

Secured VM Live Migration in Personal Cloud

Wei Wang[†], Xiaoxin Wu[†], Ben Lin[‡], Kai Miao[‡], Xiaoyan Dang[†]

[†]Intel Labs, [‡]Intel Information Technology
{vince.wang, xiaoxin.wu, ben.y.lin, kai.miao, xiaoyan.dang}@intel.com

ABSTRACT

The security issue that resides in VM live migration is a critical factor for its acceptance by IT industry. We propose to leverage Intel vPro and TPM to improve security in virtual machine live migration. A role-based mechanism is introduced, under which the VM migration is controlled by specific policies that are protected in seal storage. In the proposal, we also introduce remote attestation that does platform measurement before migration.

Categories and Subject Descriptors

H.4.0 [Information Systems]: Information Systems Applications –General. K.6.5 [Information Systems]: Management of Computing and Information Systems –Security and Protection.

General Terms: Design, Security

Keywords: Live migration, vPro, TPM, Virtualization, Personal cloud

1. Introduction

Virtualization technologies can significantly change enterprise client computing. Virtualization can increase agility because IT can introduce new capabilities and upgrade platforms more quickly. Virtualization can also reduce TCO (total cost of ownership). By abstracting the OS from the hardware platform, IT can simplify service provisioning, with a reduced building time and integration cost. Virtualization also opens the door to new usage models, such as delivering the IT environment as a managed VM while letting employees use a personal device, to keep the same working environment [4] although employee is not using a device provided and managed by IT.

Virtualization embraces multiple technologies at differing stages of maturity, which poses new questions about the optimal enterprise client computing architecture. In our work, we extend Cloud usage to personal environment, because today an individual may have multiple computing or communication devices. For example, a person may have a cellular phone or a Mobile Internet Device (MID) that he always carries with him. He probably also has a laptop or a desktop that has a stronger CPU/GPU set, a larger MEM/disk, a friendly input interface, and a larger display. This stronger device may probably be left somewhere (e.g., office or home) because of inconvenience for portability. Once the owner carries a handheld and approaches the stronger devices, e.g., when he is set at the office or at home, he can jointly use smart phone/MID and laptop/desktop through different network connections to form a personal Cloud. A user can also migrate a work from laptop to a MID or phone when he is going to a meeting room.

Our vision for future personal-centralized Cloud environment where a personal handheld device, e.g., MID, is probably the center of personal life [5], is shown in Figure 1. There is a public Cloud that is managed by Enterprise IT center. A Cloud user can access such Cloud through corporate network or VPN. There is

also a personal Cloud, which are built up by a personal handheld device and its surrounded computing or customer electronic (CE) devices. The inter-connection for the components in a personal Cloud may be, for example through near field communication (NFC) technology, under which the underlying networks can be direct cable connection or wireless networks (e.g., WLAN, WPAN, Bluetooth, etc.).

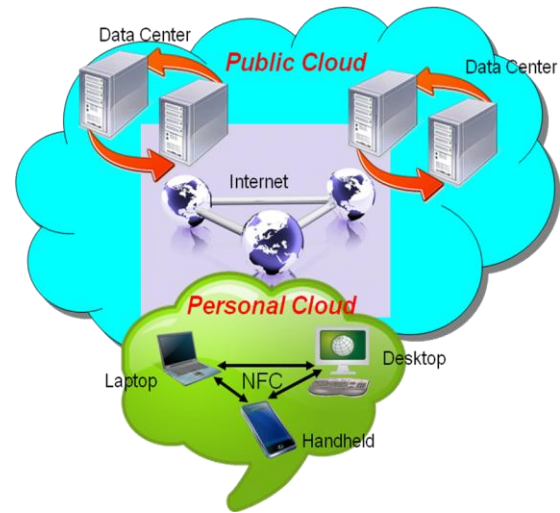


Figure 1 A future Cloud usage in enterprise environment

Live migration is a useful feature and natural extension to virtualization technology that allows for the transfer of a virtual machine from one physical machine to another with little or no downtime for the services hosted by the virtual machines. The migration functionality implemented by vendors such as XEN [1], and KVM (kernel-based virtual machine) [2] now exposes the entire machine state of a VM to device module which listens to the incoming live migration requests from remote platforms. An attack can easily hijack the device module process or Hypervisor where these migrations occur. If the process is hijacked, the information of the migrated virtual machine including states of operation system kernel, applications and services running within the operating system, the sensitive data currently being used by those applications and even the inputs from keyboard are accessible to the hackers.

In cloud computing environment, a user can't guarantee that every connected physical machine can meet the security requirement for live migration. Without doing any platform measurement, live migration is at significant security risk. If insecure migrations are processed an attacker then is able to compromise the integrity of the virtual machine being migrated.

