Study About the Trusted and Controllable Technology of the Information Network

Yu Wang
Department of Information Equipment
Equipment Academy
Beijing, China
zenheart@163.com

Weijie Han
Department of Information Equipment
Equipment Academy
Beijing, China
visc_hwj@126.com

***Abstract*—Firstly, the connotation of the trusted and controllable information network is introduced. Secondly, the key technologies are summarized for realizing the trusted and controllable network. Finally, the mechanism for building the trusted and controllable security architecture for the information network is designed.**

Keywords—information network; trusted technology; controllable technology

I. INTRODUCTION

Compared with the open internet, more strict security measures are applied for protecting the important inner information network, such as physical separation, limitation of the hardware and the software, and integrate of the configuration and the security strategy so on. But the current security architecture cannot meet the demand of the controllable network. Firstly, the integrated communication standard and interface between the security systems is lacking, so the integrated security perception capability is insufficient. Secondly, the interaction capability between the protection system, the detection system and the reaction system hasn't been realized efficiently. Finally, it is difficult to implement the security strategy based on the white-list mechanism because the configuration of the hardware and software of different hosts and servers is not unified and the uncertainty of the information network becomes higher and higher. Currently the efficiency for detecting and protecting the network attack especially the APT is lower because of lacking controllability. So the trusted and controllable capability[1] is studied by this paper aiming for protecting the important inner information network against the network attack.

II. CONNOTATION OF THE TRUSTED AND CONTROLLABLE NETWORK

If an entity acts according to what is expected, the entity is trusted. The trusted prosperity of the information network includes three implications: realizing the traditional network security and insuring the confidentiality, integrity and availability; insuring the authenticity of the users, information and the content; providing the auditability of the entity.[2]

A trusted network is consisted of the trusted devices, architecture, agreement and services. The trusted devices are implemented by TCM (Trusted Cryptography Module) and trust chain mainly. The trusted architecture is realized by dividing the security domain reasonably and deploying the trusted gateway to connect the network and interchange the data. The trusted agreement must be the secure mark-able agreement. The trusted services are realized by the white-list, software sand-box, and the audit mechanisms.

If the pattern of taking use of the information resources by a subject can be controlled, the subject is controllable. If the operation of the system by the users and the interior status transformation are detectable, controllable, auditable, traceable, the system is controllable. The controllable property of the network consists of identification control, cryptography control, access control, content control, structure control and communication control.

It is helpful to improve the capability for detecting and resisting the attack and survivability of the system by enhancing the credibility and controllability of the information network.

III. KEY TECHNOLOGIES OF THE TRUSTED NETWORK

The trusted information network is built by enhancing the credibility of the network terminals by combining the trusted computing technology and the virtual machine technology on one hand, and applying the trusted terminals and gateways based on the virtual technology so as to partition the network security domain dynamically and control the information exchange on the other hand. Furthermore, the terminal equipment which will access the information network should be controlled in order to protect against the virus and Trojan attack and reduce the risk of leakage by controlling the scope where the secret is spreading.

The key technologies for realizing the trusted network include:

(1) The technology for enhancing the credibility of the terminal base on the VM (virtual machine) technology[3]

This technology is realized by enhancing the credibility based on Ukey, PCI-E expansion card and the professional trusted chip and combining with the VM technology in order to implement fine-grained mandatory access control of the

terminals and isolate applications of different security classification.

(2) The technology for enhancing the credibility of the network based on the trusted label

On the basis of enhancing the credibility of the terminal, the trusted labels[4] are added to the packets sent by the trusted terminals, and the added trusted labels will be verified and access controlled by the trusted gateway. The labels are used to realize access control, insure the authenticity of the data, and protect the IP address, port and packet contents from being modified maliciously. Furthermore, the labels can be used to control the net flow and trace the attack source.

IV. KEY TECHNOLOGIES OF THE CONTROLLABLE NETWORK

The major network security control technologies include: structure control technology, encryption control technology, code control technology, net flow control technology, access control technology, authentication control technology, detection response technology, honeypot protection technology, anti-virus technology and fault-tolerant technology so on. The interconnection between the above technologies and the network security control mechanism is shown as Table 1.

