HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

# Sigurnost IIS 6.0 poslužitelja

**CCERT-PUBDOC-2004-11-96**

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

Internet Information Services (IIS) Microsoft-ov je Web poslužitelj razvijen za NT porodicu Windows operacijskih sustava. Preciznije, riječ je o programskom paketu koji uključuje HTTP, SMTP, FTP i NNTP poslužitelje, ASP i ASP.NET razvojno okruženje, te niz dodatnih alata namijenjenih lakšem održavanju poslužitelja.

Ranije inačice IIS poslužitelja poznate su po velikom broju sigurnosnih propusta koji su napadačima omogućili uspješno provođenje napada te preuzimanje kontrole nad ciljnim sustavom. Još uvijek se pamte imena kao što su Nimbda, Code Red i sl., poznati mrežni crvi koji su prouzročili brojne štete i financijske gubitke širom Interneta. Iako su za većinu otkrivenih propusta zakrpe bile objavljene vrlo brzo nakon otkrivanja ranjivosti, brojni sustavi bili su kompromitirani s obzirom da problemi nisu bili pravovremeno uklonjeni. Čak i danas, skoro 3 godine nakon prve pojave Nimbda mrežnog crva (prva inačica primijećena je u siječnju 2002. godine) na Internetu se mogu naći poslužitelji na kojima nisu instalirane sigurnosne zakrpe koje uklanjaju ranjivost putem koje se širio ovaj destruktivni crv.

Vjerojatno potaknut lošom reputacijom koju je IIS programski paket stekao kroz godine, Microsoft se kod najnovije 6.0 inačice odlučio na velik zaokret i potpuni redizajn kako bi stvorio Web poslužitelj koji će sa stanovišta sigurnosti, pouzdanosti i jednostavnosti u potpunosti zadovoljiti potrebe korisnika. U novoj inačici promijenjena je kompletna arhitektura poslužitelja, većina programskog koda napisana je iznova, a posebna pažnja posvećena je i inicijalnim postavkama poslužitelja (aktivnim servisima, ovlastima pristupa i sl.) koje su kod ranijih inačica donijele brojne probleme.

U nastavku dokumenta biti će opisane osnovne karakteristike IIS 6.0 poslužitelja te sigurnosna poboljšanja u odnosu na ranije inačice.

## 2. Ranije inačice IIS poslužitelja

Prvu inačicu Internet Information Server poslužitelja Microsoft je objavio u travnju 1996. godine. IIS poslužitelj razvijen je s ciljem probijanja na IT tržište, ali i promocije tada aktualnog Windows NT 3.51 operacijskog sustava. Nedugo nakon inačice 1.0 objavljena je i inačica 2.0, koja se isporučivala s operacijskim sustavom Windows NT 4.0. Inačica 2.0 nudi poboljšane performanse i bolju podršku za povezivanje Web stranica s bazama podataka. Do većih promjena došlo je tek u inačici 3.0, koja se pojavila krajem 1996. godine, kada je programskom paketu dodano i okruženje za razvoj Web aplikacija. IIS 3.0 uključuje razvojno okruženje ASP (*Active Server Pages*), podršku za skriptne jezike VBScript i JavaScript, baze podataka, ActiveX i Java aplikacije i mnogo drugih. IIS 3.0 je tada Web programerima omogućio veliku fleksibilnost pri razvoju dinamičkih Web sadržaja, što je u to vrijeme svakako bila jedna od prednosti ovog programa. No, s porastom popularnosti i raznolikosti sadržaja počeli su se javljati i različiti problemi vezani uz sigurnost i pouzdanost poslužitelja. Pronađeni su mnogi sigurnosni nedostaci zbog kojih su Web aplikacije i sam IIS poslužitelj postali osjetljivi na mnoge vrste napada.

Sljedeća inačica, Internet Information Server 4.0, objavljena je u Windows NT 4 Option Pack proširenju. Slično kao i kod prethodne inačice, s vremenom su pronađeni novi sigurnosni propusti koji su rezultirali brojnim problemima i sigurnosnim incidentima. Osnovni problem kod IIS 4.0 programskog paketa bilo je vrijeme potrebno za instalaciju, instalacija sigurnosnih zakrpi, te naknadno podešavanje servisa kako bi se postigla zadovoljavajuća razina sigurnosti. Inicijalna instalacija IIS 4.0 paketa, naime, uključuje HTTP, SMTP i FTP poslužitelje. Također, inicijalno su bili aktivni mnogi servisi, koji većini korisnika nisu bili neophodni, a unosili su dodatni sigurnosni rizik. S obzirom na spomenute probleme administrator sustava morao je nakon inicijalne instalacije utrošiti mnogo vremena na instalaciju sigurnosnih zakrpi, podešavanje postavki poslužitelja i sl., kako bi se razina sigurnosti poslužitelja podigla na zadovoljavajuću razinu. Više informacija o spomenutoj problematici moguće je pronaći na adresi http://www.securityfocus.com/infocus/1311, gdje su navedene detaljne upute o tome kako na "siguran" način instalirati IIS 4.0 poslužitelj.

Internet Information Services 5.0 programski paket dio je Windows 2000 Server operacijskog sustava. Iako je osnovna zamisao bila olakšati instalaciju i korištenje IIS 5.0 paketa te podići razinu sigurnosti poslužitelja, nakon određenog vremena pokazalo se da i inačica 5 sadrži ozbiljne sigurnosne propuste i da je potrebno dosta vremena posvetiti konfiguraciji poslužitelja kako bi se postigla odgovarajuća razina sigurnosti. Više informacija o spomenutoj problematici moguće je naći na adresi http://www.securityfocus.com/infocus/1312.

