XXII Seminarium

ZASTOSOWANIE KOMPUTERÓW W NAUCE I TECHNICE' 2012
Oddział Gdański PTETiS
Referat nr 14

MECHANIZMY OCHRONY INTEGRALNOŚCI PLIKÓW NA POZIOMIE MONITORA MASZYNY WIRTUALNEJ

Jerzy KACZMAREK[1], Michał WRÓBEL[2]

1. Wydział Elektroniki, Telekomunikacji i Informatyki, Politechnika Gdańska
tel: (58) 347 26 82 fax: (58) 347 27 27 e-mail: jkacz@eti.pg.gda.pl
2. Wydział Elektroniki, Telekomunikacji i Informatyki, Politechnika Gdańska
tel: (58) 347 10 37 fax: (58) 347 27 27 e-mail: wrobel@eti.pg.gda.pl

Streszczenie: Mechanizmy ochrony integralności plików umożliwiają wykrywanie nieautoryzowanych zamian w kluczowych do działania systemu operacyjnego plików. Dotychczas rozwiązania tego typu działały jako aplikacje systemowe lub były integrowane z jądrem systemu operacyjnego. Wraz ze zwiększeniem dostępności technik wirtualizacji pojawiła się możliwość przeniesienia systemu ochrony na poziom monitora maszyny wirtualnej, co zapewnia izolację mechanizmu ochrony od chronionego systemu operacyjnego. W artykule opisano projekt systemu ochrony integralności działającego na poziomie monitora maszyny wirtualnej. Przedstawiono wady i zalety takiego rozwiązania. Omówiono również problemy konieczne do rozwiązania przed implementacją mechanizmu ochrony integralności plików na poziomie monitora maszyny wirtualnej.

Słowa kluczowe: bezpieczeństwo, wirtualizacja

1. WSTĘP

Zagadnienie bezpieczeństwa we współczesnej informatyce jest problemem niezwykle istotnym. Istniejące rozwiązania informatyczne pozwalają na ochronę danych użytkowników oraz samego systemu operacyjnego. Rozwiązania te można podzielić na takie, które chronią system przed atakiem, oraz takie, które pozwalają na wykrywanie i minimalizowanie skutków włamań. Do tej drugiej grupy należy m.in. opracowany przez autorów mechanizm o nazwie *ICAR*. Jest to system ochrony integralności plików, który pozwala na wykrycie włamania na podstawie monitorowania zmian kluczowych plików systemu operacyjnego. W celu poprawy skuteczności działania zaprojektowany mechanizm działa na poziomie jądra systemu operacyjnego, dzięki czemu możliwa jest ciągła ochrona wybranych plików. Dodatkowo *ICAR* automatycznie przywraca zawartość zmodyfikowanych plików z kopii zapasowej. Takie podejście pozwala na ciągłą pracę, nawet w systemie, do którego intruz uzyskał pełny dostęp.

Pomimo licznych zalet rozwiązanie to posiada szereg wad. System *ICAR* w celu zabezpieczenia kluczowych dla swojego działania danych – jądra systemu operacyjnego, bazy danych wzorców oraz kopii chronionych plików, wykorzystuje nośniki zabezpieczone przed zapisem na poziomie sprzętowym. Takie podejście powoduje, że w przypadku konieczności aktualizacji chronionych plików niezbędne jest przeprowadzenie czasochłonnej operacji generowania nowego, niemodyfikowalnego nośnika. Drugą wadą, którą obciążona jest większość systemów zabezpieczeń, jest fakt, że system ochrony jest zainstalowany w tym samym systemie operacyjnym, który ma chronić. Poprzez zastosowanie niemodyfikowalnych nośników danych system *ICAR* został zabezpieczony przed wyłączeniem jego działania nawet w przypadku, gdy intruz przełamie wszystkie zabezpieczenia. Jednak nie można wykluczyć, że zostaną wykryte nieznane obecnie błędy, które pozwolą na wyłączenie systemu ochronnego. Rozwiązaniem przedstawionych problemów jest przeniesienie systemu ochrony na poziom monitora maszyny wirtualnej. W tym celu zapoczątkowano projekt *VmICAR* (ang. *Virtual-machine Integrity Checking And Restoring*).

