HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Autentikacija korisnika na Windows sustavima

CCERT-PUBDOC-2004-10-95

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

Osnovni pojmovi kao što su identifikacija, autentikacija, autorizacija, zaštita i praćenje rada (eng. *accounting*) i sl., koji su usko vezani uz proces prijave i rada na sustavu, ponekad se pogrešno interpretiraju.

Pojam identifikacije označava predstavljanje korisnika, odnosno predstavljanje identiteta korisnika sustavu. Prilikom uobičajene prijave za rad na sustavu korištenjem korisničkog imena i zaporke, identifikacijom se podrazumijeva unošenje korisničkog imena. U drugim sustavima, identifikacija se može provoditi i na druge načine. Npr. u sustavima gdje se implementira fizička kontrola identifikacija se može provoditi korištenjem identifikacijskih kartica ili biometrijskih (otisak prsta, uzorak zjenice i sl.) podataka.

Autentikacija podrazumijeva potvrdu predstavljenog identiteta. Generalno, autentikacija se provodi korištenjem jedne ili više od idućih značajki:

- nešto što osoba zna,
- nešto što osoba posjeduje ili
- nešto što osoba jest.

Na računalnim sustavima, tradicionalno se koristi prva značajka, odnosno autentikacija korisnika se provodi unošenjem zaporke (nešto što osoba zna). Prilikom identifikacije sustavu (npr. kod POS uređaja ili bankomata, ali i računalnih sustava) korištenjem magnetskih ili pametnih kartica uobičajeno se provodi i dvostruka autentikacija: onim što osoba posjeduje (kartica) i onim što osoba zna (PIN).

Pojam autorizacije predstavlja ovlasti korisnika na sustavu nakon što je isti uspješno identificiran te autenticiran. Npr. na Windows sustavima autorizacija se implementira korištenjem ACL (eng. *access control list*) pristupnih lista koje su vezane uz svaku pojedinu datoteku na sustavu, i u kojima su definirana prava pristupa (dozvola ili zabrana) i načini pristupa (čitanje, pisanje, promjena itd.) za pojedine korisnike i/ili grupe (diskreciona prava pristupa).

Konačno, nadzor i praćenje rada podrazumijeva mogućnosti jednoznačnog praćenja svih aktivnosti koje korisnik provodi za vrijeme dok je prijavljen u sustav. Na računalnim sustavima praćenje rada tipično se implementira bilježenjem aktivnosti (eng. *logging*) korisnika u posebne log datoteke.

Ovaj dokument bavit će se isključivo metodama autentikacije na Windows operacijskim sustavima (LM, NTLM i Kerberos). U nastavku će biti detaljno opisane različite autentikacijske sheme koje Windows bazirani sustavi podržavaju, te načini i mogućnosti autentikacije u heterogenim Windows okruženjima gdje se koriste različiti operacijski sustavi, od Windows 95 sve do Windows Server 2003 sustava. U dokumentu će biti opisane isključivo standardne autentikacijske metode koje se baziraju na prijavi za rad korištenjem korisničkog imena i zaporke.

2. Osnovni pojmovi

Na Windows operacijskim sustavima, svaki korisnik ili računalo predstavljaju tzv. sigurnosne principale. Sigurnosni principali su ti koji mogu pristupati objektima kao što su datoteke i mape. Općenito, korisnički računi mogu biti lokalni ili domenski. Lokalni korisnički računi pohranjeni su u SAM (eng. *security accounts manager*) bazi koja se nalazi na lokalnom disku radne stanice ili poslužitelja. Kod Windows NT domena, korisnički računi su također pohranjeni unutar SAM baze, koja se nalazi na svim DC (eng. *domain controller*) poslužitelja unutar domene. Jedina SAM baza u koju je dozvoljeno pisanje nalazi se na PDC (eng. *primary domain controller*) poslužitelju, dok je na ostalim, BDC (eng. *backup domain controller*) poslužiteljima, gdje se nalaze sinkronizirane kopije, moguće isključivo čitanje iz SAM baze.
Kod *Active Directory* sheme na Windows 2000 i Windows 2003 sustavima korisnički računi više se ne pohranjuju unutar SAM baze, već su dio *Active Directory* strukture. Također, unutar *Active Directory* organizacije, gubi se podjela na PDC i BDC domenske poslužitelje, tako da na svim DC poslužiteljima neovisno postoji mogućnost promjena na korisničkim računima koje se onda međusobno sinkroniziraju *Active Directory* replikacijom među DC poslužiteljima.

2.1. SID

Korisnik se identificira korištenjem svog korisničkog imena. Na NT sustavima korisničko ime bilo je oblika: `računalo\korisnik` ili `domena\korisnik` (npr. `test\pperic`), dok Windows 2000 i noviji sustavi koriste tzv. UPN (eng. *user principal name*) konvenciju formata `korisnik@domena` (npr. `pperic@test.ad`).
SID, odnosno sigurnosni identifikator predstavlja internu reprezentaciju korisničkog imena odnosno UPN imena na temelju koje operacijski sustav identificira pojedinog korisnika. SID je oblika S-R-A-P-P i sastoji od nekoliko komponenata:

- revizije (R),
- identifikatora autoriteta (A),
- identifikatora podautoriteta (P).

Revizija označava inačicu SID strukture koja se koristi (na dosadašnjim Windows sustavima koristi se revizija 1). Identifikator autoriteta duljine je 48 bita i označava autoritet. U tablici (*Tablica 1*) prikazan je popis postojećih identifikatora autoriteta.

Identifikator autoriteta	Oznaka
Null	S-1-0
World	S-1-1
Local	S-1-2
Creator	S-1-3
Non-unique	S-1-4
NT	S-1-5

Tablica 1: Postojeći identifikatori autoriteta

Identifikatora podautoriteta, odnosno relativnih identifikatora – RID (eng. *relative ID*) duljine 32 bita može biti nekoliko i oni jedinstveno označavaju korisnika ili grupu u odnosu na određeni autoritet. Tablice (*Tablica 2* i *Tablica 3*) daje prikaz postojećih univerzalnih SID-ova.

SID	Oznaka
Null	S-1-0-0
World	S-1-1-0
Local	S-1-2-0
Creator Owner	S-1-3-0
Creator Group	S-1-3-1
Creator Owner Server	S-1-3-2
Creator Group Server	S-1-3-3
Non-unique	S-1-4

Tablica 2: Postojeći univerzalni SID-ovi

SID	Oznaka
Dialup	S-1-5-1
Network	S-1-5-2
Batch	S-1-5-3
Interactive	S-1-5-4
Logon Session	S-1-5-5-X-Y
Service	S-1-5-6
Anonymous	S-1-5-7
Proxy	S-1-5-8
Enterprise Domain Controllers	S-1-5-9
Self	S-1-5-10
Authenticated Users	S-1-5-11
Restricted Code	S-1-5-12
Terminal Server Users	S-1-5-13
Local System	S-1-5-18
NT Authority (Local Service)	S-1-5-19
NT Authority (Network Service)	S-1-5-20
Administrators	S-1-5-32-544
Users	S-1-5-32-545
Guests	S-1-5-32-546
Power Users	S-1-5-32-547
Account Operators	S-1-5-32-548
System Operators	S-1-5-32-549
Print Operators	S-1-5-32-550
Backup Operators	S-1-5-32-551
Replicator	S-1-5-32-552

Tablica 3: Neki NT relativni SID-ovi

Postoje i poznati NT domenski SID-ovi s RID-ovima koji definiraju ugrađene domenske grupe (*Tablica 4*).

