CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Sigurnosna poboljšanja 64-bitnih operacijskih sustava Windows

NCERT-PUBDOC-2010-11-318

Nacionalni CERT

Nacionalni CERT+

Sadržaj

1 Uvod

Pojavom 64-bitnog operativnog sustava Windows (za x64 arhitekturu), namijenjenog širokom potrošačkom tržištu, odnosno „običnom“ korisniku, ušli smo u novo, 64-bitno razdoblje. Sve više softvera razvija se za 64-bitne platforme, a sve to kako bi dobili veće performanse sa većom količinom memorije. Najnovija istraživanja pokazuju da udio prodanih 64-bitnih operacijskih sustava Windows premašuje udio onih 32-bitnih [1].

Microsoft je ovaj prijelaz iskoristio kako bi s njime uveo i nove sigurnosne tehnologije, odnosno politiku. Sigurnost ovisi o podršci proizvođača softvera, tako da je novu politiku lakše uvesti na novim 64-bitnim platformama te tako, na neki način, prisiliti proizvođače da iz početka izrađuju softver koji poštuje novu sigurnosnu politiku. Isto tako, pošto je Microsoft sa novom 64-bitnom arhitekturom, morao razviti i potpuno novu jezgru operacijskog sustava, bilo je lakše u novu jezgru implementirati i nove sigurnosne tehnologije.

Ovaj dokument daje pregled sigurnosnih tehnologija i značajki vezanih uz 64-bitne operacijske sustave Windows. Dio tehnologija Microsoft je predstavio, sa prvom x64 verzijom operacijskog sustava Windows XP (Professional), a dio sa operacijskim sustavom Windows Vista. Također, Microsoft je navedene tehnologije stalno nadograđivao.

2 O 64-bitnim Windows operacijskim sustavima

2.1 Prednosti arhitekture

Kada se govori 64-bitnoj verziji operacijskih sustava u ovom dokumentu, podrazumijeva se verzija koja podržava procesorsku arhitekturu x64. Naime, još 2001. skupa sa predstavljanjem Windows XP operacijskog sustava, Microsoft je predstavio i 64-bitnu verziju, ali za serverske procesore sa Intel Itanium arhitekturom (ia64). Za razliku od Itanium arhitekture, x64 arhitektura namijenjena je procesorima širokog potrošačkog tržišta.

Glavni dobitak od korištenja 64-bitne arhitekture je povećanje količine RAM memorije koje operacijski sustav može iskoristiti. Kod 32 bitnih sustava teoretski maksimum je 4 GB za aplikacije i jezgru, odnosno, uz posebne postavke, maksimum koji mogu koristiti aplikacije je samo 3 GB. Kod 64-bitnih sustava teoretski je maksimum 16000 TB. Druga poboljšanja uključuju stabilniju jezgru, veće performanse sa 64-bitnim aplikacijama (posebno kod kodiranja video i zvučnih zapisa te u igrama), veću otpornost na viruse i drugi maliciozni softver (pisane za 32-bitne sustave) te mogućnost korištenja dodatnih procesorskih registara x64 arhitekture.

Što se tiče operacijskih sustava namijenjenih poslužiteljima, njihove 64-bitne verzije pružaju mnogo veću skalabilnost.

2.2 Povijesni pregled

2.2.1 Windows XP i Windows Server 2003

Microsoft je 25. travnja 2005. predstavio 64-bitnu (x64) verziju svojeg operacijskog sustava Windows XP, točnije Windows XP Professional x64 Edition. Istodobno je predstavljena i nova x64 verzija operacijskog sustava za poslužitelje, Windows Server 2003. Dva operacijska sustava dijelila su istu jezgru i kasnije su imali zajedničke nadogradnje. Najveća razlika između 32-bitnih i 64-bitnih verzija navedenih operacijskih sustava bila je podržana količina RAM memorije. Kod 64-bitnih verzija ona je nekoliko puta veća. Tako je kod Windowsa XP Professional x64 maksimum 128 GB fizičke te 16 TB virtualne memorije. Kako bi novi operacijski sustav bio kompatibilan sa 32-bitnim aplikacijama, Microsoft je uveo tehnologiju *Windows on Windows 64* (WOW64) koja je omogućila izvršavanje 32-bitnih aplikacija na 64-bitnom operacijskom sustavu. WOW radi na principu izmjene 32-bitnog i 64-bitnog načina

rada centralnog procesora te ne uzrokuje gubitak u performansama sustava. Miješanje 32 i 64-bitnog programskog koda u istom procesu nije moguće.

2.2.2 Windows Vista

Windows Vista prvi je operacijski sustav od Microsofta koji je izdan i u 32-bitnoj i u 64-bitnoj verziji istovremeno. Predstavljen je 30. siječnja 2007. Vista je sa sobom donijela mnogo novih mogućnosti i poboljšanja. Najistaknutije bilo je novo grafičko sučelje, odnosno vizualni stil Aero. Također, Vista je uključivala i *NET Framework 3.0* te je tako omogućivala programerima lakši razvoj softvera. Uvedene su nove tehnologije za ubrzanje performansi sustava putem korištenja pričuvne (*cache*) memorije. To su *ReadyBoost* i *ReadyDrive*. Druga tehnologija, nazvana *SuperFetch* koristila je analiziranje uzoraka ponašanja za određivanje sadržaja koji treba biti stalno prisutan u sistemskoj memoriji.

