CARNet

HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

# Virtualizacija računala

## CCERT-PUBDOC-2009-12-285

Nacionalni CERT

u suradnji s

LSS

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem Nacionalni CERT kontinuirano radi.

Rezultat toga rada je i ovaj dokument, koji je nastao suradnjom Nacionalnog CERT–a i LS&S–a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

## **Nacionalni CERT**, www.cert.hr

Nacionalno središte za **sigurnost računalnih mreža** i sustava.

## **LS&S**, www.LSS.hr

Laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

# Sadržaj

# 1. Uvod

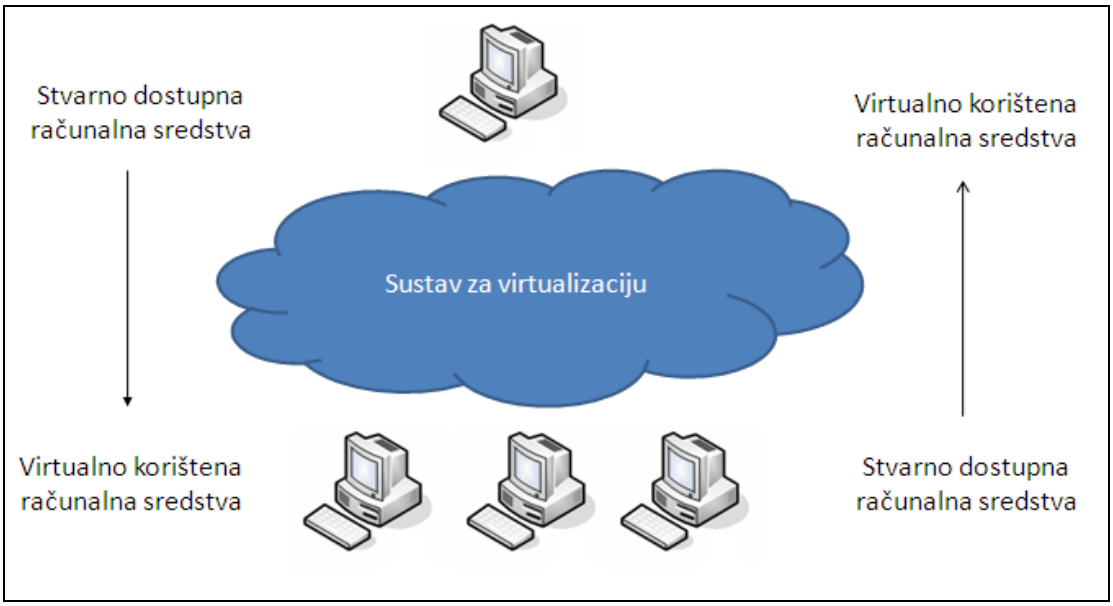
Virtualizacija računala koncept je koji se počeo razvijati još sredinom prošlog stoljeća. Podrazumijeva apstrakciju i enkapsulaciju računalnih sredstava tako da se oni mogu koristiti na način koji odgovara određenoj primjeni. Virtualiziraju se računalne mreže, programi i operacijski sustavi. Virtualizacijom se postiže bolja iskorištenost računalnih infrastruktura jer se omogućuje njihovo istovremeno korištenje u različitim sustavima. Moguće je postići i druge korisne učinke kao što je sigurnost ili pouzdanost. Primjerice, kod virtualizacije sustava cilj je postići izolirano izvođenje nekoliko različitih sustava na jednom fizičkom računalu. Izolacija i ograničenja na dostupnu memoriju, procesorsko vrijeme i slično automatski doprinose sigurnosti zato što izoliraju sustav od neovlaštenih korisnika, onemogućuju napade uskraćivanja usluge na cijelom sustavu, a kompromitiranost jednog virtualnog sustava neće utjecati na ostale.

Načini na koje se ostvaruje virtualizacija operacijskih sustava mogu uključivati emulaciju (oponašanje) cjelokupnog potrebnog sklopovlja, te nepotpune virtualizacije koje uključuju djelomičnu i paravirtualizaciju. Poboljšanje performansi takvog sustava može se postići i posebno oblikovanim sklopovljem koje potpomaže virtualizaciju. Zbog raširenosti x86 arhitektura, čiji su radni kapaciteti znatno veći od potreba jednog OS-a, virtualizacija u posljednje vrijeme postaje sve češće rješenje. Njome se poboljšava iskorištenost sustava i ostvaruju se uštede na skupom sklopovlju.

Programska i sklopovska podrška za virtualizaciju još uvijek nije dosegla razinu standarda pa je dostupno relativno mnogo različitih rješenja. Uz općeniti uvod u koncepte i problematiku virtualizacije te pitanja sigurnosti, dat će se pregled tri takva programska sustava: Xen, VirtualBox i VMware.

# 2. Virtualizacija

Pod pojmom „virtualizacija“ u računarstvu podrazumijeva se apstraktno predstavljanje pojedinih funkcionalnosti i resursa. Odnosno, izvana za korisnika (čovjek ili program) nema razlike između stvarnog i virtualnog ostvarenja funkcionalnost, ali stvarne vrijednosti i aktivnosti u virtualnoj izvedbi razlikuju se od onih prikazanih korisniku. Primjerice, stvarni operacijski sustav komunicira izravno sa sklopovljem računala, dok virtualni operacijski sustav ima za korisnika sva obilježja stvarnog sustava, ali se pokreće u drugom stvarnom sustavu. Dakle, komunikacija se ne obavlja sa sklopovljem već sa drugim sustavom. Pritom taj drugi sustav oponaša sklopovlje u komunikaciji s virtualnim sustavom. Rad sklopovlja se u ovom slučaju simulira programski pa je riječ o virtualnom sklopovlju. Virtualizacija može značiti da korisnik preko virtualnog sučelja skup računala koristi kao jedino računalo, a može i značiti da se na jednom računalu simulira rad nekoliko sustava.




***Slika 1. Grafička ilustracija virtualizacije računalnog sustava***

## *2.1. Povijest virtualizacije*

Razvoj virtualizacijskih tehnologija započinje 1960-tih godina u IBM-u. Riječ je bila o projektu M44/44X kojem je cilj bio logički podijeliti fizički sustav na različite virtualne strojeve kako bi se poboljšala iskorištenost sklopovlja. Takav središnji sustav podržavao je istovremeno izvođenje većeg broja procesa i programa. Zbog skupog sklopovlja i veće iskorištenosti računala to je značilo značajne financijske uštede. IBM je uz to dao najznačajnije doprinose na području razvoja virtualizacijskih tehnologija. Na IBM računalima razvijen je i prvi CTSS (eng. Compatible Time Sharing System) sustav na MIT-u. Riječ je o sustavu koji omogućuje dijeljenje sredstava računalnog sustava između različitih korisnika (ljudi ili programa). Na taj način omogućuje se naizgled istovremeno obavljanje više različitih zadataka.

IBM je u 60-tim i 70-tim godinama prošlog stoljeća također razvio čitav niz računala čije je sklopovlje podržavalo virtualne sustave i odgovarajućih virtualnih platformi: CP-40 sustav za IBM 360/40 računala, CP-67 sustav za IBM 360/67 računala, VM/370 sustav i druge. IBM-ovi virtualni strojevi simulirali su identično IBM-ovo sklopovlje na kakvom su se izdvojili, a VMM (eng. Virtual Machine Monitor) sučelje izvodilo se izravno na sklopovlju.

Daljnjim razvojem računala, uvođenjem 32-bitnih arhitektura te porastom složenosti i zahtjevnosti programa raste iskorištenost računala te virtualizacija gubi na popularnosti u 80-tim i 90-tim godinama. U to vrijeme razvija se model klijent/poslužitelj programa i distribuiranog programiranja na više umreženih računala.

Otkako posljednjih desetak godina x86 arhitekture postaju dominantne u poslovnim poslužiteljima, javlja se sličan problem neiskorištenosti poslužitelja kao i u 1960-tima. Tu se opet kao rješenje nameće virtualizacija. Javljaju se AMD-V i Intel VT tehnologije koje sklopovlje čine pogodnima za

virtualizaciju. One uvode mogućnost sklopovski potpomognute virtualizacije čija će svojstva detaljnije biti opisana u nastavku teksta. Javlja se i čitav niz platformi za virtualizaciju: VMware, Xen, VirtualBox, Hyper-V, KVM (eng. Kernel-based Virtual Machine) i drugi.