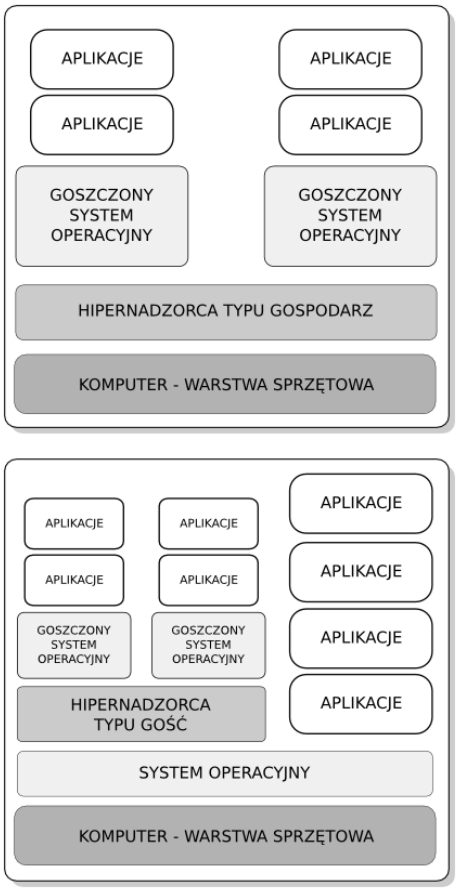
2. ZASTOSOWANIE WIRTUALIZACJI W BEZPIECZEŃSTWIE

Wirtualizacja pozwala na jednoczesne uruchamianie kilku systemów operacyjnych zainstalowanych w tzw. maszynach wirtualnych, na jednym fizycznym komputerze. Maszyny wirtualne są uruchamiane i zarządzane przez program monitora maszyny wirtualnej (ang. *Virtual Machine Monitor*, *VMM*), inaczej zwanego również hipernadzorcą (ang. *hypervisor*). Żądania dostępu do zasobów sprzętowych przez system operacyjnych gościa (ang. *guest operating system*) jest przechwytywane przez hipernadzorcę, który w zależności od typu operacji emuluje środowisko lub przekazuje operację bezpośrednio do sprzętu. Dzięki temu monitor maszyny wirtualnej umożliwia dostęp do ograniczonych zasobów sprzętowych przez wiele działających równocześnie systemów operacyjnych.

Recenzent: Prof. dr hab. inż. Kazimierz Goczyła – Wydział Elektroniki, Telekomunikacji i Informatyki Politechnika Gdańska

W latach sześćdziesiątych ubiegłego wieku IBM rozpoczął prace nad jednoczesnych uruchamianiem wielu złożonych zadań na komputerach typu mainframe. W 1972 roku został udostępniony pierwszy system operacyjny z możliwością wirtualizacji o nazwie VM/370 [1]. Z uwagi na duże wymagania sprzętowe wirtualizacja upowszechniła się jednak dopiero na przełomie XX i XXI wieku. Powszechnie dostępne obecnie procesory wspierają sprzętową wirtualizację, która jest znacznie wydajniejsza w porównaniu do wirtualizacji czysto programowej.

Wyróżniane są dwa typy hipernadzorców: typu 1, zwany gospodarzem (ang. *native virtual machine monitor*) oraz typu 2, zwany gościem (ang. *hosted virtual machine monitor*). Hipernadzorca typu 1 jest minimalnym systemem operacyjnym instalowanym bezpośrednio na komputerze. Hipernadzorca typu 2 jest natomiast zwyczajnym programem komputerowym, który jest uruchamiany wewnątrz istniejącego systemu operacyjnego. Różnica między typami hipernadzorców została pokazana na rysunku 1.



