# Seguretat a Internet

Carlos Borrego Iglesias, Sergi Robles

Calos.Borrego@uab.cat, Sergi.Robles@uab.es

Departament d'Enginyeria de la Informació i de les Comunicacions
Universitat Autònoma de Barcelona

Tecnologies avançades d'Internet

# Contingut

# Protecció de recursos

## La seguretat a Internet és

**Important** → La informació té molt valor.

**Difícil** → Cal entendre quan i com els usuaris, els ordinadors, els serveis i les xarxes han de confiar els uns en els altres. L'entorn és molt heterogeni.

La seguretat ha d'estar a tots els nivells. Un únic punt feble pot comprometre la seguretat de tot el sistema.

# Protecció de recursos

Seguretat en la xarxa i seguretat de la informació són termes que s'utilitzen en un sentit molt ampli, incloent:

- Accés a la informació i als serveis només per usuaris autoritzats
- Integritat de les dades
- Protecció contra comunicacions "punxades"
- Denegació de serveis

Cal tenir clar que la seguretat absoluta no és possible, i que generalment només s'aconseguirà que els atacs tinguin una probabilitat d'èxit molt baixa.

Un pla general per a la seguretat implica normalment la protecció de recursos lògics i físics.

## Protecció recursos

→ La protecció física inclouria la protecció de discos, panys als armaris dels routers, cables segurs, etc.

→ La protecció de recursos lògics, com ara la informació, resulta molt més complicada.

L'Enginyeria Social és també un factor extremadament important a tenir en compte (*wetware*).

→ Els humans són quasi sempre el punt més feble en un esquema de seguretat (la baula més feble de la cadena).

La seguretat de la informació engloba molts aspectes de la protecció:

**Integritat** Un sistema segur ha de protegir la informació d'alteracions no autoritzades.

**Disponibilitat** El sistema ha de garantitzar que un servei no és blocat als usuaris legítims (DoS).

**Confidencialitat** Les dades intercanviades entre dues parts han de ser secretes per a terceres parts.

**Autorització** L'accés al recurs només ha de ser possible per les parts que hi tinguin dret d'accés.

**Autenticació** Garantia de que l'origen de les dades és el que diu que és.

**No reutilització** Prevenir que terceres parts capturin i reutilitzin més tard informació intercanviada entre dues parts.

**No repudi** Evitar que alguna part implicada en un intercanvi d'informació negui haver-hi participat, totalment o parcial.

Abans d'aplicar seguretat en xarxa, una organització ha de calcular els riscos i desenvolupar una **política de seguretat** clara sobre l'accés i protecció de la informació.


## En un política de seguretat s'especifica:

- Qui té accés autoritzat a cada unitat d'informació.
- Les regles que s'han de seguir per a disseminar la informació a altres.
- Com reaccionarà l'organització a les violacions de la política de seguretat.

# Seguretat IP (IPsec)

La seguretat en una Internet és difícil ja que els datagrames que hi circulen travessen xarxes i routers que no són propietat del remitent ni del destinatari.

→ No podem confiar, doncs, en la informació dels datagrames.

Les adreces IP, així com altres camps de les capçaleres, també són fàcilment falsejables. Recordem els atacs vistos de *IP Spoofing*, per exemple.

## Per a mantenir el secret farem servir xifrat

Per a xifrar un missatge, l'emissor aplica una funció depenent d'una clau que canvia els bits deixant illegible el missatge. El receptor podrà invertir aquest procés només si coneix la clau.

$\rightarrow$ Un bon algorisme de xifrat, una clau, i un contingut del missatge ben triat poden fer extremadament difícil (mai impossible!) que hosts intermitjos puguin falsejar els confinguts.

L'IETF ha dissenyat un conjunt de protocols que permeten les comunicacions segures sobre Internet.

Aquests protocols es coneixen col·lectivament com **IPsec** (forma abreujada d'*IP security*), i ofereixen serveis d'autenticació i confidencialitat a nivell IP.

IPsec és flexible i extensible, permetent indicar exactament quines propietats de seguretat es volen de manera asimètrica (p.e. autenticació de només una part comunicant i xifrat només en un sentit).

