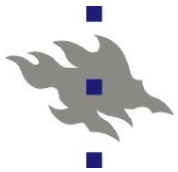
HELSINGIN YLIOPISTO
HELSINGFORS UNIVERSITET
UNIVERSITY OF HELSINKI

Linux-ylläpito: Verkkopalvelut

Jani Jaakkola
jjaakkol@cs.helsinki.fi
http://www.cs.helsinki.fi/u/jjaakkol/lyp2010

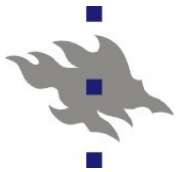
Verkkopalvelut: sisältö

- Yleistä verkkopalveluista
- Etähallinta
  - Ssh, X, vnc, rdesktop
- SSL/TLS ja sertifikaattien hallinta
- WWW-palvelut
  - Apache, proxyt,java-sovellusalustat
- Tietokannat
  - Postgres, Mysql, Oracle(?)
- Mikroverkkopalvelut
  - Käyttäjätunnukset: NIS, LDAP, Kerberos, MS:n AD
  - Tulostus
  - Tiedostojen jakaminen: NFS, Samba
- Virtualisointi
  - VMWare, Xen, KVM
- Sähköposti



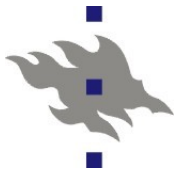
Verkkopalvelut – viikko 1

- Yleistä
  - Linuxin ominaisuudet palvelinkäytössä
  - Tietoturva
  - Palveluiden käynnistys ja hallinta
  - Ssh-etäylläpito
- Ssh-etäylläpito
  - Ssh-etäylläpito
  - Avainten generointi ja hallinta
- SSL/TLS Kryptaus
  - SSL/TLS-protokolla
  - Sertifikaattiauktoriteetit
  - Sertifikaatit
    - Ominaisuudet
    - Generointi
    - Allekirjoittaminen



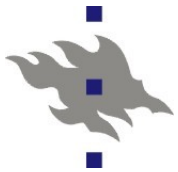
Linux palvelinalustana

- Miksi valita Linux palvelimeen?
- Unix-tyyppisissä käyttöjärjestelmissä **etäylläpito** on aina toiminut.
  - Ei jälkeenpäin päälle liimattu ominaisuus
  - Myös graafisen työpöydän käyttäminen verkon yli
- Ohjelmistojen ilmaisuus
- Avoin lähdekoodi voi pelastaa ohjelmointitaitoisen ylläpitäjän päivän
- Palvelinpuolella Linux on hyvin tuettu
  - Palvelinvalmistajat tarjoavat ajurit ja Linux-tukea
  - IBM, Dell, HP
- Linux on palvelinkäytössä hyvin stabiili
- Linux on riittävän tehokas ja skaalautuva
  - palvelimen teho ei kulu käyttöjärjestelmän pyöritykseen



Linux palvelinkäytössä

- SoftaRAID
  - RAID ilman erillisiä ohjainkortteja
  - RAID1 ja RAID5
- Logical Volume Management
  - Tiedostojärjestelmä sijaitsee loogisella levyllä, joka koostuu yhdestä tai useammasta varsinaisesta fyysisestä levystä
- Virtualisointi
  - Palvelut pyörivät virtuaalikoneilla
  - Virtuaalikoneita voi olla useita yhtä fyysistä konetta kohti
  - Virtuaalikone voi siirtyä fyysiseltä koneelta toiselle
- Klusterilaskenta
  - Linux on vallannut laskentaklusterien markkinat
  - Laitoksen konehuoneessa odottaa käyttöönottoa upouusi Linux-klusteri
- High Availibility Clusters
- Klusteritiedostojärjestelmät?



Tiedostojärjestelmät

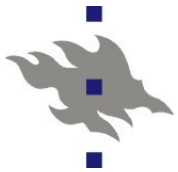
- Vaihtoehtoina käytännössä ext4 ja ehkä brtfs
- Kaikki tukevat oleellisimpia ominaisuuksia
  - Journalointi: tiedostojärjestelmän tila konsistentti kaatumisenkin jälkeen
  - ACL: access control lists
- Tehokkuuserot?
  - Hakemistojen indeksointi ja fragmentoituminen?
- Luotettavuuserot?
  - **Kun** laitteisto-ongelmia lopulta ilmenee, pystyykö tiedostojärjestelmän parsimaan kasaan?
- LVM ja RAID
  - Linuxissa tiedostojärjestelmien alapuolelle erillisinä palikoina. Ylläpitäjän kannalta väärässä paikassa
- Klusteritiedostojärjestelmät?

