Fakultet elektrotehnike i računarstva
Zavod za elektroničke sustave i obradbu informacija

Sustavi za praćenje i vođenje procesa

SIGURNOSNI PROBLEMI MICROSOFTOVIH APLIKACIJA

Milan Gvozdić
0036369072

Zagreb, svibanj 2007.

S A D R Ž A J

1. Uvod

U današnje vrijeme kada se tehnologija razvija neslućenom brzinom i kada sve više počinje postajati sastavni dio apsolutno svakog područja ljudske aktivnosti i djelatnosti posebna se pozornost pridaje problemu sigurnosti. Svaki moderan sustav razvijen na temeljima najnovijih tehnoloških dostignuća vrlo je ranjiv ako sigurnosni dio toga sustava ne funkcionira na najvišoj mogućoj razini, a ta ranjivost može dovesti do katastrofalnih posljedica po sam sustav koje mogu u najgorem slučaju učiniti sustav u potpunosti neupotrebljivim.

Isti takvi problemi muče microsoftove inžinjere prilikom razvoja operacijskih sustava *(OS)* i programske podrške *(softver)*. Sve brži razvoj kompjutorskih komponenti *(hardver)* zahtjeva brz razvoj pratećeg softvera te kvalitetnih i pouzdanih operacijskih sustava. U svoj toj brzini da razvoj softvera paralelno prati razvoj hardvera te u želji da se i dalje održi primat na području operacijskih sustava Microsoft je u razvoju svojih operativnih sustava Microsoft Windows XP, Microsoft Windows 2003 Server i Microsoft Windows Vista, u nekim aplikacijama koje su dolazile kao sastavni dio tih operativnih sustava (Internet Explorer, Windows Explorer) i odvojenim aplikacijama (Microsoft Office, Microsoft SQL 2005) učinio kardinalne sigurnosne propuste koje mogu dovesti (a u nekim slučajevima su i doveli) do velikih problema u funkcioniranju sustava, potpunog gubitka kontrole nad sustavom pa čak i do potpunog, nepovratnog gubitka sustava.

U ovom seminaru biti će prikazani i obrađeni najčešći načini na koji se mogu iskoristiti sigurnosni proposti te će se na par primjera prikazati na koji se način oni mogu upotrijebiti na Microsoftovim operacijskim sustavima i nekim važnijim Microsoftovim aplikacijama.

2. Računalna sigurnost

Pojam *računalna sigurnost (computer security)* može se interpretirati na više načina ovisno o razdoblju u kojem se taj pojam koristio. Danas kada su stolna računala postala sastavni dio svakodnevnog života i kada većina ljudi ima mogućnost pristupa globalnoj mreži *(Interet)* pojam računalne sigurnosti predstavlja zaštitu od kradivaca podataka *(data thieves)* i mrežnih napadača *(network attackers)* koje danas često nazivamo zajedničkim imenom : hakeri *(hackers)*. Moderna računalna sigurnost u svijetu biznisa podrazumijeva i još neke dodatne zahtjeve na sigurnost koji se odnose na probleme vezane uz kontinuitet posla te mogućnosti spriječavanja oštećenja i uništenja podataka. *(corruption & data loss)*.

Računalna sigurnost fokusira se na tri bitna pojma: povjerljivost *(confidelity)*, integritet *(integrity)* i dostupnost *(availability)*. Podaci su povjerljivi ako ostaju nedostupni svima osim onima koji imaju pravo pristupa. Pod pojmom integriteta misli se na cjelovitost i nepromjenjivost podataka unutar sustava tj. sustav ne smije dopustiti slučajno ili namjerno oštećivanje i uništenje podataka. Dostupnost također igra vrlo bitnu ulogu u funkcioniranju sustava. Računalni sustav mora omogućiti dostupnost podataka svim svojim korisnicima, a to znači da hardverski i softverski dio sustava funkcioniraju učinkovito te da se sustav u slučaju da nešto krene po zlu može brzo i u potpunosti vratiti u normalan način rada bez ikakvih trajnih posljedica po sam sustav i podatke koji se nalaze u njemu.