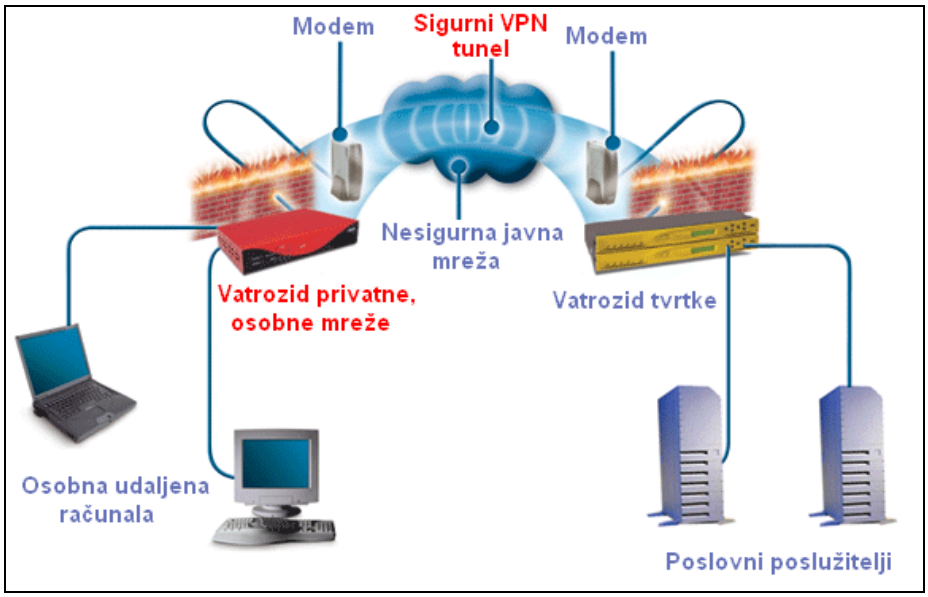
## 2.2. Različite primjene koncepta

Virtualizacija omogućuje učinkovitije korištenje računalnih, memorijskih i mrežnih resursa. Zbog svojstva apstrakcije omogućuje i zaštitu osjetljivih dijelova sustava tako što im ograničava pristup virtualnim sučeljem. U ovom dijelu poglavlja dan je pregled nekoliko različitih primjera primjene koncepta virtualizacije u računarstvu. Uključene su privatne virtualne mreže (VPN), virtualizacija memorije i virtualizacija programa.

### 2.2.1. VPN

Virtualna privatna mreža (eng. VPN – Virtual Private Network) je ponešto drugačija virtualizacijska tehnologija od virtualizacije operacijskih sustava. U ovom slučaju virtualizacija se obavlja u mrežnim uređajima, a virtualiziraju se svojstva mrežne komunikacije.

Naime, VPN omogućuje uspostavljanje zaštićene komunikacije između računala u nesigurnoj javnoj mreži. Na taj način između uključenih čvorova simulira se komunikacija sa svojstvima one koja bi se odvijala u lokalnoj mreži. Ostala računala iz javne mreže nemaju pristup podacima koji se šalju preko VPN veze.



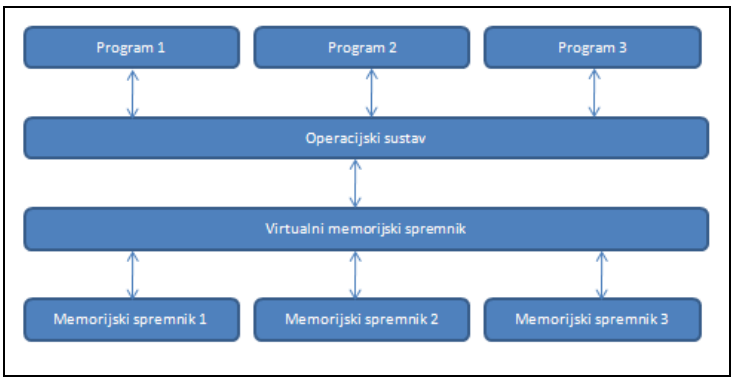

***Slika 2. VPN mreža***

***Izvor: Virtual Private Network Guide***

Ova metoda zasniva se na IP tuneliranju. Riječ je o postupku koji se koristi za ostvarivanje virtualno izravne poveznice između računala u javnoj mreži. IP paketi virtualne mreže enkapsuliraju se u IP pakete koji se zatim šalju između vanjskih ulaza u zaštićene podmreže ili računala. Sadržaj se pritom kriptira kako bi se očuvala tajnost.

### 2.2.2. Virtualizacija memorije

Virtualizacije memorije je postupak kojim se u grozdovima računala (eng. cluster) stvara jedinstveni *bazen* RAM (eng. Random Access Memory) memorije kojem mogu pristupati sva računala. Na taj način distribuirani i umreženi poslužitelji imaju dostupne veće RAM kapacitete što omogućuje povećanje učinkovitosti i lakše dijeljenje podataka. Ova vrsta virtualizacije ostvaruje se tako da se fizički adresni prostori preslikaju u virtualne adresne prostore preko kojih se pristupa stvarnim memorijskim adresama u različitim spremnicima. Osim već navedenih prednosti ove tehnologije, ona može negativno utjecati na brzinu izvođenja zbog korištenja udaljene memorije.

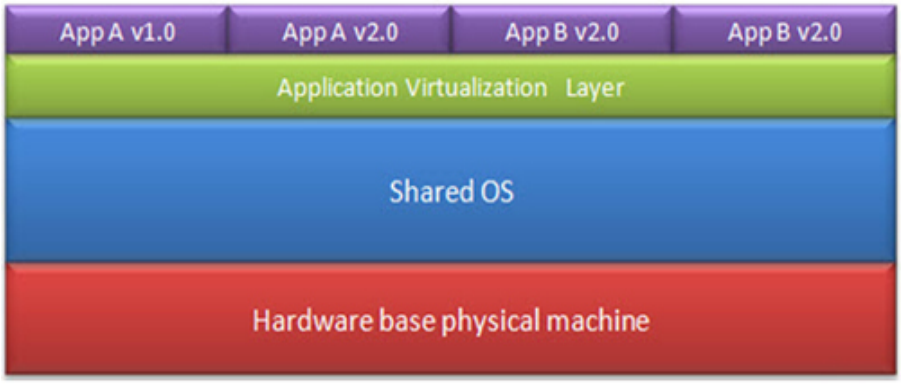



***Slika 3. Shema virtualizacije memorije***

Uz virtualizaciju memorije valja spomenuti i virtualizaciju memorijskih spremnika (eng. storage). Riječ je o procesu kojim se pomoću apstrakcije razdvajaju logički i fizički pristup memoriji. Metoda se zasniva na preslikavanju adresnih prostora i prevođenju zahtjeva za virtualnim logičkim adresama u odgovarajuće fizičke zahtjeve. Poslužitelj pritom koristi logički adresni prostor, a sve promjene u fizičkom adresnom prostoru maskiraju se mijenjanjem postavki prevoditelja zahtjeva ili tzv. „meta-data“ maskiranjem. To znači da će u slučaju premještanja podataka, zahtjev za stalnom logičkom lokacijom tih podataka u prevoditelju jednostavno preusmjeriti na novu fizičku lokaciju. Time se očito postiže jednostavnije upravljanje podacima i bolja iskorištenost memorije. Negativnosti mogu biti vezane uz sporije izvođenje zbog prividno bliskih logičkih adresa koje su u stvarnosti udaljene, složenosti izvedbe prevoditelja zahtjeva ili neusklađenosti različitih programskih izvedbi.