Els algorismes d'autenticació i xifrat no estan restringits a uns d'específics, sinó que IPsec permet a cada extrem triar els algorismes i els paràmetres (com per exemple longituds de les claus).

Per a guanyar interoperabilitat IPsec inclou un conjunt mínim d'algorismes de xifrat que totes les implementacions han de reconèixer.

$\rightarrow$ IPsec no és només un protocol de seguretat, sinó que dóna un conjunt d'algorismes i un marc general que permeten a dues parts comunicants utilitzar la seguretat més adient en una situació concreta.

# Capçalera d'Autenticació

## La capçalera d'autenticació

IPsec no canvia les capçaleres habituals de IP! En lloc d'això, s'afegeix una capçalera d'autenticació separada: *Authentication Header* (**AH**).

### Datagrama IP amb TCP

| Capçalera IP | Capçalera TCP | Dades TCP |
|---|---|---|

### Datagrama IP amb AH

| Capçalera IP | **AH** | Capçalera TCP | Dades TCP |
|---|---|---|---|

El header AH va entre el de IP i el de TCP. En IPv6 és una extensió més de la capçalera.

$\rightarrow$ El camp de protocol en la capçalera IP ha de canviar! El valor **51** indica la presència del AH (*Next Header* en IPv6).

Com sap el destinatari del datagrama el protocol que va dins del datagrama?

$\rightarrow$ Hi ha un camp en el AH que indica el "següent" protocol (*next header*). IPsec posa en aquest camp el valor original que hi havia en la capçalera IP.

# Capçalera AH

| 0 7 | 8 15 | 16 31 |
|---|---|---|
| Següent capçalera | Longitud del *payload* | Reservat |
| Índex de paràmetres de seguretat | | |
| Número de seqüència | | |
| Dades d'autenticació (variable) | | |

**Longitud:** Només és la longitud del AH.
**Número de seqüència:** S'incrementa en un per cada datagrama enviat. Comença en zero.
**Índex de paràmetres de seguretat:** Especifica l'esquema de seguretat utilitzat.
**Dades d'autenticació:** Conté les dades de l'esquema de seguretat.

Un esquema de seguretat necessita molts detalls, com ara l'algorisme d'autenticació, una clau, o el temps d'utilització de l'algorisme.

$\rightarrow$ Tota aquesta informació no entra en la capçalera!

## Índex de paràmetres

Cada receptor haurà de tenir tots els detalls en una abstracció anomenada associació de seguretat. A cadascuna d'aquestes associacions se li assigna un número, l'índex de paràmetres de seguretat.

A cada datagrama se li posa l'índex de l'associació de seguretat, en comptes de tota la informació.

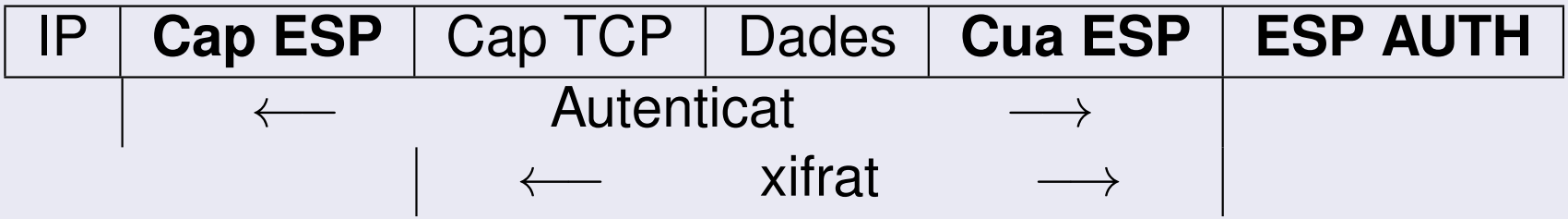
Les associacions de seguretat són negociades amb el protocol IKEv2 (*Internet Key Exchange*).

# Contingut Securitzat

## Contingut securitzat

Per a oferir confidencialitat, IPsec utilitza un "contingut securitzat": *Encapsulating Security Payload*, **ESP**.

