The Research on Security Access Control Method of Power Intranet Terminal

SHAO Zhipeng[1, a], CHEN Huazhi[2,b] and Li Weiwei[1,c]

[1] State Grid Smart Grid Research Institute, Nanjing 210003, China

[2] Electric Power Research Institute of State Grid Zhejiang Electric Power Company, Hangzhou 310000, China

[a]shaozhipeng@epri.sgcc.com.cn, [b]chz6719@163.com, [c]liweiwei@epri.sgcc.com.cn

Keywords: terminal security; access control; authentication.

Abstract. With the acceleration of power information construction, the need of intranet security construction is increasingly. How to build a credible and controllable information intranet become more and more intractable. This paper focus the source of security problem-terminal, puts forward a new method for security access control of power intranet terminal, reflects the combination of terminal security measures and network access control means, realized a better credible and controllable intranet.

Introduction

At present, power enterprises construct internal network to support themselves' information construction, physical isolation is achieved between internal network and Internet, with the expansion of the internal network construction's scale, the information security problems are increasing[1-2]. Currently, the majority of network security preventive emphasis come from external network, people develops and applies such hardware technology as firewall, IDS, IPS, VPN, antivirus software. Even though these technologies' arrangements cost too much, these preventive measures are not enough to coping security problem originate from the interior of enterprises. It is proved that insecurity factors at the interior of enterprises are the biggest threat to affects the power gird's steady operation. And it is also a hard problem that internal security manager of power enterprises are faced with.

However, research on internal network security should return to terminals, the source which harms information security. The focus terminals types of power gird include: slave station terminals of distribution network; office computer terminals of information internal and external network; mobile operation terminals; information collection terminals and so on. For terminals which access internal network, invalid terminals should be stop to access internal network, restricting user's safety behavior, reinforcing terminals' access control.

Present situation analysis of terminals access

Currently, in terms of internal network of power enterprises, although it is separated from Internet on the whole, it will suffer a series of network harm such as virus, bugs. Once internal network is under attacking, economic benefits and social influence is enormous. The popular security problem encountered by terminals as follows[3]:

(1) Terminals access internal network fail to pass identity authentication, and visiting external network illegally;
(2) Internal network terminals that justified security strategy are occupied illegally, unauthorized visits to information internal network;
(3) Internal network terminals that justified security strategy visit illegal net section;
(4) Internal network terminals that justified security strategy still visit Internet at the state that not justified security assessment results;

(5) Internal network terminals visit illegal website, suffering threats such as virus, Trojan Horse, worm;
(6) Internal network terminals download by P2P, cause inefficient waste of bandwidth;
(7) Internal network terminals listen in to other legal terminals' authentication information. And Disguised as legal terminals after get information, visiting application system illegally;
(8) Internal network terminals modify IP address optionally, to avoid audit.

To analyze the security problems specific as above, the major reasons as follow:

(1) The lack of unified management ;
(2) Illegal access;
(3) Illegal external connection;
(4) The abuse of mobile devices;
(5) The use of loopholes in the system.

Control method of security access

Terminals security access control combines a series of terminals security protection measures and identify authentication such as terminals security monitoring, terminals security evaluation, terminals security reinforcing and a series of network access control measures such as access control, both of which have the characteristic of active defense. Its main way of thinking is: terminals test with the security strategy which is made beforehand before requesting access internal network, and it must accept terminals safe state evaluation, only the security strategy justified terminals should be allowed access network and vice versa. Meanwhile taking the terminals not satisfied with the security strategy into the area of security repairing, or deciding the access permission by the test results.

