UNINETT
Nyhetsbulletin
UNINyTT
Nr 4 1996

Beskyttelse

Hvem har ansvaret for at du og dine (brukere) er beskyttet? Hvordan kan en bruker unngå å drukne i informasjonsflommen på Internett? Hva er uønsket informasjon på institusjonsnivå og for hver enkelt bruker?

Internett er sammensatt av mange ulike tjenester, og disse krever ulike tiltak for å gi trygge omgivelser. Hva som er en trygg omgivelse vil variere sterkt, et forskningsinstitutt som er åpent og består av bare voksne mennesker har en helt annen definisjon av trygt enn en barneskole eller et folkebibliotek.

Definisjonen på hva som institusjonen ønsker skal være trygt vil påvirke de tiltak som igangsettes. Dersom alt av informasjon er åpent, er det sløseri å bruke ressurser på å beskytte seg mot innbrudd. Dersom personalsystemet ikke skal kunne endres av hvem som helst, må dette beskyttes.

IT-drift har stadig utfordringer med å oppgradere og tilrettelegge slik at programvare ikke medfører sikkerhetsrisiko for institusjonen. For at et system skal være sikkert, må det følges opp jevnlig og man må holde seg oppdatert på hvilke problemer som er oppdaget.

Det vanskeligste i hverdagen kan være å beskytte seg mot den flom av informasjon som eksisterer på Internett, å unngå alt det man ikke er interessert i å kaste bort tid på. Flere artikler i dette bladet går igjennom hvordan man kan filtrere bort uønsket eller uinteressant informasjon og hvilke tiltak som kan iverksettes.

Arbeidet med å definere hva som er uønsket informasjon kan oppleves som stort, men dersom institusjonen har nytte av å sile vekk informasjon, kan det være verdt bryet å tenke gjennom problemstillingene. Uinteressant informasjon er en problemstilling som går direkte mot den enkelte bruker, og variasjonene i hva som er interessant er store. For forskning og utdanning er det store variasjoner i hva som er relevant for hvert enkelt fagområde. Ting som mange vil oppfatte som uviktig kan være svært viktig for enkelte forskere. Dette gjør at UNINETT ønsker at hver enkelt forsker skal ha tilgang på relevant informasjon, noe som bare kan realiseres ved at UNINETT er så åpent som norsk lov tillater.

Det er viktig at styringen med hva som er ønsket informasjon ligger så nært brukeren som praktisk mulig. Dersom institusjonen ønsker å begrense adgang til enkelte typer tjenester eller deler av tjenester, bør dette dokumenteres i brukeravtaler. Brukere vil kunne skaffe seg tilgang til materiale som er uønsket ved institusjonen ved å bryte retningslinjer og gå utenom tekniske sperrer, dette gjør retningslinjene viktige og det bør gå klart fram av disse hva konsekvenser av overtredelser kan bli.

Innhald

Hovudemnet for dette nummeret er kva kvar enkelt institusjon kan gjera for å filtrera ut uønska informasjon.

Institusjonane har ansvar for å setja opp retningslinjer og velja kva som skal vera tilgjengeleg for sine tilsette og studentar.

Utgiver av UNINyTT er
UNINETTs sekretariat
Postboks 6883 Elgeseter
7002 Trondheim
Redaktør: Ingrid Melve
Telefon: 73 59 29 80
Epost: uninytt@uninett.no

Sperring av trafikk i rutere

Hva gjør et IPpakke-filter i en ruter?

IP-pakkefiltre skal normalt søke å avgrense flyten av IP-pakker til gitte subnett, bare pakker som kommer fra riktig adresserom får lov til å gå inn på avsperrede tjenester og/eller nett.

KOMPAKT

I forbindelse med KOMPAKT prosjektet har nettet på de regionale høgskolene blitt omstrukturt og segmentert i ulike sikkerhetsnivåer med studenter på ett segment, administrasjon/ansatte på eget segment. Ruterene vil få lagt inn filter som sikrer at bare administrasjonen har tilgang til f.eks lønnssystem. Sikkerhet for administrasjonen har vært det viktigste, administrasjonen skal være sikret mot angrep utenfra og innenfra (f.eks. studenter).

Kostnader

En kostnad ved å installere filter i rutere kan være at trafikken går langsommere dersom ruteren har for liten pakkeprosesseringskapasitet, spesielt hvis aksesslistene er omfattende og hastigheten på sambandet stort. KOMPAKT-prosjektet har oppgradert store deler av ruterparken ved høgskolene til å kunne tåle denne ekstra belastningen. Hver eneste pakke som er innom ruteren må sjekkes mot alle filtreringsregler som er etablert før man sender pakken videre til riktig mottaker. Dette er en arbeidskrevende jobb for ruteren.

