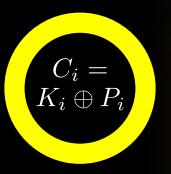
Keys to the kingdom

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 $0 \times 10001 \Rightarrow$ see cleptography
- private key: d
- encryption: $(m^e)^d \equiv m \pmod{n}$
- ightharpoonup signing: $(m^d)^e \equiv m \pmod{n}$
- ▶ padding schemes: PKCS1 1.5, OAEP, PSS
- OpenSSL: rsa and rsaut1





X.509

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





Sniffing certificates

Wireshark

Standard query response 0x13ea A camp.hsbp.org A 88.151.101.208 RRSIG Standard query response 0xbe45 TLSA _443._tcp.camp.hsbp.org MSEC3 RRSI

37878 → 443 [RCK] Seq=1823 Rck=6463 Win=51288 Len=8 TSval=1784499 TSe

SSL/TLS Certificates packet right after Server Hello

ver Hello, Certificate, Server Keu Exchange, Server Hello Done Length: 3028 37878 → 443 [ACK] Seg=193 Ack=3787 Win=36864 Len=8 TSval=1784378 TSeg ▼ Handshake Protocol: Certificate Client Keu Exchange, Change Cipher Spec, Hello Request, Hello Request Handshake Tupe: Certificate (11) Application Data Length: 3024 443 → 37878 [ACK] Seg=3707 Ack=319 Win=30080 Len=0 TSval=1321920574 T Certificates Length: 3021 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message ▼ Certificates (3021 butes) Application Data, Application Data Certificate Length: 1841 37878 - 443 [ACK] Seg=673 Ack=4742 Win=43008 Len=0 TSval=1784384 TSeci Application Data Certificate D Expand Subtrees Application Data, Application Data ▶ Certificate: 37878 → 443 FBCK1 Sen=1837 Bck=5548 Win=46888 Len=8 TSval=1784488 TSe TLSv1.2 Record Layer: F Expand All Application Data Content Type: Hands Application Data 37878 → 443 [RCK] Seg=1488 Rck=5750 Win=49152 Len=0 TSval=1784428 TSec Standard guery 0xf9ec TLSA _443._tcp.camp.hsbp.org OPT Standard guery 0xca09 A camp.hsbp.org 0P1 Standard query response 0xf9ec TLSR _443._tcp.camp.hsbp.org NS ns1.ati Standard gueru response 0xca09 A camp.hsbp.org NS ns1.atv.hu NS ns5.a Standard gueru 0x13ea A camp.hsbp.org OPT Standard gueru 0xbe45 TLS0 443, tcp.camp.hsbp.org OPT

Length: ▼ Handsha Hand Leng ▶ EC I ▼ TLSv1.2 Ren Content Version	Version: TLS 1.2 (0) Length: 589 ▼ Handshake Protocol: Handshake Tupe: - Length: 585 ▶ EC Diffie-Hellma	Collapse <u>A</u> ll	Ctrl+Left
		Apply as Column	
		Apply as Filter	
	TLSv1.2 Record Layer: F	Prepare a Filter	
	Content Type: Hands Version: TLS 1.2 (0	Conversation Filter	
	Length: 4 ▼ Handshake Protocol:	Colorize with Filter	
	Handshake Type: Length: 0	Follow	
		Сору	
898 8a8	d0 00 0b cd 00 07 31 36 83 82 81 82 82 12 83 63	Show Packet Bytes	
868 868	81 29 b8 85 8b 2e 82 lt f7 8d 81 81 8b 85 88 36	Export Packet <u>B</u> ytes	Ctrl+H
8d8	84 86 13 82 55 53 31 16 8d 4c 65 74 27 73 28 45	Wiki Protocol Page	



Who has 192,168,1,1? Tell 192,168,1,24

Application Data
Application Data, Application Data

Shift+Right

Ctrl+Right

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: openss1 pkcs12





Thanks for your attention!

Facebook vsza@silentsignal.hu

web

e-mail