EXT4: ominaisuuksia ja vipuja

- Tiedostojärjestelmää luotaessa valittava:
  - Inode lukumäärä: tiedostojen max lukumäärä
  - Tiedostojärjestelmän nimi ja UUID
    - UUID on universaalisti yksikäsitteinen ID
    - Tiedostojärjestelmän fyysinen sijainti voi vaihdella
    - *Fstab*-tiedostossa tiedostojärjestelmään voi viitata nimen tai UUID:n perusteella
  - Ylläpitäjälle varattujen blokkien lukumäärä (oletus 5%)
  - Hakemistoindeksit
  - Kuinka usein ajetaan e2fsck
  - Journalin koko ja sijainti
  - Quotan alustaminen
- Ext4-tiedostojärjestelmän kokoa voi kasvattaa
  - Myös lennossa

EXT4: ominaisuuksia ja vipuja

- Tiedostojärjestelmää liitettäessä (mount):
  - Miten journalia käytetään:
    - Vain metadata: tiedostojärjestelmän tila on aina konsistentti, mutta tiedostojen sisältö voidaan hukata
    - Synkronoitu: ennen kuin tiedoston metadatan muutokset kirjoitetaan journaliin kaikki tähän saakka kirjoittamaton varsinainen data pakotetaan levylle
    - täysi journalointi: myös data kirjoitetaan ensin journaliin
  - ACL – Access Control List
    - Käytetäänkö pääsylistoja
  - Virhetilanteiden käsittely
    - Vaihtoehtoina tiedostojärjestelmä read-only tilaan, kaatuminen tai tietojen korruptoituminen
  - Kuinka kauan tietoja voidaan pitää keskusmuistissa ennen levylle kirjoitusta



Tietoturva

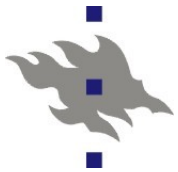
- Jokainen verkkoon näkyvä palvelu on tietoturvariski
- Linuxin palvelinohjelmistoista löytyy aukkoja yhtä säännöllisesti kuin muistakin käyttöjärjestelmistä
- Distribuution paketoimat tietoturvapäivitykset ovat paras turva ohjelmien aukkoja vastaan
- Hyväksytyn asiakasjoukon rajoituksella pienennetään riskiä (palomuurit, tcp_wrapper)
- Palveluita pyöritetään mahdollisimman vähäisin etuoikeuksin (mikä ei aina ole helppoa tai edes mahdollista)
- Palvelut on eristetty toisistaan
  - Jokaisella palvelulla oma käyttäjätunnus, oma juurihakemisto tai oma virtuaalipalvelin
- Selinux – kernelin tason järjestelmä prosessien oikeuksien rajoittamiseen

Verkkopalvelut Linuxissa

- Yksinkertaisempia verkkopalveluja hoitaa xinetd
  - Korvaa perinteisen inetd:n
- *xinetd* ”metapalvelu” käynnistää varsinaisen palveluprosessin palvelupyynnön saapuessa
- Tyypillisesti kuitenkin palvelupyyntöjä käsittelevät erilliset daemon-prosessit
  - Verkkopalveluita hoitavat prosessit vastaanottavat palvelupyyntöjä tyypillisesti IP-pistokkeiden kautta
- Eri ohjelmistoissa on tavallisesti hieman erilainen menetelmä palvelun käynnistämiseen ja sammuttamiseen
- Distribuutiot paketoivat ohjelmistot käynnistymään ja sammumaan sysvinit- tai *xinetd*-järjestelmien kautta
  - Tämä tarjoaa yhtenäisen rajapinnan palveluiden hallintaan

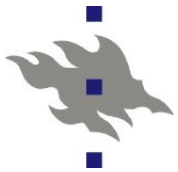
Jos jokin voi mennä pieleen...