SID	Oznaka
Administrator	S-1-5-domain-500
Guest	S-1-5-domain-501
KRBTGT	S-1-5-domain-502
Domain Admins	S-1-5-domain-512
Domain Users	S-1-5-domain-513
Domain Guests	S-1-5-domain-514
Domain Computers	S-1-5-domain-515
Domain Controllers	S-1-5-domain-516
Cert Publishers	S-1-5-domain-517
Schema Admins	S-1-5-root domain-518
Enterprise Admins	S-1-5-root domain-519
Group Policy Creator Owners	S-1-5-domain-520
RAS and IAS Servers	S-1-5-domain-533

Tablica 4: Neki NT domenski SID-ovi

Kompletan popis poznatih SID-ova dostupan je na Microsoftovim Web stranicama:
http://support.microsoft.com/default.aspx?scid=kb;EN-US;Q243330
Korisnicima i grupama na domeni (ili računalu) generiraju se jedinstveni SID-ovi, kod kojih korisnički, odnosno grupni RID počinju od broja 1000 na više. Tipičan primjer korisničke SID oznake izgleda ovako:

```
S-1-5-21-1952333102-9715652321-115325518-1003
```

Pri tome `S-1-5` označava NT autoritet, `21-1952333102-9715652321-115325518` je jedinstvena oznaka domene (računala), a `1003` je jedinstvena oznaka korisnika (grupe). Ovako generirana SID oznaka mora jednoznačno identificirati korisnika, grupu ili računalo na domeni.

2.2. SAM baza

Kako je ranije rečeno, SAM baza pohranjuje korisničke podatke na računalima i poslužiteljima (NT, 2000, XP) koji nisu domenski poslužitelji unutar *Active Directory* strukture. SAM baza se nalazi u *registry* datoteci (`HKEY_LOCAL_MACHINE\SAM`), odnosno fizički na disku kao `%WINDIR%\system32\config\SAM`. U njoj se nalaze podaci koji služe prilikom autentikacije korisnika (korisničko ime, *hash* vrijednosti zaporke).
U ranijim inačicama NT sustava (prije NT 4 SP 3) SAM baza predefinirano nije bila zaštićena, već su podaci bili pohranjeni u otvorenom tekstu (engl. *plain text*) Novije inačice šifriraju SAM bazu korištenjem RC4 algoritma, a ključ za šifriranje može biti pohranjen lokalno, na drugom mediju ili se može generirati iz posebno definirane zaporke. Više informacija o zaštiti SAM baze može se pronaći u dokumentu "Prednosti i nedostaci uporabe Syskey alata, CCERT-PUBDOC-2003-12-53", http://www.cert.hr.
Slika 1 prikazuje tipičan izgled lokalne SAM baze. U zapisu je moguće uočiti korisničko ime, RID korisnika, te LM i NTLM *hash* vrijednosti korisničkih zaporki.

```
Administrator:500:7853634c59943a40aad3b435b51404ee:961493c34f0d6581e9acfbb8ba2090a2:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b83c59d7e0c089c0:::
HelpAssistant:1000:f1274813f856e06eccbf067040fbee7d:ffb88fb18a1b2f339bd5ec7fd174d4b9:::
Hrvoje:1003:aad32435b51403eeaad3b435b51404ee:31d6cfe0d16ae9f1b73c59d7e0c089c0:::
pperic:1004:1ac14ad86dc275e5aad3b435b51404ee:9633e5b2d68b633f71edb6b997844b0d:::
SUPPORT_388945a0:1002:aad0b435b51404eeaad3b435b51404ee:5ebed211f3ecb7e59ab073db134aa86e:::
```

Slika 1: Tipičan izgled SAM baze

2.3. *Active Directory*

Kod Windows 2000 Server i Server 2003 domenskih poslužitelja podaci o principalima pohranjuju se kao objekti. Svaki objekt sastoji se od skupa atributa, među kojima se nalaze i korisnička imena, SID-ovi, *hash* vrijednosti zaporki itd.
Fizičkom pohranom tih podataka upravlja DSA (eng. *directory system agent*) agent, koji je dio LSA podsistema na DC poslužitelju. Klijentima nije omogućen izravan pristup podacima, već isključivo kroz ADSI (eng. *Active Directory service interface*) sučelje prema DSA agentu. Objekti unutar *Active Directory*-ja zaštićeni su ACL listama, a za osjetljive atribute mogu se postaviti i još restriktivnija prava pristupa. Obzirom da je zaporka, odnosno njena *hash* vrijednost najvažniji dio korisničkog računa, unutar *Active Directory*-ja ona se dodatno štiti korištenjem Syskey-a.

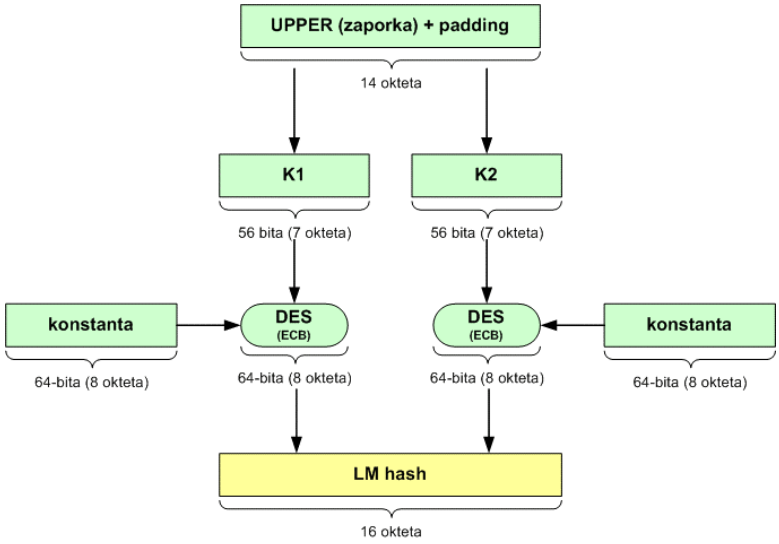
2.4. Pohrana zaporke

Na Windows sustavima zaporka se pohranjuje u obliku *hash* vrijednosti koja se koristi za provjeru prilikom autentikacije korisnika. Postoje dvije funkcije koje Windows sustavi koriste za generiranje *hash* vrijednosti zaporke: LM i NTLM. Kako će u nastavku biti pojašnjeno, način pohrane *hash* vrijednosti usko je povezan i s metodama autentikacije na Windows sustavima, no isto tako ne treba miješati način pohrane zaporke i način autentikacije, iako se pri tome koriste isti ili slični termini.

2.4.1. LM hash

LM *hash*, odnosno LAN Manager vezan je uz LAN Manager postupak autentikacije koji su koristili stariji klijenti (Windows 9x i raniji). Duljina zaporki na sustavima koji koriste LM ograničena je na 14 znakova (OEM skup).
Na sustavu se zaporka pohranjuje tako da se koristi tzv. LM OWF (eng. *one way function*) jednosmjerna funkcija. OWF generira *hash* vrijednost iz zaporke u sljedećim koracima (*Slika 2*):
1. Korisnička zaporka se modificira tako da su sva slova velika (eng. *uppercase*).

2. Niz od 14 znakova dobiven ispunom (za ispunu se koristi vrijednost 0x00) ili skraćivanjem (ukoliko je zaporka dulja od 14 znakova) se dijeli na dva bloka od 7 znakova.
3. Iz svakog od ta dva bloka generira se po jedan 56-bitni DES ključ kojima se zatim šifrira konstantni niz "KGS!@#$%" (nije poznato iz kojih razloga je odabrana baš ta vrijednost) duljine 8 okteta (što odgovara ulaznom bloku DES algoritma).
4. Dva bloka dobivena DES šifriranjem spajaju se u 16-oktetnu *hash* vrijednost.

