Exploring the Unknown DTLS Universe: Analysis of the DTLS Server Ecosystem on the Internet
USENIX Security '23

Nurullah Erinola¹, Marcel Maehren¹, Robert Merget², Juraj Somorovsky³, Jörg Schwenk¹

¹Ruhr University Bochum
²Technology Innovation Institute
³Paderborn University
DTLS is “TLS over UDP”
DTLS Must Solve Different Problems

Unreliable Transport

- M1 → M2
- M2 → M3
- M3 → M1

Denial-of-Service

- M1

Amplification

- M1

Small Maximum Transmission Unit

- M

Retransmissions

Anti-DoS Cookies

Fragmentation
DTLS Must Solve Different Problems

Unreliable Transport

Denial-of-Service

Amplification

Small Maximum Transmission Unit

Do these new features open vulnerabilities unique to DTLS implementations?

Retransmissions

Anti-DoS Cookies

Fragmentation
Exploring the Unknown DTLS Universe:
Analysis of the DTLS Server Ecosystem on the Internet

Indiscreet Logs: Persistent Diffie-Hellman Backdoors in TLS

Kristen Dorey
Western University, Canada
kdorey@uwo.ca

Nicholas Chang-Fong
Western University, Canada
nchangfo@uwo.ca

Aleksander Essex
Western University, Canada
aessex@uwo.ca

Markus Huber
FH St. Pölten, Austria
markus.huber@fhstp.ac.at

Narseo Vallina-Rodríguez
IMDEA Software Institute
Universidad Politécnica de Madrid

Robert Merger1, Juraj Somorovsky1, Nimrod Aviram2, Craig Young3, Janis Fumienschmidt1, Jörg Schwendel1
1Ruhr University Bochum
2Münster University of Applied Sciences
3Paderborn University

TLS in the Wild: An Internet-scale Analysis of TLS-based Protocols and Their Implementation Issues

Hanno Böck
Ruhr University Bochum

Robert Merger1, Juraj Somorovsky1, Nimrod Aviram2, Craig Young3, Janis Fumienschmidt1, Jörg Schwendel1
1Ruhr University Bochum
2Münster University of Applied Sciences
3Paderborn University

Return Of Bleichenbacher

ALPACA: Application Layer Protocol Confusion - Analyzing and Mitigating Cracks in TLS Authentication

Marcus Brinkmann1, Christian Dresen2, Robert Merger1, Damian Podlebski2, Jens Müller1, Juraj Somorovsky3, Jörg Schwendel1, and Sebastian Schinzel2
1Ruhr University Bochum
2Münster University of Applied Sciences
3Paderborn University
The DTLS ecosystem is unexplored!
Methodology

- RFCs
- Related Work
- TLS Attacks

Test Catalog

- Lab Evaluation
- Internet Scan
We Added 17 DTLS-Specific Tests

**Cookie Exchange: 8 Tests**
Issues the server an anti-DoS cookie?

**Retransmissions: 2 Tests**
Processes the server retransmissions?

**Fragmentation: 4 Tests**
Supports the server fragmentation?

**Other: 3 Tests**
Processes the server reordered messages?

*Implemented in TLS-Scanner*

- Scanner for **black box** evaluation of TLS servers
- Searches for supported features and vulnerabilities

1https://github.com/tls-attacker/TLS-Scanner
DoS & Amplification Attacks are a Threat

<table>
<thead>
<tr>
<th>Test</th>
<th>Botan</th>
<th>Gnu/TLS</th>
<th>JSSE</th>
<th>LibreSSL</th>
<th>MatrixSSL</th>
<th>mbed TLS</th>
<th>OpenSSL</th>
<th>Pion/DTLS</th>
<th>Scudellum</th>
<th>Tiny/DTLS</th>
<th>wolfSSL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Issues a cookie during a new handshake</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Issues a cookie during a resumption with session ID</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Issues a cookie during a resumption with session ticket</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Issues a cookie during a renegotiation</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Performs no HelloVerifyRequest retransmissions</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Performs recommended cookie computation</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Validates the received cookie</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Cookie length</td>
<td>32</td>
<td>16</td>
<td>32</td>
<td>20</td>
<td>16</td>
<td>32</td>
<td>20</td>
<td>20</td>
<td>32</td>
<td>16</td>
<td>16</td>
</tr>
<tr>
<td>Sends retransmissions without requesting</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Processes client-requested retransmissions</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Processes fragmented ClientHello in a single datagram correctly</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Processes fragmented ClientHello in cross datagrams correctly</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Processes fragmented ClientKeyExchange in a single datagram</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Processes fragmented ClientKeyExchange in cross datagrams</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Rejects unencrypted Finished</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Rejects unencrypted Application Data</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Processes reordered ChangeCipherSpec and Finished correctly</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

