HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Sigurnosni nedostaci .NET platforme

CCERT-PUBDOC-2003-07-28

CARNet CERT u suradnji s LS&S

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

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

CARNet 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

.NET platforma pojavila se 2000. godine. Od tog vremena promijenilo se značenje i proizvodi koji su dijelovi ili su vezani uz .NET platformu. Inicijalno je .NET zamišljen kao programska platforma. Osnovni koncepti predstavljaju proširenje i unaprjeđenje već ranije poznatog Microsoft OLE-a (engl. *Object Linking and Embedding*). OLE dozvoljava kopiranje objekata i podataka između više aplikacija. ActiveX objekti koji su ustvari izvršni programi, također predstavljaju evoluciju OLE-a, a mogu se skinuti i pokrenuti unutar Internet preglednika.

.NET donosi još unaprjeđenja, omogućavajući da čitava aplikacija bude instalirana i pokrenuta na drugom mjestu (time omogućavajući potencijalno jedinstveno korisničko okruženje). Također, .NET omogućava kreiranje aplikacije korištenjem distribuiranih programskih dijelova. Npr., Windows Desktop okruženje, aplikacije i podaci biti će dostupni u istom obliku s bilo kojeg mjesta, bez obzira da li je to ured, dom ili Internet kiosk; dovoljna je samo prijava za rad. Predviđa se postojanje raznih aplikacija koje će zajednički, korištenjem Weba, osiguravati takvo integrirano okruženje. Jedan proizvođač biti će zadužen za autentikaciju i autorizaciju, drugi će vršiti pohranu podataka, a svaka od aplikacija biti će sastavljena od posebno prilagođenih komponenti.

Sve to je potencijalno moguće korištenjem distribuirane .NET programske platforme i mnogih Microsoftovih razvojnih alata poput C#, Visual J#, VB.Net, Visual Studio .NET, ASP.NET, XML-a te drugih alata i platformi.

.NET okruženje prilično podsjeća na Java model. Da bi se Java *applet* mogao pokrenuti, on mora biti izvršen unutar Java virtualnog stroja (engl. *JVM – Java Virtual Machine*). .NET izvršni programi (odnosno Windows 32 - Portable Executables) pokreću se u sličnom okruženju koje se naziva *Common Language Runtime* (CLR). To je ustvari okruženje koje se instalira prilikom instalacije Microsoft .NET Framework komponente. CLR obavlja sigurnosne provjere, provjere tipova, provjere pokazivača memorija, učitava zavisne komponente, te prema potrebi prevodi platformski neovisni kôd u izvršni kôd (engl. *JIT – Just-In-Time* prevođenje). Nadalje, postoje posredne reprezentacije izvornog koda (engl. *MSIL – Microsoft Intermediate Language*), datoteke klasa, moduli za učitavanje klasa, te posebno tretiranje provjerenog (kojem se vjeruje) i neprovjerenog programskog kôda. Neprovjereni kôd se izvršava u zasebnim okruženjima i nije mu dozvoljen pristup zaštićenim resursima sustava.

Vidljivo je da .NET i Java dijele mnoge zajedničke ideje i postavke, no .NET je mnogo složenija platforma. Poznato je da su složenost i sigurnost često suprotni zahtjevi. Npr. Java se smatra vrlo sigurnom i prilikom njenog razvoja velika pažnja je obraćena na sigurnost, no isto tako činjenica je da je od pojave Java platforme izašao velik broj zakrpi za sigurnosne nedostatke koji su naknadno pronađeni. Sigurnost Jave temelji se na međusobnoj povezanosti odgovarajućih komponenti, ukoliko neka od tih komponenti zakaže, zakazat će i cijeli sustav. Na sličan način funkcionira i .NET model izvršavanja. Logički je pretpostaviti da će i na .NET platformi naknadno biti pronađen veći broj sigurnosnih propusta i nedostataka.

