Journal of Computing and Electronic Information Management

ISSN: 2413-1660

Research and analysis of network security and preventive measures for power systems

Yuebei Liu, Yanyan Wu, Tingxu Pu
School of Electrical Engineering and Electronic Information, Xihua University, Chengdu, Sichuan, 610039, China

Abstract: With the continuous development of the power grid, there are frequent incidents of the grid being attacked. This paper first introduces the security definition of the grid network, the security objectives and the necessity to ensure its normal operation and not to be hacked. Then we summarize the main processes of several international attacks on the power grid, which play an important role in targeting the prevention of the attacked events. Finally, we argue that the overall consideration of preventive measures should be carried out in terms of personnel, technology, and management, while the key steps of the intrusion process should be targeted to ensure the grid and its data security as much as possible.

Keywords: Grid attack; data security; grid security.

1. Introduction

In recent years, as information and communication network technology continue to iterate and update, information technology represented by 5G communication, Internet of Things technology, artificial intelligence, and blockchain continues to integrate with the physics of the power grid, the power system network is developing in the direction of intelligence and digitalization. At the same time, the amount of data on the grid is increasing, and the daily data volume is growing in spurts, which makes the protection of the grid and its data indispensable. However, attacks on the grid and its data are occurring worldwide to varying degrees, with intruders bypassing the grid's security mechanisms, targeting the grid's transmission and distribution systems through unauthorized control of the grid's control system, and stealing data, resulting in massive power outages and data leaks.

2. Network data security of power system

2.1 Definition of grid network and its data security

Grid cybersecurity refers to a set of practices to protect power systems, power communication networks and their associated software from malicious digital attacks. The purpose of these attacks is mainly to obtain, modify and destroy grid data and information, but also to directly interrupt the normal operation of the grid and thus blackmail the grid company or users.

Network security protection is for all communication lines, communication equipment, related business systems and hardware facilities in the network, and its security protection is extremely rich in content, covering a wide range of content, and requires comprehensive security of links, nodes, topologies, physical equipment, systems, environments, etc., otherwise they may threaten the normal, stable and safe operation of the power information and communication network [1]. The network security of power system is closely related to our life, in order to better implement the network security of power system can be considered from strengthening the network boundary security deployment, reasonable configuration of network security equipment, strengthening host security management, and attaching importance to application software security protection, so as to guarantee the power grid and its information and data security.

The prerequisite for the stable development of the work of the power system is the safe and stable operation of the power grid. The latest version of China's Electric Power System Security and Stability Guidelines [2] was officially released on December 31, 2019, and with the development and promulgation of various security and stability standards, CEC has increased the analysis and management of the security and stability of the electric power system, which has become more and more accident-resistant, more and more stable, and the accident rate has decreased significantly.

2.2 Cybersecurity goals for the power grid

1) Confidentiality: Ensure that information on the grid system and data communicated through the IT network are not accessed by unauthorized third parties. In other words, this means that hackers are not free to spy on information in the power service company.

2) Integrity: This includes maintaining data consistency, accuracy and trustworthiness throughout the data collection cycle, while ensuring that data cannot be altered during transmission, which requires that the grid service company must take steps to ensure that unauthorized people cannot alter the data.

3) Availability: Information and data are continuously and readily accessible to authorized parties at all times, which involves proper maintenance of the hardware and technical infrastructure and systems that hold and display the information.

2.3 The necessity to ensure grid security

The current grid network is a multi-layered system consisting of three main layers: the generation and transmission layer, the control and dispatch layer, and the near-end distribution layer, as shown in Figure 1. Among them, the generation and transmission layer interconnects power generation units such as wind farms, PV parks, battery storage and conventional power plants. The control and dispatch layer provides centralized monitoring and control capabilities for transmission and distribution system operators. The near-end distribution layer can power homes and cities, including: electric vehicle charging infrastructure, electric transportation, microgeneration, (smart) homes and buildings, heat pumps and smart meters in place. And Internet of Things (IoT) technology can connect all these smart facilities or devices via 5G technology. Combining cities with multiple automated transmission and distribution stations can create a Wide Area Network (WAN). Different neighborhoods or cities are connected to each other through substations and high-voltage transmission networks. On top of this, a telecommunication layer is deployed, resulting in a wide network that can be monitored, controlled and protected from a central control room. This allows for more efficient and secure operation of the system. In the WAN, data is communicated wirelessly via substation gateways or communication towers or fiber optic cables. All these elements are part of the OT network, and although telecommunication towers are used, these are not channels used for phone calls or Internet access, but channels dedicated to utilities.

