Journal of Applied Sciences

ISSN 1812-5654

science alert

ANSInet
an open access publisher
http://ansinet.com

Journal of Applied Sciences 13 (8): 1311-1317, 2013
ISSN 1812-5654 / DOI: 10.3923/jas.2013.1311.1317

Virtual Desktop Information Confidentiality Mechanism Based on Information Flow Model

Wei Ma, Congdong Lv and Xiaoyong Li
School of Computer and Information Technology, Beijing Jiaotong University,
Beijing, 100044, China

Abstract: The application of the virtual desktop in the production system is characterized in saving costs, reducing operation maintenance workload and reducing management difficulty. However, because the overall architecture of the virtual desktop is different from the traditional terminal mode, the availability of the traditional information confidentiality mechanism is not high enough in the virtual desktop environment. So in this study an access control model, Virtual Desktop Information Flow Model (VDIFM) based on the information flow, is proposed, through which the single-direct information flow can be effectively ensured. At the same time, in this study, the prototype system is also designed for verification and tested and the test results show that the model has a certain practicality.

Key words: Virtual desktop, information flow, access control, confidentiality

INTRODUCTION

The virtual desktop (also known as "desktop virtualization" or "client virtualization") means the C/S service model in which the user's personal computer desktop environment is separated from the physical computer through the virtualization technology. Virtual desktop brings a lot of advantages. First, a large amount of independent desktops can be integrated into a small amount of physical servers. Second, users can connect to those virtual desktops with multiple devices such as traditional PCS, thin client terminals, tablet computers, PDAs and smart phones, etc. And the last advantage is that the user's experience is entirely consistent with the traditional PC desktop.

The virtual desktop has many obvious advantages. Firstly, a high-performance server is able to be virtualized into several virtual desktops to reduce the cost of hardware. Secondly, the office flexibility and adaptability are improved and the office costs can be accordingly reduced. And finally, the costs of system management and maintenance will reduce and the efficiency will be improved.

Huge market and economic benefits can arise above the ad- vantages of the virtual desktop. Now, a variety of active virtual desktop products can be found in the market, such as VMware View from VMware, XenDesktop from Citrix, Huawei desktop cloud from Huawei, etc. (Vmware, 2013; Citrix, 2012; Huawei, 2012). The prospect of virtual desktops is also very broad in the market scale. It is predicted by CCW Research that during 2010 and 2015, the complex growth rate in the Chinese desktop virtualization market will reach more than 1.3 billion yuan. The compound growth rate of the Chinese desktop virtualization market will reach more than 60%. Till 2015, the desktop virtualization market scale will reach about 1.1 billion yuan. In 2010, the pilot operation of desktop virtualization was carried out by China Mobile in seven provinces and cities including Guangdong, Fujian, etc. And the pilot scope of desktop virtualization will further expand in the following years. Shanghai Unicom plans to introduce the desktop virtualization into all the call centers of Shanghai Unicom and China Unicom will select more than 10 cities to promote the Shanghai mode.

But the convenience of the virtual desktop technology has also brought some new problems, especially the information confidentiality issue in the desktop environment. In the products type information system, some sensitive or confidential in-formation will be stored and how to ensure that such sensitive or confidential information will not be disclosed has become a hot issue in the research. When the production system is transferred into the virtual desktop environment, such issues still exist and some new features will arise. For example, with traditional terminal mode, some methods will be used to avoid the leakage of sensitive information. Typical methods such as shutting down USB interface, monitoring the plug-and-plug device, etc. However, with

Corresponding Author: Wei Ma, School of Computer and Information Technology, Beijing Jiaotong University, Beijing, 100044, China

virtual desktop environment, those methods will be invalid because the user cannot access the computing platform directly.

Hence, due to the ascending usage of virtual desktop and the risk of information leakage, it is particularly important to design a novel information confidentiality mechanism suitable for virtual desktop features. This mechanism should be able to avoid the leakage of sensitive information effectively and the extra overhead brought by this mechanism should be limited. So in this study an access control model, Virtual Desktop Information Flow Model (VDIFM), is proposed, through which the single-direct information flow can be effectively ensured.