### 2.2.3. Virtualizacija programa

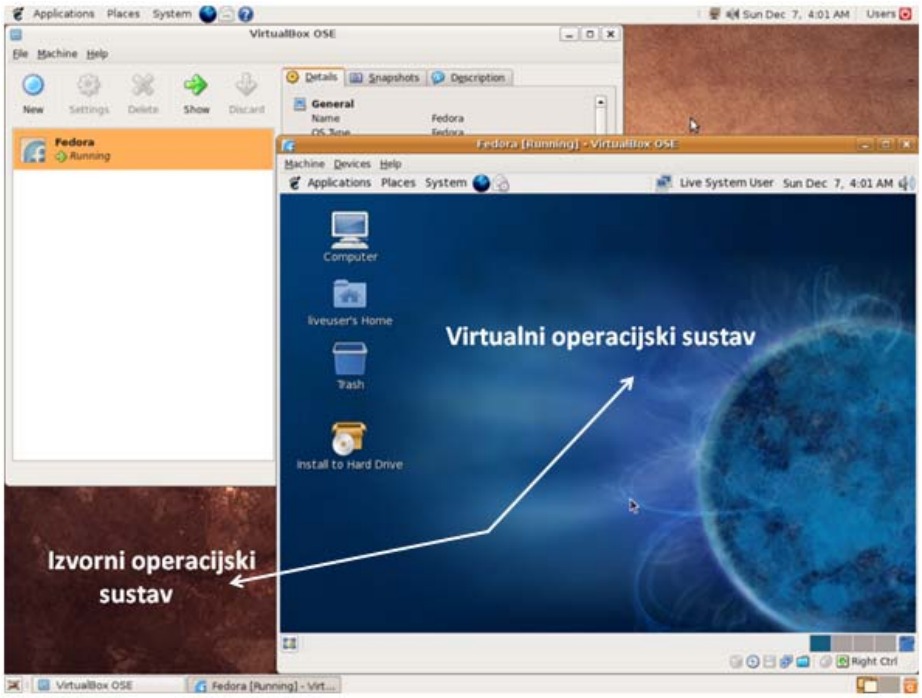
Programi se također mogu virtualno izvoditi na operacijskim sustavima. Pritom se pokreću na jednom sustavu, a koriste datoteke i sredstva udaljenog računala. Instalacija programa primjerice može uključivati instalaciju klijenta za neki mrežni protokol (npr. HTTP) pomoću kojeg se distribuirano pristupa dijelovima programa i usluga. Time se olakšava izvođenje programa na operacijskim sustavima za koje nisu izravno oblikovani, izbjegava se virtualizacija cijelog OS-a na klijentskom računalu, a štiti se i računalo od možda loše napisanog programskog koda. Virtualizacija programa općenito preusmjerava zahtjeve programa za pristup datotekama u druge posebno oblikovane datoteke preko kojih se dobivaju potrebni podaci. Tako se primjerice omogućuje istovremeno izvođenje programa koji se inače ne mogu istovremeno izvoditi zbog međusobnog ispreplitanja sredstava koja koriste.




***Slika 4. Virtualizacija programa***
***Izvor: MSDN Architecture Center***

## *2.3. Virtualizacija računalnog sustava*

Virtualizacija računalnog sustava omogućuje simuliranje računalnog okruženja čime se sakrivaju svojstva izvorne platforme. Pritom se virtualna računala izvode kao da su izravno povezana na sklopovlje, no u stvarnosti njihov je pristup računalnim sredstvima ograničen virtualnom okolinom.




***Slika 5. Virtualni sustav***
***Izvor: Wikipedia***

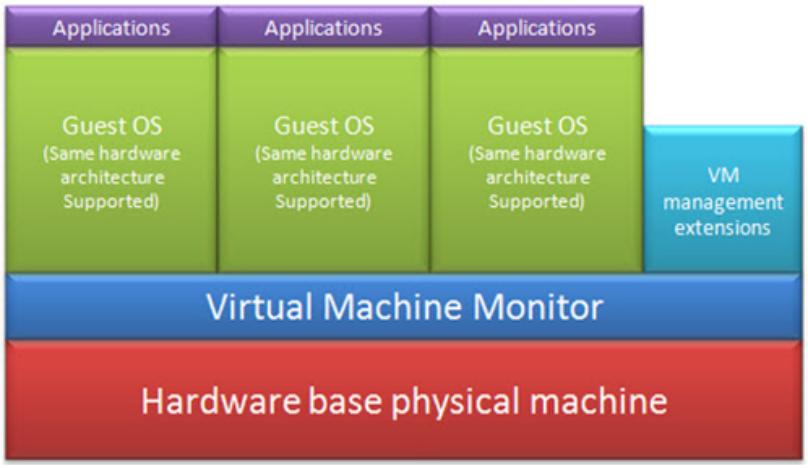
### 2.3.1. Potpuna virtualizacija

Potpuna virtualizacija oponaša dovoljno sklopovske potpore da se operacijski sustav nepromijenjen može izvoditi na virtualnom računalu. Sklopovsko okruženje pritom uključuje procesor, radnu memoriju te dodatne memorijske i periferne uređaje (USB, grafičke, zvučne kartice i slično). Potpuna virtualizacija uključuje ispunjavanje sljedeća tri zahtjeva:

1. ekvivalencija – programi pokrenuti na virtualnom sustavu ponašaju se potpuno jednako kao što bi se ponašali na odgovarajućem realnom sustavu,
2. upravljanje sredstvima – virtualizacijska podrška potpuno upravlja virtualnim sredstvima i
3. učinkovitost – većina strojnih instrukcija može se izvoditi izvan virtualne okoline.

Kako bi se zadovoljili uvjeti potpune virtualizacije skup strojnih naredbi procesora (eng. ISA – Instruction Set Architecture) mora zadovoljavati određena svojstva. Naime, osjetljive naredbe koje virtualni stroj mora presresti su one koje mijenjaju konfiguraciju računalnih sredstava ili čije ponašanje i rezultat ovisi o konfiguraciji računalnih sredstava. Takve naredbe moraju se izvoditi na način da ih virtualni stroj može presresti i prilagoditi. U tu svrhu može se koristiti i binarno prevođenje naredbi kojim se kritične naredbe zamjenjuju skupom sigurnih naredaba.

Potpuna virtualizacija nije moguća na svim sustavima, uključujući starija izdanja AMD-V i Intel-VT sklopovlja.



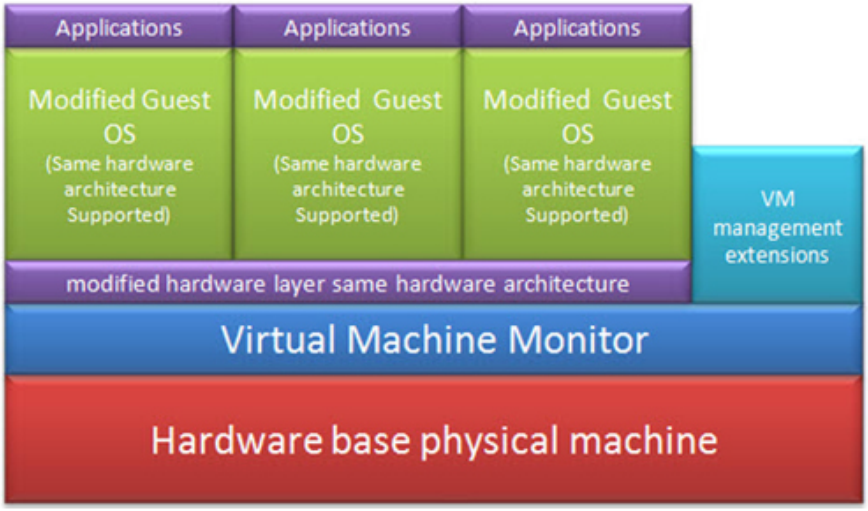

***Slika 6. Potpuna virtualizacija***
***Izvor: MSDN Architecture Center***

Gornja slika prikazuje shemu potpune virtualizacije. Na njoj se vidi kako se VMM sustav, koji presreće, obrađuje i prosljeđuje naredbe pojedinačnih operacijskih sustava sklopovlju, nalazi izravno iznad sklopovlja. Uz programsku potporu za komunikaciju korisnika s VMM sustavom (eng. VM management extensions), iznad VMM sloja izvode se i nepromijenjeni operacijski sustavi te programi u njima.

### 2.3.2. Djelomična virtualizacija

Djelomična virtualizacija za razliku od potpune virtualizacije ne uključuje simulaciju cijelog sklopovlja, već samo određenog dijela. To najčešće znači da se na virtualnom stroju ne može pokretati cijeli operacijski sustav, ali može se pokretati velik broj programa. Primjer djelomične virtualizacije je odvajanje adresnih prostora, odnosno dodjeljivanje zasebnog virtualnog adresnog prostora svakom virtualnom stroju. Ovaj tip virtualizacije koristan je kod dijeljenja memorijskih sredstava među različitim korisnicima. Općeniti značaj ove metode više je povijestan nego praktičan, a odnosi se na približavanje ostvarenju potpune virtualizacije.

Uz djelomičnu virtualizaciju postoji i tzv. „paravirtualizacija“. Riječ je o metodi koja omogućuje simuliranje operacijskih sustava, ali za razliku od potpune virtualizacije ne simulira se izravan rad sa sklopovljem već se komunikacija obavlja preko posebnog API-ja (eng. Application Programming Interface) koji se naziva „*hypervisor*“. Zbog toga se sustavi ne mogu instalirati na virtualnom stroju u izvornom obliku već je potrebno prilagoditi ih za komunikaciju s nadzornim (eng. hypervisor*)* sučeljem.