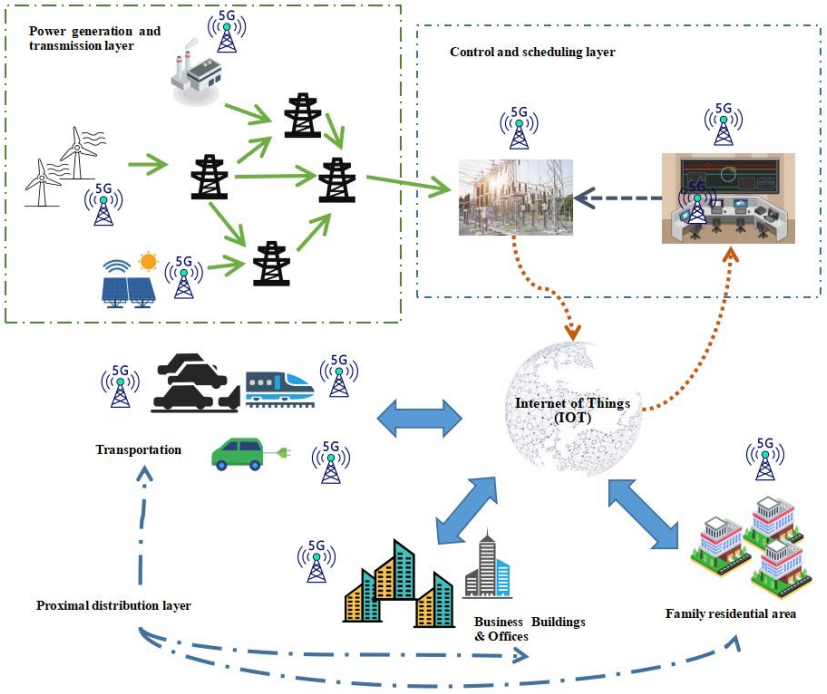

Figure 1 Grid network hierarchy diagram

Today's cyberspace is not only about the security of people's basic information, but also a means for countries to play games. In the area of cybersecurity, hackers around

the world are "working" by taking orders and attacking the power networks of other countries, leading to massive power outages. Now the technology of each country is advancing rapidly, no country can make an absolutely safe network data system, so in order to create a real-time security data network, we can only do real-time detection, real-time improvement, to ensure that personnel, technology, management of the three aspects of the balance.

3. Typical grid attack examples and process summary

3.1 Summary of typical grid attack examples

Since 2015, there have been about 385 hacking incidents on power grids worldwide, and we have selected the following five typical incidents to analyze their attack content, attack process and impact.

Table 1 List of typical grid attack times in recent years

Time	Location	Attack content	Causes impact
2015.12.23	Ukraine	Operated malware to disconnect the main control computer of the power company from the substation, and then planted a virus in the system to paralyze all the computers	Nearly 1.4 million people were without power in their homes, and all areas were without power for between one and six hours. Two months after the attack, the control center is still not fully operational.
2018.3	United States	The attacker implants a program that collects information, captures screenshots, records details about the computer, and saves information about the user on that computer	Intelligence and information about users has been compromised
2019.3.7-3.9	Venezuela	Guri hydropower plant deliberately sabotaged by opposition	Several states and municipalities suffered severe power outages and the regional water and communications networks were greatly affected as a result, leading to disruptions in Internet connectivity
2019.7	South Africa	The virus encrypted all databases, applications, Web Apps, and official websites of the power company	Power outages in several residential areas prevented prepaid customers from buying electricity, topping up, processing invoices, or

			accessing City Power's official website
2020.6	Brazil	Power company Light S.A hacked for ransom	Threatened with $1400 ransom, the ransomware family does not have a global decryptor and requires the attacker's key to decrypt the files

It is easy to see that the main steps of the attack are similar for the specific cases as in Table 1, which we will elaborate in the next section. From the results, the economic and social depletion caused by the power network once it is hacked cannot be underestimated. Due to the rapid development of the power industry and the increasing interconnection between industries, the demand for grid security performance needs to be further enhanced as a result. At the same time, more sophisticated and worse malware is increasing. If corresponding protection measures are not made in advance, once the security mechanism of the power grid is breached by malware, it will evolve into a serious consequence of data information leakage to individuals, society and even the whole country. This again proves the importance and necessity of securing the power grid.

