VIRTUAL MACHINE MIGRATION

PERFORM TRUSTED BOOT OF VM IN 1ST ZONE

STORE TRUST VALUES FROM BOOT OF VM

INITIATE MIGRATION TO NEW ZONE

ACCESS TRUST VALUES FROM TRUSTED BOOT

DETERMINE IF TRUST VALUES OK

IF NOT, PERFORM PREDETERMINED ACTION

Publication Classification

Int. Cl. G06F 21/00 (2006.01)

U.S. Cl. ........................................................................ 726/25

ABSTRACT

Attesting a virtual machine that is migrating from a first environment to a second environment includes in response to initiation of migration of the virtual machine from the first environment to the second environment, accessing one or more stored trust values generated during the trusted boot of the virtual machine in the first environment, determining if the accessed trust values define a security setting sufficient for the second environment, and if the accessed trust values do not define a security setting sufficient for the second environment, performing a predetermined action in relation to the migration of the virtual machine to the second environment.
Fig. 2
PERFORM TRUSTED BOOT OF VM IN 1ST ZONE

STORE TRUST VALUES FROM BOOT OF VM

INITIATE MIGRATION TO NEW ZONE

ACCESS TRUST VALUES FROM TRUSTED BOOT

DETERMINE IF TRUST VALUES OK

IF NOT, PERFORM PREDETERMINED ACTION
VIRTUAL MACHINE MIGRATION

CLAIM FOR PRIORITY


BACKGROUND

[0002] 1. Technical Field

[0003] This invention relates to a method of and system for, attesting a virtual machine migrating from a first environment to a second environment. More specifically, the invention provides the re-attestation of migrated virtual machines.

[0004] 2. Description of the Related Art

[0005] A virtual machine provides a complete system platform which supports the execution of an operating system. An essential characteristic of a virtual machine is that the software run by the virtual machine is limited to the resources and abstractions provided by the virtual machine. In the case of virtual machine migration, the entire memory contents of the running system is moved over the network as it migrates from a source physical system to a target physical system. When the memory pages are moved over the network, they are more vulnerable to a particular type of cyber attack.

[0006] It is the case in virtual machine migration that the attestation on the original physical system may have been less stringent than what is required by the security level of the target system. For example security zones can be used within a private cloud which has a test zone and a release zone. These operational zones would have different security policies based on the sensitivity of the data being processed and the criticality of the system operating within the perspective zones. The separate security policies governing these zones could include trusted boot requirements, security configuration, firewall and anti-virus software, for example.

[0007] The virtual machines in the test zone are instantiated and removed frequently, as is the nature of test systems. Once a test system is approved for release for general availability, it would be migrated out to the release zone. However the release zone would have stricter security requirements. An enterprise would want this migration to proceed with the same automation and ease of migration, and with the (re) attesting to a higher security level integrated into this process.

BRIEF DESCRIPTION OF THE DRAWINGS

[0011] Embodiments of the present invention will now be described, by way of example only, with reference to the accompanying drawings, in which:

[0012] FIG. 1 is a schematic diagram of a virtual machine migrating between two zones.

[0013] FIG. 2 is a schematic diagram similar to FIG. 1, showing more detail.

[0014] FIG. 3 is a flowchart of a method of migrating a virtual machine.

[0015] FIG. 4 is a further schematic diagram similar to FIG. 1.

DETAILED DESCRIPTION

[0016] Owing to the invention, it is possible to automate, within a migration process, the re-attesting to a higher or different security level during virtual machine migration. Currently as part of the TCG (Trusted Computing Group) standardized architecture, a system is remotely attested and allowed to connect to a network. Remote attestation is the action of an external trusted security management unit requesting security parameters or measurements from the computer system under inspection. Within the TCG architecture, this process of attestation and connection is called a TNC (Trusted Network Connect). Currently the TNC attestation process only occurs during the system’s initial connection to the network. The invention provides the capability that a virtual machine that has been TNC attested for one VLAN or security zone, once it is being migrated to a different VLAN and security zone with different security requirements will be checked before the virtual machine migration can go ahead.

