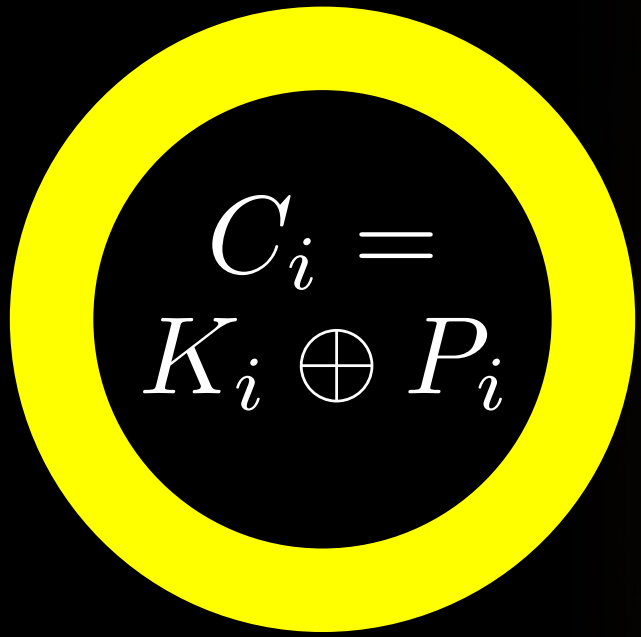
Keys to the kingdom

András Veres-Szentkirályi (Silent Signal)

Camp++ 0x7e1
2017-07-07

Content advisory



Because of practical simplifications, this talk should only be attended by cryptographers if accompanied by a non-cryptographer

RSA

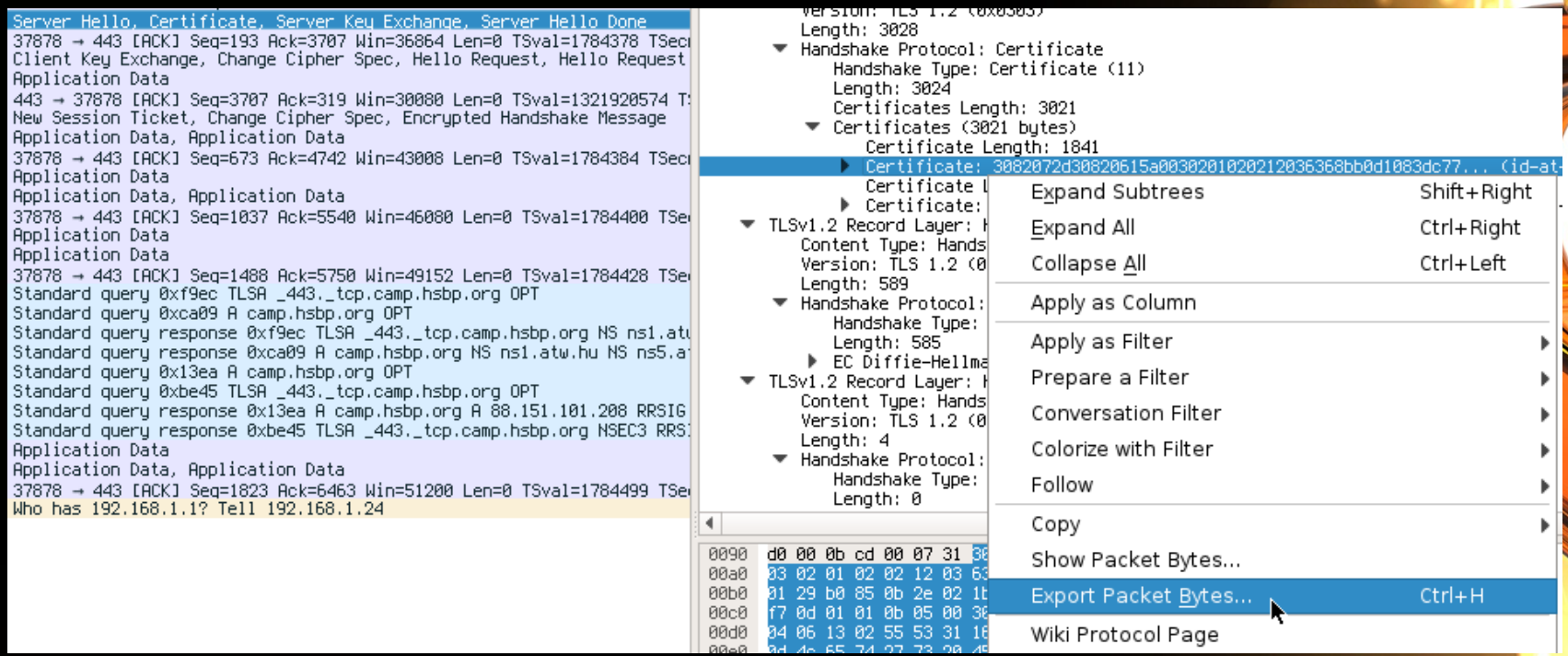
- public key: n, e
  - latter is typically 0x10001 $\Rightarrow$ see cleptography
- private key: d
- encryption: $(m^e)^d \equiv m \pmod{n}$
- signing: $(m^d)^e \equiv m \pmod{n}$
- padding schemes: PKCS1 1.5, OAEP, PSS
- OpenSSL: `rsa` and `rsautl`

X.509

- certificate serialization based on ASN.1
  - X says that the public key of Y is Z
  - $RSA_{PUB_X}(Y||PUB_Z)$
- RSA, SHA-1/SHA-2
- OpenSSL: `x509` and asn1parse

Sniffing certificates

- Wireshark
- SSL/TLS Certificates packet right after Server Hello



Pinning

- certificate vs. key pinning
- hash vs. “the real thing”
- HPKP: SHA2 of ASN.1 encoded key

Java KeyStore

- password protected binary storage
- CLI management program: `keytool`
- JCA legal problems result in Android using *Bouncy Castle* (BKS) instead of *Sun* (JKS)
- 15:12 Nail in the Java Key Store Coffin by Tobias “Floyd” Ospelt in PoC||GTFO 15 pg. 89 $\Rightarrow$ 8 billion password tries per second on single NVidia GTX 1080 GPU

PKCS#12

- password protected binary storage
- complex standard
- CLI management program: `openssl pkcs12`


Thanks for your attention!
Facebook
vsza@silentsignal.hu
web
e-mail
SILENT SIGNAL
VÉSZJELZÉS HELYETT...
WWW.SILENTSIGNAL.HU