Application of Trusted Computing Technology in Active Defense of Smart Substation

Liandong Chen¹, Tao Yang*, Gang Li², Xin Liu³, Ning Lu³, Kai Cheng², and Xiaopeng Xin²

¹State Grid HeBei Information and Telecommunication Branch, Shijiazhuang, Hebei, China
²North China Electric Power University/School of Control and Computer Engineering, Baoding, Hebei, China
³State Grid HeBei Electric Power Co. Ltd, Shijiazhuang, Hebei, China
*Corresponding author’s e-mail: lg_seek@ncepu.edu.cn

Abstract—Nowadays, most security systems mainly use firewall, intrusion detection, virus killing and other technologies to defend against external attacks. This passive defense mode has low efficiency and high false positive rate, and active defense technology can solve these problems to the greatest extent. At present, the intelligent substation is in the development stage with weak security. After a large number of terminals are connected, although the operation efficiency of the whole station is improved, it also brings more risks. This paper takes the access security of terminal equipment in intelligent substation as the research object. By mining the security vulnerabilities of substation, an active defense method based on trusted computing is proposed, the applicability and efficiency of trusted computing technology in the field of substation active defense are proved and the effectiveness of the method is verified to realize the trust guarantee of the whole process of terminal access to intelligent substation.

1. Introduction

In recent years, cyber attacks have occurred frequently. In the "Earthquake Network" virus incident in 2010, a large number of nuclear power plants were paralyzed; The power outage in Ukraine in 2015 reflected the actual power of hackers attacking the power grid. It was a power control system paralyzed by taking the terminal as the attack springboard[1], which became the world's first publicly reported large-scale power outage. As an important national energy conversion facility, intelligent substation has weak protection measures for a large number of terminal equipment connected, so it can become the object of attack. Terminal equipment plays an important role in substation and is full of crisis. Terminal equipment has already become the key target and main springboard to attack substation.

Intelligent substation has the characteristics of Cyber physical system(CPS). The close coupling between information system and physical system makes the asset information and real-time data of substation face the risk of theft. Network attacks can cause data leakage or data tampering, resulting in the risk of invading the substation with the terminal.

The research on trusted computing has become an international research hotspot. The National Science Foundation (NSF) focuses on how to build and manage the security and privacy of the network; Microsoft has also proposed a 10-year "trusted computing" strategy, with the goal of making computers more secure and stable[2]; China also attaches great importance to the research of system credibility.
There are relevant topics of credibility in the National Natural Science Foundation and national key basic research projects. In 1995, on FTCS-15, IEEE fellow, Professor A. Avizienis and others proposed the concept of trusted computing[3], and implanted a security chip on the PC hardware platform to improve the security of terminal equipment when accessing the system.

In recent years, trusted computing technology has been widely used in the field of power security. Literature[4] uses trusted computing to build a multi-agent active defense framework to better protect substation communication in Wan; Literature[5] combines trusted computing with immune system theory to build a trust chain transmission mechanism suitable for power platform, which greatly improves the security of power grid dispatching control system; According to the idea of trusted network connection, document[6] analyzes the behavior of power grid users and determines their continuous credibility, so as to realize the whole process security control of terminal access; In reference[7], considering the Intranet environment of terminal operation, a terminal security inspection and access control system is designed. The trusted access control of terminal is realized by checking and repairing the operating environment of terminal equipment.

In this paper, the hierarchical structure and data flow of intelligent substation are studied by using the information physical system theory, and the vulnerability of intelligent substation under the extensive use of terminal equipment is analyzed; Then, based on trusted computing technology, the terminal trusted access process is constructed; Finally, the performance of trusted computing platform is tested by simulating the corresponding experimental environment, and the effectiveness of this technology for active defense of intelligent substation is verified.

2. Safety problems of intelligent substation under CPS

2.1. Structure and data flow of Intelligent Substation

Smart substation is an important pillar in the construction of smart grid, which can realize power conversion and transmission and distribution control. However, the cost of high intelligence is to face many security threats. Because the asset information and real-time data of substation can bring great benefits to attackers, once leaked, the consequences are difficult to estimate, so it is necessary to strictly ensure the information security of substation.

The data transmission of intelligent substation mainly depends on the network between layers. In order to ensure the transmission efficiency and security, different networks use different transmission protocols. The data transmitted between layers and the transmission mode used are shown in Tab. 1. It can be seen that the division of work at each layer of substation is clear, which is also the basis for the stable operation of substation.

| Data flow direction | Data content | Transmission mode |
|---------------------|--------------|------------------|
| Process layer to interval layer | Merge unit voltage and current sampling values, circuit breaker switching status, diagnostic information, etc | SV |
| Interval layer to process layer | Trip command, control command, status information, etc | GOOSE |
| Bay layer to station control layer | Equipment protection data, etc | MMS |

2.2. Communication mode of intelligent substation under CPS

Since the primary equipment and secondary equipment of intelligent substation are perfectly corresponding to CPS, the communication mode of substation can be analyzed by CPS theory. CPS realizes the close combination and deep cooperation between information system and physical system, and can realize the real-time perception of large-scale system operation state and the dynamic control of interactive process. Intelligent substation has CPS characteristics to a great extent, such as the combination of virtual and real energy flow and information flow, and the dynamic interaction of data
generated by primary equipment and secondary equipment. Although CPS has not been fully integrated into the intelligent substation, it still improves the working efficiency of the equipment to a certain extent and ensures its stable operation.

