

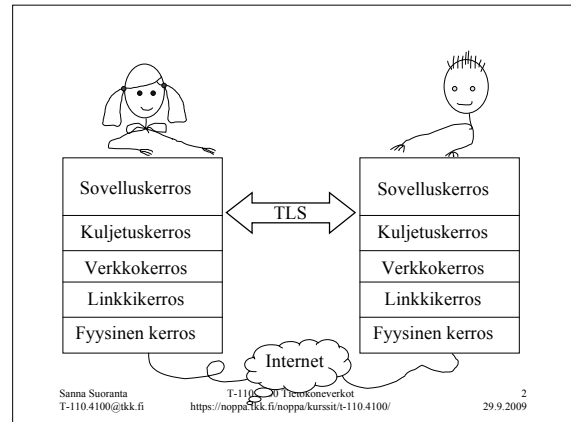
## Kuljetus- ja sovelluskerroksen tietoturvaratkaisut

Transport Layer Security (TLS)  
ja  
Secure Shell (SSH)

Sanna Suoranta  
T-110.4100@tkk.fi

T-110.4100 Tietokoneverkot  
<https://noppa.tkk.fi/noppa/kurssit/t-110.4100/>

1  
29.9.2009



## Transport Layer Security (TLS)

- Sopii monenlaisille sovellusprotokollille, esim.
  - HTTP
  - Sähköposti (IMAP)
- Toimi luotettavan kuljetusprotokolla päällä
  - esim. TCP
- Perustuu Netscapen Secure Socket Layer (SSL) protokollan versioon 3.0
  - Eivät toimi yhteen ”kuin periaatteessa”

Sanna Suoranta  
T-110.4100@tkk.fi

T-110.4100 Tietokoneverkot  
<https://noppa.tkk.fi/noppa/kurssit/t-110.4100/>

3  
29.9.2009

## TLS:n turvaama HTTP

- Kuin käyttäisi tavallista TCP-yhteyttä
  - Kuitenkin ensin sovitaan TLS-yhteyden avaamisesta
- Ennen HTTP-yhteyden sulkemista, suljetaan TLS-yhteys
  - HTTP-palvelimen toivuttava asiakkaan epämääräisestä toiminnasta
  - Jos HTTP-yhteys suljetaan suoraan, ei voida uudelleenkäyttää TLS-yhteyttä

Sanna Suoranta  
T-110.4100@tkk.fi

T-110.4100 Tietokoneverkot  
<https://noppa.tkk.fi/noppa/kurssit/t-110.4100/>

4  
29.9.2009

## TLS:n suojaama sähköposti

- SMTP-palvelin voi käyttää TLS:ää toisten SMTP-palvelimien ja asiakkaiden tunnistamiseen ja yhteyden suojaamiseen
  - Vain jos palvelimeen ei julkisesti viitata (eli se ei ole MX-rekordissa DNS:ssä!)
  - Ei estä sähköpostin kuljetusta runkoverkossa
  - Mutta ei kyllä takaa tietoturvaakaan yleisessä tapauksessa
  - SMTP-yhteys ei ole päästä-päähän yhteys!

Sanna Suoranta  
T-110.4100@tkk.fi

T-110.4100 Tietokoneverkot  
<https://noppa.tkk.fi/noppa/kurssit/t-110.4100/>

5  
29.9.2009

## TLS:n suojaama sähköposti

- Asiakasohjelman ja sähköpostipalvelimen välinen salasanakysely suojataan TLS:llä IMAP:ssa (Internet Message Access Protocol)
  - Alkuperäinen selväkielinen salasanakyselyä käyttävä menetelmä kielletään
- Kun autentikoitu yhteys on käytössä, uusitaan palvelinta koskevat tiedot sitä käyttäen
- Ei suoja sähköpostin siirtoa lähettäjältä vastaanottajalle palvelinten välillä

