VSIM: a Provable Secure Virtual Security Isolation Model

Jun Ma
Zhengzhou Information Science and Technology Institute
ZhengZhou,China,450004
sijunhan@163.com

Yuanbo Guo,Hongzhao Kou
Zhengzhou Information Science and Technology Institute
ZhengZhou,China,450004
yuanbo_g@hotmail.com

***Abstract*—With the continuous development of the network technology and the significant raising of the hardware's performance-price ratio, it is a popular tendency that users access different kinds of network via endpoint computers for obtaining share/free resources. Meanwhile, endpoint computers act as endpoint computing platforms to provide basic serve for different security level networking. In this condition, different security level resources stored in personal endpoint computers incurs security threat which come up with new challenges to the existing security isolation mechanisms. In this paper, a new security isolation model is presented based on hardware level virtualization technology by comparing available isolation execution technologies, and is proved to satisfy the Bell-LaPadula (BLP) confidentiality model.**

Keywords-Virtualization, Security isolation, BLP model, Provable Secure

I. INTRODUCTION

With the computer technology boomingly developing and the gradually raising of Internet applications, it is a popular tendency that users access different kinds of network via endpoint computers. The users of the endpoint computer are willing to download and share resources on the different security level networking. However, this evolvement incurs more serious security threats to the endpoint computing platforms: (1) Local resources accessing, low-grade authority identity can access high-grade authority resources in illegal ways; (2) Networking resources accessing, due to one of network connect be intruded, others connecting via the same endpoint computing platforms can not operation normally. Consequently, these threats come up with several new challenges to the existing protecting mechanisms. Traditional Role-Based Access Control (RBAC) [1], Attribute-Based Access Control (ABAC) [2] and Mutil-level security protection can not solve these new security problems. However, through virtualization [3], constructing a transparent isolated execution environment, which can confine the potential threats of the untrusted resource and monitor the behavior of this resource without negating its functionality benefits, will serve as the important technology approach to protect the endpoint computing platforms against the security threats of the untrusted software.

Our Contributions. First, we propose the basic requirement of isolated execution environment, on that basis, we choice available isolated technology to solve aforementioned security threats. Second, we present concrete model for investigating the security of endpoint physically and virtually system. In the model, we make some concrete attributes about the isolation system, which allows us to derive some concise analytic and provable security. Furthermore, we introduce Bell-LaPadula[4] confidentiality model to certify security of our proposed model. The innovation of this paper is that VSIM, the mandatory access control model which is built in virtual machine systems, is applicable to multi-level security environments. Not only can it regulate fine grained overt communications between virtual machines, but also isolate covert communications which are incurred by sharing hardware.

The rest of the paper is organized as follows. Available security isolation technology is discussed in Section2. Our virtual security isolation model (VSIM) is proposed in secion3, and certify security of this model in Section4. Finally, Section 5 offers our conclusion.

II. OVERVIEW OF SECURITY ISOLATION TECHNOLOGY

In this section, we firstly propose security attributes which endpoint computer system should possess, and then applicative security isolation mechanisms is adopted, according to existing security isolation mechanisms are introduced.

A. essential attributes

The chief reason of aforementioned security threats is that untrusted software is operated on endpoint computing system. For example, some software with malicious code is downloaded from networking, in this case, all malicious code executed will have its full bad effect. Besides of software with malicious code, unstable software and vulnerable software are defined in untrusted software in this paper. All of them can destroy stabilization of endpoint computing system. In the view of destructive act of untrusted software, we can adopt isolation mechanism to protect endpoint computing system against intrusion. We proposed isolation execution environment abide by some attributes as follows:

- Isolation. Operating software can not change state of OS without being authorized. This stronger isolation provides malicious programs or hackers can be contained within the one OS and not adversely affect on the other parts of the OS.
- Integrality. Software operating normally on one OS of endpoint computing platform can operate on the other

Published by Atlantis Press, Paris, France.