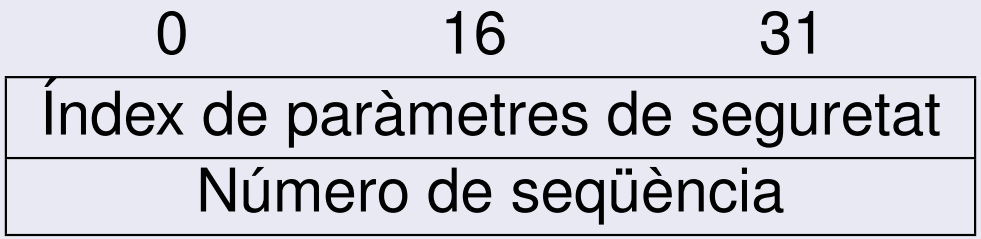
El ESP és més complexe que el AH. En el camp de protocol IP posarà el valor **50** per a indicar que el datagrama porta un ESP.



ESP afegeix tres noves parts al datagrama:

- **Capçalera ESP.** Està entre la capçalera IP i el cos xifrat.
- **Cua ESP (*ESP trailer*).** Va xifrat juntament amb el contingut.
- **ESP AUTH.** És de mida variable i anirà al final del datagrama.

## Capçalera ESP



## Cua ESP

La cua ESP conté un *padding* opcional, la longitud del *padding*, un indicador de quin és el protocol següent, i unes dades d'autenticació ESP.

| 0 — 15 | 16 — 23 | 24 — 31 |
|---|---|---|
| *Padding* (0-255) | Longitud del *pad* | Següent capçalera |
| Dades d'autenticació ESP (variable) | | |

El *padding* és opcional, però pot interessar per:

- Alguns algorismes requereixen zeros al final.
- És necessari ajustar la capçalera per alinear-la.
- Amagar la mida del datagrama original.

L'autenticació d'IPsec està dissenyada per garantitzar que el datagrama que arriba és idèntic al datagrama que va ser enviat.... o no?

L'autenticació d'IPsec està dissenyada per garantitzar que el datagrama que arriba és idèntic al datagrama que va ser enviat.... o no?

→ Això no es pot aconseguir! IP s'utilitza en transmissions de màquina a màquina (no d'extrem a extrem). Cada router li resta el TTL i recalcula el *checksum*.

## Camps Mutables

A IPsec s'anomenen **camps mutables** els camps de la capçalera de IP que poden canviar durant el trànsit.

Per a que aquests camps no portin a errors d'autenticació no s'utilitzen en els càlculs. Només s'autentiquen els camps invariants (p.e. tipus protocol o adreça origen).

# Tunneling

Els túnels IP-in-IP poden combinar-se amb IPsec per a obtenir túnels segurs (autèntics i/o confidencials).

Per a fer-ho només cal afegir al datagrama les capçaleres corresponents de IPsec:

| Capçalera IP | AH | Capçalera IP' | Dades IP |
|---|---|---|---|

Túnel autèntic ↑ ↓ túnel secret i autèntic

| IP | Cap ESP | IP' | Dades IP | Cua ESP | ESP AUTH |
|---|---|---|---|---|---|
| | autenticat | | | | |
| | | xifrat | | | |

# SSL

A mitjans dels 90 es va fer evident que la seguretat era vital pel comerç a Internet.

Molts grups van proposar mecanismes de seguretat per a utilitzar en la Web. Netscape Inc. va proposar el que esdevendria estàndard de facto: ***Secure Sockets Layer* (SSL)**.


La seva evolució és TLS (*Transport Layer Security*), essent pràcticament equivalents SSL 3.0 i TLS 1.0.

Com el seu nom indica, SSL/TLS està sobre la interfície *socket*, i és utilitzat des de la capa de transport.