2. Web servisi

Web servisi jedan su od razloga zbog kojih je .NET toliko složen. Web servisi uključuju XML aplikacije, sučelja i podatke koji su oblikovani tako da se mogu dijeliti preko raznih platformi na Internetu. Web servis može biti pojedina aplikacija koja je pokrenuta na odgovarajućem poslužitelju (engl. *ASP – Application Service Provider*), no isto tako Web servis može biti i kombinacija nekoliko aplikacija različitih proizvođača integriranih u jedinstveni servis, jednoznačan za korisnika.

Microsoft Passport prvi je primjer Web servisa. Korištenjem Passport servisa korisnik unošenjem jednog korisničkog imena i zaporke dobiva pristup svim resursima (*Web siteovima*) koji podržavaju autentikaciju korištenjem Passport servisa. U ovom trenutku Passport ima milijune korisnika, no isto tako pronađen je veći broj sigurnosnih nedostataka. Najpoznatiji i vrlo ozbiljan nedostatak otkriven je u svibnju ove godine kada je primijećeno da udaljeni napadač slanjem trivijalnog, zlonamjernog URL-a na `hotmail.com`, može promijeniti zaporku bilo kojeg korisnika Passport servisa. Na taj način napadač(i) su mogli doći do povjerljivih korisničkih podataka i/ili izazvati financijsku štetu.

Na ovom primjeru vidi se da nedostatak unutar servisa koji je toliko raširen u trenutku može utjecati na milijune ljudi i da je prilikom implementacije takvih servisa sigurnost kritična. Današnji crvi i virusi

mogu inficirati milijune računala u nekoliko minuta ili sati, no kompromitirani Web servis mogao bi dovesti do provođenja milijuna neovlaštenih komercijalnih transakcija u istom vremenskom razdoblju. Složenost i popularnost .NET modela izvršavanja brine mnoge sigurnosne stručnjake. Raširenost aplikacija, programskog kôda i podataka na Internetu mogla bi rezultirati pojavnom novih, do sad nepoznatih *exploita*. Na svu sreću, do sada su se ti *exploiti* ograničavali na nekoliko problema s već spomenutim MS Passport servisom te par crva i virusa.

3. .NET Virusi

Do sad su pronađena barem tri .NET virusa ili crva: Donut, Serot i Sharpei. Donut, koji se pojavio u siječnju 2002. godine, bio je prvi .NET virus. Poslan kao konceptualni *malware*, Donut, koji je i sam imao nedostatke, pokušavao je inficirati sve `.exe` datoteke u trenutnoj mapi i do 20 mapa iznad nje. U sebi je sadržavao nikad prikazanu poruku i mali dio MSIL kôda. Sastoji se od uglavnom uobičajenog 32-bitnog strojnog jezika, a .NET datoteke koje inficira pretvara u obične PE (engl. *portable executable*) datoteke. Donut je bio prvi .NET virus, no ubrzo zatim uslijedili su i drugi.

Ubrzo nakon Donuta pojavio se i Serot, crv koji se širio kroz lažiranu poruku elektroničke pošte s adresom pošiljatelja `support@microsoft.com`. Crv inficira sve .NET (MSIL) `.exe` datoteke na disku C: te se pokušava poslati na sve adrese elektroničke pošte koje pronađe u Windows Address Book adresaru i unutar Internet Explorer cache mapa. Slično kao i drugi virusi koji su se pojavili kasnije, Serot sadrži VBS datoteku koja služi za masovno širenje poruka elektroničke pošte. Pokazuje se da je napadačima jednostavnije korištenje skriptnih jezika nego samog MSIL-a. Serot osim toga pokušava zaustaviti antivirusne procese na zaraženim računalima i sadrži *plug-in* arhitekturu sličnu onoj koju je uspješno koristio Hybris crv.

