

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

USENIX Security '23

Nurullah Erinola¹, Marcel Maehren^{1,2}, Robert Merget²,
Juraj Somorovsky³, Jörg Schwenk¹

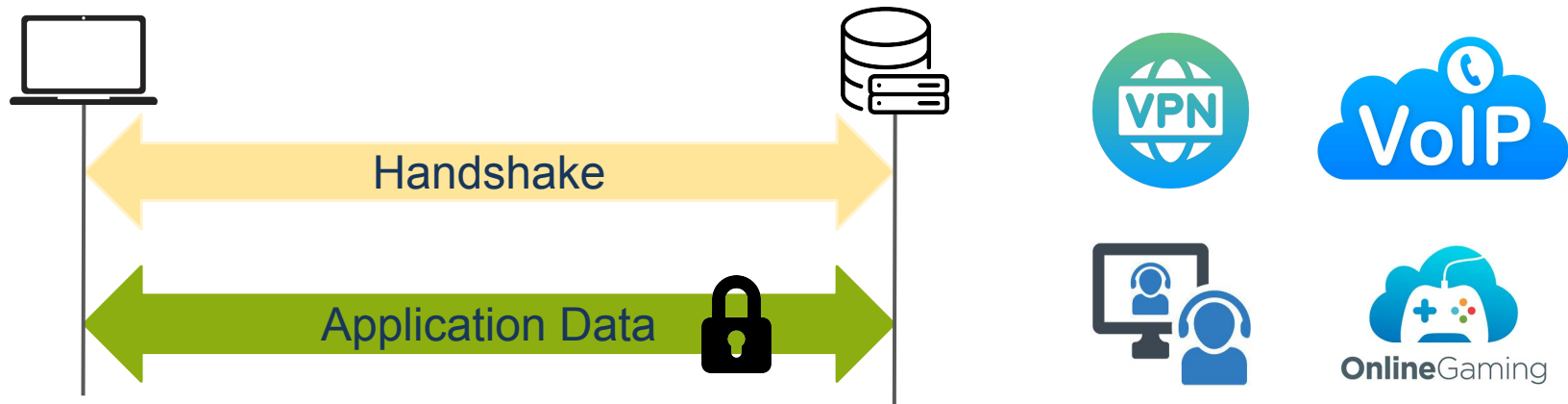
¹Ruhr University Bochum

²Technology Innovation Institute

³Paderborn University

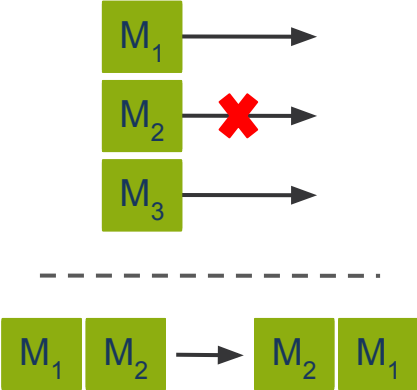


DTLS is “TLS over UDP”



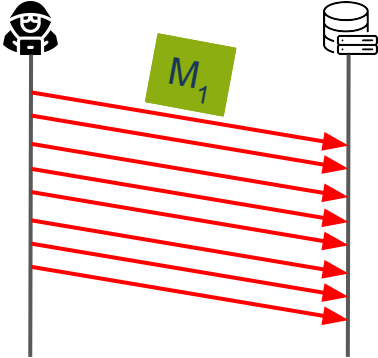
DTLS Must Solve Different Problems

Unreliable Transport

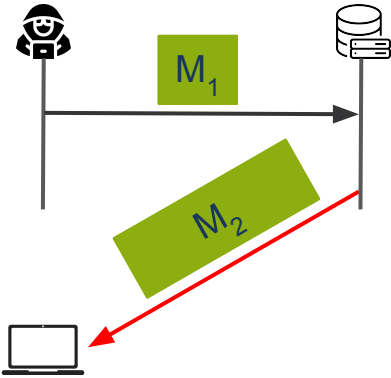


Retransmissions

Denial-of-Service

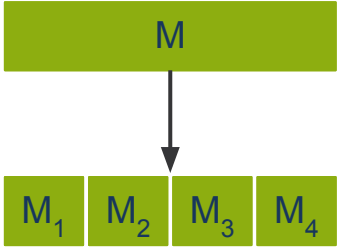


Amplification



Anti-DoS Cookies

Small Maximum Transmission Unit



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?