Slika 2.1: logotip Windows Vista

Možda i najveća pozornost pridodana je sigurnosti jer je operacijski sustav Windows XP najviše kritiziran upravo zbog toga. Vezano za sigurnost, najveća novost bila je nova kontrola pristupa, *User Account Control* (UAC). UAC je sigurnosna tehnologija koja korisnicima omogućuje normalno korištenje računala sa manje privilegija nego dosad. Prijašnji oblik ograničenog pristupa (*limited account*) pokazao se previše restriktivnim i nekompatibilnim sa mnogim aplikacijama. Kada korisnik izvršava neku aktivnost za koju su potrebne administratorske ovlasti (npr. instalacija novog softvera), mora unijeti administratorovu

lozinku (i korisničko ime, ako korisnik nije administrator). Dok UAC traži navedene povjerljive podatke, cijela radna površina operacijskog sustava je zatamnjena i blokirana (tzv. *Secure Desktop Mode*) radi potencijalnog sprječavanja malicioznog softvera da navedene korisnika na neku radnju sa kojom bi ugrozio vlastitu sigurnost. Redovito korištenje računala, kao što je surfanje Internetom, od korisnika ne zahtjeva prethodno opisanu radnju. U Web preglednik koji dolazi sa Vistom, Internet Explorer 7, također su dodana mnoga sigurnosna poboljšanja kao što je anti-phishing filter. U operacijski sustav je po prvi put ugrađen i anti-spyware alat - *Windows Defender*.

2.2.3 Windows Server 2008 i Windows 7

Operacijski sustav namijenjen poslužiteljima, Windows Server 2008, predstavljen je 27. veljače 2008, kao nasljednik Windows Server 2003 operacijskog sustava. Većinu arhitekture i funkcionalnosti, dijeli sa Windows Vistom, pošto se temelji na istoj jezgri. Jedna od novosti u novom operacijskom sustavu bila je *Windows Powershell*, naredbena ljuska i skriptni programski jezik, temeljena na objektno-orijentiranom programiranju. Uključivala je 120 administrativnih alata. Druga velika novost je bila je virtualizacijski sustav *Hyper-V* koji omogućuje pokretanje nekoliko virtualiziranih poslužitelja na jednom fizičkom. Funkcionalnost ovog sustava potpuna je samo na 64-bitnim verzijama operacijskog sustava.
Windows Server 2008 R2 (namijenjen poslužiteljima, izašao samo kao 64-bitni) i Windows 7 (namijenjen širokom spektru platformi od stolnih do ručnih računala) izdani su 22. listopada 2009. Windows 7, za razliku od svojeg prethodnika, Viste, nije donio mnogo novih mogućnosti, nego poboljšanja postojećih. Ipak, od novina, tu su: podrška za *multi-touch* (prepoznavanje višestrukog dodira ekrana), nova programska traka, podrška za virtualne diskove i bolje performanse za višejezgrene procesore. Tablica daje pregled dostupnih verzija Windows 7 i usporedbu maksimalne količine podržane RAM memorije u 32, odnosno 64-bitnim verzijama:

Tabela 2.1: maks. podržane količine RAM memorije po verzijama OS Windows 7

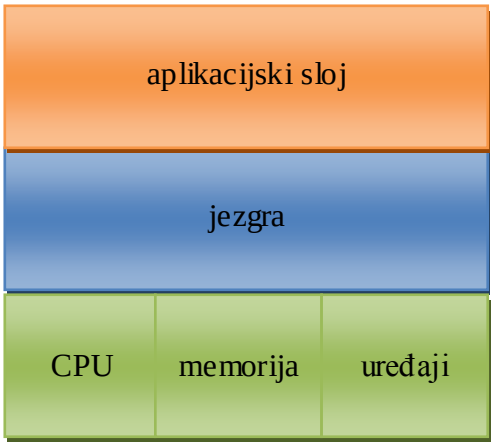
verzija Windows 7 OS	limit RAM memorije (32 bit)	limit RAM memorije (64 bit)
Ultimate	4 GB	192 GB
Enterprise	4 GB	192 GB
Professional	4 GB	192 GB
Home Premium	4 GB	16 GB
Home Basic	4 GB	8 GB
Starter	2 GB	/

3 Sigurnosne tehnologije

Ovo poglavlje daje pregled sigurnosnih tehnologija karakterističnih za 64-bitne operacijske sustave Windows.