Rys. 1. Architektura hipernadzorcy typu 1 i typu 2.

Wirtualizacja znajduje szerokie zastosowanie w wielu dziedzinach informatyki, w tym w podnoszeniu bezpieczeństwa systemów informatycznych. Jedną z zalet umieszczenia systemu ochrony na poziomie monitora maszyny wirtualnej jest izolacja. System operacyjny traktuje warstwę hipernadzorcy wraz z działającymi tam procesami jako sprzęt komputerowy. W związku z tym, w przypadku, gdy intruz uzyska dostęp do systemu operacyjnego, nawet z największymi przywilejami nie będzie w stanie wyłączyć czy zmodyfikować systemu ochrony działającego na poziomie monitora maszyny wirtualnej.

2.1. Wirtualizacja w systemach bezpieczeństwa

Prace nad wykorzystaniem wirtualizacji do poprawy bezpieczeństwa prowadzone są przez liczne ośrodki badawcze i naukowe. Można wymienić szereg kierunków rozwojów tych badań, z których najważniejsze to:

- separowanie usług systemowych (Qubes [2]),
- przywracanie systemu operacyjnego po jego awarii (ang. disaster recovery),
- kopie bezpieczeństwa całego środowiska, tzw. migawki,
- zbieranie danych o aktywności systemu (ReVirt [3], ExecRecorder [4]),
- wykrywanie włamań (HyperSpector [5], VMwatcher [6]),
- bezpieczne systemy plików (SVFS [7], VDisk [8]).

Celem autorów artykułu jest opracowanie systemu, który łączy wykrywanie włamań z zabezpieczaniem kluczowych do działania systemu operacyjnego plików. Dotychczas tego typu systemy były tworzone jedynie z wykorzystaniem parawirtualizacji i działały głównie na monitorze maszyny wirtualnej Xen. W związku z tym, za ich pomocą można chronić tylko specjalnie zmodyfikowane systemy operacyjne. W praktyce oznacza to, że systemem gościa mogą być tylko otwarte systemy, takie jak Linux czy BSD.

Opracowywany przez autorów system ochrony działać ma na monitorze maszyny wirtualnej typu 2 (goszczony hipernadzorca) i w związku z tym będzie mógł chronić integralność plików dowolnego systemu operacyjnego, w tym systemu Windows.

3. OCHRONA NA POZIOMIE HIPERNADZORCY

Z punktu widzenia projektowanego systemu ochrony integralności systemu plików najważniejsze jest uzyskanie informacji o plikach, które przetwarza system operacyjny gościa. W systemie ICAR, który działa na poziomie jądra systemu operacyjnego Linux, każda operacja odczytu oraz modyfikacji plików jest przechwytywana za pomocą mechanizmu *LSM* (ang. *Linux Security Modules*), a następnie uruchamiany jest moduł ochrony.

W przypadku przeniesienia mechanizmu ochrony na poziom monitora maszyny wirtualnej proces ochrony bardziej skomplikowany. Częściowym rozwiązaniem problemu jest wykorzystanie parawirtualiazacji, jak ma to miejsce w przypadku wymienionych wcześniej systemów ochrony. W tym przypadku jądra chronionego systemu operacyjnego komunikuje się z warstwą hipernadzorcy i może mu przekazywać informacje np. o nazwa otwieranych plikach.

Jednak w przypadku wykorzystania pełnej wirtualizacji, a tylko takie podejście pozwoli na ochronę plików dowolnych systemów operacyjnych, sytuacja jest o wiele bardziej skomplikowana. System operacyjny traktuje monitor maszyny wirtualnej jako warstwę sprzętową. W przypadku konieczności otworzenia lub zapisu plików hipernadzorca otrzymuje tylko informację o blokach dyskowych, które mają zostać zmodyfikowane. Zatem w celu identyfikacji, czy żądana operacja dotyczy chronionego pliku, konieczne jest przeprowadzanie w locie operacji konwersji odwołań do warstwy fizycznej dysku twardego na warstwę logiczną systemu plików.

