

Keys to the kingdom

András Veres-Szentkirályi (Silent Signal)

Camp++ 0x7e1
2017-07-07

$$C_i = K_i \oplus P_i$$

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

- ▶ 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`

- ▶ 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

The image shows a Wireshark network traffic capture. The main pane displays a list of packets, with the selected packet being a TLS Certificate. The packet details pane on the right shows the structure of the certificate, including the handshake protocol, handshake type, and the certificate itself. The packet bytes pane at the bottom shows the raw data of the certificate in hexadecimal and ASCII format.

```
Server Hello, Certificate, Server Key Exchange, Server Hello Done
37878 -> 443 [ACK] Seq=193 Ack=3787 Win=36864 Len=0 TSval=1784378 TSecr
Client Key Exchange, Change Cipher Spec, Hello Request, Hello Request
Application Data
443 -> 37878 [ACK] Seq=3787 Ack=319 Win=30080 Len=0 TSval=1321928574 T
New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
Application Data, Application Data
37878 -> 443 [ACK] Seq=673 Ack=4742 Win=43008 Len=0 TSval=1784384 TSecr
Application Data, Application Data
37878 -> 443 [ACK] Seq=1837 Ack=5540 Win=46080 Len=0 TSval=1784400 TSecr
Application Data, Application Data
37878 -> 443 [ACK] Seq=1488 Ack=5750 Win=49152 Len=0 TSval=1784428 TSecr
Standard query 0xc19ec TLSA _443._tcp.camp.hsbg.org OPT
Standard query 0xc0a89 A camp.hsbg.org OPT
Standard query response 0xc19ec TLSA _443._tcp.camp.hsbg.org NS ns1.atu
Standard query response 0xc0a89 A camp.hsbg.org NS ns1.atu.HS ns5.a
Standard query 0x13ea A camp.hsbg.org OPT
Standard query 0xbe45 TLSA _443._tcp.camp.hsbg.org OPT
Standard query response 0x13ea A camp.hsbg.org A 80.151.101.208 RRSIG
Standard query response 0xbe45 TLSA _443._tcp.camp.hsbg.org NSEC3 RRSIG
Application Data, Application Data
37878 -> 443 [ACK] Seq=1823 Ack=6463 Win=51200 Len=0 TSval=1784499 TSecr
Who has 192.168.1.1? Tell 192.168.1.24
```

Version: TLS 1.2 (0x0303)
Length: 3028
Handshake Protocol: Certificate
Handshake Type: Certificate (11)
Length: 3024
Certificates Length: 3021
Certificates (3021 bytes)
Certificate Length: 1841
Certificate: 3062072d38828615a0836201820212036368bb0d1863dc77... (id=at)
Certificate:
Content Type: Handshake
Version: TLS 1.2 (0x0303)
Length: 589
Handshake Protocol:
Handshake Type:
Length: 585
EC Diffie-Hellman
TLSv1.2 Record Layer: Handshake
Version: TLS 1.2 (0x0303)
Length: 4
Handshake Protocol:
Handshake Type:
Length: 0

Expand Subtrees Shift+Right
Expand All Ctrl+Right
Collapse All Ctrl+Left
Apply as Column
Apply as Filter
Prepare a Filter
Conversation Filter
Colorize with Filter
Follow
Copy
Show Packet Bytes...
Export Packet Bytes... Ctrl+H
Wiki Protocol Page

0090 00 00 0b cd 00 07 31 58
00a0 83 02 01 02 02 12 03 65
00b0 01 23 00 05 0b 2e 02 11
00c0 07 0d 01 01 0b 05 00 3d
00d0 04 06 13 02 55 53 31 18
00e0 01 41 55 7a 27 73 2a 18

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 ⇒ 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