DOI 10.15302/J-SSCAE-2016.06.012

TC Assurance Architecture for Cybersecurity Infrastructure Based on Active Defense

Zhang Dawei, Shen Changxiang, Liu Jiqiang, Zhang Feifei, Li lun, Cheng Lichen

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

Abstract: This paper introduces the status, problems, and future strategies of the cyberspace security infrastructure system, and proposes that cyberspace security infrastructure must be based on active defense. Therefore, this paper proposes several suggestions for a trusted technology insurance system, which include the following: In order to build a trusted technology insurance system, independent innovation in active defense must be the breaking point; key information security systems must be developed by local institutions; independent innovation must be increased; research, product development, and active defense applications must be promoted; the development of trusted computing standards must be promoted; and experimental demonstrations must be carried out.
Keywords: active defense; active immunity; trusted computing; trusted technology insurance system; cybersecurity infrastructure

1 Introduction

With the rapid development of both cyber technology and "Internet Plus" applications, economic and social development is increasingly dependent on information networks and important information systems. The Internet is widely used in information management by governments, societies, and individuals in political, financial, and military fields. Cyberspace security has inevitably become a new topic of national security in this world.

From the late 1990s to the early 21st century, the US information security strategy has aimed to maintain the confidentiality, integrity, availability, and controllability of information security. It has also become an official part of the national security strategy. From 1998 to 2012, the US National Security Agency had developed the Information Assurance Technical Framework, which proposed the Defense-in-Depth strategy using multi-layered, in-depth security measures to protect user information and information system security. In 2005, the US President's Information Technology Advisory Committee (PITAC) submitted a report entitled "Cyber Security: A Crisis of Prioritization." It asserted that the safety construction of short-term redeeming in cyberspace did not solve the fundamental problem of security and was cost-effective but flawed. The US INFOSEC Research Council (IRC) published the Federal Plan for Cyber Security and Information Assurance Research and Development in April, 2006. It proposed modifications to the inexhaustible patching strategy of passive sealing. After President Obama took office in 2008, International Strategy for Cyberspace, National Cybersecurity Protection System, Cybersecurity National Action Policy, Improving Critical Infrastructure Cybersecurity, Critical Infrastructure Security and Resilience, and other policies to further enhance the active defense capacities of cyberspace were released successively. In terms of cyberspace security, the EU has also formulated a series of policies and standards. Council Decision 92/242/EEC in the area of security of information became the starting point for the European information security legislation in 1992, after which the EU promulgated Council Resolution on A Common Approach and Specific Actions in the Area of Network and Information Security, Commission on Critical Information Infrastructure Protection—Protecting Europe from Large Scale Cyber-Attacks and Disruptions: Enhancing

Received date: 12 October 2016; **revised date:** 18 October 2016
Corresponding author: Zhang Dawei, Beijing Jiaotong University, Associate Professor. Major research field is information security. E-mail: dwzhang@bjtu.edu.cn
Funding program: CAE Major Advisory Project "Research on Cyberspace Security Strategy" (2015-ZD-10)
Chinese version: Strategic Study of CAE 2016, 18 (6): 058–061
Cited item: Zhang Dawei et al. TC Assurance Architecture for Cybersecurity Infrastructure Based on Active Defense. *Strategic Study of CAE*, http://10.15302/J-SSCAE-2016.06.012

Preparedness, Security and Resilience, A Strategy for A Secure Society, and other initiatives. These policies effectively ensured information security throughout the EU.

In China, the term "important infrastructure network" mainly refers to telecommunications, broadcasting, railway, banking, customs, taxation, civil aviation, electricity, securities, insurance, and other important systems used by domestic industries. Currently, the protection of critical infrastructure network is based primarily on the protection of national information system grading standards. Among these, the Information Security Technology—Classification Guide for Classified Protection of Information System Security (GB/T 22240–2008) stipulates that current information security protection is divided into five levels; the Information Security Technology—Baseline for Classified Protection of Information System Security (GB/T 22239–2008), which determines the basic technical requirements for cybersecurity and management; and the Information Security Technology—Technical Requirements of Security Design for Information System Classified Protection (GB/T 25070–2010) determines the requirements of security design for Internet network information system and serves as the foundation of the technology framework of China's cybersecurity protection system [1–3]. With the increasing diversity and complexity of both cyber attacks and the tools used to carry them out, passive approaches (such as firewall, IDS etc.) are unable to satisfy security requirements [4–6]. However, observing the situation from a deeper perspective led us to the realization that this could be attributed to the several directional issues existing in China's cybersecurity systems, including security program design, security product linkage, and security mechanism design. This leads to birth defects in the protection technology systems of cybersecurity and affects the improvement of the ecological cybersecurity industry environment [7,8].

Therefore, a global consensus exists on the necessity of creating active cyberspace security defense systems. In this context, we design the infrastructure security systems of cybersecurity based on new theoretical methods and technical means in order to improve China's overall level of the protection of national cyberspace security, and this study has practical significance in this context.