- **1x Plaintext Injection**
- **3x Amplification Vulnerabilities**
  - CVE-2023-21835
  - CVE-2022-2576
  - CVE-2022-34293
- **5x DoS Vulnerabilities**
- **2x Crashes**
Exploring the Unknown DTLS Universe:
Analysis of the DTLS Server Ecosystem on the Internet

Where is DTLS deployed on the Internet?
On which ports is DTLS mostly deployed?

Host discovery with ZMap

1https://github.com/zmap/zmap
More Than 600,000 DTLS Servers Across Eight Ports

1. Scan of $2^{17}$ IPv4 addresses for each port

2. Scan of $2^{20}$ IPv4 addresses for each port where we discovered at least one host

3. Scan of the whole IPv4 range for the top eight ports

<table>
<thead>
<tr>
<th>Port</th>
<th>Hosts Found</th>
</tr>
</thead>
<tbody>
<tr>
<td>443</td>
<td>273,140</td>
</tr>
<tr>
<td>10443</td>
<td>262,724</td>
</tr>
<tr>
<td>1106</td>
<td>47,654</td>
</tr>
<tr>
<td>3391</td>
<td>36,719</td>
</tr>
<tr>
<td>4433</td>
<td>17,874</td>
</tr>
<tr>
<td>12346</td>
<td>15,334</td>
</tr>
<tr>
<td>12446</td>
<td>9,388</td>
</tr>
<tr>
<td>12681</td>
<td>1,368</td>
</tr>
<tr>
<td>$\Sigma$</td>
<td>664,201</td>
</tr>
</tbody>
</table>

78.42% of hosts evaluated
We Identified Five DTLS Services

![Diagram showing the fraction of hosts using different DTLS services on various ports.]

- Port 443: VPN - Fortinet, TURN, STUN
- Port 10443: Unknown
- Port 1106: Unknown
- Port 3391: Unknown
- Port 4433: Unknown
- Port 12346: Viptela - Cisco
- Port 12446: Unknown

Fraction of Hosts:
- VPN - Fortinet
- TURN
- STUN
- VPN - Citrix
- Viptela - Cisco
- Unknown
Preferred Key Exchange Methods: ECDHE & RSA

- **RSA-PSK**: 0
- **ECDHE-PSK**: 0
- **PSK**: 0
- **DHE-PSK**: 0
- **DHE**: 0
- **RSA**: 28
- **ECDHE**: 0

**Vulnerabilities:***
- Bleichenbacher vulnerabilities: 0
- Invalid Curve vulnerabilities: 0
- Logjam & Freak vulnerabilities: 0
Forbidden and Weak Encryption Algorithms Supported

- **DES**
- **IDEA**
- **NULL**
- **RC4**
- **3DES**
- **ARIA**
- **CAMELLIA**
- **CHACHA**
- **AES**

- **No confidentiality**
- **Forbidden in DTLS**
- **87,263 potentially vulnerable to Sweet32**
- **472 Padding Oracle vulnerabilities**
DTLS-Specific Properties in Practice

- 13.5% of servers on port 443 contain amplification vulnerabilities
  - Amplification factor up to 33

- On three ports, almost all servers do not support fragmentation & reordering
  - Influences their stability and interoperability

- On five ports, almost all servers do not implement a retransmission timer
  - Only send retransmissions themselves when they receive retransmissions
Conclusions

Tested (D)TLS properties & DTLS-specific features

➔ Published the first comprehensive dataset

Unsupported DTLS-specific features

➔ Influences the stability and interoperability

DTLS-specific features open new vulnerabilities

➔ DoS & Amplification attacks are a threat

@nerinola1  nurullah.erinola@rub.de  https://github.com/tls-attacker/TLS-Scanner