3.1 Kernel Patch Protection

Jezgra je središnji dio operacijskog sustava, most između aplikacijskog sloja i hardverskih komponenti. Ona predstavlja najniži sloj resursa sa kojim aplikacije moraju komunicirati kako bi mogle upravljati hardverom, posebno centralnim procesorom i ulazno-izlaznim jedinicama. Slika 3.1. daje prikaz slojeva operacijskog sustava:



Slika 3.1: operacijski sustav po slojevima

Krpanje jezgre (*Kernel Patching*) je korištenje poziva internim funkcijama ili neki drugi mehanizam sa kojim se mijenja kod ili kritične strukture u jezgri Windows operacijskog sustava kodom i podacima koje Microsoft nije inicijalno dostavio kao dio jezgre. Razvojni programeri često krpaju jezgru mijenjajući funkcijske pokazivače u sistemskoj tablici servisa, odnosno niz funkcijskih pokazivača na sistemske servise u memoriji. Kada se poziva određeni sistemski servis, otpremnik za servise koristi broj servisa kako bi dohvatio funkcijskog pokazivača kojeg onda koristi za pozivanje servisa. Kada je funkcijski pokazivač izmijenjen tako da pokazuje na memorijsku adresu koda napisanog od treće strane, onda se pokreće taj kod, umjesto originalnog koda jezgre. Taj novi kod može biti nadogradnja funkcionalnosti Windows operacijskog sustava, ali može biti i maliciozan. Prema tome, krpanje jezgre zapravo krši integritet jezgre i može

negativno utjecati na pouzdanost (stabilnost), brzinu izvođenje i što je najvažnije, sigurnost. Krpanje jezgre jedan je od mehanizama kojeg koriste napadači za napade na Windows operacijske sustave. Upravo zbog navedenog Microsoft je uveo zaštitu od krpanja jezgre (Kernel Patch Protection, skraćeno KPP), poznatu i pod imenom *PatchGuard*.

Tehnologija KPP predstavljena je 2005. godine u 64-bitnim (x64) verzijama operacijskih sustava Windows XP i Windows Server 2003 (sa Service Pack 1). To je prva od tri postojećih verzija te tehnologije. Druga verzija je izašla zajedno sa 64-bitnom verzijom Windows Vista operacijskog sustava, dok je treća izašla uz Windows Server 2008 Beta 3 izdanje, a za ostale operativne sustave bila je dostupna kao nadogradnja.

Tehnologija radi tako da štiti nekoliko sistemskih struktura u 64-bitnom operacijskom sustavu. Također, ne dopušta softveru treće strane da zauzme određeni memorijski prostor, te da ga proglasi i koristi kao da je riječ o stogu jezgre. Ako sustav otkrije jednu od nedopuštenih modifikacija ili neku neautoriziranu nadogradnju (krpanje), pokreće se provjera greške i gašenje sustava, sa tzv. plavim ekranom ili samo ponovo pokretanje sustava. Oznaka provjere greške je CRITICAL_STRUCTURE_CORRUPTION.

Nedopuštene modifikacije su:

- modificiranje tablice sistemskih servisa (*system service table*)
- modificiranje tablice opisivača prekida (*interrupt descriptor table*)
- modificiranje tablice globalnih opisivača (*global descriptor table*)
- korištenje memorijskih stogova koje nije zauzela sama jezgra
- modificiranje ili nadograđivanje koda same jezgre (ili HAL ili NDIS biblioteka jezgre)

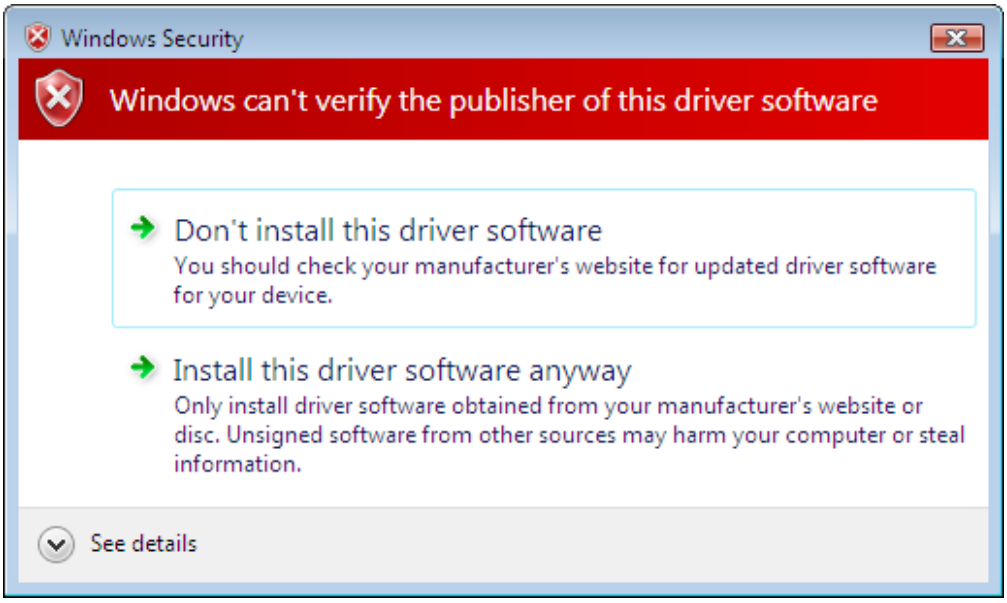
KPP je izvedena kao skup programskih rutina koje spremaju u pričuvnu memoriju (*cache*) postojeće strukture koje štite te ih potom provjeravaju u slučajnim terminima (otprilike svakih 5-10 minuta). Isto tako, kako bi se zaštitio, mehanizam koristi i prikrivanje vlastitog koda.

