DOI 10.15302/J-SSCAE-2016.06.011

The Strategy of TC 3.0: A Revolutionary Evolution in Trusted Computing

Shen Changxiang, Zhang Dawei, Liu Jiqiang, Ye Heng, Qiu Shuo

Center of Information Security Architecture in Beijing Jiaotong University, Beijing 100044, China

Abstract: This paper introduces the status, problems, and future strategies of traditional defense systems, analyzes issues in current protection structures and a revolutionary evolution in trusted computing (TC), and proposes the strategy of TC 3.0, which is an active defense architecture based on active immunity. Furthermore, this paper provides an example of TC 3.0 in a cloud computing environment and some advice to enforce active defense.

Keywords: TC 3.0; active defense; active immunity; hierarchical protection; protection structure

1 Introduction

With the continuous change and escalation of cyber attacks in recent years, China's cybersecurity is still a highly important issue. According to the Statistical Report on Internet Development in China issued by China Internet Network Information Center (CNNIC), up to June 2016, China's Internet users have reached 710 million. The Internet penetration rate has reached 51.7% [1,2]. The rapid development of the Internet brings us great convenience. However, security issues have also arisen and have shocking effects. The independent monitoring data from National Computer Network Emergency Response Technical Team/Coordination Center of China (CNCERT/CC) shows that more than 105 000 Trojans and botnet control terminals were found in 2015. The number of Internet malware programs is nearly 1.48 million, an increase of 55.3% compared to 2014. The distributed denial-of-service (DDoS) attack method is changing. During the first three quarters of 2015, the number of DDoS attacks whose traffic used over 1 Gbit/s reached nearly 380 000, for a daily average of 1 491 attacks.

With the development of cloud computing, big data, the Internet of Things, and other emerging technologies, increasing amounts of government, enterprise, university, and individual user information is uploaded into cloud information systems, including information about China's future infrastructure system, people's livelihoods, and the survival of enterprises. If the loopholes in these systems were found and exploited, the consequences would be unbearable. Traditional passive defense systems are obviously too weak to defend against such attacks [3–5]. It is imperative to construct active defense systems.

2 Problems in the construction of traditional defense systems

With the implementation of hierarchical protection work in 1994, the hierarchical protection system has become an important basis for China's cybersecurity protection systems, and has achieved great success. However, there are still some problems in the construction of the current hierarchical protection.

(1) Security managers have inadequate attention in the hierarchical protection system

This is mainly shown in the following aspects: a lack of knowledge among security managers, lack of prevention awareness, lack of standard management and methods, and simple work habits. Because of the lack of standardized security technology management tools and the diversity of attacks, even with the establishment of good corresponding safeguards, there are still loopholes in normal management. All of these issues affect

Received date: 12 October 2016; revised date: 18 October 2016

Corresponding author: Shen Changxiang, Chinese Academy of Engineering, Academician. Major research field is information security. E-mail: 13911888336@163.com

Funding program: CAE Major Advisory Project "Research on Cyberspace Security Strategy" (2015-ZD-10)

Chinese version: Strategic Study of CAE 2016, 18 (6): 053–057

Cited item: Shen Changxiang et al. The Strategy of TC 3.0: A Revolutionary Evolution in Trusted Computing. *Strategic Study of CAE*, http://10.15302/J-SSCAE-2016.06.011

the comprehensive implementation of an information security hierarchical protection system [6].

(2) The security foundation is not controllable, and active defense is missing

The core of the current information security approach is active defense. Hierarchical protection is more like a pre-means of protection. Passive protection measures are always palliatives. Because many security products rely on the operating platform, this security mechanism is easy to bypass, so it is difficult to protect such information systems from the source security [7].

(3) Technical standards are out of date

With the development of cloud computing, the Internet of Things, and big data, the convenient services provided by the emerging technology industry are popular among enterprises and ordinary users. The large market potential brings about formidable security issues. With the level of policy standards regarding hierarchical protection lagging behind, it has been difficult to meet the information security needs of the application of new technology [8].