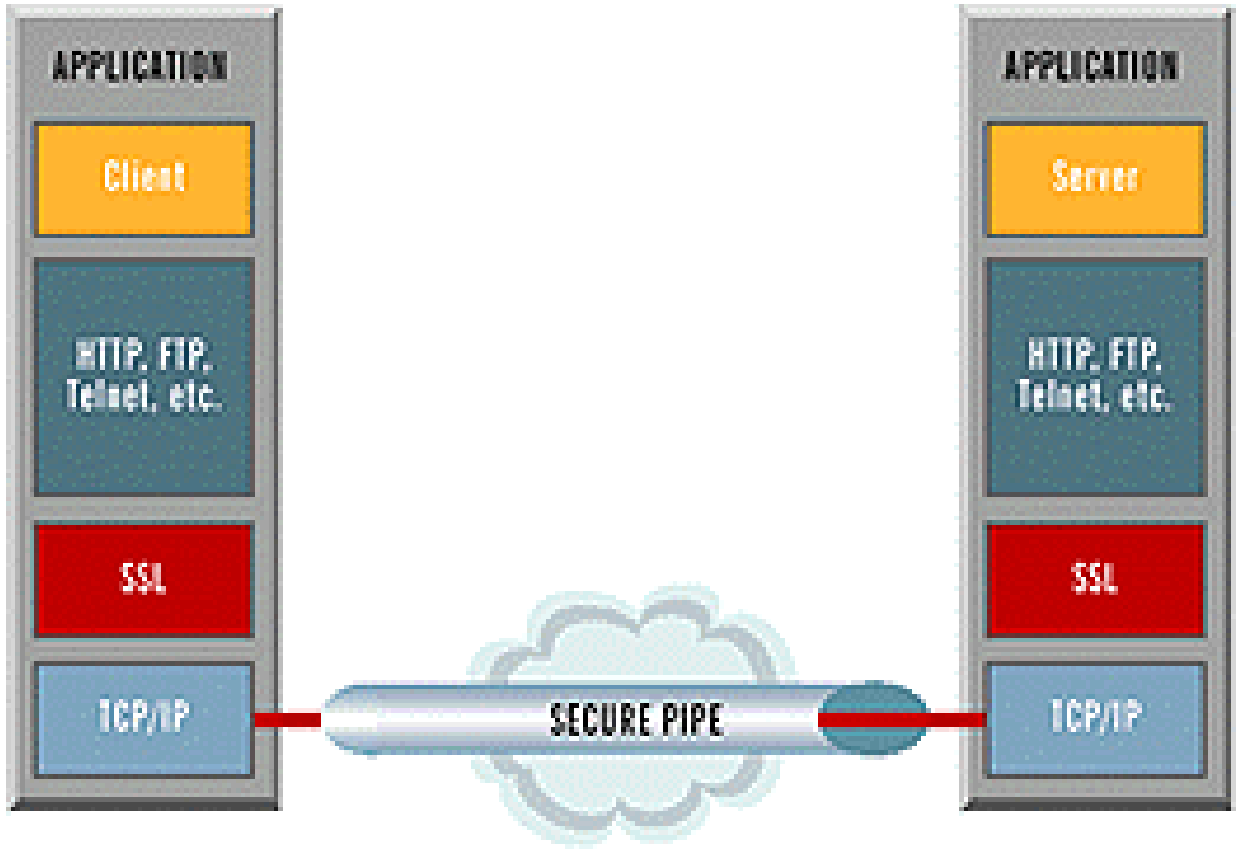
## Passes del protocol

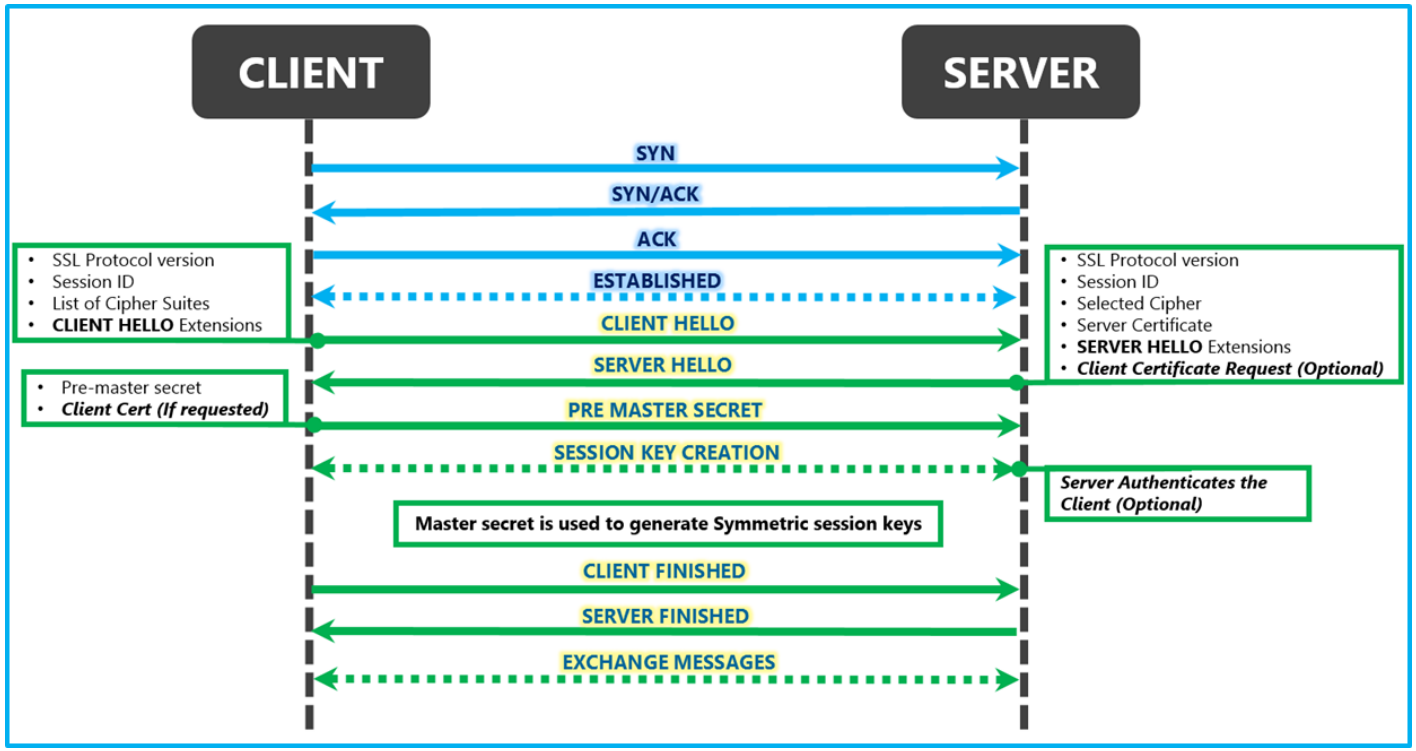
- Quan un client utilitza SSL/TLS per a comunicar-se amb un servidor, els dos extrems negocien primer l'algorisme que faran servir per autenticar-se i xifrar la informació.
- El següent pas és autenticar-se i intercanviar claus segons es què s'hagi negociaciat anteriorment.
- Finalment, els dos extrems poden transmetre informació xifrada i autèntica.

Hi ha molts protocols que utilitzen SSL/TLS per a oferir un servei segur:

- HTTPS és HTTP sobre SSL/TLS (`https://...`)
- SSH utilitza un protocol semblant a SSL/TLS per sota
- SMTP pot operar també de manera segura sobre SSL/TLS
- POP3S i IMAPS són POP3 i IMAP4 sobre SSL/TLS

La biblioteca lliure més utilitzada de SSL/TLS és `OpenSSL`.


APPLICATION
Client
HTTP, FTP,
Telnet, etc.
SSL
TCP/IP
SECURE PIPE
APPLICATION
Server
HTTP, FTP,
Telnet, etc.
SSL
TCP/IP
Add Trusted Protocol Security to Your Internet Applications
Quickly and Easily


CLIENT
SERVER
SYN
SYN/ACK
ACK
ESTABLISHED
CLIENT HELLO
SERVER HELLO
PRE MASTER SECRET
SESSION KEY CREATION
CLIENT FINISHED
SERVER FINISHED
EXCHANGE MESSAGES
• SSL Protocol version
• Session ID
• List of Cipher Suites
• CLIENT HELLO Extensions
• SSL Protocol version
• Session ID
• Selected Cipher
• Server Certificate
• SERVER HELLO Extensions
• Client Certificate Request (Optional)
• Pre-master secret
• Client Cert (If requested)
Server Authenticates the Client (Optional)
Master secret is used to generate Symmetric session keys

