Research and Design of Crypto Card Virtualization Framework

Lei SUN, Ze-wu WANG and Rui-chen SUN
Zhengzhou Information Science and Technology Institute

Keywords: Cloud computing, Virtualization, Crypto cards.

Abstract. To satisfy the demand of functional, safety and efficiency in the use of crypto card virtualization, designing a new crypto card virtualization framework. By reconstructing the key structure and adding a virtual domain named virtualized password card domain which contains three modules of identity authentication, key management and communication management, reaching the purpose of Remote identification authentication, data security storage and optimization the performance of virtualization. Experiment shows that the new cipher card virtualization framework can support the function of physical cipher card in virtualized environment and optimize the efficiency of inter-domain communication.

Introduction

In recent years, cloud computing technology enjoys rapid development. With the method of renting calculating resources provided by the cloud service provider, the user can get easy and quick access to software and hardware resources. As the core of cloud computing, virtualization technology maps the virtual resources to physical resources and uses local hardware in the calculation of virtual machine, the kind of virtual hardware supported by data center determines the type of service. Existing virtualized-structure hardware can support the virtualization of most commonly used hardware, but cannot support the use of crypto cards and other hardware under special environment. As a common cryptographic hardware resource, crypto card is widely used in field of military, electronic commerce and electronic government affairs, which are demanding for safety[1]. Compared to hard disk, sound card, network card and so on, it has the characteristics of high security, high sensitivity and communication data. Due to these characteristics, the crypto card has the following problems in the existing virtualization architecture: Concerning the identity authentication, the crypto cards’ local start of authority and rights management is not applicable any more due to the remoteness between the service provider and service users under the virtualization environment. For the implementation of password function safety, there exist potential security risks for the secret key and cryptogram information stored in the service data center simultaneously. Regarding the data communication, the inter-domain communication performance bottleneck[2] existed in the current virtualization architecture will cause relatively higher waiting delay by improving the CPU utilization during the cryptographic services with high throughput such as network encryption and large files’ symmetrical encryption etc.

At present, there are few relevant studies on the crypto card virtualization. Even the similar studies are mainly involved with the TPM virtualization. TPM is a cipher chip with rather simple implement function. As the main component of trusted computing, its main function is to conduct integrity measurement and platform identity authentication[3]. Its virtualization architecture can be divided into full virtualization and para-virtualization. The full virtualization simulates the hardware’s function performance and interface for the upper-level application in the form of software. The para-virtualization is to revise the driver interface and then conduct the data communication by separating the driver. The majority of studies will adopt the para-virtualization architecture in the TPM virtualization, because the full virtualization is lack of physical protection for the secret key under the virtualization architecture. The virtual TPM domain separation structure is adopted in the latest TPM 2.0 virtualization architecture to isolate the mini virtual domain to conduct virtual TPM management. The isolation mechanism provided by the VMM guarantees the safety of function
realization. However, the composition of crypto cards is more complex than the TPM chip with richer implement functions. The current TPM virtualization architecture far can not satisfy the actual demands of crypto cards virtualization in the practical application. Aiming at the inter-domain communication performance bottleneck problems, the relevant studies[4] indicated that the performance overhead brought by the hyper-call in the communication process is far greater than the other operations. The frequent hyper calls are the main reasons to cause the communication performance bottleneck. However, the specific solutions are not proposed aiming at this problem.

In general, the current virtualization architecture can not support the crypto cards’ virtualization use requirements completely. In order to solve the problems encountered in the process of crypto cards virtualization, this paper put forward a new crypto cards virtualization framework. The new framework adds the new function modules and USB-key device interface, which guarantees its availability, safety and high efficiency at the time of achieving the virtualized password functions.

Related Knowledge Introduction

The new framework's core hardware is USB-key and crypto card devices, we will have a brief introduction to USB-key and crypto card in following.

USB-key is a kind of hardware which contains microcontroller or smart card chip in the internal and has space to store the user's private key and digital certificate. It has USB interface, with the built-in public key algorithm, users can digitally sign data[5].

Crypto card is a kind of hardware which can provide encryption function. Currently, the most widely used crypto card is PCI crypto card, it provides symmetric encryption, asymmetric encryption and integrity measurement functions[6]. The crypto card has 3-level key management structure. The first level key is equipment protection key, the second level key is user key, key-encrypting key and device key, the third level key is data encryption key. The first level key protects and manages the second level key and second level key protects and manages third level key. All keys are stored inside the crypto card in order to ensure safety.

Xen[7] is the most widely used virtualization platform at present. It realizes hardware virtualization by driver domain separation architecture which divided into two parts of privileged domain and virtual domain. Privileged domain contains native drivers and back-end drivers, and the front-end drivers locate in virtual domain. The native drivers are responsible for calling the hardware and the front-back-end drivers are responsible for transmitting the command of Guest OS from virtual domain to privileged domain. The communication between front and back end drivers is realized through memory sharing[8] technology.

