UNINyTT
Nyhetsbulletin

Nr 1 1995

Varslingsrutiner ved mistanke om brudd på sikkerheten i UNINETT og tilknyttede systemer

Alf Hansen

UNINETT Sikkerhetsansvarlig

Dersom du som bruker mener at du eller dine data på en eller annen måte er angrepet gjennom din bruk av UNINETT, skal du straks varsle din lokale sikkerhetskontakt i din organisasjon. Dersom du er i tvil om hvem dette er, spør din lokale EDB ansvarlige.

Alle medlemsinstitusjoner i UNINETT har en sikkerhetsansvarlig. Alle medlemsinstitusjoner i UNINETT er selv ansvarlige for den interne sikkerheten i sine systemer.

Sikkerhetskontakten vil analysere ditt problem og om nødvendig varsle UNINETT CERT (CERT=Computer Emergency Response Team). UNINETT CERT vil kunne gi en samlet vurdering av den varslede hendelsen, og om nødvendig varsle andre berørte parter. Sammen vil de kartlegge alle fakta slik at man best mulig får et grunnlag for å vurdere i hvilken grad tilfellet skal etterforskes med hensyn på identifisering av kilde og eventuell rettslig oppfølging.

I de tilfellene angrep på sikkerheten i UNINETT og tilknyttede systemer har internasjonale forgreninger, vil UNINETT CERT ta kontakt med relevante CERTer i andre land, eventuelt via CERT COORDINATION CENTER i USA.

Resultatet av etterforskningen vil rapporteres tilbake til den lokale sikkerhetskontakten, og man vil i fellesskap vurdere tiltak som skal settes i verk for å minske følgene av et angrep, identifisere og straffeforfølge kilden til angrepet og tette de huller som eventuelt ble oppdaget som en følge av at hendelsen oppsto.

UNINETT CERT sin e-post adresse er

cert@uninett.no

og mer informasjon fra UNINETT CERT er lagt ut på

http://www.uninett.no/info/cert/home.html

Innhald

Dette nummeret av UNINyTT tar særleg for seg tryggleik ved bruk av nettenester. UNINETT ønskjer i 1995 å fokusera på tryggleik i nettet.

Utgiver av UNINyTT er
UNINETTs sekretariat
Postboks 6883 Elgeseter
7002 Trondheim
Redaktør: Ingrid Melve
Telefon: 73 59 65 02
Epost: uninytt@uninett.no

Redaktørhjørnet

Tryggleik

UNINyTT kjem i tida framover til å ta for seg ulike aspekt ved tryggleiken i nettet. I dette nummeret står det litt om UNINETT sin nye tryggleikspolicy.

Mykje av tryggleiksarbeidet framover vil dreia seg om kryptering, som ein første introduksjon til emnet har UNINyTT ein innføringsartikkel om kryptering og litt om PGP som har vore ein av dei mest populære krypteringsmetodane (spesielt i samband med e-post).

UNINETT vil i løpet av kort tid ha eit sertifiseringssenter og eit tilbod om praktisk bruk av kryptering for alle UNINETT medlemsinstitusjonar. Dette krypteringssenteret vil basera seg på bruk av PEM (offentleg nøkkel kryptering). Sjå artikkel om dette. Meir informasjon om krypteringstenesta vil bli sendt ut.

Artiklar

Dersom nokon av lesarne ønskjer å skriva artiklar eller har emne dei ønskjer å ta opp, ta kontakt med redaktøren.

Elektronisk utgåve

UNINyTT ligg tilgjengeleg i elektronisk utgåve både på ftp, gopher og WWW under UNINETTINFO.

UNINETTINFO finn du på

http://www.uninett.no/info/uninettinfo.html
gopher://gopher.uninett.no/UNINETT%20 informasjonstjener
ftp://ftp.uninett.no/uninettinfo

Nye medarbeiderar i UNINETT sekretariat

Grete Duna

Grete Duna er sekretær. Ho har ansvar for sentralbordfunskjonen i sekretariatet og kontakt med nye medlemsinstitusjonar.

Roald Torbergsen

Roald Torbergsen kjem til UNINETT frå SINTEF RUNIT. Han skal ha ansvar for val av teknologi, nettplanlegging og koordinering av telefoni- og dataløysingar mellom høgskulane. Hovudoppgåva blir oppfølging av KOMPAKT-prosjektet ovafor høgskulane.

Thomas Øhrbom

Thomas Øhrbom er tilsett som adminsitrativ/teknisk medarbeider. Han er sivilingeniør frå IDT, NTH og har tidlegare arbeidd som prosjektsekretær for KOMPAKT.

Han har ansvar for medlemskapshandtering ved nye medlem og namneautoritet ved administrativ registrering av nye domenenamn i Norge.

Olaf Schjelderup

Olaf Schjelderup er tilsett som teknisk medarbeider. Han kjem frå Regionssykehuset i Trondheim. Han skal særleg arbeida med tryggleik og Internet koordinering.