- Kernelin bugi laitoksen meiliserverillä..
  - Meilisilmukan ansioista serverille syntyi hakemisto jossa oli ~1M tiedostoa. Ei hakemistoindeksejä.
  - Lopulta tiedostojen lukumäärä aiheutti hakemiston maksimikoon ylivuodon. Tiedostojärjestelmä korruptoitui
  - e2fsck yritti siivota 1M inodea lost+found-hakemistoon
  - e2fsck:n suoritusaika olisi ollut enemmän kuin 24h
  - Lähdekoodin muokkauksen jälkeen uusi e2fsck kesti n. 3h
- IDE-korruptio allekirjoittaneen kotikoneella...
  - RAID1-konfiguraatio, toinen levy IDE toinen SATA
  - IDE-levy ei viihtynyt DVD-aseman kanssa samalla väylällä
  - IDE-levyltä luetut bitit olivat hiljaisesti korruptoituneita
    - Kerneli ei pudottanut levyä pois RAID-pakasta
    - myös ehjä sata-levy oli vaarassa korruptoitua
  - Ext3 siirtyi read-only tilaan. E2fsck ilman hajonnutta levyä (ilmeisesti) korjasi tilanteen



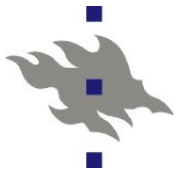
Sysvinit

- Sysvinit-järjestelmä on linux-distribuutioiden menetelmä hallita buutissa käynnistettäviä palveluja
- Asennettu ohjelmistopaketti lisää */etc/rc.d/init.d*-hakemistoon skriptin, joka osaa käynnistää ja sammuttaa palvelun
  - Skripti voi myös osata kertoa tietoja palvelun tilasta
- Ylläpitäjälle sysvinit tarjoaa työkalun
  - Asennettujen palvelujen listaamiseen
  - Automaattisesti käynnistettävien palvelujen valintaan
  - Käynnissä olevien palvelujen listaamiseen



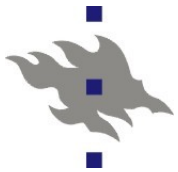
Ssh-protokolla

- Ssh-palvelin on ylläpitäjän tärkein etäylläpitotyökalu
  - Joskus jopa ainoa
  - Tatu Ylösen kehittämä perinteiset telnet, rlogin ja rsh komennot (ja protokollat) korvaava ohjelmisto
- Verkkoliikenne kryptattu
- Palvelimen ja asiakkaan identiteetin varmistus
  - Voi autentikoida salasanan sijasta salaisella avaimella
- Kerran autentikoidulla ssh-yhteydellä voidaan
  - Avata Login-istuntoja tai suorittaa komentoja
  - Tunneloida TCP-yhteyksiä
  - Tunneloida X-asiakkaita
  - Etäkäyttää tiedostoja (sftp)
- Monet komentorivin työkalut suunniteltu toimimaan ssh-yhteyden yli
  - *rsync*, *cvs*, *svn* ja *tar*



Ssh

- Ssh-ohjelmistot
  - ssh.com – se alkuperäinen, nykyään kaupallinen
  - f-secure/WRQ kaupallinen ssh-asiakas
  - Lsh – ssh GNU-lisenssillä
  - Putty – portattava OS-asiakas. Hyödyllinen windows- ja kännykkäkäyttäjille
  - Openssh – OpenBSD-projektin vanhasta ssh-v1:stä forkkaama versio. Tätä kaikki distribuutiot käyttävät
- Linux-verkkoa pystytettäessä mietittävää
  - Palvelinten julkisten avainten hallinta
  - Ylläpitoavaimet
  - Ssh-agent
  - Single sign on kerberos-lautentikoinnilla

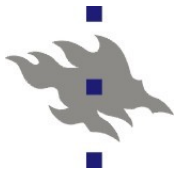


Openssh

- OpenBSD-projektin edelleen kehittämä versio vanhasta Tatu Ylösen OS ssh:sta
- Ominaisuudet
  - Tuki ssh-protokollan versioille 1 ja 2
  - Asiakas- ja palvelintuki
  - *scp* yksinkertaiseen tiedostojen kopiointiin
    - perintökalu joka ei suostu kuolemaan (rcp)
  - Sftp-palvelin
  - Yksinkertainen komentorivi sftp-asiakas
  - *ssh-agent* daemoni salaisten avainten säilytykseen
  - Kerberos-tikettien uudelleenohjaus
  - Valmiiksi autentikoidun yhteyden jakaminen
  - Nykyään myös VPN-tuki
    - Tosin IP-liikenteen tunnelointi TCP-putken yli ei ole välttämättä hyvä idea