Design of Crypto Card Virtualization Framework

To solve the problems existing in the process of crypto card virtualization, we argues that the crypto card virtualized framework should be designed to meet the requirements of the following three:
Requirement 1: The ability for users’ remote identity authentication in virtual environments.
Requirement 2: Decryption operation must be combined with users’ identity information to prevent the malicious attacks from interior of data centers.
Requirement 3: Optimizing communication capabilities and improving communication efficiency to reduce the performance loss brought by virtualization.

The Architecture of Crypto Card Virtualization Framework

According to the above requirements presented in the previous section, we design a new crypto card virtualization framework. It consists of hardware platform, virtual crypto card management domain, virtual crypto card domain and Guest OS four parts. The architecture is shown in Figure 1.
The framework uses driver domain separation architecture. Virtual crypto card management domain is privileged domain, it contains virtual crypto card management module and native crypto card driver and is responsible for VM's creation, deletion and recovery. Virtual crypto card domain is a separated mini virtual domain, it provides virtual crypto card to VM. Virtual crypto card domain adds identity authentication module, key management module and communication optimization module inside to satisfy the requirements of crypto card virtualization. The new framework adds USB-key interface at VM to realize remote identity authentication and sensitive information safe storage. The specific work process of each part will be described in detail in the following sections.

The New Key Structure of Framework

In order to solve the storage problem for the three-level secret key, the new secret key structure removes the encrypted three-level secret key (session key) from the inside to the outside of the card. After the crypto card is completed with the encryption, the three-level secret key will not be preserved any more. The three-level secret key, after encryption is conducted completely through the secondary key, will be exported with cipher-text to the outside of the card to return to the guest virtual machine for mutual preservation. Under such combined action with the chain encryption mechanism of the secret key structure and three-level secret key structure, the encrypted three-level secret key and cipher-text can only be returned mutually to the inside of the crypto card to obtain the decrypted three-level secret key to complete the decryption for cipher-text. As the virtual crypto card domain is responsible for the identity authentication, the new secret key structure is added with virtual identification secret key to avoid impersonation attack. Such key is generated and encrypted when crypto card virtual domain is created to be stored in virtual crypto card domain. The new secret key structure is shown in Figure 2.
Although the new secret key structure can ensure the safety of sensitive information through physical protection, it also brings the new problem. As the cipher-text and secret key are all stored at the service provider’s data center, the attack from the internal server may steal the cipher-text and secret key information to conduct data decryption through other legal user identity and even steal the plaintext. The solution to solve this problem will be introduced and explained in the next chapter.

The Virtual Crypto Card Management Module

The new framework is added with the identity authentication module in the domain of the virtual crypto card, only with the USB-key inserted for identity authentication, users can operate the crypto card’s management tool. Through transparent transmission technology[9], USB-key digital signature function can be used on the virtual machine to solve the safety problems brought by the new secret key structure. Next, the encryption and decryption process will be introduced combined with the data flow chart.

For data encryption, firstly, the user’s identity authentication should be carried out. After it is completed via the identity authentication module, user can be able to use the virtual crypto card management tool. After the authentication, the encrypted data in the virtual machine is passed through the virtual crypto card domain to the virtual crypto card management domain. The primary drive is adopted to invoke crypto card for encryption purpose. After the completion of the encryption to the crypto card, the third level key, which is included with cipher-text and is done encryption, is returned to the virtual password domain through the virtual crypto card management domain. After the data is returned, the identity authentication module can bind and store the returned data, including the cipher-text, the three-level secret key information and user’s identity information. At the same time, in order to ensure that the secret key has a full life cycle[10], the secret key management module will keep the encrypted three-level secret key as backup and store it in the secret key management module. After the completion of the above work, the encrypted information will be returned and stored in the virtual machine. The flow chart for encrypted data is shown in Figure 3.

![Figure 3. The data flow chart for encryption.](image-url)

For data decryption, firstly, the digital signature should be conducted to the decryption information, which is included with the cipher-text and secret key, and then the decryption information is sent to the virtual password domain for identity authentication through the authentication module. If the identity authentication is passed, decryption work will be continued. Otherwise decryption work can not be conducted. After the identity authentication is passed, the decryption information is transmitted to the crypto card through the virtual password management domain. After the completion of the decryption, the crypto card will not keep the three-level secret key, while the cipher-text will be returned to the virtual machine. Under this mode, user can decrypt the cipher-text only if he has a legal status. This method can avoid the malicious attacks from the inside server. The data flow chart for decryption is shown in Figure 4.
The Communication Optimization Module

The inter-domain communication for Xen has a higher working efficiency when the input rate of communications data is high, as this is caused due to the characteristics of the transmission mechanism of the memory sharing pages. In order to solve the problem to meet the needs of 3, a new framework is added with the communications management module, so as to optimize the performance of the inter-domain communications of the encrypted data.

According to the characteristics of the data communications, communications management module is mainly invoked to complete the symmetric encryption, network encryption or other data processing with huge throughput. Communications management module is divided into two parts, one is to be responsible for the management of data receiving, and the other is to be responsible for the management of data transmission.

