Hasso Plattner Institut
Digital Engineering · Universität Potsdam

Exploiting Export Ciphers in TLS

Kryptanalytische Angriffe auf Internet-Protokolle

2021-08-06

Hadrian Burkhardt, Oliver Derwisch, Daniel Goßen, Niko Lockenvitz

Agenda

- How Does the Attack Work?
- How to Compute the Discrete Log?
- Live Demo

TLS Handshake - Ephemeral Diffie-Hellman

ClientHello: I can speak DHE_3DES, DHE_AES128, ...

ServerHello: Let's talk DHE_AES128
Certificate
ServerKeyExchange: 1024 bit prime, g, g^{Ys} (signed)
ServerHelloDone

$k = (g^{Ys})^{Yc}$ ClientKeyExchange: g^{Yc} $k = (g^{Yc})^{Ys}$

Finished: Hash(handshake)

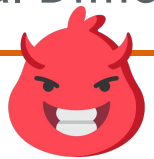
Finished: Hash(handshake)

GET /

...

TLS Handshake - Ephemeral Diffie-Hellman

ClientHello: I can speak DHE_3DES, DHE_AES128, ...



ClientHello: I can speak DHE_EXPORT_DES40

ServerHello: Let's talk DHE_AES128

ServerHello: Let's talk DHE_EXPORT_DES40
Certificate
ServerKeyExchange: 512 bit prime, g, g^{Ys} (signed)
ServerHelloDone

Compute Ys

$k = (g^{Ys})^{Yc}$ ClientKeyExchange: g^{Yc} $k = (g^{Yc})^{Ys}$

Finished: Hash(handshake)

Finished: Hash(handshake)

Finished: Hash(handshake)

Finished: Hash(handshake)

GET /

GET /

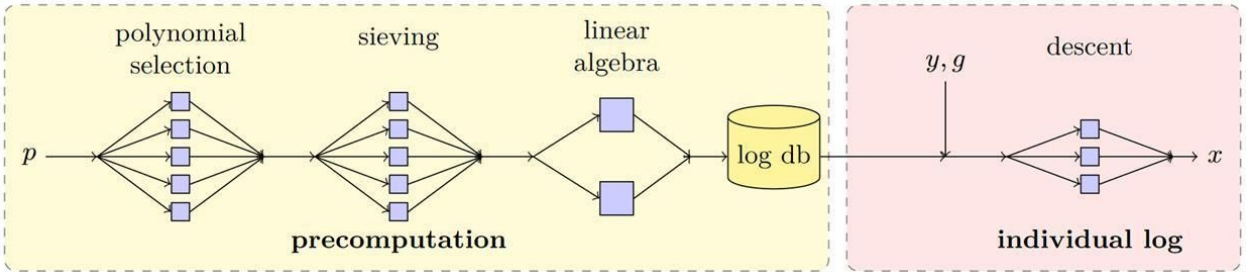
...

Exploiting Export Ciphers in TLS

Burkhardt, Derwisch, Goßen, Lockenvitz
2021-08-06

Computing the Discrete Log: Four Phases

- Discrete Log can be computed with enough resources
- Four phases where only the last one depends on the public key
- We did a pre-computation for a 512 bit prime

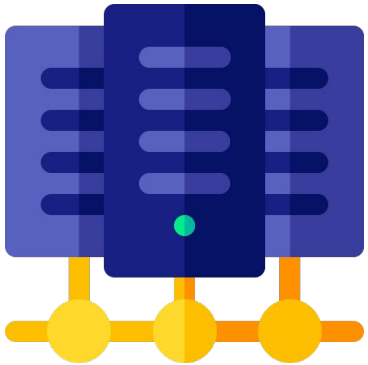


Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice, 22nd ACM Conference on Computer and Communications Security, October 2015

Exploiting Export Ciphers in TLS

Burkhardt, Derwisch, Goßen, Lockenvitz
2021-08-06

Cluster & Runtime



Cluster (Future SOC Lab):

- 15 nodes, each 40 CPU cores, 1 TiB RAM
- Only effectively used during early stages
- MPI usage was not efficient to parallelize tasks
- Linear algebra was executed on only 1 node

Runtime:

- Polynomial selection ~7,600 core-hours (~2 days)
- Sieving ~21,400 core-hours (~5 days)
- Linear algebra ~15,000 core-hours (~2 weeks)
- Descent ~25 core-min (~80 s)

Why Are Pre-Computations Worth It?