3 TC 3.0: construction of an actively immune defense system

The development of trusted computing (TC) has gone through several stages. The original TC 1.0 was based on computer reliability, and mainly used in troubleshooting and redundant backup, which are safety precautions based on security measures. TC 2.0 was developed while the Trusted Computing Group (TCG) was introducing the trusted platform module (TPM) 1.0 standard. TC 2.0 mainly uses a hardware chip as the root of trust, the credibility of measurement, trusted storage, and trusted reports as the means to achieve stand-alone computer protection. The downside is that because security issues are not considered at the computer architecture level, it is difficult to achieve active defense. China's trusted computing technology has been developed to the 3.0 phase, the "active defense system." TC 3.0 ensures that the entire process can be measured and controlled without human intervention, that is, a defense and computing parallel "actively immune computing model [9]."

TC 3.0 has formed a system of independent innovation in many areas to carry out the scale of the application. China has made great achievements after years of research, including the innovation of the platform cryptography scheme; the proposal of the trusted cryptography module (TCM), which adopts a national self-designed algorithm and the double-certificate structure; the proposal of the trusted platform control module (TPCM), which is embedded into the trusted root as an autonomous and controllable trusted node, and starts before a central processing unit (CPU) startup and performs basic input/output system (BIOS) validation; the addition of the trusted metrics node to the trusted platform motherboard, so that the host and the trusted node ensure the construction of a trusted chain once the power is on; the proposal of the framework of trusted base support software, which adopts the dual-system architecture of the host software system and trusted software base; and the proposal of the trusted connection framework, based on a three-ternary peer-to-peer design, which improves the overall credibility, security, and manageability of the network connections. Innovation can be summed up in six phrases: independent cryptography-based, controllable chip as a pillar, dual-functional motherboard for the platform, trusted software as the core, peer-to-peer network as a link, and ecological application into the system.

At the same time, after years of technical research and application demonstration, TC 3.0 already has the conditions for industrialization. The TC 3.0 standard system gradually completes, and the related standard-setting units are more than 40, covering the chips, complete machines, software, and network connections. With more than 40 authorized patents, the standard innovation points have been technically validated, resulting in strong support for industrialization. In 2014, the Zhongguancun Trusted Computing Industry Alliance (z-TCIA) was established to promote the industrialization of TC 3.0. The alliance has more than 180 member units, and is composed of 13 professional committees, related to the domestic trusted computing industry chain of all links, with a wide range of representation, covering the industries, universities, research institutes, and users with all walks of life. TC 3.0 has successful applications in some implementations of key information infrastructure security. Trusted computing technology products with the ability of active defense have also been applied to closed-circuit TV (CCTV) systems, the national power grid dispatching system protection, and other systems, successfully building a defense system in line with the fourth level of hierarchical protection.

4 Application of the TC 3.0 active defense strategy in cloud computing

According to the ideas described in the previous section, we propose the "trusted computing as the foundation, access control as the core, constructing the triple framework of active immunity protection under the trusted security management center's support" implementation plan. The framework is shown in Fig. 1.

The framework uses active immunity technology as the core, and it centers on the trusted security management center to build an active defense system in depth. This defense system is composed of trusted computing environment, a trusted boundary, and trusted network communication. This framework establishes strategic linkages between protection mechanisms, response mechanisms, and audit mechanisms at various levels in the defense system.

Cloud computing is a kind of dynamically scalable virtualization resource, which is provided to the user through the Internet network. The security risk of cloud computing is caused by its own technical characteristics and service modes. At present, trusted computing serves in two main aspects of cloud security. First, it ensures the reliability of the security mechanism of nodes in the cloud and prevents the security mechanism from being destroyed or tampered with; second, it provides trusted coordination for security mechanism, integrating different security mechanisms together to serve the cloud security [10].

