusion and model-based fusion. Rule-based fusion integrates specific rules from different data sources to form complete security intelligence, such as IP addresses and time stamps. Model-based fusion models various data sources through machine learning and other technologies and integrates multiple models to form more comprehensive network security analysis results.

Data fusion technology plays a vital role in enterprise network security. It can reduce information lag and redundancy caused by data silos and provide more comprehensive and accurate network security situation awareness results. At the same time, data fusion technology can also optimize the automatic disposal of security incidents, enhance network security's self-healing ability, and reduce network security incidents' loss to enterprises.

It is worth noting that the application of data fusion technology still faces challenges and problems. For example, the formats and semantics of different data sources are similar, so integrating them and keeping the data transparent, timely, and accurate still needs further research and discussion. In addition, in data fusion, attention should be paid to data security and privacy to prevent data leakage, abuse, and other security problems. To further improve the accuracy and timeliness of network security situation awareness, enterprises need to strengthen the application of data fusion technology, formulate corresponding data fusion strategies and management processes, and establish sound data collection, transmission, storage, and analysis mechanisms. At the same time, enterprises also need to strengthen the construction of talents and technological innovation, use advanced algorithms and models, and constantly optimize the application effect and technical level of data fusion technology.

3.2. Data Mining Technology

Data mining technology plays a vital role in network security situation awareness. It provides strong technical support for real-time monitoring, rapid analysis, and dynamic feedback of network security information to realize the early warning and prevention of network security threats.

Data mining techniques can be applied in many ways. Firstly, network traffic is analyzed by data mining technology, which can identify abnormal traffic and attack traffic and provide real-time intelligence and control decisions. Secondly, data mining technology can detect anomalous behaviors in the network using a data mining algorithm and find the connection and development trend between different security events. In addition, data mining technology can also analyze malicious code, identify and defend against unknown attacks, and predict possible security threats and attacks in the future by analyzing historical data.

The application of data mining technology helps to strengthen the visualization degree and real-time of network security, realize the instant identification and early warning of security threats, and also helps to improve the ability to prevent network security. However, data mining still faces some challenges in practical application, such as privacy leakage and false positives, which needs to strengthen the research and exploration of data security, algorithm optimization, and the introduction of artificial intelligence.

Data mining technology has many application prospects in network security situation awareness. In further research and application, we need to conduct an in-depth exploration of data security, algorithm optimization, and algorithm fusion to achieve the network security situation awareness goal better.

3.3. Feature Extraction Techniques

In the process of network security situation awareness analysis, feature extraction technology plays a crucial role to better revealing the nature and characteristics of network attacks and abnormal behaviors. Therefore, feature extraction technology is essential to network security situation awareness.

Feature extraction technology in network security situation awareness is mainly applied to analyzing network traffic, behavior, and event data, aiming at mining the nature and characteristics of network attacks and abnormal behaviors and carrying out related intelligence analysis and countermeasures. The primary purpose of feature extraction technology is to extract meaningful information and features by

DOI: 10.54254/2755-2721/30/20230089

analyzing and processing network data for further study and research. For example, information such as protocol, port, and packet length in network traffic, as well as user access frequency, access time, and access target, can be used as characteristics for identification and classification.

Feature extraction technology in network security situation awareness mainly includes mathematical modeling, machine learning, natural language processing, and other technical means. Using these technical means, the original network data can be converted into identifiable information and characteristics to better reveal the nature and characteristics of network attacks and abnormal behaviors.

Feature extraction technology is an integral part of network security situation awareness. Its application can speed up security intelligence analysis and countermeasures, improve the results of each module, and further improve the accuracy and effectiveness of network security situation awareness. In the future, network security situation awareness and feature extraction technology will pay more attention to algorithm innovation and efficiency improvement to cope with the constantly changing and complex challenges of network attacks and threats.

3.4. Situation Prediction Technique

Situation prediction technology is an integral part of network security situation awareness. By analyzing existing data and historical trends, it can predict possible security threats in the future and formulate corresponding countermeasures in advance.

Network security threats take various forms, such as DDoS attacks, malicious code, and phishing. These attacks often have sudden, global, and long-term characteristics, bringing significant losses to enterprises and government agencies. Against such attacks, traditional security protection is often passive defense, and it is difficult to predict future attack threats based on the existing data and experience. Therefore, situation prediction technology is critical.

Facebook suffered a major DDoS attack in which attackers flooded its servers with data packets from botnets, bringing down its services. After analyzing the attack data, the Facebook security team discovered the critical information of the attack, including the time, location, and mode of attack, through situation prediction technology. It took targeted defensive measures to defend against the attack successfully.

The core of situation prediction technology is data analysis. It needs to rely on big data, artificial intelligence, machine learning, and other technical means to mine and analyze historical and real-time data, establish a suitable prediction model, and predict possible threats in the future. Familiar data sources include network traffic, operating system logs, configuration files, etc. The prediction model mainly involves clustering, classification, regression, and other methods.

It is necessary to clean, slice, and extract data features regarding data processing. Cleaning ensures the effectiveness and accuracy of data, slicing divides long-term data into small segments for analysis and improves data processing efficiency, and feature extraction extracts meaningful features from complex data as input to the prediction model.

In terms of model formulation, different algorithm models should be selected according to different application scenarios, such as random forest, support vector machine, decision tree, etc. To evaluate the model, it is necessary to use KPI indicators to test its performance, such as accuracy rate, recall rate, accuracy rate, and so on.