2.1. Prijetnje računalnoj sigurnosti *(security threats)*

Kada govorimo o prijetnjama računalnoj sigurnosti i načinima spriječavanja prijetnji najčešće se tada misli na slijedeća tri pojma: slabosti sustava, direktne prijetlje računalnom sustavu *(direct threats)* i protumjere u slučaju napada *(countermeasures*).

2.1.1. Slabosti sustava *(vulnerabilities)*

Slabosti sustava predstavljaju točke unutar sustava koje su osjetljive na napad. Preko tih slabih točki napadač *(attacker)* želi prodrijeti u sustav sa namjerom ostvarenja svojeg cilja koji može, ali i ne mora biti uvijek destruktivne prirode. Softverske slabosti mogu dovesti do pada cijelog sustava, zatim do otvaranja drugih rupa unutar sustava koje omogućuju napadaču brži i efikasniji ulaz u sustav, a u krajnjem slučaju se preko njih može sustav učiniti do te mjere nepouzdanim da korisnik više ne može biti siguran u njegov ispravan i učinkovit rad.

2.1.2. Direktne prijetnje *(direct threats)*

Direktne prijetnje računalnoj sigurnosti dijeli se u tri kategorije: prirodne i fizičke, namjerne i nenamjerne. Pod prirodne i fizičke prijetnje smatraju se prijetnje usko vezane uz probleme sa hardverom, elementarnim i drugim nepogodama. (požar, poplava, nestanak struje...). Namjerne prijetnje predstavljaju osoba ili više njih koje rade u firmi *(insiders)* ili su ubačene u firmu *(outsiders)* u svrhu pribavljanja povjerljivih i osjetljivih informacija i podataka te u svrhu degradiranja razine sigurnosti. Nenamjerne prijetnje najčešće su uzrokovane nemarom i neznanjem: puno više podataka je kompromitirano, oštećeno ili izgubljeno zbog neznanja i nemara nego zbog nekih vanjskih utjecaja.

2.2. Načini iskorištavanja slabosti unutar sustava

Svaki prosječan korisnik osobnog računala se u svom radu na njemu gotovo sigurno susreo sa pojmom kompjutorskog virusa. Upravo je to glavni razlog zašto se velika većina korisnika u tu svrhu odluči kupiti anti-virusni program misleći pritom da je njihov kompjutor siguran od nepoželjnih korisnika. Anti-virusna zaštita je uz redovito osvježavanje *(update)* baze podataka učinkovita protiv virusa, trojanskih konja i u zadnje vrijeme spyware-a, ali je zato vrlo neučinkovita po pitanju drugih oblika prijetnji sustavu. Virusi uglavnom svojim djelovanjem oštećuju ili uništavaju osobne podatke, mijenjaju djelove sistemskih datoteka kako bi što više onemogućili korisniku da sam može ukloniti virus, dok u slučaju trojanskih konja se otvaraju dodatne rupe u sustavu koje će omogućiti napadaču da se preko Interneta i određenog porta spoji sa svog računala na tuđe i pritom mu pružiti mogućnost da u potpunosti ovlada računalom te podacima koji se nalaze u njemu. Viruse i trojanske konje korisnik treba u većini slučajeva samostalno pokrenuti da bi oni počeli destruktivno djelovati na sustav. Upravo ta činjenica je i odgovor na pitanje kako se učinkovito može braniti od takvih oblika prijetnji. Datoteke koje su sumnjivog imena, koje su poslane na e-mail od korisniku nepoznatog pošiljatelja i datoteke koje su sa ekstenzijama .exe, .com, .bat (iako niti druge ekstenzije tipa .jpg, .bmp i mnoge druge nisu sigurne jer postoje programi sa kojima se unutar jedne datoteke sakriju dvije i koje se obje pokreću istovremeno sa dvostrukim klikom na ikonu) jednostavno ne treba otvarati ili treba skenirati sa anti-virusnim programom koji ima osvježenu bazu podataka o virusima. Nažalost, sa virusima i trojanskim konjima ne prestaju „muke po sigurnosti“.

