The security solution for Windows XP end of life with trusted computing technology

Cui Zhanhua[1, a *], Pan Hongyi[2]

[1]China Information Security Research Institute Co. Ltd., Beijing, China

[2]Full BGP INC., China National Petroleum Corporation, Hebei, China

[a]cuizhanhua@163.com

Keywords: Trusted computing, Windows XP end of life, Security control.

Abstract. The system based on trusted computing is proposed to secure IT system after the Windows XP end of life. The system consists of a series of software, hardware and firmware, including Trusted Platform Module, BIOS, Operating System, Trusted Software Base, Trusted Management Center, etc. It performs functions of interface services, measurement, access control with trusted measurement, trusted storage and trusted report mechanism. The proposed system has been deployed in many IT systems, including the state grid, a department in Beijing municipal government, a military IT system, etc. The application results show that the system could effectively protect their IT system from attacks.

Introduction

Microsoft ended support for Windows XP on April 8, 2014, which means that there will be no more security updates or technical support for the Windows XP operating system. Without critical Windows XP security updates, computers may become vulnerable to harmful viruses, spyware, and other malicious software which can steal or damage the business data and information. Anti-virus software will also not be able to fully protect computers once Windows XP itself is unsupported.

Windows XP end of life does make a great influence on china[1]. There are a great number of users using Windows XP, including private, government, military, research institute users, etc. According to security report from Microsoft by the end of 2013, Windows XP users amounts to 57.8% of Chinese users. The authority statistics shows that Windows XP at least amounts to 60%, even maximum to 95% in Chinese government departments and state-owned corporations. Microsoft will stop to provide after-sale services for Windows XP users, such as hot repair, product update and security patch, which will trigger more attacks on Windows XP security bugs. There will be much greater potential threat from hackers and Trojan virus[2-3] for Windows XP users leading to sensitive information leakage, system crash and property loss, which will influence more than 200 million Chinese users. Microsoft claims that there will be a probability of 2/3 for computers with Windows XP to be attacked by malwares after Windows XP end of life. Therefore, Windows XP end of life will threaten Chinese users, even national security. Recently, Chinese related government departments, research institutes, IT developers, security technology experts have paid more attention to Windows XP end of life, and developed different solutions with access control [4-6], application white list[7-10], identity authentication mechanism, etc.

The paper proposes trusted computing technology-based solutions for windows XP end of life, introduces the solution implementations and the applications, which shows that the proposed solutions are convenient, effective to solve Windows XP end of life.

Security Solutions and Implementation

The Principles. To solve the security problems resulted from Windows XP end of life, the paper proposed the solutions of “Security Strengthening, Gradually Replacing, Nation-owned Design and Manufacturing” achieved by the system with trusted computing technology.

First, Security Strengthening. For IT system in which Windows XP is supposed to be indispensable, the system is proposed to strengthen the security of Windows XP after Microsoft end support for it. Online and offline service channels for the system are provided. Therefore, users could install the system on their computers themselves and get related technical supports and services online, or they could deploy the system in their IT system and maintenance it themselves. It' will be not necessary to update or package Windows XP after applying the system because malwares and virus could not run and could not delete or tamper sensitive data protected by the system.

Second, Gradually Replacing. For IT system that needs to expand capacity or update, or for new IT system that has been developed without the support for nation-owned operating system, both nation-owned cloud operating system and Windows XP are applied to support IT system running. After establishing virtualization platform with nation-owned cloud operating system, Windows XP is moved to virtualization machine and all applications run in Windows XP without changing IT system framework. Users work and run applications as they used to. The system is used to provide protection for such IT system.

Finally, Nation-owned Design and Manufacturing. For new IT system that could be moved to nation-owned operating system, Windows XP is replaced by the nation-owned operating system with trusted computing technology. Therefore, all applications run in nation-owned operating system with security strengthening by the system.

Security model based on trusted computing. The system consists of a series of software, hardware and firmware, including Trusted Platform Module, BIOS, Operating System, Trusted Software Base, Trusted Management Center, etc. It provides drivers for related hardware and API for different system applications with core functions of trusted measurement, trusted storage and trusted report.