Skuleverket og Internet

Handlingsplan for IT i utdanninga

1. april kjem KUF (Kyrkje-, Undervising og Forskingsdepartementet) med sin handlingsplan for IT i utdanninga. Denne handlingsplanen vil det vera naturleg å leita etter på KUF si heimeside på WWW

http://www.unik.no/KUF/kufforside.html.

Handlingsplanen vil leggja rammene for kva som vil skje framover når det gjeld bruk av nett-tenester innan skuleverket.

Tekniske løysingar

Skuleverket treng tekniske løysingar som er tilpassa dei tilhøva som er på datasida ute på skulane. Det vil kreva stor innsats å læra opp heile skuleverket i bruk av Internet.

Bruk av ISDN er interessant for dei skulane som har installert lokalnett. I Hordaland er ei gruppe på omlag 30 vidaregåande skular i ferd med å testa ut korleis ISDN fungerer. Desse skulane har tatt i bruk ISDN ved å kopla lokalnettet sitt til ein ISDN-rutar som så kommuniserer med UNINETT.

UNINETT har fleire prosjekt som ser på låg-kostløysingar for tilknyting, desse prosjekta vil vera ferdige til somaren. Kostnader med dei ulike tilknytingsformene er avhengige av kva tekniske løysingar ein vel.

Det er heilt klart at ein i ein undervisningssituasjon ikkje kan bruka oppringt Internet som utgangspunkt, ein må kopla opp heile klassen og la alle elevane få tilgang samstundes. Oppringt Internet er ei løysing for ein enkeltståande PC/Mac, ikkje for ein klasse.

UNINETT

UNINETT har under arbeid ei utgreiing om korleis ein kan knyta til eit stort volum skular. Denne utgreiinga ser på organisering av tilknyting for skulane, og arbeidsgruppa som gjer utgreiinga har kome med innspel til KUF sin handlingsplan ut frå dei tekniske og organisatoriske erfaringane UNINETT har.

Utgangspunktet for utgreiingsarbeidet har vore Stortingsmelding 24 (1993-94) der UNINETT blir tillagt ansvar for å tilby nett-tenester til skuleverket.

Tilbod til skuleverket

Etter at handlingsplanen har blitt handsama vil det bli klart kva tilbod KUF ønskjer at UNINETT skal gje til skulesektoren når det gjeld Internet-tilknyting og kva nett-tenester KUF ønskjer skulesektoren skal få tilgang til.

UNINyTT utsending

Det har vore problem med utsendinga av UNINyTT, difor skjer det no ei omlegging av utsendingsrutinene. Meld frå til uninytt@uninett.no viss det er endringar i abonnementet (personar eller tal på eksemplar).

UNINyTT blir sendt ut gratis til dei som ønskjer det.

KOMPAKT II

Roald Torbergsen
Koordinator, KOMPAKT

I 1994 bevilget KUF midler til å gjennomføre et pilotprosjekt for å få etablert en felles telefoni- og datainfrastruktur mellom studiestedene ved Høgskolen i Telemark og Høgskolen i Nord-Trøndelag som ble utpekt til pilothøgskoler.

Infrastrukturen er basert på ISDN mot offentlig nett og leide 2 Mbit/s linjer for telefon og data mellom studiestedene. Teknologivalg og løsninger er beskrevet i KOMPAKT-rapporten som man finner under ftp://ftp.uninett.no/uninettinfo/prosjekt/KOMPAKT/. De valgene som er beskrevet i rapporten må samordnes med eksisterende utstyrspark og høgskolens IT-strategi.

Departementet har bevilget midler for å videreføre prosjektet til nye høgskoler i 1995 og prioriterer følgende områder:

- Bidra til en tilfredsstillende nettsikkerhet og segmentering mellom ansatte og studenter ved høgskolene.
- Etablere tilfredsstillende infrastruktur for de mest distribuerte høgskolene.

Lokale "Infrastruktur-prosjekter" er nå igangsatt ved følgende høgskoler:

- Høgskolen Stord/Haugesund
- Høgskolen i Agder
- Høgskolen i Sogn og Fjordane
- Høgskolen i Hedmark
- Høgskolen i Buskerud
- Høgskolen i Østfold

Departementet har i brev til høgskolene forutsatt at alle sentralanskaffelser skjer gjennom UNINETT. Høgskoler som har behov for assistanse enten i forbindelse med valg av løsninger eller egne anskaffelser kan ta kontakt med UNINETT.

Administrative systemer.

Departementet har valgt en løsning basert på Oracle som felles databasesystem med en sentral server ved hver høgskole.

Det er prøvedrift med Agresso økonomisystem ved Høgskolene i Agder og Høgskolen i Nord-Trøndelag. Departementet vil i løpet av kort tid ta stilling til videreføring av prosjektet.

Det er fremdeles 13 høgskoler som ikke har valgt arkivjournalsystem. For å få bedre samordning av anskaffelsene sender Høgskolen i Sør-Trøndelag ut en prisforespørsel til aktuelle leverandører på vegne av resterende høgskoler.

