Research on the Trusted Enhancement Technology Based on Bare Metal Model Virtual Machine

Fei Wang, Yu Wang, Jie Qiang

Space Engineering University, Space Information Institute, Beijing, China

Abstract. This paper proposes a trusted enhancement model for bare-metal VMs, which can provide credible guidance and application credible enhancement in combination with the startup and booting characteristics of bare-metal VMs. The model is suitable for terminals with multi-security service requirements. It can be divided into several trusted virtual isolation terminals according to the actual needs of users. It has the characteristics of not changing the existing network topology, high security and rapid deployment.

1 Introduction

With the intensification of national informatization construction, the construction of various information systems is increasing day by day, and the access equipment and applications have become increasingly complex. Due to the different service types and security levels of the information system, users often need to operate multiple terminals at the same time, which makes it more and more difficult for a user to manage daily usage and operation and maintenance. Virtual machine technology can work in different virtual environments by separating different types of applications such as office, business processing, and information access to meet users' needs of safely handling different dense-level services in the same physical terminal environment. Despite all the advantages, virtual machine systems face the same security vulnerabilities and are vulnerable to code security threats [1].

Starting with the bare-metal virtual machine, this paper proposes a credible and enhanced technology based on the bare-metal virtual machine through the study of the start-up and operation mechanism of the bare-metal virtual machine, and establishes a credible and safe operating environment for the bare-metal virtual machine system , Which not only can provide users with technical support for the safe deployment and use of multi-level security business systems, but also is of great significance to the development of virtualization technology and the construction of important information systems.

2 Virtual machine technology

2.1 A Virtual machine classification and characteristics

The concept of virtual machines appeared in the 1960s. The virtual machine monitor (VMM) is an important part of the virtual machine system. It divides the entire computing platform into many isolated virtual machines [2]. The operating environment of each virtual machine is almost the same as that of a normal terminal operated by a user, and all the virtual machines have access to the hardware resources through the VMM. According to VMM, the virtual machine system can be classified into three types: host type, bare-metal type and hybrid type at different levels of the system [3], as shown in Fig. 1.

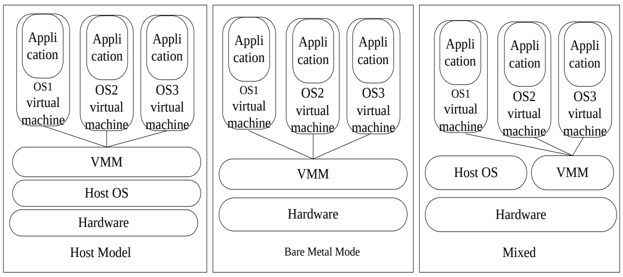

Figure 1. Virtual machine system classification.

(1) Host VMs VMM is located on the host operating system, so that the physical resources owned by the host operating system can be fully utilized. The VMM invokes the services provided by the host operating system to complete the virtualization work and multiple user operations The system runs on the same host operating system.
(2) VMM bare metal model is located in the hardware layer above, you can directly call the hardware interface, it controls and is responsible for managing all the hardware resources and the upper virtual machine environment. IO requests for each operating system are handled by the VMM.

(3) A hybrid virtual machine is a hybrid of the above two structures. The VMM is still created on the host operating system. It needs to modify the kernel of the host operating system to assume part of the VMM functions, and the VMM can directly access the hardware resources。

The three types of virtual machines each have their own characteristics. Specifically, the comparison between them is shown in Table 1.

Table 1. Virtual machine classification comparison.