Filterspesifikasjonen kan lett bli stor og tung å vedlikeholde og forutsetter inngående kjennskap til protokollene ovenfor IP-laget. **En** feil er nok til at sikkerheten ikke lenger er slik den burde være. Derfor er det viktig at man først stabiliserer tjenesteinfrastrukturen med hensyn på i hvilke subnett tjenestene (DNS, epost, web, databaser o.l.) skal ligge.

Spesialisert kompetanse er en av grunnene til at man i KOMPAKT har valgt å legge filter i rutere som en sentralisert oppgave. Det forutsettes også god kunnskap om den aktuelle rutertypen før man kan legge inn filter.

Det er liten hensikt med en spesiell brannmurløsning før de underliggende infrastrukturen og segmentering er på plass. Løsningen reduserer kapasiteten i nettet og er arbeidskrevende å drive.

En ruter med pakkefiltrering er egentlig også en brannmur, men krever lite adminsitrasjon

Sikring av rutere og sikring ved hjelp av rutere

Aktuelle tiltak som iverksettes for å sikre rutere og sikre andre nettressurser ved hjelp av rutere kan være:

- Avlåsing av rom og nøkkeladministrasjon
- Selektiv kabling og segmentering av nett for ulikt personell og/eller studenter,
- Aksesslister for pålogging til rutere
- Anti-IP-spoofing pakkefiltre
- Adgangsbegrensing til nettressurser/maskiner ved hjelp av pakkefiltre
- Sikker utveksling av rutingsinformasjon
- Oppgradere/bytte ruterteknologi

Mange av disse tiltakene er i dag gjennomført i UNINETTs infrastruktur.

Bruk av ruter som brannmur kombinert med en fornuftig organisering av tjenesteinfrastruktur er et optimalt kompromiss mellom høy sikkerhet, ytelse og pris.

Pris på ISDN tilknytning går ned

Informasjon om nye prisar for tilknyting til Internett over ISDN er tilgjengeleg på

http://www.uninett.no/uks/lan/pris-lan.html

Den årlege ISDN tenesteavgifta har gått ned, det same har etableringsavgifta for tilknyting.

Redaktørhjørnet

Styggedom

All styggedomen som er i verda lar heller ikkje Internett vera i fred, sjølv om enno ingen har blitt overkøyrd av nett-tenester (det nærmaste eg har kome fysisk skade, var då eg snubla i ein nettkabel som låg og slang).

Forskjellen mellom det miljøet vi er vant til og Internett er at vi i mykje større grad kan velja kva informasjon vi ønskjer å motta.

Intelligente hjelparar og agentar

Mekanismane for å velja tenester og kva deler av tenester ein skal bruka har blitt stadig betre, men framleis er det eit stykke igjen. Eit steg på vegen framover er tenester som på oppdrag frå meg vel ut informasjon og presenterer resultatet til meg når eg har tid og høve til å sjå på det. Stadig fleire slike intelligente agentar er tilgjengelege på web.

Ulempa med intelligente agentar er at dei gjer det dei får beskjed om. Fordelen er at dei gjer det dei får beskjed om. Eit menneske som gjer same jobben (noko som ville blitt dyrt for meg) ville vera i stand til å fylgja opp relaterte emne som såg interessante ut, litt på same vis som journalistar arbeider i dagens aviser og radio/fjernsyn.

Nøye på kva du gjev frå deg, tolerant med kva du mottar?

Eit grunnleggjande prinsipp for den tekniske sida av tenestene har vore at ein skal vera nøye på kva ein sender frå seg, og tolerant med kva ein mottar. Det kan vera at dette også er fornuftig når ein ser på innhaldet i tenester, at ein ikkje godtar kva som helst i eigne rekkjer.

Eit år med CERT

Ansvarleg for CERT er Alf Hansen. Her kjem eit intervju med han om kva som har vore dei viktigaste sakene for UNINETT CERT i året som gjekk.

Kva er UNINETT CERT?

UNINETT CERT (*Computer Emergency Response Team)* tar imot meldingar om angrep frå interne og eksterne kjelder. Trusselnivået blir vurdert i kvart enkelt tilfelle, og oppgåvene for utføring av eventuelle tiltak blir fordelt til ressurspersonar i tilknyting til UNINETT.

Alle medlemsinstitusjoner i UNINETT har ein tryggleiksansvarlig. Alle medlemsinstitusjoner i UNINETT har sjølv ansvar for den interne sikkerheten i sine system.

Meir informasjon om UNINETT CERT er tilgjengeleg på

http://www.uninett.no/info/cert/home.html
Epost: cert@uninett.no
Telefon: 73 59 29 80

CERT skal vera ei hjelp for lokal IT-ansvarleg og tryggleiksansvarleg, ikkje for den enkelte brukar.

Brukarar skal ta kontakt med lokal IT-drift dersom dei har grunn til å tru at det har oppstått hendingar relatert til tryggleik.

Kva er typiske saker for CERT?