OS with same function. The function Integrality of software can not change in different OS environment.

- Adaptability. The performances of operating software in one OS environment are comparable with those of operating software in the other OS environment. Adding a layer of software to a system adds overhead, which can not adversely affect the performance of the software running in other system.
- Controllability. The operating state of software can be controlled by system; therefore, authorized users can monitoring and control the state of software by system-level operation.

B. Analyze of existing security isolation mechanisms

The purpose of security isolation mechanism is to protect OS from destruction of untrusted software operation. According to different execution hierarchy, existing security isolation mechanisms are divided into Access Control Sandbox Model, Mono virtualization model and hardware level virtualization model.

Sandbox [5] is an HLL(High Language Level) security isolation model, which make different security strategies to protect OS and prevent destruction of untrusted software or malicious code. Due to the different OS can make different security strategies to solve different level security, Sandbox has high flexibility. Nevertheless, different security strategies bring about incomparable inconsistent protection of endpoint computing system. Furthermore, it is difficult to generate or improve a strategy dynamically in the process of system operation. Some sand box system, such as Janus, Peterson, and Strata etc, are typical representative prototype systems, which, however, dissatisfies uniform of integrality and adaptability.

Mono virtualization model [6] adopts one-way isolation mechanism to protect system sources from destruction of untrusted software. With respect to sandbox model, it is simple to implement without complex strategy configuration. Nevertheless, mono virtualization model can not kernel-level isolation that modification and attack of malicious code happens without a hitch. Alcatraz and Entropia virtual machine are example of mono virtualization which does not adequately meet the characteristics of isolation.

Hardware level virtualization model [3] follows the norm of virtual machine technology. Virtual machine itself has a set of attributes, compatibility, isolation, encapsulation and performance. According to different implementation levels, VM technologies is divide into instruction-level virtualization, hardware-level virtualization, operating system-level virtualization, and application-level virtualization, among of them, hardware-level virtualization can more effectively the isolation and adaptability of the OS. Meanwhile, virtual machine monitor (VMM) of hardware-level virtualization provides controllability perfectly to manage software sources operating on different operating systems in a safe, transparent, and efficient way. At present, hardware-level virtualization has been used in more security areas, such as intrusion detection, malicious code detection, honeypot and security isolation mechanism. Many papers [7] [8] propose different security isolation model, and have their own advantage, however, some aspects have not been considered as follows:

- Security isolation model is applicable to endpoint computing platform with less compute capability.
- Aforementioned four attributes are considered to Collaborative Design.

This paper proposes virtual security isolation model (VSIM) to take above factors into account. Meanwhile, security of VSIM will be proved in accord with BLP model in next section.

III. PROPOSED VSIM ISOLATION MODEL

A. constraint condition

For achieving the balance among security isolation, functional integrity, performance adaptability and behavior controllability of the isolated execution environment, VSIM must meet the following four constrains.

Constrain A: Isolation between OS. Runtime environments of endpoint computing platform typically provide some form of isolation mechanism between operation systems that untrusted software running one OS can not ruin the other OS. It is an essential condition to runtime environments against privilege malicious code attack and ensure the safety of isolation.

Constrain B: Runtime OS and execution programs transparency. The transparency of runtime OS is to refer one OS can normally restart, operating and ending, but need to care other OS state on the endpoint computing platform. The transparency of execution programs means programs do not care about runtime environment to execute with less performance loss.

Constrain C: Data privacy protection. Without influence user accessing, strong protection mechanism should be provided to prevent adversary eluding isolating mechanism to access user information.

Constrain D: State monitor of untrusted software in isolation environment. It is indispensable to watch untrusted software running state and read/write trusted data state so that isolation system can properly adjust isolation strategy. Moreover, it has been provided as a necessary instrument for improving and management of isolation execution environment.