3.2 Attack process

As the power industry relies more and more on the network, network attacks pose a great threat to the safe operation of the power grid system. The types of attacks on power systems are mainly classified as ransomware, DDoS attacks, APT attacks, vulnerabilities, malware, etc. The power industry is an important part of the national infrastructure, not only in the people's daily life occupies a place, personal, corporate, and even national information security are closely related to it. Therefore, it is extremely important to find better protection measures through the attack process of the previous example of the power grid attack. As shown in Figure 2, the process of grid attack is outlined as:

Phase 1 (reconnaissance): The attacker collects information about the attacked target, e.g., information about the operator of the grid distribution system.

Phase 2 (creating a virus and sending it): The attacker creates a virus that can access the target (e.g., a malicious plug-in that can open the IT system gateway) and delivers it to the attacked target.

Phase 3 (induce): Using the virus program as a carrier attachment, send it to the target computer and induce the attacked to open the attachment thus infecting the computer with the virus (e.g.: send a copy of the malicious plug-in to the grid employees via email to Excel and guide the poor security conscious employees to install the software with the virus).

Phase 4 (using the virus to take control): after the victim is lured to open the program containing the virus, the attacker obtains administrator privileges through the malware and can then install more malware to achieve the purpose of the attack.

The fifth stage (attack on the target): after the attacker has control, the target to implement damage actions (such as control of the server, disconnect the circuit breaker, etc.).

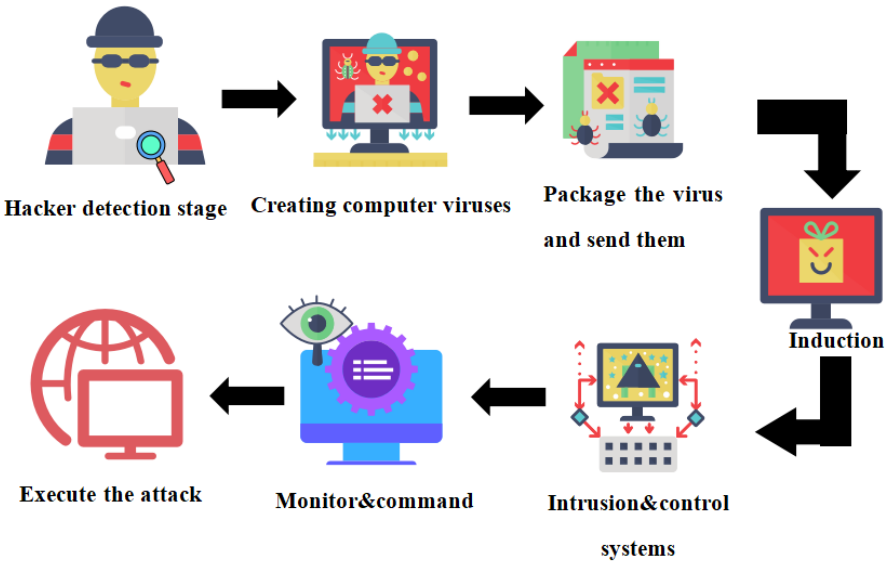

Figure 2 Attack flow diagram

4. Reflections and some suggestions for securing the grid and its data

4.1 Embedded system technology

Through the analysis of the grid attack process in the second part and the authors' understanding of the current state of the grid, we believe that three aspects should be considered in general: personnel, technology, and management.

First is the personnel aspect. The internal personnel of the power network system is an important part of the system security guarantee. Professionals are prone to use their positions to obtain illegal information and use illegal means to access the secrets of the power grid system, thus leading to information leakage. Technical personnel may not pass the technical level or confidentiality is not strong, password protection level is too low, encryption strength is not enough, a variety of confidential documents without the relevant permission control, etc. [3], resulting in information leakage. Moreover, the comprehensive quality of personnel is required for the timely monitoring and removal of external hacking and virus implantation, as well as the ability of personnel to avoid information or files containing viruses in their operations.

The second is the technical aspect. The analysis of the case of foreign attacks on the power grid can be seen, the hacker attack on the national grid is actually a technical competition between hackers and national technicians, so the technology is the core

of the network completely protected, it can determine how we establish a set of network protection technology. Establishing a network security system with a higher level of more effective protection requires the necessary means to improve network communication lines and equipment defects, guarantee the use of private networks or trusted networks technology, improve network anti-virus technology capabilities, and strengthen the network supervision system to prevent hacking [3].