Microsoft je odlučio uvesti KPP sa 64 bitnim operacijskim sustavom kako bi prekinuo redovitu praksu neovlaštenog krpanja jezgre od strane upravljačkih programa u 32-bitnim sustavima. Prema tome, KPP može naštetiti kompatibilnosti softvera, što se vidjelo u slučaju anti-virusnih alata. Poznati proizvođač anti-virusnog softvera, tvrtka Mcafee žalila se Microsoftu [3] i tražila uklanjanje ove tehnologije ili da se napravi iznimka za „sigurne“ tvrtke kao što su oni. Poznato je i da se neki ostali proizvođači anti-virusnog softvera, kao što su Symatec i Kaspersky služe krpanjem jezgre. Glavni argument protivnika nove tehnologije

bio je da će napadači lako zaobilaziti novu zaštitu, dok će istodobno ona sprječavati rad sigurnosnog softvera, kao što su anti-virusni alati i sustavi za otkrivanje upada (eng. *intrusion detection system*). Međutim, Scott Field [2], sistemski arhitekt koji radi na KPP-u, istaknuo je da nije moguće izraditi listu „dobrog“ softvera za koji se zaštita ne bi primjenjivala. Razlog tome je što ne postoji pouzdan način koji bi odvojio „dobar“ softver od malicioznog te ne postoji mehanizam koji bi spriječio napadača da svoj maliciozni softver lažno prikaže „dobrim“.

3.2 Kernel Driver Signing

Sa 64-bitnom verzijom operacijskog sustava Windows Vista, Microsoft je uveo obavezno digitalno potpisivanje svih upravljačkih programa koji rade na razini jezgre. Ime nove sigurnosne politike je *Kernel Mode Code Signing* (KMCS). Upravljački programi koji nisu potpisani se tako ne mogu učitati i pokrenuti. Cilj je veća stabilnost i sigurnost za krajnjeg korisnika. Slika 3.2 prikazuje upozorenje korisniku pri pokušaju instalacije nepropisno potpisanih upravljačkih programa.

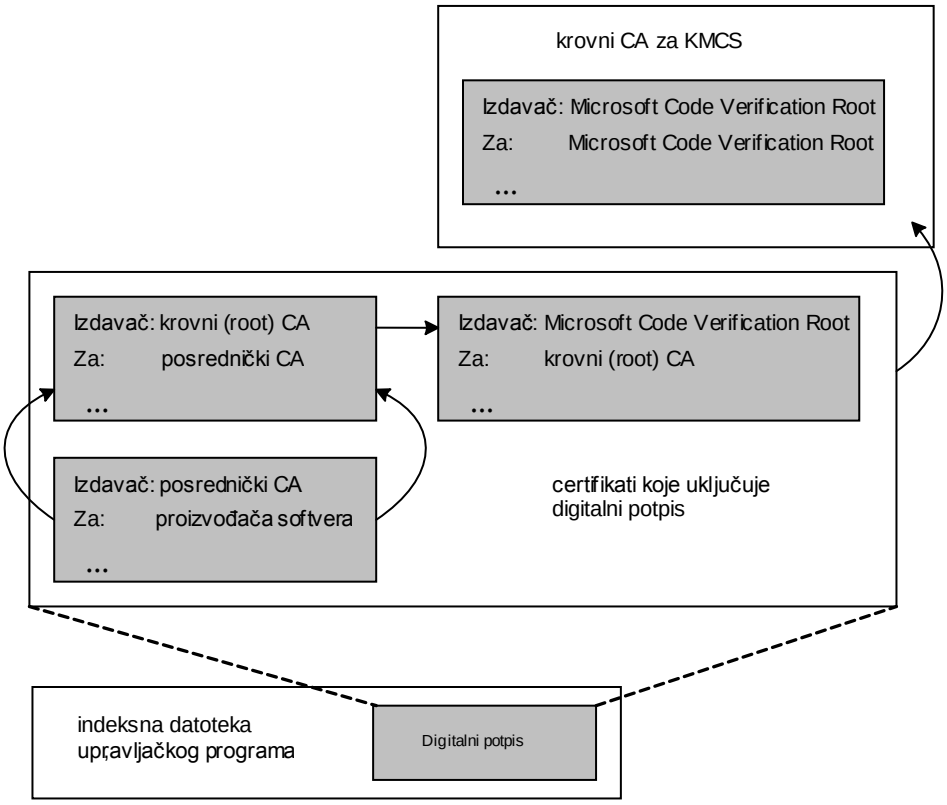


Slika 3.2: upozorenje kod instalacije nepotpisanih upravljačkih programa

Za stručnjake koji rade na razvoju softvera, ova politika ima sljedeći značaj:

- za svaku komponentu koja radi na razini jezgre, a nije digitalno potpisana, izdavači moraju dobiti certifikat za izdavanje softvera (*software publishing certificat, SPC*) i sa njim potpisati sav svoj softver;

- izdavači čiji je softver potpisan preko programa *Windows Logo Program*, moraju kataloge svojih upravljačkih programa potpisati WHQL (*Windows Hardware Quality Labs*) potpisom;
- u slučaju da je riječ o upravljačkim programima zaduženih za pokretanje (*boot*) operacijskog sustava, izdavači moraju koristiti certifikat SPC za potpisivanje.



