XXI Seminarium

ZASTOSOWANIE KOMPUTERÓW W NAUCE I TECHNICE' 2011
Oddział Gdański PTETiS
Referat nr 14

MOŻLIWOŚCI STOSOWANIA WIRTUALIZACJI W SYSTEMACH KOMPUTEROWYCH

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: Wykorzystywana dotychczas głównie w zastosowaniach wojskowych i przemysłowych, na komputerach typu mainframe, wirtualizacja wchodzi obecnie do powszechnego użytku. Wzrost mocy obliczeniowej komputerów osobistych pozwala na wydajne wirtualizowanie nawet kilku systemów operacyjnych na raz. W artykule została przedstawiona zasada działania wirtualizacji oraz nadzorcy i maszyny wirtualnej. Opisano trzy obszary zastosowań wirtualizacji: edukacja informatyczna, systemy mobilne oraz bezpieczeństwo systemów komputerowych.

Słowa kluczowe: wirtualizacja, bezpieczeństwo.

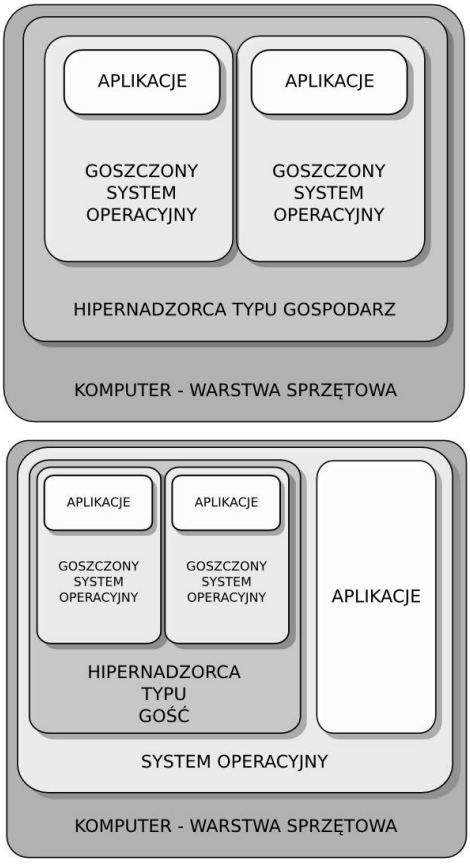
1. WSTĘP

Wirtualizacja jest obecnie uważana za jeden z najważniejszych kierunków rozwoju informatyki. Umożliwia jednoczesne uruchomienie wielu systemów operacyjnych na jednym komputerze. Monitor maszyny wirtualnej (ang. Virtual Machine Monitor, VMM), inaczej zwany również hipernadzorcą (ang. hypervisor), jest programem komputerowym pozwalającym na uruchamianie jednocześnie wielu systemów operacyjnych na jednym komputerze. Kiedy zainstalowany w maszynie wirtualnej system operacyjny (ang. guest operating system) odwołuje się do sprzętu komputerowego, żądanie takie jest przechwytywane, a następnie obsługiwane przez hipernadzorcę. Monitor maszyny wirtualnej umożliwia równoległy dostęp do sprzętu komputerowego przez wiele działających równocześnie systemów operacyjnych.

Pomimo tego, że technika wirtualizacji zaczęła być powszechnie wykorzystywana dopiero na początku XXI wieku, sama koncepcja stworzenia maszyny wirtualnej nie jest nowa. Pierwsze badania były prowadzone przez firmę IBM w latach sześćdziesiątych XX wieku. Ich celem było umożliwienie wykorzystywania komputerów typu mainframe do wykonywania wielu zadań jednocześnie. Stworzony w 1972 roku system operacyjny VM/370 firmy IBM oferował praktycznie wszystkie funkcje dostępne we współczesnych programach maszyn wirtualnych [1].

Wyróżniane są dwa typy hipernadzorców: gospodarz (ang. native virtual machine monitor) i gość (ang. hosted virtual machine monitor), których architektura została przedstawiona na rysunku 1.

