”Minä täällä” eli keskinäinen autentikointi verkossa

Tutkielma kurssille Tik-110.401

Markus Peuhkuri
37681e
Teknillinen korkeakoulu

12. joulukuuta 1997

Tiivistelmä

Turvallinen liikennöinti verkossa vaatii osapuolten tunnistamista. Nykyisin käytössä olevissa tunnistamisjärjestelmissä on puutteita, joista monet ovat helposti väärinkäytettävissä. Erilaisilla järjestelyillä voidaan torjua osa hyökkäyksiä, mutta yleisesti konepohjainen turvallisuus ei skaalaudu.

Tässä työssä tutustutaan tavallisimpiin tunnistamisuhkiin IP-verkoissa ja tutustutaan tarkemmin kahteen turvallisen tunnistuksen tarjoavaan tekniikkaan ja arvioidaan niiden mahdollisuuksia.

Asiasanat: tunnistaminen, tietoturva, tietoturvauhka, hyökkäykset, IP-verkot

1 Johdanto

Internet-verkko [KH93] ja siinä käytetyt protokollat tarjoavat itsessään hyvin vähän turvallisuutta eri tietoturvauhkia vastaan. Internet-verkon alkuvaiheessa verkossa oli muutamia, hyvin hallinnoituja laitteistoja eikä nykyistä kymmenien miljoonien verkkoon kytkettyjen tai siihen ajoittain liittyvien laitteiden määrää voitu kuvitellakaan.

Useimpien protokollien sunnittelussa ei siten oltu huomioitu sitä, että useissa tapauksissa on mahdollista lähettää verkkoon mielivaltaisia IP-sähkeitä ja tätä kautta aiheuttaa virheellisiä osapuolien tunnistuksia tai toimintoja. Tästä on seurauksena, että turvallisuutta joudutaan lisäämään sovelluksiin ja järjestelmiin jälkikäteen. [WC94]

Tässä työssä käsitellään lähinnä väärän tunnistamisen mahdollisuuksiin ja sen aiheuttamiin uhkiin IP-verkoissa. Varsinaisiin tiedon eheyden tai luottamuksellisuuden takaaviin protokolliin (SSL, SSH, IPSEC, IPv6 [FKK96, YKS97, Atk95, DH96]) ei tutustuta.

2 Eräitä hyökkäysmenetelmiä

2.1 Tekeytyminen toiselle IP-osoitteelle

Paikallisessa lähiverkossa erilaiset hyökkäykset ovat kaikkein helpoimmin toteutettavissa, jopa ilman mitään erillisiä ohjelmistoja yksinkertaisesti vaihtamalla koneen IP-osoite. Useimmissa verkoissa ei ole mitään kontrollia edes koneen laitteisto-osoitteen tai sijainnin perusteella käytettyihin osoitteisiin. Edellytyksenä on tietenkin, että kone, joksi tekeydytään, on sammutettuna tai liikennöintikyvytön esimerkiksi DoS-hyökkäyksen seurauksena.

Yhteystiedot: Sähköposti: *Markus.Peuhkuri@hut.fi*; Puhelin: (09) 451 2467; Fax: (09) 451 2474; Kotisivu: URL:*http://www.iki.fi/puhuri/*.

2.2 Mielivaltaisten datagrammien lähettäminen

Mikäli käyttäjä pystyy ohittamaan käyttöjärjestelmän suojaukset tai koko käyttöjärjestelmän[1] useimmissa järjestelmissä voidaan lähetettävän viestin koko sisältö, mukaan lukien verkko- ja linkkitason kehys, muokata halutusti.

Tämä asettaa puhtaasti viestien lähdeosotteeseen perustuvan pääsynvalvonnan hyvin haavoittuvaksi. [Bel89]

2.2.1 IP lähdereititys

IP-protokollaan kuuluu lähdereititys-optio, jolla lähettävä kone voi lähetää datagrammin toiselle koneelle käyttäen tiettyä reittiä. Mikäli kaikki matkalla olevat reitittimet ja palvelinkone tukevat lähdereititysoptiota, voi vihamielinen järjestelmä tekeytyä luotetuksi järjestelmäksi, koska palvelin vastaa samaa reittiä takaisin. [Bel89]

2.2.2 Sokeat hyökkäykset

Väärennetyiden datagrammien tapauksessa hyökkääjällä on usein ongelmana, että hän ei näe kohteen lähettämiä datagrammeja, mikä on edellytys esimerkiksi TCP-yhteyden alkukättelyn ja kuittausten onnistumiselle. Vanhemmat TCP/IP-toteutukset kuitenkin loivat yhteyksien alkusarjanumerot determinisesti, joten mikäli hyökkääjä onnistui ensin luomaan ”laillisen” yhteyden kohteesen, pystyi hyökkääjä arvaamaan seuraavan, väärennetyn yhteyden sarjanumerot. [Mor85]

Seuraavalla menettelyllä eri verkossa oleva E voi esiintyä A:lle B:nä: Aluksi tulee varmistua siitä, että B on vastauskyvytön: mikäli B on toiminnassa, voidaan luoda puoliavoimia yhteyksiä johonkin palvelinporttiin, jotta vastaanottojono täyttyy. Tämän jälkeen E ottaa laillisen yhteyden A:han ja tutkii yhteyden alkusarjanumeron. Tästä pystytään (4.2BSD:ssä) laskemaan seuraavan yhteyden alkusarjanumero: luodaan datagrammi, jonka lähdeporttina on B:n tukittu portti ja lähdeosoitteena B:n osoite ja kohteena A:n haluttu portti. Kuittaukseen pystytään vastaamaan, koska alkusarjanumero on arvattu eikä B reagoi kuittaussegmenttiin vastaanottojonon ollessa täynnä.