Jedan od poznatijih sigurnosnih propusta kod IIS 5.0 poslužitelja je *buffer overflow* ranjivost unutar ISAPI modula za rukovanje printer datotekama (`C:\WINNT\System32\msw3prt.dll`) koji implementira podršku za IPP (*Internet Printing Protocol*). Nedugo nakon objave ove ranjivosti na Internetu se pojavio maliciozni program pod imenom `jill`, koji je neovlaštenim korisnicima omogućavao iskorištavanje propusta te pristup sustavu pod ovlastima SYSTEM korisničkog računa. Sličan problem uskoro je uočen i kod `idq.dll` ISAPI modula koji dolazi kao dio Windows 2000 Indexing Service servisa. Uskoro se pojavio i poznati Code Red mrežni crv koji je iskorištavao upravo opisane propuste. Srećom, Code Red crv nije bio toliko destruktivan koliko je mogao biti s obzirom na način njegova širenja i problem koji je iskorištavao.

# 3. Sigurnost IIS 6.0 poslužitelja

S ciljem podizanja razine sigurnosti i zaboravljanja loših iskustava, Microsoft se odlučio napraviti značajne izmjene u odnosu na prijašnje inačice IIS poslužitelje. Riječ je o potpuno redizajniranom proizvodu koji bi trebao biti znatno pouzdaniji, sigurniji i lakši za održavanje i koji bi u potpunosti zadovoljavao stroge sigurnosne zahtjeve koji se danas nameću pred proizvode ovakvog tipa.
Microsoft govori o poboljšanjima na svim razinama - od unaprjeđenja samog programskog koda, preko načina na koji poslužitelj odgovara na klijentske zahtjeve, pa do inicijalnih postavki i načina instalacije poslužitelja.

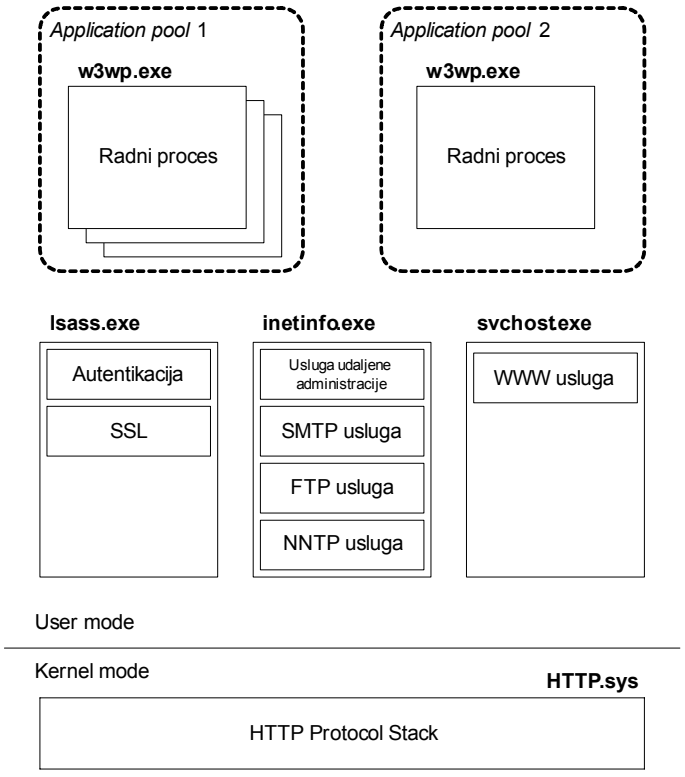
## 3.1. Arhitektura

Osnovne komponente IIS 6.0 poslužitelja su:

- HTTP stog (`HTTP.sys`),
- WWW servis (`svchost.exe`),
- Servis za administriranje te FTP, SMTP i NNTP servisi (`inetinfo.exe`),
- Autentikacija i SSL podrška (`lsass.exe`),

Aplikacijski bazeni koji sadrže radne procese (`w3wp.exe`).

Osnovna arhitektura IIS 6.0 poslužitelja prikazana je na sljedećoj slici (Slika 1).




**Slika 1:** Arhitektura IIS poslužitelja

HTTP stog (*HTTP Protocol Stack*), sadržan u `HTTP.sys` komponenti, zadužen je za primanje i obradu zahtjeva, provjeru njihove ispravnosti, te razvrstavanje zaprimljenih zahtjeva u redove iz kojih ih preuzimaju odgovarajući procesi. Realiziran je kao upravljački program koji radi na razini jezgre, operacijskog sustava, čime se postižu znatno bolje performanse budući da se prilikom obrade zahtjeva ne prelazi u korisnički način rada. Također se smanjuje i vrijeme utrošeno na promjene konteksta, jer