W związku z tym, że badany problem jest złożony, projekt mechanizmu ochrony kluczowych plików systemu operacyjnego działającego w maszynie wirtualnej został podzielony na trzy etapy:

VmICAR-1 – cykliczne wykrywanie zmian w chronionych plikach.

VmICAR-2 – ciągłe monitorowanie zmian w chronionych plikach.

VmICAR-3 – ochrona przed modyfikacją wybranych plików.

3.1. Cykliczne wykrywanie zmian w chronionych plikach

Pierwszym etapem projektu było opracowanie systemu ochrony integralności plików działającego w przestrzeni użytkownika systemu gospodarza (*VmICAR-1*). Jego zasada działania jest oparta na pierwszym upowszechnionym programie ochrony integralności plików o nazwie *Tripwire*, który powstał na Uniwersytecie Purdue w 1992 roku. Różnica polega na tym, że w odróżnieniu od pierwowzoru system *VmICAR-1* sprawdza integralność systemu plików zapisanego w wirtualnym systemie plików.

Dane maszyny wirtualnej są przechowywane na wirtualnych dyskach. Dyski takie mają postać zwykłego pliku zapisanego w systemie gospodarza. Z punktu widzenia systemu operacyjnego gościa dysk taki nie różni się od dysków fizycznych, posiada m.in. cylindry, głowice czy sektory. Operacja odczytu lub zapisu jest przez hipernadzorcę wykonywana na pliku z obrazem dysku.

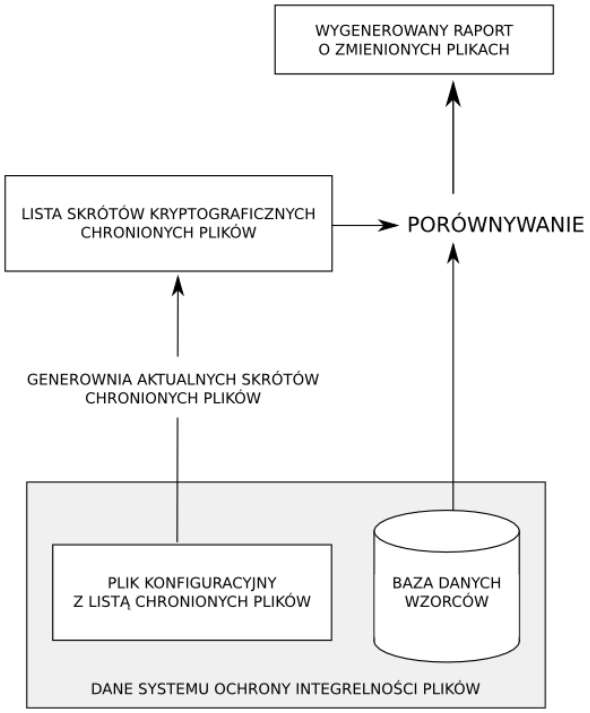
Wiodący producenci hipernadzorców, tacy jak *Vmware*, *Oracle* oraz *Microsoft*, zaproponowali własne specyfikacje wirtualnych dysków, które różnią się wewnętrzną strukturą oraz funkcjonalnością. Do najczęściej wykorzystywanych dysków należą:

- *VHD* (*Virtual Hard Disk*) – Microsoft: Virtual PC,
- *VMDK* (*Virtual Machine Disk*) – VMware: Workstation, Player, Server, Fusion, ESX,
- *VDI* (*Virtual Disk Image*) – Oracle: VirtualBox.