MATERIALS AND METHODOLOGY

Materials

BLP model: The Bell-LaPadula Model (hereafter referred to as BLP Model) was founded in (Bell and LaPadula, 1973), which focuses on the security classification of the military type. In the earliest stage, the BLP Model was the most common computer security model, which affects the development of other models in the future and affects the development of the computer security technology to a large degree (Bishop, 2002; Bell and LaPadula, 1973).

In the BLP Model, the entity able to initiate the action is defined as the subject, such as the system user, process, etc., the action undertaker of the subject is defined as the object, such as data, file, etc. The operation of the subject to the object mainly includes r (read), w (read-write), a (append), e (execute), etc. All the subjects and objects within the system are assigned security levels, the main purpose of the BLP security model is to prevent the subject to read the object with the security permit higher than its security level, the model is a typical confidentiality model, emphasizing the concept of "reading downward and writing upward" and not too much consideration is made to the integrity of the information.

The basic idea of the BLP Model is to ensure that the information cannot flow to the low security level from the high security level, that is, the information can only flow upward in a unidirectional way. This is achieved based on the following two rules:

- **Simple security property:** S can read O and if and only if S dominates O, S has the independent read access authority to O
- **Property:** S can write O, if and only if O dominates of O, S has the independent write authority to O

Wherein, S represents the subject and O represents the object.

Information flow model: Denning (1976) proposed lattice-based information flow model (Bishop, 2002; Denning, 1976) and he pointed out that the information must freely flow in the members of the certain type, that is, to meet the reflexivity; if the members of some type can read information from another type, they can store the achieved information in the object of the first type. In this way, if the member of the third type can read information from the first type, that is, they can read the content of the object of the first type, they can effectively read information from the second type and therefore the transitivity arises. In accordance with the Denning's information flow model, the information flow policy I can be defined as the triple $I = (SC_I, \leq_I, joint_I)$, wherein, SC_I is the collection of security level, $\leq_I$ is the ordered relation of the elements in SC_I, while $joint_I$ is the combination of the two elements in SC_I.

The lattice-based information flow model is suitable for the system conducting detailed classification to the information resources, being a multi-level security model.

Methodology: In this study, methods such as modeling, algorithm design and experiments verification are adopted:

- First, based on the ideas of BLP model and information flow model, virtual desktop system is formalized with symbols and some necessary rules are defined
- Second, an algorithm is designed to describe the access control method in virtual desktop system
- At last, experiments base on prototype are made to verify the function and performance of this model

Section III shows the confidentiality model and section IV illustrates the algorithm of access control method. In section V, functional test and performance test are made, respectively.

CONFIDENTIALITY MODEL

RDP protocol: Among the existing virtual desktop products, VMware View from EMC, XenDesktop from Citrix, etc., are in main stream. Wherein, VMware View adopts the RDP protocol (Forsberg, 2006; Montoro, 2005) to achieve the communication between the user terminal and the desktop environment, while XenDesktop adopts the ICA protocol to achieve communication. With respect to the RDP protocol, the ICA protocol mainly improves the performance. Therefore, the research of the

information flow control of the virtual desktop and the achievement of the prototype system based on the RDP protocol have the common sense.

In the RDP protocol, the virtual channel technology has important application in the virtual desktop environment. The virtual channel is an independent customized data formats associated with the RDP protocol. In an RDP session, the mapping of the device on the client side at the service side can be achieved through the virtual channel and therefore the device on the client side can be assessed in the virtual desktop like the local device. In the original RDP protocol (Zhu *et al*., 2011), the virtual channels for serial port device, printer, file system, clipboard, audio device and smart card device are mainly included. This study mainly focuses on the mapping of the devices possibly causing the flow of the sensitive information, including printers, file system and the clipboard. Through the establishment of the appropriate model, the corresponding mechanism is adopted to control the establishment of the channel when a new RDP conservation is opened, to ensure the information to flow in accordance with the rules, which is the issue to be focused on in this study.