Sharpei se pojavio u veljači iste godine, a napisan je u C# jeziku. Dolazi u tijelu poruke elektroničke pošte koja glumi Microsoftovu zakrpu `MS02-010.exe`. Virus sadrži `Sharp.VBS` datoteku koja se šalje svim kontaktima u MS Outlook adresaru. Nakon što su poruke poslane, one se brišu iz Outlook *Sent Items* mape, da bi se uklonili tragovi.

Oba virusa, Sharpei i Donut na direktan način inficiraju sustav, što znači da se izvršavaju, čine zlonamjerne akcija, da bi se zatim njihovo izvršavanja prekinulo do sljedećeg pokretanja. U budućnosti se međutim, može očekivati i pojava rezidentnih .NET virusa.

Pošto su sva tri spomenuta programa imala su određene nedostatke i zahtijevala instalaciju .NET platforme, njihovo širenje bilo ograničene naravi. No ključna stvar u svemu tome jest da mogućnosti zlonamjernog iskorištavanja .NET okruženja postoje. Samo je pitanje vremena kada će se pojaviti virusi i crvi koji će efikasnije iskoristiti mogućnosti širenja korištenjem .NET platforme.

4. Windows XP

Windows XP unapređuju NT HAL (engl. *Hardware Abstraction Level*) model, jezgru i funkcioniranje korisničkih procesa. Međutim, činjenica je da Internet Explorer i Outlook i dalje predstavljaju slabe točke u Microsoftovoj viziji "*Trustworthy Computing-a*", no operativni sistem kao takav ipak postaje sigurniji. Istovremeno, Microsoft dodaje nove opcije, od kojih se mnoge ne mogu smatrati sigurnima.

4.1. Media Player

Nekad su korisnici morali brinuti samo o zlonamjernim izvršnim programima. Podaci su bili podaci i nisu se mogli iskoristiti za pokretanje napada. No, situacija se promijenila, tako da se podaci, odnosno sadržaj u današnjem multimedijskom svijetu može također iskoristiti za napade. Moguće je zlonamjerno korištenje sadržaja za prepisivanje spremnika ili kroz umetnute skriptne jezike. Druga mogućnost zlouporabe jest korištenje lažnih zaglavlja koja pokazuju da se radi o jednoj vrsti datoteke, dok datoteka sadrži nešto potpuno drugo, što omogućava zaobilaženje sigurnosnih mehanizama. Multimedijske aplikacije često su i same ciljevi napada. Ukoliko sučelje omogućava skriptnu podršku ili osvježavanje naličja (engl. *skin*), napadači mogu izvesti stvari koje bi inače bile ograničene kroz sigurnosne zone Internet Explorera.

MS Windows Media Player instalira se sa svakom inačicom Windowsa. Windows XP izvorno su dolazili s inačicom 8.0, a nadgradnja na inačicu 9.0 je besplatno dostupna. Unazad zadnjih nekoliko godina pronađeno je više nedostataka unutar Media Player-a, a Microsoft je izdavao zakrpe nakon što su

nedostaci uočeni. Starije inačice imaju više sigurnosnih nedostataka, no mnogi korisnici oklijevaju s nadgradnjom iz raznih, uglavnom neopravdanih razloga. Naravno, Media Player nije jedina multimedijska aplikacija kod koje su uočeni sigurnosni nedostaci; Macromedia Flash, RealPlayer i Winamp, također popularne multimedijske aplikacije, isto tako sadrže brojne sigurnosne propuste.

4.2. WebDAV

WebDAV (engl. *Web Digital Authoring and Versioning*) je opcija koja se instalira na Windows XP sustavima te na sustavima na kojima je pokrenut IIS 5 ili noviji. WebDAV je otvoreni i vrlo popularni standard, no u Microsoftovoj implementaciji standarda pronađen je velik broj sigurnosnih nedostataka koji omogućavaju DoS napade ili napade prepisivanjem spremnika. Najveći problem WebDAV-a jest u tome da se predefinirano instalira i pokreće, iako ga većina korisnika uopće ne treba. WebDAV je kvalitetan alat sa kolaboraciju, no zahtijeva značajnije sigurnosne provjere i ne bi trebao biti automatski uključen u sustav. Windows Server 2003 i IIS 6 ne uključuju automatski WebDAV:

4.3. Remote Desktop Connection

Remote Desktop Connection je alat koji služi za pružanje Desktop okruženja s udaljenih lokacija na XP sustavima, slično kako je to ranije bilo moguće korištenjem NetMeeting Remote Desktop Sharing opcije ili nekih drugih komercijalnih rješenja. Remote Desktop, koji je moguće podešavati kroz *Control Panel*, koristi RDP (engl. *Remote Desktop Protocol*) te osluškuje na TCP portu 3389. Ne uključuje se automatski i do sada nije poznata mogućnost napada. Ipak, saznanje da je instaliran na svakom Windows XP sustavu i da omogućava interaktivni pristup, čini ga vrlo privlačnom metom potencijalnih napadača.

4.4. Remote Assistance

Za razliku od Remote Desktop komponente, Remote Assistance se uključuje automatski. Remote Assistance komponenta omogućava XP korisniku da korištenjem elektroničke pošte ili *instant messaginga* pozove drugog XP korisnika i omogući mu udaljeni pristup računalu. Osim kontrole radnog okruženja (engl. *desktop*), udaljeni korisnik može sudjelovati u *chat* sjednicama i prijenosima datoteka. Pozivi mogu ostati otvoreni dulje vrijeme, a predefinirana postavka je 30 dana. Jedna od najvećih zamjerki ovog sustava jest nepostojanje bilo kakvog ozbiljnijeg mehanizma autentikacije. Napadač se može lažno predstaviti kao tehnička podrška i podmetnuti zlonamjerne datoteke. Iako do sad ne postoje javno poznati *exploiti* koji bi iskorištavali Remote Assistance komponentu, ne treba zanemariti potencijalnu prijetnju od napada prepisivanjem spremnika i spojeva koji koriste slabe zaporke.

4.5. Internet Connection Firewall

Internet Connection Firewall (ICF) predstavlja prvi Microsoftov pokušaj da napravi vatrozid da osobnu uporabu. ICF-ov glavni nedostatak jest nemogućnost blokiranja odlaznog prometa. Na taj način, mnogi zlonamjerni programi, jednom kad se instaliraju, mogu inicirati komunikaciju i nastaviti s radom. Na ovaj način i dalje nisu onemogućeni npr. trojanski programi koji oglašavaju uspješnu kompromitaciju sustava ili e-mail crvi s vlastitim SMTP servisom. U oba slučaja korisnik neće biti upozoren pošto ICF dozvoljava sav odlazni promet. Većina drugih osobnih vatrozida ovakve pokušaje bi detektirala i obavijestila korisnika. Za očekivati je da će Microsoft nastaviti podržavati ICF, te dodati opcije koje će unaprijediti razinu sigurnosti koju ICF pruža.

4.6. UPnP

Univerzalni *Plug and Play* (UPnP) je još jedna opcija koja bi trebala biti predefinirano isključena. UPnP omogućava Windows sustavu da otkrije UPnP uređaje (pisače, skenere itd.) na mreži i automatski konfigurira način njihove uporabe. Pokazalo se da je UPnP bio prva pronađena sigurnosna rupa na Windows XP. Napad prepisivanjem spremnika mogao se izvesti s udaljenih lokacija (Interneta), te ukoliko vatrozid nije blokirao promet prema UTP portu 1900, nedostatak se mogao iskoristiti za preuzimanje potpune kontrole nad sustavom. Na Windows 2003 Server UPnP se uopće ne instalira.