Slika 3.3: postupak potpisivanja upravljačkih programa

Za dobivanje SPC certifikata, izdavači upravljačkih programa moraju obaviti sljedeće korake [5]:

1. Dobiti certifikat komercijalnog certifikacijskog tijela, popis onih koji izdaju certifikate za KMCS je dostupan na Web stranicama Microsofta.

2. Sa Microsoftove Web stranice skinuti odgovarajući **cross-certificate** za certifikacijsko tijelo pod 1. **Cross-certificate** je certifikat (po standardu X.509) kojeg izdaje neko certifikacijsko tijelo i njime potpisuje javni ključ drugog certifikacijskog tijela. U ovom slučaju, taj cross-certifikat izdaje Microsoftovo krovno certifikacijsko tijelo

(*Microsoft Code Verification Root*) te je tako omogućeno postojanje samo jednog krovnog certifikacijskog tijela, ali i ulančavanje certifikacijskih tijela.

Slika 3.3 [5] prikazuje hijerarhijski put kojeg treba proći neki upravljački program kako bi bio certificiran putem KMCS-a.

Negativna strana ovakvog pristupa je činjenica da proizvođač koji dobije certifikat, svejedno može proizvesti nestabilan ili maliciozan kod ili prodati svoj certifikat nekom tko bi to učinio. U tom slučaju, Microsoft može povući certifikat što bi automatski onemogućilo rad cijelog softvera od tog proizvođača. Za izdavanje certifikata, Microsoft surađuje sa nekoliko komercijalnih certifikacijskih tijela, među kojima je i VeriSign.

Kako bi se razvojnim programerima olakšao razvoj upravljačkih programa, u naprednim postavkama pri pokretanju operacijskog sustava (koji je dostupan pritiskom na tipku F8 pri pokretanju sustava) postoji opcija *„Disable Driver Signature Enforcement“* koja isključuje provjeru digitalnog potpisa. Time se olakšavaju testiranja pri razvoju upravljačkih programa.
Kako ističe Scott Field [4], glavna dobit od korištenja ove tehnologije je, što je ona način pouzdane identifikacije autora koda što pomaže pri rješavanju izvještaja koje Microsoft analizira putem svojeg mehanizma *Microsoft Online Crash Analysis*. Također, time se korisniku osigurava veća transparentnost jer može vidjeti izvor softvera kojeg ima instaliranog na svojem računalu.

3.3 Data Execution Prevention

Data execution prevention (DEP) je skup softverskih i hardverskih tehnologija koje obavljaju dodatne provjere memorije radi zaštite od malicioznog koda. Microsoft je DEP uveo sa 32-bitnim Windows XP Service Pack 2 i Windows Server 2003 Service Pack 1. Kod Microsoftovih 64-bitnih operacijskih sustava DEP je inicijalno (*default*) uključen za sve 64-bitne aplikacije, dok upotreba kod 32-bitnim aplikacija nije obavezna.

Hardverski DEP označava sve memorijske lokacije procesa kao *non-executable* (ne mogu se koristiti za izvršavanje programskog koda), osim ako ne sadrže eksplicitno izvršiv kod. Neke vrste napada upravo.koriste ubacivanje koda na te memorijske lokacije i njegovo izvršavanje, tako da DEP sprječava to te izbacuje iznimku o povredi pristupa (STATUS_ACCESS_VIOLATION (0xC0000005)). Za označavanje memorijskih lokacija, DEP se oslanja na mogućnosti centralnog procesora računala. Način na koji je DEP

implementiran ovisi o arhitekturi centralnog procesora. Glavni proizvođači procesora, AMD (tehnologija *No Execute*) i Intel (*Execute Disable*) uključili su podršku za DEP u svoje procesore.

Za razliku od hardverskog, softverski DEP neovisan je o centralnom procesoru. Riječ je o skupu sigurnosnih provjera koje su dizajnirane s ciljem sprečavanja zlouporabe mehanizma za rad sa iznimkama na Windows operacijskom sustavu.

Glavna prednost korištenja DEP-a što može blokirati maliciozni program u kojem je virus ili neki drugi oblik malvera da u proces ubaci kod koji se onda pokušava izvršiti. Kad se to dogodi, DEP izbacuje iznimku koja, ako se ne obradi, dovodi do toga da proces prekine svoje izvršavanje.