Access control model: Under the virtual desktop environment, the virtual desktop information flow model (VDIFM) can be defined as the quintuple as follows:

$$VDIFM = \{S, D, SC, A, \rightarrow\}$$

where, S represents the subject and can be considered user in the system, D represents the object and can be considered the virtual desktop in the system, SC represents the security level, mainly including disclosure, secret, confidential, top secret, A represents the operation of the subject to the object and can be considered as the virtual desktop here, the authority can be simply divided into r (read) and w (write), → indicates the information flow direction.

However, there is an issue in the above model, that is, in the virtual desktop environment, although the user can be defined as the subject, under the condition that the user is taken as the subject and at the same time the virtual desktop is taken as the object, the access control is conducted in accordance with the model, only the flow of the information from the virtual desktop to the user can be controlled and the external disclosure of the information cannot be ensured. For example, the following disclosure scenes shall be considered:

- The security level of the user S_1 $SC(S_1)$ is higher than the security level $SC(D_1)$ of the virtual desktop D_1, that is, $SC(S_1) \geq SC(D_1)$ and then $D_1 \rightarrow S_1$ can be achieved
- Suppose that the users S_2 and S_1 have a shared printer P, that is, S_1 dom $P \cap S_2$ dom P and at the same time $SC(S_2) \leq SC(D_1)$
- When the user S_1 uses the printer P, $D_1 \rightarrow P$ can be achieved, while because S_2 dom P, the information flow of $D_1 \rightarrow S_2$ is generated

Thus it can be seen that in the virtual desktop environment, the above model must be further refined, to ensure its effectiveness. In accordance with the connection mode between the virtual desktop and the user terminal, the virtual channel can be considered as the true subject to access the information on the virtual desktop and the user is the subject owning such virtual channels. The information flow model can be modified as follows:

$$VDIFM = \{S, S', D, SC, A, \rightarrow\}$$

where, S' represents the collection of subjects owned by the user S, mainly including the three virtual channels of printer, file system and clipboard and S' has its own independent security level.

At the same time, in accordance with the characteristics of the RDP protocol in the virtual desktop environment, the following three rules can be defined:

Rule 1: If S_1' is the access subject of S_1, the security level of S_1 shall dominates the security level of S_1', that is, $SC(S_1) \geq SC(S_1')$.

Rule 1 defines the subordination relation of the subject S_1 and the access subject S_1'.

Rule 2: The security levels of different elements can be different in S', that is, if s_1', s_2', s_3' are the elements of S', there exists no mutual dominant relations between $SC(s_1')$, $SC(s_2')$ and $SC(s_3')$.

Rule 2 defines that the security levels of the different elements in the access subject S' are different and the fine-grained access control to the various terminal devices of the users can be allowed with this rule.

Rule 3: Under the constraint of Rule 1 and Rule 2, the security levels of the elements in S' can differ, while the security level cannot be higher than S and the operation of the change of the security level cannot be completed by S.

Rule 3 enhances the flexibility of this model.

ACCESS CONTROL ALGORITHM

In accordance with the above VDIF model, the corresponding access control algorithm can be designed. The following Fig. 1 is the process of VDIF Design-based Access Control Algorithm:

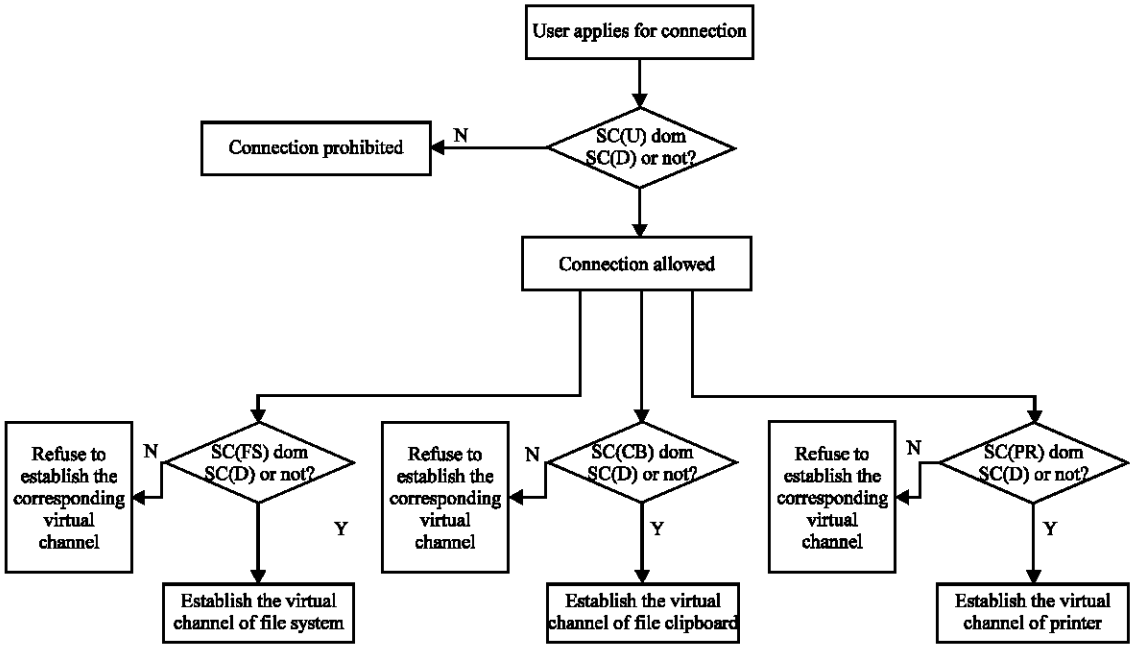

Fig. 1: VDIF design-based access control algorithm process

The algorithm is specifically described as follows:

Algorithm: VitualDesktopAcessControl
Input:
Access request Request=<user,userchannel,virtualdesktop,type>
Output:
View obtained by the visitor
Algorithm Processing Process:
[Step 1]
Obtaine the security level of the access subject: SC_{user}=getSC(user);
Obtain the security level of the virtual desktop of the object: $SC_{desktop}$=getSC (virtualdesktop);
[Step 2]
if $SC_{user} \geq SC_{desktop}$
then
connection established
else
refuse the request
[Step 3]
Obtain the security levels of the actual access subjects respectively:
$SC_{filesystem}$=getSC(virtualchannel1),
$SC_{clipboard}$=getSC(virtualchannel2),
$SC_{printer}$=getSC(virtualchannel3),
[Step 4]
if $SC_{filesystem} \geq SC_{desktop}$
then
virtualchannel$_{filesystem}$ established
else
refuse to establish virtualchannel$_{filesystem}$
if $SC_{clipboard} \geq SC_{desktop}$
then
virtualchannel$_{clipboard}$ established
else
refuse to establish virtualchannel$_{clipboard}$
if $SC_{printer} \geq SC_{desktop}$
then
virtualchannel$_{printer}$ established
else
refuse to establish virtualchannel$_{printer}$

Through the comparison of the security level between the subject and the object, the algorithm decides whether to establish the connection and whether to agree to open the corresponding virtual channel. In this way, it is ensured that the information can only flow to subject with a higher level from the object with a lower level, to achieve the unidirectional flow of the information and effective control the external disclosure of the sensitive information.

RESULTS

In order to verify the functionality and practicality of the model, in this study, the prototype based on Xen and the remote desktop client terminal rDesktop of Linux is implemented to apply the experimental testing. And the experimental environment is shown as following:

Server side: CPU: Intel Core i5-750, Memory: 8G, Operating, System: CentOS 5.5, Hypervisor: Xen 4.1.2.

Virtual desktop: Operating System: Windows XP SP3, RDP Version: 5.5.

Client side: Operating System: CentOS 5.5, RDP.

Software: rDesktop 1.7.0.

Network: 100M LAN.

