Research on the technology of preventing illegal terminal access

ZhiMeng Shu1*, YongGuang Liu1, HuiNan Wang2, ChaoLiang Sun1 and ShanShan He1

1XJ Group Corporation, Xuchang City, Henan Province, 416000, China
2State Grid Shanxi Marketing Service Center, Taiyuan, Shanxi Province, 030001, China
*Corresponding author’s e-mail: shuzhimeng@xjgc.sgcc.com.cn; 22045600@qq.com

Abstract. As an important part of energy Internet construction, power consumption information acquisition system, as the "total entrance of power information data acquisition and the total exit of control instruction execution", plays an increasingly important role in the safe and stable operation of the system. At present, the on-site access equipment is diversified, but there is a lack of unified active security defense early warning module, and there is no perfect security monitoring system. There are security risks such as illegal replacement of on-site terminals and private upgrade of terminals. In order to further improve the security and stability of smart grid operation, this paper makes an in-depth study on the existing security problems of the acquisition terminal and the online security monitoring of the acquisition terminal, and adopts the device fingerprint technology and password technology to meet the needs of the security protection of the acquisition terminal.

1. Introduction

In the process of on-site operation, the acquisition terminal is faced with security risks such as illegal replacement and private upgrade by the terminal manufacturer. At the same time, the terminal itself has security risks, especially the lack of security protection measures for the network port and local port, and the risk of malicious attack, which is easy to become the main target and springboard of attacking the power grid[1].

In order to solve the above problems, we should start from two aspects. One is the new terminal online security monitoring module on the main station side, which is used to deal with the security problems such as illegal terminal access and online monitoring of security events, to help improve the security protection level of the acquisition terminal, and to form a closed-loop processing mechanism of pre prevention, in-process processing and post feedback[2]. The second is to reinforce and upgrade the security of the terminal, including reducing the vulnerability of the terminal operating system, avoiding the weak password, requiring temporary authorization for terminal maintenance, increasing the LCD operating password, and increasing the active reporting of security events[3].
2. Technical study

2.1. Technical principles

2.1.1 Device fingerprint technology
Device fingerprint is to generate unique fingerprint information for the terminal by using static and dynamic information (static information includes terminal software version, ESAM serial number, uplink module network standard information, downlink module chip ID; dynamic information includes acquisition success rate[4], meter reading efficiency, response speed, etc.) of the acquisition terminal, and monitor the field equipment through fingerprint information.

Combined with the current situation of field equipment, the following fingerprint information is mainly set:

- Version information: manufacturer code, software version number, software version date, hardware version number, hardware version date, manufacturer extension information, applicable to 09 version terminal.
- Version information + ESAM serial number, suitable for 13 version and 698 terminal.
- Version + ESAM serial number + uplink module network standard information + downlink module chip ID, suitable for 13 version, 698 terminal and energy controller.
- Static information + dynamic information (success rate, meter reading efficiency, response speed, etc.).

2.1.2 Cryptography
The key management system of power consumption information realizes the whole process management of key generation, transmission, backup, recovery, update and application; realizes the security authentication, data encryption and decryption of ESAM module of smart meter, acquisition terminal, power selling card and other metering equipment[5]; realizes the security protection of communication information between acquisition system and meter, acquisition terminal, field operation terminal and other metering equipment Functions: including key management system, key detection system, cryptographic equipment and other modules[6].

2.2. Implementation mode

2.2.1 Security monitoring of master station terminal access
There are many types of terminals operating on site, including 1367.1 protocol terminals (version 09 and 13), 698.45 protocol concentrator and energy controller, which are quite different from each other. Therefore, illegal terminal access monitoring is carried out from different dimensions.