2.3 Salakuuntelu, yhteyksien kaappaus ja tiedon muuttaminen

Verkossa liikkuvan tiedon perusteella voidaan saada haltuun tieto, joka riittää tekeytymiseen, esimerkiksi käyttäjätunnus-salasanapari. Salakuuntelun mahdollistavissa tilanteissa on usein myös mahdollista kaapata yhteyksiä sekä muuntaa yhteyksiä.

2.3.1 Samassa lähiverkossa käytettävät tekniikat

Perinteinen lähiverkko, erityisesti Ethernet, on hyvin helposti salakuunneltavissa. Samassa Ethernet-verkossa[2] kaikki liikenne leviää kaikille verkossa oleville päätelaitteille. Normaalisti verkkosovittimet lukevat ainoastaan k.o. sovittimen laiteosoittelle (MAC) sekä jakelu- ja levitysosotteisiin lähetetyt viestit. Useimmat verkkosovittimet voidaan kuitenkin asettaa kaappaamaan kaikki verkossa kulkevat viestit, jolloin viesteistä voidaan automaattisestikin lukea käyttäjätunnus-salasanat parit sekä muita tunnistettavia merkkijonoja kuten luottokorttinumeroita. [Cen94]

Kuunteluun voidaan käyttää jotain verkossa olevaa konetta, johon ohjelmisto on asennettu mahdollisesti taustalla toimimaan, tai piilottamalla muu kone esimerkiksi kaapelihyllylle.

[1] Ts. käyttöoikeuksienvalvonnalla varustetussa koneessa pääkäyttäjän oikeuksilla. Monissa mikrokäyttöjärjestelmissä (MS-DOS, Windows95) ei ole mitään suojauksia, lisäksi monet (PC-)järjestelmät sallivat käynnistämisen levykkeeltä.

[2] Joka voi muodostua useista toistimilla eroitetuista segmenteistä.

Uudemmissa verkoissa, kuten ATM- ja kytkentäisissä Ethernet-verkoissa liikenne ei enää leviä kaikkialle verkossa. Eräissä kytkimissä (esim Whitetree Workgroup) on kuitenkin mahdollisuus kopioida kaikki tietyn portin liikenne toiseen porttiin, joten k.o. laitteiden turvallisuus on koko verkon turvallisuuden kannalta kriittistä. [Peu]

2.3.2 ICMP redirect

IP-toteutuksiin kuuluu ICMP-uudelleenohjausviesti. Tämä on tarkoitettu siihen, että reititin voi ilmoittaa viestä lähettävälle koneelle suositeltavan, suoremman reitin kohdekoneelle. Hyökkääjä lähettää liikennöinnin molemmille osapuolille uudelleenohjausviestin, joka ohjaa liikenteen hyökkääjän hallussa olevalle koneelle. Tässä on hyökkääjällä on täydet mahdollisuudet kuunnella ja muokata liikennettä. Hyökkäys on myös käyttökelpoinen, mikäli vain toinen puoli liikenteestä onnistuttaisiin ohjaamaan uudelleen Tässä korvattavan tiedon (TCP-yhteyksillä) on oltava yhtä pitkä kuin alkuperäinen, jotta kuittaukset toimivat oikein. [Bel89]

Monet toteutukset tottelevat sokeasti uudelleenohjausta, paremmin toteutetut ja uudemmat järjestelmät totetuttavat jomman kumman seuraavista:

- Uudelleenohjausta ei noudateta. Tämä ei usemmiten ole ongelma, koska aliverkosta on yleensä vain yksi reititin ulos. Kahden tai useamman reitittimen tapauksessa tämä aiheuttaa tehottomutta, mikäli reititystaulut eivät ole kunnossa.
- Uudelleenohjaus hyväksytään vain jos [Bel89]
  - uudelleenohjausviestin lähettää nykyinen yhdyskäytävä k.o. kohteeseen ja
  - uusi yhdyskäytävä on samassa aliverkossa ja
  - kohdekone ei ole samassa aliverkossa ja
  - on olemassa yhteys k.o. koneeseen.