Podešavanje DEP-a u operacijskom sustavu se radi promjenom postavki u datoteci boot.ini ili *Administrator* odjelu u *Control Panel*. Potrebne su, naravno, administratorske ovlasti. Postoje četiri moguće konfiguracije i za hardverski i za softverski DEP. To su [6]:

Tabela 3.1: pregled konfiguracija za DEP

Konfiguracija	Opis
OptIn	Ova konfiguracija je početno uključena. Na sustavima sa procesorima koji podržavaju hardverski DEP, on je uključen i ograničen samo na sistemske izvršne datoteke. Ipak, uključen je i za sve 64-bitne aplikacije (naravno na 64-bitnim operacijskim sustavima), dok je za 32-bitne potrebno eksplicitno definirati da bude uključen.
OptOut	Sa ovom konfiguracijom, DEP je uključen za sve procese. Moguće je napraviti listu (Sytem dio u Control Panel) specifičnih programa za koje se neće primjenjivati DEP. Pomoću alata *Application Compatibility Toolkit*, moguće je isključiti neke aplikacije iz DEP-a (ovo ne vrijedi za 64-bitne aplikacije)
AlwaysOn	Ova konfiguracija podrazumijeva pun rad DEP-a za sve procese na sustavu. Ne postoji lista iznimki za koje se neće uključivati DEP. DEP se izvodi i uz aplikacije koji su isključeni uz pomoć alata *Application Compatibility Toolkit*.
AlwaysOff	Sa ovom konfiguracijom, DEP je stalno isključen, bez obzira da li je hardverski, odnosno procesorski podržan.

Navedene konfiguracije djeluju i na hardverski, odnosno softverski DEP.

Kao što vidimo u tablici 3.1, kod 64-bitnog operacijskog sustava, ako je hardverski DEP podržan, uvijek će se primjenjivati za sve 64-bitne procese i za memorijski prostor jezgre, te

se ne može isključiti. Dok je DEP postavljen na OptOut način rada, moguće ga je isključiti za pojedinačne 32-bitne aplikacije, ali ne i za 64-bitne.

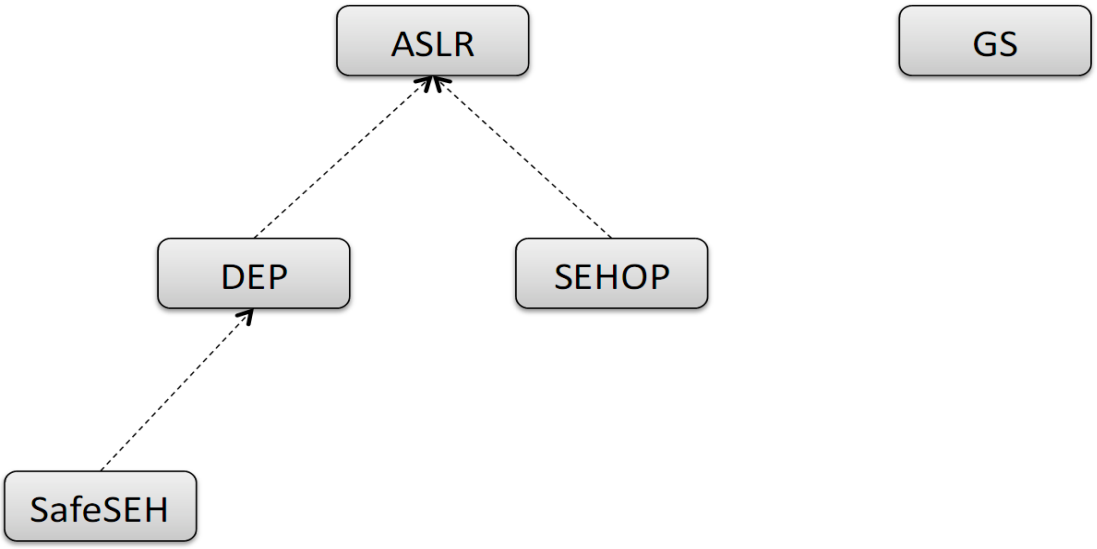
DEP je dio šireg Microsoftovog skupa sigurnosnih tehnologija, od kojih su najvažnije [7]:

- ASLR (*Address space layout randomization*);
- SEHOP (*Structured Exception Handler Overwrite Protection*);
- /SafeSEH (*Safe Exception Handlers*);
- /GS (*Stack-Based Buffer Overrun Detection*).

ASLR je sigurnosna tehnika koja uključuje nasumično postavljanje sistemskog koda, koji se izvršava, na različita, nepredvidljiva mjesta u memoriji. Time je malicioznom kodu jako teško locirati određenu sistemsku funkciju (sistemskih biblioteka u DLL datotekama) kako bi je iskoristio. ASLR u Windowsima djeluje na gomilu (dinamička memorijska mjesta), stog za pozivanje, procesni (*Process Environment Block*) i dretveni (*Thread Environment Block*) memorijski blok. DEP bez ASLR-a je potpuno neučinkovit, kao i obrnuto.