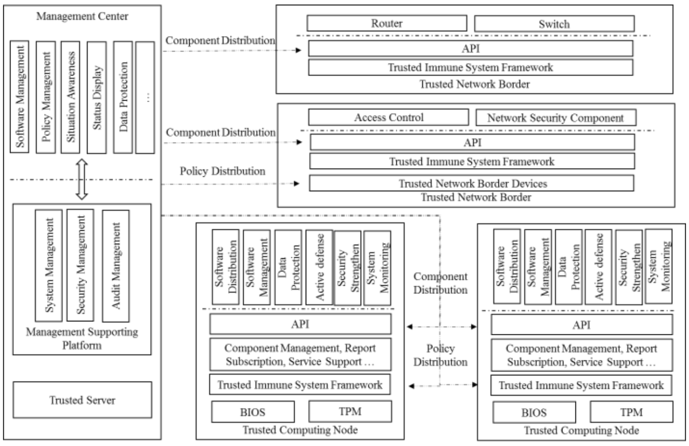

Fig. 1. . System framework based on trusted computing technology

Trusted Platform Module is the key control module for trusted applications and the trusted root storing encryption keys of trusted measurement, trusted storage and trusted report and other confidential information, and performing some encryption operations. It mainly consists of micro-processor, non-volatile storage unit, volatile storage unit, random number generator, cipher algorithm engine, key generator, timer, in/out bridge unit and control modules. Trusted Platform Module could apply key information to execute trusted applications by directly reading the device identity information linking to it and getting information related to the current operators. It is designed to actively perform hash operation with the features data of software, hardware and firmware in the system, which is used as input for measurement function.

Trusted Software Base is the action element to perform trusted measurement, trusted storage and trusted report in the system, building trusted computing and connecting environment for system software and applications with Trusted Platform Module. The system could use interfaces providing by Trusted Software Base to call Trusted Platform Module security functions. Trusted Software Base could control applications to access to hardware resources in the system, ensuring trusted chain in the system and integrity measurements of upper-layer software. On the other hand, it provides interfaces for users and applications to call Trusted Platform Module functions.

Trusted Management Center consists of system management, security management and audit management, performing functions of software and hardware management, security management and operation surveillance on all computing nodes and network device in the system. Trusted Management Center provides interfaces for external Certificate Authority, enables trusted certification mechanism and trusted connection mechanism by the unified security management system. It also could communicate with all Trusted Software Base with standard protocols and data formats, enforce unified security policies with the modules of security management, system management, audit management and cipher management. During the process of security maintenance, update, and management, it plays a key role as a trusted computing protection system in heterogeneous computing environments by collecting security states, correlation analysis and quick response.

During the system operation, system software and application software may have bugs, which could be utilized to attack the system by hackers. The proposed system performs real-time check on the system and processes to verify whether they are trusted, measures key kernel data(system call table, interrupt description table and key operation pointer, etc.), kernel codes, process codes, process-shared library to keep the integrity of the system and processes. If their integrity is destroyed, the system call operation will be prohibited to prevent against malicious code injection using system vulnerabilities and penetration attacks on processes. Therefore, the system achieves functions of unified security states analysis, real-time response and systematic protection by building standard system architecture, interface, protocol and data structure, providing trusted functional modules and middle-ware, developing unified security management mechanism and dynamic correlation response mechanism.

The proposed system implementation. The system is developed based on the security model mentioned above. The system consists of both kernel and system layer, providing functions of interface services, measurement, access control, etc.

Standard interfaces. The system provides standard interfaces for applications and kernel calls. The unified and standard API interfaces of trusted services for users functions as interface libraries, providing transparent services which makes it for users easier without dealing with internal call relations in the system. It is what is needed for users to provide correct call parameters to use trusted services.

The kernel services interfaces consist of trusted storage interfaces, trusted connection interfaces, trusted measurement interfaces and trusted authentication interfaces. All trusted storage requests must follow standard rules to pass to trusted storage interfaces, which will calls Trusted Platform Module to perform encryption and decryption operation and send operation results to users. Trusted connection interfaces are the only entry to the system kernel, which will decide whether the entities are permitted to connect the trusted computing environment by performing functions of verifying endpoint identities, authenticating users and measuring the platform state. Trusted measurement interfaces mainly deliver all measurement requests that include requests on the file systems, processes, network and memory, etc. to Trusted Platform Module and return measurement results to requesters. Trusted authentication interfaces mainly perform authentication on system logon users.

Trusted measurement is the key technology to keep the trusted chain correctly delivered. It has two functions, one of which is to measure initiated items in the system, the other one of which is to measure key resource state and process behavior of the operating system in real time. Before every item is started, it will be measured to verify whether it is trusted. The system control will be delivered to next item only if it is verified to be trusted. When the system is running, the key system resources and states will be measured dynamically to keep the system run correctly, which will prevent the system security attacks effectively.