se zahtjev prosljeđuje izravno od sistemskog procesa korisničkom procesu koji odgovara na zahtjev (za razliku od ranijih inačica kod kojih je zahtjev bilo potrebno proslijediti od jednog korisničkog procesa drugom korisničkom procesu).
HTTP stog zadužen je i za generiranje odgovora na korisničke zahtjeve. S ciljem podizanja razine sigurnosti, ova komponenta realizirana je tako da radi sama za sebe i nikad ne poziva ili izvršava vanjski kod koji bi mogao ugroziti sigurnost sustava.
Iz reda u koji ga svrsta HTTP stog, zahtjev preuzima odgovarajući korisnički proces, koji se naziva i radni proces (engl. *worker process*). Njegova je zadaća dohvat statičkih HTML stranica, kao i interpretiranje koda Web aplikacija, obrada CGI skripti, pozivanje ISAPI ekstenzija i sl. Web aplikacije se grupiraju u skupine nazvane *Application Pools*. Za svaku takvu skupinu zadužen je najmanje jedan radni proces. Na taj način se postiže veća pouzdanost, jer prekid rada jednog radnog procesa ne utječe na rad ostalih Web aplikacija na poslužitelju (štoviše, ukoliko je za Web aplikaciju istovremeno zaduženo više radnih procesa, prekid rada jednog od njih neće rezultirati prekidom rada aplikacije).
Još jedna novost u arhitekturi IIS-a 6.0 je komponenta za administriranje i nadzor rada WWW servisa (engl. *WWW Service Administration and Monitoring component*), koja je realizirana u `svchost.exe` komponenti. Prilikom pokretanja poslužitelja ova komponenta čita postavke Web poslužitelja iz *metabase* baze i inicijalizira tablicu za usmjeravanje zahtjeva (*namespace routing table*) koju HHTP stog koristi prilikom prosljeđivanja zahtjeva procesima. Tijekom rada ova se komponenta brine za pokretanje novih radnih procesa, gašenje i ponovno pokretanje blokiranih radnih procesa i sl. Programski kod ove komponente izvršava se u korisničkom načinu rada (s ovlastima korisničkog računa *Local System*).
`Inetinfo.exe` komponenta sadrži FTP, SMTP i NNTP poslužitelje, te uslugu za udaljeno administriranje IIS poslužitelja, koja omogućava izmjene postavki poslužitelja putem Interneta (što se svodi na izmjene u *metabase* bazi). Slično kao i kod `inetinfo.exe` komponente, kod se izvršava s ovlastima korisničkog računa *Local System*. Iz sigurnosnih razloga ova komponenta također nikad ne učitava vanjski kod.
Većina postavki IIS poslužitelja pohranjena je u XML bazi, nazvanoj *metabase*. Kako je riječ o datoteci u čistom tekstualnom obliku istu je moguće uređivati bilo kojim tekstualnim editorom, no za to su razvijeni i specijalizirani alati, primjerice *Metabase Explorer* ili *MetaEdit*.
Kako bi se izbjegli problemi sa starijim Web aplikacijama, razvijenima za IIS 5.0 poslužitelj, IIS 6.0 ima dva načina rada koji se nazivaju *Application Isolation Modes*. Prvi način je *Worker process isolation mode*, kod kojeg nova arhitektura IIS programskog paketa dolazi do punog izražaja. Drugi način rada je *IIS 5.0 isolation mode*, namijenjen isključivo starijim Web aplikacijama koje koriste specifičnosti arhitekture ranijih inačica IIS poslužitelja. Proces odgovaranja na zahtjeve kada je IIS 6.0 poslužitelj konfiguriran da radi u ovom načinu rada gotovo je identičan onome kod IIS 5.0 poslužitelja. Osnovna razlika je u tome što u ovakvom načinu rada proces `inetinfo.exe` odgovara na zahtjeve aplikacijama niskog nivoa izoliranosti (IIS 5.0 razlikuje tri nivoa izoliranosti – niski, srednji i visoki), dok na zahtjeve aplikacijama srednjeg i visokog nivoa izoliranosti odgovaraju zasebni procesi, no njihov kod nije sadržan u `w3wp.exe`, već `DLLhost.exe` komponenti. Nadalje, u ovom načinu rada mnoga poboljšanja u sigurnosti, pouzdanosti i performansama ne dolaze do punog izražaja (primjerice, *Application Pool* komponenta za administraciju i nadzor WWW servisa nije aktivna itd.). Ovaj način rada preporuča se samo ukoliko Web aplikacija ili neka njena komponenta ne može raditi u *Worker process isolation* načinu rada.

## 3.2. Inicijalna instalacija

IIS 6.0 programski paket dio je Windows Server 2003 operacijskog sustava. No, u odnosu na IIS 5.0 inačicu, inicijalna instalacija ovog operacijskog sustava ne uključuje i IIS programski paket već ga je potrebno zasebno instalirati. Nadalje, inicijalna instalacija IIS 6.0 programskog paketa uključuje samo statički HTTP poslužitelj. FTP, SMTP, NNTP poslužitelji, moduli za prikaz dinamičkog sadržaja (ASP i ASP.NET moduli), te mnogi drugi dodatni sadržaji moraju se naknadno instalirati. Usporedba inicijalnih instalacija IIS-a 5.0 i IIS-a 6.0 prikazana je u tablici 1.1.
Na ovaj način smanjuje se mogućnost da na poslužitelju budu pokrenuti nepotrebni servisi, čime se znatno umanjuje mogućnost provođenja napada.

| Komponenta IIS poslužitelja | Inicijalna instalacija IIS-a 5.0 | Inicijalna instalacija IIS-a 6.0 |
|---|---|---|
| Statički HTML poslužitelj | Aktivan | Aktivan |
| CGI podrška | Aktivna | Neaktivna |
| ASP podrška | Aktivna | Neaktivna |
| ASP.NET podrška | Ne postoji | Neaktivna |
| Server-side includes podrška | Aktivna | Neaktivna |
| Internet Data Connector podrška | Aktivna | Neaktivna |
| WebDAV | Aktivan | Neaktivan |
| Index Server ISAPI | Aktivan | Neaktivan |
| Internet Printing ISAPI | Aktivan | Neaktivan |
| Microsoft FrontPage® podrška | Aktivna | Neaktivna |
| Background Intelligence Transfer Service | Ne postoji | Neaktivan |
| Sučelje za promjenu zaporke | Aktivno | Neaktivno |
| SMTP poslužitelj | Aktivan | Neaktivan |
| FTP poslužitelj | Aktivan | Neaktivan |