***Slika 7. Paravirtualizacija***

***Izvor: MSDN Architecture Center***

Usporedba paravirtualizacije i potpune virtualizacije vidljiva je i na slici paravirtualizacije koja uključuje dodatan sloj između VMM sloja i operacijskih sustava (*hypervisor*) preko kojeg se obavlja prilagođena komunikacija.

### 2.3.3. Sklopovski potpomognuta virtualizacija

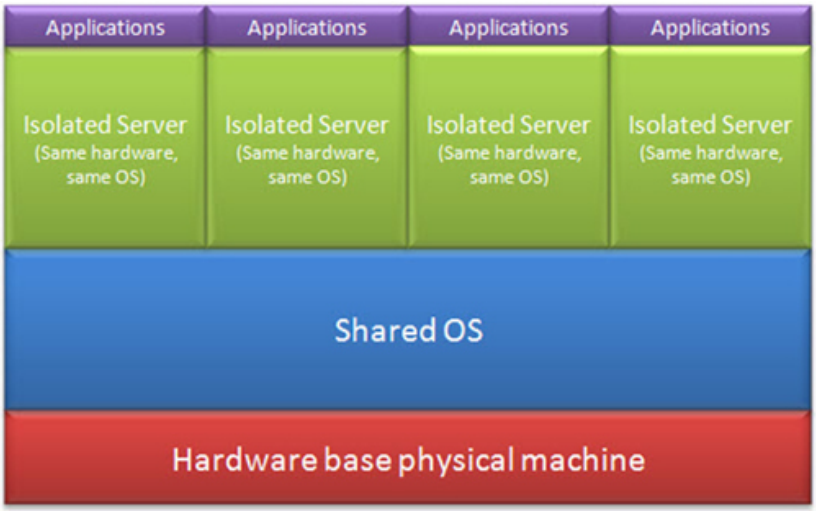
Ova vrsta virtualizacija odnosi se zapravo na potpunu virtualizaciju koja koristi posebno prilagođene procesore fizičkog poslužitelja. Riječ je o prilagodbama koje omogućuju uočavanje osjetljivih instrukcija te njihovu zamjenu i oponašanje skupom odgovarajućih sigurnih instrukcija u sklopovlju. Naspram programskog ostvarenja, sklopovska virtualizacija strojnih instrukcija znači veću učinkovitost. Primjeri ovih tehnologija za x86 arhitekture procesora su Intel VT i AMD-V, VT-i. Virtualne okoline koji koriste sklopovsku potporu su WMware Workstation, Xen 3.x, Linux KVM i Mycrosoft Hyper-V.

Problem kod ove vrste virtualizacije je zahtjev za posebnim sklopovljem koje povećava učinkovitost rada u virtualnim okolinama, ali smanjuje učinkovitost kod drugih primjena.

### 2.3.4. Virtualizacija na razini OS-a

Kod ove vrste virtualizacije jezgra ili operacijski sustav omogućuju odvajanje korisničkih prostora koji sa strane korisnika izgledaju kao potpuni poslužitelji. Pritom su često uključeni alati za upravljanje računalnim sredstvima (memorijom, diskom i sl.). Problem kod ove vrste virtualizacije je taj što se ne mogu koristiti virtualni poslužitelji s različitim operacijskim sustavima od stvarnog poslužitelja. Prednosti su pak što nema narušavanja učinkovitosti rada virtualnih strojeva jer se izravno koristi stvarni operacijski sustav, bez sklopovskog ili programskog prevođenja virtualnih u stvarne naredbe.

Na donjoj slici vidljivo je kako u ovom slučaju nema VMM sloja, već se virtualni sustavi pokreću iznad operacijskog sustava domaćina. Pritom su svi sustavi isti kao i sustav domaćin jedino su podijeljeni u odvojene poslužitelje.




***Slika 8. OS Level virtualizacija***
***Izvor: MSDN Architecture Center***

### 2.3.5. Usporedba svih tehnika virtualizacije

U sljedećoj tablici dana je sažeta usporedba svih tehnika virtualizacije računala.

| | Prednosti | Nedostaci |
|---|---|---|
| **Potpuna virtualizacija** | Omogućuje instalaciju izvornog operacijskog sustava na virtualno računalo | Nije moguća na svim sustavima |
| **Djelomična virtualizacija** | Omogućuje dijeljenje memorijskih sredstava među korisnicima | Sam dio programa može se virtualno pokretati |
| **Paravirtualizacija** | Omogućuje instalaciju operacijskih sustava na virtualno računalo | Zahtjeva izmjene u OS-ovima koji se instaliraju |
| **Virtualizacija na razini OS-a** | Učinkovito korištenje sredstava operacijskog sustava domaćina | Svi OS-ovi moraju biti iste vrste |
| **Sklopovski potpomognuta virtualizacija** | Brži i učinkovitiji rad za virtualne sustave | Moguća smanjena učinkovitost kod drugih primjena |

***Tablica 1. Usporedba metoda virtualizacije***

## *2.4. Koristi i problemi u primjeni*

Prednosti virtualizacije se ponajviše odnose na poboljšanje učinkovitosti i olakšavanje održavanja poslužitelja. Današnji procesori, osobito x86 arhitekture, izuzetno brzo rade u odnosu na potrebe većine računalnih sustava. To znači da je velik dio sklopovskih sredstava neiskorišten. Umjesto velikog broja skupih fizičkih poslužitelja koji su slabo iskorišteni, virtualizacija omogućuje njihovu simulaciju na jednom ili manjem broju poslužitelja. Pritom je maksimizirana iskorištenost skupog sklopovlja i minimiziran trošak njihove nabave i održavanja. Osim učinkovitosti, više virtualnih poslužitelja na jednom računalu lakše je održavati nego više fizičkih odvojenih poslužitelja, ako ništa drugo zbog jedinstvenog fizičkog pristupa i jedinstvenog okruženja u kojem se pokreću.

Kod primjene metoda virtualizacije valja voditi računa o primjenama sustava i programa. Ukoliko se radi o računalno zahtjevnijim primjenama, virtualizacija može štetiti, umjesto koristiti učinkovitosti. Trajno veća iskorištenost sredstava također uzrokuje trajno pojačano zagrijavanje sustava. Uz to, svi virtualni sustavi ovise o fizičkom poslužitelju i njegovo rušenje ili isključivanje izazvat će istu pojavu kod svih virtualnih poslužitelja. Propusti u ostvarenju programske podrške za virtualni rad mogu uzrokovati različite sigurnosne probleme: od pretjeranog trošenja zajedničkih sredstava u samo jednom virtualnom sustavu do narušavanja svojstva izolacije. Posljednje bi uključivalo mogućnost pristupa podacima drugog virtualnog sustava na istom poslužitelju i utjecanja na njegov rad.

# 3. Virtualizacija i sigurnost

Virtualizacija kao metoda ima određene prednosti u smislu sigurnosti jer prema definiciji potpuno logički odvaja dijelove istog fizičkog sustava i na taj način ih štiti. S druge strane pretpostavka takve odvojenosti može biti opasna jer su u slučaju propusta u virtualizacijskoj platformi virtualni sustavi izloženiji međusobnim napadima nego oni fizički odvojeni. U ovom poglavlju razmatra se virtualizacija s gledišta njezinih sigurnosnih prednosti i nedostataka.

## *3.1. Sigurnosni ciljevi i rizici*

Općenito, računalna sigurnost podrazumijeva nekoliko različitih ciljeva. Oni se mogu podijeliti na sljedeći način:

- **Dostupnost podataka i usluga** – korisnik u svakom trenutku može pristupiti podacima i uslugama za koje ima ovlasti i taj se pristup prekida tek po završetku cjelokupne radnje, odnosno ne može biti neočekivano prekinut djelovanjem treće strane. Također, dostupnost podrazumijeva i prihvatljivu brzinu komunikacije, tj. korisnik ne mora neopravdano dugo čekati reakciju poslužitelja ili programa.
- **Tajnost** – vrijednosti podataka mogu doznati samo ovlašteni korisnici
- **Integritet** – podatke mogu mijenjati samo ovlašteni korisnici
- **Autentičnost** – Osoba ili program koji izvode neku radnju nesumnjivo su ti za koje se identifikacijskom oznakom predstavljaju.