Munjevitim razvojem Interneta u posljednjih 10-tak godina problem sigurnosti postao je vrlo ozbiljan problem prvenstveno zato što su na mrežu povezani milijuni korisnika diljem svijeta i što se zaraza može širiti velikom brzinom. Na tom principu širenja zaraze rade kompjutorski crvi *(computer worms)* koji su

po dizajnu vrlo slični virusima, ali za razliku od virusa se šire sami od sebe od kompjutera do kompjutera i pritom se repliciraju u tisuće kopija. Granajući se u svim smjerovima i šireći se velikom brzinom crvi zagušuju mrežu što najčešće dovodi do preopterećenja mrežnih servera i osobnih računala što za posljedicu ima blokiranje i na koncu rušenje sustava. Najčešći način širenja je taj da se crv samoreplicira i pošalje na sve e-mail adrese koje korisnik ima pohranjene u svom adresaru. Neki od crva imaju i mogućnost da tuneliranjem u sustav omoguće napadaču da preko određenog porta upravlja korisnikovim kompjuterom te tako da potpuno ovlada sustavom.

Od drugih načina kojima se iskorištavaju rupe u sustavu napadači se najčešće se koriste pomoću slijedećih metoda: preljev međuspremika, injekcija koda i Cross-site skriptiranje.

Preljev međuspremnika *(buffer overflow)* je greška u kodu koja može prouzrokovati iznimno pristupanje memoriji *(memory access exception)* i gašenje programa, a u slučaju zlonamjerne upotrebe može se iskoristiti za zaobilaženje i razbijanje sigurnosti sustava. Napadač pokušava iskoristiti taj proces za upisivanje podataka izvan granica fiksno definiranog međuspremnika sa ciljem dodavanja novih podataka prepisivanjem susjednih memorijskih lokacija, a posljedica toga upisivanja može biti rušenje pokrenutog procesa ili dobivanje netočnih rezultata. Preljev pomoću stoga *(stack-based overflow)* događa se kada prilikom izvršavanja neke funkcije pomoću preljeva međuspremnika se prepiše povratna adresa koja se nalazi na stogu. Na taj način napadač može preusmjeriti povratak iz funkcije na neku drugu memorijsku lokaciju na kojoj se nalazi maliciozni *(malicious)* kod koje će napadač iskoristiti u svrhu ostvarenja svoga cilja.

Napad injekcijom koda *(code injection)* bazira se na načinu da se maliciozni kod ubaci u kompjutorski program ili sustav iskoristivši pritom slabost sustava koji ne provjerava pretpostavke koje sustav ima prema ulaznim podacima. Glavna svrha injekcije koda je da se zaobiđe ili izmjeni glavna namjena i funkcionalnost programa što može imati katastrofalne posljedice. Ta metoda se najčešće koristi u svrhu hakiranja i krekiranja *(cracking)* sustava da bi se došlo do osjetljivih i vrlo

osobnih informacija. Postoji više vrsta injekcije koda: SQL injekcija, Cross-site skriptiranje, ASP injekcija, PHP injekcija, Shell injekcija, HTML/Script injekcija. Ovdje ćemo opisati samo SQL injekciju i Cross-site skriptiranje.

SQL injekcija *(SQL injection)* je tehnika koja iskorištava sigurnosne propuste koji se pojavljuju u sloju baze podataka *(database layer)* unutar programa. Ovaj propust se pojavljuje kada su ulazni podaci nepravilno filtrirani ili kada njihove vrijednosti nisu strogo i jednoznačno definirane *(strongly typed)* što može dovesti do nepravilnog izvršavanja programa. To se najčešće događa u situacijama kada je jedan programski ili skripti jezik implenentiran *(embedded)* unutar drugog.