Autentikointi ssh-avaimilla

- Ssh-protokolla osaa käyttää salaisia avaimia käyttäjän autentikointiin
  - Ja ohittaa niillä normaalin salasana-autentikoinnin
- Käyttäjä tai ylläpito luo avainparin
  - Julkinen avain talletetaan kohdekoneen käyttäjän kotihakemistoon *.ssh/authorized_keys* -tiedostoon
  - Salainen avain talletetaan levylle
    - Mielellään salasanalla kryptattuna
- Erillinen ohjelma säilyttää salaiset avaimet koneen RAM-muistissa
  - *Ssh-agent*
  - *gnome-keyring*
- Ssh-asiakas osaa käyttää levyltä tai agentilta löytyviä salaisia avaimia
  - Ssh-protokolla osaa myös tunneloida salaiset avaimet etäkoneilla (openssh -A vipu)

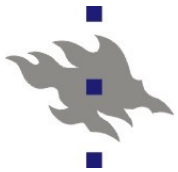


Ssh:n ongelmia

- Ei PKI-infrastruktuuria avainten jakamiseen ja allekirjoittamiseen
  - openssh:lle on X509-sertifikaattituen toteuttava paikka
  - Laitoksella 777 riviä */etc/ssh/ssh_known_hosts* -tiedostossa
  - Avaimet nimipalvelussa
- Salaisia ssh-avaimia pitää suojella yhtä hyvin kuin salasanoja
  - Levyllä salaiset avaimet pitäisi säilyttää kryptattuna
- X-yhteyksiä ei pitäisi tunneloida oletusarvoisesti
  - X on monipuolinen protokolla, jonka yli voi tehdä (ainakin) näppäinpainallusten lokia ja ruudunkaappauksia
- Vastaavasti kerberos tikettien ja *ssh-agent* yhteyksien tunnelointi voi olla vaarallista
- FUSE:n avulla kernel-tason tuki sftp-protokollalle
- Ssh-palvelinten ”koputtelu” on pysyvä ongelma
  - Löydettyjä salasanoja tai kryptaamattomia ssh-avaimia käytetään muiden palvelinten murtamiseen

Openssh:n konfigurointi

- Sshd:n konfiguraatiotiedosto */etc/ssh/sshd_config*
  - PAM:in konfiguraatiotiedosto */etc/pam.d/sshd*
  - Openssh:n autentikointiprosessi ei oletusarvoisesti toimi rootin oikeuksin, vaan erityisen autentikointia varten olevan käyttäjätunnuksen alla
- Käyttäjän kotihakemistossa
  - *.ssh/authorized_keys*
  - Käyttäjän omat luotetut ssh-avaimet ja niiden parametrit
- Ssh-asiakkaan konfiguraatiotiedosto */etc/ssh/ssh_config*
  - Tai kotihakemiston *.ssh_config*
  - Kohdekonekohtainen konfigurointi



SSL/TLS-protokolla

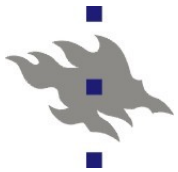
- SSL on netscape.com:in kehittämä protokolla http-yhteyksien kryptaamiseen
  - Secure Sockets Layer
  - V2.0 löytyi jo netscape 1.x selaimista
  - V3.0 on ekspiroitunut ”internet draft”, netscape-4.x selaimissa toteutettu
- TLS v1.1 on ehdotettu Internet standardi
  - RFC 4346 – Proposed Standard (huhtikuu 2006)
- X.509 - sertifikaatit
  - Joukko RFC:itä
  - PKI – Public key Infrastucture
    - Palveluiden, olioiden tai ihmisten identiteetin varmistaminen julkisilla ja salaisilla avaimilla
- Jatkossa näissä kalvoissa viitataan SSL/TLS/X.509 kolmikkoon SSL-nimellä