The trusted cloud architecture can provide trusted computing support for the security mechanism in the cloud environment. Specifically, the construction of a trusted chain in the cloud environment provides a reliable guarantee for the virtual operating environment; the establishment of monitoring technology based on a trusted third party can effectively monitor the implementation of cloud services, which could solve the problem of lack of trust in cloud services; isolation technology based on trusted root support, where multilayer isolation defense built in a cloud environment cannot be bypassed, providing security and trusted isolation environment for cloud tenants; and trusted access technology that can provide reliable access to the cloud environment and help a cloud platform to solve problems due to its openness [11].

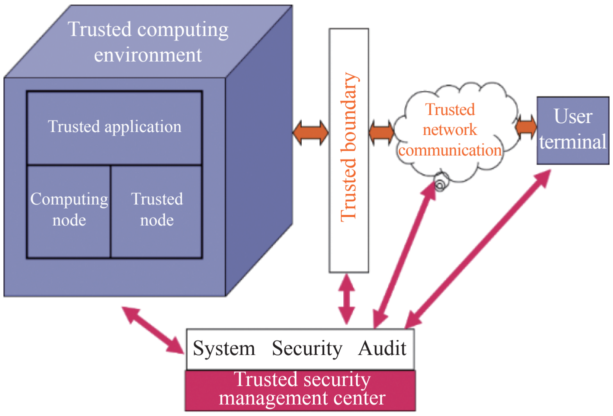

Fig. 1. Triple framework of active immunity protection.

The trusted cloud architecture is a distributed trusted system consisting of a cloud environment security management center, host, virtual machine, and cloud boundary equipment on different nodes' trusted root, trusted hardware, and trusted software. They connect to each other over a trusted connection. The trusted cloud architecture supports the security of cloud environment, and provides users with trusted services. In general, the trusted cloud architecture must be connected with a trusted third party, and trusted services acknowledged by the cloud service providers and cloud users should be provided to by the trusted third party. In addition, the trusted third party monitors the trusted cloud environment. The security architecture of the trusted cloud computing system is shown in Fig. 2 [12].

In the trusted cloud architecture, the security mechanisms and trusted functions of each node are different, so the trusted functions implemented by basic trusted software are also different. These trusted functions cooperate with each other to provide the overall credibility of the cloud environment support function. The functions of each security component in the architecture are as follows.