Sanna Suoranta  
T-110.4100@tkk.fi

T-110.4100 Tietokoneverkot  
<https://noppa.tkk.fi/noppa/kurssit/t-110.4100/>

6  
29.9.2009

## TLS:n tavoitteet

1. Turvallinen yhteys kahden osapuolen välille
2. Ohjelmoijat pystyvät luomaan TLS:ä käyttäviä sovelluksia välittämättä toistensa koodista
3. Uudet salausmenetelmät on helppo lisätä olemassaolevaan TLS:än sitä muuttamatta
4. Tehokas toiminta yhteyksiä tallettamalla

Sanna Suoranta  
T-110.4100@tkk.fi

T-110.4100 Tietokoneverkot  
<https://noppa.tkk.fi/noppa/kurssi/t-110.4100/>

7  
29.9.2009

## TLS:n toiminta

- Viestivien osapuolten
  - Yksityisyys ja
  - Siirretyn tiedon eheysturvataan
- Jokaiselle istunnolle oma symmetrinen salausavain (ei pakko käyttää salausta)
- Viesteihin lasketaan MAC (Message Authentication Code) eheyttä suojaamaan

Sanna Suoranta  
T-110.4100@tkk.fi

T-110.4100 Tietokoneverkot  
<https://noppa.tkk.fi/noppa/kurssi/t-110.4100/>

8  
29.9.2009

## TLS:n osaprotokollat

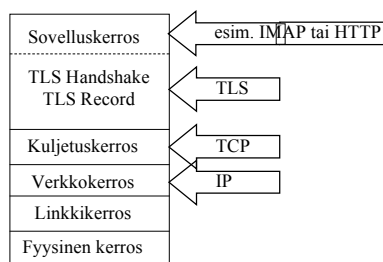
- TLS-kättelyprotokolla (Handshake Protocol)
  - Asiakas ja palvelin tunnistavat toisensa
  - Salausalgoritmin ja –avaimen sopiminen
- TLS Record Protocol
  - Istunnon viestien suojaus salaamalla
  - Myös TLS-kättelyprotokolla käyttää tätä

Sanna Suoranta  
T-110.4100@tkk.fi

T-110.4100 Tietokoneverkot  
<https://noppa.tkk.fi/noppa/kurssi/t-110.4100/>

9  
29.9.2009

## Protokollapino



Sanna Suoranta  
T-110.4100@tkk.fi

T-110.4100 Tietokoneverkot  
<https://noppa.tkk.fi/noppa/kurssi/t-110.4100/>

10  
29.9.2009

## TLS-kättely

TLS-kättely

- Osapuolen identiteetti voidaan tunnistaa joko julkisen tai salaisen avaimen menetelmällä
  - Yleensä ainakin toinen (eli palvelin) osapuolista tunnistetaan
- Sovitaan symmetrinen istuntoavain
  - Man-in-the-Middle hyökkäyksen esto
  - Hyökkääjä ei voi muuttaa eikä lukea viestejä

Sanna Suoranta  
T-110.4100@tkk.fi

T-110.4100 Tietokoneverkot  
<https://noppa.tkk.fi/noppa/kurssi/t-110.4100/>

11  
29.9.2009

## TLS-kättely

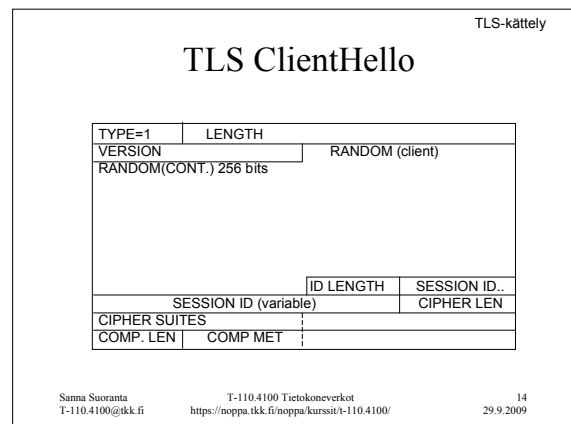
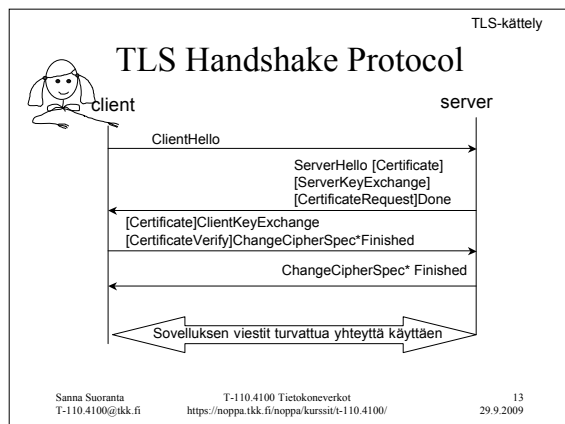
TLS-kättely