Cross-site skriptiranje *(Cross-site scripting)* je sigurnosni propust koji se može pronaći u mrežnim aplikacijama koji omogućava napadaču injekciju malicioznoga koda na mrežne stranice koje gledaju drugi korisnici. Kod se najednostavnije injektira u korisnikov sustav pomoću mrežnog preglednika *(Web browser)* koji otvaranjem stranice na Internetu koja sadrži maliciozni kod preko rupe u kodu Web preglednika zarazuje korisnikovo računalo.

Uz gore navedene postoje i drugi načini kako iskoristiti propuste unutar programa i sustava (format string attack, integer overflow...) ali u današnje vrijeme se koriste rijeđe.
Za neke primjere sigurnosnih problema Microsoftovih aplikacija koristiti ćemo samo ove načine koji su detaljnije opisani.

3. Sigurnosni problemi Microsoftovih aplikacija

Tvrtka Microsoft je vodeći svjetski proizvođač operacijskih sustava. Uz razvoj operacijskih sustava tvrtka se bavi i razvojem programskih paketa različite namjene te softvera koji je integriran u operacijski sustav. Microsoftove aplikacije ćemo podijeliti u tri kategorije te ih tako i obrađivati. Prva kategorija čine operacijski sustavi *(OS)* Microsoft Windows XP, Microsoft Windows 2003 Server i Microsoft Windows Vista. Drugu kategoriju čine programi poput Internet Explorera, Windows Explorera koji su integrirani u operacijske sustave i čine njegov sastavi dio. Treću kategoriju čine samostalni programi i programski paketi poput Microsoft Office, Microsoft SQL 2005... Za svaku od ovih kategorija biti će navedeno i ukratko opisano nekoliko specifičnih sigurnosnih propusta za aplikacije koje su u svakodnevnoj upotrebi, a za koje korisnik ne zna ili ne obraća pozornost na njih.

3.1. Microsoft Windows operacijski sustavi

Microsoft Windows TCP, IP, and ICMP Processing Errors Let Remote Users Deny Service and Execute Arbitary Code

Za Windows TCP/IP stog prijavljeno je više propusta, a ovaj spada u jedan od njih. On omogućava napadaču da preko mreže uzrokuje prekid rada sustava *(denial of service)* ili da se izvrši maliciozni kod na korisnikovom računalu. Sustav zbog tog propusta neispravno potvrđuje IP pakete tako da napadač može poslati posebno kreirani IP paket koji će se izvršiti na korisnikovom računalu. Slanjem posebno kreiranog ICMP paketa napadač može resetirati sve trenutne TCP veze. Također, slanjem podvaljene *(spoofed)* TCP/IP poruke može se onemogućiti korisnikovom računalu da ostvari mrežnu konekciju. Propust postoji u procesiranju TCP SYN paketa kada

su polazna IP adresa i port *(source IP and port)* jednake destinacijskoj adresi i portu pri čemu nastaje mrežna petlja.

OS: MS Windows XP SP2, MS Windows 2003 Server SP1

Microsoft Windows Winsock and DNS Client Buffer Overflows Lets Remote Users Execute Arbitrary Code

Propust se nalazi u Winsock i DNS Client modu što omogućuje napadaču izvršenje malicioznog koda na korisnikovom računalu. Napadač pomoću posebno isprogramiranog HTML koda u trenutku kada korisnikov Web preglednik učita taj kod izaziva buffer overflow u Winsock API-ju pri čemu se istovremeno izvršava maliciozni kod. Slanjem malicioznih DNS podataka može se izazvati buffer overflow u DNS klijent sloju i naposlijetku pokretanje malicioznog koda.