Terminals access control methods as follow Fig 1

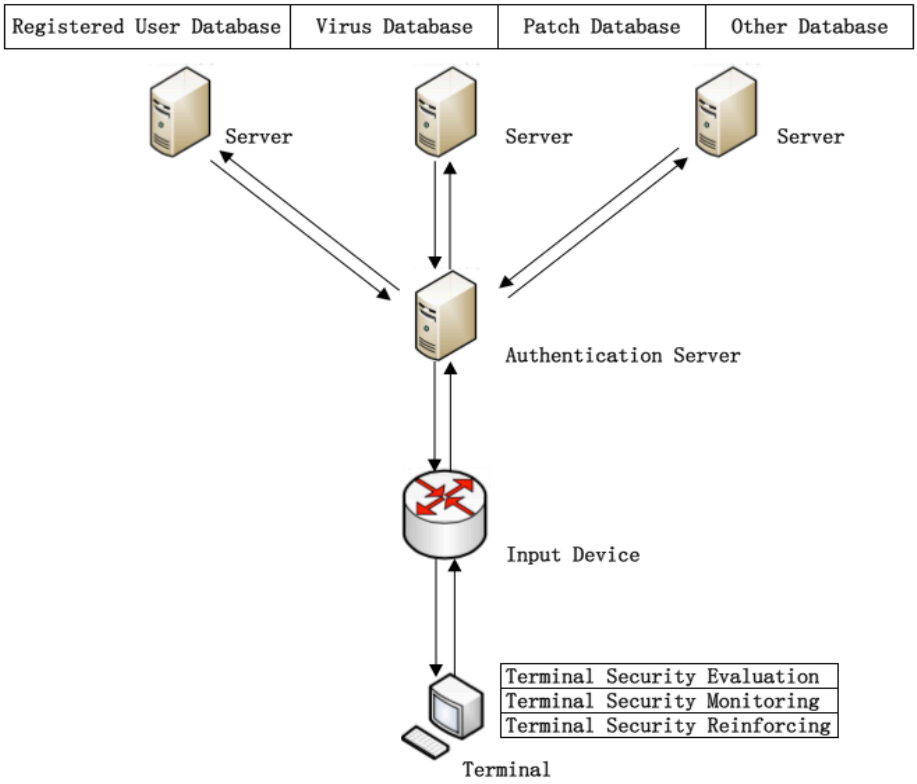

Fig1 network access control method

(1) terminals security evaluation

Terminals security evaluation mode is designed to get security evaluation of terminals by evaluate terminals secure, it can understand the security of terminals in time.

(2) terminals security monitoring

Integrate their original function on condition that open architecture environment, and analyzing all information offered by monitoring and auditing tools by comprehensive connection. Get more

convictive and evidently comprehensive auditing result by analyzing and auditing the monitoring information.

(3) terminals security reinforcing

Data prevent leakage system can reinforce terminals, preventing network confidential information leakage, ensuring data security. Data security usually consists three aspects: local-storage data security, mobile storage data security, temporary data security.

Design discipline. To design security access control method applies to power grid terminals, the balance should be reached between security and serviceability, optimizing the internal network information dealing. Meanwhile, the design of security access control method should follow international and domestic security management experience, security method of design should “keep up with the times”, key technology should “guarantee is in place”. The design of security access control method should revolve around terminals security state detection. Access period as Fig 2

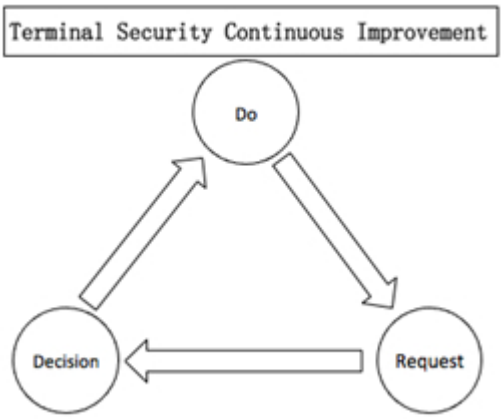

Fig 2 ”Request-Enforcement-Decision”cycle

The period of this method consists Request- Do-Decision three aspects. After terminals Request, combines terminals security monitoring, terminals security evaluation, terminals security reinforcing. Testing security state of terminals, then making strategy decisions rely on testing results and security strategy, and implement decisions, terminals only accord with security strategy can be allowed to access internal network and achieve the internal network access authority. Periodic terminals testing should be executed so as to ensure terminals which have access internal network in a safe state. This is a continuous cyclic process and continuous improvement. The process is activated when period time or security state of terminals are changed

Method design.

(1) Logical structure

In the design of this method, terminals and protected internal network server isolates by device. Internal network resource can be access when terminals satisfy security strategy. Internal network can be divided into three areas from the logic: normal working area, access isolation area, security repair area. Logical structure as Fig 3:

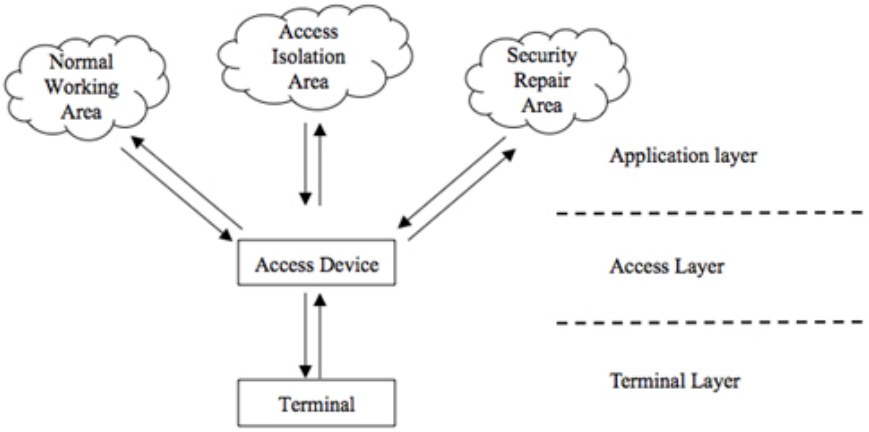

Fig 3 The logical structure of terminal access to internal network

Divided into three layers:

1) Application layer: includes registered users database, virus database, patch database, information processing center.
2) Terminal layer: detecting and collecting terminals security state information, receiving security strategy and executing corresponding action are the concern of it.
3) Access layer: terminals access internal application by access devices, it can be design for accord with system concrete module.

(2) Operation process

Firstly, terminals security access should authenticate terminals' identity legally, terminals not pass the identity authentication can not access internal network, otherwise, puts it into the security repair area, reinforce terminals until satisfy security strategy.

Terminals access internal network flow chart as Fig 4:

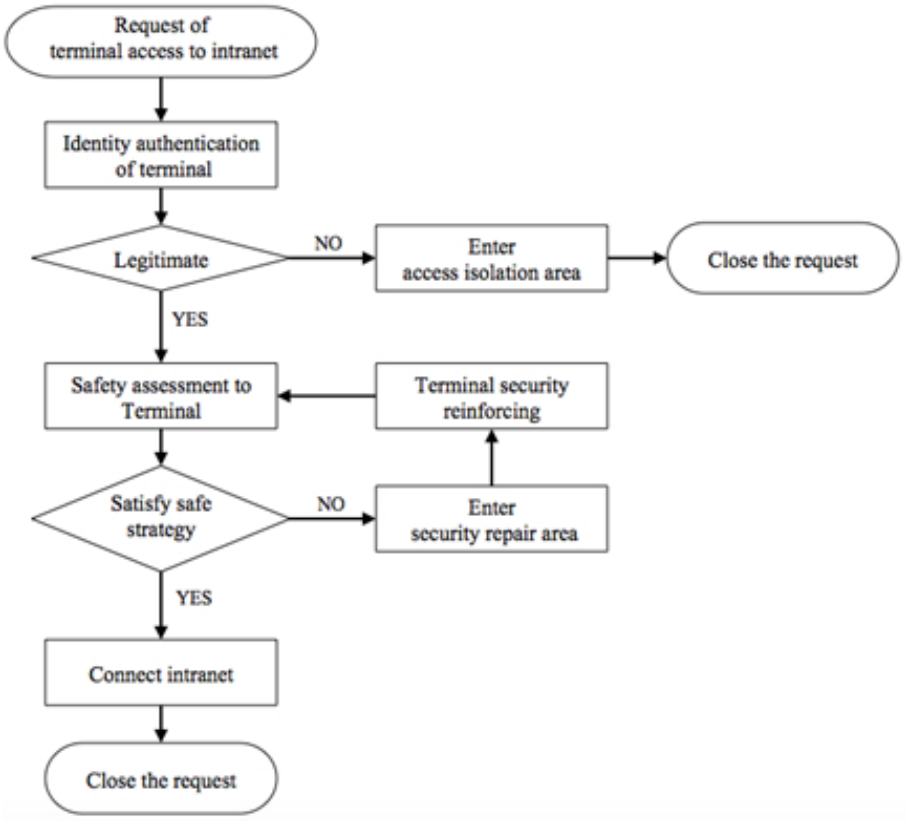

Fig 4 The operation process of terminal access to internal network

3) Access procedures

Terminals security access control method design by this paper. Reinforcing terminals security of access internal network and guaranteeing the trustworthy and controllable by checking, isolating, repairing, management and monitoring to terminals access.