Hipernadzorca typu gospodarz jest prostym systemem operacyjnym uruchamianym bezpośrednio na komputerze. Hipernadzorca typu gość jest natomiast programem komputerowym uruchamianym wewnątrz zainstalowanego już systemu operacyjnego.



Rys. 1. Modele działania maszyny wirtualnej

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

Z uwagi na wysokie koszty sprzętu komputerowego o wydajności pozwalającej na efektywne obsługiwanie wirtualizacji, do końca XX wieku była ona praktycznie używana tylko w specjalistycznych zastosowaniach. Obecnie istnieją możliwości wykorzystywania maszyn wirtualnych, w związku ze znacznym zwiększeniem mocy obliczeniowej komputerów. Powszechnie są dostępne specjalne procesory, które umożliwiają dokonywanie prawdziwej, sprzętowej wirtualizacji, co znacznie przyspiesza działania wirtualizowanych systemów.

2. WIRTUALIZACJA W EDUKACJI

Szeroko pojęta edukacja informatyczna jest jedną z tych dziedzin, które najszybciej rozpoczęły wykorzystywanie wirtualizacji w procesie kształcenia. Najbardziej oczywistym jest wykorzystanie technik wirtualizacji do nauki budowy systemów operacyjnych, a także zarządzania i administrowania nimi. Przygotowanie odpowiedniego środowiska do nauki polega na instalacji systemu operacyjnego wewnątrz maszyny wirtualnej. W takim środowisku student może pracować z najwyższymi przywilejami, dzięki czemu może przeprowadzać najbardziej zaawansowane operacje. Może nie tylko uruchamiać nowe serwisy, instalować i konfigurować oprogramowanie systemowe, ale również instalować sterowniki urządzeń, także własne, a nawet modyfikować jądro systemu operacyjnego. Wszystkie te kroki mogą być wykonywane bez obawy, że środowisko pracy zostanie zniszczone i nie będzie nadawało się do ponownego wykorzystania. Zainstalowany w maszynie wirtualnej system operacyjny jest przechowywany w postaci pliku binarnego, który może zostać skopiowany do kopii zapasowej, a następnie w prosty sposób odtworzony.

Możliwe jest nawet wykonanie tzw. migawek (ang. snapshot) systemu operacyjnego, który polega na zapamiętaniu nie tylko aktualnej zawartości dysku twardego wirtualnego komputera, ale również stanu uruchomionych procesów. Dzięki temu przed wykonaniem krytycznej operacji, na przykład instalacji nowego modułu jądra systemu operacyjnego, można wykonać migawkę maszyny wirtualnej i w razie problemu przywrócić ją do działającego stanu.