- Algoritmien sopiminen, satunnaislukujen (nonssien) vaihto
- Yhteisen salaisuuden luominen
- Sertifikaattien vaihto ja osapuol(t)en tunnistus
- Istuntoavainten luonti
- Vastapuolen tilan tarkistaminen (eli yhteinen salaisuus todella on ko. osapuolten välinen)

Sanna Suoranta  
T-110.4100@tkk.fi

T-110.4100 Tietokoneverkot  
<https://noppa.tkk.fi/noppa/kurssi/t-110.4100/>

12  
29.9.2009

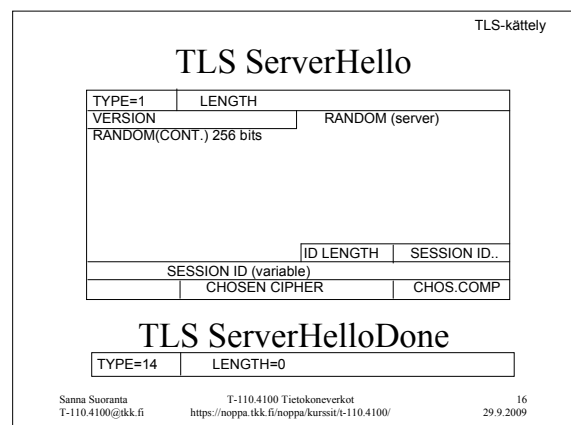


TLS-kättely

## TLS ClientHello

- RANDOM: gmt\_unix\_time+random
- SESSION ID: (pituus = 0, jos ei ole)
  - Asiakasohjelman toivoma tunniste
- CIPHER SUITE LIST
  - Asiakasohjelman tukemat salausmenetelmät, ensimmäisenä ensisijainen
  - Jokaisella kahden oktetin mittainen tunniste
- COMPRESSION METHOD
  - Asiakasohjelman tukemat tiivistysmenetelmät
  - Jokaisella oktetin mittainen tunniste

Sanna Suoranta T-110.4100 Tietokoneverkot 15  
T-110.4100@tkk.fi https://noppa.tkk.fi/noppa/kurssit/t-110.4100/ 29.9.2009



TLS-kättely

## SESSION ID Hello-viesteissä

- Jos asiakasohjelman lähettämä session id ei löydy palvelimen tietokannasta
  - uusi istunto perustetaan
- Jos löytyy ja palvelin suostuu
  - Uudelleenavataan vanha istunto
  - Käytetään vanhaa / luodaan uusi
- Jos palvelin lähettää tyhjän session id:n
  - Istunnon tietoja ei tallenneta eikä sitä voi siten avata uudelleen.