4.7. Jednostavno dijeljenje datoteka

Jednostavno dijeljenje datoteka (engl. *simple file sharing*) opcija je na Windows XP Home sustavima. Jednom kada se mapa proglasi dijeljenom, ona je automatski dostupna svim korisnicima na lokalnoj mreži. Nikakve eksplicitne dozvole ne mogu se postaviti. Mapa se može proglasiti dostupnom samo za čitanje (engl. *read-only*), no ukoliko su omogućene i promjene, potpunu kontrolu nad mapom može imati bilo tko na lokalnoj mreži. Virusi i crvi koji imaju mogućnost širenja korištenjem lokalnih mreža ovu mogućnost mogu iskoristiti za svoje nesmetano širenje.

4.8. Windows Messenger

MS Windows *Messenger* je *instant messaging* (IM) aplikacija koja se predefinirano instalira na XP sustavima. IM klijenti otvaraju razne mogućnosti napada na sustav. Kao prvo, postoji velik broj napada prepisivanjem spremnika na razne IM klijente, čak i ako nisu uključeni već samo instalirani. Kao drugo, IM klijenti omogućavaju prihvaćanje raznih, a potencijalno i zlonamjernih datoteka od drugih korisnika. Većina antivirusnih programa, međutim, ne nadgleda takve transfere datoteka. Konačno, postoji grupa zlonamjernih programa i virusa koja isključivo cilja na Microsoftove IM klijente. Iako Windows Messenger nije ni izdaleka napadan kao npr. IRC ili AOL AIM klijenti, potencijalne sigurnosne nedostatke koje donosi svakako valja uzeti u obzir.

4.9. Office XP

Iako se Office XP ne odnosi samo na Windows XP sustave, ovdje ga svakako treba spomenuti. Jedna od značajki Office XP paketa jest mogućnost čitanja i pisanja datoteka u XML formatu. Makro virusi, koji su svojedobno predstavljali jedan od najraširenijih načina zaraze, uglavnom su onemogućeni kroz Office *macro security* te korištenjem antivirusnih alata. XML otvara mogućnost pojave nove klase virusa u Office dokumentima. Razlog tome je što se XML osim oblikovanja mogu definirati i razne druge mogućnosti poput izvršnog programskog i skriptnog kôda, multimedijskih sadržaja itd. Iskustvo podučava da fleksibilnost i razne opcije otvaraju razne mogućnosti napada.

4.10. Sigurnost

Sigurnost u Windows XP sustavima, a još više u Windows 2003 unaprjeđena je na razne načine. Windows XP su prvi Microsoftov sustav koji nudi osobni vatrozid i bez obzira na sve njegove nedostatke, razina sigurnosti može se povećati u odnosu na sustav koji nema nikakvu zaštitu takvog oblika. Također, XP koristi šifrirani datotečni sustav (engl. *EFS – Encrypted File System*), tu su još i WFP (engl. *Windows File Protection*), Certificate Services, IPSec, Kerberos, sigurnosne politike i System Restore. Sve ove dodatne opcije omogućavaju bolju zaštitu od zlonamjernih programa. Također, Winows XP i Windows 2003 predefinirano isključuju sve nepotrebne opcije, te unapređuju zaštitu datotečnog sustava i *registry* datoteke.

5. Zaključak

Složenost i raširenost .NET izvršne okoline svakako je razlog je za zabrinutost. Jednom kada se sustav raširi, zlonamjerni napadači će pronalaziti sigurnosne propuste među povezanim slojevima i aplikacijama. Sama priroda Web servisa omogućava brzo, gotovo trenutno, kompromitiranje velikog broja sustava. Do sada su poznata tri .NET virusa ili crva; iako su ti prvi zlonamjerni programi bili nespretno napisani, budući nasljednici će svakako moći iskoristiti postojeće nedostatke i ozbiljnije napasti .NET platformu.

Windows XP donose mnoga unapređenja i poboljšanja u funkcionalnosti; za neke od opcija pokazalo se nažalost da mogu biti iskorištene i u zlonamjerne svrhe, no XP sustavi također sadrže i mnoge nove sigurnosne opcije kao npr. WFP ili ICF, korištenjem kojih se može efikasnije oduprijeti prijetnjama koje mogu narušiti pouzdanost i integritet sustava.