- Ulovleg spreiing av kommersiell programvare
- I det siste har kjedebrev og liknande breidd om seg, sjølv om det stort sett har vore same saka har fleire institusjonar vore involvert.
- Innbrot er ei problem. Mellom anna har det vore fleirstegs innbrot der ei kjede av maskiner plassert rundt om i landet (også i utlandet) har vore utsett for innbort.
- Endring av data er eit anna problem, enkelte bryt seg inn på maskiner for å endra t.d. websider.
- Klage på epostmeldingar kan koma innom CERT.

Kva med dette som alle avisene skriv om: porno

Det har stort sett vore annonsering av porno og ikkje direkte ulovleg porno som har blitt tatt opp, men det har vore lasta ned ulovleg porno via UNINETT og då tok den institusjonen der brukaren sat kontakt for å få vita kva tiltak UNINETT har sett i verk på området. Meir informasjon om dette kjem i neste UNINyTT.

Kva er CERT si viktigaste oppgåve?

CERT prioriterer å få fram fakta om hendingar, slik at ein kan iverksetja tiltak for å tetta eventuelle hol i tryggleiken og forfølga saka. Ved straffeforfølging er det opp til kvar enkelt institusjon å melda saker til politiet. Dersom UNINETT sine system blir utsett for kriminelle handlingar, vil UNINETT melda dette til politet.

Koordinering av innsats ved hendingar som involverer fleire institusjonar eller fleire nettverk er viktig, nasjonalt og internasjonalt.

Du nemner internasjonal koordinering, er det ein europeisk CERT?

Ikkje enno, men TERENA (den europeiske akademiske nettorganisasjonen) arbeider med å etablera eit europeisk koordineringssenter. Eit slikt senter vil bli eit stort skritt framover.

Skal ein melda frå om hendingar som skjer lokalt?

Det er fint å få beskjed sidan det som skjer lokalt kan vera del av eit større mønster. Dei som melder frå veit ofte ikkje korleis dei skal takla situasjonen, CERT har som regel hatt liknande saker og kan hjelpa til med råd.

UNINETT har utarbeidet retningslinjer for aktsomhet, der det klargjøres hvilket ansvar UNINETT mener å ha. Det er opp til hver enkelt institusjon å sette opp egne retningslinjer og kunngjøre disse for ansatte og studenter.

UNINETT retningslinjer for aktsomhet (UNOT-95-008)

Det er i dag ikke klart hvilke juridiske retningslinjer som vil gjelde i fremtiden for Internet i Norge.

Inntil slike regler er kjent vil UNINETT praktisere følgende retningslinjer:

1. UNINETT tar intet ansvar for innhold i data som formidles over UNINETTs linjenett fra eller til steder utenfor UNINETTs kontroll.
2. UNINETT tar intet ansvar for innhold i data som formidles direkte fra person til person (eks e-post), selv om dette blir mellomlagret midlertidig på UNINETTs utstyr.
3. UNINETT vil søke å følge et generelt aktsomhetsprinsipp når det gjelder ting som gjøres offentlig tilgjengelig gjennom UNINETTs utstyr (f.eks. News).
4. UNINETT står ansvarlig for det UNINETT har skrevet og gjort tilgjengelig (f.eks. UNINETTINFO)

Med generell aktsomhet menes i dette tilfelle:

1. UNINETT vil søke å fjerne materiale som åpenbart er i strid med norsk lov.
2. Dersom UNINETT blir gjort oppmerksom på materiale som er i strid med norsk lov, vil UNINETT forsøke å fjerne dette fra UNINETTs utstyr.

UNINETT tar ikke på seg noe ansvar for å sjekke alt som formidles via UNINETT utstyr.

News, diskusjonsgrupper

Mads Eilertsen, tjenesteansvarlig News

Avgrensing av News

Når det gjelder hvilke newsgrupper/-hierarkier som spres til medlemsinstitusjonene med egen newstjener er det institusjonene selv som forteller oss hva de ønsker tilsendt. Noen vil ha alle grupper, mens andre har bedt om f.eks. ikke å få alt.binaries.*.

Medlemsinstitusjonene kan også be om at deres leseadgang på UNINETTs egne newstjenere begrenses. Dette ble presisert for medlemmene i UNINYTT nr. 2 1996. Der ble det også opplyst at institusjoner som ønsker å gjøre slike avgrensninger kan henvende seg til

news-hjelp@uninett.no

Grupper som er sperret

UNINETT har fjernet en del grupper som åpenbart er i strid med norsk lov fra sine servere. Det betyr i praksis også at gruppene ikke blir videreformidlet til andre fra oss. Her er *noen* av gruppene som ikke tas inn:

alt.binaries.multimedia.erotica
alt.binaries.pictures.erotica.gymnast-girls
alt.binaries.pictures.erotica.male.anal
alt.binaries.pictures.erotica.schoolgirls
alt.binaries.pictures.erotica.spanking
alt.binaries.pictures.erotica.spatch
alt.binaries.pictures.erotica.tasteless
alt.binaries.pictures.erotica.uncut
alt.sex.pedophilia.pictures
alt.sex.animals
alt.sex.balls
alt.sex.bestiality
alt.sex.incest
alt.sex.masturbation.pictures.female.teen
alt.sex.necrophilia
alt.sex.pedophilia
alt.sex.snuff.cannibalism
alt.sex.stories.incest
alt.sex.tasteless
alt.sex.teens

Newsgrupper som er sperret kan være tilgjengelige via andre newstjenere i eller utenfor UNINETT.