TABLE I. THE SECURITY CONTROL TECHNOLOGIES FOR THE INFORMATION NETWORK

Control Technology / Control Mechanism	structure control	encryption control	code control	net flow control	access control	Authenti -cation control	detection response	honey pot protect --ion	anti-virus	fault-tolerant
detection mechanism				√	√	√	√		√	
hidden mechanism	√			√				√		
response mechanism	√						√			
authentication mechanism		√				√			√	
notarization mechanism		√				√				
encryption mechanism		√								
error control mechanism			√	√			√		√	√
route control mechanism				√	√			√		
access control mechanism	√				√			√	√	
net flow control mechanism	√			√	√					√
digital signature mechanism		√				√				
authentication mechanism		√				√				
backup recovery mechanism	√		√	√						√

(1) The structure control technology: The technology aims for analyzing and designing the network topology, and controlling the controllability and visibility of the message. This technology is realized by graph theory and network performance analysis. By this technology, the reliability of the network connection and the continuity of the information link are realized by designing good network topology and information structure. Furthermore, the network security is realized by designing good network layout and connectivity and enhancing the access control between the internal and external network.

(2) The encryption control technology: This technology plays the basis role for the information network security. It aims for producing, storing, allocating, restoring and destroying the cipher codes safely by the data encryption method, encryption/decryption algorithms, and cipher management and distribution technology.

(3) The code control technology: This technology aims for controlling the system logical structure, improving the software quality, and reducing the security risk due to the software vulnerability by analyzing, controlling and restoring the software vulnerability automatically, and designing secure code, and overcoming the buffer overflow so on.

(4) The net flow control technology: This technology aims for improving the security and reliability of the protocol, enhancing the adaptability and invulnerability of the network by filling, hiding and pre-allocating the net flow, and allocating the broadband reasonably.

(5) The access control technology: This technology aims for controlling the access between the users and the network devices, and the users and the information resources. The control mechanisms include the discretionary access control mechanism, the mandatory access control mechanism, and the multi-level access control mechanism.

(6) The authentication control technology: This technology is the prerequisite for realizing the other control. It includes user authentication and information integrity authentication by authentication protocol, one-way and peer-to-peer authentication algorithms, and message authentication technology.

(7) The detection response technology: This technology plays an important role on realizing the secure feedback control, evaluating the effectiveness of the network security and decision-making. This technology is realized by detecting security incidents, evaluating the security effectiveness, the audit technology, the intrusion response technology and the disaster recovery technology.

(8) The honeypot protection technology: This technology is realized by building the virtual machines, the virtual networks, the virtual services, capturing the attack net flow and tricking the attacker, and configuring and managing the honeypot.

(9) The anti-virus technology: This technology involves analyzing and researching the running, spreading, replicating and masking technologies of the virus, Trojan, backdoor and

logical bombs. The anti-virus technology is realized based on the above technologies.

(10) The fault-tolerant and redundant technology: This technology aims for realizing the fault-tolerant and redundant services for the computer system and network system. The redundant backup includes hardware devices, codes, data and services. The fault-tolerant includes codes, data and devices.

V. TRUSTED AND CONTROLLABLE NETWORK SECURITY ARCHITECTURE

Based on the active trust architecture[5], the reliability and controllability of the information network is realized by drawing up the security baseline, controlling the risk in the manageable scope due to the vulnerabilities and capturing the attack effectively. The reliability and controllability depends on trusted computing, trusted label, trusted gateway and virtual technologies. Furthermore, the following measures should be carried out:

(1) The security agent system deployed on the terminal devices should be single-function and can support different services including anti-virus, patches upgrading, security configuration, I/O management and status monitoring so on.

(2) Under permitted conditions, the white-list technology should be applied to the servers to reduce the complexity of the detection and management process.

(3) The information network should be divided into multiple security domains according to the belonged business category and security classification in order to control the access and the information exchange between the domains.