OS: MS Windows XP SP2, MS Windows 2003 Server SP1

Microsoft Windows Plug And Play Stack Overflow Lets Remote Users Execute Arbitrary Code

Na temelju ovog propusta Internetom se širio crv pod nazivom Zotob.A. On je iskorištavao sustave koji su imali taj propust preko porta TCP/445. Crv ja najprije testirao port TCP/445 i preko njega je pokušao iskoristiti slabost u sigurnosti sustava. Ako je napad uspješan, crv otvara program cmd.exe na portu 8888. Preko tog porta crv šalje FTP skriptu koja instrurira korisnikovo računalo da skine i otvori malicioznu datoteku sa FTP servera koja se nalazi na napadačevom kompjutoru. FTP server se stalno nalazi u osluškujućem modu *(listen mode)* čekajući da posluži zahtjeve crva koji su uspjeli iskoristiti slabosti i zaraziti računala. Datateka koja se skine sa FTP servera sprema sa na korisnikov disk pod nazivom „haha.exe“. Crv također promijeni ne postavke u Windows registry tako da zabrani pristup sa korisnikovog računala nekim

Internet stranicama koje su uglavnom u vlasništvu antivirusnih tvrtki i tvrtki koje se bave kompjutorskom sigurnošću.

OS: MS Windows XP SP2, MS Windows 2003 Server SP1

Microsoft Windows DNS Service RPC Stack Overflow Lets Remote Users Execute Arbitrary Code

Ovaj propust se nalazi u Windows DNS service RPC (Remote Procedure Call) sučelju koji napadač može iskoristiti za izvršenje malicioznog koda. Ovaj propust se može iskoristiti samo kod serverskih sustava i to najčešće preko TCP/UDP portova 139 i 445. Kod će se pokrenuti sa svim privilegijama lokalnog DNS servisa koji se nalazi na korisnikovom računalu.

OS: MS Windows 2003 Server SP1

Microsoft Windows RPC Service May Let Remote Users Deny Servce

Napadač iskorišenjem ovog propusta može prouzročiti prekid rada na korisnikovom računalu. Pomoću nepravilnog alociranja memorije u RPC servisu može se postići stanje da sustav prestane raditi na način da proces počne koristiti previše memeorije što u konačnici dovede do pada sustava.

OS: MS Windows XP SP1

3.2. Microsoft Windows integrirani programi

Microsoft Windows Animated Cursor Bug Lets Remote Users Execute Arbitrary Code

U ovom slučaju propust u Windowsima se nalazi u procesiranju animiranih kursor datoteka što može dovesti do do izvršenja malcioznog koda. Napadač može kreirati posebnu kursor datoteku koja će pokrenuta iskorititi taj propust. Ovaj propust se može iskoristiti putem HTML-a, e-maila i nije limitiran samo na datoteke sa .ani ekstezijom. Ova rupa se može iskoristiti na više aplikacija poput Internet Explorera, Windows Explorera, Microsoft Outlooka i drugih aplikacija.

OS: MS Windows XP SP2, MS Windows Vista

Microsoft Windows Explorer COM Object Bug Lets Remote Users Execute Arbitrary Code

Propust u ovom slučaju se događa zbog nepravilnog obrađivanja pojedinih COM objekata. Napadač u slučaju ovog propusta može pomoću posebno kreiranog HTML koda prisilno spojiti korisnikov kompjutor na svoj server te pokrenuti maliciozni kod uz sve privilegije koje ima korisnik.

OS: MS Windows XP SP2, MS Windows 2003 SP1

Microsoft Windows Task Scheduler Buffer Overflow Lets Remote Users Execute Arbitrary Code

Propust u ovom slučaju se nalazi u nepravilnom izvršavanjaju kontole imena aplikacija od strane Task Schedulera pri čemu napadač može iskoristiti propust te napraviti preljev međuspremnika. Posebno kreirani HTML kod i

korisnikovo pokretanje istog u Internet Exploreru za posljedicu ima preljev međuspremnika. Napadač može isto tako i kreirati posebnu .job datoteku sa kojom će omogućiti pokretanja malicioznog koda u slučaju korisnikovog otvaranja Network Share direktorija.