Dostupnost podataka često se može narušiti pretjeranim zauzimanjem računalnih ili mrežnih sredstava koji onda postaju nedostupni za druge korisnike i/ili programe. Tajnost i integritet podataka mogu se narušiti ukoliko se zbog programskih propusta stekne pristup određenom dijelu sustava (diska ili memorije). Također, narušavanje svojstva autentičnosti (odnosno lažno predstavljanje) za sobom povlači i sva prava napadnutog korisničkog računa što može uključivati i pristup podacima koji su inače zaštićeni.

## *3.2. Virtualizacija kao metoda zaštite*

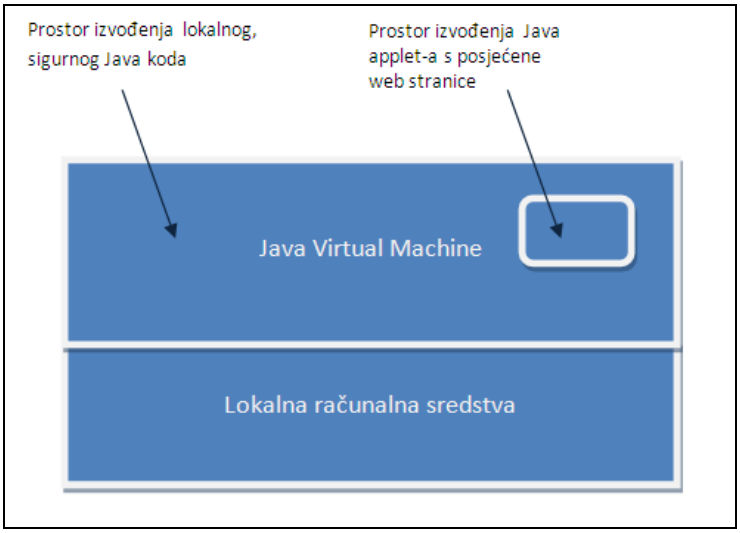
Ideja virtualizacije sama po sebi uključuje sigurnosne ciljeve zbog toga što u idealnom slučaju potpuno razdvaja dijelove sustava. Može ograničiti procesorska, memorijska i druga računalna sredstva koja se koriste. To povlači za sobom i ograničavanje okruženja u kojem se izvode različiti programi. Šteta koju crv, virus ili drugi štetni program nanese virtualnom sustavu ostaje izolirana u tom sustavu, a drugi dijelovi fizičkog sustava su netaknuti. Zato se virtualne okoline često koriste i kao metoda za ispitivanje programa i njihov razvoj (npr. osjetljivi dijelovi programa u izradi pokreću se u virtualnom stroju kako bi eventualna šteta ostala na razini tog virtualnog sustava). Osim toga, virtualni sustavi se nakon rušenja mnogo lakše i brže oporavljaju jer se mogu ponovno pokrenuti na istom ili na drugom računalu. To podrazumijeva i veću dostupnost sustava jer je manje vremena izvan funkcije - upravo zato što se jednostavno odmah može prenijeti (prekopirati) na ispravno fizičko računalo i pokrenuti. Virtualizacija spremnika podataka isto tako poboljšava njihovu dostupnost. Lakše kopiranje i prijenos virtualnih sustava na druga računala također omogućuje lakše forenzičke analize u slučaju zlouporaba. Virtualizacija se može koristiti i za ispitivanje ponašanja napadača i zlonamjernih korisnika te načina na koji pokušavaju ugroziti sustav. Takve spoznaje mogu bitno doprinijeti zaštiti stvarnih sustava.

Primjer sigurnosne tehnologije koja se može zasnivati na virtualizaciji je Sandbox. Riječ je o zaštiti računala i podataka od neželjenih i štetnih programa koja se provodi tako da se ograničavaju računalna sredstva dostupna tim programima. To mogu biti:

- procesorsko vrijeme i memorija,
- mrežni pristup,
- pristup datotekama na lokalnom ili nekom drugom poslužitelju i
- učitavanje datoteka s udaljenog poslužitelja.

Ograničavanjem prostora i mogućnosti koje program ima pri komunikaciji s operacijskim sustavom, njegova se okolina predstavlja manjom nego što zaista jest. Popularni primjeri Sandbox

alata su tzv. *appleti*. Riječ je o čestim dodacima za web preglednike koji omogućuju pokretanje programskog koda na web stranicama. Ograničavanjem uvjeta u kojima se takvi programi pokreću smanjuje se šteta koju mogu nanijeti operacijskom sustavu [10].




***Slika 9. Prostor izvođenja Java applet programa***

## *3.3. Sigurnosni problemi virtualizacije*

Sigurnosni problemi koje donosi virtualizacija povezani su s činjenicom da su i virtualni sustavi ranjivi kao i realni. To znači da sustav koji podržava virtualne sustave posjeduje ranjivosti svakog od tih sustava uključujući i ranjivosti sustava na kojem se virtualni strojevi izvode. Nadalje, sama podrška za virtualizaciju kao i svaki drugi programski kod zasigurno posjeduje propuste. Zato se ne može pretpostaviti povezanost virtualnih strojeva na istom računalu onakvom kakva je povezanost između dva udaljena računala. O slučaju virtualnih poslužitelja osim mrežne komunikacije za napad se može iskoristiti i fizička povezanost. Prema tome, posebno se važna pažnja treba posvetiti sigurnosti već spomenutog *hypervisor* sučelja koje upravlja virtualnim sustavima.

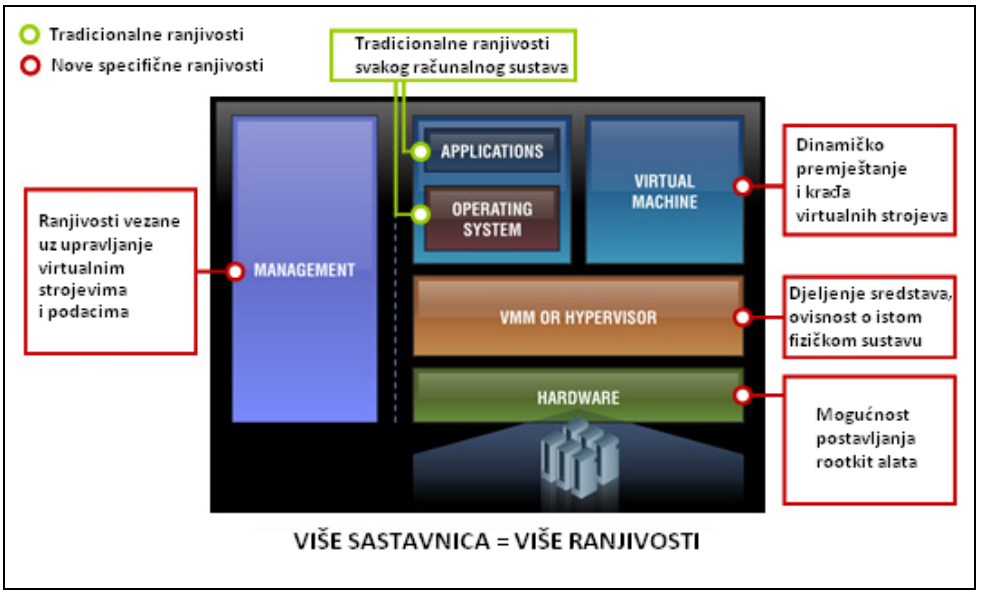
Virtualni sustavi koji se oslanjaju na izravnu komunikaciju sa sklopovljem umjesto nadogradnje nad OS sigurniji su već zbog same činjenice da nemaju problema s ranjivostima operacijskog sustava domaćina. Osim toga prednosti su sljedeće:

- Sustavi povezani izravno na sklopovlje ne dijele nikakve podatke s središnjim OS-om što stvara manje mogućnosti za otkrivanje podataka
- Dodjela sredstava preko operacijskog sustava podložna je programskim propustima takvog sustava više nego *hypervisor,* koji je izravno povezan na sklopovlje i ciljano oblikovan za dodjelu sredstava virtualnim strojevima
- Operacijski sustavi često su izloženiji djelovanju virtualnih strojeva pa su time i ranjiviji na štetne aktivnosti u njima, dok kod sklopovske podrške nema nikakve komunikacije između bilo koja dva virtualna sustava.

Zaštita virtualne sigurnosti uključuje:

1. zaštitu središnjeg sustava,
2. zaštitu sustava za virtualizaciju,
3. ispravnu izvedbu komunikacija između virtualnih sustava te
4. zaštitu svakog zasebnog virtualnog sustava.