SSL:n ominaisuudet

- SSL-protokolla tarjoaa TCP-yhteyksien salakirjoitukseen ja palvelinten ja asiakkaiden autentikoinnin
- SSL tarjoaa seuraavat kryptografiset ominaisuudet:
  - Tiedon salaus
  - Tiedon ehjyys: muutokset havaitaan
  - Asiakas voi varmentaa palvelimen identiteetin palvelimen julkisen avaimen avulla (palvelimen sertifikaatti)
  - Palvelin voi valmistua asiakkaan identiteetistä asiakkaan julkisen avaimen avulla (asiakkaan sertifikaatti)
  - Ennestään tuntemattoman osapuolen identiteetti voidaan varmistaa kolmannen luotetun osapuolen avulla
    - Tällöin kyseinen kolmas osapuoli on aikaisemmin allekirjoittanut asiakkaan ja/tai palvelimen sertifikaatit (CA-sertifikaatilla)

SSL-Sertifikaatti

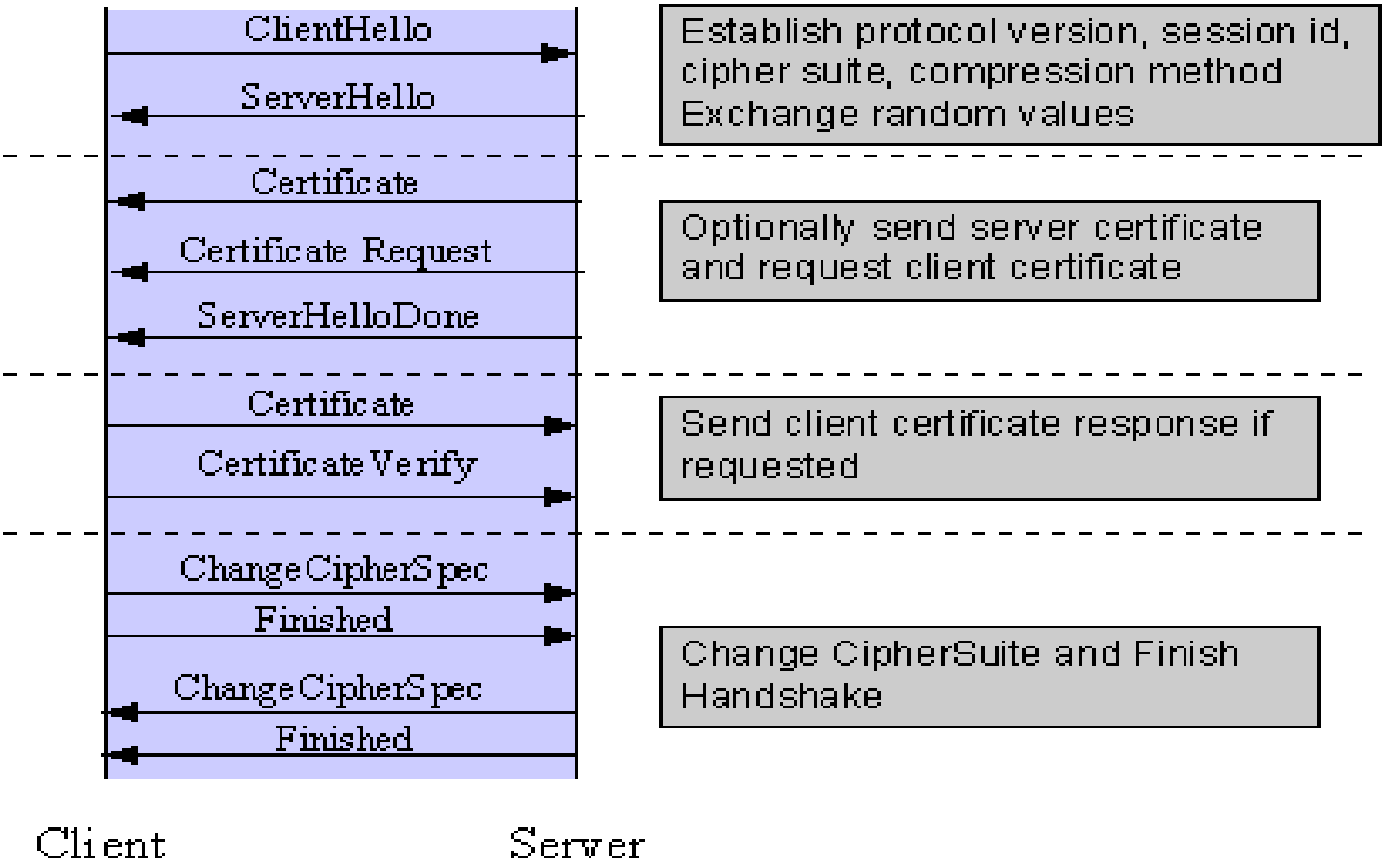
- Sertifikaatti on (jonkin) subjektin identiteetti pakattuna jonoksi bittejä
  - Sertifikaatin formaatti annettu X.509 standardissa
  - Formaatilla useita esitystapoja (valitettavasti)
  - Subjekti voi olla palvelin, henkilö, yritys, jne
- Sertifikaatti sisältää:
  - Subjektin nimen
    - Serverin tapauksessa www.serveri.com tai *.verkko.com
  - Julkisen avaimen
    - Salainen avain ei tavallisesti ole osa sertifikaattia
  - Sertifikaatin myöntäjän nimen (issuer)
    - Sertifikaatin myöntäjä on tavallisesti sertifikaatti auktoriteetti (CA, certificate authority)
  - Voimassaoloajan
  - Sertifikaatin käyttötarkoituksen
    - Käyttötarkoituksia voi rajoittaa