Trusted security control. Access control is an effective protection method by allowing an authorized body to access to the object of resources, at the same time, refusing to provide service for unauthorized body [11].Trusted security control takes advantage of access control based on Trusted Platform Module and Trusted Software Base to control access to objects by subjects, white list of process operation, in and out network, device connection and use with the proposed system. It will perform surveillance on the system operation in real time to check whether the security policies are strictly followed. Moreover, users are allowed to logon only if the user identity authentication is successful. At the meanwhile, it will perform audit on the system.

White list management mechanism. White list security management mechanism based on trusted computing [12-16] will keep the operating conditions safe in its full life-cycle. Before the system is loaded, the system verification and protection is implemented by the trusted computing platform from a hardware perspective; When the system is loaded, it is verified by trusted roots layer by layer, which guarantees the safety and consistency of white list itself; After the system is loaded, the white list runs to protect the safety of the system. White list management mechanism in the system mainly protects the programs startup process by trusted measurement, which performs the integrity measurement to prevent them from malicious code.

Applications

The proposed system has been deployed in many IT systems, including the state grid[17], a department in Beijing municipal government, a military IT system, etc. The application results show that the system could effectively protect their IT system from attacks.

As we know, a new zero-day vulnerability in Internet Explorer is published in April 28, 2014, which was also confirmed by Microsoft with a security advisory 2963983. The zero-day vulnerability could be used by hackers to steal or delete data with all versions of Internet Explorer running on Windows. The vulnerability is due to a use-after-free error. A remote attacker could exploit this vulnerability by enticing the target user to open a malicious web page. In the case of successful exploitation, arbitrary attacker code would be executed in the security context of the target user. It is reported that an American company was attacked with the vulnerability. The report showed that hackers get control over the system, and could delete related data, install applications and create accounts with administrator right.

The analysis and application results show that the proposed system could protect Internet Explorer running on Windows XP against attacking with the vulnerability in the following protection points(as shown in Fig.2).

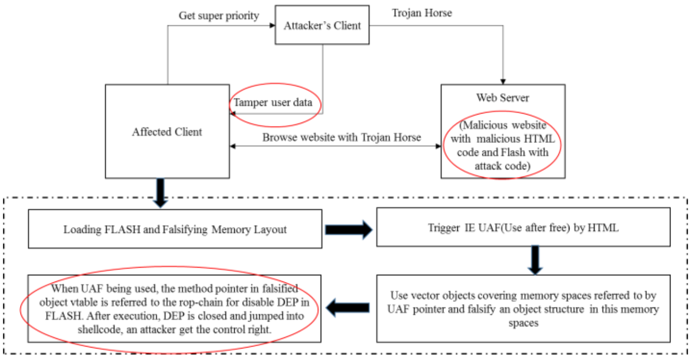
Get super priority
Attacker's Client
Trojan Horse
Tamper user data
Affected Client
Browse website with Trojan Horse
Web Server
(Malicious website with malicious HTML code and Flash with attack code)
Loading FLASH and Falsifying Memory Layout
Trigger IE UAF(Use after free) by HTML
Use vector objects covering memory spaces referred to by UAF pointer and falsify an object structure in this memory spaces
When UAF being used, the method pointer in falsified object vtable is referred to the rop-chain for disable DEP in FLASH. After execution, DEP is closed and jumped into shellcode, an attacker get the control right.

Fig. 2. How does the system prevent attacks from IE Zero-Day vulnerability (CVE-2014-1776)

First, Protect sensitive information and key files in the affected clients with trusted measurement. When the system startup and is running, it performs trusted measurement to verify Windows XP and Internet Explorer integrity to keep them untampered.

Second, Prevent the website and scripts in web servers from tampering. The system will perform trusted measurement on the website and scripts in running time to check whether they have been tampering, or infecting by Trojan horse, which will effectively prevent website and Flash with malicious HTML code running.

Finally, Prevent DEP mechanism from closing to ensure that the shellcode without execution right cannot run. when UAF being used, the method pointer in the falsified object table is referred to the rop-chain for disable DEP in FLASH. After execution, DEP is closed and jumped to shellcode and the attacker get the control right. The system prevent any changes in Windows XP and Internet Explorer, including DEP mechanism. Therefore, the vulnerability could not be utilized by hackers to perform attacks.