Sa operacijskim sustavima Windows Server 2008 i dodatkom Service Pack 1 za Windows Vistu, Microsoft je predstavio SEHOP. Kao što samo ime kaže, cilj ove tehnike je sprječavanja napadača da iskoristi ranjivost sustava za odašiljanje iznimki u 32-bitnim operacijskim sustavima. Čak oko 20% napada uključenih u Metaspolit, popularni alat za penetracijsko testiranje, temelji se na iskorištavanju navedene ranjivosti [11]. SEHOP sprječava napade tako što dinamički provjerava listu upravljača dretvi za iznimke prije poziva nekom od upravljača. Ako se uoči da je lista modificirana, odnosno da joj je narušen integritet, proces pozivanja iznimke se prekida. SEHOP je početno uključen u operacijskom sustavu Windows Server 2008, dok je za Windows Vista isključen zbog slabe podrške proizvođača softvera. Sljedeće dvije tehnologije, također služe za obranu od napada koje koriste sustav za odašiljanje iznimki.

Jedna od njih je SafeSEH. SafeSEH je postavka za prevođenje koda koju je Microsoft ugradio u razvojni alat Visual Studio 2003. Radi tako da sastavlja statičku listu „dobrih“ upravljača iznimki i ugrađuje ju kao meta-podatak u izvršni kod. Izvršne datoteke koje podržavaju SafeSEH dopuštaju dodatne provjere od strane sustava za odašiljanje iznimke koji tako provjerava da li je pronađeni upravljač iznimki „dobar“. Sigurnost, koju pruža ova tehnologija, može se jedino iskoristiti ako je koriste sve izvršne datoteke koje su učitane u memoriju. U suprotnom, napadač može iskoristiti bilo koju memorijsku adresu koju pronađe za svojeg zlonamjernog upravljača iznimki.



Slika 3.4: graf ovisnosti sigurnosnih tehnologija [izvor: Sotirov [8]]

GS je također postavka, odnosno zastavica koja se postavlja prilikom prevođenja koda, a služi za sprječava prelijevanje spremnika (*buffer overrun*). Radi tako da postavlja slučajno generiran broj (tzv. *cookie*) na funkcijski stog upravo prije povratne adrese. Kada se završi izvršavanje funkcije, provjerava se da li je došlo do promjene tog broja. Ako je, onda se zaustavlja izvođenje procesa. Microsoft je u sljedećim izdanjima alata Visual Studio (2005 pa 2008), unaprijedio ovu naredbu dodatnim mogućnostima.

Većina nabrojanih tehnologija ovise jedna o drugoj, odnosno ne implementirati jednu, znači drugu učiniti beskorisnom. Slika 3.4 prikazuje graf ovisnosti [8]. GS je jedina tehnologija koja je neovisna o ostalim, dok SafeSEH ovisi o DEP-u koji potom ovisi o ASLR-u, kao i SEHOP.

4 Problemi

4.1 Nedovoljna podrška proizvođača softvera

Sigurnosna tvrtka Secunia je u lipnju 2010. napravila istraživanje [9] o tome koliko pažnje proizvođači najpopularnijeg softvera pridodaju podršci za DEP i ASLR. Ovi mehanizmi ne mogu raditi bez podrške softvera. Istraživanje je obuhvatilo 16 popularnih aplikacija te pokazalo da samo njih šest ima podršku za DEP, a samo jedna ima potpunu podršku za ASLR. Stanje je bolje nego ono iz svibnja 2008. kad je samo jedna aplikacija imala podršku za DEP, ali i dalje nezadovoljavajuće. Tablica daje pregled aplikacija i podrške za DEP i ASLR za lipanj 2010.

Testiranje je provedeno na 32 bitnim operacijskim sustavima Windows XP i Windows 7. U slučaju kad DEP nije radio, podrška za ASLR se nije niti razmatrala jer ona bez DEP-a ne može funkcionirati.

Tabela 4.1: Podrška za DEP i ASLR kod popularnih aplikacija [izvor: Secunia]

Aplikacija	DEP (Windows 7)	DEP (Windows XP)	ASLR (potpuno)
Adobe Flash Player	nepoznato	nepoznato	+
Sun Java JRE			
Adobe Reader	+	+	
Mozilla Firefox	+	+	
Apple Quicktime			
VLC Media Player			
Apple iTunes	+		
Google Chrome	+	+	+
Shockwave Player	nepoznato	nepoznato	
OpenOffice.org			
Google Picasa			
Foxit Reader			
Opera	+	+	
Winamp			
Real Player			
Apple Safari	+	+	

Većina proizvođača nije implementirala DEP, a neki od onih koji jesu, nisu ga implementirali podjednako na različitim verzijama operacijskih sustava Windows. Gotovo svi proizvođači, nisu pravilno implementirali ASLR i ne sprječavaju napade jer im se dio izvršnih datoteka izvršava na fiksnim memorijskim lokacijama.

Kao što vidimo, propusti u navedenim 32-bitnim aplikacijama, mogu ugroziti i 32-bitne i 64-bitne operacijske sustave. Kada se jednog dana sve aplikacije budu pisale kao 64-bitne, morat će uključivati i podršku za DEP, inače ih operacijski sustavi Windows neće moći izvoditi.