	Host model	Bare model	Hybrid
Typical representative	VMware Workstation and so on	VMware EXS Server, WindRiver Hypervisor and more	Xen、 Sun Logical Domain and more
Isolation	better	it is good	better
System performance	general	high	Higher
Trusted computing base size	Larger	Smaller	Larger
The main advantage	You can directly use the host operating system driver, IO device virtualization easier to achieve	VMM can control all hardware; System isolation, stability is better.	You can directly operate the hardware to improve the operating efficiency of the virtual machine
Mainly inadequate	The efficiency of resource access has declined	VMM itself is relatively large, need to include a large number of drivers	Need to make changes to the host operating system

From the above analysis, VMM in a bare-metal VM takes over the system boot and operation before the operating system starts up, thereby having better isolation and higher system performance. From the perspective of trusted computing, both host and hybrid virtual machines are built on the host operating system, and the trusted computing base is relatively large. Therefore, this subject chooses bare-metal virtual machine to carry out credible security enhancement research.

2.2 Bare-metal virtual machine startup process

Bare-metal VMs include components such as the VM monitor, management VMs, user VMs, and I / O VMs, and the startup process for the VMs is shown in FIG 2.

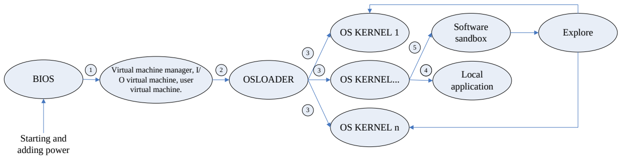

Figure 2. Virtual machine system classification.

Step 1: Power-on and power-on The BIOS loads the VMMs, user VMs, and I / O VMs respectively;

Step 2: VM Manager loads OSLOADER;

Step 3: According to the preset number of virtual machines, OSLOADER loads OS KERNEL for each user virtual machine respectively;

Step 4: Load the local application of the user VM according to the user selection or the latest usage, at this time, the user can use the terminal normally;

Step 5: If the user needs to switch to another virtual machine, the software box is loaded by the current virtual machine. After the user selects a virtual machine to be switched in the software sandbox, the software box loads Explore, Explore, and loads the selected virtual Machine applications and services, and the selected virtual machine interface to switch to the user view, the original virtual machine interface to switch to the background.

3 Trusted model based on bare-metal virtual machine

In the startup and booting phase of a bare-metal virtual machine, there are more entities involved in the system than the ordinary PC. In addition to the boot program and the operating system, the system also includes a virtual machine monitor, an IO virtual machine, and a management virtual machine. During the operational phase, a collection of applications that need to maintain multiple virtual machines introduce new vulnerabilities, both in terms of program count and complexity. On the one hand, the introduction of these special modules will reduce the credibility of the system; On the other hand, during system operation, attackers can more easily exploit vulnerabilities in a certain module to implant malicious programs such as viruses and Trojan horses and cause damage to the system. Bare metal virtual machine to achieve credible security enhancement, we must guide from the system to the actual operation of business software, fully guarantee the credibility of the system.

3.1 Virtual machine trust transfer model

Definition 1:

S Virtual machine boot process all entities collection, $s \in S$;

H The set of expected summary values for all entities in the virtual machine's boot process, $h \in H$;

R The integrity status of the entity. $R = \{trusted, untrusted\}$;

In the system before the first start, that the system is credible, calculated S The expected summary values for all entities in Generate Collection H , And save it at credible root.

Definition 2:

Summary value calculation function $hash: S \to H$, Generates a digest value for each entity calculation.

Integrity verification function $validate: S \times hash(S) \times H \to R$,for $\exists s_i, s_j \in S$,by s_i an examination s_j The integrity of the meet expectations.

If $hash(s_j) = h_j$,then

$validate(s_i, hash(s_j), h_j) = trusted$,otherwise

$validate(s_i, hash(s_j), h_j) = untrusted$.

Definition 3:

for $\exists s_i, s_j \in S$,

if $validate(s_i, hash(s_j), h_j) = trusted$,then s_j Is credible, and vice versa s_j Is not credible. This is also the method used by the TCG in establishing the chain of trust to indicate whether it is trustworthy by measuring the integrity value of the data.