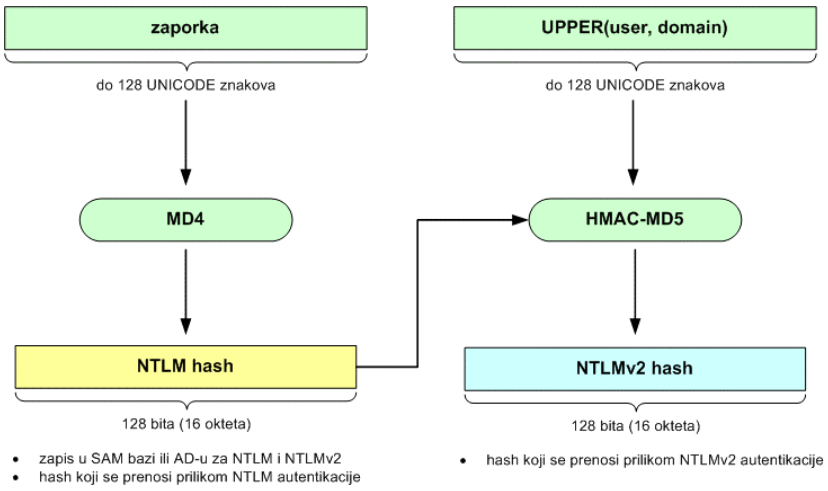


Slika 2: Generiranje LM hash vrijednosti

LM *hash* nije Microsoftovo vlastito rješenje već je algoritam preuzet od IBM-a koji ga je tijekom 70-ih godina 20-og stoljeća koristio na IBM IBM 360/370 sustavima. Obzirom na slabosti DES algoritma (DES Algoritam, CCERT-PUBDOC-2003-06-24, http://www.cert.hr) i na činjenicu da je inicijalni prostor DES ključeva sužen na isključivo velika slova i, u najvećem broju slučajeva, na tzv. *printable* znakove te da se u slučaju prekratkog niza znakova koristi ispuna *null* znakovima, sasvim je jasno da je ovakav način generiranja *hash* vrijednosti u današnje vrijeme neprikladan.
Bilo koji *password cracker* alat razbit će većinu zaporki u LM *hash* obliku u svega nekoliko sekundi ili minuta (najpoznatiji takav alat je L0phtCrack).

2.4.2. NTLM i NTLMv2 hash

NTLM, odnosno NT LAN Manager pojavio se s NT sustavima. Sa sigurnosnog stajališta generiranje NTLM *hash* vrijednosti sigurnije je od LM *hasha* iz više razloga. Kao prvo, maksimalni broj znakova za zaporku povećan je na 128 znakova u UNICODE formatu te ne postoje nikakva ograničenja na skup znakova. Kao jednosmjerna OWF funkcija koristi se MD4 (http://www.ietf.org/rfc/rfc1320) koja na temelju varijabilnog ulaznog niza (ne koristi se proizvoljna ispuna, već je ona sastavni dio MD4 algoritma) kao izlaz daje 128-bitni (16 oktetni) niz.
Od Windows NT 4.0 SP4 postoji i NTLMv2 autentikacija, koja pruža dodatnu sigurnost. *Hash* vrijednost koja je pohranjena u SAM bazi, odnosno *Active Directory*-ju i dalje je identična kao kod NTLM-a, no pri samoj autentikaciji se koristi dodatna zaštita korištenjem MD5 *hash* funkcije s autentikacijskim kodom HMAC-MD5 (http://www.ietf.org/rfc/rfc2104) koja kao ulazne parametre koristi korisničko ime i domenu (u formatu velikih slova), dok se kao ključ koristi 16-oktetna NTLM *hash* vrijednost. Više riječi o NTLMv2 autentikacijskom protokolu biti će u nastavku dokumenta.



Slika 3: NTLM i NTLMv2 hash

Valja napomenuti da je na NT 4.0 i starijim NT klijentima zbog ograničenja korisničkog sučelja broj znakova zaporke i dalje bio ograničen na 14 znakova, no s Windows 2000 sustavima taj propust je ispravljen.

2.4.3. Kompatibilnost

Zbog kompatibilnosti unazad, i novi sustavi u SAM bazu (ako se radi o NT domenama, NT/2000/XP radnim stanicama ili NT/2000/2003 *standalone* poslužiteljima) odnosno u *Active Directory* zapisuju obje, LM i NTLM, *hash* vrijednosti, što te baze čini ranjivim na *offline* napade (ukoliko napadač na neki način dođe do SAM baza ili *Active Directory* podataka). Postoji nekoliko načina da se onemogući pohranjivanje LM *hash* vrijednosti, čime se naravno gubi kompatibilnost unazad.

1. Prvi način je da korisnik odabere zaporku dulju od 14 znakova (na sustavima koji podržavaju unos takve zaporke) ili koristi znakove koji nisu dio OEM skupa. U tom slučaju LM *hash* se uopće neće generirati.
2. Na Windows 2000 i novijim sustavima je moguće je i:
   a. definiranje *Group Policy* politike:
      Network security: Do not store LAN Manager hash value on next password change unutar *Computer Configuration, Windows Settings, Security Settings, Local Policies, Security Options* grane *Group Policy* objekta (lokalnog ili unutar *Active Directory*ja),
   b. podešavanje *registry* REG_DWORD vrijednosti NoLMHash na veličinu 1 unutar `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa` ključa.

   Oba ova postupka uklanjaju LM *hash* vrijednost tek prilikom sljedeće promjene zaporke.

Ukoliko se ukloni LM *hash*, niz autentikacija klijenata koji ne podržavaju NTLM više nije moguća (Win 3.x i Windows 9x bez *Active Directory client extension* komponente).

3. Windows autentikacija

3.1. Prijava za rad

Prijava za rad (eng. *logon*) je proces u kojem se korisnik (može biti i servis ili računalo) autenticira sustavu. Windows sustavi podržavaju nekoliko načina prijave za rad:

– Interaktivna prijava (eng. *interactive logon*) – korisnička prijava na računalo gdje korisnik ima direktan pristup. Interaktivna prijava može biti lokalna ili udaljena (korištenje *Remote Desktop* ili *Terminal Services* rada na udaljenim računalima). Korisnik se interaktivno može autenticirati na lokalnom računalu ili domenski. Autentikacija korištenjem pametnih kartica (eng. *smart cards*) također predstavlja interaktivnu prijavu.

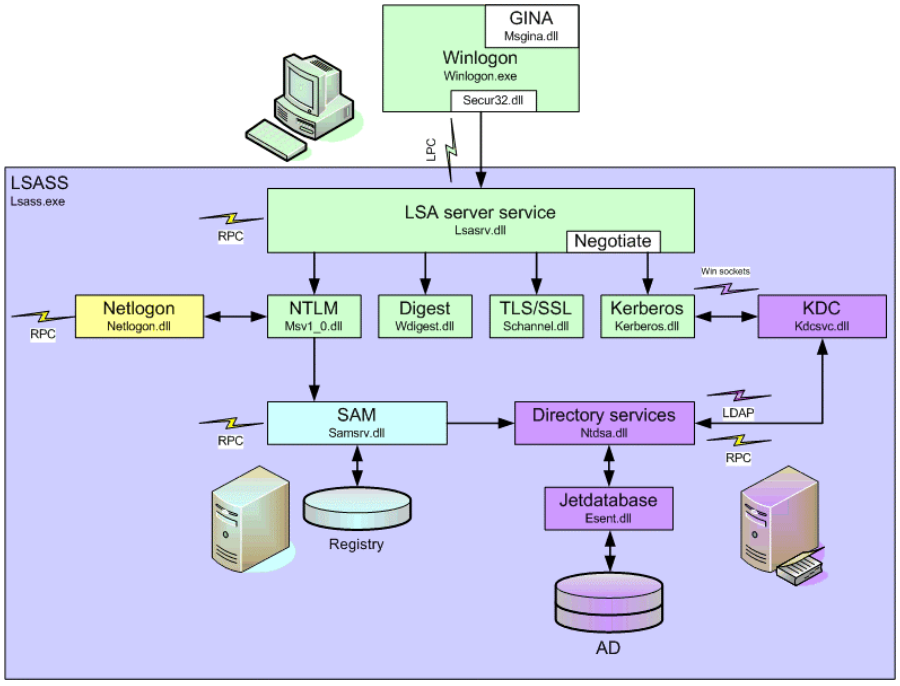
- Mrežna prijava (eng. *network logon*) – pristup NT baziranom sustavu s računala na koje je korisnik prijavljen, a temelji se na korištenju onih ovlasti koje je korisnik dobio prilikom interaktivne prijave, ili ovlasti koje imaju servisi ili računala koja pokušavaju ostvariti mrežnu prijavu.
- *Service logon* – prijava za rad servisa prilikom pokretanja sustava koja se odvija korištenjem *LocalSystem* ili nekog drugog lokalnog ili domenskog korisničkog računa (u tom slučaju servis ima mogućnost pristupa mrežnim resursima).
- *Batch logon* – ova vrsta prijave za rad rijetko se koristi i obično je rezervirana za aplikacije koje se pokreću kao *batch* procesi. Korisnički račun koji se koristi za ovu prijavu mora imati *logon as a batch job* ovlasti.