This poster presents security solutions for VM live migration among un-trusted/open platforms in personal clouds. In particular,

this work proposes methodologies for 1) checking/verifying the security level of a migration destination and 2) defining migration policy. The solution is based on a trusted computing base (TCB) [9] that should only include a small part of software and hardware. Security depends on these software and hardware that distinguish from a much larger amount that can misbehave without affecting security. Because any vulnerability in the TCB can potentially be exploited by an attacker to initiate serious attacks, in this work, we make the TCB small enough, which only includes vPro hardware and the secure hypervisor. To serve for enterprise scenario, the secure hypervisor is designed in a way so that it is able to be updated from IT center during secure migration process.

2. Secured Live Migration

In this security framework we propose a Policy-controlled secure live migration that is based on Intel vPro hardware platform for virtual machine migration protection. Figure 2 shows the high level architecture of this proposal.

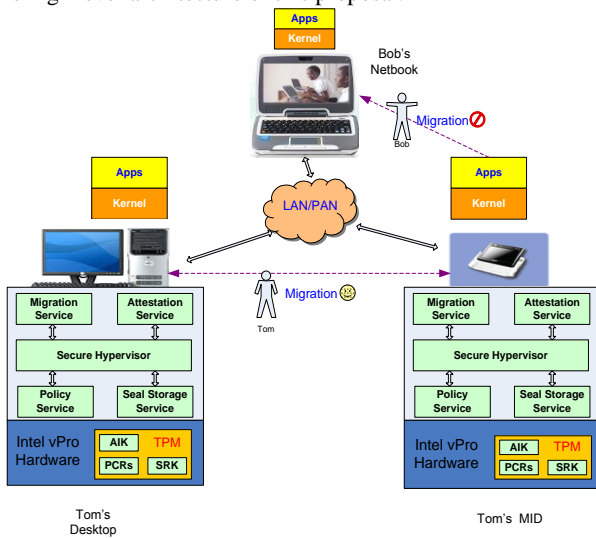


Figure 2 Architecture of Secured Live migration

This design depends on the following features that hardware may support.

- All platforms support sealed storage and remote attestation.
- Intel vPro technology is enabled.

Figure 2 shows a typical usage scenario. Tom migrates one of his virtual machines between its devices with the underlying secure framework. At the same time, he updates policies for the virtual machine to the policy server in the targeted device. When Bob asks Tom to migrate this VM to his machine, according to the policy the migration is forbidden, either because the virtual machine is not allowed to migrate out, or because the operating environment at Bob's machine cannot reach a required security level. Note that it may happen the VM cannot be migrated to another device of Tom as well, due to the same reasons.

2.1 Security Modules

We implement a secure hypervisor which consists of the following modules:

Attestation Service: This module allows a running hypervisor to cryptographically identify itself to a remote hypervisor, that is, to tell the remote hypervisor what is running

inside the secure box. This allows the remote hypervisor trust the application, i.e. to be confident that any application will behave as required.

Seal Storage: This module encrypts data using the private key of the tamper resistant TPM that is responsible for attestation. A hash of the booted trusted OS is also included with the encrypted data. The TPM only allows a trusted OS with the same hash to unseal it. This functionality is used by the secure hypervisor to persistently store its private key and role-based policies.

Policy Service: This module parses and manages the role-based policies provisioned with the VM image for virtual machine migration decisions, such as who has the right to migrate a virtual machine, and to which hosts this virtual machine can be migrated.

Migration Service: This module is responsible for migration. One of its duties is initiating attestation requests to remote machines to check whether the target machines meet the security requirement, and if not, it will require them to do software upgrade or patching.

Secure Hypervisor: This module protects the process of guest OS by Runtime Memory Measurement [7].

The proposal relies on the key technologies, e.g. Intel vPro and TPM, to enhance the security level for virtual machine migration. They provide the following abilities:

- The ability that makes the virtual machine work in an open environment in a secure way.
- The ability to encrypt and store keys, data or other secrets within hardware on the platform, which makes sure that these secrets can only be released (decrypted) to an executing environment that has the same level of security as when the secrets were encrypted
- The ability of remote attestation to ensure that the trustworthy environment was correctly invoked.

These features help the scheme to secure Virtual Machine during migrations between open platforms.

2.2 Building trustworthy container for virtual machine

The design uses remote attestation to check whether the target virtual machine container meets the security requirement for the virtual machine being migrated. The detailed flowchart is shown in Figure 3. After a successful attestation, i.e., when the target host of the virtual machine meets the security requirement, the session for live migration starts.

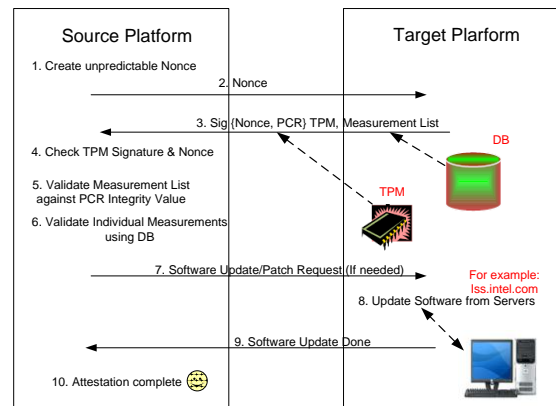


Figure 3 Build trustworthy container for virtual machine

2.3 Role-based live migration

After building the trustworthy virtual machine container, one session for the virtual machine migration will be started as shown in Figure 4.