Sanna Suoranta T-110.4100 Tietokoneverkot 17  
T-110.4100@tkk.fi https://noppa.tkk.fi/noppa/kurssit/t-110.4100/ 29.9.2009

TLS-kättely

## Avaintenvaihto

- Asiakasohjelma lähettää avainmateriaalia master-avainta varten
  - salattuna palvelimen julkisella avaimella
- Yhdessä satunnaislukujen kanssa ko. avainmateriaalista saadaan master-avain
- Istuntoavaimet luodaan master-avaimesta
  - salaus- ja allekirjoitusavaimet sekä alustusvektorit

Sanna Suoranta T-110.4100 Tietokoneverkot 18  
T-110.4100@tkk.fi https://noppa.tkk.fi/noppa/kurssit/t-110.4100/ 29.9.2009

TLS-kättely

## ClientKeyExchange

|         |        |                     |
|---------|--------|---------------------|
| TYPE=16 | LENGTH |                     |
| LENGTH2 |        | MASTER SECRET (var) |

## ServerKeyExchange

|                    |        |                 |
|--------------------|--------|-----------------|
| TYPE=12            | LENGTH |                 |
| LENGTH (MODULUS)   |        | MODULUS (var)   |
| LENGTH (EXPONENT)  |        | EXPONENT (var)  |
| LENGTH (SIGNATURE) |        | SIGNATURE (var) |

Sanna Suoranta T-110.4100 Tietokoneverkot 19  
T-110.4100@tkk.fi https://noppa.tkk.fi/noppa/kurssit/t-110.4100/ 29.9.2009

TLS-kättely

## Sertifikaatit

- Palvelimen pitää (yleensä) lähettää sertifikaattinsa heti
  - Yleensä X.509-sertifikaatti
  - Sisältää palvelimen julkisen avaimen ja tunnisten
- Palvelin saattaa pyytää asiakasohjelmaa kertomaan sertifikaattinsa
  - Jos asiakkaalle ei ole sertifikaattia palvelimen sitä vaatiessa, kättely epäonnistuu

Sanna Suoranta T-110.4100 Tietokoneverkot 20  
T-110.4100@tkk.fi https://noppa.tkk.fi/noppa/kurssit/t-110.4100/ 29.9.2009

TLS-kättely

## Certificate request

|              |        |                             |
|--------------|--------|-----------------------------|
| TYPE=13      | LENGTH |                             |
| Len typelist |        | list of types of keys (var) |
| Len CA list  |        | Len CA name 1               |
|              |        | CA 1 name (var)             |
|              |        | ...                         |

## Certificate

|                |        |              |
|----------------|--------|--------------|
| TYPE=11        | LENGTH |              |
| LENGTH2        |        | CERT Len1    |
| (jatkuu)       |        | CERT 1 (var) |
| CERT Len 2 ... |        | CERT 2 ...   |

Sanna Suoranta T-110.4100 Tietokoneverkot 21  
T-110.4100@tkk.fi https://noppa.tkk.fi/noppa/kurssit/t-110.4100/ 29.9.2009

TLS-kättely

## https://www.example.com/home.html

- Palvelimen nimen (URI:ssa) pitää olla sama kuin sertifikaatissa mainittu
  - Jos asiakkaalla on jotain muuta tietoa palvelimesta, ei nimeä tarvitse tarkistaa
  - Jos nimi ei täsmää, siitä pitää kertoa käyttäjälle ja yhteys pitää katkaista
- Jos URI saatu epäluotettavasta paikasta, voi hyökkääjä vaihtaa URI:n, jolloin nimen tarkistaminen ei riitä

Sanna Suoranta T-110.4100 Tietokoneverkot 22  
T-110.4100@tkk.fi https://noppa.tkk.fi/noppa/kurssit/t-110.4100/ 29.9.2009

TLS-kättely

## ChangeCipherSpec-viesti

- Kumpikin osapuoli kertoo toisilleen, kun siirtyä käyttämään sovittuja salaus- ja tiivistysmenetelmiä
  - Viesti sisältää yhden tavun salattuna ja tiivistettynä sovitulla menetelmällä
- Kättelyn päättävät Finished-viestit, jotka lähetetään heti tämän viestin jälkeen

|         |         |        |
|---------|---------|--------|
| TYPE=20 | VERSION | LENGTH |
| =1      | =1      |        |

Sanna Suoranta T-110.4100 Tietokoneverkot 23  
T-110.4100@tkk.fi https://noppa.tkk.fi/noppa/kurssit/t-110.4100/ 29.9.2009