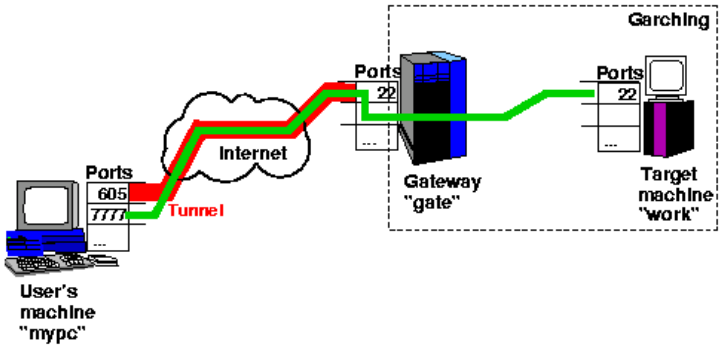
# IPsec i SSL

## Diferències entre IPsec i SSL

- IPsec dóna seguretat a baix nivell, protegint directament els datagrames IP. IPsec permet crear una xarxa segura d'ordinadors a partir de canals insegurs, com ara Internet o línies dedicades.
- SSL/TLS treballa a nivell de transport, d'extrem a extrem. SSL/TLS opera entre dos hosts que no tenen per què estar en la mateixa xarxa segura.

$\rightarrow$ SSL fa "segures" dues aplicacions, mentres que IPsec fa "segura" la xarxa.

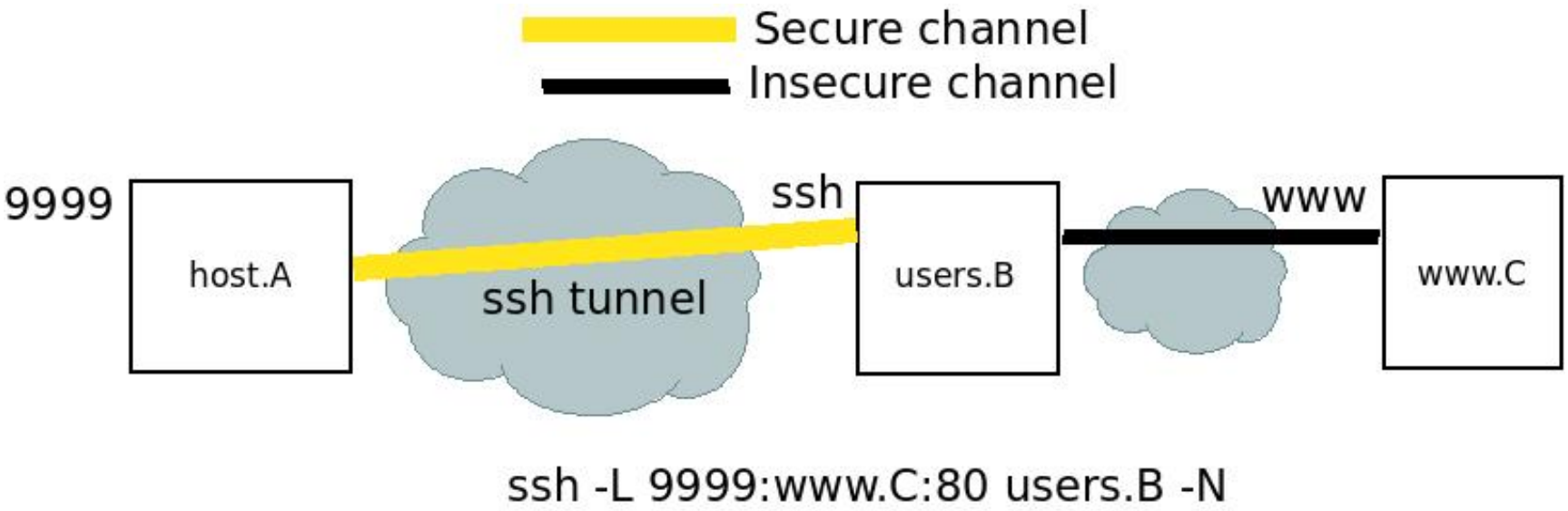
# Túnels ssh




## Arquitectura

- Un túnel SSH consisteix en un túnel xifrat mitjançant una connexió SSH.
- El client SSH "forwardejaün port local específic a un port en una maquina remota.
- Una vegada el túnel SSH s'ha establert, l'usuari pot connectar-se al port local per accedir el servei de xarxa remot.