Source	Popularity	Prime
Apache	82%	9fdb8b8a004544f0045f1737d0ba2e0b 274cdf1a9f588218fb435316a16e3741 71fd19d8d8f37c39bf863fd60e3e3006 80a3030c6e4c3757d08f70e6aa871033
mod_ssl	10%	d4bcd52406f69b35994b88de5db89682 c8157f62d8f33633ee5772f11f05ab22 d6b5145b9f241e5acc31ff090a4bc711 48976f76795094e71e7903529f5a824b
(*others*)	8%	(463 distinct primes)

Table 1: **Top 512-bit DH primes for TLS.** 8.4% of Alexa Top 1M HTTPS domains allow DHE_EXPORT, of which 92.3% use one of the two most popular primes, shown here.

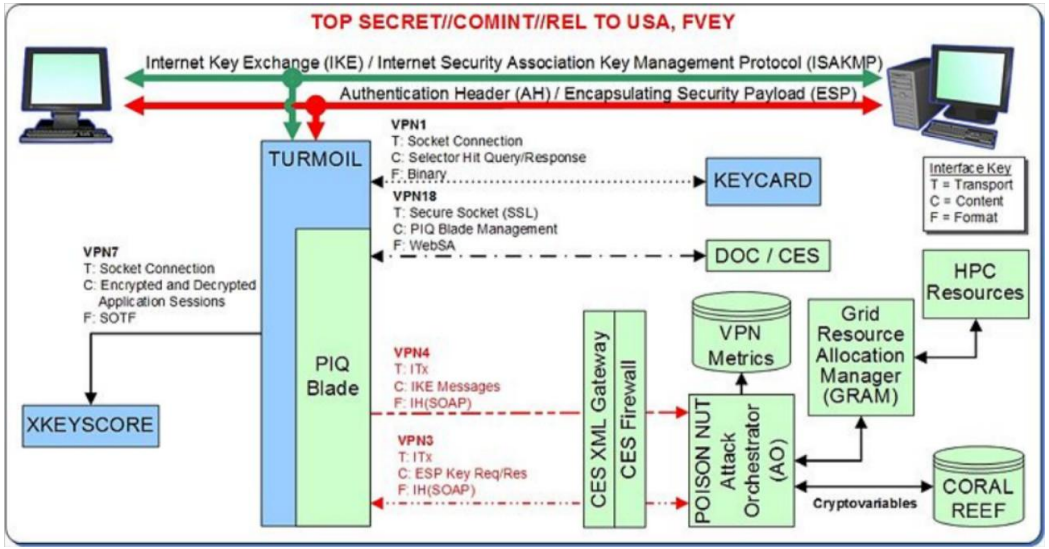
- Pre-computation of two 512 bit DH primes for TLS is enough to attack ~78,000 of Alexa Top 1M HTTPS domains
- Attacking 1024 bit and above is currently only achieved by state-level adversaries

Exploiting Export Ciphers in TLS

Burkhardt, Derwisch, Goßen, Lockenvitz
2021-08-06

Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice, 22nd ACM Conference on Computer and Communications Security, October 2015