Sikkerhet

Høgskolen må spesifisere egne krav til sikkerhet og lokal løsning. Høgskoler som ennå ikke har fått sluttført arbeidet med segmentering av nettet kan ta kontakt med UNINETT for assistanse. UNINETT vil utvide avtalene med de regionale sentrene slik at de også kan bistå i forbindelse med sikkerhet i nettet.

UNINETT'95

Tid og stad

Konferansen UNINETT'95 finn stad i Trondheim 21. og 22. november 1995.

Arrangør er UNINETT i samarbeid med Universitetet i Trondheim (UNIT), og arrangementet blir på Dragvoll (AVH).

Teknisk konferanse

UNINETT'95 blir ein teknisk retta konferanse for UNINETT sine medlemsinstitusjonar. Dagen før konferansen vil det bli arrangert ulike kurs for driftspersonell.

Emna som vil bli tatt opp på konferansen er

- tryggleik
- PC-nett
- tenester i nettet, med vekt på WWW og multimedia
- dagens nett-teknologi, mellom anna ISDN
- utvikling av nett-teknologi i nær framtid

Programmet kjem til hausten.

Påmelding

Påmelding til UNINETT'95 vil bli kunngjort etter somarferien. Det vil bli høve til å melda seg på både ved e-post, papir-post og via ei WWW-side. Påmeldingsskjema og nærmare annonsering vil bli sendt ut til alle UNINETT medlemsinstitusjonar.

Invitasjon til foredrag

Det går ut ein invitasjon til dei som ønskjer å halda foredrag på UNINETT'95. Alle som ønskjer å bidra til programmet kan senda inn eit samandrag på ei side av foredrag innanfor eitt av dei fem hovudemna innan 10. mai.

Ta kontakt med programkomiteen på

uninett95-pgk@uninett.no

for meir informasjon.

Meir informasjon

Meir informasjon om UNINETT'95 konferansen finn du på

http://www.uninett.no/info/uninett95/

Der vil det til ei kvar tid liggja oppdatert informasjon.

Datatilsynet

Informasjon frå Datatilsynet finn du på

http://www.uio.no/~jonnyb/personvern/tilsyn.html

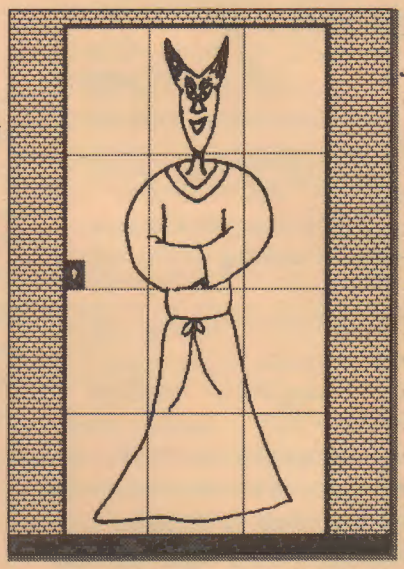
Datatilsynet har der lagt ut mellom anna personregisterlova med forskrifter og kommentarar. I tillegg ligg årsmeldingar og andre forskrifter tilgjengelege.

Hvordan fengsle en demon

Lars Slettjord, Universitetet i Tromsø

Sikring av informasjonstjenester under unix

Nett-tjenester som anonym ftp, gopher og www er oftest implementert som en spesiell type programmer på Unix-maskiner, såkalte demoner (daemons). Disse kjører vanligvis ikke i sikrede omgivelser. Dersom en inntrenger først klarer å komme seg forbi beskyttelsesmekanismene i en slik demon har han fritt spillerom på hele maskinen. Det skal ikke så mye til for å rette på dette. I denne artikkelen vil jeg beskrive hvordan en maskin kan beskyttes mot inntrengere ved å la demoner kjøre i sikrede omgivelser.



Hva er "en sikret omgivelse?"

Når en demon startes vil den vanligvis ha tilgang til hele filtreet på den maskinen der den kjører. Dette er ganske unødvendig siden de fleste demoner bare trenger adgang til noen få systemfiler, samt de datafilene den skal tilby.

Så hvorfor ikke kopiere disse filene ned i en underkatalog og starte demonen på en slik måte at den kun kjenner til denne delen av filtreet? Det er nettopp dette som er essensen av et chroot-miljø (vår sikrede omgivelse). En inntrenger i et slikt miljø vil kun få tilgang til filene i denne underkatalogen. Inntrengeren har ingen mulighet til å gjøre noe med resten av systemet. Og siden det kun er et lite antall systemfiler og verktøy i dette miljøet vil en inntrenger ha veldig lite å jobbe med. Det er i tillegg mulig å begrense anvendeligheten av de verktøy som legges ned i dette miljøet.

Jeg tar for meg en web-tjener (CERN httpd) som et eksempel på hvordan dette gjøres i praksis. Prinsippene som brukes i eksempelet gjelder for de fleste andre unix demoner også.