2.2.1.1 Terminal without ESAM chip
Because the terminal without ESAM chip only verifies the terminal address and administrative code when logging in to the master station, its device fingerprint is relatively simple, and these information is easy to forge, so it does not have the ability to restrict it before access, and can only check the suspected illegal devices after the terminal access. The illegal access monitoring process is shown in Figure 1.
When the master station monitors the meter reading parameter setting triggered by the non-debugging process of the terminal without ESAM chip, or the manufacturer code of the terminal version is not in the system code base, it will enter the next process.

- The historical frozen data, terminal version, terminal parameters and other data items of the call test terminal are compared with the fingerprint information stored in the master station. At the same time, the communication protocol used in the call test data is compared with the terminal protocol type stored in the master station. If the comparison results are inconsistent, the terminal is added to the suspected illegal equipment troubleshooting list.

- According to the list of suspected illegal equipment, the on-site confirmation work order is issued through the closed-loop system to confirm whether the equipment has changed.

### 2.2.1.2 ESAM officially enabled terminal

ESAM officially enabled terminals can log in only after authentication through the security encryption isolation gateway, and their device fingerprint content is more abundant. Therefore, the access of illegal terminals can be completely eliminated through fingerprint comparison. The secret key authentication is required when the terminal goes online for the first time every day. Each time the terminal logs in, it first judges whether the "fingerprint" of the device is correct. If it is not correct, it carries out secret key authentication. If the secret key authentication fails, it issues a work order to confirm on site. The illegal access monitoring process is shown in Figure 2.
2.2.1.3 ESAM not enabled terminal
If the ESAM is not enabled, the ESAM will be formally enabled if the enabling conditions are met. After the ESAM is enabled successfully, the processing flow is shown in Figure 2. If ESAM is not enabled successfully, add the terminal to the early warning terminal list for key monitoring. The monitoring process is the same as that of the terminal without the secret key. The processing flow is shown in Figure 3.

2.2.1.4 Secret key terminal not installed
Compared with the terminal without ESAM chip, the terminal without secret key has ESAM and can obtain the information of ESAM chip, so its device fingerprint information is relatively rich. This kind of terminal monitoring process is similar to the terminal monitoring without ESAM chip, and the monitoring and comparison information is more[7]. The illegal access monitoring process is shown in Figure 3.
Figure 3. Terminal illegal access monitoring process (Secret key terminal not installed).

- When the master station monitors the meter reading parameter setting triggered by the non-debugging process of the terminal without ESAM chip, or when the terminal version manufacturer code is not in the system code base, or when the sampling monitoring conditions are met (starting from the terminal offline and online, start a research and judgment mechanism within a period of time, and make a research and judgment within a cycle), enter the next step It's a process.
- Call test ESAM chip information, terminal historical frozen data, terminal version, terminal parameters, uplink communication parameters, equipment production date and other data items, and compare with the fingerprint information stored in the master station. At the same time, according to the communication protocol used when calling test data, compare with the terminal protocol type stored in the master station. If most of the comparison results are inconsistent, add the terminal List of suspected illegal equipment.
- According to the list of suspected illegal equipment, the on-site confirmation work order is issued through the closed-loop system to confirm whether the equipment has changed.

2.2.2 Terminal security reinforcement

2.2.2.1 Terminal parameter abnormal monitoring
- Sampling monitoring: Sampling monitoring is carried out for the running acquisition terminal, and the terminal parameters are called to test, and the consistency is compared with the parameters stored in the acquisition system. At the same time, it is judged whether the parameters set by the terminal meet the setting requirements, and whether the terminal parameters are abnormal, so as to strengthen the monitoring and management of abnormal acquisition terminal parameters[8]. The verification parameters include communication parameters of uplink communication port, authentication parameters of uplink communication message, configuration and setting parameters of
event record, etc. The sampling monitoring process of terminal parameter abnormality is shown in Figure 4.