2.3.3 Yhteyksien kaappaus

TCP-yhteyksien kaappaus onnistuu monitoroimalla liikennettä. Tämän jälkeen toiselta liikennöintiosapuolelta (A) katkaistaan yhteys väärentämällä RST-viesti lähteväksi toiselta osapuolelta (B). Tämän jälkeen voidaan väärennetyillä datagrammeilla liikennöidä B:n kanssa. Ongelmana on että A lähettää vastauksena RST-viestin, mikäli B:n vastausdatagrammit menevät A:lle. Näin A täytyy joko saada liikennöintikyvyttömäksi joko hyökkäämällä suoraan siihen tai pyrkimällä tukkimaan A:n verkkoyhteys, jotta kuittausdatagrammit eivät pääse perille. [Cen95]

3 Protokollien ominaisuudet ja niihin pohjautuvat hyökkäykset

Useat palveluprotokollat on suunniteltu toimimaan turvallisessa ympäristössä luotettujen koneiden kesken, millaisena ympäristöksi nykyistä Internettiä ei voida enää pitää.

3.1 Koneen IP-osoitteen perusteella autentikoivia järjestelmiä

Usemmiten IP-osoitteeseen perustuvissa järjestelmissä luotetut koneet esitetään nimen perusteella: tämä tekee autentikoinnin IP-osoitteiden väärentämisen lisäksi haavouttuvaksi myös DNS-järjestelmään perustuville hyökkäyksille (kappale 3.2, s. 4).

3.1.1 rlogin, rsh ja rcp

Nämä nk. "r"-komennot[3] mahdollistavat helpon tavan siirtyä järjestelmästä toiseen antamatta salasanaa. Luotetut koneet, joissa tyypillisesti on samat käyttäjätunnukset, on tyypillisesti lueteltu tiedostossa `/etc/hosts.equiv`. Käyttäjä, jolla on sama käyttäjätunnus molemmissa järjestelmissä ja jonka lähdekone on listattu kohdekoneen `/etc/hosts.equiv`-tiedostossa voi kirjottautua antamatta salasanaa.

Lisäksi käyttäjällä on mahdollisuus luoda omaan kotihakemistoonsa tiedosto `.rhosts`, jossa hän voi luetella koneet ja tunnukset, joiden on sallittua kirjottautua tunnukselleen. Luottamussuhteiden lisämisen salliminen käyttäjäille mahdollisesti heikentää huomattavasti järjestelmän turvallisuutta. [Bel89] Etuna telnet-yhteyksiin verrattuna on kuitenkin, että verkossa ei yleensä välity salasana. [BBC+94]

3.1.2 Network File System

NFS:n autentikointi perustuu yksinomaan koneen osoitteeseen. Levyjä jakavassa NFS-palvelimessa määritellään[4], mihin tiedostojärjestelmiin milläkin asiakaskoneella on oikeus. Näinollen NFS on hyvin haavoittuvainen kaikille tekeytymistekniikoilla.

NFS-palvelimen uudelleenkäynnistyksen tulee olla asiakkaille näkymätön, niinpä tiedostojen käsittely NFS-järjestelmässä perustuu tiedostokahvoihin (64 bittinen luku), jotka muodostuvat usein levyjärjestelmätunnisteesta ja inode-numerosta. Mikäli tunkeutuja (normaalikäyttäjänä) jossain luotetussa järjestelmässä saa selville nämä tiedot, voi hän räätälöidä kirjoitus- tai poistokäskyn, jonka lähettää verkon ulkopuolelta väärennetyillä lähettäjätiedoilla.

3.2 Väärän DNS-tiedon antaminen

DNS-järjestelmä muodostaa hajautetun hierarkkisen tietokannan kaikista Internettiin kytketyistä koneista.[5] Useat IP-pohjaiseen autentikointiin perustuvat järjestelmät perustuvat yksipuoliseen nimikyselyyn joka on hyvin helposti huijattavissa.

Koneen ottaessa yhteyttä rajoitettuun palvelimeen, palvelin tekee käänteisen nimipalvelukyselyn eli koneen osoitteen perusteella selvittää nimen. Nimenä vihamielinen nimipalvelin voi kuitenkin palauttaa minkä tahansa nimen. Tämän estämiseksi tulee tämän nimen perusteella tehdä nimipalvelukysely nimestä osoitteeksi. Mikäli tästä saatu osoite vastaa alkuperäistä osoitetta, voidaan paremmin varmistua siitä, että osapuoli on oikea.

3.2.1 Nimipalveluvastausten väärentäminen

Nimipalvelukyselyssä on mukana sarjanumero, joka monissa järjestelmissä on luotu deterministesti: mikäli hyökkääjä saa tämän selville kuuntelemalla verkkoa, pystyy hän palauttamaan vastauksena haluamansa tiedon. Näin ollen käyttäjä tai sovellus ohjataan väärään palvelimeen. [Bel89]

Eräitä nimipalvelinohjelmistoja voidaan myös huijata vastaavalla tavalla. Lisäksi kaikki nimipalvelimet eivät tarkista, että saatu vastaus on vastaus siihen mitä kysyttiin vaan saatu vastaus viedään suoraan tietokantaan. Tätä menetelmää käyttäen syksyllä 1997 erään suomalaisen internet-palveluntarjoajan asiakkaat näkivät oikeiden asiapalveluiden sijalla pornopalvelimia. [Peu]

[3] R tulee sanasta "remote".