Osim spomenutih načina prijave, na Windows operacijskim sustavima prije 2000, postoje još neki načini, no njihov opis nije cilj ovog dokumenta.

3.2. LSA

LSA podsistem (eng. *local security authority*), odnosno LSASS (eng. *local security authority security subsystem*) zadužen je za kompletno upravljanje sigurnošću unutar Windows sustava što podrazumijeva autentikaciju, autorizaciju, bilježenje, generiranje sigurnosnih tokena, sigurnosnu politiku itd.

LSA se pokreće kao servis (`lsass.exe`) prilikom pokretanja Windows sustava i nije ga moguće pauzirati niti zaustaviti. Sustav se sastoji od više komponenti koje međusobno komuniciraju korištenjem LPC i RPC poziva, LDAP protokolom te korištenjem Windows socket-a (*Slika 4*).



Slika 4: LSA sigurnosni podsistem

Tablica 1 opisuje osnovnu funkcionalnost komponenti LSA sigurnosnog podsistema. Neke komponente nalaze se samo unutar LSA podsistema *Active Directory* poslužitelja (KDC, *Directory Services* i AD baza). Također, stariji NT sustavi ne implementiraju sve autentikacijske pakete (npr. Kerberos) prikazane na slici i opisane u tablici.

Komponenta	Opis
`Winlogon.exe`	izvršna datoteka zadužena za sigurnu interaktivnu prijavu korisnika na NT/2000/XP/2003 sustavima
`Msgina.dll`	dinamička biblioteka za grafičku identifikaciju i autentikaciju korisnika

Komponenta	Opis
`Netlogon.dll`	dinamička biblioteka koja pruža više usluga: – održavanje sigurnog kanala između klijenta i autentikacijskog poslužitelja i prijenos informacija kroz taj kanal – objavu DNS SRV zapisa na Windows Server 2000 i 2003 sustavima – RPC sinkronizaciju PDC i BDC NT poslužitelja
`Msv1_0.dll`	NTLM autentikacijski paket (LM, NTLM, NTLMv2)
`Schannel.dll`	SSL/TLS autentikacijski protokol
`Kerberos.dll`	Kerberos V5 autentikacijski paket (ne postoji na NT sustavima)
`Wdigest.dll`	digest *challenge/response* protokol
`Lsasrv.dll`	LSA server servis koji provodi sigurnosnu politiku i upravlja sigurnosnim paketima
`Samsrv.dll`	SAM; pohranjuje lokalne korisničke račune, provodi lokalnu sigurnosnu politiku
`Secur32.dll`	sučelje vanjskih aplikacija prema LSA podsistemu
`Kdcsvc.dll`	KDC servis nužan za Kerberos autentikaciju (samo na 2000 i 2003 AD poslužiteljima)
`Ntdsa.dll`	Active Directory modul (samo na 2000 i 2003 AD poslužiteljima)
`Esent.dll`	implementacija Jet baze (samo na 2000 i 2003 AD poslužiteljima)

Tablica 5: Komponente LSA sigurnosnog podsistema

U nastavku dokumenta će biti detaljnije pojašnjena funkcionalnost većine navedenih komponenti, a posebno onih koje implementiraju autentikacijske protokole.

3.3. Interaktivna prijava za rad

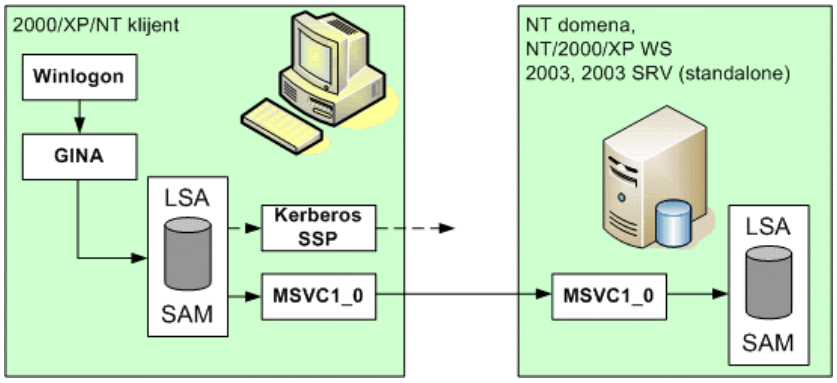
Interaktivna prijava podrazumijeva korisničku prijavu za rad, odnosno autentikaciju korisnika. Windows NT sustavi podržavaju LM, NTLM i NTLMv2 protokole za autentikaciju. Windows 2000, XP i 2003 sustavi, osim navedenih protokola, podržavaju i Kerberos v5, koji je i predefinirani protokol na tim sustavima.

Iako sa sigurnosnog stajališta to nije dobro, novije inačice Windows sustava (2000, XP i 2003) i dalje podržavaju i stare protokole. S druge strane, to je nužno da bi se osigurala kompatibilnost unazad.

Općeniti postupak autentikacije (na Windows 2000 i novijim sustavima) kod interaktivne prijave za rad provodi se na sljedeći način:

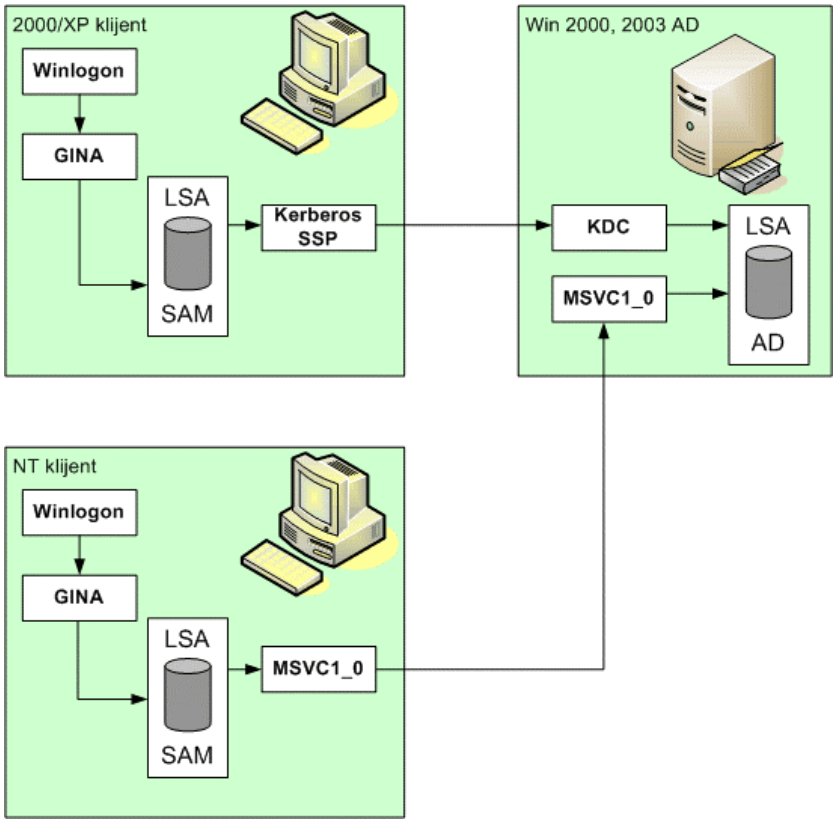
1. Korisnik unosi svoje korisničko ime i zaporku. GINA (eng. *graphical identification and authentication*) komponenta zaprima informacije.
2. GINA prosljeđuje informacije LSA podsistemu. LSA za komunikaciju s Kerberos i NTLM servisima koristi SSPI (eng. *security support provider interface*) sučelje. Korištenjem tog sučelja, implementacija autentikacijskog protokola je transparentna za aplikacije koje provode autentikaciju korisnika.
3. SSPI sučelje prosljeđuje autentikacijske podatke Kerberos SSP komponenti. Kerberos SSP prvo provjerava da li se traži autentikacija na lokalnom računalu (prema imenu računala/domene). Ako se traži lokalna autentikacija, Kerberos SSP javlja internu pogrešku. Ako se traži domenska autentikacija, Kerberos SSP pretražuje mrežu (u DNS-u se pretražuju `_kerberos` SRV zapisi). Ukoliko zapis nije pronađen, ponovno se dojavljuje interna pogreška.
4. Ukoliko SSPI primi dojavu o pogrešci od Kerberos SSP komponente, postupak se ponavlja tako da GINA ponovno prosljeđuje autentikacijske podatke LSA modulu, koji ponovno poziva SSPI sučelje.
5. SSPI ovaj put prosljeđuje autentikacijske podatke NTLM komponenti (MSV1_0) koja poziva Netlogon servis za autentikaciju na domeni (odnosno DC poslužitelju) ili sama provodi autentikaciju, ako se radi o lokalnoj SAM bazi.
6. U slučaju uspješne autentikacije (Kerberos ili NTLM), korisniku, odnosno korisničkom procesu, dodjeljuju se odgovarajuće SID oznake (ovisno o članstvima u grupama). Sam format u kojem su pohranjeni svi ti podaci ovisi o načinu autentikacije.