Merk at kryssposting (det å poste en newsartikkel til flere grupper) kompliserer bildet noe. En artikkel kryssposted til de to gruppene alt.sex.animals,alt.binaries.pictures.erotica.breasts vil bli formidlet av oss siden vi formidler den siste gruppa. Slikt er det vanskelig å gjøre noe med. For en tid tilbake ble Telenor Online uthengt som "Statens Pornosentral". Dette var basert på innhold i gruppa alt.binaries.misc. Dette høres ut som en uskyldig gruppe, og det meste av det aktuelle materialet var kryssposted der og i "sex-grupper".

Leseadgang på UNINETTs newstjenere

Når det gjelder leseadgang på UNINETTs newstjenere gjelder følgende begrensninger:

Grunnskolene har siden juni 1995 ikke hatt leseadgang til gruppene

alt.sex.*
alt.binaries.pictures.erotica.*

Når det gjelder hvilke newsgrupper/-hierarkier som spres til medlemsinstitusjonene med egen newstjener er det institusjonene selv som forteller oss hva de ønsker tilsendt. Noen vil ha alle grupper, mens andre har bedt om begrensninger.

Noen trekk jeg har observert etter en gjennomgang av mellom annet alt.binaries.pictures.erotica.teen.* er:

- En god del av materialet er reklame (bilder + URL) til firmaer som tilbyr mer materiale.
- Det meste av materialet er bilder av unge mennesker, for det meste kvinner, i mer eller mindre utfordrende posisjoner. Jeg vil tro at det meste av dette ikke er i strid med norsk lov.
- Det hersker en viss selvjustis. I de få tilfeller jeg har sett "dårlige" ting har det blitt kommentert. "Keep this shit out of here".
- Noe av materialet er nok forbudt, men på de gruppene jeg har sett på er det i klart mindretall.
- Det er ikke alltid like lett å forutse innholdet ut fra navnet på newsgruppa.
  På alt.binaries.pictures.erotica.breasts forventet jeg å finne nettopp det ja, men det var stort sett annonser og andre kroppsdeler...

En foreløpig konklusjon på den siste delen er at dette med sperring av newsgrupper basert på innhold ikke er enkelt. Hvis 90% av materialet er OK, 8% greit under tvil og 2% ikke greit, hva gjør vi da?

En av gruppene vi ikke tar imot er alt.sex.incest. For alt jeg vet kan det godt hende at den brukes til å diskutere incest-problemet. Er det riktig av oss ikke å ta den inn? Dette er ikke trivielt!

Jeg mener vi har vist at vi tar problemstillingen på alvor ved at vi

- har fjernet newsgrupper som åpenbart er i strid med loven
- har sperret lesing av "sex/erotikk" for grunnskolene,
- har gjort medlemmene oppmerksom på mulighetene til å velge hva de skal ha adgang til
- prøver å holde et øye med hva som skjer i utvalgte newsgrupper
- lytter når noen forteller oss om ulovlig materiale

UNINETTs web-cache tjeneste

Lars Slettjord, EDB-Sentret - Universitetet i Tromsø

Det er ikke uten grunn at World Wide Web er blitt omdøpt til World Wide Wait. Alle som har surfer på WWW opplever ofte å måtte vente lenge på å få lastet ned dokumenter. UNINETT driver en web-cache tjeneste som kan brukes av alle UNINETT medlemmer, og som kan redusere ventetiden drastisk. UNINETTs web-cache tjeneste er tilgjengelig fra www-cache.uninett.no på port 81.

Dersom din internett forbindelse er overbelastet kan du også redusere trafikken på linjen ved å starte en egen web-cache tjeneste.

Introduksjon til caching av web

Introduksjon til webcaching finner du i UNINyTT 1-96

Policy for bruk av UNINETTs web-cache tjeneste

Alle UNINETT medlemmer har tilgang til web-cache tjenesten. Men dersom en institusjon blir en stor bruker av tjenesten vil vi anbefale at de starter sin egen web-cache tjeneste (mer om dette under).

De som ikke er UNINETT medlemmer vil normalt ikke få tilgang til web-cache tjenesten. Men vi er interessert i å samarbeide med andre web-cache tjenere, så dersom noen utenfor UNINETT driver en egen web-cache tjeneste vil vi kunne tilby en gjensidig avtale med begrenset tilgang.