Situation prediction technology has a broad application prospect in the future network security threat prevention. In enterprises and government organizations, situation prediction technology can be implemented to improve network security protection and timely detect and prevent potential threats. At the same time, in the face of increasingly complex cyber-attacks, situation prediction technology can help enterprises and government agencies develop more scientific and accurate countermeasures to reduce security risks.

3.5. Visualization Technology

As an essential technical means, the visualization technology in the network security situation awareness paper can visually present massive network security data so that security professionals can more

DOI: 10.54254/2755-2721/30/20230089

intuitively understand the network security situation, timely discover abnormal conditions, and take appropriate measures to improve network security.

First, visualization technology can visually present network security data through charts, maps, topologies, and other forms. For example, visualization of network attacks can display information such as attack source, attack mode, and target of attack, making it easier for security professionals to understand and identify the characteristics and trends of network attacks.

Second, visualization technology can also support real-time monitoring and analysis, location of network security incidents, and timely response. Dynamically updated charts and maps can help security professionals grasp the network security situation in time, quickly respond to network security incidents, and effectively reduce network security risks.

Finally, visualization technology can be combined with other security technology means, such as artificial intelligence, machine learning, etc., to improve further the accuracy and efficiency of network security situation awareness. For example, by applying machine learning algorithms to visualization technology, automatic data classification and analysis can be achieved to identify cyber-attacks and protect network security quickly.

4. Conclusion and Discussion

Network security situation awareness technology has become a hot issue in security in the Internet era. It is an essential tool in the field of modern information security. It can provide timely network security status information, help security professionals perceive security threats in the network environment, and carry out rapid and accurate responses and disposal of security incidents. This paper discusses network security situational awareness technology's related concepts, principles, and technologies. With the rapid development of the Internet, network security situation awareness technology faces many complex security data processing and analysis problems. Therefore, it is necessary to introduce new security awareness methods and tools to improve accuracy and real-time security prediction.

Network security situation awareness technology has made some progress, but there are still some challenges and room for improvement. First, we need to use better modern technologies, such as machine learning, deep learning, and artificial intelligence, to improve the perception and prediction of cyber security. These technologies can identify the characteristics of cyber threats by analyzing large amounts of security data and help security professionals conduct fast, accurate, and comprehensive security detection and classification.

Secondly, we need to strengthen the research on network security threats and have an in-depth understanding of the characteristics, forms, and changing trends of network security threats to perceive and identify security threats more refinedly and realize more effective security monitoring and prevention. At the same time, we also need to improve cybersecurity data processing and storage methods to support real-time processing and analysis of massive security data.

In addition to the technical challenges and room for improvement, the application of cybersecurity situational awareness technology also needs to be enhanced. We need to understand further user and business requirements, design and support convenient, fast, and reliable data visualization tools to help security professionals visually analyze and predict security threats, and improve security decision-making ability.

Cybersecurity situational awareness technology development is expected to continue to strengthen, and technology innovation and application research will become the focus of future research. We must introduce new technologies and approaches to address the rapid evolution of security threats. In addition, we need to strengthen testing and verification in real scenarios, optimize and improve security data presentation and visualization technology, and present relevant information on network security situations to information security experts and decision-makers visually to enhance the level and quality of network security comprehensively.

Network security situation awareness technology is essential to modern information security. Future research needs to strengthen technological innovation and application research, explore more innovative and collaborative solutions, optimize and improve network security awareness technology and

DOI: 10.54254/2755-2721/30/20230089

visualization tools, enhance the level and quality of network security in the field of information security, and help users better understand and grasp the network security situation, and make better contributions to network security.

References

[1] Jin Liuliu. (2014). Analysis of the main hidden dangers and management measures of computer network security. Network security technology and application (08),228+230. doi: CNKI: SUN: WLAQ.0.2014-08-148.

[2] Endsley M R. Design and evaluation for situation awareness en- hancement[C]/ / Proceedings of the Human Factors Society Annual Meeting. Los Angeles: Sage Publications,1988: 97-101.

[3] YANG Yu & GU Yuheng. (2022). A Review of Cybersecurity Situational Awareness. Science Technology and Engineering (34),15011-15019. doi: CNKI: SUN: KXJS.0.2022-34-003.

[4] Bass T,Gruber D. A glimpse into the future of ID[J]. The Maga-zine of USENIX & SAGE,1999,24(3) : 40-49.

[5] ZHAO Peiyong. (2022). Cybersecurity situational awareness system structure and key technologies. Wireless connectivity technology (22),154-156. doi: CNKI: SUN: WXHK.0.2022-22-036.

[6] LI Zhijian. (2022). Research on the Application of Multi-head Self-Attention Mechanism in Cybersecurity Situation Prediction (Master's Thesis, Hebei Normal University).https://kns.cnki.net/kcms2/article/abstract?v=ZUUpU2TibaJwdav6_9hqBO6_DQdyYoIeveRmHvFiXsMXP22W9yQTycdasQBGcgUL3LajginT91klRYCUHVeKhlrSx98sDFNfJd_QskFRNaqA2WDiFCTJYA==&uniplatform=NZKPT&language=CHS

[7] WEN Renyuan. (2023). Research on Cybersecurity Situational Awareness Technology Based on Big Data. Network security technology and application(01),57-58. doi:CNKI:SUN:WLAQ.0.2023-01-026.

[8] www.voipchina.cn/html/38-1/1531.htm