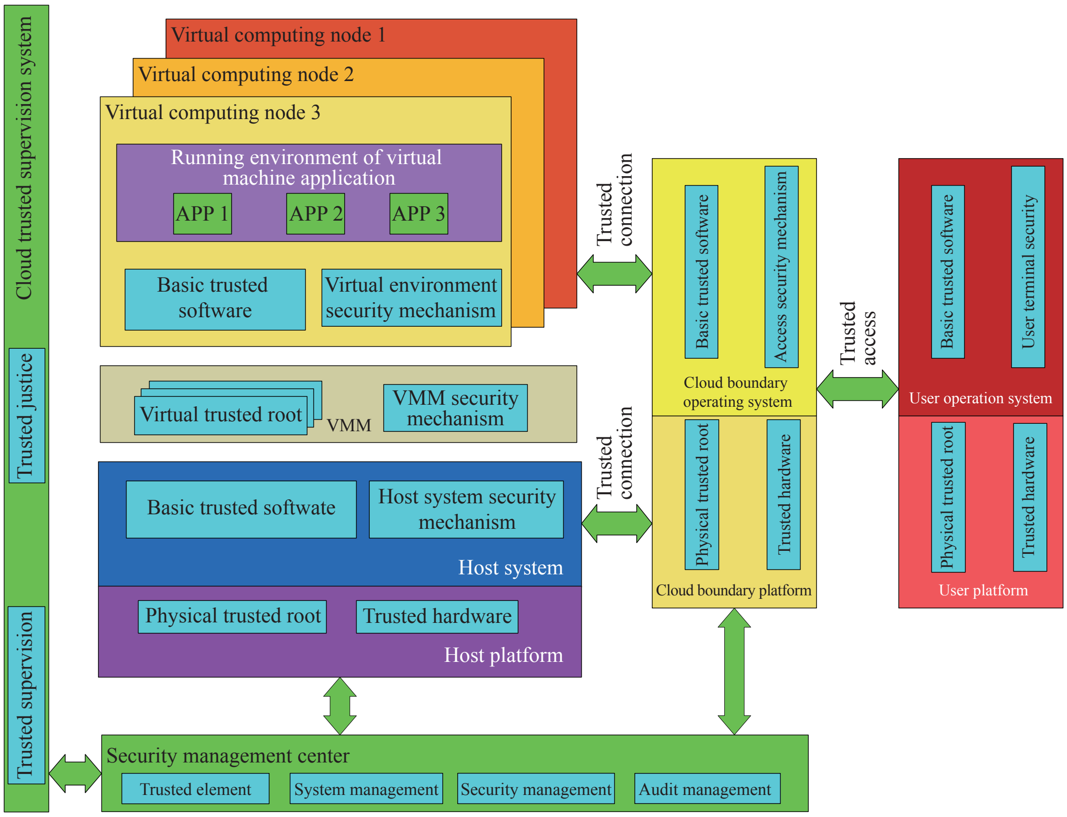

Fig. 2. The security architecture of the trusted cloud computing system. VMM: virtual machine monitor.

(1) Security management center

The security management center runs the application of cloud security management, including the system management, security management, and audit management mechanisms. The basic trusted software in the security management center is the management center of the trusted cloud architecture. It can monitor the security management behavior and connect to the basic trusted software in each node of hosts to achieve system security.

(2) Cloud boundary equipment

The operating environment of cloud boundary equipment has access to security mechanism. The coupling of the basic trusted software and the boundary security access mechanism ensures the credibility of the security access mechanism. At the same time, the software can provide trusted identification and trusted verification services to the boundary security access mechanism.

(3) Host

The trusted support mechanism for the basic trusted software of a host must ensure the security mechanism of the host and the virtual machine is safe. In addition, it should provide a virtual trusted root for the virtual machine. The active monitoring mechanism of the host security mechanism is equivalent to a trusted server of cloud environment. It receives the trusted management strategy of the cloud security management center and localizes the strategy. It also provides trusted services to the virtual environment on the basis of trusted strategy.

(4) Virtual machine

The basic trusted software in the virtual machine provides support for its own trusted security mechanism. Meanwhile, it actively monitors the cloud application running environment in the virtual machine. The virtual machine, host, and the basic trusted software in the security management center constitute a ternary distributed trusted cloud architecture, including a user terminal, a proxy server, and a management center.

(5) Trusted third party

The trusted third party is acknowledged by cloud service providers and cloud users. It can refer to a governmental cloud computing supervision department and evaluation and certification center. The trusted third party provides credible and fair services and credible monitor functions for the trusted cloud architecture.

(6) User trusted terminal

The cloud user terminal can also install the basic trusted software and construct the trusted computing base. A user terminal that installs the basic trusted software and constructs the trusted computing base can be regarded as a trusted user terminal.

5 Countermeasures and suggestions

China's General Secretary Xi Jinping pointed out that cybersecurity is dynamic rather than static. China needs to establish a dynamic and integrated protection concept. To implement the "cyber power" strategic thinking, China needs to change the traditional theory of cybersecurity protection, actively adapt to the dynamic characteristics of cybersecurity, and on the basis of the hierarchy protection concept in active defense thinking to build an active defense system characterized by active immunity.