Aller først må du bestemme hvor i filsystemet chroot-miljøet skal være. Jeg foretrekker å kjøre web-tjeneren fra */usr/local/www*, så da kopierer jeg web-tjeneren til */usr/local/www/etc/httpd*.

Konfigurering av demonen

Demoner skal ikke kjøres som bruker root. Lag en bruker (www) og en gruppe (wwwadmin) med så få privilegier som mulig og kjør demonen som denne brukeren. For å få CERN httpd til å kjøre som bruker www med gruppe wwwadmin legges de følgende inn i */etc/httpd.conf*:

```
UserId www
GroupId wwwadmin
```

Merk at bruker www ikke skal eie filer i chroot-miljøet, det bør root eller andre brukere gjøre. Dermed vil en inntrenger ikke være i stand til å slette/endre filer.

Siden demonen nå har fått en ny root-katalog må en også huske på å endre alle parametre med sti-informasjon i konfigurasjonsfilen. Der en f.eks før brukte `'Pass /* /usr/local/www/htdocs/*'` må en nå bruke `'Pass /* /htdocs/*'`.

Hvordan finne systemfilene demonen trenger

En demon er som nevnt avhengig av et lite sett med systemfiler. Det er mulig å gjøre dette settet mindre ved å linke demonen statisk under kompileringen. Dersom du ikke har mulighet til dette må du finne ut hvilke bibliotek demonen er avhengig av og kopiere disse ned i chroot-miljøet. På noen systemer (sun og linux) finnes kommandoen ldd som viser hvilke bibliotek kjørefilen til en demon er avhengig av. Dersom du ikke har ldd kan du isteden prøve å starte demonen med kommandoen `'chroot /usr/local/www /etc/httpd'` og se hvilke feilmeldinger du får. Hvis demonen da ikke finner *dld.sl* kopierer du */lib/dld.sl* til */usr/local/www/lib/dld.sl*. Gjenta så dette til alle bibliotek er på plass.

Web-demonen er også avhengig av noen filer fra */etc* katalogen. Den trenger *resolv.conf* for å finne DNS tjeneren slik at den kan finne navnet til en maskin ut fra IP adressen. Den trenger *services* for å finne portnummer og protokoll til en gitt tjeneste. Her kan du godt kutte ut tjenester som ikke skal brukes. Den trenger *group*, men her bør du kun ta med de gruppene som skal brukes i dette miljøet.

Den trenger også *passwd* filen, **men den må aldri kopieres rett over fra /etc/passwd**. Lag en ny passordfil og sørg for at

1. bare nødvendige brukere (root og www) er med.
2. passordfeltet settes til * slik at ingen kan knekke passord dersom de får tak i filen.
3. brukerne ikke har noe login-shell. Sett feltet for login-shell til */bin/false*

Her er et eksempel på en slik minimal passordfil:

```
root:*:0:3::/:/bin/false
www:*:201:15:Web tjener,,,:/usr/
    staff/www:/bin/false
```

Demonen trenger også */dev/tty* og */dev/null* (eventuelt */dev/zero*). Disse filene kan ikke kopieres over, men må lages med kommandoen `mknod`. For å lage en slik spesialfil trenger du å vite 'major' og 'minor' 'device number', samt hvilken type fil som skal lages. Denne informasjonen varierer fra system til system, du finner den ved å liste ut originalfilen på denne måten:

```
rincewind:~> ls -l /dev/null
crw-rw-rw- 1 root sys 1, 3 Nov 30 1993 /dev/null
```

filtype major minor

Her blir kommandoen 'mknod /usr/local/www/dev/null c 1 3'. Manualfilene til systemet du sitter på vil gi mer informasjon.

Her er et eksempel (fra HP-UX) på hvordan filstrukturen i /usr/local/www/ kan se ut:

bin/false	No login
cgi-bin/	Katalog for cgi-script
dev/null	Søppelbøtte
dev/tty	
etc/group	Dummy versjon. Bør kun inneholde aktuelle grupper.
etc/passwd	Kun bruker root og www bør være med. Og det krypterte passordet erstattes med '*'
etc/resolv.conf	For oppslag i DNS
etc/services	Port 80 bør være definert som http
etc/httpd.conf	Konfigurasjonsfil for web-tjeneren
etc/httpd	Kjørefilen til web-tjeneren
icons/	Ikoner som tjeneren bruker
logs/	Loggfiler fra tjeneren
htdocs/	Her legges HTML dokumentene
lib/dld.sl	Diverse bibliotek
lib/libc.sl	

Start av demonen

For at gruppe staff skal være i stand til å starte web-tjeneren dersom noe går galt har jeg laget et lite c-program som setter opp et minimalt miljø og starter tjeneren. Den ferdige kjørefilen har jeg lagt under /usr/etc/httpd-start, og den har gruppe staff og er setuid root.

```
#include <sys/types.h>
#include <sys/stat.h>
#include <fcntl.h>
```