Konfigurasjon av klienter

Det finnes mange forskjellige web-klienter, og noen av dem kan konfigureres til å bruke en web-cache tjener på flere forskjellige måter.

Den klienten som per i dag er best egnet til å samarbeide med en web-cache tjener er Netscape Navigator 2.0 eller nyere. Den har noe som heter *Automatic Proxy Configuration* som gjør det mulig å konfigurere klienten slik at den selv velger hvilken web-cache tjener den skal kontakte ut fra gitte kriterier. Den kan også hente dokumentet direkte fra web-tjeneren når det ligger så nært at det ikke lønner seg å gå gjennom web-cache tjenesten. Klienten vil også oppdage om web-cache tjenesten går ned. Den vil da automatisk gå over til å bruke neste web-cache tjener, eller gå direkte. Når web-cache tjenesten kommer opp igjen vil den oppdage dette og begynne å bruke den igjen. Netscape 2.0 (eller nyere) kan sette inn

http://www.uninett.no/cgi-bin/pac

for å ta i bruk UNINETTs web-cache tjeneste med Automatic Proxy Configuration.

Dokumentet WWW og Caching som du finner på

http://www.uit.no/uninett/caching.html

gir en oversikt over hvordan forskjellige klienter konfigureres til å bruke en web-cache tjeneste. Husk at det nesten aldri er nødvendig å gå via web-cache tjenesten når du skal hente dokumenter fra ditt lokale domene. Så jeg vil anbefale at no_proxy (eller tilsvarende) settes til det lokale domenet.

Enkelte web-klienter cacher dokumenter på den lokale disken også. Dersom du har mange brukere som deler en disk vil du få bedre diskplass ved å slå av eller minimalisere denne cachingen. Dersom du har en egen web-cache tjener kan du slå av den lokale disk-cachingen i klientene.

Start av en egen web-cache tjeneste - SamSquid

Den største fordelen med å ha en egen web-cache tjeneste er at brukerne ofte vil laste ned dokumenter fra en lokal tjener. Dette går mye raskere enn å f.eks hente det fra USA. HENSA (i England) har regnet ut at de som bruker deres web-cache tjeneste sparer 25 sekunder i snitt for hver nedlasting.

Siden klientene ofte henter dokumentene fra den lokale web-cache tjeneren vil trafikken på linjen ut til resten av verden bli mindre. En slik førstenivå web-cache tjener kan faktisk få en treffprosent på opp mot 50%. Siden UNINETTs web-cache tjeneste stort sett er et andrenivå cache (d.v.s den brukes mest av første nivå web-cache tjenere) har den en treffprosent på 15-30%.

Programvaren som UNINETT bruker er Squid. Dette er et public domain program som etter hvert har blitt meget bra. Squid tjenere kan samarbeide med hverandre, og med andre typer web-cache tjenere. En egen lettinstallert distribusjon for Linux og HP-UX er tilgjengelig fra SamSquid på

http://www.uit.no/uninett/samsquid/

Etter hvert vil det også komme en versjon for SAMSOFT maskiner.

Det som trengs for å starte en egen web-cache tjeneste er en UNIX maskin med en del ledig minne og disk. Hvor mye disk som trengs avhenger av brukermassen, men jeg vil anbefale mins 250 MB. (UNINETTs web-cache tjeneste har 4 GB, men vi utvider sansynligvis til 8 GB før dette går i trykken.) Det er vanskeligere å beregne hvor mye minne som trengs, men ut fra erfaring med UNINETTs web-cache tjener bør en ha ca 20 MB RAM per 1 GB disk. D.v.s minst 5 MB RAM for 250 MB disk. Men disse tallene må tas med en klype salt. Det som er viktig er at web-cache prosessen har så mye minne at den slipper å swappe til disk. Noe swapping vil det alltid være, men dersom den må swappe for mye går effektiviteten drastisk ned.

Kontaktpunkter for web-caching i UNINETT

cache-hjelp@uninett.no

Dette er adressen å bruke dersom du har spørsmål rundt caching av web.

cachemaster@uninett.no

Dersom det er noe galt med UNINETTs web-cache tjeneste skal det meldes hit. Dersom du vil dra i gang din egen web-cache tjeneste, evt. samarbeide med UNINETTs web-cache tjeneste kan du også sende post hit.

IAB og IESGs uttalelse om kryptografisk teknologi og Internett

24 juli 1996, Request For Comment 1984

Internet Architecture Board (IAB)[1] og *Internet Engineering Steering Group* (IESG)[2], organisasjonene som adminstrerer arkitektur og standarder for Internett, er opptatt av behovet for øket beskyttelse av internasjonale kommersielle transaksjoner over Internett, og av behovet for å tilby alle Internett-brukere en tilstrekkelig grad av konfidensialitet.