5.1 Achieve the transition from passive protection to active defense; integrate active immunity with hierarchical protection

The main characteristic of today's information security is establishment of an active defense system in which hierarchical protection is a pre-protection approach. However, these passive protection measures are palliatives, and cannot match the current information security requirements with real-time and active defense. TC 3.0 can achieve active immunity of computer system. Like the human body's immune mechanism, it can identify "self" and "non-self" in real time, which prevents vulnerabilities from being used by the attacker. Therefore, the traditional triple protection can be upgraded to the triple protection in trusted environment which consists of the trusted computing environment, trusted boundary, and trusted communication network. In this way, a proactive defense system with active immunity can finally be constructed.

5.2 Establish the technical support system of cybersecurity; improve the formulation of new trusted defense standards

With technology changing rapidly, it is difficult to meet the requirements of information security because the current protection policy of cybersecurity is lagging behind. For example, new applied technologies (such as the Internet of Things, cloud computing, and mobile Internet) are currently exhibiting new features that inform new security requirements. The government, finance industry, energy industry, and manufacturing industry, who are accustomed to being isolated, are now connected to the Internet more frequently. From the aspect of computing resources, the applications of cloud computing have exhibited multiple features such as the disappearance of the boundary, dispersion of services, and data migration, which cause business applications and information data security to face more complex problems. From the aspect of user terminals, the popularity of the mobile Internet and intelligent terminals have engendered new challenges for information security management.

Establishing the hierarchical protection technology standards of cloud computing, big data, the Internet of Things, industrial systems, and other new information systems can improve the technical support of the entire procedure (implementation, classification, evaluation, and management) which is of utmost priority. Then, the goals that attackers cannot get in, unauthorized information cannot go out, stolen information cannot be read, system information cannot be changed, system service cannot be paralyzed, and attacks cannot be allowed can be achieved. Finally, the effect that "to be actively immune is simply to be effectively protected" can be obtained.

5.3 On the basis of China's national conditions, seek for appropriate safety to gradually develop and improve active defense system

During the transition from passive protection to trusted active defense, China should be patient and insist on the correct techniques according to national conditions, and then make a strong foundation with appropriate safety to gradually develop and improve active defense system.

References

[1] Shen C X. Construction of the active defense and comprehensive prevention protection system [J]. Information Security and Communications Privacy, 2004, 2 (5):1–3. Chinese.

[2] China Internet Network Information Center (CNNIC). The 38th statistical report on internet development in China [EB/OL]. (2016-08-03) [2016-10-08]. http://www.cnnic.net.cn/hlwfzyj/hlwxzbg/hlwtjbg/201608/t20160803_54392.htm. Chinese.

[3] Shen C X. Cloud computing security and hierarchical protection [J]. Information Security and Communications Privacy, 2012 (1): 16–17. Chinese.

[4] Shen C X. Building a defense security system with trusted computing [J]. Information Security and Communications Privacy, 2016 (6): 34–34. Chinese.

[5] Shen C X, Zhang H G, Wang H M, et al. Research and development of trusted computing [J]. Scientia Sinica Informationis, 2010, 40 (2): 139–166. Chinese.

[6] Zhang W L. Discussion the status of information security base on graded protection [J]. Information Security and Technology, 2014 (9): 9–13. Chinese.

[7] Song Y W, Ma Q D, Zhang J. Information security level protection policies and standard system [J]. Information and Communications Technologies, 2010, 4 (6): 58–63. Chinese.

[8] Shen C X. The rectification routes of hierarchical protection [J]. Netinfo Security, 2008 (11): 14–15. Chinese.

[9] Shen C X. Developing the trusted computing technology and industry [J]. Information Security and Communications Privacy, 2007 (9): 19–21. Chinese.

[10] Shen C X. The Security of Cloud Computing [J]. Information Security and Communications Privacy, 2010 (12): 12. Chinese.

[11] Shen C X. Independent innovation to accelerate the development of trusted computing [J]. Network and Computer Security, 2006 (6): 2–4. Chinese.

[12] Shen C X. Building a cyberspace security system with trusted computing [J]. China Information, 2015 (11): 33–34. Chinese.