**Tablica 1:** Usporedba inicijalnih instalacije IIS-a

### 3.2.1. Testne skripte

Starija 4.0 inačica IIS programskog paketa uključivala je različite primjere ASP skripti (engl. *sample scripts*), čija je osnovna namjena bila upoznavanje Web programera s osnovnim mogućnostima i karakteristikama ASP jezika. Između ostaloga, u IIS programski paket uključena je i `showcode.asp` skripta (inačice imena: `viewcode.asp`, `codebrws.asp`), koje omogućuje pregledavanje izvornog koda testnih aplikacija na udaljenim računalima. No, osim željene funkcionalnosti, spomenuta skripta sadrži i ozbiljan sigurnosni propust koji potencijalnom napadaču omogućuje pregledavanje bilo koje tekstualne datoteke na poslužitelju, što predstavlja ozbiljan sigurnosni propust. Više informacija o ovom sigurnosnom problemu moguće je pronaći na sljedećim adresama http://www.atstake.com/research/advisories/1999/showcode.txt, http://www.microsoft.com/technet/security/bulletin/ms99-013.mspx.
Kako bi se izbjegli slični problemi i podigla razina sigurnosti poslužitelja, IIS 6.0 programski paket ne uključuje nikakve primjere skripti, pa tako ni mehanizme za njihovo pregledavanje.

### 3.2.2. Virtualni direktoriji bez dozvole izvršavanja

Virtualni direktoriji omogućuju dohvat datoteka koja se nalaze izvan korijenskog (engl. *root*) direktorija Web stranica, ponekad čak i na drugom računalu. Starije inačice IIS poslužitelja prilikom instalacije stvaraju određeni broj virtualnih direktorija, čiji se sadržaj nalazi izvan korijenskog direktorija Web poslužitelja. Kako neki od tih direktorija imaju postavljene ovlasti za izvršavanje (engl. *execute*), iskusan maliciozni korisnik mogao je iskoristiti *directory traversal* ranjivost te ostvariti pristup naredbenom retku sustava (`cmd.exe`). *Directory traversal* je poznata tehnika kojom maliciozni korisnici različitim tehnikama pokušavaju izaći iz inicijalnog direktorija te na taj način ostvariti neautorizirani pristup datotekama sustava. Primjer *directory traversal* napada, priložen je u nastavku:

```
http://www.test.com/primjer.asp?item=../../../../WINNT/win.ini
```

Detaljni opis načina na koji je moguće iskoristiti opisani sigurnosni propust moguće je pronaći na sljedeći adresi http://neworder.box.sk/newsread.php?newsid=8465.
U inicijalnoj instalaciji nove inačice IIS poslužitelja nema virtualnih direktorija s postavljenim ovlastima za izvršavanje, čime se sprječavaju opisani *directory traversal* napadi, napadi podmetanjem koda (engl. *code upload*), te drugi slični napadi na koje su prijašnje inačice IIS programskog paketa bile osjetljive.

### 3.2.3. Onemogućena pod-autentikacija

Mehanizam tzv. pod-autentikacije je u inicijalnoj instalaciji IIS poslužitelja onemogućen. Sva autentikacija obavlja se preko SAM datoteke i *Active Directory* imeničkog servisa. Modul za pod-autentikaciju, `IISSUBA.dll`, nije uklonjen iz inicijalne instalacije Windows 2003 Server operacijskog sustava, tako da je po potrebi moguće naknadno omogućiti pod-autentikaciju.

### 3.2.4. Onemogućen pristup nadređenim direktorijima

Pristup nadređenim direktorijima (engl. *parent path*) inicijalno je onemogućen. Ovakvim pristupom želi se onemogućiti provođenje *directory traversal* napada kojima maliciozni korisnik može doći do datoteka koje se nalaze izvan matičnog direktorija Web site-a (obično se radi o direktoriju `C:\Inetpub\wwwroot`). Ova činjenica, međutim, može uzrokovati probleme prilikom prenošenja Web aplikacija sa starijih inačica IIS poslužitelja.

### 3.2.5. Pridjeljivanje ovlasti

Inicijalno dodjeljivanje ovlasti kod ranijih inačica IIS poslužitelja, u kombinaciji s drugim ranjivostima, omogućavala je malicioznim korisnicima prepisivanje Web sadržaja na poslužitelju, *upload* malicioznih skripti i izvršnih datoteka i sl. Uspješno provođenje opisanih napada napadačima je moglo poslužiti kao podloga za izvršavanje mnogo destruktivnijih napada poput udaljenog izvršavanja naredbi i sl.
Kod 6.0 inačice anonimni korisnici više nemaju ovlasti pisanja u matični direktorij Web poslužitelja. Dodatno, FTP korisnici izolirani su u vlastitim matičnim direktorijima.

