Workshop
Applied Crypto Hardening

bettercrypto·org

Agenda

Warum?

Ein wenig in die Theorie

Hardening Ciphersuites

Konfiguration von Services

Q&A

Warum?

Theorie

Block vs Stream Cipher (AES vs RC4)

Key Exchange (DH)

Public Key Encryption (TLS, GPG)

Hash Functions (MD5,SHA2)

Message Authentication Codes (SHA2)

Authenticated Encryption with Associated Data (GCM SHA384)

Keylength (128bit vs 256bit)

openssl cipher suite schreibweise

KeyExchange	Authentication	Cipher	MAC
EDH	RSA	AES256	SHA256

KeyExchange	Authentication	Cipher	AEAD
EDH	RSA	AESGCM	SHA384

Cipher A

Starke Ciphers jedoch weniger Clients

- TLS 1.2
- Perfect forward secrecy / **e**phemeral DH
- Starke MACs (SHA2)

```
EDH+aRSA+AES256:EECDH+aRSA+AES256:!SSLv3
```

Kompatibilität

WIN7/WIN8.x

OpenSSL ≥ 1.0.1e

Safari 6 iOS 6.0.1

Safari 7 OS X 10.9

Cipher B

Nicht so starke Ciphers jedoch mehr Clients

- TLS 1.2, TLS 1.1, TLS 1.0
- Perfect forward secrecy / ephermal DH
- MAC SHA1 … ja aber was mit 2^{63} Ops Kollisionen?

Cipher B

Mehr Clients mehr Platz

```
EDH+CAMELLIA:EDH+aRSA:EECDH+aRSA+AESGCM:EECDH+aRSA+SHA384:EECDH+aRSA+SHA256:EECDH:+CAMELLIA256:+AES256:+CAMELLIA128:+AES128:+SSLv3:!aNULL:!eNULL:!LOW:!3DES:!MD5:!EXP:!PSK:!DSS:!RC4:!SEED:!ECDSA:CAMELLIA256-SHA:AES256-SHA:CAMELLIA128-SHA:AES128-SHA
```

Genug Theorie
ran an das Gerät

Services

Check via Internet

Webserver:	https://ssllabs.com
Mailserver:	https://starttls.info
XMPP:	https://xmpp.net
SSH Key Check:	http://factorable.net/keycheck.html
Browser:	https://howsmyssl.com

Check via Commandline

cipherscan:https://github.com/MacLemon/cipherscan

sslyze: https://github.com/iSECPartners/sslyze

sslscan: apt-get install sslscan

...

nmap –script=ssl-enum-ciphers || ssl-cert IP -p443

openssl s_client -connect http://host:443

Kontakt

W: http://bettercrypto.org

M: http://lists.cert.at/cgi-bin/mailman/listinfo/ach

G: https://github.com/BetterCrypto/Applied-Crypto-Hardening/