Finally, there is the management aspect of the power grid company. The management level is the center of network security, both technology and personnel are dispatched and improved by the management, and most of the security loopholes originate from the lack of management, so it is especially important to establish a security management system. Nowadays, many network security departments have similar problems at the management level, with inadequate management systems, imperfect supervision systems, inadequate personnel training, and lack of attention from managers. Strengthen the periodic assessment of the network system, improve and increase the supervision system, pay attention to the security training of personnel and the continuous learning of new technologies in security, in order to better protect network security.

(1) Strengthen the system security protection level. With the advent of the information age, the power network system security vulnerabilities are exposed and vulnerable to hacker attacks, thus seriously threatening the security of the power network system. Therefore, it is important for electric power companies to recognize the importance of system repair as well as upgrading, which can be done by regularly changing the boot password, logging into the system requires security authentication, and strong authentication makes it difficult for attackers to access files or systems. Two-factor authentication is an example of a system that can make logging in more secure. The system is regularly tested for vulnerabilities and other means to strengthen the security level of the system, Intrusion Detection and Prevention System (IDPS) and firewall can prevent illegal access to the IT-OT network. IDPS can have more advanced features than firewall. It can use machine learning to adaptively learn which activity is suspicious and block it.

(2) Strengthen network security protection. Hackers on external networks often carry out network invasion by planting Trojan horses and spreading viruses, which are system network security hazards, and enterprises need to strengthen the relevant network security protection level. Firewalls can be set up to protect the data transmission process and data security; antivirus software should be installed on the computer and the antivirus system should be updated in a timely manner. Antivirus software can stop attacks at an early stage and prevent malicious programs, such as BlackEnergy3, which can use antivirus software to prevent malicious software from

performing its tasks, thus guaranteeing the timely update of the system's functions. For the enterprise internal personnel management system to improve, enhance the professionalism and confidentiality of personnel, prohibit personnel from private illegal outreach, but also to increase the management of mobile hard disk, to avoid the virus through this route into the system network.

(3) strengthen data security protection. Data security is the core of the entire power network system security. For the relevant personnel of the enterprise to strengthen personnel training work, to standardize the operating system, for the work of personnel to carry out strict management. At the same time, increase the level of data security protection, encrypt the transmission of key information, restrict data access rights for different departments, encrypt data transmission channels, prevent hacker attacks and protection against electromagnetic interference. The introduction of data backup and other recovery procedures ensures business continuity, which means that normal operations can be quickly resumed after an attack. In addition, data encryption processing is also an important means to ensure data security. Data encryption here is a kind of encryption technology means for the process of uploading and downloading data in the power system network, i.e., the encrypted data information must be decrypted when it is used, and the decryption process also requires the input of the correct key, and the cipher text is the correct data after restoration. [4]

In addition, the construction of an autonomous information security framework (including key algorithms, operation control platforms, databases, etc.) is an important issue to be addressed by each power service company. To build a hardware and software supply chain with strong relative security and controllability, so as to realize a multi-dimensional intelligent protection system of "cloud-end-border", complete the construction of four major infrastructures of security access, authentication, interaction and isolation, and fill in new technologies such as big data and cloud computing on the basis of the traditional framework to realize a collaborative and linked technical protection system. [5]

5. Conclusion

The grid of the future is intelligent. With the concept of integrated energy system, the energy system, including the grid, will continue to be coupled and expanded, and the devices connected to the system are intelligent, which means that the energy network will face more serious challenges. Someone wants to hack into the energy system for some reason, steal data or information, or manipulate the operation of the energy system to create partial power outages or other catastrophic events. As the grid introduces more IT-OT interconnection capabilities and machine learning, it will increase the probability of threats to the grid. Thus, if the grid is more intelligent and

digital, it will be more vulnerable to manipulation and control. At this stage, for many countries, including China, this has become one of the existing threats to energy security. Therefore, we should continue to focus on grid security and use more methods to ensure the safe operation of the grid and reduce the risk of intrusion.

References

[1] Zhao Ning. Exploration of security protection strategies for information and communication networks in power systems [J]. Electronic components and information technology.2022(01)
[2] GB 38755-2019, Guidelines for security and stability of power systems [S].
[3] Sun Wenjia. An introduction to the role of the three elements of security in network information security [J]. Network and Information,2011,25(12):59
[4] Yu, Lin-Wen, Ma, Chen-Yu. Thinking about the security architecture of new generation power information network[J]. Network Security Technology and Applications,2022(03):109-110.
[5] Luo Hailin. Exploration on the security architecture of power information network of Southern Power Grid[J]. Digital communication world,2017(09):160.