Conclusions

With Windows XP end of life, computers may become vulnerable to harmful viruses, spyware, and other malicious software which can steal or damage the business data and information. The paper proposed the system for Windows XP end of life with trusted computing technology. The system consists of a series of software, hardware and firmware, including Trusted Platform Module, BIOS, Operating System, Trusted Software Base, Trusted Management Center, etc. It protects computers with Windows XP with trusted measurement, trusted storage and trusted report mechanism. The proposed system has been deployed in many IT systems, including the state grid, a department in Beijing municipal government, a military IT system, etc. The application results show that the system could effectively protect their IT system from attacks.

References

[1] Zuo Xiaodong and Wnag Shi. Promote technology innovation to deal with the operating system security risk. Information and communication security. 2014(2), 22-24.

[2] L. Notargiacomo. Role-Based Access Control In ORACLE7 And Trusted ORACLE7. In Proceed-ings of the 1st ACM Workshop on Role-Based Ac-cess Control, page 17, Gaithersburg, MD, 1995.

[3] S. L. Osborn, R. Sandhu, and Q. Munawer. Con-figuring Role-Based Access Control to Enforce Mandatory and Discretionary Access Control Poli-cies. ACM Transactions on Information and System Security, 3(2):85–106, 2000.

[4] D. Ferraiolo, D. R. Kuhn, and R. Chandramouli. Role-Based Access Control. Artech House, 2003.

[5] D.F. Ferraiolo, R. Sandhu, S. Gavrila, D. R. Kuhn,and R. Chandramouli. Proposed NIST Standard for Role-Based Access Control. ACM Transactions on Information and Systems Security, 4(3), 2001.

[6] [R. France, D. Kim, S. Ghosh, and E. Song. AUML -Based Pattern Specification Technique. IEEE Transactions on Software Engineering, 30(3):193-206, 2004.

[7] Masoom Alam, Xinwen Zhang, Mohammad Nauman, Model-based Behavioral Attestation [A]. Proceedings of 13th ACM symposium on Access control models and technologies[C], New York: ACM Press, 2008:175-184.

[8] Masoom Alam, Xinwen Zhang, Mohammad Nauman, Tamleek Ali. Behavioral Attestation for Web Services (BA4WS)[A]. Proceedings of the 2008 ACM workshop on Secure web services[C], New York :ACM, 2008:21-28.

[9] Masoom Alam, Mohammad Nauman, Xinwen Zhang, Tamleek Ali, Patrick C.K. Hung. Behavioral Attestation for Business Processes (BA4BP)[A]. Proceedings of 2009 IEEE International Conference on Web Services[C], IEEE Press, 2009:343-350.

[10] Mohammad Nauman, Masoom Alam, Xinwen Zhang, and Tamleek Ali. Remote Attestation of Attribute Updates and Information Flows in a UCON System[A]. Proceedings of the 2nd

International Conference on Trusted Computing[C], Berlin, Heidelberg: Springer-Verlag, 2009:63-80.

[11] R. Sandhu and Q. Munawer. How To Do Discretionary Access Control Using Roles. In Proceedings of the 3rdACM Workshop on Role-Based Access Control(RBAC-98), Fairfax, VA, 1998. ACM Press.

[12] J Park. Towards usage control models: beyond traditional access control [A]. Proceedings of seventh ACM symposium on Access control models[C], ACM Press, 2002.

[13] L. Badger, D. F. Swme, et al. Practical domain and type enforcement for UNIX [A]. Proceedings of IEEE Symposium on Security and Privacy[C], 1995: 66-77.

[14] Safford D, Zohar M. A trusted Linux client[A]. Proceedings of 2004 Annual Computer Security Applications Conference[C], Hilton Tucson, 2004.

[15] Ahmed M. Azab, Peng Ning, Emre C. Sezer, Xiaolan Zhang. HIMA: A Hypervisor-Based Integrity Measurement Agent[A]. In Proceedings of the 25th Annual conference on Computer Security Applications[C], Piscataway NJ:IEEE, 2009:461-470.

[16] Lionel Litty, H. Andres Lagar-Cavilla, David Lie. Hypervisor Support for Identifying Covertly Executing Binaries[A]. Proceedings of the 17th conference on Security Symposium[C]. Berkeley: USENIX, 2008:243-258.

Baohua Zhao, Hao Zhang, Hao Guo, Yue Qi, White List Security Management Mechanism based on Trusted Computing Technology. Proceedings of the 2015 international Symposium on Computer & Informatics. 2015: 1369-1377.