The detail description for this role-based live migration is shown below. A VM will be either migrated to a host, or migrate out from the host.

Migrate-out: (flowchart with green lines): The owner of a VM initiates one outgoing request to the migration service module (Step 4). This service checks whether this move is allowed by checking the policy service module, which makes migration permission according to pre-deployed policies for this virtual machine. After the migration service gets the “Allow” permission from the policy service module, it gets key and certificate from the seal storage module to encrypt the entire state of the virtual machine, and then migrates the virtual machine to the targeted platform.

Migrate-in (flowchart with red lines): The owner of VM initiates one incoming migration request to the migration service module. At the mean time, policies regarding to this VM are loaded. After validating the policies, the policy service module stores it to his local environment in seal storage.

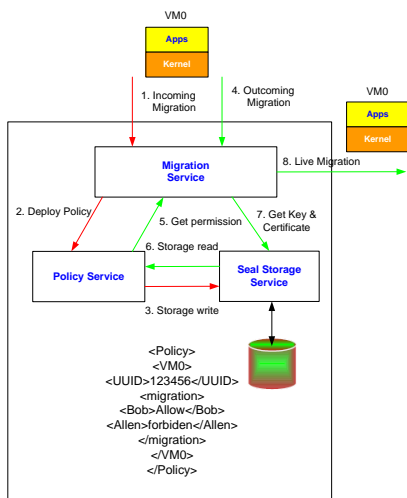


Figure 4 Role-based live migration

2.4 Secured hypervisor

Finally, the overall secure framework uses a secured hypervisor design that provides the protection on key applications in a Guest VM. We adopt the work in [6] and [7] to provide runtime memory protection. In this proposal, we utilize hardware techniques to provide trust services to software programs. Without modifying OS, we leverage Intel vPro technology to create a lightweight hypervisor for fine-grain software runtime memory protection. As a result, a program’s memory could be hidden from other high-privilege system softwares in a single commodity OS. The detailed design of secure hypervisor and its functions are shown in Figure 5.

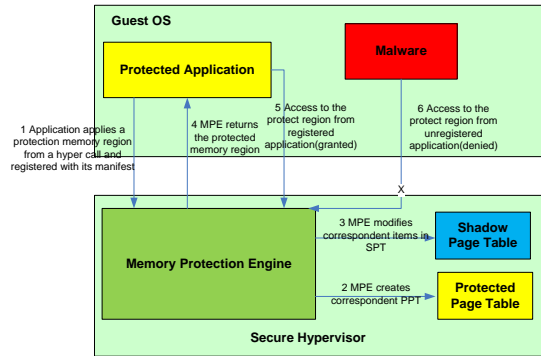


Figure 5 Secure hypervisor

3. References

- [1] P. Barham, B. Dragovic, K. Fraser, S. Hand, T. Harris, R. N. Alex Ho, I. Pratt, and A. Warfield, “Xen and the Art of Virtualization”, in *proceedings of ACM Symposium on Operating Systems Principles*, 2003.
- [2] KVM Forum, <http://www.linux-kvm.org>
- [3] Christopher Clark, Keir Fraser, Steven Hand, Jacob Gorm Hansen, Eric July, Christian Limpach, Ian Pratt, Andrew Warfield, “Live Migration of Virtual Machines”, in *NSDI 2005*.
- [4] John Dunlop, “Developing an Enterprise Client Virtualization Strategy”, in *Intel IT White Paper*, 2008
- [5] X Wu, W Wang, B Lin, K Miao, “Composable IO: A Novel Resource Sharing Platform in Personal Clouds”, in *CloudCom 2009*
- [6] Brannock Kirk, Dewan Prashant, McKeen Frank, Savagaonkar Uday, “Providing a safe execution environment”, *Intel Technology Journal*, Jun 2009, Vol. 13 Issue 2, p36-51
- [7] Dewan, P., Durham, D., Khosravi, H., Long, M., and Nagabhushan, G. 2008. “A hypervisor-based system for protecting software runtime memory and persistent storage”. In *Proceedings of the 2008 Spring Simulation Multiconference (Ottawa, Canada, April 14 - 17, 2008)*.
- [8] Ravi Sahita et al. “Towards a Virtualization-based Framework for Information Traceability”, *Advances in Information Security—Insider Attack and Cyber Security*, ISBN 978-0-387-77321-6.
- [9] B. Lampson, M. Abadi, M. Burrows and E. Wobber. “Authentication in Distributed Systems: Theory and Practice”, *ACM Transactions on Computer Systems*, page 6, 1992.