Dolazi se do zaključka da, uz sve sigurnosne prednosti koje ideja virtualizacije nosi, njezin razvoj zahtjeva osobit naglasak na izvedbi sigurnosnih mehanizama.




***Slika 10. Sigurnosne prijetnje na virtualnim sustavima***
***Izvor: IBM***

Na slici iznad prikazane su nove prijetnje koje virtualizacija uvodi uz tradicionalne ranjivosti koje posjeduje svaki računalni sustav (kako stvarni tako i virtualni). One uključuju ranjivosti kod upravljanja sustavom i podacima te mogućnost umetanja rootkit alata u virtualno sklopovlje. Rootkit alati prikrivaju tragove kompromitiranosti sustava štetnim programima. Ovisnost o istim fizičkim sredstvima znači da će pad fizičkog sustava izravno uzrokovati pad svih virtualnih sustava. Također, dinamičnost virtualnih strojeva, odnosno mogućnost da se pokrenu na bilo kojem fizičkom računalu povećava mogućnosti njihove krađe. Ono što je prednost kod forenzičkih metoda analize sustava, također može biti i ranjivost ukoliko se sustav kopira sa štetnim namjerama.

## *3.4. Budućnost virtualizacije*

Virtualizacija posljednjih godina postaje sve češće korišten koncept u poslovnim okruženjima, od virtualnih mreža do virtualnih poslužitelja. Prema Gartnerovom istraživanju iz 2008. godine [3] do 2012. godine virtualizacija će imati najznačajniji utjecaj na promjenu načina na koje se upravlja računalnim sustavima. Utjecat će na količinu sklopovske podrške koja se kupuje, način na koji se koristi te stvoriti novo područje natjecanja među proizvođačima. Takav trend očituje se već danas. Virtualiziraju se mreže, osobna računala, poslovni poslužitelji i sl.

Prema istom istraživanju procjenjuje se da je tržište x86 poslužitelja u 2006. godini smanjeno za 4% upravo zbog virtualizacije. Predviđa se i da će zbog konkurencije padati troškovi virtualnih sustava i njihovog održavanja, što će dodatno povećati broj virtualnih strojeva od 5 milijuna koliko ih je procijenjeno u 2007. do 660 milijuna koliko ih se predviđa do 2011. U istom predviđanju veći dugoročni utjecaj predviđa se virtualizaciji sustava nego virtualizaciji programa. Predviđa se i kako će proces virtualizacije i automatizacije sustava iznjedriti nekoliko dominantnih arhitektura za upravljanje infrastrukturama.

Istraživanje trendova pretraga na Google tražilici također odražava porast interesa za ovom tehnologijom u posljednjih nekoliko godina. „*Search Volume indeks"* predstavlja relativan broj pretraga za pojmom „virtualizacija" u odnosu na sveukupni broj pretraga u toj tražilici, a „*News reference volume"* pokazuje koliko se puta prikazuje taj pojam u Google News vijestima. Prema navedenim mjerilima na slici 11 vidljiv je značajan porast zanimanja za ovaj pojam od 2004. godine do danas.


***Slika 11. Rezultati Google trends pretrage pojma „virtualization“***

Očigledno je riječ o tehnologiji koja postaje sve važnija u IT sektoru, a taj će se trend rasta nastaviti idućih godina sve dok se ne postigne maksimum razvoja i stabilizira pozicija među drugim rješenjima.

# 4. Usporedba programskih rješenja

Već je spomenuto nekoliko programskih rješenja koja primjenjuju ovu tehnologiju. Među njima su:

- VirtualBox – Sunov proizvod za x86 virtualizaciju,
- Hyper-V – Mycrosoftov sustav za virtualizaciju poslužitelja koji se temelji na *hypervisor* sučelju,
- VMware – uključuje čitav niz virtualizacijskih rješenja,
- AMD-V i Intel VT – procesorske arhitekture za potpunu virtualizaciju,
- Kernel-based Virtual Machine (KVM) – infrastruktura jezgre operacijskog sustava Linux koja podržava virtualizaciju operacijskog sustava i
- Xen – VMM sustav koji omogućuje izvođenje više operacijskih sustava na istom sklopovlju.

U nastavku dokumenta dan je kratak pregled VMware, Virtualbox i Xen rješenja.

## *4.1. VirtualBox*

VirtualBox je virtualizacijski alat kojeg je izvorno razvila tvrtka Innotek, a danas ga razvija Sun Microsystems. Prvo besplatno izdanje alata pojavilo se 2007. godine. VirtualBox omogućuje virtualizaciju x86 sklopovlja na operacijskim sustavima:

- Windows,
- Solaris,
- Linux,
- Mac OS X i
- još uvijek eksperimentalno FreeBSD.

Virtualni operacijski sustavi koji se mogu pokrenuti na ovom stroju su:

- FreeBSD,
- Windows,
- Linux,
- Solaris,
- OpenBSD, DragonflyBSD, SkyOS i drugi.


***Slika 12. VirtualBox na Mac OS X sustavu***

***Izvor: VirtualBox***

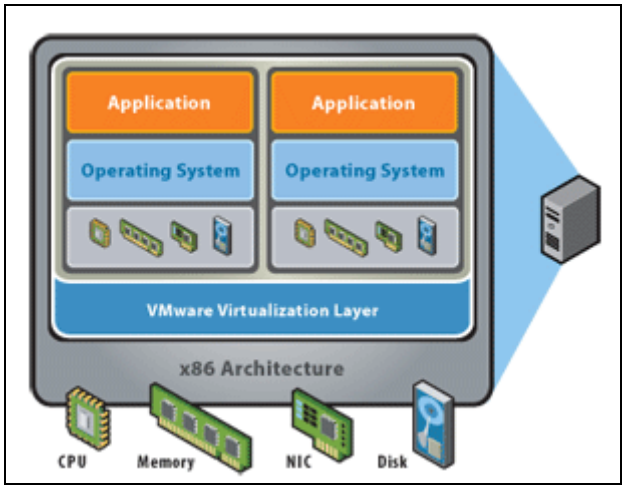
Prije nego što je postao potpuno besplatan alat, VirtualBox bio je licenciran kao tzv. „*proprietary*“ alat. To znači da se njegova uporaba naplaćivala. Također, postojala je zaštita autorskih prava i izvornog koda te ograničenja na način na koji ih korisnici mogu koristiti (kopirati, distribuirati). Danas je dostupan kao besplatan alat slobodan za neograničenu uporabu.

Na VirtualBox virtualnom stroju može istovremeno nezavisno raditi nekoliko operacijskih sustava. Svi međusobno, uključujući i OS domaćina mogu komunicirati preko zajedničkog međuspremnika ili koristeći mrežne veze. Virtualizacije sklopovlja pohranjuju se u VDI (eng. Virtual Disk Images) format. Moguće je čitati i pisati VMware-ove VMDF (eng. Virtual Machine Disk Format) i Microsoftove VHD (eng. Virtual Hard Disk) datoteke. Virtualno okruženje uključuje emulaciju mrežnih, grafičkih i zvučnih kartica pa se velik dio sustava može pokretati i bez instalacije pogonskih alata.

U slučaju problema moguće je pokrenuti ponovno prevođenje sustava dinamičkim prevoditeljem, a dostupna je i mogućnost automatske nadogradnje. Obje mogućnosti povećavaju učinkovitost i dostupnost alata. VirtualBox Web Console je izvedba ovog alata u AJAX tehnologiji, a omogućuje upravljanje sustavom korištenjem web preglednika. Nove inačice alata, uz poboljšanja učinkovitosti, trebale bi donijeti i mogućnost *paravirtualizacije* (instalacija operacijskih sustava prilagođenih virtualnoj uporabi) sustava koja trenutno nije dostupna.

## 4.2. VMware

VMWare je vodeći proizvođač virtualizacijske programske podrške. Osnovan je 1998. godine, i u većinskom je vlasništvu *EMC Corporation* organizacije. Vmware je licenciran kao već spomenuti “proprietary” proizvod. VMware proizvodi mogu se pokretati na operacijskim sustavima Windows, Linux i Mac OS X. Također, dostupan je i korporativni VMware ESX poslužitelj koji se izvodi izravno na sklopovlju čime se značajno poboljšavaju performanse.