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

Members: Testing TLS in the System at Large

Becker

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

IMDEA Software Institute
Universidad Politécnica de Madrid

Kenneth G. Paterson
University of London

Narso V
IMDEA

An

Robert Merget¹, Juraj Somorovsky¹, Nimrod Aviram², Craig Young³, Janis Flickeenschmidt¹, Jörg Schwenk¹, and Yuval Shavitt²

¹Ruhr University Bochum
²Department of Electrical Engineering

Automatic Classification of TLS Padding Oracle Vulnerabilities

TLS in the Wild: An Inter-Protocol TLS-based Protocol Confusion

Return Of Bleichenbacher

Hanno Böck

Ruhr U

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

Marcus Brinkmann¹, Christian Dresen², Robert Merget¹, Damian Poddebniak², Jens Müller¹, Juraj Somorovsky³, Jörg Schwenk¹, and Sebastian Schinzel²

¹Ruhr University Bochum
²Münster University of Applied Sciences
³Paderborn University

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

Members: Testing TLS in the System at Large

Becker

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

The DTLS ecosystem is unexplored!

Return

Hanno Böck

Ruhr U

ALPACA: Analyzing and Mitigating Cracks in TLS

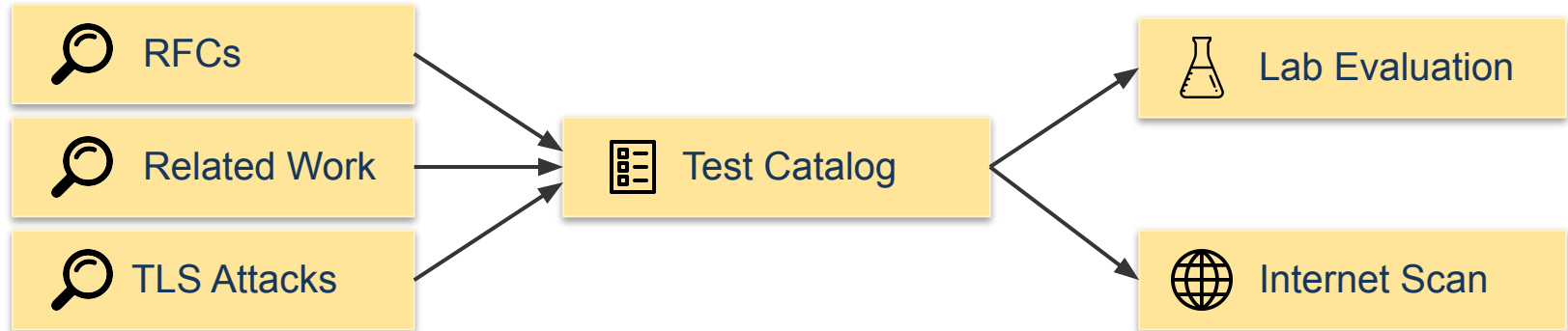
Marcus Brinkmann¹, Christian Dresen², Robert Merget¹, Damian Poddebniak², Jens Müller¹, Juraj Somorovsky³, Jörg Schwenk¹, and Sebastian Schinzel²