4.2 Ranjivosti

Sigurnosti eksperti [10] napravili su detaljnu analizu tehnologije KPP (njezine najnovije verzije) i tvrde kako postoji niz tehnika koji omogućuju njezino zaobilaženje ili čak potpuno isključivanje. Neke od tehnika uključuju modifikacije brojača vremena (eng. *timer*) i korištenje propusta u radu sustava za pozivanje iznimki.

Što se DEP-a tiče, navodno, on se lagano može zaobići ubacivanjem proizvoljnog programskog koda u dio memorije koji koristi softver bez podrške za DEP (npr. Java Virtual Machine). Također, moguće ga je onemogućiti tzv. *return oriented shellcode* napadima [8], odnosno napadima koje koriste prelijevanje spremnika (*buffer overflow*) i tzv. RET naredbe za pozicioniranje u memoriji.

Trenutno ugrađena ASLR tehnologija, osim što nije dovoljno podržana od proizvođača softvera, ne uključuje dovoljno veliku entropiju (mjeru neuređenosti), odnosno memorijske lokacije na koje šalje programski kod, su i dalje djelomice predvidljive. Što se ovog tiče, situacija kod 64-bitnih operacijskih sustava je mnogo bolja nego kod 32-bitnih. Kod 32-bitnih OS, ASLR će memorijsku adresu promijeniti u jednu od 256 mogućih. To znači, ako se 256 puta uspije izvršiti napad (tzv. brute force attack), on će pogoditi traženu memorijsku adresu i izvršiti maliciozni kod. Drugi problem je što su izvršne datoteke Windows operacijskog sustava skalirane na 64 kB. ASLR utječe samo na viših 16 bitova memorijskih adresa kod pokazivača, tako da je izmjenom tih bitova moguće pomaknuti se za 64 kB na poznatu memorijsku lokaciju unutar iste DLL datoteke [8].

5 Zaključak

Sigurnosne tehnologije koje je Microsoft uveo sa svojim 64-bitnim operacijskim sustavima, predstavljaju bitan napredak. Sa novom 64-bitnom tehnologijom dobivena je i veća razina sigurnosti. Međutim, uočene su ranjivosti u tehnologijama te će ih Microsoft morati nastaviti nadograđivati. Ove tehnologije smanjit će broj napada jer je potrebno mnogo veće znanje i uloženo vrijeme za razvoj malicioznog softvera koje ih zaobilazi. S druge strane, proizvođači se još nisu prilagodili i ne pružaju dovoljnu podršku novim tehnologijama. To se u budućnosti mora ubrzati, jer ovakva sigurnosna politika najbolje funkcionira u suradnji s proizvođačima softvera. Sve veći broj korisnika 64-bitnih operacijskih sustava, također će potaknuti proizvođače softvera na razvoj 64-bitnih aplikacija, što će donijeti veći stupanj sigurnosti.

6 Literatura

1. 64-Bit Momentum Surges with Windows 7, http://windowsteamblog.com/windows/b/bloggingwindows/archive/2010/07/08/64-bit-momentum-surges-with-windows-7.aspx, 8. srpanj 2010.
2. An Introduction to Kernel Patch Protection, http://blogs.msdn.com/b/windowsvistasecurity/archive/2006/08/11/695993.aspx, Scott Field (Microsoft), kolovoz 2006.
3. Mcafee and Microsoft tangle over Vista security, http://www.zdnet.co.uk/news/security-management/2006/10/03/mcafee-and-microsoft-tangle-over-vista-security-39283750/, listopad 2006.
4. x64 Driver Signing Update, http://blogs.msdn.com/b/windowsvistasecurity/archive/2007/08/03/x64-driver-signing-update.aspx, Scott Field (Microsoft), kolovoz 2007.
5. Digital Signatures for Kernel Modules on Systems Running Windows Vista, Microsoft, 25. srpanj 2007.
6. Data Execution Prevention, http://technet.microsoft.com/en-us/library/cc738483%28WS.10%29.aspx
7. Understanding DEP as a mitigation technology part 1, http://blogs.technet.com/b/srd/archive/2009/06/05/understanding-dep-as-a-mitigation-technology-part-1.aspx, Robert Hensing (Microsoft), 12. lipanj 2009.
8. Alexander Sotirov: Is Exploitation Over? Bypassing Memory Protections in Windows 7, prezentacija, Power of Community (POC), 2009.
9. DEP/ASLR Implementation Progress in Popular Third-party Windows Applications, Secunia (Alin Rad Pop), 29. lipanj 2010.
10. PatchGuard Reloaded, A Brief Analysis of PatchGuard Version 3, Skywing, rujan 2007.
11. Matt Miller, MSEC Security Science: Preventing the Exploitation of Structured Exception Handler (SEH) Overwrites with SEHOP, http://blogs.technet.com/b/srd/archive/2009/02/02/preventing-the-exploitation-of-seh-overwrites-with-sehop.aspx, veljača 2009.