HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Prednosti i nedostaci uporabe Syskey alata

CCERT-PUBDOC-2003-12-53

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

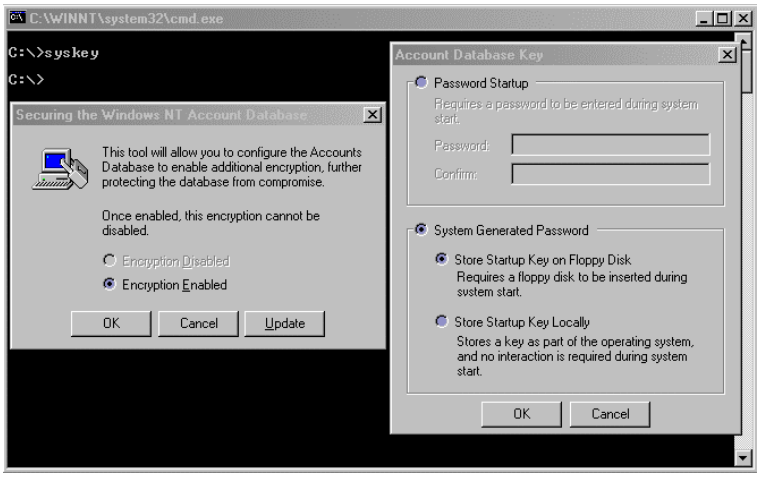
Syskey je Windows alat koji pruža dodatnu razinu zaštite SAM (engl. *Security Accounts Manager*) baze u kojoj su pohranjeni autentikacijski podaci korisnika na Windows NT, 2000, XP i 2003 sustavima.
Iako je SAM baza zaštićena od direktnog pristupa neovlaštenih korisnika na razini operacijskog sustava, pošto je takav pristup dozvoljen samo korisnicima s administrativnim ovlastima, ona je i dalje ranjiva na tzv. *offline* napade. *Offline* napadi izvode se tako da se na neki način dohvati SAM baza, te se napravi njena kopija nad kojom se kasnije provode napadi poput onog primjenom sile (engl. *brute force attack*) i/ili korištenjem rječnika (engl. *dictionary attack*).
Korištenjem Syskey alata, odnosno šifriranjem SAM baze podataka, moguće je implementirati dodatnu razinu sigurnosti. U ovom dokumentu biti će opisan rad Syskey alata na Windows NT/2000/XP/2003 sustavima, prednosti njegove uporabe, isto kao i nedostaci i slabosti koje nije moguće otkloniti niti uporabom ovog alata.

2. Syskey na Windows NT i Windows 2000/XP/2003 sustavima

Na Windows NT sustavima SAM baza predefinirano nije šifrirana, već su korisnička imena i *hash* vrijednosti zaporki bile pohranjene u dijelu *registry* datoteke kao otvoreni tekst, a jedina zaštita SAM baze implementirana je kroz kontrolu pristupa, odnosno onemogućavanje direktnog pristupa svim korisnicima osim onima s administrativnim ovlastima. Syskey alat je dostupan na sustavima koji imaju instaliran SP3 ili noviji skup zakrpi, predefinirano se koristi 40-bitna kriptografija, a za implementaciju jake (128-bitne) kriptografije potrebno je instalirati dodatnu zakrpu.
Na Windows 2000 i novijim sustavima Syskey zaštita bazirana na jakoj kriptografiji je predefinirano uključena, te je SAM baza zaštićena dodatnom razinom sigurnosti. Syskey zaštitu na Windows 2000 i novijim sustavima nije moguće isključiti. Algoritam koji Syskey koristi za šifriranje SAM baze jest RC4.
Syskey je moguće koristiti na tri načina:

- Prvi način je korištenje slučajno generiranog ključa kao sistemskog ključa i njegova pohrana na lokalnom sustavu korištenjem složenog algoritma za zaštitu.
- Drugi način također koristi slučajno generirani ključ koji se, međutim, pohranjuje na disketu. Ovaj način pruža dodatnu razinu zaštite pošto ključ nije pohranjen nigdje na sustavu, no za samo pokretanje sustava potrebna je disketa s pohranjenim sistemskim ključem.
- Konačno, sistemski ključ moguće je generirati iz zaporke koju odabire administrator sustava. U tom slučaju tijekom pokretanja sustava potrebno je unijeti odgovarajuću zaporku koja se zatim provjerava u odnosu na *hash* vrijednost pohranjenu u sustavu dobivenu korištenjem MD5 jednosmjerne funkcije.