## 3.3. Metode autentikacije

Prilikom dohvata podataka koji nisu javno dostupni svim korisnicima, već samo onima koji su prethodno autenticirani, Web poslužitelj mora provjeriti identitet korisnika od kojeg je primio zahtjev. Postupak potvrđivanja identiteta od strane korisnika naziva se autentikacija.
Metode autentikacije ugrađene u novu inačicu IIS poslužitelja ukratko su opisane u nastavku:

- **anonymous authentication** – od korisnika se ne zahtjeva korisničko ime i zaporka;
- **basic authentication** – korisničko ime i zaporka šalju se računalnom mrežom u čistom tekstualnom obliku;
- **digest authentication** – podaci se šalju preko mreže u enkriptiranom obliku, odnosno šalje se njihov MD5 hash niz;
- **advanced digest authentication** – metoda gotovo identična prethodnoj, s tom razlikom da se na domenskom poslužitelju pohranjuje MD5 hash korisničkog imena i zaporke, a ne, kao u prethodnom slučaju, reverzibilno enkriptirani podaci. Ukoliko se koristi ova metoda korisnici se mogu autenticirati isključivo putem *Active Directory* servisa;
- **integrated windows authentication** – za autentikaciju se koristi Kerberos v5 ili NTLM metode autentikacije (u oba slučaja podaci se šalju u enkriptiranom obliku);
- **UNC authentication** – korisnički podaci se prosljeđuju računalu s UNC dijeljenim direktorijom (engl. *Universal Naming Convention share*);
- **.NET password authentication** – posebna metoda autentikacije koja omogućuje korištenje istog korisničkog imena i zaporke za pristup svim Web sadržajima koji podržavaju *.NET Password*;
- **certificate authentication** – autentikacija poslužitelja i klijenata vrši se pomoću SSL (engl. *Secure Socket Layer*) certifikata.

**Anonymous authentication** metoda koristi se za pristupanje javnim Web stranicama. Od korisnika se ne traži unos korisničkog imena i zaporke, već on pristupa podacima s ovlastima anonimnog mrežnog korisnika (inicijalno IUSR_*ImeRacunala* korisnički račun).
**Basic authentication** metoda nudi najnižu razinu sigurnosti, jer se podaci šalju mrežom u Base64 formatu, koji podatke ne zaštićuje enkripcijom. Kodiranje Base64 algoritmom u današnje vrijeme ne predstavlja zadovoljavajuću razinu zaštite te se svakako preporučuje korištenje naprednijih mehanizama autentikacije.

**Digest authentication** metoda koristi se ukoliko je IIS poslužitelj nadograđen na inačicu 6.0 od instalacije starije inačice u kojoj je ova metoda bila omogućena. U svim ostalim slučajevima metoda je onemogućena. Ova metoda zahtjeva da domenski poslužitelj radi na Windows 2000 Server ili Windows 2003 Server platformi. Dodatno, ukoliko je riječ o Windows 2000 Server operacijskom sustavu, potrebno je omogućiti sustav pod-autentikacije.
U slučaju da je na poslužitelju na kojem je pokrenut IIS poslužitelj, kao i na domeskom poslužitelju, instaliran Windows 2003 Server operacijski sustav, umjesto prethodne metode koristi se **Advanced digest authentication** metoda. Ova metoda sigurnija je od prethodne iz dva razloga. Prvo, za njen rad nije potreban sustav pod-autentikacije. Drugo, u *Active Directory* imeniku na domenskom poslužitelju ne pohranjuju se korisničko ime i zaporka u reverzibilno kriptiranom obliku, već njihov *hash* niz iz kojeg nije moguće dešifrirati te podatke.
**Integrated Windows authentication** je inicijalno postavljena metoda autentikacije na Windows 2003 Server operacijskom sustavu. Klijentski program najprije pokušava pristupiti podacima koristeći ovlasti korisnika koji trenutno radi za računalom. Ukoliko ne uspije, od korisnika se traži korisničko ime i odgovarajuća zaporka. Postupak autentikacije vrši se jednom od dvije podržane metode – ukoliko domenski poslužitelj radi na Windows 2000 Server ili Windows 2003 Server platformi, a klijentski program podržava Kerberos v5 protokol, koristi se Kerberos autentikacija; u svim ostalim slučajevima koristi se NTLM autentikacija.
Ukoliko se sadržaj Web site-a ili virtualnog direktorija ne nalazi na samom poslužitelju, nego u dijeljenom direktoriju nekog drugog računala unutar domene, njegova se lokacija zadaje pomoću *UNC (Universal Naming Convetion)* puta. Upravo odatle dolazi i naziv za postupak autentikacije koji se koristi prilikom pristupa spomenutim podacima – *UNC autentikacija*. IIS poslužitelj će od korisnika zatražiti korisničko ime i zaporku (pri čemu korisničko ime mora biti u obliku *Domena/KorisnickoIme*), te će zatim u ime korisnika zatražiti podatke s drugog računala (ovaj postupak naziva se delegacija - engl. *delegation*). Autentikacija na drugom računalu vrši se pomoću neke od ranije opisanih metoda, primjerice *Basic Authentication* ili *Kerberos Authentication* metode.
**.NET Authentication** je autentikacijski model koji omogućava korištenje istih korisničkih podataka za pristup različitim Web sadržajima na različitim poslužiteljima. Korisnički podaci pohranjeni su u kriptiranom zapisu na centralnom *.NET Passport* poslužitelju. Autentikacija korisnika preusmjerava se na odgovarajući poslužitelj, tako da korisnik šalje podatke samo *.NET Passport* poslužitelju, i to putem sigurnog SSL kanala. Nakon uspješne autentikacije, centralni poslužitelj šalje Web poslužitelju korisničko ime i profil (koji ne uključuje zaporku!), u kriptiranom obliku (svaki Web poslužitelj koji podržava *.NET Passport* autentikaciju posjeduje jedinstveni ključ za komunikaciju s centralnim poslužiteljem). Web poslužitelj nakon toga šalje korisniku „kolačić“ koji mu omogućava posjet ostalim stranicama na tom, ali i drugim Web poslužiteljima s *.NET Passport* autentikacijom (Web poslužitelj se također može podesiti tako da ponovo zahtjeva autentikaciju prilikom posjeta nekoj stranici na tom poslužitelju).
Ukoliko je poslužitelj konfiguriran tako da podržava više metoda, prilikom autentikacije IIS će pokušati naći metodu najvišeg stupnja sigurnosti podržanu od strane klijenta i njome provesti postupak.
Za pristup FTP resursima koriste se samo dvije metode autentikacije, i to *Anonymous FTP Authentication* i *Basic FTP Authentication*. Obje metode su u potpunosti identične istoimenim metodama koje se koriste za pristup Web stranicama.