TLS-yhteys

## TLS Record Protocol

- Yhteyden tilatieto
  - Osapuolet: onko osapuoli asiakas vai palvelin
  - Käytetyt tiivistys-, salaus- ja eheydensuojalgoritmit
  - Käytetyt avaimet: juuriavain ja istuntoavain
- Neljäntyyppisiä tietueita
  - Käyttäjän data, kättelyviestit, hälytykset, ja salauksen muutokset

Sanna Suoranta T-110.4100 Tietokoneverkot 24  
T-110.4100@tkk.fi https://noppa.tkk.fi/noppa/kurssit/t-110.4100/ 29.9.2009

## TLS Record Protocol

1. Tiivistetään käyttäen tiivistysfunktiota
2. Lasketaan HMAC
3. Salataan
  - Täytteen avulla saadaan paketin pituus täsmäämään, jos käytetään lohkosalajaa.

### • TLS Otsikko:

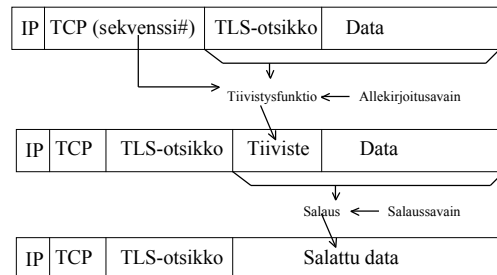
| TYPE<br>(LENGTH) | VERSION | LENGTH |
|------------------|---------|--------|
|------------------|---------|--------|

Sanna Suoranta  
T-110.4100@tkk.fi

T-110.4100 Tietokoneverkot  
<https://noppa.tkk.fi/noppa/kurssit/t-110.4100/>

25  
29.9.2009

## Suojaus



Sanna Suoranta  
T-110.4100@tkk.fi

T-110.4100 Tietokoneverkot  
<https://noppa.tkk.fi/noppa/kurssit/t-110.4100/>

26  
29.9.2009

## TLS:n laajennukset

- RFC 3546 määrittelee laajennuksia
  - Palvelimen nimi
  - Asiakkaan sertifikaatin sijainti
  - Sertifikaatin tila
  - Luotetut sertifiointiauktoriteetit
  - Jne

Sanna Suoranta  
T-110.4100@tkk.fi

T-110.4100 Tietokoneverkot  
<https://noppa.tkk.fi/noppa/kurssit/t-110.4100/>

27  
29.9.2009

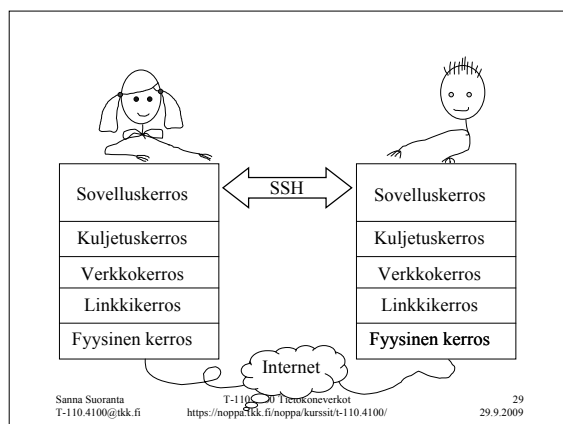
## TLS

- Sopii erilaisille sovelluksille
- Salaus ja eheys, TCP:n päällä
- Erilliset avaus- ja sulkemismekanismit TCP:n lisäksi
- Tunnistus perustuu sertifikaatteihin

Sanna Suoranta  
T-110.4100@tkk.fi

T-110.4100 Tietokoneverkot  
<https://noppa.tkk.fi/noppa/kurssit/t-110.4100/>

28  
29.9.2009



Sanna Suoranta  
T-110.4100@tkk.fi

T-110.4100 Tietokoneverkot  
<https://noppa.tkk.fi/noppa/kurssit/t-110.4100/>

29  
29.9.2009

## Secure Shell (SSH)

- Turvallinen etäyhteys palvelimeen
- Myös muita turvapalveluita yli turvattoman verkon
  - Minkä tahansa TCP/IP:n portin ja X11-yhteyden tunnelointi
  - Toimii TCP:n päällä (eli tarvitsee luotettavan kuljetuskerroksen)