Slika 5 prikazuje općeniti postupak autentikacije preko SAM baze (lokalne ili domenske). Jedina razlika između NT i novijih sustava (2000, XP) jest u tome da kod NT sustava ne postoji Kerberos SSP komponenta, nego se autentikacija provodi direktno preko MSV1_0 komponente.



Slika 5: Autentikacija klijenta na lokalnoj ili udaljenoj SAM bazi (NT domena)

Kod autentikacije kroz Windows 2000/2003 *Active Directory* servis, 2000 i noviji sustavi koriste Kerberos SSPI komponentu, dok NT i stariji sustavi koriste MSV1_0 komponentu. Za osiguranje kompatibilnosti unazad i na Windows 2000/2003 *Active Directory* poslužiteljima postoji NTLM komponenta LSA podsistema (*Slika 6*).



Slika 6: Autentikacija klijenta kroz Active Directory servis

3.4. (NT)LM autentikacijski protokoli

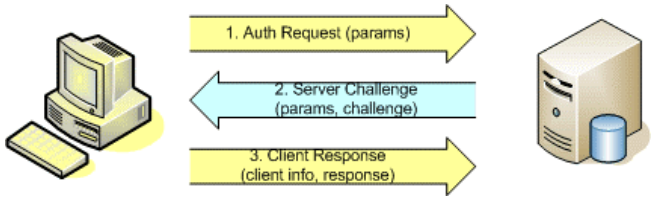
LAN Manager, NTLM i NTLMv2 spadaju u *challenge-response* kategoriju protokola,. Općenito, ti protokoli funkcioniraju na sljedeći način (*Slika 7*):

1. Klijent šalje zahtjev za autentikacijom poslužitelju (eng. *negotiation*). U toj poruci sadržani su parametri bitni za nastavak komunikacije koji su podržani od strane klijenta.
2. Poslužitelj (DC) odgovara svojom porukom u kojoj navodi parametre podržane sa svoje strane, i najvažnije od svega šalje slučajno generiranu 8-oktetnu vrijednost (eng. *challenge*).

3. Klijent odgovara na poruku slanjem klijentskih podataka (što uključuje korisničko ime i domenu), te slanjem odgovora (eng. *response*) na poslužiteljski generiranu slučajnu vrijednost.

Ukoliko poslužitelj (DC) provjerom ustanovi da su klijentske informacije ispravne, klijentu vraća informacije na temelju koji klijentski LSA može generirati sigurnosni token (eng. *security access token*).

Osim popisa parametara, ono po čemu se u biti najviše razlikuju ovi protokoli je način odgovora na poslužiteljsku *challenge* poruku.



Slika 7: NTLM challenge-response autentikacija

Na Windows sustavima za *challenge-response* autentikaciju koristi se isključivo NTLM SSPI (MSV1_0), bez obzira radi li se o LM, NTLM ili NTLMv2 autentikaciji.

3.4.1. LM odgovor

Windows 9x i stariji klijenti podržavaju samo LM protokol . Kod LM protokola za autentikaciju, odgovor na poslužiteljsku *challenge* poruku generira se na sljedeći način:

1. Na klijentskoj strani iz zaporke se generira 16-oktetna LM hash vrijednost (kako je opisano u poglavlju 2.4.1).
2. Dobiveni LM *hash* ispunjava se *null* oktetima do riječi duljine od 21 okteta.
3. Tako dobivena riječ dijeli se na tri 7-oktetna dijela iz kojih se generiraju tri 56-bitna DES ključa.
4. Svaki od ta tri ključa koristi se za šifriranje *challenge* vrijednosti, što kao rezultat daje tri različite 8-oktetne riječi.
5. 8-oktetne riječi dobivene šifriranjem spajaju se u 24-oktetnu riječ koja predstavlja LM *response* poruku.

Zbog načina generiranja *hash* vrijednosti (poglavlje 2.4.1), LM autentikacija izuzetno je ranjiva na napade primjenom sile (eng. *brute-force*), te se ne bi smjela koristiti u današnjim mrežnim okruženjima.

3.4.2. NTLM odgovor

NTLM protokol predefinirano se koristi se na NT sustavima starijim od NT 4 SP4. Kod NTLM protokola, *response* odgovor na poslužiteljski *challenge* generira se na sljedeći način:

1. Na klijentskoj strani iz UNICODE zaporke se, korištenjem MD4 funkcije generira 16-oktetna NTLM *hash* vrijednost (kako je opisano u poglavlju 2.4.2).
2. Taj *hash* ispunjava se 0x00 oktetima do riječi duljine od 21 okteta.
3. Tako dobivena riječ dijeli se na tri 7-oktetna dijela iz kojih se generiraju tri 56-bitna DES ključa.
4. Svaki od ta tri ključa koristi se za šifriranje *challenge* vrijednosti, što kao rezultat daje tri različite 8-oktetne riječi.
5. 8-oktetne riječi dobivene šifriranjem spajaju se u 24-oktetnu riječ koja predstavlja LM *response* poruku.

Može se uočiti da je jedina razlika u odnosu na LM autentikaciju u prvom koraku, odnosno u korištenju MD4 *hash* funkcije, umjesto OFW funkcije koju koristi LM.

Jedan od zahtjeva kod NTLM i LM autentikacije bio je i mogućnost tzv. *pass-trough* autentikacije koja omogućava jednostavno prosljeđivanje svih poruka između klijenta i poslužitelja. Na taj način donekle je unaprjeđena funkcionalnost, no isto tako otvorena je mogućnost brojnih *man-in-the-middle* napada, što NTLM autentikaciju, isto kao i LM autentikaciju, čini ranjivom na spomenuti tip napada.