## 3.4. Provjera ulaznih podataka

Jedna od najvećih promjena kod nove inačice IIS poslužitelja je tzv. HTTP stog (*HTTP protocol stack*). Riječ je o upravljačkom programu pod nazivom `HTTP.sys`, dijelu jezgre operacijskog sustava (engl. *kernel-mode device driver*) koji prima, obrađuje te dalje prosljeđuje HTTP zahtjeve klijenata. Zadatak je ovog programa da djeluje kao posrednik (engl. *gateway*) između klijenata i Web aplikacija, preko kojeg će se kontrolirati izvršavanje svih korisničkih zahtjeva. Osim poboljšanja performansi poslužitelja, ovakav način zaprimanja zahtjeva trebao bi smanjiti mogućnost provođenja brojnih napada usmjerenih prema Web aplikacijama.
`HTTP.sys` je proces sa sistemskim ovlastima čiji je zadatak da prima klijentske zahtjeve, provjerava njihovu ispravnost te da ih prosljeđuje odgovornim procesima (aplikacijama) koji će obraditi zahtjev

te vratiti zatražene podatke klijentu. Ti procesi oblikuju odgovore (što uključuje dohvaćanje podataka, interpretiranje koda Web aplikacija, i sl.) te ih vraćaju `HTTP.sys`-modulu koji ih prosljeđuje korisniku.
Neki od sigurnosnih mehanizama ugrađenih u `HTTP.sys` modul jesu zaštita od prepisivanja spremnika (engl. *buffer overflow protection*), napredno bilježenje log zapisa, te URL parser koji provjerava ispravnost zahtjeva i sl. Rad URL parsera moguće je podešavati preko vrijednosti ključeva u *Windows Registry* datoteci prikazanih u sljedećoj tablici.

| Ime ključa | Inicijalna vrijednost | Dopuštene vrijednosti | Značenje ključa |
|---|---|---|---|
| AllowRestrictedChars | 0 | Boolean | Ako vrijednost ključa nije 0, `HTTP.sys` prihvaća URL adrese koje sadrže heksadecimalno kodirane dopuštene znakove. |
| EnableNonUTF8 | 1 | Boolean | Ako je vrijednost ključa 0, `HTTP.sys` prihvaća samo UTF-8 kodirane URL adrese. |
| FavorUTF8 | 1 | Boolean | Ako vrijednost ključa nije 0, `HTTP.sys` prvo pokušava dekodirati URL kao UTF-8 kodirani URL. Inače, prvo pokušava URL dekodirati kao ANSI ili DBCS kodirani URL. |
| MaxConnections | MAX_ULONG | 1024(1k) – 2031616 (2MB) | Najveći dopušteni broj istovremenih veza. |
| MaxEndpoints | 0 | 0 - 1024 | Broj dozvoljenih *end point* objekata. Ako je vrijednost ključa 0, broj se određuje u ovisnosti o raspoloživoj memoriji. |
| MaxFieldLength | 16384 (byte-ova) | 64 – 65534 (64k - 2) | Najveća dopuštena veličina jednog zaglavlja (*header*). |
| MaxRequestBytes | 16384 (byte-ova) | 256 – 16777216 (16MB) | Najveća dopuštena veličina linije sa zahtjevom i svih zaglavlja zajedno. |
| PercentUAllowed | 1 | Boolean | Ako vrijednost ključa nije 0, `Http.sys` prihvaća %*uNNNN* notaciju u URL adresama. |
| UrlSegmentMaxCount | 255 (segmenata) | 0 - 16,383 | Najveći dopušteni broj segmenata URL adrese. Ako je vrijednost ključa 0, broj dopuštenih vrijednosti jednak je maksimalnoj vrijednosti ULONG tipa podatka. |
| UriEnableCache | 1 | Boolean | Ako vrijednost ključa nije 0, omogućen je *cache* za odgovore i fragmente (*response and fragment cache*). |
| UriMaxUriBytes | 262144 (byte-ova) | 4096(4k) – 16777216(16MB) | Najveća dopuštena veličina odgovora koji se smije spremiti u *cache* (*kernel response cache*). |
| UriScavengerPeriod | 120 (sekundi) | 10 - 0xFFFFFFFF | Zahtjevi i fragmenti kojima se nije pristupalo UriScavengerPeriod sekundi brišu se iz *cache*-a. |
| UrlSegmentMaxLength | 260 (znakova) | 0 - 32,766 | Najveći dopušteni broj znakova u URL segmentu. Ako je vrijednost ključa 0, broj dopuštenih znakova jednak je maksimalnoj vrijednosti ULONG tipa |