[0017] In one embodiment, the predetermined action in relation to the migration of the virtual machine to the second environment comprises preventing the migration of the virtual machine. If the stored trust values are not sufficient for the security settings of the new environment, then one way of dealing with this situation is to prevent the virtual machine from migrating to the second environment.
from migrating to the new environment. This will ensure that if there is any way that the virtual machine is compromised with respect to the second environment, then the virtual machine will not be able to operate in that environment. The migration process will be halted and will not complete.

In a different embodiment, the predetermined action in relation to the migration of the virtual machine to the second environment comprises completing the migration of the virtual machine and placing limits on the operation of the virtual machine in the second environment. In this embodiment, if the stored trust values are not sufficient for the security settings of the new environment, then the migration can still be allowed to go ahead, but with reduced options for the virtual machine in the new environment. For example, the virtual machine may be limited in the nature of the operations that it can execute, or the communication channel that the virtual machine will use in the new environment will have limits placed on it. Specific monitoring of the virtual machine may also take place, to ensure that nothing is compromised as a result of the migration and operation of the virtual machine in the target environment.

Preferably, the method further comprises, following the initiation of the migration of the virtual machine to the second environment, transferring the stored trust values generated during the trusted boot of the virtual machine to a trusted management unit for the second environment. The stored trust values for the virtual machine that is being migrated can be bound to the virtual machine and will always be transferred whenever the virtual machine is migrated to a new environment. This is useful, as the component that originally authenticated the virtual machine through the trusted boot process may not be the same component that needs to authenticate the virtual machine when it is migrated to the new environment. A trusted management unit for the second environment can then access the stored trust values for the virtual machine and compare these to the security settings required for the second environment.

A virtual machine 10 is shown in FIG. 1. The virtual machine 10 is located in a first environment (or zone) 12 and is being migrated to a second environment (or zone) 14. Virtual machines allow the sharing of the underlying physical hardware resources between different virtual machines, each running its own operating system. As a result of the use of virtual machines, multiple operating system environments can co-exist on the same hardware, in isolation from each other, and the virtual machine 10 can provide an instruction set architecture that is somewhat different from that of the real hardware underlying the virtual machine 10. The use of a virtual machine 10 provides the user with direct access to the operating system and applications of the virtual machine 10.

The migration of the virtual machine 10 can occur for a number of reasons. The first environment 12 may be a specific server that is becoming overloaded because multiple virtual machines are being run on the server and they are using an increasingly large amount of resources. There will be a management unit present that manages the load on the server and it may be decided that maximum capacity is being approached and it is therefore desirable to migrate the virtual machine 10 to a different server. The management unit will organize the wholesale copying of the memory allocated to the virtual machine 10 to the new server represented by the second environment 14.

Alternatively, the two environments 12 and 14 may be located on the same physical machine, but have different settings. The first environment 12 may be a test zone and the second environment 14 may be a production zone, for example. Different security settings will apply to the different zones 12 and 14, even though they are located on the same physical hardware. However, a virtual machine 10 that is located in the test zone 12 may be migrated to the production zone 14, for example, under the instruction of an administrator of the server that is running the two zones 12 and 14. In the case of the virtual machine 10 being moved between zones on the same physical computer, it is unlikely that the entire memory contents would be copied, as there is no need since the physical memory may be used by a virtual machine 10 in both zones. It is more likely that the underlying virtualization system will change configuration to move to the new zone, e.g., network settings may be changed to execute the migration.

When a system is moved from one zone 12 to another zone 14, the migrated virtual machine 10 may reside in a different physical system, or may just be configured to run on a different VLAN (Virtual Local Area Network). The virtual machine 10 may move under the management of a separate virtual manager such as IBM Director or HMC (Hardware Management Console) or may remain under the control of the same virtual manager, but require a higher level of security requirements. The security of a virtual machine 10 is checked when it is first loaded, in a so-called “trusted boot”. When the virtual machine 10 is booted certain trust values are captured during the boot process.

