Comunicaciones seguras

Mikel Egaña Aranguren

mikel-egana-aranguren.github.io

mikel.egana@ehu.eus

Universidad del País Vasco
Euskal Herriko Unibertsitatea
BILBOKO INGENIARITZA ESKOLA
ESCUELA DE INGENIERÍA DE BILBAO

Comunicaciones seguras

Protocolos basados en TLS/SSL - X.509 (RFC 5280):

- HTTPS: web
- S/MIME, SMTP, POP, IMAP: email
- EAP-TLS: wifi
- LDAP: autenticación
- VPN (OpenVPN): redes seguras

Transport Layer Security (TLS)

- Estándar propuesto por Internet Engineering Task Force (IETF)
- Versión actual 1.3 (RFC 8446)
- Sustituto de SSL (Secure Sockets Layer)

Transport Layer Security (TLS)

1. Comienzo TLS
2. TLS hand-shake
3. Conexión TLS propiamente dicha

Comienzo TLS

- El cliente le pide al servidor usar TLS
- HTTP: cambiar de puerto 80 a 443
- Email: comando `STARTTLS`

TLS hand-shake

- El cliente presenta al servidor una lista de algoritmos de cifrado soportados (simétricos, asimétricos, resumen)
- El servidor elige de esa lista los que soporta
- El servidor presenta un certificado al cliente; el cliente valida el certificado (con un CA)

TLS hand-shake

- El cliente genera una clave de sesión (Cifrado simétrico):
  - El cliente genera un número aleatorio, lo cifra con la clave pública del servidor y se lo envia. En el cliente y el servidor generan una clave compartida a partir de ese número
  - Usando el algoritmo Diffie-Hellman, se genera un clave secreta compartida

Conexión TLS propiamente dicha

- Solo si el hand-shake ha sido exitoso
- Los datos transmitidos se cifran con la clave de sesión y su integridad se verifica con los algoritmos resumen consensuados
- Es un conexión que mantiene el estado (stateful)

SSH (Secure Shell)

- Protocolo criptográfico para conectarse a servidores remotos
- Trust On First Use (TOFU): basta con poner nuestra clave pública en la máquina a la que nos queremos conectar
- A partir de ahi, como TLS, se usa una clave de sesión para transmitir los datos

SSH: usos habituales

- Logearse en una máquina remota y ejecutar comandos
- Transferencia de archivos mediante SFTP
- Copiar archivos mediante SCP
- Tuneles
- Port fowarding
- Conexiones X11 (Gráficos)