Definition 4:

symbol $\xrightarrow{-}$ Indicates the direct trust relationship between two entities. for $\exists s_i, s_j \in S$,

$s_i \xrightarrow{-} s_j$ Said s_i Direct trust s_j

symbol $\xrightarrow{\bar{s}}$ Represents the transfer of trust between two entities. for $\exists s_i, s_j \in S$, $s_i \xrightarrow{\bar{s}} s_j$ Said s_i Through the entity sequence $\bar{s}$ Indirect trust s_j

Definition 5:

function $parent(S) \to S$ Represents the parent entity that acquired the entity. Correct $\forall s_i, i \ge 2$,

$\exists s_j$ Make $s_j = parent(s_i)$.

Definition 6:

function $\Omega(S \times S) \to \bar{S}$ Represents a function that gets the sequence between the upper entity and the lower entity,

where the collection $\bar{S} \subseteq S$.

for $\exists s_i, s_j \in S, i > j$ If $\Omega(s_j, s_i) = \phi$, Then said s_i versus s_j There is no physical sequence between,

i.e. $s_j = parent(s_i)$ Otherwise $\Omega(s_j, s_i) = \bar{s} \neq \phi$,then said s_i versus s_j There is some entity sequence between $\bar{s}$

Theorem 1:

In the model, s_1 Is credible root. The virtual machine boot process is credible, if and only if it is satisfied $\forall s_i \in S, \exists s_j = parent(s_i)$,

∴Virtual machine boot process in line with the basic idea of trust transfer, boot process is credible.

$validate(s_j, hash(s_i), h_i) = trusted$

prove:

∵ s_1 Trusted root

∴ s_1 Unconditionally credible

∵ $\forall s_i \in S, i \ge 2$, Parent entity $parent(s_i)$ Perform an integrity check, $validate(hash(s_i), h_i) = trusted$

∴By definition 1-3, set S Any entity is credible

∵ According to definitions 1-6, $\Omega(parent(s_i), s_i) = \phi$

∴ $parent(s_i) \xrightarrow{-} s_i$

∵ $\forall s_i \in S$,

Equation $s_1 = parent(\cdots parent(s_i))$ Set up, and $\Omega(s_1, s_i) = \bar{s}$

∴ $\forall s_i \in S$, $s_1 \xrightarrow{-} s_i$ or $s_1 \xrightarrow{\bar{s}} s_i$

3.2 Based on the bare metal model of trusted enhanced architecture

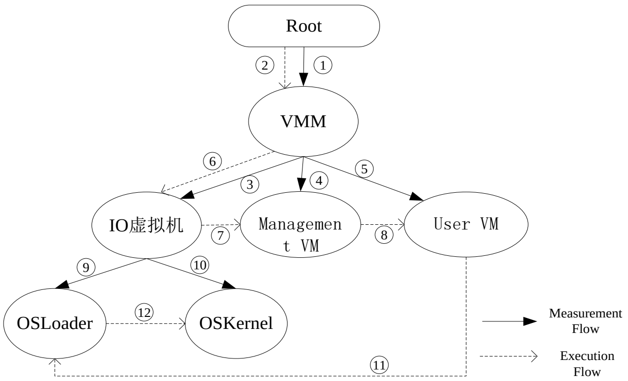

Figure 3. Trusted and enhanced architecture based on bare-metal VMs.

According to the trust transfer model of virtual machines and the startup loading order of bare-metal VMs, the trusted enhanced architecture of bare-metal VMs is shown in Fig. 3. Trusted root measures VMM integrity, verify that the VMM is trusted, and start execution

(1) Credible root Firstly, the trustworthiness of VMM is measured and loaded after verification.

(2) After the VMM is started, measure the IO virtual machines, manage the virtual machines, and then verify the integrity of the user VMs. After the VMs are verified, they are loaded and executed sequentially through the IO VMs, the management VMs, and the user VMs.

(3) After the IO virtual machine starts, the OSLoader and the OSKernel integrity are measured sequentially, and the OSLoader and the OSKernel are loaded and executed after the verification is successful.

(4) The user virtual machine loads the parent operating system and their respective incremental parts, and the boot process is completed.