Dette bestemmer hvor i chroot-miljøet tjeneren skal lete etter kjørbare programmer. Det bør være så få steder som mulig.

```
char *env[] = {
    "PATH=/bin:/usr/etc",
    (char*)0
 };
```

Bestemmer hvordan tjeneren skal startes. MERK! chroot kommandoen kan ligge andre steder på andre systemer. Det er også mulig å legge til flere argumenter, f.eks -restart

```
char *argv[] = {
    "/etc/chroot",
    "/usr/local/www",
    "/etc/httpd",
    (char*)0
 };
main()
{
    int std;
    setuid(geteuid());
    umask(022);
```

Sender stdin, stdout og stderr til /dev/null. Output kan like gjerne sendes til en loggfil, men i utgangspunktet har jeg ikke behov for det.

```
    if ((std = open ("/dev/null",
    O_WRONLY, 0)) == -1)
    perror("argv[0]: could not open
    /dev/null");
    close(0);
    dup(std);
    close(1);
    dup(std);
    close(2);
    dup(std);
    close(std);
    execve("/etc/chroot", argv,
    env);
}
```

Selv om det er mulig å starte tjeneren fra inetd vil jeg anbefale å starte web-tjeneren som 'standalone' fra */etc/rc.local* eller tilsvarende. Legg til følgende linjer:

```
# Start av web-tjener
if [ -x /usr/local/www/etc/httpd -a
-x /usr/etc/httpd-start ]; then
    /usr/etc/httpd-start
fi
```

Script og annet

Muligheten for å kjøre cgi-script som behandler input fra en bruker er en av de virkelig gode egenskapene med web, men det er også den største sikkerhetsrisikoen. Det er veldig lett å gjøre feil i behandlingen av argumentene til et cgi-script. Behandlingen av disse argumentene krever egentlig en egen artikkel, men kort sagt går den ut på å sjekke argumentene for farlige 'characters' før de brukes. Dette inbefatter semikolon (;), slash (/), tilde (~), utropstegn (!), quote ("), backtic (') ,komma (,), og punktum (.).

Referanser

- *Securing Internet Information Servers* (1994), CIAC-2308 R.2 som er tilgjengelig via ftp://ciac.llnl.gov/-pub/ciac/ciacdocs/. Dette dokumentet gir mer informasjon om sikring av ftp, gopher og web-tjenere.
- *Firewalls and Internet Security : repelling the wily hacker* William R. Cheswick, Steven M.Bellovin. ISBN 0-201-63357-4
- Man-sider for chroot, mknod, setuid, execve
- Dokumentasjonen til CERN httpd som er tilgjengelig fra http://www.w3.org/hypertext/WWW/Daemon/Status.html

Statistisk Sentralbyrå

Statistisk Sentralbyrå har lagt ut informasjon og enkelte statistikkar på

http://www.ssb.no/

Kryptering

Thomas Øhrbom, UNINETT sekretariat

Innledning

Kryptering vil si det å gjøre data uleselige for enhver som ikke har en hemmelig dekrypteringsnøkkel. Formålet med kryptering er å sikre at dataene forblir skjult for alle uvedkommende, inkludert dem som har adgang til de krypterte dataene. I datakommunikasjon kan kryptering benyttes for å oppnå sikker kommunikasjon over et usikkert medium. F.eks kryptering av elektronisk post.

Det er alltid viktig å ta standpunkt til om man virkelig har behov for å benytte kryptering, og i såfall i hvilken grad. De fleste brukere har svært sjelden noe reelt behov for å kryptere meldinger eller filer.

Symmetrisk kryptering (privat-nøkkel kryptering)

I et symmetrisk kryptosystem benyttes samme nøkkel til kryptering og dekryptering. Dersom du skal benytte symmetrisk kryptering i forbindelse med datakommunikasjon krever dette deling av en hemmelighet, dvs. krypteringsnøkkelen. Problemet blir da sikker overføring av den hemmelige nøkkelen til alle involverte parter før utvekslingen av krypterte data kan begynne.

Symmetriske krypteringsalgoritmer er generelt mye raskere enn asymmetriske algoritmer. Den mest velkjente symmetriske krypteringsalgoritmen er DES (Data Encryption Standard).

Ved overføring av store datamengder er det, pga hastigheten, anbefalt å kryptere dataene med en symmetrisk algoritme (f.eks DES), for så å foreta utvekslingen av DES nøkkelen vha en melding kryptert med offentlig-nøkkel kryptering.

Asymmetrisk kryptering (offentlig-nøkkel kryptering)

I offentlig-nøkkel kryptering består en nøkkel av to deler, en offentlig og en privat. Disse er delene kalles ofte offentlig nøkkel og privat nøkkel. Den offentlige nøkkelen kan du fritt distribuere til alle og enhver. Den private nøkkelen må holdes hemmelig. All kommunikasjon involverer bruk og overføring av den offentlige nøkkelen. Den private nøkkelen blir aldri overført. Man er altså ikke avhengig av sikker utveksling av nøkkel som ved symmetrisk kryptering. En annen stor fordel med offentlig-nøkkel kryptering er at man enkelt kan generere digitale signaturer.