As shown in Fig.1, CPS communication mode of intelligent substation is divided into physical measurement and information measurement. Physical measurement corresponds to primary equipment and information measurement corresponds to secondary equipment. The measurement information generated by the physical measurement is collected and integrated by the electronic transformer, and then transmitted to the information side as its system input. These data form control information through processing and conversion. The control information is in the form of message, and the control information is sent to the intelligent terminal. The intelligent terminal converts several types of messages to form the state quantity of the equipment on the physical side.

The operation state of the primary equipment determines the system input of the secondary equipment, and the instructions of the secondary equipment determine the operation state of the primary equipment[8], showing a strong coupling relationship. Although CPS improves the operation stability and communication efficiency of the substation, the frequent interaction between the information side and the physical measuring equipment will also have some impact, mainly as follows: the normal operation of the information side equipment requires the physical measuring equipment to supply power for it, and the safe and reliable operation of the physical measuring equipment depends on the normal operation of the information measuring equipment[9].

2.3. Vulnerability analysis of Intelligent Substation

A large number of network attacks will seriously damage the stability of CPS in intelligent substation. Common attack means include eavesdropping messages, interrupting processes, tampering with data, forging records, etc. the real-time data of substation becomes almost completely transparent to attackers, and its vulnerability is mainly reflected in the following aspects.

(1) Imperfect physical isolation: the level of firewall, anti-virus software and intrusion detection system is too low to resist external attacks;

(2) The security protocol is not involved: the IEC 61850 standard of intelligent substation improves the interoperability between different terminal equipment, but there are few security protocols in terms of terminal equipment access, resulting in many security vulnerabilities in the control message transmitted on the information side[10];

(3) Insecure communication protocol: goose, SV and manufacturing message protocol have low protocol confidentiality in the transmission process, and lack of encryption measures in access control and identity authentication, so the message is easy to be intercepted by attackers.
3. Trusted access model of intelligent substation terminal

3.1. Trusted computing platform for intelligent substation terminal
As the terminal equipment works in the communication module in the substation CPS model, security protection is extremely important, but the current terminal lacks effective isolation protection. After being attacked, it will bring hidden dangers into the substation, so as to steal confidential data or control equipment action. Therefore, it is necessary to ensure that the process of connecting the terminal to the substation is credible. For terminal equipment, if all data interaction and action signals are in normal state in the process of accessing the substation, the terminal is called trusted, and the process can be called trusted access. Trusted computing is one of the core technologies of trusted access.

Fig.2 Trusted computing platform structure of Intelligent Substation
As shown in Fig. 2, the trusted computing platform structure of intelligent substation is composed of hardware layer, kernel layer and application layer. Among them, the hardware layer is mainly responsible for the power on of the trusted cipher module, self-test[11] and the generation of measurement root, that is, the trusted start process; The kernel layer has the largest workload. First, the terminal is authenticated to detect its basic information, then the integrity measurement is carried out to ensure the credibility of its running state, and finally the trusted network connection is used to realize the secure communication between the terminal and the network nodes; The work of the application layer is almost carried out at the same time as that of the kernel layer. In this layer, the trusted password module completes the trusted guidance and trust chain transmission to the terminal operating system.

3.2. Trusted access process of terminal equipment

![Fig.3 Trusted access process of terminal](image_url)
As shown in Fig. 3, the process of terminal access to substation is divided into the following steps:

1. The terminal shall prepare the data and sort out the data interacting with the substation;
2. Trusted Network Connection Client (TNCC) and Trusted Network Connection Server (TNCS) are initialized to detect the connection status of trusted network. If it is in safe status, the terminal can apply for network access;
3. The terminal accesses the substation access gateway and carries out identity authentication at the same time. If it passes the authentication, it will carry out integrity measurement. If it fails, it will be isolated and marked as a risk terminal and stored in the database;
4. IMC collects the terminal integrity information and transmits it to TNCC. TNCC interacts with TNCS and processes the integrity information. If the integrity requirements are met, it is transmitted to IMV;
5. IMV verifies the integrity information of the terminal, and measures the integrity after passing the verification. If the measurement passes, it agrees to the terminal network access request, and the terminal can access the substation. If it passes, it can also isolate it, mark it as a risk terminal, and store it in the database.

4. Experimental analysis
Smart substation is an important part of smart grid and carries most of the power transportation work. Therefore, the CPS system of smart substation has extremely high requirements for the real-time performance of various businesses. Trusted computing technology introduces an integrity measurement mechanism[12]in the operating system, startup and execution links and the loading of executable programs, which is suitable for security inspection during the access of different types of terminals to large-scale systems and active defense against network attacks. By simulating the operation environment of the intelligent substation control system, this paper deploys the terminal server, database, primary equipment, secondary equipment and terminal equipment, and implants the trusted computing platform into the terminal equipment to provide it with trusted password module and trusted software base. The test environment adopts the current mainstream server, and the terminal equipment is installed with a virus-free operating system in advance, Ensure the safety of the initial state.