Nation-State Actors



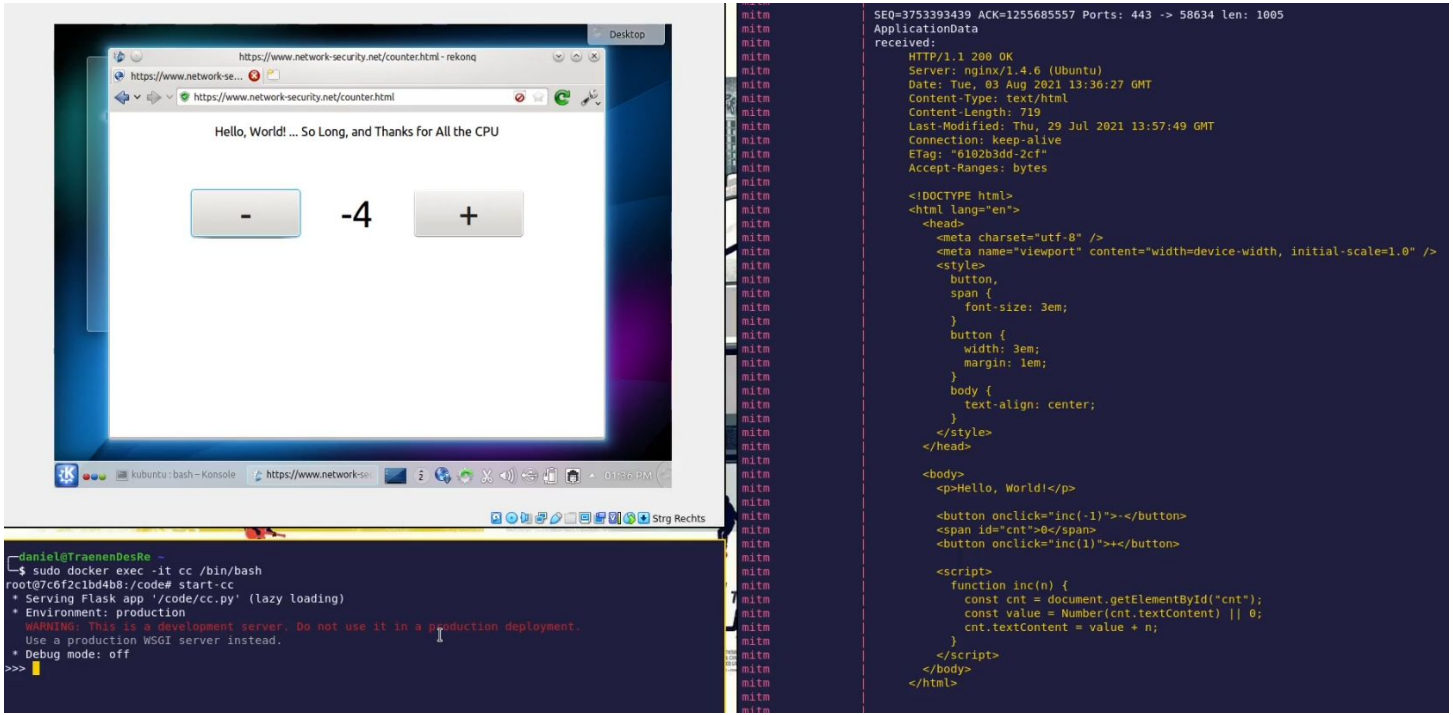
NSA suspected to use a similar approach for passive IPSec VPN decryption

Exploiting Export Ciphers in TLS

Burkhardt, Derwisch, Goßen, Lockenvitz
2021-08-06

TURMOIL VPN processing. Media leak, Oct. 2009. https://web.archive.org/web/20150103031005/www.spiegel.de/media/media-35527.pdf

Live Demo



Exploiting Export Ciphers in TLS

Burkhardt, Derwisch, Goßen, Lockenvitz
2021-08-06

Impact of the Attack

	Vulnerable servers, if the attacker can precompute for . . .			
	all 512-bit groups	all 768-bit groups	one 1024-bit group	ten 1024-bit groups
HTTPS Top 1M w/ active downgrade	45,100 (8.4%)	45,100 (8.4%)	205,000 (37.1%)	309,000 (56.1%)
HTTPS Top 1M	118 (0.0%)	407 (0.1%)	98,500 (17.9%)	132,000 (24.0%)
HTTPS Trusted w/ active downgrade	489,000 (3.4%)	556,000 (3.9%)	1,840,000 (12.8%)	3,410,000 (23.8%)
HTTPS Trusted	1,000 (0.0%)	46,700 (0.3%)	939,000 (6.56%)	1,430,000 (10.0%)
IKEv1 IPv4	–	64,700 (2.6%)	1,690,000 (66.1%)	1,690,000 (66.1%)
IKEv2 IPv4	–	66,000 (5.8%)	726,000 (63.9%)	726,000 (63.9%)
SSH IPv4	–	–	3,600,000 (25.7%)	3,600,000 (25.7%)

Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice, 22nd ACM Conference on Computer and Communications Security, October 2015

Exploiting Export Ciphers in TLS

Burkhardt, Derwisch, Goßen, Lockenvitz
2021-08-06