3.4.3. NTLMv2 odgovor

NTLMv2 protokol kreiran je s ciljem uklanjanja sigurnosnih nedostataka upravo opisanog NTLM protokola. Ukoliko se koristi verzija 2 NTLM protokola, *response* odgovor mijenja se NTLMv2

odgovorom, a LM odgovor se zamjenjuje LMv2 odgovorom (isključivo zbog kompatibilnosti s *pass-through* autentikacijom). NTLMv2 odgovor se generira na sljedeći način:

1. Klijent generira NTLM *hash* (kako je opisano u poglavlju 2.4.2).
2. NTLM *hash* koristi se kao ključ za generiranje 16-oktetnog HMAC-MD5 *hasha* na temelju ulaza koji se sastoji od korisničkog imena i domene prikazanih velikim slovima u Unicode formatu. Tako dobivena 16-oktetna vrijednost predstavlja NTLMv2 *hash*.
3. Klijent generira blob (eng. *binary large object*) strukturu u kojoj se osim NTLMv2 *hash* vrijednosti nalaze i drugi podaci od kojih su najvažniji 64-bitna vremenska značka (eng. *timestamp*), klijentski 8-oktetni *challenge* i potpis cijelog bloba korištenjem HMAC-MD5 funkcije (kao ključ se koristi NTLMv2 *hash* dobiven u koraku 2).

Zbog korištenja vremenske značke klijent i poslužitelj moraju biti vremenski sinkronizirani (predefinirani vremenski okvir unutar kojeg se može provesti autentikacija korisnika je 30 minuta).
Sa sigurnosnog stajališta, ovakav način autentikacije i dalje je podložan svim napadima kao i NTLM, osim što se, korištenjem dodatne *hash* funkcije povećava vrijeme potrebno za provođenje *brute-force* napada. Najveće unapređenje ustvari predstavlja činjenica da se kod NTLMv2 autentikacije nikad ne koristi LM *hash* (što je moguće u slučaju NTLM protokola).
Kroz NTLMv2 *challenge-response* autentikaciju klijent i poslužitelj mogu dogovoriti korištenje šifriranja i potpisivanja poruka, odnosno sigurnost sjednica (*NTLMv2 session security*). Ukoliko se koristi takva shema, osim standardnog NTLMv2 *response* odgovora može se koristiti i NTLMv2 *session response* odgovor.
U tom slučaju NTLMv2 sjednički *response* odgovor se modificira na sljedeći način:

1. Generira se 8-oktetni klijentski *challenge* koji se zatim ispunjava 0x00 vrijednostima na 24-oktetnu riječ.
2. Klijentski i poslužiteljski *challenge* se spajaju u 16-oktetnu sjedničku značku (eng. *nonce*).
3. Na tu vrijednost se primjenjuje MD5 funkcija (http://www.ietf.org/rfc/rfc1321) koja kao rezultat daje 16-oktetnu *hash* vrijednost.
4. Dobiveni *hash* niz se skraćuje na 8 okteta da bi se dobila NTLMv2 sjednička *hash* vrijednost.
5. Klijent generira 16-oktetni NTLM *hash* (kako je opisano u poglavlju 2.4.2), koji se zatim ispunjava 0x00 vrijednostima na 21-oktetnu riječ.
6. Tako dobivena riječ se dijeli u tri 7-oktetne riječi koje se koriste za generiranje 3 56-bitna DES ključa.
7. Svaki od tih ključeva koristi se za šifriranje NTLMv2 sjedničke *hash* vrijednosti dobivene u koraku 4.
8. Tako dobivene šifrirane *hash* vrijednosti spajaju se u 24-oktetnu riječ koja predstavlja NTLMv2 sjednički *response* odgovor.

3.4.4. Autorizacija

Za dohvaćanje autorizacijskih podataka u mrežnom okruženju kod (NT)LM porodice protokola odgovoran je poslužitelj od kojeg klijent traži autentikaciju. LSA podsistem tog poslužitelja mora kontaktirati DC poslužitelj i generirati sigurnosni *token*, na temelju kojeg se kasnije vrši autorizacija klijentskog zahtjeva (*Slika 8*).

Slika 8: Pass through autorizacija u NT mrežnom okruženju

Takva, tzv. *pass-through* autentikacija jedan je od najvećih nedostataka NTLM porodice protokola, odnosno koncepta NT domena.

3.4.5. Kompatibilnost

Najveći problem u heterogenim Windows okruženjima predstavlja kompatibilnost unazad. Zbog tog razloga npr. NT klijeti uz NTLM odgovor predefinirano šalju i LM odgovor, čime se efektivno gube sigurnosna poboljšanja NTLM autentikacije. Uvođenje NTLMv2 autentikacije (NT 4 SP 4) poboljšana je NTLM sigurnost, no i dalje ostaje problem što se predefinirano koriste LM i NTLM odgovori (ta činjenica vrijedi i za 2000 i XP sustave).

Razinu kompatibilnosti na Windows sustavima moguće je podesiti kroz *registry* datoteku podešavanjem REG_DWORD vrijednosti `LMCompatibiltyLevel` unutar *registry* ključa: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa`.

Na Windows 9x sustavima je za omogućavanje NTLMv2 autentikacije prethodno potrebno instalirati *Active Directory client extension* komponentu.

Na NT i novijim sustavima dozvoljene `LMCompatibiltyLevel` vrijednosti su od 0 do 5, dok Windows 9x podržavaju samo vrijednosti 0 i 3.

Tablica 6 prikazuje mogućnosti podešavanja razine kompatibilnosti u heterogenim Windows okruženjima. Stupac poslužitelj odnosi se na poslužitelje novije od NT 4 SP4 (stariji poslužitelji ne podržavaju NTLMv2).

Razina	Klijent	Poslužitelj
0	koristi LM i NTLM autentikaciju nikad ne koristi NTLMv2 sigurnost sjednica	prihvaća LM, NTLM i NTLMv2 autentikaciju
1	koristi LM i NTLM autentikaciju koristi NTLMv2 sigurnost sjednica ukoliko poslužitelj podržava	prihvaća LM, NTLM i NTLMv2 autentikaciju
2	koristi NTLM autentikaciju koristi NTLMv2 sigurnost sjednica ukoliko poslužitelj podržava	prihvaća LM, NTLM i NTLMv2 autentikaciju
3	koristi NTLMv2 autentikaciju koristi NTLMv2 sigurnost sjednica ukoliko poslužitelj podržava	prihvaća LM, NTLM i NTLMv2 autentikaciju
4	koristi NTLM autentikaciju koristi NTLMv2 sigurnost sjednica ukoliko poslužitelj podržava	prihvaća samo NTLM i NTLMv2 autentikaciju
5	koristi NTLMv2 autentikaciju koristi NTLMv2 sigurnost sjednica ukoliko poslužitelj podržava	prihvaća samo NTLM i NTLMv2 autentikaciju

Tablica 6: Podešavanje razine kompatibilnosti na Windows sustavima

3.5. Kerberos autentikacija

Kerberos autentikacija predstavlja temeljni algoritam za autentikaciju unutar Windows 2000/2003 *Active Directory* okruženja.

Inače, Kerberos protokol razvijen je 80-ih godina 20og stoljeća na MIT-u u sklopu *Athena* projekta, nakon nekoliko promjena i dorada u svojoj inačici 5 (Kerbeors v5) definiran je RFC dokumentom 1510 (http://www.ietf.org/rfc/rfc1510). Korištenjem Kerberos protokola osigurava se sigurna komunikacija između entiteta (klijenata, poslužitelja), koji sami po sebi ne moraju biti sigurni. Za osiguranje takve komunikacije Kerberos koristi centralizirane poslužitelje (kojima svi entiteti vjeruju) koji implementiraju KDC (eng. *key distribution centre*), TGS (eng, *ticket granting service*) i AS (eng. *authentication service*). Uz takvu organizaciju Kerberos autentikacija sastoji se od sljedećih koraka:

1. Entiteti koji žele uspostaviti komunikaciju (klijent i poslužitelj) razmjenjuju podatke s KDC centrom (KDC sa svim entitetima dijeli zajednički tajni ključ).
2. Kerberos autenticira klijenta traženom servisu (poslužitelju) kroz TGS servis izdavanjem privremenih sjedničkih ključeva za komunikaciju između klijenta i KDC centra, poslužitelja i KDC centra, te klijenta i poslužitelja.
3. Komunikacija između klijenta i poslužitelja odvija se korištenjem privremenih sjedničkih ključeva.