Internet Engineering Task Force (IETF) er i ferd med å utvikle sikkerhetsmekanismer som skal dekke disse behovene. Slike sikkerhetsmekanismer krever at gode kryptografiske metoder gjøres tilgjengelig på internasjonal basis. Tilgang til slike teknologier er derfor en nøkkelfaktor for å sikre den fremtidige veksten av Internett som en drivkraft for internasjonal handel og kommunikasjon.

IAB og IESG er derfor bekymret over at flere lands myndigheter har vedtatt eller foreslått lovgivning angående tilgang til kryptografisk teknologi som:

(a) pålegger begrensninger ved å pålegge eksportkontroll; og/eller

(b) begrenser kommersielle brukere til svake eller utilstrekkelige mekanismer slik som korte kryptografiske nøkler; og/eller

(c) pålegger at private dekrypteringsnøkler skal være enten i statens hender, eller hos en annen tredjepart; og/eller

(d) forbyr bruken av kryptografi fullstendig, eller kun tillater den brukt av spesielt autoriserte organisasjoner.

Det er vår oppfatning at slik lovgivning ikke er i forbrukernes eller næringslivets interesse, stort sett er irrelevant med hensyn til militær sikkerhet, og er av liten eller ingen nytte for de ulike lands politivesen, noe som utdypes lenger nedenfor.

IAB og IESG oppmuntrer til lovgivning som tillater enkel tilgang til enhetlig, sterk kryptografisk teknologi for alle Internett-brukere i alle land.

---

1. *Internet Architecture Board* er beskrevet på http://www.iab.org/iab/
2. *Internet Engineering Task Force* og *Internet Engineering Steering Group* er beskrevet på http://www.ietf.org/

IAB og IESG hevder at:

- Internett er i ferd med å bli den mest fremtredende kanal for elektronisk handel og informasjonsutveksling. Det er essensielt at infrastrukturen for disse aktivitetene garanterer brukernes konfidensialitet.
- Kryptering er ikke noen hemmelig teknologi monopolisert av noe enkelt land, slik at eksportkontroll gir noe håp om å begrense utbredelsen av denne. Enhver dataamatør kan programmere en personlig datamaskin til å utføre sterk kryptering. Mange algoritmer er vel dokumenterte, noen med kildekode tilgjengelig i lærebøker.
- Eksportkontroll på kryptering gir firmaer i land som begrenser kryptering en konkurransemessig ulempe. Deres konkurrenter fra land uten eksportrestriksjoner kan selge tilsvarende systemer med større sikkerhet enn hva de selv kan tilby.
- Begrensninger på bruken av kryptering vil også gi firmaer i et slikt land en konkurransemessig ulempe siden disse firmaene ikke enkelt og sikkert kan delta i elektronisk handel.
- Metoder for nøkkeldeponering vil uvergelig gjøre et kryptografisk system mindre sikkert, ved å introdusere nye sårbare punkter som kan og vil bli angrepet.
- Eksportkontroll og brukskontroll hemmer utbredelsen av sikkerhet samtidig som Internettet eksponensielt øker i størrelse og angripere blir stadig mer sofistikerte. Dette plasserer brukerne i en farefull situasjon siden de er nødt til å stole på usikker elektronisk kommunikasjon.

Teknisk analyse

Nøkkelstørrelse

Det er ikke akseptabelt å begrense bruken eller eksporten av kryptosystemer basert på deres nøkkelstørrelse. Systemer som er mulige å bryte av ett land vil også være mulig å bryte av andre, muligens mindre vennligsinnede land.

Store konsern, til og med kriminelle organisasjoner, har ressurser til å knekke mange kryptosystemer. Kryptert informasjon vil ofte måtte beskyttes i flere år; siden datamaskiner stadig får større hastighet, vil nøkkelstørrelser som en gang var utenfor rekkevidde av kryptoanalyse bli usikre.

Offentlig nøkkel infrastruktur

Bruk av offentlig nøkkel kryptografi (*public key encryption*) krever ofte at det finnes en *sertifiseringsmyndighet*. Det vil si en tredjepart som må signere en streng som inneholder en brukers identitet og offentlige nøkkel.

Tredjepartens nøkkel er så i sin tur gjerne signert av et høyere nivås sertifiseringsmyndighet.

En slik struktur er legitim og påkrevd. Mange regjeringer vil, og bør, drive sine egne sertifiseringssmyndigheter, om ikke annet så for å beskytte borgernes transaksjoner med sin regjering. Men sertifiseringssmyndigheter må ikke forveksles med nøkkeldeponerings-sentere. Nøkkeldeponerings-sentere er oppsamlingssentraler for private nøkler, mens sertifiseringsmyndigheter arbeider med offentlige nøkler. Faktisk er det slik at fornuftig kryptografisk praksis pålegger brukere å aldri avsløre sine private nøkler til noen, heller ikke sertifiseringsmyndigheten.