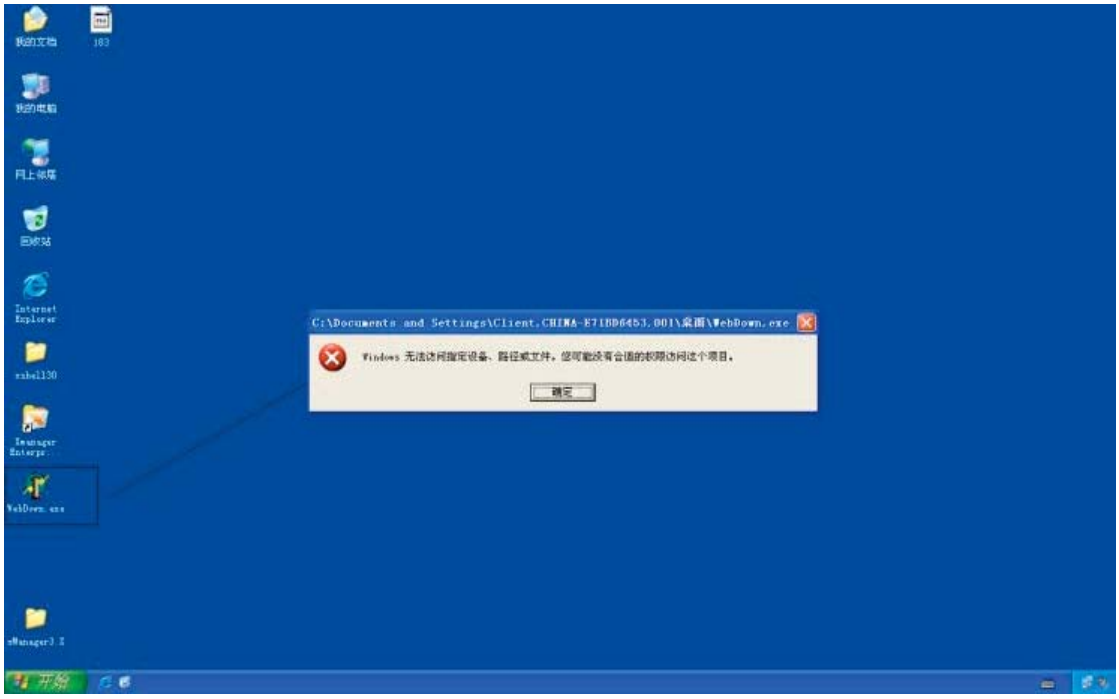

Fig. 2: File access rejection with VDIFM mechanism

The prototype testing is consisted of two parts. The first one is the functional test and the second part is performance test.

Functional test: The user uses rDesktop on the client side to connect the virtual desktop undertaken on the server side. In this study, modification is made to rDesktop, to enable it to support the judgment of the security level. A series of actions will be taken when a new RDP session is initiated. Firstly, rDesktop will check the security level of the user to determine to establish the RDP connection or not. Secondly, the security levels of virtual channels will be checked, respectively to determine that the corresponding virtual channel should be established or not.

The test results are shown as follows:

- When the user's security level is lower than the security level of the virtual desktop to be accessed, the connection establishment shall be prohibited
- When the security level of the user's virtual channel is lower than the security level of the virtual desktop, the virtual channel connection establishment shall be prohibited

Figure 2 in the following is the interface that the user cannot skip the security level to access the resources in the prototype system.

Performance assessment: Meanwhile in this study, based on the prototype system, the performance is also assessed through the comparison of the time consumed in the copying the files of various sizes between the client side and virtual desktop before and after the establishment of the virtual channel. The performance comparison before and after the involvement of the model is shown in Fig. 3 in the following.

As shown in Fig. 3, the affection of the model to the overall service performance is very slight, the performance loss is remained between 5 and 6%, so there is a very high feasibility in the introduction of the model into the production system.

DISCUSSION

With the results, it is shown that the mechanism proposed in this study is effective and efficient. First, it is illustrated that the attempt of unauthorized access of sensitive resource will be rejected by the mechanism. Second, the performance cost of this mechanism is acceptable within production environment.