After the simulation environment is built, the performance test of the intelligent substation control system is carried out. The test items include the CPU utilization of the trusted chip and the data transmission time between the devices in different processes when the terminal equipment is connected to the secondary equipment (measurement and control equipment, metering equipment and protection equipment). After the test, the influence of the trusted computing platform on the two test items in different processing time is analyzed.

![Fig. 4(a) CPU utilization of trusted chip](image-url)
As shown in Fig. 4(a), when the terminal equipment accesses the secondary equipment, the CPU utilization of the trusted chip is the highest during access, followed by before access and the lowest after access, which indicates that the terminal equipment is most vulnerable to network attacks during access. In order not to damage the experimental equipment, the malicious program is implanted into the terminal device to simulate the network attack.

As shown in Fig. 4(b), with the increase of test times, the data transmission time between the terminal and secondary equipment becomes shorter and shorter, because the longer the data transmission time, the more time left for the attacker, and the more vulnerable the terminal is to attack[13]. When the same malicious program is implanted into the terminal device every time, the defense autonomy of the trusted computing platform is improved every time it is tested. Under this effect, the data transmission time is shortened.

As shown in Fig. 5, the longer the response time, the greater the impact of the trusted computing platform on the trusted chip CPU or data transmission between devices. The curve change rate of CPU impact is small, one is because the simulated network attack power is limited, and the other is because the trusted chip has strong computing power. The curve change rate of data transmission between devices is large because the terminal equipment used in the experiment is low in intelligence. The longer the response time, the greater the probability that the terminal will be attacked, and the more the trusted computing platform will play its role.

5. Conclusion

Trusted computing technology has absolute advantages and broad application prospects in the field of active defense. Especially for large-scale industrial control systems, only active can resist external intrusion to the greatest extent. Due to the shallow research on network security technology, the network attacks simulated in the experimental test in this paper are not strong enough to verify the ability of trusted computing technology to a greater extent, but this can not deny its position in active defense. In
the future research, we will continue to improve and strengthen the encryption algorithm to improve its efficiency.

There is a saying on the Internet that "Active defense is essentially equivalent to network attack", because active defense can not only block the attack behavior, but also counterattack the intruder according to the collected effective information, so as to repel the intruder. However, whether these defense methods are legal and whether they have reached a social consensus is a problem.

In short, although active defense is considered to be an effective security strategy, there are still technical problems. In my opinion, in order to make effective use of active defense technology in the future, we not only need to strengthen technology, but also severely crack down on cybercrime and increase the punishment of cyber attackers.

Acknowledgments
This paper is supported by the Science and Technology Project of State Grid HeBei Information and Telecommunication Branch (No.SGHEXT00WLJS2000144). We would like to thank anonymous reviewers for their helpful comments and suggestions.

References
[1] Zhao J H, Liang G Q, Wen F S and Dong Z Y 2016 Automation of Electric Power Systems vol. 40, no. 7, pp 149-151
[2] Long D, Sheng W X, Wang Y, Lu Y M and Sun C 2015 Chinese Society for Electrical Engineering vol. 35, no. 14, pp 3522-3531
[3] Ji H, He Z, He Z, Jiang H, Cai S and Yang T 2019 IEEE 25th International Conference on Parallel and Distributed Systems PP 917-920
[4] Tong X Y 2011 Automation of Electric Power Systems vol. 35, no. 20, pp 53-58
[5] Gao K L, Wang Z H, An N Y and Zhao B H Advanced Engineering Sciences vol. 49, no. 2, pp 28-35
[6] Chen L and Qiao W D 2016 Electric Power Information and Communication Technology vol. 14, no. 4, pp 70-74
[7] Yang G L, Dai X and Mao H D 2013 Computer Engineering and Applications vol. 49, no. 6, pp 109-113
[8] Chen Y R, Li J E, Xu A, Yuan K, Liu K P and Ni P 2021 Automation of Electric Power Systems vol. 45, no. 3, pp 102-110
[9] Chen L J, Mei S W and Chen Y 2012 Control Theory and Applications vol. 29, no. 2, pp 240-244
[10] Zhang Y H, Ni M, Sun Y H and Li M L 2019 Automation of Electric Power Systems vol. 43, no. 21, pp 12-22
[11] Gao K L, Xin Y Z, Li Z, Sun W, Nan G L, Tao H T and Zhao B H 2015 Automation of Electric Power Systems vol. 39, no. 1, pp 48-52
[12] Chen Y Q, Wu X P and Fu Y 2013 International Workshop on Cloud Computing & Information Security vol. 52, no. 1391, pp 336-340
[13] Zhang Z, Zhang W and Wang J 2014 Information and Communication Technology-EurAsia Conference pp 59-69