Erilaisia sertifikaatteja

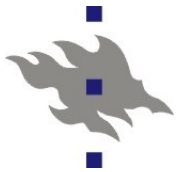
- Certificate Authority (CA) sertifikaatti
  - Luotettu juuritason sertifikaatti, joka allekirjoittaa muita sertifikaatteja
- Certicate Signing Request
  - Asiakkaan CA:lle lähettämä allekirjoittamaton sertifikaatti, jonka CA allekirjoittaa, kun allekirjoituspyynnön luotettavuus on jotenkin varmistettu
- Palvelinsertifikaatti (esim www-palvelin)
- Asiakassertifikaatti
  - Käyttäjällä oleva salainen avain (esim. Selaimessa), jolla varmistetaan käyttäjän identiteetti
  - Myös sähköpostiviestien allekirjoitukseen
  - Asiakassertifikaatti voidaan käyttää sähköpostien kryptaukseen, siten että vain viestin vastaanottaja voi avata viestin
- Certificate Revocation List sertifikaatit

SSL-neuvottelu



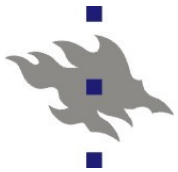
CA: Certificate Authority

- CA on luotettu kolmas taho
  - CA:lla on myös sertifikaatti
  - CA allekirjoittaa myöntämänsä sertifikaatit
  - Allekirjoitukset verifioidaan CA:n sertifikaatin julkisella avaimella
  - CA-sertifikaatti voi edelleen olla allekirjoitettu
  - Luotettuna tahona toimiminen on liiketoimintaa!
  - Selainten ja SSL-kirjastojen mukana asentuu joukko oletusarvoisesti luotettuja CA-sertifikaatteja
  - Verisign ja Thawte ovat suurimmat kaupalliset CA:t
    - Uusissa selaimissa CA vaihtoehtoja on jo paljon enemmän
  - CA:n allekirjoittama sertifikaatti on kallis
    - CA:n luotettavuus silti kyseenalaista
  - CA-sertifikaattien salaiset avaimet pidetään syvälle haudatuissa kassakaapeissa.. toivottavasti



Sertifikaatin luotettavuus?