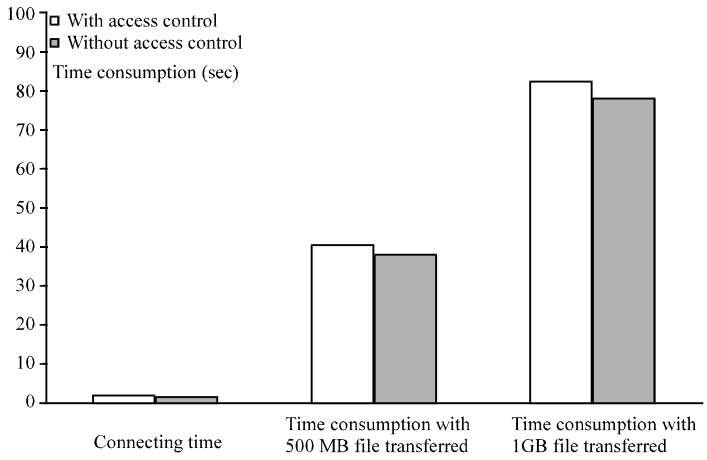

Fig. 3: Comparison of time overhead when copying various size of files with VDIFM

There are some researchers who have been work on related areas and the achievements would be discussed here. Literature (Wang *et al*., 2011) discusses the comparison of security of several different virtual desktop protocol such as PcoIP, RDP, SPICE and ICA. In literature (Li and Zhang, 2011), the usage of cryptology in virtual desktop is discussed. Literature (Yan and Li, 2012) uses filter driver in windows to control information flow in virtual desktop but this method totally relies on the client and is by-passable.

CONCLUSION

With the extensive application of the virtualization technology, the virtual desktop is also widely applied and the importance of the information confidentiality in the virtual desktop environment has become increasingly prominent. In this study, in the view of the unique characteristics of the virtual desktop environment, the information flow model of the virtual desktop is designed, the access control algorithm based on this model is also provided and finally the corresponding prototype system is achieved and the system testing results are given, providing certain reference significance to the confidentiality in the virtual desktop environment.

ACKNOWLEDGM ENT

This work was supported by Research Fund for the Doctoral Program of Higher Education of China (RFD-P20120009110007),Program for Innovative Research Team in University of Ministry of Education of China (IRT201206) and Program for Science and Technology Research and Development of Ministry of Railway of China (2012X010-B).

REFERENCES

Bell, D.E. and L.J. LaPadula, 1973. Secure computer systems: A mathematical foundations. MTR-2547, The MITRE Corporation, Bedford, Massachusetts, pp: 1-42.

Bishop, M., 2002. Computer Security: Art and Science. 1st Edn., Addison-Wesley Professional, New York, ISBN-13: 9780201440997, Pages: 1136.

Citrix, 2012. XenDesktop. Citrix Systems Inc., USA. http://www.citrix.com/products/xendesktop/overview.htm l2012.

Denning, D.E., 1976. A lattice model of secure information flow. Commun. ACM, 19: 236-243.

Forsberg, E., 2006. Reverse-engineering and implementation of the RDP 5 protocol. http://efod.se /media/thesis.pdf

Huawei, 2012. Desktop cloud solutions. Huawei Technologies Co. Ltd. http://enterprise.huawei.com /en/solutions/cloudcomputing/desktop-cloud /index.htm

Li, F.H. and B.L. Zhang, 2011. Discussing on cryptography application schema in cloud computing. Netinfo Secur., 9: 53-55 (In Chinese).

Montoro, M., 2005. Remote desktop protocol, the good the bad and the ugly. http://www.oxid.it /downloads/rdp-gbu.pdf

Vmware, 2013. Deliver desktop services from your cloud for end-user freedom and IT control. http://www.vmware.com/products/view/overview.html.

Wang, F., F. Jiang and C.Y. Li, 2011. Virtual desktop and key technology analysis. Telecommun. Technol., 1: 24-26 (In Chinese).

Yan, Z.X. and X.Y. Li, 2012. One-way control of the information in security virtual desktop. Chinese Scientific Papers Online. http://www.paper.edu.cn/releasepaper/content/201204-46.

Zhu, Y.H., B.J. Shen and B. Jin, 2011. Design and implementation of virtual cryptographic device system. Comput. Eng., 37: 108-110.