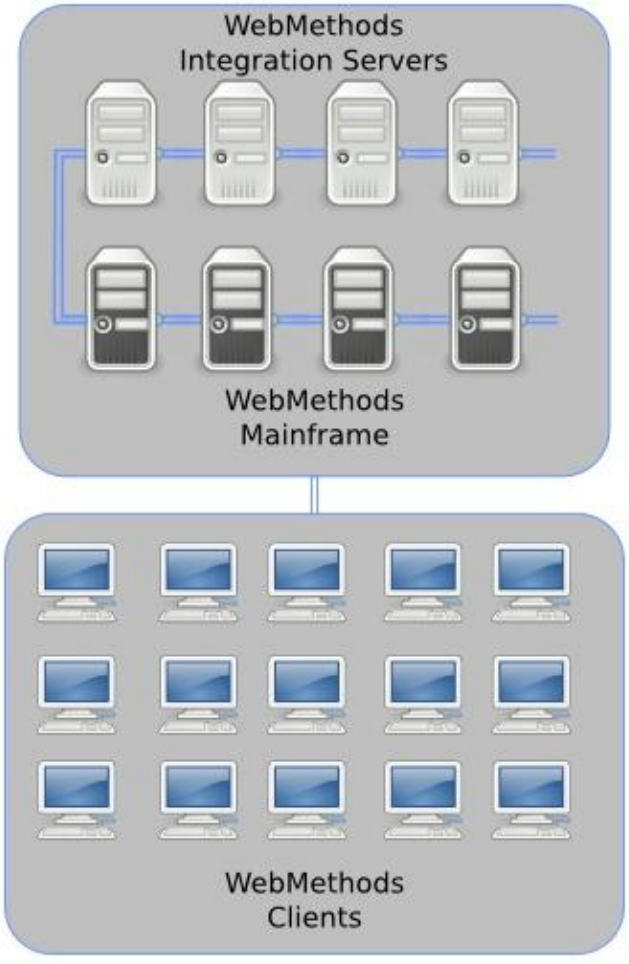
Również zarządzanie komputerami znajdującymi się w sali laboratoryjnej jest prostsze niż to ma miejsce w przypadku systemów operacyjnych instalowanych bezpośrednio na komputerach. Instalację systemu operacyjnego wystarczy przeprowadzić na jednej maszynie wirtualnej, a następnie przekopiować plik reprezentujący wirtualny dysk na dowolną liczbę maszyn gospodarzy.

Kolejną zaletą zastosowania wirtualizacji jest możliwość nauki dowolnych systemów operacyjnych. Można utworzyć kilka oddzielnych maszyn wirtualnych z zainstalowanymi różnymi systemami operacyjnymi, zarówno dojrzałymi, jak i znajdującymi się we wstępnej fazie rozwoju. Takie maszyny mogą być nawet uruchomione jednocześnie.

Programy uruchomione w maszynie wirtualnej są całkowicie odizolowane od komputera gospodarza, a także innych maszyn wirtualnych. Dlatego zarówno wersje rozwojowe oprogramowania, jak i aplikacji nieznanego pochodzenia mogą być uruchamiane bez obawy o uszkodzenie systemu operacyjnego gospodarza [2].

Niewątpliwym kosztem zastosowania wirtualizacji w przypadku edukacji, podobnie jak w innych zastosowaniach, są większe wymagania sprzętowe. Pomimo nowoczesnych rozwiązań sprzętowych, dzięki którym wirtualizowane systemy działają wydajniej istnieje pewien narzut konieczny do emulowania, choćby częściowego, systemu operacyjnego. W zależności od wybranego rodzaju wirtualizacji oraz monitora maszyny wirtualnej narzut ten może sięgać od kilku do kilkunastu procent. W zastosowaniach edukacyjnych nakład sprzętowy nie jest wykorzystywany, w odróżnieniu od np. centrów obliczeniowych czy hostingowych, gdzie jest on kompensowany pełniejszym zużyciem zasobów komputerowych [3].

Nauka systemów operacyjnych nie jest jedyną możliwością wykorzystania wirtualizacji w edukacji. Na potrzeby laboratorium z przedmiotu *Integracja Systemów* prowadzonym na Wydziale ETI, PG przygotowano we współpracy z firmą SoftwareAG środowisko emulujące centrum komputerowe. Wirtualne środowisko składa się z czterech serwerów integracyjnych, czterech systemów typu mainframe oraz kilkunastu maszyn klienckich. Schemat utworzonej wirtualnej sieci przedstawiono na rysunku 2.



Rys. 2. Schemat sieci w sali laboratoryjnej

Całość została zainstalowana na maszynach wirtualnych, w oparciu o technologię firmy Vmware. Dzięki wykorzystaniu wirtualizacji, nie została zmieniona ani konfiguracja, ani zawartość systemów operacyjnych na komputerach w sali laboratoryjnej, która może być wykorzystywana na dowolnych innych zajęciach.