- **Trigger monitoring:** When the monitoring module receives a security event with potential risk of modifying the terminal parameters, it will monitor and verify the abnormal terminal parameters. The security events that trigger terminal parameter abnormal monitoring include: Ethernet remote service port open, remote communication module port open, USB device access, local maintenance port abnormal, serial port login console, Ethernet login console.

| Monitoring module                                      | Master System                          |
|--------------------------------------------------------|----------------------------------------|
| Establish sampling monitoring files                    | Task distribution service              |
| Terminal sampling monitoring                            | Interface data return                  |
| Task distribution data return service                   | Call interface                         |
| Statistics and induction of sampling results            | Call interface                         |
| Display of sampling results                            | Call interface                         |
| Is there any abnormal terminal                         | Call interface                         |
| No                                                      | Task distribution service              |
| Yes                                                     | Interface data return                  |
| Sampling monitoring of abnormal terminal manufacturers  | Call interface                         |
| Task distribution data return service                   | Call interface                         |
| Statistics and induction of sampling results            | Call interface                         |
| Display of sampling results                            | Call interface                         |

Figure 4. Sampling and monitoring process of terminal parameter abnormality.

### 2.2.2.2 Terminal private upgrade monitoring

In order to strengthen the legitimacy and version management of terminal operation software, all terminal operation software (including upgrade packages used for centralized upgrade) must be filed in the master station. The filing contents include: software program file / upgrade package, software version number, version date, software verification code, etc. Among them, software check code refers to the code generated by checking the terminal running program file / upgrade file package according to certain check rules (such as CRC check).

The terminal shall support the master station to obtain the software check code or program file of its running program remotely, so as to verify the legitimacy of its running software. New equipment such as energy controller has a unified operating system and embedded security reinforcement app. The security reinforcement app can verify the business application app file and upgrade package, generate the corresponding software check code, and the master station can complete the software comparison by obtaining the check code.
For the terminal in operation, because there is no unified security reinforcement app, the software verification code can not be generated locally (if generated by the terminal manufacturer itself, it is easy to make a fake). The master station can only obtain the software program file of the terminal remotely, generate the software verification code in the master station and compare it with the registered verification code. In order to prevent illegal elements from stealing terminal operation files through this function (network port and local maintenance port are open without security reinforcement upgrade), this function should be extended on the basis of security reinforcement upgrade of terminal in operation and online security monitoring function.

The combination of sampling monitoring and trigger monitoring is used in the terminal private upgrade monitoring, which not only meets the monitoring requirements, but also has little impact on the implementation of the acquisition task.

- Sampling monitoring: The sampling monitoring is carried out for the collection terminal in operation, and the software comparison is carried out between the call test terminal operation file and the master station storage terminal software information (software version number, software verification code and other information), so as to determine whether the terminal has private upgrade, and improve the management and control ability of the terminal operation program version. The sampling monitoring process of private upgrade of terminal is shown in Figure 5.

- Trigger monitoring: When the monitoring module receives the relevant security events, the terminal private upgrade monitoring verification is performed on the acquisition terminal. The security events that trigger the terminal private upgrade monitoring include: USB device access, login console, key directory change.

![Figure 5. Sampling monitoring process of terminal private upgrade.](image)

2.2.2.3 Security incident monitoring

According to the "technical requirements for safety protection and online safety monitoring of acquisition terminal" issued by the State Grid measurement center in 2019, when the acquisition terminal is abnormal, an event should be generated within 2 minutes and reported to the online safety monitoring module.

When the monitoring module receives the reported security incidents, it conducts comprehensive analysis and judgment on the security incidents in combination with the terminal operation information and work order information. When it is judged that the safety event is generated in the process of work order maintenance, the monitoring module marks the event type information and archives it. When the security risk is low, the marked terminal is a low-risk terminal for continuous monitoring. When the safety risk is high, the monitoring module marks the terminal as a high-risk terminal, initiates the on-site processing work order through the closed-loop system for processing,
and dismantles the terminal when necessary. The following figure shows the processing flow when the terminal key directory file change event occurs.