Private nøkler bør ikke kunne avsløres

Sikkerheten i moderne kryptosystemer bygger fullstendig på hemmeligholdelse av nøklene. Følgelig er det et grunnleggende prinsipp at så langt som overhodet mulig skal nøkler aldri forlate brukernes sikre omgivelser. Nøkkeldeponering impliserer at nøklene må avsløres på ett eller annet vis, en direkte motsigelse av dette prinsippet. Alle slike avsløringer svekker systemets totale sikkerhet.

Gjenfinning av tapte data

Av og til blir nøkkeldeponeringssystemer fremholdt som å være bra for brukerne siden de tillater gjenfinning av data dersom nøkler mistes. Imidlertid bør det være opp til brukeren å avgjøre om de foretrekker et sikrere system hvor mistede nøkler betyr tapte data, eller et system hvor nøkler er deponert og kan gjenfinnes hvis nødvendig. På samme måte behøver nøkler som brukes for kommunikasjon (i motsetning til kryptering av lagrede data) aldri deponeres.

Et system hvor den hemmelige nøklen lagres av en regjering og ikke av data-eieren er garantert ikke praktisk for gjenfinning av tapte data.

Signaturnøkler

Nøkler som brukes til signatur og autentisering må aldri deponeres. Enhver tredjepart med tilgang til slike nøkler vil kunne gi seg ut for å være den legitime eieren, og dermed skape nye muligheter for svindel. Faktisk er det slik at en bruker som ønsker å fraskrive seg ansvar for en transaksjon kan hevde at han eller hennes deponerte nøkkel ble brukt, og dermed plassere bevisbyrden hos den som driver deponiet. Dersom regjeringen deponerte nøkkelen, kan en tiltalt hevde at bevis har blitt fabrikert av regjeringen, og dermed gjøre påtale mye vanskeligere. For elektronisk handel er sikkerhet mot ansvarsfraskrivelse et av de viktigste bruksområdene for kryptografi; og denne bygger på antagelsen om at kun brukeren har adgang til den private nøkkelen.

Beskyttelse av eksisterende infrastruktur

I noen tilfeller er det teknologisk mulig å bruke kryptografiske operasjoner som ikke involverer hemmeligholdelse. Selv om dette kan være tilstrekkelig i noen tilfeller, er det mye av den eksisterende tekniske og kommersielle infrastrukturen som ikke kan beskyttes på denne måten. For eksempel må konvensjonelle passord, kredittkortnummer og lignende beskyttes med sterk kryptering, selv om de kanskje kan erstattes av mer sofistikert teknologi en gang i fremtiden. Det er forholdsvis enkelt å forbedre eller endre et kryptografisk system; det er ikke tilfelle for omfattende endringer i store og utbredte systemer.

Motstridende internasjonal lovgivning

Forskjeller i restriksjoner på bruk av kryptering tvinger ofte internasjonale firmaer til å bruke svak kryptering for å tilfredstille ulike juridiske krav i to eller flere land. I et slikt tilfelle kan det, ironisk nok, godt tenkes at begge de involverte nasjonene betrakter den andre som en motpart som kommersielle virksomheter bør bruke sterk kryptering for å beskytte seg mot.

Det er tydelig at nøkkeldeponering ikke er et passende kompromiss siden ingen av landene ville ønske å avsløre sine nøkler til det andre landet.

Flerlags kryptering

Selv om deponering brukes er det ingen ting som hindrer en fra å bruke andre krypteringsmetoder først. Parter som ønsker å skjule si virksomhet vil med sikkerhet gjøre dette; det ytre krypteringslaget, som vil bruke deponering, brukes for å avlede mistanke.

Deponering av private nøkler vil ikke nødvendigvis tillate datakryptering

En av de viktigste truslene for brukere av kryptografiske systemer er tyveri av langtids-nøkler (muligens av en datasnok), enten før eller etter en sensitiv samtale. For å motvirke en slik trussel brukes ofte metoder med *perfekt sikkerhet forover (PSF)*. Hvis PSF brukes må angriperen ha kontroll over maskinen mens samtalen pågår. Generelt sett er PSF inkompatibelt med metoder som bruker deponering av private nøkler. (Dette er en overforenkling, men en full analyse ville blitt for omfattende for dette dokumentet).

Konklusjon

Ettersom flere og flere firmaer forbindes med Internettet, og ettersom mer og mer handel finner sted der, blir sikkerhet mer og mer kritisk. Kryptografi er det sterkeste enkeltverkttøy brukere kan anvende for å sikre sin bruk av Internettet. Å bevisst gjøre dette verktøyet svakere truer deres evne til å få til dette, og har ingen bevist nytteverdi.