# Túnel ssh. Exemple




ssh -L 9999:www.C:80 users.B -N

# Exemple

## Connexió http xifrada

```
ssh -L 9999:www.C:80 users.B -N

#Use tunnel from localhost (host.A)
$ telnet localhost 9999
Trying ::1...
Connected to localhost.
Escape character is ...
GET / HTTP/1.0
HTTP/1.0 302 Found
```

# Exemple

## Connexió http xifrada

```
#Des de localhost/host.A:
$ netstat -a
tcp  0   0 host.A:43722    users.B:ssh ESTABLISHED
tcp  0   0 localhost:9999       *:*    LISTEN
tcp6 0   0 ip6-localhost:9999 [::]:*   LISTEN

#Des de users.B
$ netstat -a
tcp  0   0 users.B:ssh   host.A:43722 ESTABLISHED
tcp  0   0 users.B:46946 www.C:http   ESTABLISHED

#Des de www.C
tcp  0  0 www.C:http   users.B:46946 ESTABLISHED
```

# DNSsec


## Arquitectura

- Les respostes DNSsec son signades digitalment fent servir clau publica/privada.
- Conprovant la signatura digital, un client DNS es capaç de comprovar si la informació es identica (correcte i complerta) a la informació al DNS autoritativo.
- DNSSEC no proveeix confidentialitat de les dades.
- El camp DNSKEY és autenticat fent servir *chain of trust*, començant con un cojunt de claus publiques verificades.
- El DNS root és el *trusted third party*.

# DNSsec

## Exemple de camp:

```
a.z.w.example. 3600 IN MX  1 ai.example.
a.z.w.example. 3600 RRSIG  MX 5 2 3600
           20040509183619 (
           20040409183619 38519 example.
           OMK8rAZlepfzLWW75Dxd63jy2wswESzxDKG2
           f9AMN1CytCd10cYISAxfAdvXSZ7xujKAtPbc
           tvOQ2ofO7AZJ+d01EeeQTVBPq4/6KCWhqe2X
           TjnkVLNvvhnc0u28aoSsG0+4InvkkOHknKxw
           4kX18MMR34i8lC36SR5xBni8vHI= )
```

# DNSsec

## Example de clau:

```
example.com. 86400 IN DNSKEY 256 3 5 (
                AQPSKmynfzW4kyBv015MUG2DeIQ3
                Cbl+BBZH4b/0PY1kxkmvHjcZc8no
                kfzj31GajIQKY+5CptLr3buXA10h
                WqTkF7H6RfoRqXQeogmMHfpftf6z
                Mv1LyBUgia7za6ZEzOJBOztyvhjL
                742iU/TpPSEDhm2SNKLijfUppn1U
                aNvv4w==  )
```

# Namecoin


## Arquitectura

- Namecoin és un criptomoneda bassada en BitCoin que també actua com una alternativa DNS descentralitzada.
- Evita la censura nom de domini al fer un nou domini de nivell superior (.bit) fora del control de la ICANN.
- La cadena de blocs és independent del block Bitcoin.
- Nom/valors es guarden a la cadena de blocks amb namecoins
- Els noms caduquen passat un temps.

# Namecoin


## Què és namecoin:

- https://www.youtube.com/watch?v=RwNwrfCVVvM

# Namecoin

## Registre de un nom:

```
$ ./namecoind name_new d/myname
[
    "1234567890123456789012345678901234567890",
    "0987654321"
]

#Primera assignació
$ ./namecoind name_firstupdate d/myname \
          0987654321 {"map":{"":"1.2.3.4"}}

#Actualització
$ ./namecoind name_update d/myname \
      {"map":{"":"1.2.3.4","www":"5.6.7.8"}}
```