2.2.2.4 Temporary authorization of terminal maintenance port

In order to ensure the safety and controllability of the acquisition terminal, all maintenance operations for the acquisition terminal should be carried out in the authorized state. Through the authorization management function, it can realize the operation of opening and closing the terminal maintenance port, record and trace the authorization history information.

There are two ways to enable the temporary authorization function of on-site maintenance of acquisition terminal: master station authorization and on-site service terminal authorization. When the on-site operation and maintenance personnel need to use the maintenance port to operate the terminal, they apply for authorization from the closed-loop system. The closed-loop system forwards the application to the monitoring module. The monitoring module carries out port authorization. After receiving the instruction, the acquisition terminal starts the authorization and starts the authorization countdown. If the authorization of master station is not successful, the field service terminal will send the command to start the authorization through infrared / 485 and tell the authorization record to the monitoring module[9]. After the completion of on-site maintenance, the authorization closing instruction is issued, and the temporary authorization ends.

Automatically turn off authorization after timeout: after the acquisition terminal turns on the authorization, if the authorization time is up, the acquisition terminal automatically turns off the authorization, and the temporary authorization ends.

3. Conclusion

This paper is based on the situation of the acquisition terminal in operation, combined with the security protection requirements of the user acquisition system, using big data analysis, artificial intelligence and other technologies to realize the security access detection and protection of the terminal without additional equipment, which has realistic economy and feasibility.

3.1. Feasibility

- By enabling the security mode of the acquisition terminal, it is the most efficient and controllable way to directly block the illegal equipment from the acquisition system. The acquisition system needs to use the existing functions to complete the key download of all ESAM chip equipment and the parameter setting of the security mode enabling. It needs to conduct on-site troubleshooting for individual failed equipment to reduce the on-site workload.
- For the equipment lacking ESAM chip, the fingerprint identification technology is used to identify the suspected illegal terminal and conduct investigation and treatment. The Metrology Center reviews the treatment results to ensure the timely detection and treatment of hidden dangers and minimize the access operation time of illegal terminal until it is eliminated.

3.2. Economy

- Using the existing terminal security mechanism, combined with the acquisition security protection architecture system, to achieve the security access of the terminal without adding additional security equipment and large-scale upgrade for the equipment with EASM conditions, which has a good economy.
- For the terminal without ESAM conditions, using the big data analysis ability and artificial intelligence analysis ability of the user acquisition system, under the premise of not installing equipment and upgrading the terminal, through the use of equipment fingerprint technology, the safe access detection and protection of the terminal in operation can be realized.

Acknowledgements

This work is supported by Science and Technology Project of SGCC. (5700-202055171A-0-0-00)
References

[1] Ziquan Gao, Analysis of common faults of acquisition terminal in power consumption information system, Communication world (2014), p. 45-46.

[2] Fusheng Wei, A fault diagnosis system of power consumption information acquisition terminal, Seminar on power system safety technology of China Society of Electrical Engineering (2013), p. 98-103.

[3] Yun Feng, Trusted power consumption information acquisition terminal based on domestic password, Rural electrification (2018), p. 55-58.

[4] Diwen Lu, Research and implementation of secure access method for IOT devices based on device fingerprint, Electronic design engineering (2019), p. 136-140.

[5] Junzhi Niu, Research and application of cryptography, Computer knowledge and technology (2005), p. 66-68.

[6] Xinming Yi, Research on IP video private network access detection scheme based on device fingerprint decision tree classification, Information network security (2016), p. 68-73.

[7] Yanhao Wang, Research and implementation of device fingerprint identification technology. Nanjing: Southeast University, 2015.

[8] Xinming Yi, Research on IP video private network access detection scheme based on device fingerprint decision tree classification, Information network security (2016), p. 68-73.

[9] Bo Yang, Trusted mobile terminal cloud service security access scheme based on TrustZone, Journal of software (2016), p. 1366-1383.