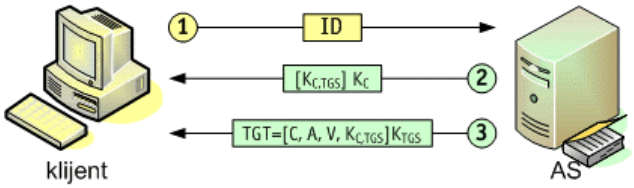
Tablica 7 opisuje pojmove bitne za proces Kerberos autentikacije koji će biti opisan u nastavku.

Oznaka	Opis
C	klijent
ID	korisničko ime klijenta
K_C	klijentski tajni ključ
A	klijentska mrežna adresa
S	poslužitelj
$K_{C,TGS}$	sjednički ključ koji dijele klijent i TGS
K_{TGS}	tajni ključ TGS servisa
K_S	poslužiteljski tajni ključ
$K_{C,S}$	sjednički ključ koji dijele klijent i poslužitelj
$T_{C,TGS}$	karta (eng. *ticket*) za komunikaciju između klijenta i TGS servisa
$T_{C,S}$	karta za komunikaciju između klijenta i poslužitelja
A_C	autentikacijska oznaka klijenta
V	vremenski period u kojem je karta važeća
T	vremenska značka
$[M]K_X$	poruka M šifrirana ključem K_X
TGT	karta za izdavanje karte (eng. *ticket granting ticket*)
K	dodatni sjednički ključ (opcionalno)

Tablica 7: Opis pojmova bitnih za Kerberos autentikaciju

Prva faza započinje korisničkim unosom korisničkog imena i zaporke na klijentskom računalu (*Slika 9*).

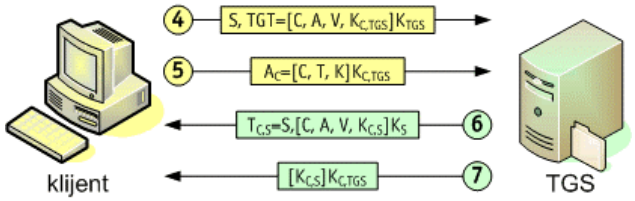
1. Klijent korištenjem jednosmjerne *hash* funkcije na temelju tih podataka generira klijentski tajni ključ (K_C) i šalje zahtjev za autentikacijom autentikacijskom servisu (AS). Zahtjev se sastoji od korisničkog imena u otvorenom tekstu.
2. Ukoliko se klijent nalazi u bazi autentikacijskog poslužitelja, AS poslužitelj vraća klijentu sjednički ključ za TGS servis ($K_{C,TGS}$) koji je šifriran tajnim ključem klijenta (K_C).
3. Također, AS poslužitelj vraća klijentu kartu za izdavanjem karte (TGT) šifriranu tajnim ključem TGS poslužitelja (K_{TGS}). Karta za izdavanje karte se sastoji od oznake klijenta (C), mrežne adrese (A), vremenskog perioda u kojem je karta važeća (V) i sjedničkog ključa za TGS servis ($K_{C,TGS}$).



Slika 9: Inicijalna razmjena podataka

Nakon što dešifrira dio poruke šifriran klijentskim tajnim ključem (K_C) koji sadrži sjednički ključ za komunikaciju s TGS servisom ($K_{C,TGS}$), klijent može obrisati iz memorije klijentski tajni ključ čime se umanjuje mogućnost njegove kompromitacije. Iduća faza predstavlja klijentski zahtjev za servisom TGS poslužitelju (*Slika 10*).

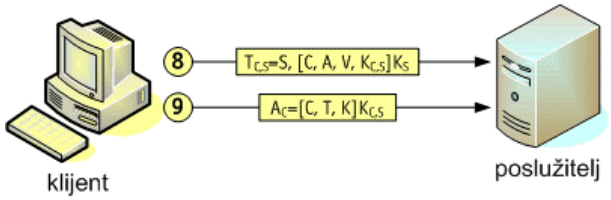
4. Prva poruka sadrži kartu za izdavanje karte (TGT) koja je šifrirana tajnim ključem TGS poslužitelja (K_{TGS}) i identifikator željenog servisa, odnosno poslužitelja (S).
5. Druga poruka predstavlja autentikacijsku oznaku klijenta TGS poslužitelju i ona sadrži oznaku klijenta (C), vremensku značku (T), te opcionalno i dodatni sjednički ključ (K), a šifrirana je sjedničkim ključem koji dijele klijent i TGS poslužitelj ($K_{C,TGS}$).
6. Nakon što TGS poslužitelj zaprimi valjanu TGT kartu i autentikacijsku oznaku klijenta koji traži servis on izdaje kartu ($T_{C,S}$) šifriranu tajnim ključem poslužitelja (K_S) klijentu. Karta sadrži ime klijenta (C), mrežnu adresu klijenta (A), vremenski period u kojem je karta važeća (V) i sjednički ključ koji će dijeliti klijent i poslužitelj ($K_{C,S}$).
7. Također, TGS poslužitelj klijentu vraća sjednički ključ koji će dijeliti klijent i poslužitelj ($K_{C,S}$) šifriran ključem koji dijele klijent i TGS servis ($K_{C,TGS}$).



Slika 10: Zahtjev za servisom

Konačno, u trećoj fazi klijent se autenticira poslužitelju od kojeg traži uslugu (*Slika 11*).

8. Klijent poslužitelju šalje kartu ($T_{C,S}$) koja sadrži ime klijenta (C), mrežnu adresu klijenta (A), vremenski period u kojem je karta važeća (V) i sjednički ključ koji će dijeliti klijent i poslužitelj ($K_{C,S}$) šifriranu tajnim ključem poslužitelja (K_S).
9. Također klijent šalje autentikacijsku oznaku klijenta koja se sastoji od imena klijenta (C), vremenske značke (T) i opcionalnog dodatnog sjedničkog ključa (K) šifriranu sjedničkim ključem koji dijele klijent i poslužitelj ($K_{C,S}$).



Slika 11: Autentikacija poslužitelju

Poslužitelj provjerava kartu ($T_{C,S}$) i autentikacijsku oznaku klijenta, te ukoliko su one valjane autenticira klijenta.

3.5.1. *Active Directory* implementacija

Kerberos autentikacija na Windows 2000 Server i Server 2003 sustavima implementirana je kroz *Active Directory* servis. Na AD poslužiteljima, unutar LSA podsistema, pokrenut je KDC servis koji se sastoji od dvije komponente:

– AS servisa i
– TGS servisa.

Prilikom kreiranja *Active Directory*-ja kreira se i korisnički račun `krbtgt` koji se ne može obrisati niti mu se može promijeniti ime. Zaporka koja je pridružena tom korisničkom računu, mijenja se automatski u regularnim intervalima i služi za generiranje tajnog ključa kojim se šifrira i dešifrira TGT (K_{TGS}).

Na klijentskoj strani za Kerberos autentikaciju zadužena je Kerberos SSP komponenta LSA podsistema.

Obzirom da se prilikom Kerberos autentikacije koriste vremenske značke, a i Kerberos karte imaju samo određeni vremenski period važenja, vremenska sinkronizacija je vrlo važan faktor u AD okruženjima. Za sinkronizaciju je zadužen *Windows Time Synchronization Service* (`W32time`) servis koji se bazira na SNTP (eng. *simple network time protocol)* koji je definiran u RFC 1769 dokumentu (http://www.ietf.org/rfc/rfc1769). Windows 2000 i XP radne stanice se sinkroniziraju DC poslužiteljem kod kojeg se autenticiraju. DC poslužitelji u domeni koriste PDC Emulator za vremensku sinkronizaciju, a domenski PDC Emulator koristi PDC Emulator u hijerarhijski višoj domeni. PDC Emulator u *root* domeni AD hijerarhije bi morao koristiti vanjski *SNTP time* poslužitelj.