OS: MS Windows XP SP2

Microsoft Windows Shell Buffer Overflows Let Remote Users Execute Arbitrary Code

Ovaj propust se manifestira u načinu na koji Windows Shell pokreće aplikacije. Windows Shell neispravno provjeri duljinu poruke prije nego što proslijedi poruku međuspremniku. Upravo na taj način napadač može iskoristiti taj propust te izazvati preljev međuspremnika i pokretanje malicioznog koda.

OS: MS Windows XP SP1

3.3. Microsoft Office i Microsoft SQL 2005 Server

Microsoft Office Allow Remote Code Execution

Propusti su pronađeni u više aplikacija koji su sastavni dio programskog paketa Microsoft Office. U MS Wordu propust se nalazi u načinu na koji program provjerava dužinu vrijednosti podataka koji su sadržani u dokumentu. U slučaju posebno kreiranog Word dokumenta, napadač može iskoristi preljev međuspremnika i preuzeti kontrolu nad sustavom. U MS Excelu sigurnosni propust postoji u načinu na koji program provjerava spreadsheetove prije čitanja makro instrukcija. Napadač može iskoristiti taj propust i zaobići makro sigurnosni model. Pokretanje malicioznog spreadsheeta, propust omogućuje izvršenje malicionznog makroa sadržanog unutar spreadsheeta.

U MS Powerpointu prostoji propust sa obrađivanjem oštećenih prezentacija koje mogu dovesti do izvršavanja malicioznog koda u slučaju da korisnik pokrene jednu od takvih prezenzacija pri čemu napadač može u potpunosti ovladati sustavom. Ovim propustom se koriste i trojanski konji Trojan.Controlppt.W i Trojan.Controlppt.X poznati kao PPDropper.F i Exploit-PPT.d.

Programski paket: MS Office 2000, MS Office 2003

Zanimljiva je situacija sa Microsoft SQL 2005 Server aplikacijom. Pretraživajući Interenet pregledao sam više stranica koje se bave problemima mrežne i kompjutorske sigurnosti i na moje veliko čuđenje nisam našao niti jedan propust koji je objavljen za Microsoft SQL 2005 Server. Sa nevjericom prelazim na pisanje zaključka...

4. Zaključak

Cilj ovog seminara bio je obraditi neke specifične prijetnje i propuste unutar Microsoftovih operacijskih sustava i aplikacija. Kao što je vidljivo iz primjera sigurnosnih propusta problem sigurnosti predstavlja vrlo ozbiljnu prijetnju po korisnika, njegovo računalo i sustav u cijelini. Problem počiva u širokom spektru propusta koje je moguće napraviti, a najveću ulogu u svemu tome igra ljudski faktor počevši od programera pa sve do krajnjeg korisnika koji u većini slučajeva igra i presudnu ulogu u cijeloj priči iako je stvarno tu teško naći neku objektivnu sredinu u krivnji. Kolika je krivnja hakera u cijeloj toj priči? Rade li hakeri to samo iz vlastite satisfakcije ili ipak žele ukazati na probleme koji postoje? Jedno je sigurno, programeri troše ogromne količine vremena i financijskih sredstava na ispravljanje propusta, korporacije troše milijune dolara na sigurnost, hakeri izmišljaju pakosti i traže načine kako iskoristi propuste, ali i dalje će postojati pametni korisnici koji će otvarati mailove i razne druge dokumente koji stižu iz Londona, glavnog grada Nigerije u kojima piše da su osvojili milijune na lotu ili dobijaju ponude za podjelu bogatsva sa udovicom nekog milijardera iz neke afričke države. Sve je to, jednostavno rečeno, Sizifov posao.