¹Ruhr University Bochum

²Münster University of Applied Sciences

³Paderborn University

Methodology



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-Scanner¹*

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

¹<https://github.com/tls-attacker/TLS-Scanner>

DoS & Amplification Attacks are a Threat

Test	Botan	GnuTLS	JSSE	LibreSSL	MatrixSSL	Mbed TLS	OpenSSL	PionDTLS	Scandium	TinyDTLS ^C	TinyDTLS ^E	wolfSSL
Issues a cookie during a new handshake	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Issues a cookie during a resumption with session ID	✓	✓	✗	✓	✓	✓	-	✗	-	-	✗	✗
Issues a cookie during a resumption with session ticket	✓	✓	✗	✓	-	-	✓	-	-	-	-	✗
Issues a cookie during a renegotiation	-	✗	-	✓	-	-	✗	-	-	-	✓	-
Performs no <i>HelloVerifyRequest</i> retransmissions	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓
Performs recommended cookie computation	✓	x ^b	x ^a	x ^b	x ^c	x ^d	x ^b	x ^b	✓	✓	x ^c	✓
Validates the received cookie	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Cookie length	32	16	32	20	16	32	20	20	32	16	16	32
Sends retransmissions without requesting	✗	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗	✓
Processes client-requested retransmissions	✗	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓
Processes fragmented <i>ClientHello</i> in a single datagram correctly	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗	✓
Processes fragmented <i>ClientHello</i> in cross datagrams correctly	✗	✓	✗	✗	✗	✓	✗	✗	✓	✗	✗	✓
Processes fragmented <i>ClientKeyExchange</i> in a single datagram	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗	✓
Processes fragmented <i>ClientKeyExchange</i> in cross datagrams	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗	✓
Rejects unencrypted <i>Finished</i>	✗	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓
Rejects unencrypted <i>Application Data</i>	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓
Processes reordered <i>ChangeCipherSpec</i> and <i>Finished</i> correctly	✗	✗	✓	✓	✗	✓	✓	✗	✓	✗	✗	✗

1x Plaintext Injection

3x Amplification Vulnerabilities

- CVE-2023- 21835
- CVE-2022-2576
- CVE-2022-34293

5x DoS Vulnerabilities


2x Crashes

Analysis of the DTLS Server Ecosystem



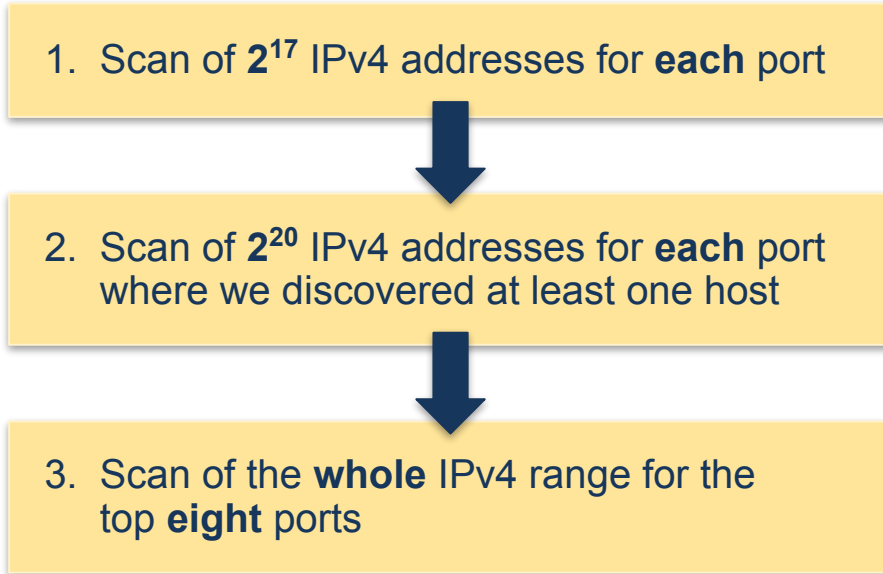
Where is DTLS deployed on the Internet?

On which ports is DTLS mostly deployed?