The one or more servers providing the virtual machines 10 will implement a trusted boot and remote attestation by allowing an initial enrollment where the virtual machine 10 sets the trust values for the system. A virtual machine 10 is booted and all of its boot and bring-up trust measurements are established by a vTPM (virtual Trusted Platform Module) process and stored in platform configuration registers 16, known as PCRs, shown in FIG. 2. During the initial enrollment, the virtual machine 10 will report these PCR values to a director unit 18, which will in turn store these values as the virtual machine’s base trust values. At any time moving forward, the director unit 18 may ask the virtual machine 10 for its current PCR values. The unit 18 will then compare some or all of these PCR values to the initial base trust values. If they do not match, then a security alert is asserted. The director unit 18 may obtain the original trust values in other ways besides during the enrollment process, which is one representative technique by which the director unit 18 can acquire the trust values.

This model is extended to solve the issue of migration of a virtual machine 10 when crossing security zones. Prior to moving the virtual machine 10 into its target security zone 14, the director unit 18 will transfer the VMs Base Trust Values. These values will be transferred to a trusted management unit 20 in the new zone 14. This could be the IBM Director controlling the target security zone 14, a third party trusted boot authority for the target security zone 14, or a component within the same directory managing the target security zone 14. In the embodiment shown in FIG. 2, the management unit 20 is a separate component specific to the target zone 14.

The method of performing the migration is summarized in FIG. 3. This method provides a way of attesting a virtual machine that is migrating from a first environment to a second environment. The method first comprises step S1, which is the step of performing a trusted boot of the virtual
machine in the first environment, and second, a step S2 of storing one or more trust values generated during the trusted boot of the virtual machine. As detailed above, when a virtual machine is first booted in the first zone, then a trusted boot is performed and the trust values generated during that boot process are recorded in a way that binds them to the specific virtual machine.

[0027] The next step in the process comprises step S3, which is the step of initiating the migration of the virtual machine to the second environment. It is not material why the virtual machine is being migrated, only that a component has decided to attempt to migrate the virtual machine to the new zone. The next step is step S4 of accessing one or more stored trust values generated during the trusted boot of the virtual machine, which is followed by step S5 of determining if the accessed trust values define a security setting sufficient for the second environment. The trust values generated during the trusted boot provide information about the virtual machine being run, such as the nature of the operating system and any updates applied.

[0028] Finally at step S6, if the accessed trust values do not define a security setting sufficient for the second environment, then a predetermined action is performed in relation to the migration of the virtual machine to the second environment. In one embodiment, this predetermined action is the prevention of the migration from taking place, but other actions are also possible. Since the trust values provide information about the virtual machine, these trust values can be said to define a security setting in the context of a security requirement of the new zone. For example, the new zone may specify that any virtual machine operating in the zone has a specific update applied to it. This can be determined from the trust values generated during the original trusted boot.

[0029] The migration of the virtual machine 10 from a first zone 12 to a second zone 14 can be organized around a comparison of the security policies of the two different zones 12 and 14. Prior to virtual machine migration from a source security zone 12 or vLAN to different target security zone 14 or vLAN, the source attestation authority will report the PCR values, event logs, and dated history of attestations, including previous PCR values and event logs, to the target attestation authority. Also prior to the virtual machine migration, the source attestation authority will also report its security attestation policy to the target attestation authority in the new zone 14.

[0030] The target attestation authority will compare its own security attestation policy with the received policy. It will determine if the source policy is equivalent or better than the target policy. The target attestation authority will also examine the attestation log history. If the log history meets the target’s policy on minimal attestation failures, remediations, attestation frequency and concerns about other security zones or vLANs, then no immediate attestation is needed and a typical migration is allow. Finally, if the above criteria is not met, then the migration is permitted to occur, but the target virtualization mechanism confines the virtual machine to a separate vLAN until a new attestation and security check can be performed and verify that the migrating VM meets the security requirements of the target.