Sanna Suoranta  
T-110.4100@tkk.fi

T-110.4100 Tietokoneverkot  
<https://noppa.tkk.fi/noppa/kurssit/t-110.4100/>

30  
29.9.2009

## SSH:n komponentit

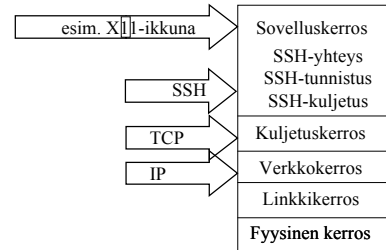
- kuljetus: Transport layer protocol
  - Palvelimen tunnistus, luotettavuus ja eheys
- tunnistus: User authentication protocol
  - Asiakasohjelman tunnistautuminen palvelimelle
- yhteys: Connection protocol
  - Limittää salatun tunnelin useampaan loogiseen kanavaan

Sanna Suoranta  
T-110.4100@tkk.fi

T-110.4100 Tietokoneverkot  
<https://noppa.tkk.fi/noppa/kurssi/t-110.4100/>

31  
29.9.2009

## SSH:n pino



Sanna Suoranta  
T-110.4100@tkk.fi

T-110.4100 Tietokoneverkot  
<https://noppa.tkk.fi/noppa/kurssi/t-110.4100/>

32  
29.9.2009

## Palvelimen avain

SSH-kuljetus

- Palvelimella pitää olla avain
  - Avaimia voi olla useampia eri algoritmeja varten
  - Useammalla palvelimella voi olla sama avain
- Palvelimen avainta käytetään avaintenvaihdon yhteydessä tunnistamaan palvelin asiakkaalle
  - Asiakkaan pitää tietää avain etukäteen
  - Palvelimen avaimen tiiviste voidaan tallettaa myös DNSään

Sanna Suoranta  
T-110.4100@tkk.fi

T-110.4100 Tietokoneverkot  
<https://noppa.tkk.fi/noppa/kurssi/t-110.4100/>

33  
29.9.2009

## Luottamusmallit

SSH-kuljetus

- Asiakasohjelmalla on paikallinen tietokanta, johon on tallennettu avain-nimipareja
  - Ei tarvita luotettavaa kolmatta osapuolta tai keskitettyä hallintaa
- Jokin luotettu kolmas osapuoli (CA) varmentaa palvelimen avaimet
  - Asiakas tietää etukäteen CA:n juuriavaimen
- Ensimmäisen yhteyden aikana ei tarkisteta

Sanna Suoranta  
T-110.4100@tkk.fi

T-110.4100 Tietokoneverkot  
<https://noppa.tkk.fi/noppa/kurssi/t-110.4100/>

34  
29.9.2009

## SSH Transport Layer Protocol

SSH-kuljetus

- Konetason tunnistus (ei käyttäjän)
- Salaus ja eheydensuojaus (+tiivistys)
  - Kumpaankin suuntaan oma
  - Joka yhteydellä omat avaimensa
- Avaintenvaihtoon käytetään Diffie-Hellman-menetelmää

Sanna Suoranta  
T-110.4100@tkk.fi

T-110.4100 Tietokoneverkot  
<https://noppa.tkk.fi/noppa/kurssi/t-110.4100/>

35  
29.9.2009

## Yhteyden sopiminen

SSH-kuljetus

- Kumpikin osapuoli lähettää listan tuetuista algoritmeista
  - salaukselle, allekirjoitukselle ja tiivistämiselle
  - Toisen osapuolen menetelmät voidaan arvata
- Suora ja epäsuora tunnistus
  - Allekirjoitus tms
  - Todistus, että palvelin tuntee yhteisen salaisuuden
- Yhteinen salaisuus ja tiiviste
  - Salaus ja eheysavaimet lasketaan näistä