The concrete access procedures as Fig 5:

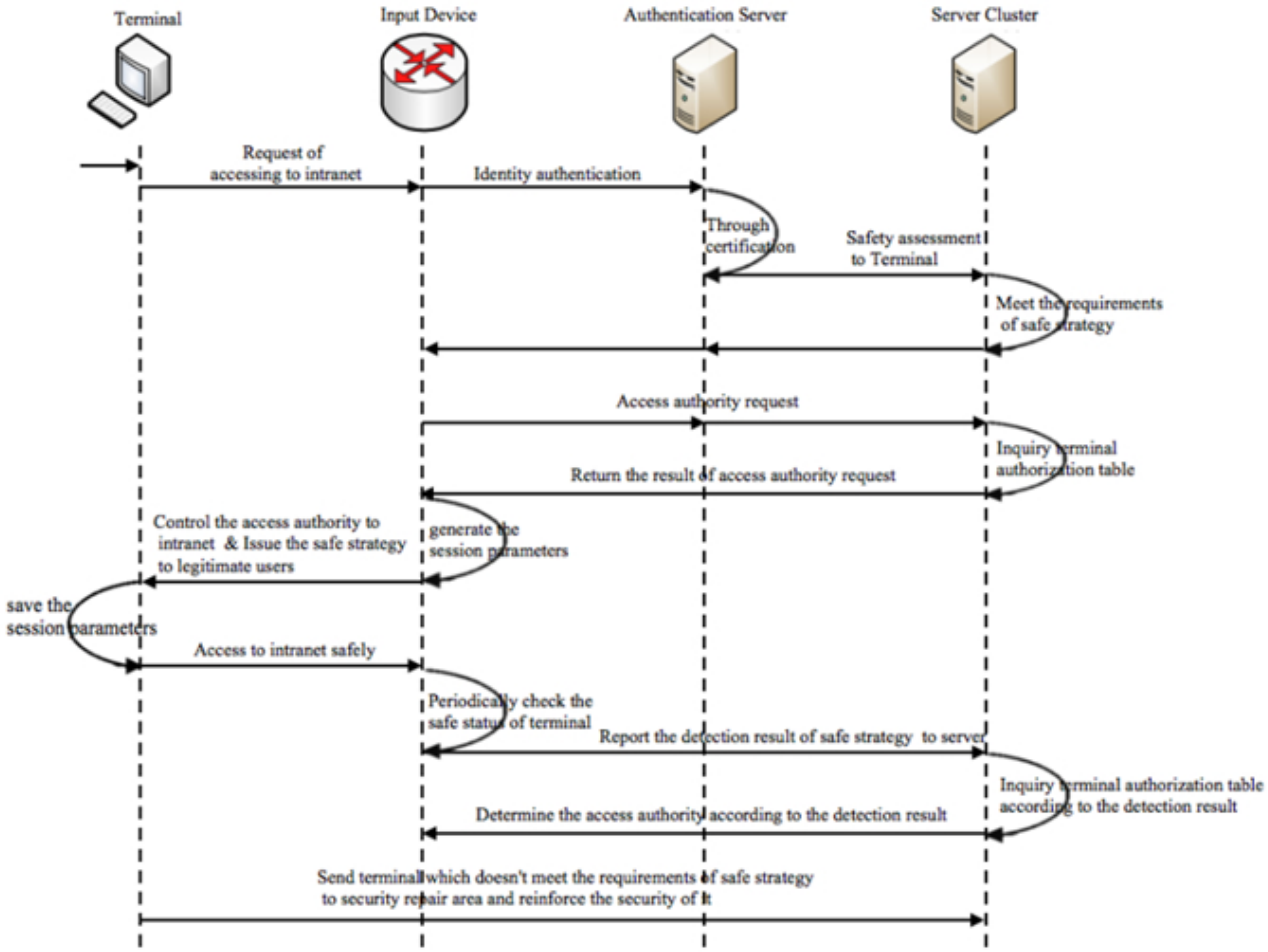

Fig 5 Terminal access procedures.

Conclusion

In order to solving the power enterprise's internal network security problem better, terminal access control should be achieved by source. This paper design a terminal security access control method, terminals' security access control implements from terminal layer, access layer, application layer. Terminal security is essential issues, network access control is means, it has the characteristic of active defense, achieving controllable of internal network.

References

[1] Rigney C, Rubens A, et al. Remote Authentication Dial In User Service(RADIUS)[Z]. IETR RF2865, June 2000.

[2] L Harn, H Y Lin. Integration of user authentication and access control[J]. Computers and Digital Techniques. IEEE PROCEEDINGS, 139(2): 139-143.

[3] Matthew J, Moyer and Mustaque Ahamad. Generalized Role-Based Access Control[C]. In Proeeedings of the 21st intimation conference on distributed computing systems. 2001:391-398.

[4] YE Xiaorong, SHAO Qing: Mobile Government System Based on the Android Platform, Science & Technology Review, Vol.29, No.21 (2011), 27-30.

[5] QIAN Yi: Design Scheme of Wireless Perambulation Terminal for Power Communication Based on Android, Journal of Electric Power, vol.26, No.1 (2011), 60-63.