W 2008 roku powstała otwarta specyfikacja wirtualnego dysku twardego *OVF* (ang. *Open Virtualization Format*), która w 2010 roku została ogłoszona jako standard ANSI [9]. Większość monitorów maszyn wirtualnych obsługuje wszystkie z przedstawionych powyżej formatów.

Schemat działania algorytmu sprawdzania integralności plików w maszynie wirtualnej jest taki sam jak dla systemu działającego w przestrzeni użytkownika. Do poprawnego działania systemu ochrony integralności plików koniecznie jest wygenerowanie bazy danych, która zawiera m.in. wzorcowe skróty kryptograficzne chronionych plików. Po dokonaniu wstępnej konfiguracji programu ochrony dalsze jego działanie polega na okresowym sprawdzaniu integralności poprzez każdorazowe obliczenie skrótów kryptograficznych na podstawie aktualnej zawartości chronionych plików i porównaniu ich ze wzorcami zapisanymi w bazie danych. Jeżeli uzyskany skrót pliku jest różny od wzorca, wszczynana jest procedura alarmowa. Na rysunku 2 został przedstawiony schemat działania programów ochrony integralności systemu plików działających w przestrzeni użytkownika [10].

Różnica pomiędzy sprawdzaniem integralności plików w obrazie maszyny wirtualnej a w fizycznym systemie plików polega na sposobie odczytu chronionych plików. W przypadku ochrony plików maszyny wirtualnej niemożliwy jest bezpośredni dostęp do plików. Dostęp taki można uzyskać na dwa sposoby. Pierwszy polega na zamontowaniu wirtualnego systemu plików w drzewie katalogów. Następnie można odwoływać się do zasobów wirtualnych tak jak do zwykłych plików zapisanych na tradycyjnych nośnikach. Taką operację można przeprowadzić zarówno w systemie Windows (od wersji Windows 7 domyślnie, poprzednie wersje wymagają zainstalowania dodatkowych programów), jak i Linux (za pomocą narzędzi z pakietu Qemu lub vdfuse). Takie rozwiązanie jest często wykorzystywane do tworzenia kopii zapasowych danych maszyn wirtualnych.



Rys. 2. Działanie systemów ochrony integralności plików

Druga metodą polega na odczytywaniu zawartości partycji wirtualnej bezpośrednio przez program ochrony. Jest to podejście bardziej skomplikowane, gdyż konieczne jest przeprowadzenie analizy wirtualnego dysku oraz odczyt plików bezpośrednio z partycji. Jednak z punktu widzenia całości projektu, opracowany mechanizm będzie można wykorzystać w kolejnych etapach projektu *VmICAR*.

Zostały przeprowadzone badania polegające na analizie kodów źródłowych narzędzi z pakietu *Qemu*, które umożliwiają manipulowanie wirtualnymi dyskami. Na podstawie zebranej wiedzy został zaimplementowany moduł umożliwiający odczytywanie dowolnego pliku z obrazu wirtualnego dysku.

Produktem wynikowym jest prototyp mechanizmu cyklicznego wykrywania zmian w chronionych plikach *VmICAR-1*. Powstał on na bazie narzędzi wytworzonych w ramach projektu *ICAR* rozszerzonych o moduł odczytu plików z wirtualnych dysków. Prototypowa implementacja została wykonana dla systemu operacyjnego Linux. Jednak, zgodnie z założeniem, kontrola integralności chronionych plików może zostać przeprowadzona dla systemów plików NTFS, FAT oraz EXT. W związku z tym może być chroniony zarówno system operacyjny Windows, jak i Linux. Jedynym warunkiem jest, aby system gospodarza działał pod kontrolą systemu Linux. W chwili obecnej nie jest istotne, jaki program pełni rolę monitora maszyny wirtualnej, gdyż *VmICAR-1* nie komunikuje się z hipernadzorcą, lecz czyta bezpośrednio plik obrazu systemu plików.