[4] Yleensä koneen nimeen perustuen.

[5] Osa koneista voi olla rekisteröimättä, esimerkiksi turvallisustä tai mikälki näillä ei ole suoraa yhteyttä verkkon.

4 Autentikointi

Käyttäjien tunnistaminen on perinteisesti ollut tärkeää ja siihen on kiinnitetty huomiota. On myös erittäin tärkeää, että käytetty palvelu tunnistetaan: esimerkiksi Englannissa onnistuttiin kaappaamaan useita pankkikortteja tunnuslukuineen käyttämällä valepankkiautomaattia, joka tallensi tunnusluvun ja otti kortin haltuun. Käyttäjälle laite ilmoitti tunnusluvun olevan virheellisen. [Peu]

4.1 Salasana ja fyysiset esineet

Valtaosa käyttäjän autentikoinnista perustuu salasanoihin. Nämä ovat kuitenkin riittämättömiä, koska [BBC$^+$94]:

- salasana voi olla arvattavissa, jaettu, kirjoitettu muistin tai unohdettu
- salasanoja ei vaihdeta usein; usein vaihdettavat salasanat unohdetaan helposti
- salasana voidaan kaapata tarkkailemalla
- salasana voidaan saada selville tai vaihdetuksi halutuksi esimerkiksi soittamalla käyttäjälle ja esintymällä ylläpitäjänä [Cen91]
- selvätekstiset salasanat liikkuvat verkossa tai tallennetaan johonkin yleisesti luettavaan paikkaan
- salatut salasanat ovat usein yleisesti luettavissa, joten ne ovat kryptoanalyysin kohteena
- lyhyet salasanat voidaan löytää brute-force -menetelmällä.

Lisäksi on erityisesti verkossa luotettava siihen, että mikään käytetty järjestelmä ei ole troijalainen tai sisällä salasanoja tallentavaa mekanismia. Eräät käyttöjärjestelmät tallentavat oletusarvoisesti käyttäjän käyttämät salasanat tiedostoihin heikosti salattuna. [Peu]

Autentikointi voi perustua myös johonkin, mitä käyttäjällä on:

fyysinen avain Turvallisuus riippuu avaimen fyysisestä turvasta ja siten hyvin pitkälle paperille kirjoitetun salasanan veroinen. Osa fyysisistä avaimista voi tosin olla vaikeasti kopioitavia, esimerkiksi älykortit.

biologiset ominaisuudet Erilaisiin biologisiin ominaisuuksiin perustuvia järjestelmiä on lukuisia ja usein vaikeasti väärennettäviä. Laitteistot näiden määrittämiseen ovat kuitenkin usein kalliita. Lisäksi tiettyyn ominaisuuteen, esimerkiksi käden suhteisiin, perustuva tunnistus edellyttää tätä omainaisuutta (esimerkissä kättä). Toiset omainaisuudet voivat muuttua hyvinkin nopeasti kuten ulkonäkö[6] ja ääni.

Näiden käyttö edellyttää myöskin, että liikennöinnin toinen osapuoli luottaa käyttäjän edessä olevaan, mittauksen suorittavaan, päätelaitteeseen, mikä on usein mahdotonta. Tälläinen autentikointi mahdollistaa uudelleensoiton mistä tahansa laitteesta, joka on mitannut ominaisuudet.

4.2 Kerberos

Kerberos [SNS88] on MIT:ssä kehitetty autentikointijärjestelmä, jossa autentikoidaan molemmat liikennöintiosapuolet. Järjestelmä on suunniteltu laajaan työasemaverkkoon, jossa ei voida luottaa siihen, että yksittäinen työasema autentikoi käyttäjän oikein. Autentikoinnissa on kaksi pääkomponenttia:

[6] Käytännön elämässä useimmiten käytetty tunnistusmenetelmä.

pääsylippu (ticket), jota käytetään käyttäjän tunnistukseen palvelimelle ja tiedon turvalliseen välitykseen.

tunnistaja (authenticator), jolla voidaan varmistua, että käyttäjä on sama, jolle pääsylippu oli myönnetty.

Käyttäjän kirjautuessa työasemalle, työasema ottaa yhteyden Kerberos-palvelimeen, jolta saa käyttäjän salasanalla salatun pääsylipun pääsylippupalvelimelle. Käyttäjän annettua oikean salasanan tämä voidaan purkaa, minkä jälkeen luodaan tunnistaja, joka salataan pääsylipussa saadulla yhteysavaimella. Tällä voidaan ottaa yhteys pääsylippupalvelimelle, joka myöntää pääsyliput halutuille palveluille.