RSA er pr idag en tilnærmet de facto standard innen offentlig-nøkkel kryptering. RSA ble oppfunnet i 1977 av Ron Rivest, Adi Shamir og Leonard Adleman. Pretty Good Privacy (se artikkel) er basert på RSA.

Slik fungerer offentlig-nøkkel kryptering:

- A ønsker å sende en kryptert melding til B.
- A får tak i B's offentlige nøkkel.
- A krypterer så meldingen med B's offentlige nøkkel og sender meldingen til B.
- B bruker så sin private nøkkel til å dekryptere meldingen.

På denne måten kan hvem som helst med adgang til B's offentlige nøkkel sende en kryptert melding til B, men bare B kan dekryptere disse meldingene.

Digitale signaturer

Digitale signaturer benyttes for å verifisere dataintegritet og for autentisering. En digital signatur kan ikke forfalskes, og et signert dokument kan ikke forandres uten at den digitale signaturen samtidig blir ugyldiggjort. En digital signatur bekrefter at en navngitt person har skrevet og/eller godkjent et dokument. Dokumentet kan være en fil eller en epost melding.

Mottakeren kan verifisere at dokumentet virkelig er skrevet av den som underskrev det, samt at dokumentet ikke er blitt forandret siden det ble underskrevet.

Slik fungerer digital signatur med offentlig-nøkkel kryptering: A ønsker å sende en signert melding til B. A genererer en digital signatur vha sin private nøkkel og selve meldingen som skal signeres. Den digitale signaturen hektes så på meldingen, og meldingen sendes til B. B benytter så A's offentlige nøkkel, selve meldingen og den digitale signaturen for å verifisere at det virkelig er A som har signert meldingen, og for å sjekke at ingen har forandret på innholdet i meldingen.

Det er fullt mulig å både kryptere en melding og å signere den med en digital signatur. Da oppnår man å sikre både autentisering, dataintegritet og konfidensialitet.

Definisjoner

Dataintegritet: Dataintegritet er den egenskapen at data ikke er blitt ødelagt eller endret på en ikke-autorisert måte. Ved datakommunikasjon bør mottageren være i stand til å oppdage om meldinger er blitt endret ved at aktivt inngrep eller ved et uhell. På et stadium må informasjonen forsegles slik at enhver påfølgende endring vil oppdages. Når vi verifiserer dataintegritet forsikrer vi oss om at det ikke har skjedd endringer i informasjonen etter at denne ble forseglet.

Autentisering: Autentisering er en mekanisme for verifisering av identiteten til en entitet (f.eks. en bruker du utveksler kryptert epost med) ved hjelp av informasjons utveksling.

Konfidensialitet: Konfidensialitet er den egenskapen at informasjon ikke blir gjort tilgjengelig, eller ligger åpen, for ikke-autoriserte personer, prosesser eller entiteter.

Referanser

D.Denning, *Cryptography and Data Security*, Addison-Wesley Publishing Company, 1982

R.L. Rivest, A. Shamir, and L. Adleman. *A method for obtaining digital signatures and public-key cryptosystems*. Communications of the ACM, 21(2):120--126, February 1978.

WWW sikkerhetsside: http://domen.uninett.no/~ohrbom/sikkerhet.html Her finner man linker til relevante newsgrupper, FTP sites, WWW sider, FAQ'er (Frequently Asked Questions) og Gopher sites.

UNINETT har en sikkerhetspolicy

Alf Hansen
UNINETT sikkerhetsansvarlig

Som kjent har UNINETT prioritert sitt arbeid med sikkerhetsproblematikk, og en overordnet sikkehetspolicy er nå formelt godkjent som et UNINETT Notat (UNOT-95-001). Notatet kan hentes ved

ftp://aun.uninett.no/drifts-data/sekr/arkiv/notater/unot-95-001.sikkerhetspolicy

UNINETTs sikkerhetspolicy skal bidra til at sikkerheten i UNINETT oppfyller kravene til UNINETT, medlemsinstitusjonene, og brukerne.

"Sikkerhet" i denne sammenheng omfatter beskyttelse av lokale og sentrale nettverksressurser mot bevisste handlinger som tar sikte på å oppnå uautorisert adgang til informasjon i UNINETT og hos institusjoner tilknyttet UNINETT, forringe nettverkstjenestene, true integritet eller konfidensialitet.

I notatet blir ansvarsfordelingen definert mellom brukere, tilknyttede medlemsorganisasjoner, UNINETT, leverandører av utstyr (som brukes i eller tilknyttes nettet) og samtrafikkpartnere.