- Viime kädessä käyttäjän pitää osata itse arvioida annetun sertifikaatin luotettavuus
- CRL - Certificate Revocation Lists
  - Vanhempi mekanismi jolla SSL-asiakkaat voivat pyytää listan sertifikaateista joihin ei enää luoteta
- OCSP – Online Certificate Status Protocol
  - Yksinkertaisempi protokolla, jolla SSL-asiakas voi tarkistaa yksittäisen sertifikaatin luotettavuuden
- Asiakasohjelmistot (tai ainakin SSL-kirjastot) tarjoavat mahdollisuuden merkata luotetut ja ei-luotetut sertifikaatit
- Verisign **on** jo kerran myöntänyt microsoft.com subject-kentällä varustetun sertifikaatin tuntemattomaksi jääneelle huijarille (ja joutui myöntämään tapauksen)
- md5-varmennetut sertifikaatit on jo murrettu

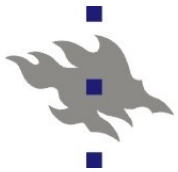


Suojatun sivun luotettavuus

- Valitettavasti keinoja man-in-the-middle -hyökkäyksiin on vaikka kuinka paljon
- Kuka tahansa voi hankkia sertifikaatin
  - Myös tietomurtohyökkäyksiin
  - Vaikka osoitteelle www.micr0soft.com
- Sertifikaateista ei ole mitään iloa, jos käyttäjät eivät lue huolella selaimen osoiterivin tekstejä
  - Jos palveluun johtava edustasivu ei ole ssl-suojattu, niin hyökkääjän kannattaa hyökätä edustasivua vastaan
  - Merkistöhyökkäyksillä voi saada väärennetyn osoiterivin näyttämään aidolta
  - SSL-suojatulla www-palvelulla ei pitäisi enää näkyä mitään kryptaamatonta, mikä voisi päätyä google-indeksiin tai kirjanmerkiksi
- Valitettavasti mikään ei auta, koska käyttäjät klikkaavat aina OK-nappia

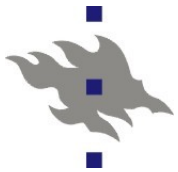
Mitä SSL ei tarjoa

- Ei suojaa tietomurtoja vastaan
- Ei suojaa DOS-hyökkäyksiltä, pikemminkin päinvastoin: SSL-neuvottelu syö CPU-aikaa
- Ei suojaa salaisen avaimen hukkumista vastaan
  - Certificate Revocation Lists (CRL) ovat standardissa (lähes) kuollut kirjain
  - Palvelimen salaisella avaimella pystyy purkamaan kaiken SSL-kryptatun liikenteen myös jälkeenpäin
  - Palvelimen salaisesta avaimesta on siis syytä pitää huolta
- Http-protokollan tapauksessa täytyy selaimen osoiterivin kenttä lukea hyvin tarkkaan
  - Sertifikaatti takaa täsmälleen vain ja ainoastaan osoiterivillä olevan serverin identiteetin. Sertifikaatti ei anna mitään takeita serverin luotettavuudesta
  - Osoiterivillä voi nykyään olla muitakin kuin ASCII-merkkejä



Hinta?

- Thawte SSL-sertifikaatti kahdeksi vuodeksi $449
- Thawte EV-sertifikaatti kahdeksi vuodeksi $995
- Sonera SSL-sertifikaatti 280e vuodeksi
  - 480e kahdeksi vuodeksi
  - 680E kolmeksi vuodeksi
- Sonera wildcard-varmenne 690e/1090e/1390e

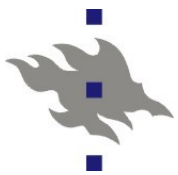


Extended Validation Certificates

- Kuka tahansa domain-nimen omistaja pystyy nykyään hankkimaan itselleen virallisen CA:n allekirjoittaman sertikaatin
  - Myös huijarit ja rikolliset
- CA:t pyrkivät palauttamaan luottamuksen sertifikaatteihin kehittämällä uudet validointikriteerit
  - Sertifikaatin omistajan on oltava tunnettu oikeustoimihenkilö, jolla on myös oikea fyysinen sijainti
  - Omistajan on omistettava domain-nimi ja todistettava että domain-nimi on hänen hallinnassaan
  - Tarkastetaan sertifikaatin ostavien henkilöiden henkilöllisyys ja heidän oikeutensa toimia sertifikaatin omistajan nimissä varmistetaan
- EVC-sertifikaatilla varmistettu sivu näkyy selaimen osoitepalkissa vihreänä
  - Ja toki tuottaa CA:lle enemmän rahaa