3. SYSTEMY MOBILNE

Telefony komórkowe nowej generacji coraz bardziej upodobniają się do komputerów. Najnowsze urządzenia są wyposażane w dwurdzeniowe procesory o częstotliwości przekraczającej 1 GHz i dorównują parametrami komputerom osobistym sprzed kilku lat [4].

Wraz ze wzrostem mocy obliczeniowej wzrasta możliwość dostosowywania oprogramowania telefonu do potrzeb użytkowników. Wszystkie wiodące platformy, takie jak Apple iOS, Google Android, czy Symbian firmy Nokia umożliwiają instalacje zewnętrznego oprogramowania. Jednak coraz częściej zdarza się, że takie aplikacje zawierają błędy, a nawet zainstalowane niebezpieczne mechanizmy, takie jak tylne drzwi (ang. backdoor). W odróżnieniu od komputerów osobistych świadomość zagrożenia i potencjalnych strat wynikających z włamania jest niska, zarówno po stronie użytkownika, jak i po stronie producentów. Jest to związane z krótkimi cyklami wytwarzania oprogramowania, wprowadzaniem nowych, niesprawdzonych rozwiązań, co jest wymuszane przez liczną i dynamicznie rozwijającą się konkurencję [5].

Telefony komórkowe są często wykorzystywane do przechowywania poufnej korespondencji, dostępu do sieci korporacyjnych, a także do przeprowadzania operacji finansowych. W związku z tym pojawia się konieczność zachowania poufności na urządzeniach mobilnych. Jednym z kierunków rozwoju systemów zabezpieczeń jest wykorzystanie wirtualizacji. Wraz ze wzrostem mocy obliczeniowej urządzeń możliwe jest wykorzystanie tej technologii bez zbytniego spadku wydajności działania systemu operacyjnego.

Jednym ze sposobów wykorzystania wirtualizacji do zapewniania poufności danych, jest separacja wrażliwych aplikacji, np. bankowych, od pozostałych procesów. Firma LG wraz z dostawcą technologii wirtualizacji firmą VMware wyprodukowała telefon komórkowy działający pod kontrolą systemu operacyjnego Android, który wyposażony jest w dwie maszyny wirtualne, jedną przeznaczoną do zastosowań służbowych, druga do zastosowań prywatnych. Dzięki takiemu podziałowi, przy zachowaniu ostrożności użytkownika, krytyczne operacje wykonywane z profilu służbowego będą bezpieczne.

Inną metodą podnoszącą bezpieczeństwo jest wykorzystanie możliwości wykonywania migawek systemu operacyjnego. Takie okresowo wykonywane zrzuty są wykorzystywane do przywracania bezpiecznej wersji systemu w przypadku wykrycia niepożądanego oprogramowania.

Pomimo niewątpliwych zalet, wykorzystanie wirtualizacji w telefonach komórkowych posiada szereg ograniczeń. Urządzenia telefoniczne są specyficzną podgrupą urządzeń wbudowanych (ang. embedded), których jednym z podstawowych wymagań są małe opóźnieniami wykonywanych operacji. W praktyce jest to realizowane poprzez ścisłą integrację oprogramowania ze sprzętem. Jednak w przypadku zastosowania wirtualizacji, która z definicji zapewnia izolację systemu operacyjnego od warstwy sprzętowej, nie jest to możliwe. Najbardziej jaskrawym przykładem jest rozmowa telefoniczna, która jest operacją czasu rzeczywistego i powinna zostać obsłużona bez zbędnych opóźnień. W nowoczesnych, wieloprocesowych urządzeniach w momencie nawiązania rozmowy mogą być uruchomione inne aplikacje, np. odtwarzacz muzyki, którego działanie przed odebraniem połączenia musi zostać wstrzymane. W przypadku, gdy część systemu działa w maszynie wirtualnej sprawa się komplikuje. W praktyce jest to rozwiązywane poprzez wykorzystanie dzielonych buforów, co jednak nie jest do końca zgodne z postulatem izolacji. Problemy pojawiają się również w przypadku szeregowania procesów, działających jednocześnie w kilku maszynach wirtualnych [6].

