



# Exploiting Export Ciphers in TLS

Kryptanalytische Angriffe auf Internet-Protokolle

2021-08-06

Hadrian Burkhardt, Oliver Derwisch, Daniel Goßen, Niko Lockenvitz

# Agenda

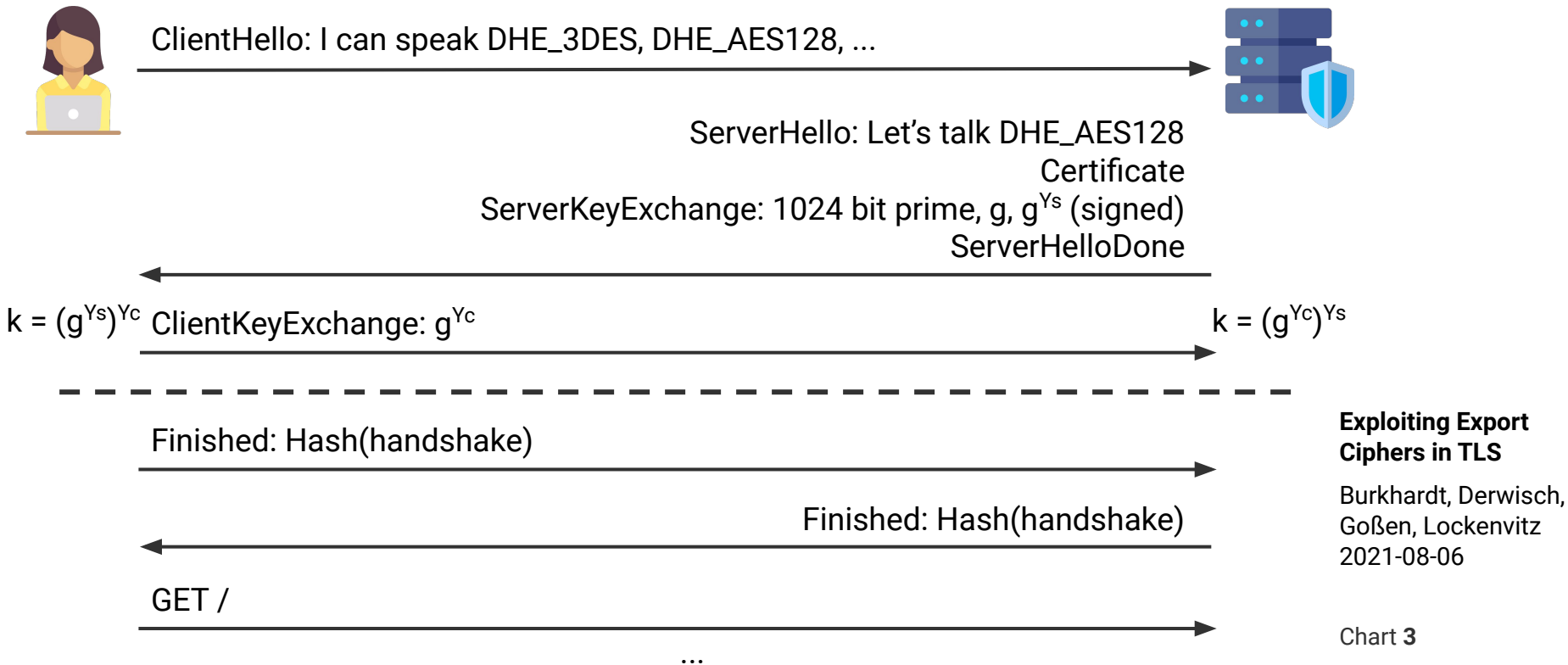
---

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

## **Exploiting Export Ciphers in TLS**

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

# TLS Handshake - Ephemeral Diffie-Hellman

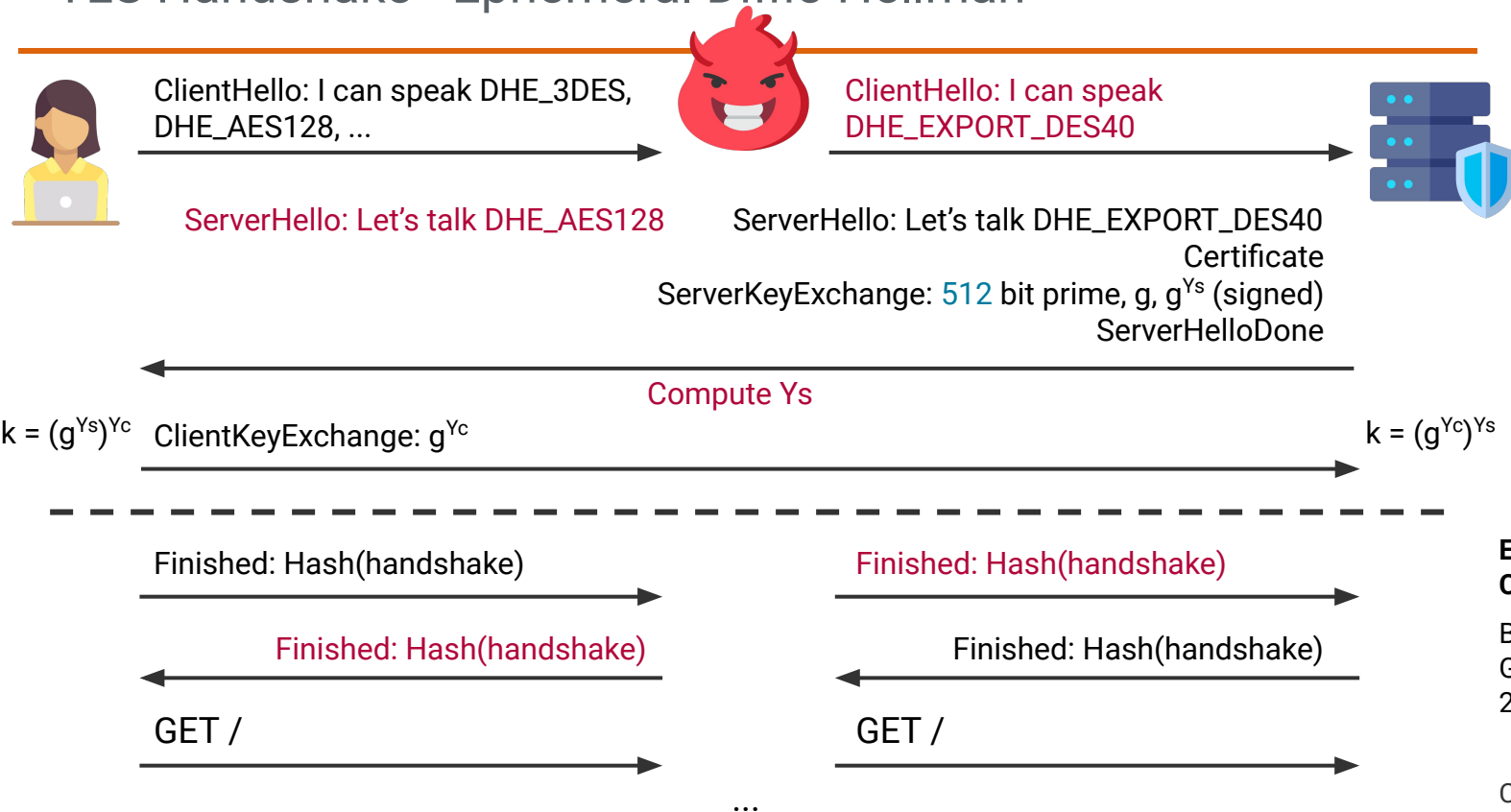


**Exploiting Export  
Ciphers in TLS**

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

Chart 3

# TLS Handshake - Ephemeral Diffie-Hellman



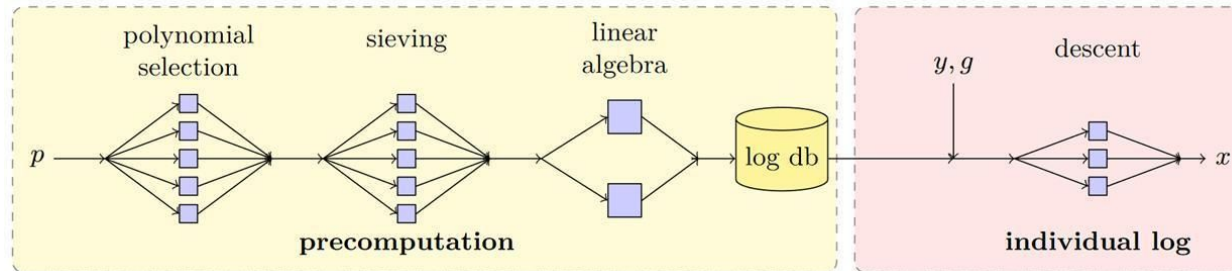
## Exploiting Export Ciphers in TLS

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

Chart 4

# 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

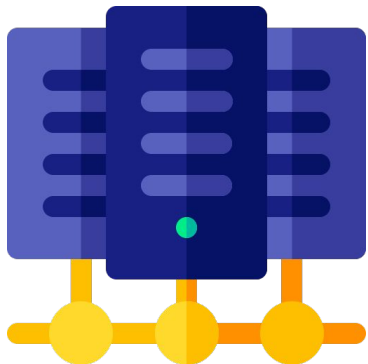


## Exploiting Export Ciphers in TLS

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

Chart 5

# 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)

## Exploiting Export Ciphers in TLS

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

Chart 6

# Why Are Pre-Computations Worth It?

Source	Popularity	Prime
Apache	82%	9fdb8b8a004544f0045f1737d0ba2e0b274cdf1a9f588218fb435316a16e374171fd19d8d8f37c39bf863fd60e3e300680a3030c6e4c3757d08f70e6aa871033
mod_ssl	10%	d4bcd52406f69b35994b88de5db89682c8157f62d8f33633ee5772f11f05ab22d6b5145b9f241e5acc31ff090a4bc71148976f76795094e71e7903529f5a824b
(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.