| | | | |
|---|---|---|---|
| | | | podatka. |

**Tablica 2:** Ključevi u Windows Registry datoteci kojima se podešava rad HTTP parsera

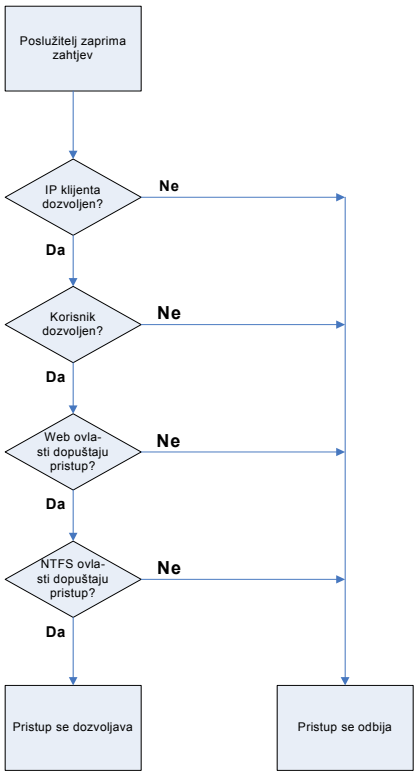
## 3.5. Provjera pristupa datotekama

Tri su osnovna mehanizma kontrole pristupa (engl. *access control*) koja se koriste u IIS programskom paketu. To su:

- **NTFS ovlasti** (engl. *NTFS permissions*) - pristup datotekama i direktorijima ograničava se na razini korisnika i korisničkih grupa;
- **Web ovlasti** (engl. *Web site permissions*) - pristup datotekama i direktorijima putem Weba ograničava se također na razini korisnika i korisničkih grupa;
- **Ograničavanje IP adresa** (engl. *IP address restrictions*) - pristup datotekama i direktorijima moguće je dozvoliti ili zabraniti na razini računala, grupe računala ili domene.

Provjeru NTFS ovlasti vrši sam operacijski sustav, dok provjeru Web ovlasti i provjeru IP adrese vrši IIS poslužitelj.
Provjera pristupa datoteci vrši se u sljedećih 8 koraka:

1. Klijent zahtjeva pristup resursu na poslužitelju;
2. Provjerava se IP adresa klijenta. Ukoliko je unutar IIS poslužitelja zabranjen pristup s te adrese, zahtjev se odbija (poruka o grešci „**403 Access Forbidden**“);
3. Poslužitelj, ukoliko je tako konfiguriran, zahtjeva autentikaciju od strane klijenta. Klijent prosljeđuje korisničko ime i zaporku;
4. IIS poslužitelj provjerava ima li korisnik važeći korisnički račun unutar Windows operacijskog sustava. Ukoliko nema, zahtjev se odbija (poruka o grešci „**401 Access is denied**“);
5. IIS poslužitelj provjerava ima li korisnik dovoljne Web ovlasti. Ukoliko nema, zahtjev se odbija (poruka o grešci „**403 Access Forbidden**“);
6. U postupak provjere uključuju se eventualni dodatni moduli (kao, na primjer, *ASP.NET impersonation*);
7. Provjeravaju se NTFS ovlasti korisnika za statičke datoteke, ASP skripte i CGI datoteke. Ukoliko korisnik nema ovlasti za pristup resursu, zahtjev se odbija (poruka o grešci „**401 Access is denied**“);
8. Ukoliko korisnik ima sve potrebne ovlasti poslužitelj odgovara na zahtjev.




**Slika 2:** Provjera pristupa datotekama

## 3.6. Bilježenje događaja

S ciljem što jednostavnijeg praćenja rada poslužitelja i što bržeg, odnosno efikasnijeg otkrivanja neovlaštenih aktivnosti, u sklopu nove inačice IIS poslužitelja razvijen je prošireni i pouzdaniji mehanizam bilježenja događaja (engl. *logging*). U odnosu na 5.0 inačicu, gdje je za bilježenje log zapisa bio zadužen glavni `inetinfo.exe` proces, kod inačice 6.0 ovaj je zadatak prepušten `HTTP.sys` modulu, koji podatke u log datoteku zapisuje prije nego što zaprimljeni zahtjev proslijedi procesu koji će ga obraditi. Na taj se način osigurava da odgovarajući log zapis postoji čak i u slučaju da proces prilikom obrade zahtjeva nasilno prekine sa radom (engl. *crash*).
Zapis u log datoteci sastoji se od datuma i vremena događaja, mrežnog porta, izvorišne i odredišne IP adrese, verzije protokola i mnogo drugih podataka koji mogu poslužiti pri određivanju uzroka pogreške. Poseban dio zapisa je i tzv. *HTTP.sys Reason Phrase* u kojem su navedene detaljne informacije o tome zašto je do pogreške došlo.
U nastavku je priložen primjer kog zapisa iz `htperr.log` datoteke, generiranog od strane IIS 6.0 poslužitelja (zapis je zbog svoje dužine razlomljen u nekoliko redaka):

```
2004-12-09  12:45:22  161.53.64.145  40045  161.53.64.240  80  HTTP/1.0
GET /msadc/msadcs.dll 400 - BadRequest
```