B. proposed isolation model

To meet the condition of constraint A, virtual machine monitor (VMM), a thin layer of software, is used to export hardware-level virtual machines, which runs on the hardware of the real machine to provide and isolate an abstraction of hardware of endpoint device to each virtual machine.[9] gives three types of VMM, VMM-TypeI , VMM-TypeII and VMM-Hybird. VMM-TypeI runs directly on the hardware to schedule and distribute hardware system resources. VMM-TypeII and VMM-Hybird need run on custom system soft-environment. Compare with VMM-TypeII and VMM-Hybird, VMM-TypeI provide strong security isolation to prevent untrusted software utilizing system bug and hole of custom system within VMM from ruining. Meanwhile, Due

to regardless of system load, VMM-TypeI can more effectively execute hardware resource scheduling than other type of VMM.

Virtual machine technology with VMM-Type I can manage more OS, for example Xen can simultaneously run hundreds of heterogeneous OS. One OS can and run independently instead of impacting other OS. Untrusted programs are isolated in running OS, and communicate with other system resources within VMM supervision. VMM-Type I, therefore, meet the condition of constrain B.

To meet the condition of constraint C, mandatory access control mechanism is introduced. Due to hardware-level virtual machine only provides independent access control mechanism that can not effectively prevent security problem such as covert channel. We adopt available scheme [10] that provide system-level mandatory access control and are appropriate for hardware-level virtual machine.

To meet the condition of constraint D, VSIM need extra monitoring module to concern information of every GuestOS. The module in VMM is responsible for attaining the messages, GuestOS using hardware devices, and transports it to VMM. The purpose is to protect GuestOS from ruining of untrusted software.

The proposed virtual security isolation model, VSIM, satisfies above four constraints is shown in Figure 1.

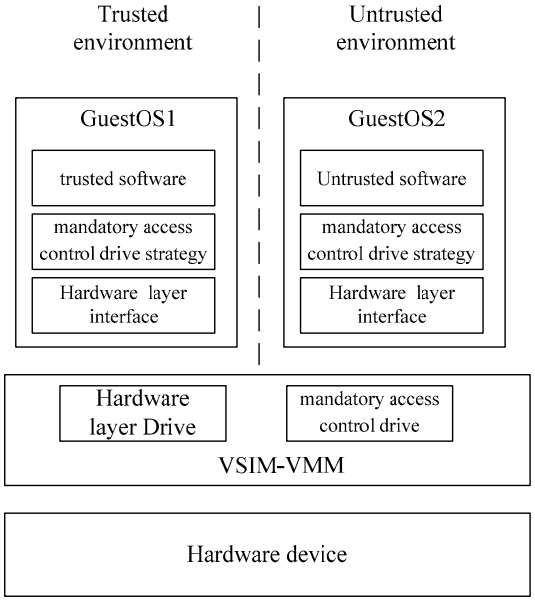

Figure 1. The VSIM isolation model

IV. Security Analysis

We firstly list available symbol and definition of BLP model. Let S be set of subject, let O be set of object; $\forall s \in S$, ls denotes security level of s, $\forall o \in O$, lo denotes security level of o; $l_i \in L(i = 0,1,...,k-1, k = |L|)$,L denotes set of security level of system, $L_i < L_{i+1}$;D denotes set of permission, $d \in D, D = \{read, write\}$.

Definition 1, $\forall \lambda_1, \lambda_2, \in S \cup O, \lambda_1 = (l_1, d_1), \lambda_2 = (l_1, d_1)$, λi denotes security level, λ_1 dominates λ_2 , iff $l_1 < l_2$ and $d_1 \subseteq d_2$ .we signs λ_1 dom λ_2 .

Definition 2, the Simple Security Property (no read-up). A subject λ_s at a given security level may read an object λ_o iff λ_s dom λ_o

Definition 3, the *-property (no write-down). A subject λ_s at a given security level can write to an object λ_o at a lower security level iff λ_o dom λ_s

Theorem 1 (Basic Security Theorem), $\forall$ (R, D, W, z0) is a secure system if z0 is a secure state and W satisfies the conditions of Simple security Property and *-property.