Kerberos tarjoaa kolmitasoisen turvallisuuden, josta sovelluskohtaisesti voidaan valita riittävä käyttöön:

1. vain tunnistus
2. tunnistus ja tiedon eheys (safe messages)
3. tunnistus sekä tiedon eheys ja luottamuksellisuus (private messages)

4.2.1 Tietokanta

Kerberos-järjestelmän tietokanta sisältää kaikkien käyttäjien ja palvelujen salaiset avaimet. Tämä tekee siitä järjestelmän kriittisen komponentin: mikäli tietokantaan päästään murtautumaan, tuhoutuu koko järjestelmän luotettavuus. Tietokanta muodostaa myös järjestelmän käytettävyyden kannalta kriittisen pisteen; tietokanta voidaan replikoida isäntä-renki-periaatteella, missä järjestelmässä on useita renkejä (joiden tietokantan on vain lukuoikeus) ja isäntä, johon muutokset tehdään.

4.2.2 SESAME

SESAME[7] [McM94] on eurooppalainen saman tyyppinen järjestelmä kuin Kerberos, joskin toiminnallisuudeltaan laajempi. SESAME-järjestelmä osaa toimia yhteen Kerberos-järjestelmän kanssa.

4.2.3 Järjestelmän skaalautuvuus

Tietokanta, jossa on salaista tietoa (useissa kopioissa) ja vain yksi paikka tehdä muutoksia, asettaa järjestelmän rajat. Vaikka Kerberos-järjestelmässä on mahdollista olla useita hallinta-alueita, vaatii joustava käyttö ainankin luottamussuhteen määrittelyä, mahdollisesti jaettua salaisuutta. Käytännössä tämä estää käyttämästä samaa Kerberos-järjestelmää useiden riippumattomien organisaatioiden kesken.

Kuten useimmat järjestelmät, Kerberos edellyttää käyttäjän luottavan järjestelmään, johon hän kirjottautuu. Järjestelmässä käytetään normaaleja salasanoja, joista salaisuus luodaan yksisuuntaisella hajautusfunktiolla.

4.3 X.509 LDAP-pohjainen julkisen avaimen järjestelmä

Julkisen avaimen järjestelmät ovat käyttökelpoisia suurissa järjestelmissä. Avaintenhallinta on julkisen avaimen järjestelmässä kriittinen tehtävä. Avainten allekirjoitus on tehtävä, jossa hierarkinen järjestelmä on edellytys joustavalle toiminnalle.

[7]Secure European System for Applications in a Multi-vendor Environment

Taulukko 1: Standardoidut avainsanat [Kil95].

Avain	Määre (X.520-avain)
CN	CommonName
L	LocalityName
ST	StateOrProvinceName
O	OrganizationName
OU	OrganizationalUnitName
C	CountryName
STREET	StreetAddress

Tässä esitetty malli perustuu Netscapen esittämään [Net97] malliin ja tuotteisiin käyttäjien autentikoinnista. Suojattuna siirtotienä käytetään SSL[8]-protokollaa, jota voidaan käyttää useimpiin luotettavaa siirtotietä vaativiin sovelluksiin (HTTP, POP, IMAP, telnet...). [FKK96]

4.3.1 LDAP-järjestelmä

LDAP[9] [YHK95] on hajautettu, puumuotoinen hakemisto, joka mahdollistaa organisaatioiden ylläpitää omaa tietokantaa toisistaan riippumattomasti. LDAP on kevennetty versio X.500 hakemistosta [IT88].

Jokaisella käyttäjällä ja organisaatiolla on oma tietue, joka yksilöi käyttäjän. Tyypillinen esimerkki alla.

```
cn=Markus Peuhkuri, o=Helsinki University of Technology, c=FI
```

4.3.2 Osapuolten autentikointi

Asiakas autentikoi palvelimen tarkistamalla palvelimen sertifikaatin. Palvelin lähettää asiakkaalle tiedon, johon asiakas lisää omaan datansa, allekirjoittaa tämän yhdistelmän salaisella avaimellaan ja palauttaa tämän sertifikaatin mukana palvelimelle.

Palvelin tarkistaa sertifikaatissa olevan tunnisteen[10] perusteella LDAP-tietokannasta, että kyse on samasta käyttäjästä. Tämän jälkeen palvelin tarkistaa allekirjoitusketjun kuvan 1(b) mukaan.

4.3.3 Avainten luominen ja hallinta

Avainten luonti tapahtuu luomalla salainen ja julkinen avain, jonka sertifioiva CA allekirjoittaa liitettynä tunnisteeseen. (Kuva 1(a)) Allekirjoitettu julkinen avain tallennetaan LDAP-tietokantaan ja salainen avain ja sertifikaatti tallennetaan käyttäjän salasanasuojattuun tiedostoon.