4 Prototype system design and safety analysis

4.1 Prototype system design

Trusted prototype system based on bare-metal virtual machine is composed of seven functional modules such as bare-metal virtual machine, Ukey credible root, authentication, trust establishment in boot phase, trust establishment in operational phase, security audit and security policy, Figure 4 shows.

(1) Bare-metal virtual machine. According to user needs from the underlying hardware virtual multi-user virtual machine.

(2) Ukey credible root. Is a trusted root for a bare-metal virtual machine and is responsible for storing confidence metrics, identity certificates, providing cryptographic services for trusted metrics, and identity authentication.

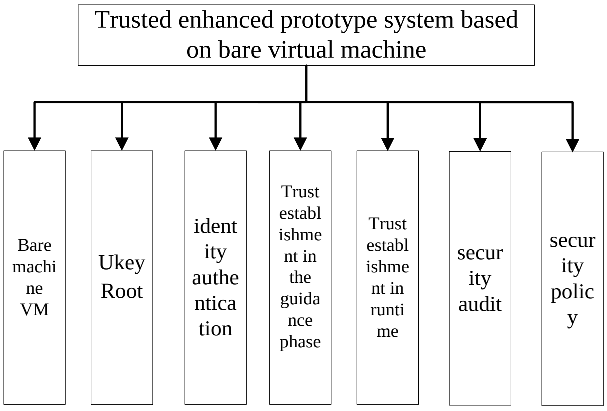
Trusted enhanced prototype system based on bare virtual machine
Bare machine VM
Ukey Root
identity authentication
Trust establishment in the guidance phase
Trust establishment in runtime
security audit
security policy

Figure 4. Prototype system functional structure.

(3) Identity authentication function. In the system start-up phase, the authentication function mainly completes the identification of the terminal user identity to prevent illegal users from accessing the system.

(4) Guide the establishment of trust. In this phase, the process of constructing the trust chain in the guiding phase is implemented, providing a credible operating environment for the virtual machine.

(5) Trust in the operational phase of the establishment. Mainly based on the white list of application layer executable program integrity verification.

(6) Security audit. Conduct security audits of user actions of trusted virtual machines.

(7) Security strategy. Maintaining and managing the bare metal trusted virtual mechanism security policy.

4.2 Security analysis

Trusted prototype system based on bare-metal virtual machine has the following features in security:

(1) It can quickly generate multiple trusted virtual isolated terminals for users without changing the existing network extension, and provide virtual isolated security for users with multiple security-grade services;

(2) By measuring the trusted state of the virtual machine monitor (VMM) in the boot phase to prevent the leakage of underlying information caused by the VMM being damaged;

(3) It can ensure that each user virtual machine can be trusted in the activated environment, and can avoid environment security threats caused by invading malicious code such as viruses and Trojans;

(4) It can control the applications that are loaded in different user virtual machine running phases as needed, that is, the applications specified with the trustworthy metric value satisfying the expectation are allowed to be loaded, so as to ensure the trusted and manageable operation in the running phase of the user virtual machine.

5 Conclusion

Starting from the bare-metal virtual machine, this paper proposes a new enhanced model based on the bare-metal virtual machine by researching the start-up and running mechanism of the bare-metal virtual machine, and designs the prototype system. The prototype system can establish a credible and safe operating environment for the bare-metal virtual machine system. It not only provides users with technical support for the safe deployment and use of the service system with multiple security levels, but also supports the development of virtualization technology and important information The construction of the system is of great significance.

References

1. Chang-xiang Shen, Network space security strategy thinking and Revelation [J], financial electronic, 2014(6):1-3.(In Chinese)
2. Chang-xiang Shen, Huan-guo Zhang, Huai-min Wang, research and development of trusted computing [J]. China Information Science (Chinese edition), 2010, 40 (2): 139-166. (In Chinese)
3. GB / T 29828-2013 Information security technology trusted computing specifications trusted connection architecture [M], Beijing: China Standard Press, 2013. (In Chinese).