(4) The security control center should be built so as to collect the security logs, alarm and audit information from the terminal devices, servers, network and security systems, and also realize perception and visualization of the network security situation.

The trusted and controllable network architecture is shown as Fig.1. Its key components including:

(1) The security management platform and toolset which include vulnerability management, threat management, personnel management, log management, assets management, identity management, cipher management, authorization management, I/O management and integrated network management so on.

(2) The supporting technologies and software and hardware system which include the trusted computing technology, the virtual technology, the white-list technology and the self-control hardware and software. The trusted computing technology aims for providing the trusted label for the data exchange and controlling the I/O of the terminal devices. The virtual technology aims for realizing enhanced access control and preventing information leakage by isolating the hosts and networks virtually.

(3) The toolset for security detection, compliance detection and attack detection can audit network flow, extract characteristics, detect intrusion, scan and analyze vulnerability, detect communications compliance, analyze malicious codes, analyze system compatibility and conflict, evaluate risks and carry out grade protection assessment. The comprehensive network security situation can be analyzed by the toolset.

(4) The architecture provides the standards and operation regulations according with the security technology.

(5) The architecture provides the integrated security infrastructure for identification authentication and cipher management.

(6) An information security team consisted of security managers, security auditors, security assessors, security professors and security incident response personnel is the most important part of the architecture.

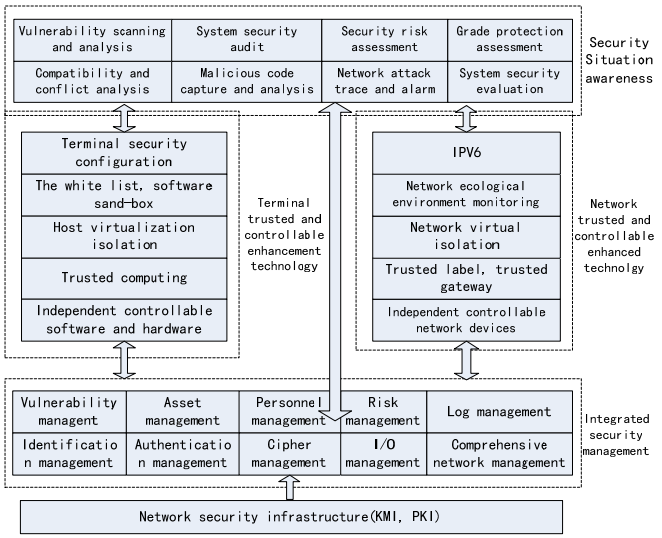

FIG.1 THE TRUSTED AND CONTROLLABLE NETWORK SECURITY ARCHITECTURE

VI. CONCLUSIONS

The network reliability technology and independent controllability technologies play the key role for the network security which complement each other and develop coordinately. The perfect security architecture is built by insuring the reliability of the network system and meeting the demand of the key system on one hand, adopting the independent controllable software and hardware and trusted and controllable technologies based on the defense-in-depth model and dynamical and automatic defense model on the other hand.

REFERENCES

[1] Liu xian Gang, Gong bei. Unified Trusted measurement Model of Trusted Network. 2012 International Conference Control and Electronics Engineering, 1082-1084.

[2] Fuxiong Wang, Ziqian Xiao, Jing you Chen. Research on Security of Trusted Network and Its Prospects. 2010 Second International Workshop on Education technology and Computer Science. 256-259.

[3] Wu Yue, Liu xiang-dong, Duan Yi-zhen. Design and implementation of secure access control architecture of desktop virtualization. Computer Engineering and Design, 2014, 35(5):1572-1577.

[4] Jian wang, Yanheng Liu, Xiangpeng Jia et al. A New Framework for Accessing Trusted Network. 2009 Second International Conference on Intelligent Networks and Intelligent Systems. 189-192.

[5] Yan Xiao xia, Qin Hua. Trusted network framework research and design. Net Security Technologies and Application, 2014(4):163-164.