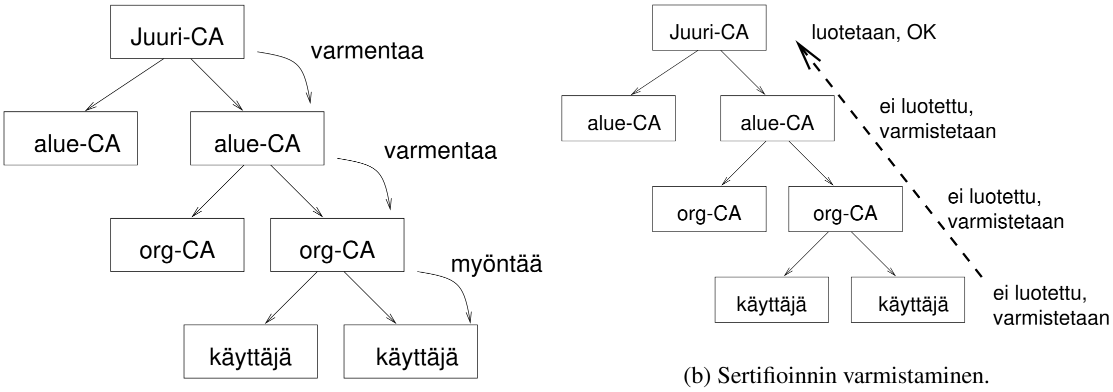
4.3.4 Järjestelmän puutteita

Järjestelmässä itsessään on kaksi puutetta: toinen on käyttäjien ja palvelimien avainten säilytys ja toinen on CA:den avainten toimittaminen käyttäjille. Lisäksi ohjelmien käyttöliittymässä on puutteita.

[8] Secure Sockets Layer

[9] Light-weight Directory Access Protocol

[10] DN: distinguished name



(a) Sertifiointipuu.

(b) Sertifioinnin varmistaminen.

Kuva 1: Sertifiointiketjujen rakenne [Net97]

Avainten säilytys Käyttäjältä kysytään tämän aloittaessaan istunnon (ja mahdollisesti määrävälein) salasanaa, jolla paikalliselle levylle tallennettu avaintietokanta voidaan avata. Tämä asettaa järjestelmän periaatteeltaan samojen ongelmien eteen kuin normaali salasanapohjainen ratkaisu (kappale 4.1), jonka lisäksi avaimet ovat vaarassa kadota levyrikon tai salasanan unohtamisen yhteydessä. Tämä on erityisen ongelmallista, mikäli avaimia on käytetty pysyvän tiedon salaamiseen.

Eräs ratkaisu avainten säilyttämiseen on kerätä keskitysti varmuuskopio näistä, jolloin taas joudutaan tekemisiin avaimien luottamuksen kanssa. Eräs esitys on käyttää mekanismia, jolloin tarvitaan N:stä henkilöstä vähintään M avaamaan salaus. [Net97]

Palvelimien kohdalla ongelmana taas on avaimen turvallinen säilyttäminen. Mikäli salassa pysymisestä halutaan olla varma, tulee tämä levyllä oleva avain salasanasuojata, jotta mahdollisen murtoyrityksen yhteydessä avain pysyy salaisena. Ongelmana on kuitenkin se, että salasanaa tarvitaan aina järjestelmän käynnistyksessä, jolloin DoS-hyökkäyksen, virtakatkon tai muun uudelleenkäynnistyksen vaativan tapahtuman seurauksena järjestelmä voi olla käyttökelvoton kunnes salaisuuden tietävä henkilö saadaan kirjoittamaan se.

Sertifioijien avainten toimittaminen käyttäjälle Käyttäjän tulee luonnollisesti tietää ainankin palvelimen avaimen sertifioineen CA:n avain ennekuin hän voi autentikoida palvelimen. Tehokkuus- ja käytettävyyssyistä olisi edullista, että käyttäjä tuntisi muidenkin kuin juuri-CA:n avaimen. WWW-selainohjelmistojen mukana tulee yleensä tiedosto, joka sisältää useiden juuri-CA:den avaimet. Tämä asettaa luonnollisesti kovat vaatimukset ohjelmapaketin eheydelle ja jakelukanavalle.

Ohjelmien käyttöliittymä WWW-selainohjelmistot eivät yleensä ilmaise vastapuolen sertifikaattia kuin erikseen katsomalla. Tämä mahdollistaa man-in-middle-hyökkäykset: riittää, että on onnistunut hankkimaan jonkun selaimen tunteman CA:n allekirjoittaman sertifikaatin. Ainoastaan, mikäli selain ei tunnista vastapuolen avaimen allekirjoittanutta CA:ta, tulee liitteen A mukainen dialogiketju.

4.4 Älykortti

Edellä esitetyissä järjestelmissä kaikissa on ollut sama ongelma: on luotettava järjestelmään, jolta otetaan yhteyksiä. On lisäksi kiinnitettävä huomiota salasanaan, jolla avaintietokanta salataan, mikäli avaimia säilytetään järjestelmässä.

Useista ongelmista selvitään, mikäli salaisia avaimia ei koskaan päästetä suljetun (luotettavan ja kuljetettavan) järjestelmän ulkopuolella vaan kaikki salaista avainta vaativat operaatiot suoritetaan tällä suljetulla kortilla. Tämäkään ei ratkaise kaikkia ongelmia: käytetty laitteisto voi esimerkisi pyytää allekirjoitusta johonkin käyttäjän tietämättä. PIN-koodin kysely vaatii lisäksi erillisen näppäimistön yhdistettyn lukijan, jotta PIN-koodia ei kaapattaisi.