Det beskrives hvordan UNINETT organiserer sin sikkerhetsaktivitet med en ansvarlig sikkerhetskoordinator som leder UNINETT CERT (CERT=Computer Emergency Response Team). UNINETT CERT er et knutepunkt for innrapportering og spredning av informasjon i forbindelse med sikkerhetshendelser. UNINETT CERT vil være ett ledd i en internasjonal ring av tilsvarende grupper som hver for seg følger opp sikkerhets-spørsmål innen sine respektive nett. Sammen fungerer disse som et internasjonalt kontaktnett for håndtering av sikkerhetshendelser som har forgreninger over landegrensene.

Ved hver medlemsinstitusjon skal det finnes en person som har som oppgave å være UNINETT sikkerhetskontakt. UNINETT skal gi medlemsinstitusjonene råd om utformingen av deres egen sikkerhetspolicy.

Informasjon om sikkerhetskravene og sikkerhetsnivået i UNINETT vil være åpent tilgjengelig for alle. Tre sikkerhetsklasser er definert: HEMMELIG (helseopplysninger og tilsvarende), FORTROLIG (administrativt fortrolig) og ÅPEN (åpen informasjon). Hver klasse vil ha definerte krav som må være oppfylt. Kravene og de tekniske løsningene skal være godkjent av Datatilsynet. Klassene er foreløbig et rammeverk. UNINETT arbeider videre med å utarbeide detaljene i dette.

UNINETT har rett til å avstenge tilknyttede medlemsinstitusjoner fra UNINETT dersom tilknytningen representerer et sikkerhetsproblem for UNINETT, og institusjonen ikke er i stand til eller villig til å foreta de nødvendige tiltak i denne forbindelse.

Når UNINETT tegner avtaler med andre parter om drift, overvåkning eller andre tjenester som har betydning for UNINETTs funksjonalitet eller sikkerhet, skal avtalen regulere ansvarsfordelingen for sikkerheten, og slå fast hvilke krav UNINETT stiller til sikkerhetsnivå og tiltak.

Som nevnt er dette en overordnet sikkerhetspolicy som setter rammene for videre arbeid. UNINETT har igangsatt og planlegger en rekke utviklingsprosjekter som arbeider videre med å sikre bruken av nettet. Vi deltar i et konsortium innen telematikkprogrammet i EUs 4. rammeprogram, og dette gir oss (hvis programmet blir tildelt EU-midler) mulighet til å gjøre mer enn vi ellers kunne gjort uten disse midlene. Internasjonalt samarbeid innen sikkerhet er en nødvendighet siden angrep på ressurser i nettet som kjent ikke lar seg stoppe av landegrenser. Deltakelse i EUs rammeprogram vil gi oss verdifulle kontakter og impulser som kommer hele UNINETT miljøet til gode.

Medlem i UNINETT

Medlemstalet i UNINETT aukar sterkt, særleg gjeld dette for skulesektoren. For eit år sidan var ingen skular tilknytta UNINETT, no er til saman 90 lågare grads skular medlem i UNINETT.

Totalt hadde UNINETT 27. mars 294 medlemsinstitusjonar. Av desse var 95 forskingsinstitusjonar og 53 høgskular (under høgskulane høyrer dei 98 høgskulane som blei omorganiserte til 26 høgskular i 1994).

Passord

Dei aller fleste brot på tryggleik skjer ved at nokon misbruker passord. Det er viktig at ingen andre enn du sjølv har tilgang til ditt passord. Dersom ingen andre skal ha tilgang, må passordet vera slik at det heller ikkje er lett å gjetta.

- **skift passord regelmessig**, minst ein gong i året
- **skriv aldri ned passord** på ein gul lapp
- **del aldri passord** med nokon
- **oppgje aldri passord** til nokon som spør
- ikkje lag deg eit passord som er så kryptisk at du må skriva det ned
- ikkje lag deg eit enkelt passord (eit ord eller namn, breuk minst eitt spesialteikn)
- dersom du somlar bort passordet eller gløymer det, spør IT-ansvarleg om eit nytt, skift dette passordet første gongen du loggar deg inn
- bruk ulike passord på ulike maskiner
- skift ikkje passord så ofte at du ikkje hugsar det (det ender ofte opp på ein gul lapp klistra til skjermen)

UNINETT og PEM

Harald Tveit Alvestrand, UNINETT sekretariat

UNINETT har våren 1995 kjørt prosjektet "Sertifiseringshierarkier" ved Norsk Regnesentral.

Prosjektet var ment å gi svar på spørsmålene:

- Kan jeg stole på at den informasjonen jeg mottar er fra den som gir seg ut for å ha sendt den?
- Kan jeg stole på at det jeg mottar er det avsender sendte?
- Hvordan vet jeg at jeg kan stole på det jeg mottar?

Muligheten for svar på disse spørsmålene ligger i teknologien som kalles sertifisering (se artikkel om kryptering).

Signert E-post: PEM og PGP

Det finnes flere programmer som gir deg tilgang til de mulighetene du får med sertifikater.