Slika 1 prikazuje generiranje ključa sustava na Windows 2000 sustavu temeljem slučajno generirane vrijednosti i njegova pohrana na disketu. Kako je na slici vidljivo opcija *Encryption Disabled* je onemogućena, odnosno SAM baza je uvijek zaštićena korištenjem Syskey alata.



Slika 1: Korištenje Syskey alata na Windows 2000 sustavu

3. Nedostaci Syskey zaštite

Ukoliko je Syskey zaštita implementirana korištenjem zaporke i uz pretpostavku da je da takva zaporka odgovarajuće odabrana, odnosno dulja od 12 znakova (minimalna duljina nije definirana, dok je maksimalna vrijednost 128 znakova), može se reći da je sustav siguran, pošto napadač može provoditi napade samo nad šifriranom SAM bazom (na sustavu je pohranjena samo MD5 vrijednost odabrane zaporke). Podjednako sigurnim može se smatrati i pohrana sistemskog ključa na disketi.

Ukoliko je pak sistemski ključ pohranjen na disku računala (predefinirana opcija na sustavima koji imaju automatski uključenu Syskey zaštitu), situacija je drugačija. Da bi se pojasnio taj slučaj potrebno je opisati kako se sistemski ključ pohranjuje na disku, te kako se pristupa SAM bazi.