4. BEZPIECZEŃSTWO

Wirtualizacja jest obecnie powszechnie wykorzystywana do zwiększania bezpieczeństwa systemów operacyjnych w komputerach osobistych.

Zastosowanie wirtualizacji pozwala na odseparowanie środowisk roboczych. Oznacza to, że atak, włamanie czy zainfekowanie wirusem systemu gościa nie jest groźne dla systemu gospodarza. Również inne wirtualne systemy pozostają bezpieczne z uwagi na ich odseparowanie.

Jednym ze sposobów wykorzystania wirtualizacji do podnoszenia bezpieczeństwa usług sieciowych jest odseparowanie poszczególnych serwerów. Można na przykład uruchomić na osobnym serwerze wirtualnym usługę WWW, a na innym serwerze wirtualnym usługę ftp, a jeszcze na innym pocztę elektroniczną. Istnieje też możliwość utworzenia osobnych, dedykowanych systemów wirtualnych do obsługi różnych domen, usług czy klientów. W takim przypadku udane włamanie na serwer konkretnej domeny nie pociągnie za sobą zagrożenia dla bezpieczeństwa innych domen.

Wirtualizacja jest również coraz częściej wykorzystywana w procedurach pozwalających na przywracanie systemu operacyjnego po jego awarii (ang. disaster recovery). Zwykle w przypadku sprzętowej awarii, przeniesienie zainstalowanego na dysku twardym systemu operacyjnego na komputer o innej konfiguracji sprzętowej jest zadaniem skomplikowanym, a często wręcz niemożliwym. W związku z tym, że wirtualne systemy nie są związane z konfiguracją sprzętową, istnieje możliwość łatwego przenoszenia obrazu wirtualnego systemu na inny komputer z całkowicie różną konfiguracją sprzętową.

Wirtualizacja jest obecnie również wykorzystywana do automatycznego tworzenia migawek, które są rodzajem kopii zapasowej systemu gościa na stacjach roboczych. W takiej postaci można zapisać nie tylko stan systemów plików, ale również stan procesów. Po wykryciu włamania lub infekcji wirusem plików systemowych migawka może stać się alternatywą działającego już systemu i pozwolić na przywrócenie bezpiecznej konfiguracji tego systemu.

Wirtualizacja jest stosunkowo nową, ale bardzo skuteczną metodą zapewniania bezpieczeństwa systemów operacyjnych, o dużym potencjale i możliwościach rozwoju. Pozwala przede wszystkim na zarządzanie bezpieczeństwem systemów operacyjnych w sposób kompleksowy. Rola komputera, na którym zainstalowano wiele wirtualnych serwerów znacznie wzrasta, a jego sprzętowa awaria może pociągać za sobą bardzo poważne konsekwencje. Dlatego ze względów bezpieczeństwa stosuje się zrównoleglenie tego typu serwerów, co pozwala na uniknięcie zjawiska zwanego pojedynczym punktem awarii (ang. single point of failure).

Dotychczas zostało stworzonych również kilka skutecznych mechanizmów ochrony systemów operacyjnych działających na poziomie hipernadzorcy, z których warto wymienić systemy ReVirt, CoVirt, HyperSpector, Livewire, czy system plików SVFS [7].

Ciekawe podejście zastosowali autorzy systemu Qubes, którzy utworzyli nowy system operacyjny, mający na celu zachowania poufności przeprowadzanych operacji. Zamiast projektować mechanizmy zabezpieczania systemów operacyjnych, połączyli monitor maszyny wirtualnej z jądrem systemu operacyjnego Linux. Każdy proces może być uruchomiony w jednej z niezależnych domen, uruchomionych w oddzielnych maszynach wirtualnych. Zaletą opracowanego rozwiązania jest całkowita izolacja domen. Uruchomienie złośliwego oprogramowania w jednej domenie nie będzie miało wpływu na system operacyjny ani na procesy działające w innych domenach [8].