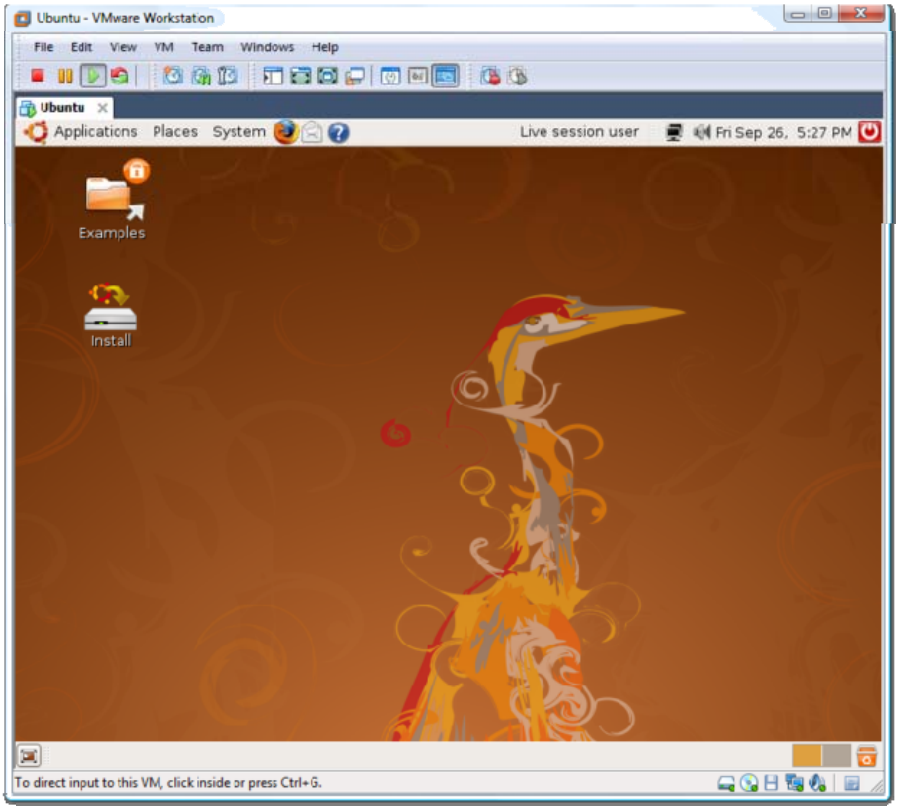



***Slika 13. Sklopovski potpomognuta VMware virtualizacija***
***Izvor: VMware***

Virtualne okoline emuliraju cjelokupno sklopovlje, tj. mrežne i diskovne uređaje, video pretvarače, uključujući i USB priključke što većina drugih virtualnih strojeva ne podržava. VMware Workstation, Server i ESX proizvodi ne prevode strojne naredbe, odnosno koriste isti skup strojnih instrukcija koji koristi stvarno sklopovlje. To značajno poboljšava performanse sustava, ali može stvarati probleme kod prenošenja virtualnih strojeva na druge fizičke arhitekture. Primjerice, virtualni stroj se mora zaustaviti prije nego se prebaci na drugi procesor. Neki od VMware proizvoda su:

- VMware Workstation – omogućuje emulaciju više različitih x64-x86 sustava na jednom računalu.
- VMware Fusion – ima istu funkcionalnost kao prethodni alat, no namijenjen je Intel Mac sustavima.

- VMware Player – riječ je o besplatnoj inačici VMware virtualnog stroja koja je dostupna za osobnu primjenu.
- VMware ESX – već spomenuti korporativni sustav koji se izvodi izravno na sklopovlju čime se bitno poboljšavaju njegove performanse.
- VMware Server – je program koji se izvodi iznad operacijskog sustava i omogućuje stvaranje više virtualnih sustava, a dostupan je besplatno kao i VMware Player.



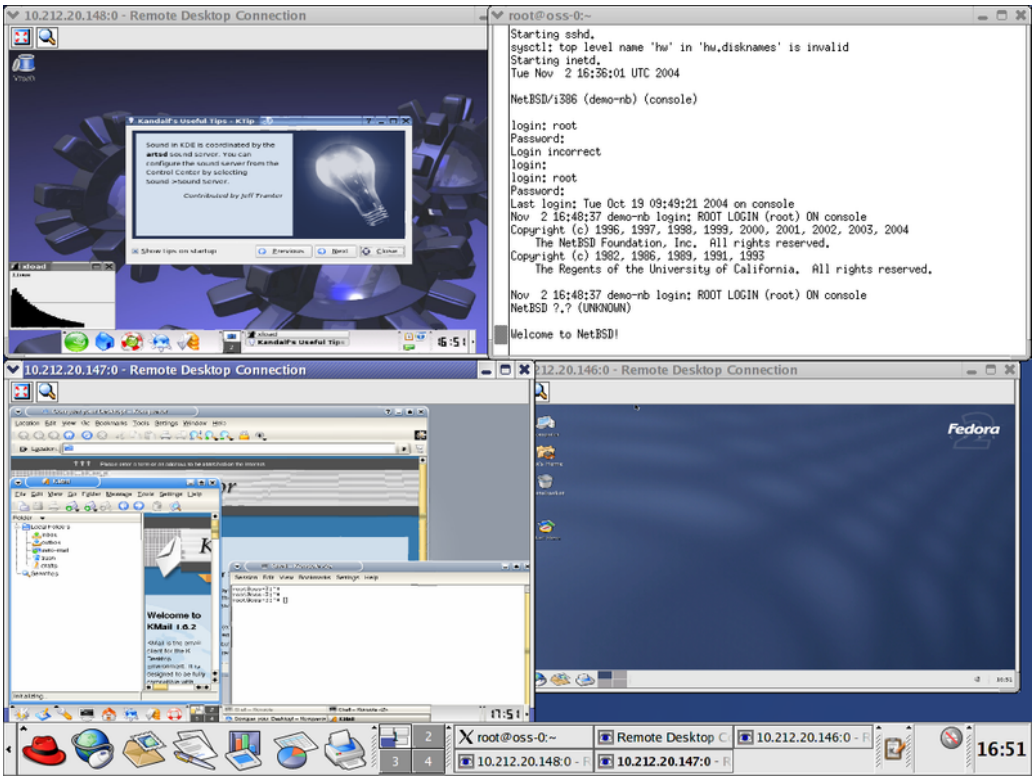

***Slika 14. VMware Workstation***
***Izvor: Wikipedia***

Drugi VMware alati omogućuju virtualizaciju programa (VMware ThinApp), upravljanje ESX/ESXi okolinom (VMware Infrastructure), virtualizaciju složenih sklopovskih i programskih infrastruktura (VMware vSphere) i druge primjene.

## *4.3. Xen*

Xen je potpuno besplatni VMM (eng. Virtual Machine Monitor) program koji omogućuje virtualizaciju na x86, x86-x64, Itanium i PowerPC 970 arhitekturama. Prvotno je razvijan na Cambridge sveučilištu i javno objavljen 2003. godine. 2007. godine dolazi u vlasništvo tvrtke Citrix System, a od ove godine dostupan je kao besplatan alat.

Xen radi kao *hypervisor* iznad sklopovlja, a omogućuje virtualizaciju više različitih operacijskih sustava istovremeno. Prvi operacijski sustav (tzv. „domain 0“) koji se izravno pokreće kod podizanja sustava, ima prava pristupa sklopovlju i preko njega se može upravljati svim drugim virtualnim operacijskim sustavima (u tzv. „domain U“ domeni). Kao *domain 0* sustav mogu se pokretati prilagođene inačice Solaris, Linux i NetBSD sustava. Prilagođene inačice nekih UNIX sustava također se mogu izvoditi i u *domain U* domeni, kao posluživani OS-ovi. Novije inačice Xena omogućuju virtualno pokretanje izvornih Windows sustava ako sklopovlje podržava x86 virtualizaciju. Takvo sklopovlje uključuje već spomenute Intel VT i AMD-V arhitekture. Xen se dakle kod različitih sklopovskih arhitektura oslanja na paravirtualizaciju, a u pojedinim slučajevima omogućuje potpunu virtualizaciju. Komercijalno dostupna inačice Xen-a je Citrix XenServer.




***Slika 15. Xen virtualni sustav***

***Izvor: Wikipedia***

Dostupan je veći broj alata za upravljanje Xen sustavom preko korisničkog sučelja. Među njima su:

- Xen Tools – perl alati za Debian GNU/Linux,
- Ganeti – orijentiran na upravljanje grozdovima računala i paralelizaciju,
- web orijentirani HyperVM – *proprietary* alat namijenjen Linux sustavima.