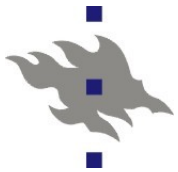
Tuoreita SSL tietoturvaongelmia

- Vaikka itse protolla toimisi, kirjastoissa on usein ongelmia
- md5-tarkastussummat sertifikaateissa
  - Vanhoissa sertifikaateissa oli vain md5-tarkastussumma
  - Sertifikaatista allekirjoitetaan vain tarkastussumma
  - Md5 on murrettu: nykyään on mahdollista generoida kaksi eri sertifikaattia, joilla on sama md5 tarkastussumma
- Null-merkit sertifikaateissa
  - CA:t ja selaimet tulkitsivat null-merkin domain nimissä eri tavalla
  - www.microsoft.com\0mundomain.com
- Uudelleenneuvottelu MITM
  - MITM ottaa yhteyden SSL-serveriin, neuvottelee yhteyden valmiiksi ja lähettää serverille joukon bittejä
  - Sitten antaa aidon SSL-asiakkaan jatkaa neuvottelun loppuun
  - Asiakas neuvottelee yhteyden: palvelimen sertifikaatti validoituu ja kaikki näyttää olevan kunnossa



SSL ja Linux-toteutukset

- OpenSSL-kirjasto
  - Oli aikoinaan standardikirjasto, jota kaikki käyttivät
  - Työkalut sertifikaattien generointiin, allekirjoituksiin, esitysmuotokonversioihin ja tarkasteluun
  - Keskitetty CA-lista */etc/pki/certs/*
  - BSD-lisenssi
- Mozilla-projektin nss-kirjasto
  - Käytössä lähinnä mozilla-projektin ohjelmistoissa
  - CA-lista on käännetty kirjastobinäärin sisään: libnssckbi.so pitää kääntää uudelleen, jos haluaa lisätä uuden CA:n
- GNU TLS: GNU-projektin TLS-toteutus
  - Ei sisällä keskitettyä sertifikaattilistaa!
    - Oletetaan, että työpöydällä on avaintenhallintaohjelma käytössä
- Javan SSL(?)



OpenSSL

- Varoitus: OpenSSL-kirjaston eri versiot eivät ole keskenään binääriyhteensopivia (edes taaksepäin)
- Sertifikaattiformaatit:
  - *.der* binääriformaatti
  - *.pem* base64-koodattu versio *.der* formaatista johon on lisätty aloitus- ja lopetusrivi
- OpenSSL-kirjaston mukana tulee yleiskäyttöinen SSL-työkalu nimeltään *openssl*
  - Openssl:n konfiguraatiotiedosto kuvattu config(5) manuaalisivussa
  - Ympäristömuuttuja OPENSSL_CONF
  - *openssl req -x509 -newkey rsa:2048 -out cacert.pem -outform PEM*
    - Generoi uuden CA-sertifikaatin pem-formaatissa ja sitä vastaavan salaisen avaimen

Openssl:n käyttö, osa 2

- *openssl x509 -in cacert.pem -noout -text*
  - Ihmisen luettava versio sertifikaatin sisällöstä
- *openssl req -newkey rsa:1024 -keyout private/csl2-crypted.pem -keyform PEM -out tempreq.pem -outform PEM*
  - Serverin salaisen avaimen ja sertifikaatin allekirjoituspyynnön (certificate request) generointi
  - Sertifikaatin yksityiskohdat tiedostossa csl2*.conf*
  - CA:n ei siis tarvitse nähdä itse salaista avainta: allekirjoituspyyntö riittää
- *openssl ca -in tempreq.pem -out hollikari_crt.pem*
  - Sertifikaattiallekirjoituspyynnön allekirjoitus CA:n toimesta

Gnutls: *certtool* -työkalu

- Helpompi käyttää kuin kilpailijoiden vastaavat
- Avaimen generointi:
  - *certtool --bits 2048 --generate-privkey --outfile ca-key.key*
- CA-sertifikaatin generointi
  - *certtool --generate-self-signed --load-privkey ca-key.key --outfile ca-cert.pem*
- Sertifikaatin tiedot:
  - *certtool -i --infile ca-cert.pem*
- Allekirjoituspyynnön generointi:
  - *certtool --generate-request --load-privkey server.key --outfile server.request*
- Sertifikaatin allekirjoitus CA:lla
  - *certtool --generate-certificate --load-request server.request --load-ca-certificate cert.pem --load-ca-privkey secret.pem --outfile server.cert*