2 Trusted computing technology based on active defense

The security defense of cyberspace is closely related to one in human society. In human society, trust is the basis of cooperation and interaction. Owing to the openness of cyberspace, two Internet entities are allowed to interact with each other without any prior arrangement or qualification. This makes it impossible for us to know anything about other entities when we interact with them. The other entity may be eager to destroy our data or send us malicious programs through the interaction, or it may be a computing platform being controlled by a hacker. If we cannot quickly judge the credibility of other entities during interactions, it is likely to cause huge losses to us. Thus, we should determine a way to allow users to decide whether their own interactions with other entities are trusted or not, thus ensuring the safety of cyberspace. This is the basic starting point for trusted computing (TC). It can be said that TC is the successful management of human social experience in computer information systems and cyberspace [9].

Traditional firewalls, antivirus software, and intrusion detection systems (IDS) block viruses and update virus code bases. These systems cannot defend proactively. Accordingly, we must begin with an architecture that can solve the basic problem of information security. We believe that active defense trusted CT based on active immunity can improve the overall protective effectiveness of systems [9]. TC refers to computing operations performed at the same time as the security protection. We assume that the result is always the same and can be measured to calculate the full amount of control, which is not disturbed among users. TC is a kind of protective operation and coexists with the new computing model with active defense. It can identify users, measure statuses, secure storage, and perform other functions. It can also promptly recognize "self" and "non-self" elements. Therefore, it can disrupt the rejection of harmful substances by an entity. By implementing a trusted chip into the hardware, TC can solve vulnerability issues existing in the simplification of the personal computer architecture. From the powering on of a platform to the implementation of the application, a complete chain of trust is built based on this hardware chip wherein each level is certified and trusted by the other levels. If a program has not been verified, it cannot be executed. Through this process, information systems can achieve sufficient immunity for use in building high-security information systems [10]. The dual architecture of TC based on active defense is shown in Fig. 1.

3 TC assurance architecture based on active defense

In order to solve the security threats facing China's most important information systems, we should return to the concept of hierarchical protection. We should consider access relationships as the basis of achieving security, use active defense technology to protect security strength, and manage security functions through a unified security strategy. We should construct a cybersecurity technology framework by adopting in-depth security defense systems to control risk. The core ideas in designing this framework are provided in this section.

(1) From a security mechanism perspective, credible entities and controllable relationships should be focused on access relationships to achieve. In information systems, the entity refers to a subject that executes operations on behalf of the users (such as

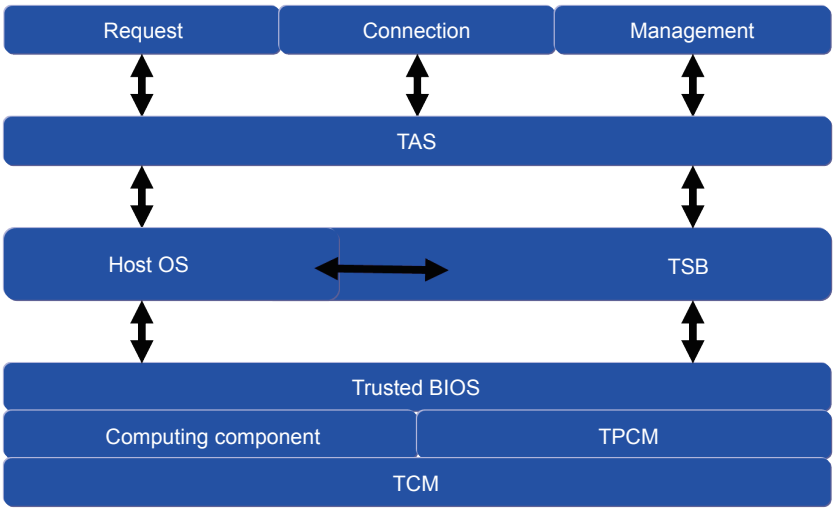

Fig. 1. Dual architecture of TC based on active immunity. TAS: trusted application software; OS: operating system; TSB: trusted software base; BIOS: basic input/output system; TPCM: trusted platform control module; TCM: trusted cryptography module.

the execution of a program) and an object that serves as an information container (such as file, devices, and data storage). The relationships between entities are established through the subjects' read and write access to objects. Subject-object relations and access relations in information systems related to business processes should be identified. The credibility of subjects and objects can be ensured by using trust measurement and trust attestation mechanisms. The controllability of access relations can be ensured via access control mechanisms, and thereby to exclude the cases of abnormal operations except for normal business operations. Information systems can be made immune to both known and unknown security threats, which is a fundamental method of improving the security of information systems.

(2) From a security assurance perspective, structured assurance of security mechanisms should be focused on active defense to implement. Security assurance ensures the reliable operations of security mechanisms and determines their strength. It constitutes the main evaluation index for the fourth-level security systems and above. In the current situation, the information security industry is controlled by people, and TC technology is used for active immunity to support the implementation of security mechanisms and perform trusted executive components, trusted security configuration, and trusted connections, as well as to achieve structured security assurance. Trusted TC technology is the only realistic option for achieving these aims.