Theorem 2, VSIM isolation model is BLP-secure that satisfies the conditions of Simple security Property and *-property.

Proof:

(i) In VSIM, GuestOS usually adopts the Windows OS, Linux OS or Unix OS that has been proved BLP-secure, and the reality of VMM system uses customized Linux OS that has also been proved BLP-secure.

(ii) Let $\lambda_v = (l_v, d_v)$ be VMM system security level and $\lambda_g = (l_g, d_g)$ be GuestOS security level. In VSIM, The security level of VMM system is higher than that of GuestOS, then $l_v \geq l_g$, and security and trusted software in VMM system, then $d_v \supseteq d_g$. Therefore, λ_v dom λ_g .

According to (i),(ii), The VSIM is BLP-secure.

V. Conclusion

This paper analyzes existing isolation execution technology and proposes a new virtual machine based isolation model-Virtual Security Isolation Model (VSIM) which satisfies proposed isolation, integrality, adaptability and controllability. In addition, this paper proves in theory that VSIM isolation model satisfies the BLP confidentiality model. The next step is that utilizing available virtualization technology, such as Xen, realizes prototype system to verify feasibility and performance of the propose security isolation model.

Acknowledgment

This paper is supported by the scientific innovation talents Foundation of Henan, China under Grant No. 104100510025;

References

[1] DUAN Ming-de; GAO Zuo-bin; MA Wei; LI Ji-shun. Application of RE in the Development of Tractor Covering Parts. Tractor & Farm Transporter [J], 2007, PP:86-88

[2] Sandhu, R., Coyne, E.J., Feinstein, H.L. and Youman, C.E. (August 1996). "Role-Based AccessControl Models" (PDF). IEEE Computer (IEEE Press) 29 (2): 38–47

[3] W. Johnston, S. Mudumbai, and M. Thompson,"Authorization and Attribute Certificates for Widely Distributed Access Control", Proceedings of the IEEE 7th International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises, 1998, p. 340

[4] Armstrong, W. J. Arndt, R. L. Boutcher, D. C., Kovacs, R. G., Larson, D., Lucke, K. A., Nayar, N., Swanberg, R.C. 2005. Advanced virtualization capabilities of Power systems. IBM Journal of Research and Develop-ment 49(4/5): 523–532.

[5] D. E. Bell and L. J. LaPadula, Secure Computer Systems: Unified Exposition and Mastics Interpretation[R], the MITRE Corporation, March 1976

[6] Boulay Claude, de Larrard Francois.Sand-box.Concrete International, 15 (4), pp. 63-66.

[7] Chiueh T,Sankaran H,Neogi A.Spout:A Transparent Distributed Execution Engine for Java Applets[C].Proceedings of the 20th International Conference on Distributed Computing Systems ICDCS'00),Taipei,Taiwan,ROC.2000: 394-401.

[8] Whitaker A,Shaw M,Gribble S D.Denali:A Scalable Isolation Kernel[C]. Proceedings of the 10th ACM SIGOPS European Workshop, Saint-Emilion, France.2002:10-15.

[9] Whitaker A,Shaw M,Gribble S D.Scale and Performance in the Denali Isolation Kernel[C].Proceedings of the 5th Symposium on Operating Systems Design and Implementation OSDI'02),Boston,Massachusetts,USA.2002:195-209.

[10] Goldberg, Robert P. Architectural Principles for Virtual Computer Systems. Harvard University.973:22–26

[11] Sylvia Osborn, Ravi S. Sandhu and Qamar Munawer. Configuring Role-Based Access Control to Enforce Mandatory and Discretionary Access Control Policies. ACM Transactions on Information and Systems Security, 3 (2):85–106, 2000.