Data receiving: When the communications management module is opened, the back-end drive in the domain of the virtual crypto card will no longer directly apply for a super transfer, instead, it gives the authority to the communications management module, and the back-end drive will transmit the received authorization reference GR to the communications management module for analysis. If the number of the memory page is small, then the application for the super transfer is not conducted, and the included memory pages is accumulated for the next authorization reference GR. Communications management module is set with memory pages memory threshold. When the memory pages accumulated value exceeds the threshold, triggers super transfer for function application is triggered to read the memory pages to complete the data transmission. In order to avoid long time waiting and huge delay, the wait time threshold is set. When the timer reaches the wait time threshold, it can also trigger the super transfer for function application to complete data transmission. Each time when a page transmission is completed, it will trigger a memory page count and timer reset conducted by the function. The working flow chart is shown in Figure 5.
Data transmission: When communications management module is opened, the front-end drive in the virtual crypto card will no longer directly send the authorization reference GR to the target virtual domain, instead, it gives the transmission authority to the communications management module, and then the front-end drive passes the authorization reference GR to the communications management module for analysis. If the number of the memory transmission is also relatively small, then the authorization reference GR is not authorized to send, and the included memory pages is accumulated to wait for the next authorization reference GR. After receiving the new GR, these two GRs are combined together for operation and a new GR creation. Through the memory pages and time threshold, the transmission by authorization reference GR is controlled. Each time when an authorization reference is completed, it will also trigger a memory page count and timer reset conducted by the function. The working flow chart is shown in Figure 6.

**Experiment and Analysis**

In the test platform, Xen4.4.2 server is equipped with Intel CPU, 16G’s memory, CentOS6.5 operating system, one PCI crypto card, 10 sets of CentOS6.5 virtual machine with 4G’s memory and two USB-key crypto equipment. Two parts are mainly designed for the test, namely the function implementation and encryption performance tests.

**Functions to Achieve**

The test is to create a virtual password domain through the virtual crypto card management domain at first, and then create a virtual machine on the server and install the crypto card management application program to bind the USB-key with the login permission. When login in is carried out,
insert the USB-key password device firstly for the initialization of identity information. After that, the encryption and decryption functions can be realized accordingly.

Firstly, data encryption is carried out for the tests, and then the tests are implemented under three different conditions, that is, to adopt the legal status of USB-key, illegal status of USB-key and test with no USB-key. In the case of the application of the legal status of USB-key, decryption is completed successfully; in the case of the use of illegal status of USB-key, there is error occurred to the application program and the decryption cannot be completed; for test with no application to the USB-key, the virtual crypto card management procedure cannot be opened to complete the decryption.

Through the tests, the new crypto card virtualization framework can be used to realize the crypto card function, and guarantee the security of the physical crypto card in the virtual environment.

**Performance Testing of Communication Optimization Module**

In this section, the test scheme is designed to adopt communications management module and not to adopt communications management module for data symmetric encryption, so as to test through comparison made to the data consumption time in inter-domain communications and CPU’s utilization rate on the performance optimization capability of the communication management module in inter domain communication process. The test content is to transmit a plurality of files with 64K. In the communications management module, the memory page threshold is set at 32, and the time threshold is set at 1500 (microsecond). The tests adopt Netperf[11] to conduct test to the communications transmission time. The test results are shown in Figure 7.

![Figure 7. The time of inter-domain communication.](image)

At the same time when the test is being conducted to the inter-domain communications time, the test also uses xentop command to extract the CPU utilization information from the privileged virtual machine and the guest virtual machine. The average utilization rate for CPU is shown in Figure 8.

![Figure 8. CPU usage information.](image)
Through the test data, it can be found, with the increasing number of the data packets, that there is a huge reduction to the encryption time after the communications management module is adopted. Besides, the CPU utilization rate in privileged domain also has a huge decrease. Meanwhile, the use rate of CPU in virtual machine has a greater degree of improvement. On the whole, the efficiency of the inter-domain communication is improved greatly by using the communications management module.

Conclusion

In this paper, the author, based on the actual situations, conducted studies on the virtual structure of crypto card and designed a new virtual framework for the use of crypto card in virtual environment. The framework is added with a virtual crypto card domain to the user virtual machine and the privileged domain (crypto card management domain). The test results show that the framework can support the functions of crypto card in the virtual environment, and it has a greater improvement in the security and communications performance compared with the traditional separation drive model. However, there are still some problems in the framework, such as the frequent movement of the virtual machine under cloud environment and the proper design for a suitable movement solution. In communications management module, the threshold setup will have an impact on the performance of communications, thus, how to set a reasonable threshold or set according to the real situations a dynamic threshold to achieve the best performance, etc. is also a problem. Thus, studies on these issues will be carried out continuously.

Acknowledgement

This research was supported by National Key Research Program of China “Collaborative Precision Positioning Project” (No.2016YFB0501900).

References