(3) From a security policy perspective, policy linkage between security mechanisms should be implemented under a unified management. Security mechanisms provide entities with the ability to perform security control. Specific processes for security control should still be implemented by the deployed security strategies in addition to the security mechanism. Each security policy that boosts the security mechanism should be unified to ensure the security of business processes, and these policies should follow changes in security threats. In order to effectively manage security functions, the security policies of each security mechanism cannot be deployed in isolation. They should form a whole through the linkages between policies. Moreover, security administrators should manage the security policies of information systems with a unified security management center to deal with changes in the security requirements and threats proactively.

(4) From a security system perspective, in-depth defense systems should be designed based on business processes. Currently, as a representative of the advanced persistent threat (APT), a information security system encounters a large volume of three-dimensional and combined attacks. Information security mechanisms based on the characteristics of business processes are required to build multi-level, in-depth defense systems for confrontations. An in-depth defense system cannot be designed out of thin air. Instead, it should be developed on the basis of classification, analysis, and risk assessment of business processes, and it should be implemented by creating a classification of security region for system and deploying security mechanisms with different functions for regional computing environments, boundaries, and communication network. In-depth defense systems can focus resources on the core areas of protection, which effectively prevent the spread of security attacks and greatly influence the controllability of security risks in important information systems.

4 Countermeasures and suggestions

In using innovative TC architecture based on active immunity as the breakthrough point for building trusted cyberspace security technology insurance systems, it is necessary to innovate systems and mechanisms. First, it needs to coordinate national security and business interests; second, it is important to innovate technological development and industrial resource organization modes; third, it is also necessary to allow industrial alliances

to play a role in the development of standards, joint research, industrial application and promotion, and active promotion of pilot and demonstration application.

(1) Promoting innovative systems and mechanisms, coordinating national security and business interests, and gradually forming the endogenous driving force for national industrial development. China should introduce policies to provide market application space for autonomous, controllable, and trusted products, and enable technological innovation, performance improvement, and industrial applications to develop together. For example, the localization-substitution projects of political parties, governments, armies, and the core key system are fully funded by the state, and it should set aside special funds for the improvement of the integrated adaptation and optimization of applied trusted products in the implementation of projects, making up the financing gap of direct research. China should continually promote the development of the industry chain of trusted computing products and actively optimize the industrial ecological environment, thereby to effectively improve the endogenous power of enterprise in trusted technology protecting the research and development of products.

(2) Realizing a mutually beneficial and win-win strategy for opening up, implementing the strategic cooperation of localizations of information security systems, and ensuring that substantial localizations are actually formed. Cooperative negotiation with foreign IT enterprises is not only the function of the enterprise itself but also related to national information security. It cannot be considered based on business interests only. It must consist of a rigorous credible inspection using independent rules, strategies, and architecture and must guarantee sufficient information for real control by using concrete active immunity TC mechanisms.

(3) Increasing independent innovation and adding active defense research into the approval of major national research projects. It is indisputable that TC technology based on active defense is very important. China's TC technology is innovative in system architecture, operation modes, and service modes. The government should lead and strengthen its support of active immunity technologies. In major national research projects, the government should provide support to the research on trusted TC technologies based on intellectual property rights to promote the theoretical research on active defenses, product research and development, and engineering applications.

(4) Actively promoting the formulation and popularization of TC standards and carrying out pilot demonstrations. At present, the lack of TC standards has seriously restricted the innovative development and industrialization of TC. In pilot demonstrations and applications in key industries, it is necessary to summarize lessons, identify problems, constantly improve standards, and gradually expand the scale to form the ecological environment of whole industry chain. Moreover, for the basic software and key products, such as desktop operating systems, embedded operating systems, and cloud computing systems, it is important to recommend the demonstrations of active defense systems to further improve the TC technology assurance architecture and the support capabilities of cyberspace security.

References

[1] Zhang W L. Discussion the status of information security base on graded protection [J].Information Security and Technology, 2014, 9 (1): 9–13. Chinese.

[2] Wang D C, Wang Y S, Lin H. Analysis of computer information system hierarchical protection [J]. China Public Security (Academy Edition), 2009, 16 (3): 4–10. Chinese.

[3] Zhu J P, Li M. Research on information security classified protection standard system [J]. Information Technology & Standardization, 2005 (5): 21–24. Chinese.

[4] Luo L. Analysis of information security and hierarchical protection technology [J]. Heilongjiang Science and Technology Information, 2015 (12): 155–155. Chinese.

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

[6] Shen C X, Zuo X D. Focus of hierarchical infosec protections [J]. Information Security and Communications Privacy, 2004 (4): 16–18. Chinese.

[7] Shen C X. Accelerate the work of information security hierarchical protection [J]. Netinfo Security, 2008 (5): 4–7. Chinese.

[8] Ma L, Bi M N, Ren W H. Research of the relationship between popular security protection model and security protection requirements for classified protection of information system security [J]. Netinfo Security, 2011 (6): 1–4. Chinese.

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

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