Komunikazio seguruak

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

Komunikazio seguruak

https://doi.org/10.5281/zenodo.4302267

https://github.com/mikel-egana-aranguren/EHU-SGSSI-01

Komunikazio seguruak

TLS/SSL - X.509 (RFC 5280) protokoloan oinarritutakoak:

- HTTPS: web
- S/MIME, SMTP, POP, IMAP: email
- EAP-TLS: wifi
- LDAP: kautotzea
- VPN (OpenVPN): sare seguruak

Transport Layer Security (TLS)

- Internet Engineering Task Force (IETF)-k proposaturiko estandarra
- Oraingo bertsioa 1.3 (RFC 8446)
- SSL (Secure Sockets Layer) ordezkatzeko

Transport Layer Security (TLS)

1. TLS hasiera
2. TLS hand-shake
3. TLS konexioa

TLS hasiera

- Bezeroak zerbitzariari TLS erabiltzeko eskatzen dio
- HTTP: 80 portutik 443 portura aldatu
- Email: `STARTTLS` komandoa

TLS hand-shake

- Bezeroak zerbitzariari balio zaizkion algoritmoen zerrenda bat aurkezten dio: simetrikoak, asimetrikoak, laburpen
- Zerbitzariak zerrenda horretatik balio zaizkionak hautatzen ditu
- Zerbitzariak bezeroari ziurtagiria aurkezten dio, bezeroak CA-ri esker baliozkotzen duena

TLS hand-shake

- Bezeroak saio gako bat sortzen du (Zifraketa simetrikoa):
  - Bezeroak ausazko zenbakia ekoizten du, zerbitzariaren gako publikoarekin zifratzen du eta zerbitzariari bidaltzen dio. Bai bezeroak bai zerbitzariak gakoa sortzen dute zenbaki horretatik abiatuta
  - Diffie-Hellman algoritmoa erabiliz gako amankomun bat sortzen dute bezeroak eta zerbitzariak

TLS konexioa

- hand-shake ondo atera bada soilik
- Datuak sesio gakoarekin zifratzen dira eta osotasuna adostutako laburpen algoritmoekin bermatzen da
- Egoera mantentzen duen konexioa da (stateful)

SSH (Secure Shell)

- Urruneko zerbitzarietara konektatzeko erabiltzen den protokolo kriptografikoa
- Trust On First Use (TOFU): konexioa ezartzeko gure klabe publikoa urruneko zerbitzarian jartzea nahiko dugu
- Hortik aurrera, TLS moduan, saio gako bat erabiltzen da datuak transmitizeko

SSH: erabilpenak

- Urruneko makina batean sartu eta komandoak exekutatu
- SFTP bidezko artxiboen transferentzia
- SCP bidez datuak kopiatu
- Tunelak
- Port fowarding
- X11 (Grafikoak)