3.5.2. Autorizacija

Kerberos je prije svega autentikacijski protokol, odnosno njime se ne osigurava autorizacija. Međutim, protokolom je predviđeno polje za autorizacijske podatke. Kod Windows implementacije Kerberos protokola, u autorizacijskom polju karte nalazi se popis SID-ova koji identificiraju sigurnosnog principala i njegovo članstvo u grupama. Ti podaci prikupljaju se u dva koraka:

1. Prilikom pripreme TGT karte koju je korisnik (klijent) zatražio. Tom prilikom autorizacijski podaci uključuju korisnički SID i sve ostale SID-ove koji označavaju korisničko članstvo u domenskim

sigurnosnim grupama (u višedomenskom okruženju dodaju SID-ovi koji označavaju članstva u univerzalnim grupama).

2. Prilikom korisničkog zahtjeva za izdavanje karte od strane TGS poslužitelja, KDC provjerava članstvo poslužitelja za kojeg klijent traži kartu. Ako je domena poslužitelja različita od korisničke, KDC provjerava da li je korisnik član neke od lokalnih domenskih sigurnosnih grupa te ih dodaje u autorizacijsko polje.

Na temelju tog autorizacijskog polja i uspješne provjere klijentskih podataka (karte i autentikacijske oznake klijenta) poslužitelj može generirati pristupni token i na temelju njega provesti autorizaciju bez kontaktiranja DC poslužitelja, što je ključna razlika u odnosu na (NT)LM autentikaciju.

3.6. Drugi mehanizmi za autentikaciju korisnika

3.6.1. Schannel

Schannel (*security channel*) autentikacija predstavlja skup protokola koji označavaju implementaciju SSL (eng. *secure socket layer*), odnosno TLS (eng. *transport layer security*) protokola na Windows sustavima (2000, XP, 2003).

Schannel autentikacija implementirana je kroz TLS/SSL SSPI sučelje (`Schannel.dll`) koje je dio LSA podsistema (TLS/SSL sučelje aplikacije mogu pozivati i izravno). Sam proces autentikacije definiran je SSL, odnosno TLS protokolima a u većini slučajeva podrazumijeva jednostranu ili obostranu autentikaciju korištenjem digitalnih certifikata, iako su mogući i drugi oblici autentikacije. TLS/SSL autentikacija izlazi iz okvira ovog dokumenta, a više informacija o TLS protokolu (koji predstavlja IETF standardizaciju SSL 3.0 protokola) moguće je naći u dokumentu "The TLS Protocol Version 1.0" (http://www.ietf.org/rfc/rfc2246).

Korištenjem TLS/SSL protokola osigurava se fleksibilnost, interoperabilnost i jednostavnost korištenja. Tipična primjena Schannel autentikacije, odnosno TLS/SSL protokola jest autentikacija i stvaranje komunikacijskog sigurnog kanala aplikacija kao što su e-mail, e-commerce, Web, udaljeni pristup, SQL pristup itd.

3.6.2. Digest autentikacija

Digest autentikacija (eng. *digest authentication*) je oblik dvostupanjske (eng. *two tier*) *challenge-response* autentikacije (i autorizacije) koji se uglavnom koristi u specifičnim aplikacijama kao što su LDAP i HTTP. Digest autentikacija provodi kao *challenge-response* autentikacija između klijenta i poslužitelja. Ta autentikacija može biti i SASL (eng. *secure authentication socket layer*) bazirana čime se osigurava povjerljivost i integritet komunikacije. Razlika u odnosu na standardni *challenge-response* je u tome da, ukoliko klijentski *response* odgovor odgovara *challenge* upitu, poslužitelj prosljeđuje taj *response* odgovor DC poslužitelju koji odobrava ili odbija autentikaciju. Ako je autentikacija uspješna, DC poslužitelj šalje poslužitelju poruku u kojoj je sadržan sjednički ključ za daljnju Digest komunikaciju. Na taj način klijent se autenticira i istovremeno mu se odobrava pristup traženom resursu (autorizacija).

3.6.3. Negotiate autentikacija

Negotiate autentikacija predstavlja mehanizam unutar kojeg je moguće odabrati neku od autentikacijskih shema a bazira se na RFC dokumentu "The Simple and Protected GSS-API Negotiation Mechanism" (http://www.ietf.org/rfc/rfc2478) koji specificira GSS (eng. *generic security service*) API sučelje.

Negotate paket trenutno se koristi za odabir između NTLM i Kerberos autentikacije.

3.6.4. Passport autentikacija

Passport autentikacija predstavlja mehanizam kojim razni Web servisi mogu osigurati korisnicima *single sign-on*, odnosno jedinstvenu autentikaciju za pristup raznim Web servisima. Passport autentikacija temelji se na uporabi kolačića (eng. *cookies*) i TLS/SSL protokolima.

4. Zaključak

U ovom dokumentu ponajviše su opisani NTLM c*hallenge-response* i Kerberos protokoli. Najnesigurniji od svih opisanih protokola je svakako LM, koji se ne bi smio koristiti osim ako je to zaista nužno zbog kompatibilnosti unazad. NTLM i NTLMv2 protokoli pružaju nešto veću razinu sigurnosti, no zbog načina autentikacije i dalje ostavljaju mogućnosti za razne napade, a posebno su osjetljivi na *man-in-the-middle* varijacije napada.

Za razliku od tih protokola, Kerberos autentikacija onemogućuje opisane vrste napada, osim toga sam postupak autentikacije prilikom pristupa mrežnim resursima je brži nego kod NT *passthrough* autentikacije. Nadalje, Kerberos osigurava obostranu autentikaciju klijenta i poslužitelja (NTLM protokolima autenticira se samo klijent). Konačno, Kerberos je otvoreni standard, a ne proizvođački standard (kao NTLM). Samim time osigurana je i kvalitetna dokumentacija protokola.

Zbog svih tih razloga u Windows domenskim mrežnim okruženjima potrebno je težiti uspostavi *Active Directory* infrastrukture, a-domensku autentikaciju pokušati maksimalno osigurati podizanjem na najsigurniju moguću razinu, odnosno na NTLMv2. Također, svakako je uputno ukloniti LM *hash* vrijednosti iz SAM baza i *Active Directory*-ja gdje je to moguće.

Implementacijom takvih sigurnosnih mjera postiže se temelj za izgradnju sigurnog informacijskog sustava.

5. Reference

[1] Prednosti i nedostaci uporabe Syskey alata, CCERT-PUBDOC-2003-12-53, http://www.cert.hr.

[2] Well-known security identifiers in Windows Server operating systems, Concept – SID, http://support.microsoft.com/default.aspx?scid=kb;EN-US;Q243330.

[3] Local Logon Process for Windows 2000, http://support.microsoft.com/kb/231789.

[4] The NTLM Authentication Protocol, http://davenport.sourceforge.net/ntlm.html.

[5] Proces autentikacije kod Windows 2000 operacijskih sustava, CCERT-PUBDOC-2003-03-07, http://www.cert.hr.

[6] How to enable NTLM 2 authentication, http://support.microsoft.com/default.aspx?scid=KB;en-us;239869.

[7] How to prevent Windows from storing a LAN manager hash of your password in *Active Directory* and local SAM databases, http://support.microsoft.com/default.aspx?scid=KB;EN-US;q299656&.

[8] Windows 2000 Kerberos Authentication, http://www.microsoft.com/windows2000/techinfo/howitworks/security/kerberos.asp.

[9] Logon and authentication Technologies, http://www.microsoft.com/Resources/Documentation/windowsserv/2003/all/techref/en-us/w2k3tr_sec_authn_over.asp.

[10] Windows Time Synchronization Service, http://www.winnetmag.com/Articles/Index.cfm?ArticleID=8383.

[11] Windows Security Resource Kit, *Ben Smith and Brian Komar, Microsoft Press*