Obecnie trwają prace nad kolejnym etapem projektu, w którym opracowany mechanizm jest integrowany z

monitorem maszyny wirtualnej. Oczekiwanym produktem wynikowym będzie zmodyfikowany hipernadzorca umożliwiający ciągłą kontrolę integralności chronionych plików. Prace są prowadzone na bazie programu VirtualBox firmy Oracle, z uwagi na dostęp do kodów źródłowych upublicznionych na licencji Open Source.

4. PODSUMOWANIE

Wykorzystywanie wirtualizacji do ochrony systemów komputerowych jest uważane za jeden z najbardziej perspektywicznych kierunków rozwoju bezpieczeństwa. Zaproponowany w artykule system ochrony, działając na poziomie monitora maszyny wirtualnej, umożliwi wykrywanie i przeciwdziałanie atakom na systemy komputerowe. Izolacja maszyny wirtualnej od hipernadzorcy gwarantuje, że intruz nawet w przypadku uzyskania pełnego dostępu do atakowanego systemu operacyjnego nie będzie mógł wyłączyć systemu ochrony. W pierwszym etapie projektu został opracowany mechanizm sprawdzania integralności plików w obrazie dysku maszyny wirtualnej. W dalszej kolejności mechanizm ten zostanie włączony do monitora maszyny wirtualnej, aby zapewnić ciągłą ochronę systemu operacyjnego i danych w nim zapisanych

5. BIBLIOGRAFIA

1. Arce I.: Ghost in the virtual machine, IEEE Security & Privacy, vol. 5, no. 4, pp. 68—71, 2007
2. Rutkowska J., Wojtczuk R.: Qubes OS Architecture, Invisible Things Lab, Tech. Rep, 2010
3. Dunlap G. W., King S.T., Cinar S., Basrai M.A., Chen P.M.: ReVirt: enabling intrusion analysis through virtual-machine logging and replay, SIGOPS Oper. Syst. Rev.,vol. 36, 2002, ACM
4. de Oliveira D.A.S., Crandall J.R., Wassermann G., Wu S.F., Su Z., Chong F.T.: ExecRecorder: VM-based full-system replay for attack analysis and system recovery, Architectural Support for Programming Languages and Operating Systems, vol. 21, no 21, pp 66—71, 2006
5. Kourai K., Chiba S., HyperSpector: virtual distributed monitoring environments for secure intrusion detection, Proceedings of the 1st ACM/USENIX international conference on Virtual execution environments, 2005, ACM
6. Jiang X., Wang X., Xu D.: Stealthy malware detection and monitoring through VMM-based "out-of-the-box" semantic view reconstruction, ACM Transactions on Information and System Security (TISSEC), vol. 13, no. 2, 2010, ACM
7. Zhao X.. Borders K., Prakash A.: Towards protecting sensitive files in a compromised system, Third IEEE International Security in Storage Workshop, 2005, IEEE
8. Wires J., Feeley M. J.: Secure file system versioning at the block level, SIGOPS Oper. Syst. Rev.,vol. 41, no. 3, 2007, ACM
9. INCITS 469-2010 Information Technology – Open Virtualization Format (OVF) Specification
10. Debar H., Dacier M., Wespi A.: Towards a taxonomy of intrusion detection systems, Computer Networks, vol. 31, no. 8, pp. 805—822, 1999

FILE INTEGRITY PROTECTION ON THE HYPERVISOR LEVEL

Key-words: security, virtualization

Files integrity protection mechanisms allow detection of unauthorized modifications to the critical files of the operating system. So far, these types of systems acted as system utilities, or have been integrated with the operating system kernel. Dissemination of virtualization technology allowed security system integration on the virtual machine monitor level, which provides isolation between protection mechanism and protected operating system. This paper describes the design of a file integrity protection system integrated with the virtual machine monitor. It presents the pros and cons of such a solution. It also discusses the problems that need to be resolved before implementation of a protection mechanism on the hypervisor level.