Sanna Suoranta  
T-110.4100@tkk.fi

T-110.4100 Tietokoneverkot  
<https://noppa.tkk.fi/noppa/kurssi/t-110.4100/>

36  
29.9.2009

## SSH: Käyttäjän tunnistaminen

- Toimii SSH:n kuljetusprotokollan päällä
  - Eheys ja luottamuksellisuus -> yksityisyys
- Palvelin kertoo käytettävissä olevat menetelmät, joista asiakas valitsee
  - Julkinen avain
  - Salasana
  - Tunnettu tietokone
  - (ei käyttäjän tunnistusta)

## SSH-yhteys

- Etäyhteys, komentojen suorittaminen, TCP/IP-porttien ja X11-yhteyksien edelleenlähetys
  - Samaan salattuun tunneliin
  - Kumpi tahansa osapuolista voi avata yhteyskanavan ja kanavia voidaan sulkea
- Käyttää edelläesitettyjä SSH:n kuljetus- ja tunnistusprotokollia

## SSH-yhteys

| Paketin pituus  |       |
|-----------------|-------|
| Täytteen pituus | Data  |
|                 | Täyte |
| MAC             |       |

## SSH

- Turvallinen etäkäyttö
  - TCP/IP-porttien edelleenlähetys
  - X-ikkunoiden tunnelointi
- Toimii TCP:n päällä
- Palvelimen ja käyttäjän tunnistus
  - useita tapoja
- Yhteyksien liittämisen samaan turvattuun tunneliin

|                   | IPsec | TLS | SSH |
|-------------------|-------|-----|-----|
| Tunnistus         |       |     |     |
| Salauk            |       |     |     |
| Eheys             |       |     |     |
| Man in the Middle |       |     |     |
| Toistohyök.       |       |     |     |
| Yksityisyys       |       |     |     |
| DoS               |       |     |     |

## Lähteet

- RFC 2246 The TLS Protocol Version 1.0, 1999
- RFC 3546 Transport Layer Security (TLS) Extensions, 2003
- RFC 2595 Using TLS with IMAP, POP3 and ACAP, 1999
- RFC 2818 HTTP over TLS, 2000
- SSH Protocol Architecture, 2005
  - Draft-ietf-secsh-architecture-22.txt
- RFC 4253 SSH Transport Layer Protocol, 2006
- RFC 4252 SSH Authentication Protocol, 2006
- RFC 4254 SSH Connection Protocol, 2006
- RFC 4255 Using DNS to Securely Publish Secure Shell (SSH) Key Fingerprints, 2006
- C. Kaufman et al. Network Security, Prentice Hall, 2002

## Lisää turvakursseja

- T-110.4200 Tietoturvaluustekniikka
- T-110.5200 Tietoturvaluuden laboriotyöt
- T-110.5211 Cryptosystems
- T-110.5220 Tietoturva ja käytettävyys
- T-110.5230 Special course in practical security of information systems
- T-110.5240 Network security
- T-110.5290 Seminar on network security
- T-79.5501 Cryptology
- T-79.5502 Advanced course in cryptology

Sanna Suoranta  
T-110.4100@tkk.fi

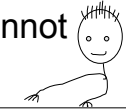
T-110.4100 Tietokoneverkot  
<https://noppa.tkk.fi/noppa/kurssit/t-110.4100/>

43  
29.9.2009

## Seuraavat luennot

6.10. Samuli Sorvakko: ohjelmointi

HUOM! To 1.10 luento  
alkaa klo 9:15!  
Aiheena harjoitustyö



Sovelluskerros

Kuljetuskerros

Verkkokerros

Linkkikerros

Fyysinen kerros

Sanna Suoranta  
T-110.4100@tkk.fi

T-110.4100 Tietokoneverkot  
<https://noppa.tkk.fi/noppa/kurssit/t-110.4100/>

44  
29.9.2009