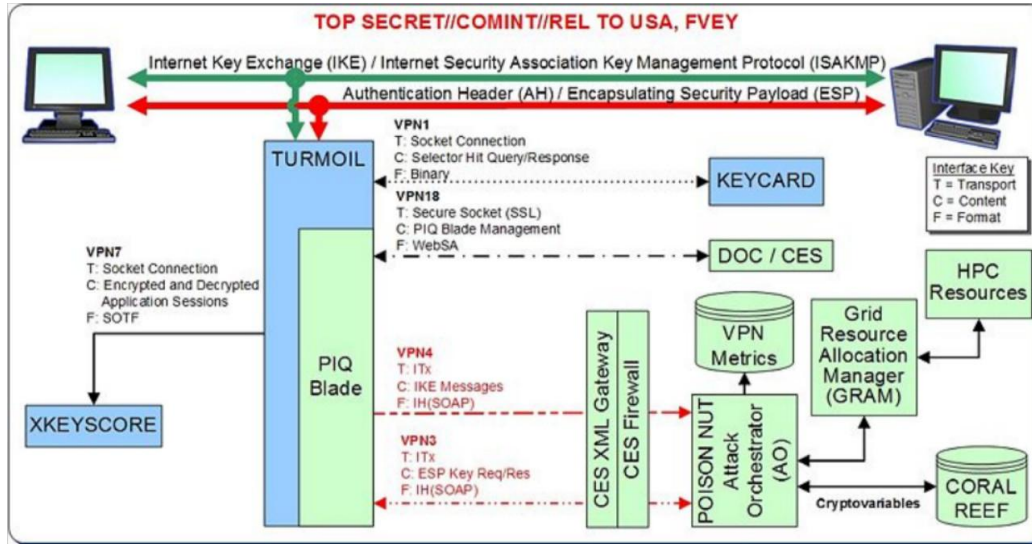
- Pre-computation of two 512 bit DH primes for TLS is enough to attack ~78,000 of Alexa Top 1M HTTPS domains
- Attacking 1024 bit and above is currently only achieved by state-level adversaries

## Exploiting Export Ciphers in TLS

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

Chart 7

# 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

Chart 8



# Live Demo

The screenshot displays a live demo environment. On the left, a terminal window shows the command `sudo docker exec -it cc /bin/bash` being executed, followed by `root@7c6f2c1bd4b8:/code# start-cc`. The output indicates that a Flask app is serving on port 5000. Below this, a web browser window is open, displaying the URL `https://www.network-security.net/counter.html`. The browser shows a simple web page with the text "Hello, World! ... So Long, and Thanks for All the CPU" and a large number "-4" between two buttons labeled "-" and "+". On the right, a terminal window shows the source code of the web application. The code is a Flask app that serves a static HTML page. The HTML page has a meta charset of "utf-8" and a viewport that scales to the device width. It contains a single button with the text "Hello, World!" and a script that increments a counter by 1 when the button is clicked. The counter is initially set to 0 and is displayed in a span with the id "cnt".

```
mitm SEQ=3753393439 ACK=1255685557 Ports: 443 -> 58634 len: 1005
mitm ApplicationData
mitm received:
mitm HTTP/1.1 200 OK
mitm Server: nginx/1.4.6 (Ubuntu)
mitm Date: Tue, 03 Aug 2021 13:36:27 GMT
mitm Content-Type: text/html
mitm Content-Length: 719
mitm Last-Modified: Thu, 29 Jul 2021 13:57:49 GMT
mitm Connection: keep-alive
mitm Etag: "6102b3dd-2cf"
mitm Accept-Ranges: bytes
mitm
mitm <!DOCTYPE html>
mitm <html lang="en">
mitm <head>
mitm <meta charset="utf-8" />
mitm <meta name="viewport" content="width=device-width, initial-scale=1.0" />
mitm <style>
mitm button,
mitm span {
mitm font-size: 3em;
mitm }
mitm button {
mitm width: 3em;
mitm margin: 1em;
mitm }
mitm body {
mitm text-align: center;
mitm }
mitm </style>
mitm </head>
mitm
mitm <body>
mitm <p>Hello, World!</p>
mitm
mitm <button onclick="inc(-1)"></button>
mitm <span id="cnt">0</span>
mitm <button onclick="inc(1)"></button>
mitm
mitm <script>
mitm function inc(n) {
mitm const cnt = document.getElementById("cnt");
mitm const value = Number(cnt.textContent) || 0;
mitm cnt.textContent = value + n;
mitm }
mitm </script>
mitm </body>
mitm </html>
```

## Exploiting Export Ciphers in TLS

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

# Impact of the Attack

	<i>Vulnerable servers, if the attacker can precompute for ...</i>			
	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%)

## Exploiting Export Ciphers in TLS

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

Chart 10