## 4.4. Usporedba alata

Među navedena tri alata VMware je prema performansama i širini mogućnosti možda najbolje rješenje. VirtualBox se približava VMware virtualnim strojevima, dok Xen podržava veći broj arhitektura i UNIX sustava. Ipak, njegova učinkovitost zaostaje za druga dva alata i zahtjeva prilagodbu virtualnog OS-a. Xen je pogodniji za korisnike UNIX/Linux sustava, dok će Mac OS X i Windows korisnici više koristi ostvariti od drugih dviju izvedbi.

Sva tri alata dostupna su u komercijalnim inačicama. Za razliku od VirtualBox-a i VMware-a koji podržavaju samo virtualizaciju (s izuzetkom VMware Workstationa koji podržava i paravirtualizaciju), Xen podržava samo paravirtualizaciju. Prema performansama, kao što je već spomenuto, Xen je nešto lošiji kod računalno zahtjevnijih mrežnih ili diskovnih operacija. Za razliku od Xen-a i VirtualBox-a koje je moguće prebacivati na druge procesore prilikom rada, to nije moguće na svim VMware sustavima. Xen također nema podršku za virtualni USB priključak.

| Programsko rješenje/ Podržani sustavi | Stvarni CPU | Virtualni CPU | OS domaćin | OS gost |
|---|---|---|---|---|
| **VirtualBox** | x86-x64, x86 | x86 (x86-64 u VirtualBox 2 uz sklopovsku podršku) | Windows, Linux, Mac OS X (Intel), Solaris, FreeBSD | Windows, Linux, FreeBSD, Solaris, |
| **Xen** | x86-x64, x86, IA-64 | Kao i stvarni CPU | NetBSD, Linux, Solaris | FreeBSD, NetBSD, Linux, Solaris, Windows XP (inačica 3.0 uz sklopovsku podršku) |
| **VMware** | x86-x64, x86 | x86-x64, x86 | Mac OS X, Windows, Linux | Windows, Linux, Solaris, FreeBSD, |

***Tablica 2. Usporedba alata***

| Tehničke značajke/ Programsko rješenje | VirtualBox | Xen | VMware |
|---|---|---|---|
| **GUI** | DA | DA | DA |
| **USB** | NE | DA | DA |
| **Brzina u odnosu na fizički sustav** | Približna | Približna s većim gubicima | Približna s vrlo malim gubicima |
| **Dinamička alokacija memorije** | DA | DA | DA (osim za Intel Mac) |
| **Dinamička migracija sustava** | DA | DA | DA (na većini, ali ne na svima) |
| **Moguće pokretanje sustava na drugoj diskovnoj jedinici kao virtualnog sustava** | Djelomično | DA | DA (ne većini ali ne na svima) |

***Tablica 3. Usporedba tehničkih značajki***

Detaljnija usporedba većeg broja virtualizacijskih platformi može se pronaći na Wikipediji[4].

## *4.5. Ranjivosti alata*

Ranjivosti alata za virtualizaciju najčešće se mogu iskoristiti za izvođenje napada uskraćivanja usluge, neovlašteno stjecanje većih ovlasti, stjecanje neovlaštenog pristupa i otkrivanje osjetljivih informacija. Prema statistici tvrtke Secuina za alat VirtualBox zabilježen je samo jedan propust. Riječ je o ranjivosti otkrivenoj 2008. godine koju lokalni napadač može iskoristiti za podizanje ovlasti. Propust je okarakteriziran kao lakši, a izdani su i potrebni sigurnosni ispravci.

Za VMware proizvode zabilježen je veći broj ranjivosti. Primjerice za VMware ESX Server 4.x objavljeno je 6 sigurnosnih preporuka tijekom 2009. godine. Ranjivosti su vezane uz stjecanje neovlaštenog pristupa sustavu, otkrivanje podataka, napade uskraćivanja usluge, lažno

predstavljanje itd. Pritom je čak 50% ranjivosti ocijenjeno visokim rizikom, a preko 80% njih moguće je zlorabiti pomoću udaljenog pristupa. Samo trećina ranjivosti potpuno je otklonjena. Slično stanje je sa starijim inačicama ovog proizvoda i s drugim VMware proizvodima.

Za XenServer 4.x otkrivene su dvije ranjivosti u 2008. godini. Moguća je lokalna i udaljena zlouporaba, a posljedice uključuju XSS (eng. Cross Site Scripting) napad (podmetanje proizvoljnih HTML i web skripti) i stjecanje neovlaštenog pristupa. Ranjivosti su ocjenjene niskim rizikom, a objavljena su i potrebna programska rješenja.

U ovoj usporedbi važno je napomenuti da su ranjivosti VMware proizvoda iz ove godine pa dio njih još uvijek nije saniran. Osim toga, VMware ima znatno širi spektar proizvoda, duže je na tržištu i češće se koristi od druga dva alata što ga čini i zanimljivijom metom napadačima. Zato ga ne treba doslovce shvatiti slabije zaštićenim alatom. Bez obzira na to koji alat se koristi važno je pratiti sigurnosne preporuke i redovno ga nadograđivati.

# 5. Zaključak

Virtualizacija nije novost u računarskom svijetu, ali u novije vrijeme doživljava znakovit porast interesa korisnika i proizvođača. Osim virtualizacije platformi mogu se virtualizirati programi, mreže, podatkovne infrastrukture i slični sustavi. Na novim snažim x86 računalima ona predstavlja metodu za povećanje iskorištenosti sustava i ostvarenja financijskih ušteda. Načina na koji se ova tehnologija primjenjuje na operacijskim sustavima ima mnogo: potpuna, sklopovski potpomognuta, djelomična i paravirtualizacija. Virtualni sustavi pritom se mogu pokretati izravno na sklopovlju ili na sloju OS-a.

Osim različitih načina primjene, dostupno je i mnogo različitih programskih proizvoda namijenjenih virtualizaciji. Među njima se kao vodeći ističe VMware koji nudi komercijalne, polu-komercijalne (eng. proprietary) i slobodne proizvode. Neki se mogu koristiti za osobnu primjenu, a drugi su poslovno orijentirani. VMware također odlikuje i prednost u performansama u odnosu na druge sustave. Od ostalih u ovom dokumentu predstavljeni su Xen i VirtualBox. Riječ je o potpuno slobodnim alatima koji su prema svojoj podršci više orijentirani na Unix sustave. Budući da virtualizacija nije standardizirana tehnologija svaki korisnik među mnoštvom ponuđenih rješenja odabire njemu najpogodnije.

Virtualizacija ponešto mijenja pristup računalnoj sigurnosti. S jedne strane sama po sebi izolira dijelove sustava što može biti sigurnosno iskoristivo ali s druge strane, kao i svaka druga tehnologija, sa sobom uvodi nove specifične ranjivosti. Pritom ne treba zaboraviti niti na standardne opasnosti koje prijete svakom sustavu.

U svakom slučaju riječ je o tehnologiji koja već sada ima značajno mjesto u IT sektoru, a u idućim godinama njezina stvarna uloga će se dodatno iskristalizirati. Kod njezine primjene na vlastitom sustavu dobro je biti upoznat sa prednostima koje uvodi, osobitostima upravo odabranog načina programske izvedbe i svih sigurnosnih pitanja koja se uz nju vežu. Na taj način omogućuje se svođenje sigurnosnih rizika na najmanju mjeru te postizanje najvećih mogućih dobrobiti od njezine primjene.

# 6. Reference

[1] Amit Singh, An Introduction to Virtualization, http://www.kernelthread.com/publications/virtualization/, prosinac 2009.

[2] History of Virtualization, http://www.aiosolutions.com/what_is_virtualization.php, prosinac 2009.

[3] Gartner Says Virtualization Will Be the Highest-Impact Trend in Infrastructure and Operations Market Through 2012, http://www.gartner.com/it/page.jsp?id=638207, prosinac 2009.

[4] Wikipedia, Comparison of platform virtual machines, http://en.wikipedia.org/wiki/Comparison_of_platform_virtual_machines, prosinac 2009

[5] Wikipedia, Virtualization, http://en.wikipedia.org/wiki/Virtualization, prosinac 2009.

[6] Scott Granneman, Virtualization for security, http://www.securityfocus.com/columnists/397, prosinac 2009.

[7] Xen.org, http://xen.org/, prosinac 2009.

[8] VirtualBox, http://www.virtualbox.org/, prosinac 2009.

[9] VMware, http://www.vmware.com/, prosinac 2009.

[10] Metode za poboljšanje sigurnosti web preglednika, http://www.cert.hr/filehandler.php?did=391, prosinac 2009.