Filter for epost

Automatisk sortering av epost slik at berre det eg ser som viktig hamnar i innboksen min, er ein av dei tinga som gjer at eg overlever arbeidsdagen min. All epost blir filtrert gjennom eit filter som spesifiserer kvar posten skal, sortert etter adresse, kven det kjem frå, kva emnet er osb.Denne funksjonaliteten er på veg inn i stadig fleire epostprogram, mellom dei viktige som har implementert filtrering i den seinare tid er Eudora (3.0 Pro-versjonen).

Knut L. Vik
Norges Teknisk
-Naturvitenskapelige Universitet
ITEA/DESK
7034 Trondheim

UNINyTT nr 4 1996

Webfilter

PICS

Standarden for filtrering av websider i barnevaktprogramvare og i webklientar heiter PICS (Platform for Internet Content Selection) og er under utarbeiding av Webkonsortiet.

Meir informasjon om PICS, mellom anna med oversiktar over programvare som støtter PICS, finn du på

http://www.w3.org/pub/WWW/PICS/

PICS baserer seg på merking av filer, enten gjort av informasjonsleverandøren inne i sjølve dokumentet, eller gjort av merkesentralar som ein stoler på vil vurdera stoffet på ein måte brukaren kan ha tiltru til.

Bakgrunnen for PICS er at foreldre skal kunna velja kva borna deira skal ha tilgang til på Internett, merkesentralane kjem inn fordi det er enklare å stola på at ein sentral er oppdatert enn at foreldre individuelt skal følgja med.

Barnevaktprogram

Eit barnevaktprogram er eit program som køyrer på brukaren si maskin og passer på at berre det som er godtatt av innhald på web blir vist fram til brukaren.

Det er mange ulike barnevaktproram på marknaden i dag, det dei har felles er at det er opp til den som har passord og kontroll over maskina kva brukaren av maskina skal få tilgang til. Dei tekniske løysingane og kvaliteten på barnevaktprogramma varierer sterkt.

Filter i webklient

Filter i webklientar tar også utgangspunkt i PICS-standarden, det fremste eksemplet er Internet Explorer 3.0 som har innebygd funksjonar for å setja opp filter.

Dei som ønskjer å testa dette kan setja opp IE til ikkje å godta noko som har med sex å gjera og så prøva å få vist fram Playboy sine websider, framvisinga vil mislukkast sidan Playboy har merka sine sider med at dei inneheld sex.

Webcachefilter

Dersom ein institusjon skal leggja sperrer på webtilgang og ønskjer at dette skal skje samla, kan dei setja opp ein webcachetenar der dei legg filter mot sider dei ikkje ønskjer skal vera tilgjengelege, desse filtera kan skilla mellom ulike brukergrupper. Det er ingen PICS-kompatible webcachar tilgjengeleg i dag, filter må vedlikehaldast manuelt av webcacheadministrator.

I tillegg må ein sperra tilgangen til å gå direkte på web, slik at all trafikk går gjennom webcachetenaren som inneheld filteret.

Personopplysningar

Alle som har tilgang til informasjon som kan innehalda personopplysningar i UNINETT, har underteikna "UNINETTs taushetserklæring". Statistikk generert ut frå loggar er tilgjengeleg, men loggar er ikkje tilgjengelege.

Personvernlov

Personvernlova set grenser for kva du kan publisera av informasjon om andre.

Arbeid med ny personvernlov finn du meir informasjon om på

http://www.jus.uio.no/iri/afin/persvern/

Det er også gitt høve til å senda meldingar og kommentarar til utvalet sitt arbeid.

Adresseopplysningar

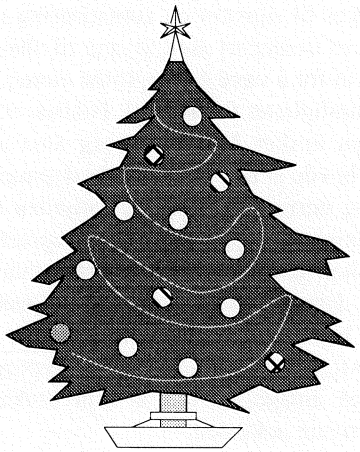
Det er populært å leggja ut informasjon om adresser til tilsette og andre på web, for å gjera dette treng du avklaring med dei tilsette.

UNINETT katalogprosjekt har i lang tid jobba opp mot Datatilsynet for å få klarlagt regelverk for publisering av adresseinformasjon på elektronisk form. Katalogprosjektet har publisert fleire oversiktar som blir oppdatert ved endringar i regelverk. Dersom du har spørsmål, ta kontakt med

katalog-hjelp@uninett.no

eller sjå den informasjonen som ligg på

http://www.katalog.uninett.no/



Oppgradering av utanlandslinja

Under treet i år finn vi utanlandslinja frå UNINETT til Stockholm og vidare at i verda. Utanlandslinja blei 9. desember oppgradert til 34 Mbps, noko som var sårt tiltrengt ettersom trafikken har auka sterkt.