Ongelmista huolimatta käyttökelpoisimmalta vaikuttaa salaisen avaimen älykortti yhdistettynä LDAP-pohjaiseen julkisen avaimen jakeluun.

5 Yhteenveto

Yksittäisiten koneiden eheyteen tai koneiden IP-osoitteisiin tuottavat tunnistusmenetelmät ovat yleisesti epäluotettavia. Erityisesti koneiden ja niitä hallinnoivien organisaatioidan määrän kasvaessa ongelmat ja mahdollisuudet väärinkäyttöön kasvavat.

Erityistä huolta järjestelmän suunnitelussa on kiinnitettävä, mikäli järjestelmä suunnataan suurelle (ei-tekniikka-orientoituneelle) käyttäjäjoukolle. Kaikille käyttäjille sovelutuva autentikointi ei saa riippua käyttäjän kyvystä muistaa pitkiä merkkijonoja eikä myöskään yksittäisen käyttäjän koneen turvallisuudesta. Järjestelmän tulee olla sellainen, että käyttäjä ei edes tarkoituksellisesti vahingosta puhumattakaan pysty paljastamaan omaa salaisuuttaan.

Hajautettu tietokanta on toimivuuden ja käytettävyyden edellytys. Tietokannan tulee mahdollistaa eri osien riippumaton hallinnointi. Teknisesti kehitys alkaa olla varsin pitkällä, eri maiden lainsäädäntö kuitenkin haittaa vahvojen autentikointijärjestelmien leviämistä.

Viitteet

[Atk95] R. Atkinson. Security architecture for the internet protocol. Request for Comments (Proposed Standard) RFC 1825, Internet Engineering Task Force, August 1995. URL:ftp://ds.internic.net/rfc/rfc1825.txt.

[BBC+94] R. Bagwill, J. Barkley, L. Carnahan, S. Chang, R. Kuhn, P. Markovitz, A. Nakassis, K. Olsen, M. Ransom, and J. Wack. Security in open systems. NIST Special Publication 800-7, National Institute of Standards and Technology, July 1994. John Barkley (editor).

[Bel89] S. M. Bellovin. Security problems in the tcp/ip protocol suite. *Computer Communication Review*, 19(2):32–48, April 1989.

[Cen91] CERT Coordination Center. Unauthorized password change requests via mail messages. CERT(sm) Advisory CA-91:03, CERT Coordination Center, April 1991.

[Cen94] CERT Coordination Center. Ongoing network monitoring attacks. CERT(sm) Advisory CA-94:01, CERT Coordination Center, February 1994.

[Cen95] CERT Coordination Center. Ip spoofing attacks and hijacked terminal connections. CERT(sm) Advisory CA-95:1, CERT Coordination Center, January 1995.

[DH96] S. Deering and R. Hinden. Internet protocol, version 6 (ipv6) specification. Request for Comments (Proposed Standard) RFC 1883, Internet Engineering Task Force, January 1996. URL:ftp://ds.internic.net/rfc/rfc1883.txt.

[FKK96] Alan O. Freier, Philip Karlton, and Paul C. Kocher. The ssl protocol. Technical report, Netscape Communications, March 1996. Internet Draft.

[IT88] ITU-T. The directory: Overview of concepts, models and service. ITU-T Recommendation X.500, International Telecommunication Union, 1988.

[KH93] E. Krol and E. Hoffman. FYI on "what is the internet?". Request for Comments (Informational) FYI 20, RFC 1462, Internet Engineering Task Force, May 1993. URL:ftp://ds.internic.net/rfc/rfc1462.txt.

[Kil95] S. Kille. A string representation of distinguished names. Request for Comments (Draft Standard) RFC 1779, Internet Engineering Task Force, March 1995. (Obsoletes RFC1485). URL:ftp://ds.internic.net/rfc/rfc1779.txt.

[McM94] P V McMahon. Sesame v2 public key and authorisation extensions to kerberos. In *ISOC Symposium*, 1994.

[Mor85] Robert T. Morris. A weakness in the 4.2bsd unix™ tcp/ip software. Technical report, AT&T Bell Laboratories, Murray Hill, New Jersey 07974, February 1985. URL:ftp://ftp.research.att.com/dist/internet_security/117.ps.Z.

[Net97] Single sign-on deployment guide. Technical report, Netscape Communications, 1997.

[Peu] Markus Peuhkuri. Muistelut. Tarkemmin yksilöimätöntä tai (tätä esitystä varten) tarkistamatonta tietoa, joka on peräisin eri lähteistä, mm. erinäisiltä postituslistoilta ja muista tietolähteistä kuten keskusteluista.

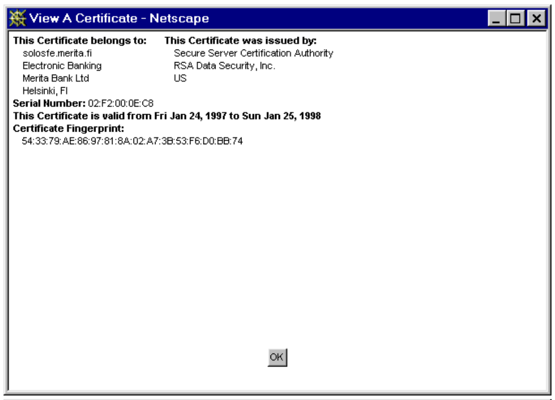
[SNS88] Jennifer G. Steiner, Clifford Neuman, and Jeffrey I. Schiller. Kerberos: An authentication service for open network systems. In *USENIX Conference Proceedings*, pages 191–202. USENIX, 1988.