[0031] Post-migration re-attestation of a migrating VM is illustrated in FIG. 4. The director unit 18 that relates to the first environment has a log history 22 for the specific virtual machine 10 and also its own policy 24 in relation to the security settings that are relevant for virtual machines that are booted in the first zone. The management unit 20 for the second zone 14 also has its own policy 26. The director unit 18 passes the log history 22 and the security policy 24 to the management unit 20. This information enables the unit 20, which is responsible for allowing the migration of the virtual machine 10 to proceed or to be restricted in some way, to determine whether the trust values of the virtual machine 10 are sufficient for the new zone 14.

1. A method of attesting a virtual machine migrating from a first environment to a second environment comprising: in response to initiation of migration of the virtual machine from the first environment to the second environment: accessing one or more stored trust values generated during trusted boot of the virtual machine in the first environment; determining that the accessed trust values define a security setting that is not sufficient for the second environment; and in response to the determination that the accessed trust values define the security setting that is not sufficient for the second environment, performing a predetermined action in relation to the migration of the virtual machine to the second environment.

2. The method of claim 1, wherein performing the predetermined action in relation to the migration of the virtual machine to the second environment comprises preventing the migration of the virtual machine.

3. The method of claim 1, wherein performing the predetermined action in relation to the migration of the virtual machine to the second environment comprises completing the migration of the virtual machine and placing limits on the operation of the virtual machine in the second environment.

4. The method of claim 1 further comprising transferring the stored trust values to a trusted management unit for the second environment.

5. A system for attesting a virtual machine migrating from a first environment to a second environment comprising: a computer processor; and a computer readable storage medium comprising a trusted management unit executable by the computer processor to: responsive to initiation of migration of the virtual machine from the first environment to the second environment: accessing one or more stored trust values generated during trusted boot of the virtual machine in the first environment; determining that the accessed trust values define the security setting that is not sufficient for the second environment; and in response to the determination that the accessed trust values define the security setting that is not sufficient for the second environment, performing a predetermined action in relation to the migration of the virtual machine to the second environment.

6. The system of claim 5, wherein performing the predetermined action in relation to the migration of the virtual machine to the second environment comprises preventing the migration of the virtual machine.

7. The system of claim 5, wherein performing the predetermined action in relation to the migration of the virtual machine to the second environment comprises completing the migration of the virtual machine and placing limits on the operation of the virtual machine in the second environment.
8. The system of claim 5, wherein the trusted management unit is further executable by the computer processor to transfer the stored trust values to a trusted management unit for the second environment.

9. A computer program product on a tangible computer readable storage medium for attesting a virtual machine migrating from a first environment to a second environment, the product comprising instructions executable by a computer to cause the computer to perform:
   
   - responsive to initiation of migration of the virtual machine from the first environment to the second environment:
     - accessing one or more stored trust values generated during trusted boot of the virtual machine in the first environment;
     - determining that the accessed trust values define a security setting that is not sufficient for the second environment; and
   - in response to the determination that the accessed trust values define the security setting that is not sufficient for the second environment, performing a predetermined action in relation to the migration of the virtual machine to the second environment.

10. The computer program product of claim 9, wherein the instructions for performing the predetermined action in relation to the migration of the virtual machine to the second environment comprise instructions for preventing the migration of the virtual machine.

11. The computer program product of claim 9, wherein the instructions for performing the predetermined action in relation to the migration of the virtual machine to the second environment comprise instructions for completing the migration of the virtual machine and placing limits on the operation of the virtual machine in the second environment.

12. The computer program product of claim 9, further comprising instructions for transferring the stored trust values generated during the trusted boot of the virtual machine to a trusted management unit for the second environment.