Značenje pojedinih polja je sljedeće:

| Vrijednost | Značenje |
|---|---|
| `2004-12-09` | Datum upita |
| `12:45:22` | Vrijeme upita |
| `161.53.64.145` | IP adresa s koje je upit iniciran |
| `40045` | Izvorišni TCP port |
| `161.53.64.240` | Odredišna IP adresa |

| | |
|---|---|
| `80` | Odredišni port |
| `HTTP/1.0` | Verzija protokola |
| `GET /msadc/msadcs.dll` | Upit |
| `400 - BadRequest` | Odgovor poslužitelja |

## 3.7. Pouzdanost IIS 6.0 poslužitelja

### 3.7.1. Izolacija aplikacija

IIS 6.0 poslužitelja omogućuje administratorima grupiranje Web aplikacija, Web site-ova, direktorija i virtualnih direktorija u grupe nazvane *application pool.* Svakoj od tih grupa pridjeljuje se vlastiti poslužiteljski proces koji je zadužen za odgovaranje na zahtjeve usmjerene aplikacijama iz te grupe. Ovakvom raspodjelom zahtjeva među procesima, osigurano je da problemi u radu jedne skupine aplikacija ne utječe na rad ostalih (engl. *application isolation*).

Ovakav pristup nije bio primjenjiv kod ranijih inačica IIS poslužitelja zbog degradiranja sveukupnih performansi poslužitelja. Novi dizajn i povećana efikasnost IIS 6.0 poslužitelja omogućili su da podjela na grupe aplikacija i njihova međusobna izolacija ne utječe bitno na performanse sustava u cjelini.

Poslužiteljski procesi nemaju sistemske ovlasti kao `HTTP.sys` modul, već isključivo korisničke ovlasti. Na taj se način smanjuje mogućnost da maliciozni korisnik ostvari pristup jezgri operacijskog sustava što bi omogućilo preuzimanje potpune kontrole nad sustavom.

### 3.7.2. Rapid-fail zaštita

IIS 6.0 poslužitelj omogućuje podešavanje programa tako da zaustavlja ili ponovno pokreće procese koji više puta (zadani broj puta u zadanom vremenu) nisu uspjeli odgovoriti na korisničke zahtjeve. Budući da učestali neuspjesi u izvršavanju neke Web aplikacije mogu biti indikacija napada (prvenstveno tzv. *Denial of Service* napada) na sustav, ovakvim se pristupom u određenoj mjeri može preventivno djelovati na njihovo provođenje.

### 3.7.3. Poštivanje principa minimalnih ovlasti

Između ostalih svojstava, IIS 6.0 poslužitelj također je dizajniran tako da zadovoljava jedan od temeljnih principa računalne sigurnosti – princip minimalnih ovlasti (engl. *least privilege*). Prema ovome načelu svakom programu, odnosno servisu pridjeljuje se najmanja razina ovlasti koja je potrebna za izvršavanje pojedinih zadataka. Kod IIS 6.0 poslužitelja to je postignuto razdvajanjem programskog koda koji zahtjeva najniže sistemske ovlasti (ovlasti korisničkog računa *Local System*) od koda koji se pokreće s korisničkim ovlastima (ovlastima različitih korisničkih računa kao što su *Local Service*, *Network Service* i sl.). Sistemske ovlasti ima programski kod koji se izvršava unutar `lsass.exe`, `inetinfo.exe` i `svchost.exe` komponenti, dok radni procesi posjeduju ovlasti spomenutih korisničkih računa (moguće je poslužitelj konfigurirati i tako da radni procesi unutar nekog *application pool*-a koriste sistemske ovlasti, no to nije preporučljivo). Poseban slučaj je `HHTP.sys` modul, koji osim što se izvršava sa sistemskim ovlastima, radi na razini jezgre operacijskog sustava (engl. *kernel mode*). Dodatno, inačica 6.0 IIS poslužitelja samo administratoru dozvoljava izvršavanje komandno linijskih programa, čime se dodatno podiže razine zaštite od različitih malicioznih programa koji za svoje širenje koriste sistemske alate koji se pokreću putem naredbenog retka. Također valja napomenuti da anonimni korisnici više nemaju ovlasti pisanja u matični direktorij Web poslužitelja, a FTP korisnici izoliraju se u vlastite home direktorije.

# 4. Zaključak

Na temelju provedenih analiza i testiranja može se zaključiti kako je Microsoft objavom 6.0 inačice IIS poslužitelja napravio veliki pomak u smislu sigurnosti svojih proizvoda. Program je većim dijelom iznova napisan, pri čemu se ozbiljno vodilo računa o osnovnim načelima računalne sigurnosti i sigurnosnim kontrolama koje bi trebale podići razinu sigurnosti poslužitelja. Očiti zaokret napravljen je u inicijalnim sigurnosnim postavkama poslužitelja, čime se znatno podiže sigurnost sustava nakon inicijalne instalacije. Bitno je naglasiti i značajne promjene u arhitekturi sustava te načinu bilježenja log zapisa koji omogućuju nadzor i praćenje rada sustava.
Dokument opisuje osnovne karakteristike IIS 6.0 poslužitelja, promjene u odnosu na ranije inačice te osnovna svojstva značajna sa stanovišta sigurnosti.

## 5. Reference

[1] Microsoft, http://www.microsoft.com/resources/documentation/IIS/6/all/techref/en-us/default.mspx
[2] ServerWatch, http://www.serverwatch.com/tutorials/article.php/3294371
[3] SecurityFocus, http://www.securityfocus.com/infocus/1765
[4] Windowsitlibrary, http://www.windowsitlibrary.com/Content/435/11/1.html
[5] InformIT, http://www.informit.com/articles/article.asp?p=101750&seqNum=6