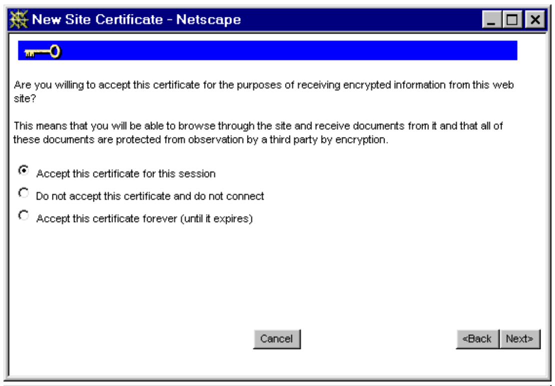
[WC94] John P. Wack and Lisa Carnahan. Keeping your site comfortably secure: An introduction to internet firewalls. NIST Special Publication 800-10, National Institute of Standards and Technology, December 1994.

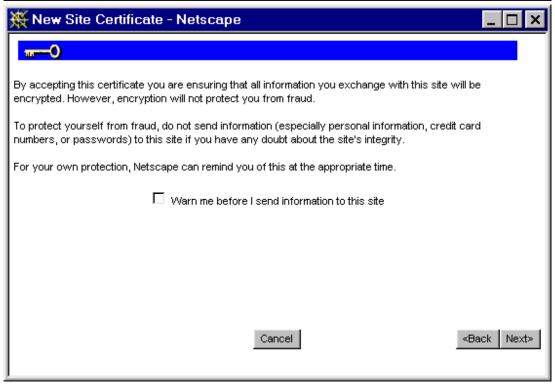
[YHK95] W. Yeong, T. Howes, and S. Kille. Lightweight directory access protocol. Request for Comments (Draft Standard) RFC 1777, Internet Engineering Task Force, March 1995. (Obsoletes RFC1487). URL:ftp://ds.internic.net/rfc/rfc1777.txt.

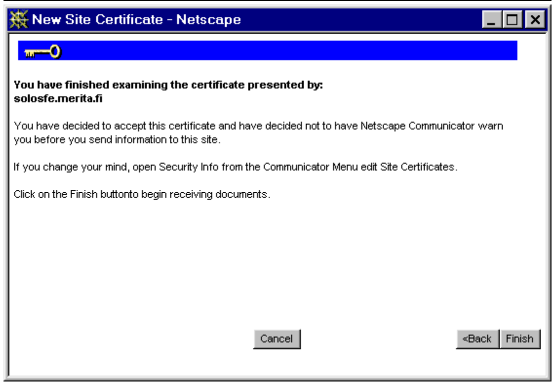
[YKS97] T. Ylönen, T. Kivinen, and M. Saarinen. Ssh protocol architecture. Internet Draft draft-ietf-secsh-architecture-01, Internet Engineering Task Force, Nov 1997.

A Sertifikaatin hyväksyntä Netscape Navigator 4.0:ssa


View A Certificate - Netscape
This Certificate belongs to:
solosfe.merita.fi
Electronic Banking
Merita Bank Ltd
Helsinki, FI
This Certificate was issued by:
Secure Server Certification Authority
RSA Data Security, Inc.
US
Serial Number: 02:F2:00:0E:C8
This Certificate is valid from Fri Jan 24, 1997 to Sun Jan 25, 1998
Certificate Fingerprint:
54:33:79:AE:86:97:81:8A:02:A7:3B:53:F6:D0:BB:74
OK


New Site Certificate - Netscape
Are you willing to accept this certificate for the purposes of receiving encrypted information from this web site?
This means that you will be able to browse through the site and receive documents from it and that all of these documents are protected from observation by a third party by encryption.
Accept this certificate for this session
Do not accept this certificate and do not connect
Accept this certificate forever (until it expires)
Cancel
<Back
Next>


New Site Certificate - Netscape
By accepting this certificate you are ensuring that all information you exchange with this site will be encrypted. However, encryption will not protect you from fraud.
To protect yourself from fraud, do not send information (especially personal information, credit card numbers, or passwords) to this site if you have any doubt about the site's integrity.
For your own protection, Netscape can remind you of this at the appropriate time.
Warn me before I send information to this site
Cancel
<Back
Next>


New Site Certificate - Netscape
You have finished examining the certificate presented by:
solosfe.merita.fi
You have decided to accept this certificate and have decided not to have Netscape Communicator warn you before you send information to this site.
If you change your mind, open Security Info from the Communicator Menu edit Site Certificates.
Click on the Finish buttonto begin receiving documents.
Cancel
<Back
Finish