Innym podejściem do zapewniania bezpieczeństwa systemów komputerowych charakteryzuje się mechanizm o nazwie ICAR (ang. Integration Checking And Restroring), rozwijany przez autorów niniejszego artykułu. Opracowany mechanizm wykrywa i przeciwdziała włamaniom do systemu operacyjnego, poprzez kontrolę zawartości kluczowych plików. Istnieje możliwość przeniesienia mechanizmu zapewniania bezpieczeństwa systemu plików z poziomu jądra systemu operacyjnego na poziom monitora maszyny wirtualnej. Takie rozwiązanie pozwala na całkowitą izolację mechanizmu ICAR od chronionego systemu, gdyż system operacyjny traktuje hipernadzorcę jako warstwę sprzętową, która jest niemodyfikowalna.

Obecna wersja mechanizmu ICAR jest przeznaczona do ochrony systemu Linux. Jednak zintegrowanie mechanizmu ochrony z monitorem maszyny wirtualnej, umożliwia zabezpieczanie plików w dowolnych systemach operacyjnych.

5. WNIOSKI KOŃCOWE

Od początku XXI wieku zwiększa się liczba obszarów zastosowań technik wirtualizacji. Już nie tylko systemy serwerowe, czy komputery osobiste wykorzystują jej możliwości, ale również systemy przenośne, takie jak telefony komórkowe. Wirtualizacja w sposób istotny zwiększa bezpieczeństwo zarówno systemów plików jak również samych systemów operacyjnych i uruchamianych w nich aplikacji. Jest to ważna cecha tej technologii w dobie nieustannego zagrożenia bezpieczeństwa systemów komputerowych.

Wirtualizacja umożliwia jednoczesne wykorzystywanie różnych systemów operacyjnych, integrację technologii i aplikacji, co jest ważne przy współczesnych rozwiązań przetwarzania rozproszonego np. typu *cloud computing*. W związku z ciągłym wzrostem wydajności systemów komputerowych można przewidywać, że wirtualizacja będzie powszechnie wykorzystywana już w niedalekiej przyszłości.

5. BIBLIOGRAFIA

1. Arce I.: Ghost in the virtual machine, IEEE Security & Privacy, vol. 5, no. 4, pp. 68—71, 2007.
2. Luce T.: Virtualization in the Classroom, Issues in Information Systems, vol. 8, no. 1, 2007
3. Gaspar A., Langevin S., Armitage W.: Virtualization technologies in the undergraduate it curriculum, IT Professional, vol. 9, no. 4, pp. 10—17, 2007.
4. Acharya A., Buford J., Krishnaswamy V.: Phone virtualization using a microkernel hypervisor, Internet Multimedia Services Architecture and Applications (IMSAA), 2009.
5. Selhorst M., Stuble C., Feldmann F., Gnaida U.: Towards a trusted mobile desktop, Trust and Trustworthy Computing, pp. 78—94, 2010, Springer.
6. Heiser G.: The role of virtualization in embedded systems, Proceedings of the 1st workshop on Isolation and integration in embedded systems, pp. 11—16, 2008, ACM.
7. Kaczmarek J. Wróbel M.: Nowoczesne mechanizmy ochrony integralności systemów plików, Zeszyty Naukowe Wydziału Elektrotechniki i Automatyki Politechniki Gdańskiej. 2009, ISSN 1425-5766.
8. Rutkowska J., Wojtczuk R.: Qubes OS Architecture, Invisible Things Lab, Tech. Rep, 2010.

VIRTUALIZATION OF COMPUTER SYSTEMS

Key-words: virtualization, security

Previously used mainly in military and industrial applications on the mainframe systems, virtualization comes into common use today. The increase in computing power of personal computers allows to virtualize even multiple operating systems at once. The article describes the principle of the virtualization, the hypervisor and virtual machine role. Three areas of virtualization were presented: IT education, mobile systems and security systems.