Prilikom pokretanja Windows sustava, prije nego se korisnici mogu prijaviti na sustav glavna nit `Smss` procesa (engl. *Session Manager*) pokreće `Winlogon` proces. Winlogon proces učitava `Lsass` (engl. *Local Security Subsystem*), koji pak prema potrebi pokreće *Security Accounts Manager* servis koji predstavlja sučelje prema SAM bazi. Spomenuti procesi pristupaju sljedećim ključevima *registry* datoteke:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\JD
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\Skew1
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\Data
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\GBG
```

Istim ključevima pristupa i `Syskey.exe` alat prilikom generiranja ključa sustava. Detaljnija analiza programskog kôda koji je zadužen za pristup ključu pokazuje da je algoritam za njegovu zaštitu jednostavna permutacija imena klasa gore spomenutih ključeva, te je izrada alata koji može ekstrahirati sistemski ključ iz *registry* datoteke gotovo trivijalna. Na starijim sustavima (NT SP3) pristup tim ključevima bio je dozvoljen čak i običnim korisnicima, no taj je nedostatak kasnije ispravljen.

Napadač u ovom slučaju ima dvije mogućnosti. Ukoliko ima administrativne ovlasti na sustavu, može korištenjem specifičnih alata (npr. `Bkreg.exe`) doći do ključa sustava. Druga mogućnost je da prilikom krađe same SAM baze ukrade i gore spomenute ključeve na temelju kojih se može doći do Syskey ključa sustava (`Bkhive.exe`).

Ovakvi napadi mogući su ukoliko napadač ima fizički pristup sustavu ili je došao do administrativnih ovlasti iskorištavanjem nekog drugog nedostatka na sustavu. Ukoliko napadač ima fizički pristup sustavu ili se na neki drugi način uspio domoći diska (krađa), očekivani scenarij za izvršavanje napada je sljedeći:

1. Pokrenuti sustav korištenjem nekog operacijskog sustava koji ima mogućnost čitanja NTFS datotečnog sustava.
2. Iz `%WINDIR%\System32\config` direktorija kopirati SAM i SYSTEM dijelove *registry* datoteke (engl. *hive*).
3. Korištenjem proizvoljnog alata (npr. `Bkreg.exe`, `Bkhive.exe` ili `SAMInside.exe`) ekstrahirati sistemski ključ.
4. Dohvatiti dešifrirane *hash* vrijednosti zaporki.
5. Izvršiti napad primjenom sile ili korištenjem rječnika.

4. Dodatna razmatranja

Jedan od potencijalnih problema koji može proizaći iz ranije opisanog nedostatka Syskey zaštite jest mogućnost kompromitacije EFS šifriranog datotečnog sustava koji je podržan na Windows 2000 i novijim sustavima.

EFS sustav koristi kriptografske metode temeljene na javnim i tajnim ključevima da bi zaštitio korisničke datoteke kada zaštita korištenjem NTFS pristupnih lista nije dovoljna. Algoritam koji služi za šifriranje jest DESX, a kao parametar se koristi slučajno generirani simetrični ključ – FEK (engl. *File Encryption Key*). FEK se zatim šifrira javnim ključem korisnika i javnim ključem tzv. *key recovery agent*-a, te eventualnim drugim javnim ključevima korisnika koji također imaju pravo pristupa specifičnoj datoteci. *Key recovery agent* služi da se omogući dešifriranje podataka ukoliko na bilo koji način dođe do gubitka ključeva za šifriranje/dešifriranje. Predefinirani *recovery agent* na sustavu je

lokalni (ili domenski) administratorski korisnički račun. Na Windows 2000 sustavima korištenje *recovery agent*-a je nužno, dok na Windows XP i 2003 sustavima to nije slučaj.
Poznato je da je EFS datotečni sustav osjetljiv na *offline* napade (npr. ukoliko dođe do krađe diska sa šifriranim podacima) ukoliko je *recovery agent*-ov privatni ključ pohranjen na disku. Najjednostavniji način je brisanje SAM baze. Ukoliko se SAM baza obriše, sustav prilikom sljedećeg pokretanja automatski otvara novu SAM bazu s administratorskim korisničkim računom i praznom zaporkom. Nakon toga napadač se može prijaviti kao administrator te kao *recovery agent* pristupiti bilo kojoj datoteci unutar EFS sustava. Zbog toga se za postizanje više razine sigurnosti preporuča pohrana tog ključa na sigurno mjesto.
No, isto tako treba znati da, ukoliko je Syskey ključ sustava pohranjen na disku, napadač ga može kompromitirati korištenjem nekog od alata dostupnih na Internetu, te promijeniti zaporku bilo kojeg korisnika na sustavu, uključujući i administratora. Nakon što je promijenio zaporku željenog korisnika, napadač se može prijaviti na sustav predstavljajući se kao legitimni korisnik te na taj način pristupiti korisničkom privatnom ključu koji se upotrebljava za dešifriranje EFS šifriranih datoteka. Ovaj nedostatak bi se teoretski mogao izbjeći tako da svi korisnici svoje privatne ključeve pohranjuju na sigurnom mjestu; no na taj način izgubio bi se velik dio funkcionalnosti.

5. Zaključak

Zaštita korištenjem Syskey enkripcije SAM baze predstavlja unaprjeđenje u odnosu na pohranu korisničkih imena i *hash* vrijednosti zaporki u otvorenom obliku. Pošto su NTLM, a posebno LM zaporke osjetljive na napade primjenom sile, dodatni stupanj zaštite svakako je potreban.
Način korištenja Syskey zaštite posebno je važan u onim situacijama gdje je potencijalnom napadaču omogućen fizički pristup sustavu. Pokazuje se da je predefinirana Syskey zaštita, kod koje se automatski generirani ključ sustava pohranjuje na istom disku kao i SAM baza u takvim situacijama nedostatna, te u tom slučaju ne predstavlja dodatni problem za napadača. Također, kod tako konfigurirane Syskey zaštite mogu proizaći i neki drugi nedostaci, od kojih je svakako najosjetljivija opisana mogućnost kompromitacije EFS datotečnog sustava.
Ukoliko se želi osigurati maksimalna razina zaštite, što se odnosi na sustave koji sadrže najpovjerljivije informacije, Syskey zaštitu potrebno je implementirati tako da se slučajno generirani ključ sustava ne nalazi na istom disku s informacijama koje štiti (SAM baza) nego na drugom mediju (disketa). Zaštita korištenjem ključa generiranog iz zaporke također je dobra ukoliko je zaporka pravilno odabrana (zadovoljavajuće složenosti).

6. Reference

How to Use the SysKey Utility to Secure the Windows 2000 Security Accounts Manager Database, http://support.microsoft.com/default.aspx?kbid=310105

Windows NT System Key Permits Strong Encryption of the SAM, http://support.microsoft.com/default.aspx?kbid=143475,

Syskey Cracking, http://www.schizm.netfirms.com/docs/syskeyhackingfinal.htm,

Windows 2k/NT/XP's syskey encryption, http://studenti.unina.it/~ncuomo/syskey/syskey.txt,

Analysis of Alleged Vulnerability in Windows 2000 Syskey and the Encrypting File System, http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/news/efs.asp,

Default SYSKEY configuration compromises encrypting file system, http://www.securiteam.com/windowsntfocus/5FP0B0U1FW.html