To av de viktigste er PEM (Privacy Enhanced Mail) og PGP (Pretty Good Privacy). Disse to har omtrent samme funksjonalitet i det å signere og/eller kryptere meldinger, men PEM har gått atskillig lengre når det gjelder å etablere prosedyrer og formater som tillater oppbygning av et kontrollerbart, hierarkisk system for å verifisere signaturer, mens PGP baserer seg på signering av sertifikater brukere i mellom, uten etablerte mekanismer for å finne noen som kan garantere for den som har signert signaturen.

En annen forskjell er at PGP er et program, mens PEM er en standard; det finnes flere forskjellige programmer som kan "snakke PEM", og spesifikasjonene er utarbeidet av en åpen arbeidsgruppe og publisert som RFCer i Internet, mens alle versjoner av PGP stammer opprinnelig fra den samme kildekoden, og alle bestemmelser om meldingsformater og så videre er tatt av en enkelt person, Phil Zimmermann.

PEM i praktisk bruk

Norsk Regnesentral har utviklet en innbygging av PEM programvare i E-post programmet Z-Mail for Unix og DOS.

Om ønskelig kan sikkerheten gjøres bedre ved at hemmelig nøkkel lagres kryptert på et smartkort; dette er enda for dyrt til å bruke i stor skala, men ventes å bli betraktelig billigere i løpet av året.

Hva som enda mangler

PEM er enda ikke helt klar til bruk i UNINETT. Det som mangler er infrastrukturen: Vi må etablere de databasene og rutinene som tillater oss å gi alle som ønsker det et sertifikat, og å la alle som ønsker det få tilgang til sertifikatene. Disse vil trolig bygge på X.500 katalogen.

Vi håper å ha rutinene på plass slik at organisasjoner som ønsker å gi sine brukere sertifikater vil kunne gjøre dette i løpet av sommeren 1995.

Andre prosjekter prøver å utbre samme typen infrastruktur i Europa, slik at en kan få tilsvarende funksjoner over hele Internet. Inntil disse er etablert er det antagelig enklest og best å basere seg på PGP (se PGP artikkel).

Pretty Good Privacy

Thomas Øhrbom, UNINETT sekretariat

PGP står for Pretty Good Privacy, og ble opprinnelig skrevet at amerikaneren Philip Zimmermann. PGP er pr idag på god vei til å bli en de facto standard for ikke-kommersiell kryptering. PGP er såkalt freeware, du trenger altså ikke å betale for å bruke PGP. Forutsetningen er at du ikke benytter PGP i kommersiell virksomhet. Siste versjon av PGP er pr idag er 2.6.i (internasjonal versjon, grunnet eksportrestriksjoner på kryptering i USA).

Det vanligste bruksområdet for PGP er kryptering av epostmeldinger. Men man kan også benytte PGP i annen datakommunikasjon, og til kryptering av filer. Det er utviklet en del PGP applikasjoner. Disse applikasjonene er freeware og finnes tilgjengelig på nettet. Ta utgangspunkt i referansene i denne artikkelen.

PGP har flere klare fordeler:

- PGP er svært sikkert. PGP algoritmen er tilnærmet umulig å knekke. Kildekoden og algoritmen til PGP er tilgjengelig og PGP's sikkerhet er blitt verifisert en rekke ganger.

  Du kan selv velge hvor stor nøkkel du benytter, og jo større nøkkelen er desto mer sikker er PGP. Største mulige nøkkel er nå på 2048 bits.
- PGP er tilgjengelig på en rekke maskin plattformer, bl.a. MS-DOS, UNIX, OS/2, Amiga, Atari, Mac og Archimedes.
- PGP kan generere digitale signaturer (se krypto artikkel)
- PGP er basert på RSA, en offentlig-nøkkel krypteringsmetode (se krypto artikkel). Dette gjør utveksling av hemmelige meldinger lettvint og greit. Enhver som har fått din offentlige nøkkel kan uten noen forhåndsavtale sende deg en kryptert melding som bare du selv kan lese.
- En annen fordel med PGP er at det er relativt enkelt å bruke, og flere epost-klienter har eller kan utstyres med PGP støtte. Dette gjelder blant annet Pine, Z-mail og Exmh.

PGP har også et par klare ulemper:

- PGP mangler støtte for organisert sertifiseringshierarki. Du er avhengig av å selv spre din offentlige nøkkel, eller benytte en nøkkelserver (Universitetet i Tromsø har startet opp Norges første offisielle PGP nøkkelserver http://www.uit.no/pgp/servruit.html).
- Autentisering av nøkler er et annet problem. Så sant du ikke får personlig overrakt en offentlig nøkkel kan du ikke være 100 % sikker på at den tilhører den personen som den utgir seg for å tilhøre. Man kan i PGP definere i hvilken grad man stoler på en offentlig nøkkel.

Referanser:

Ståle Schumacher : http://www.ifi.uio.no/~staalesc/PGP/

Min egen PGP side:
http://domen.uninett.no/~ohrbom/pgp/pgp.html

UiT's nøkkelserver: http://www.uit.no/pgp/servruit.html