↳ *Host discovery with ZMap¹* 

¹<https://github.com/zmap/zmap>

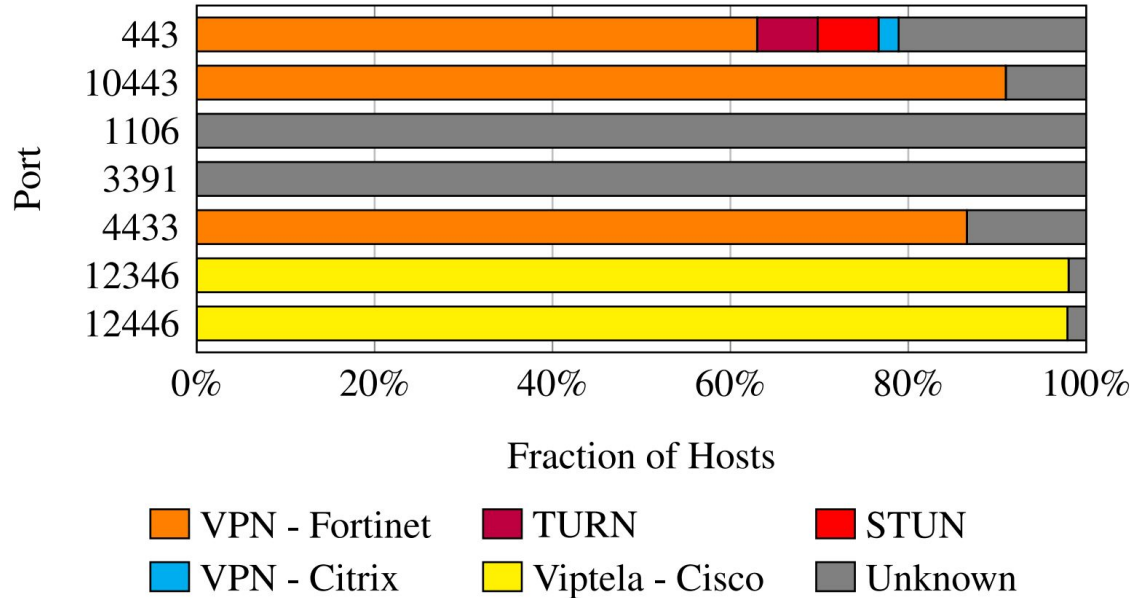
More Than 600,000 DTLS Servers Across Eight Ports



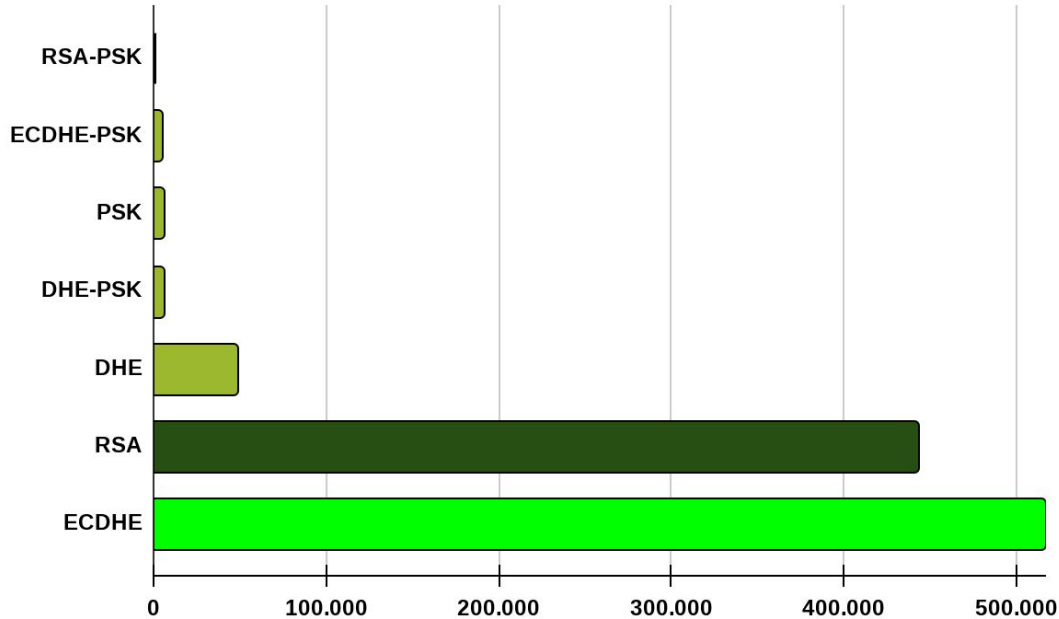
Port	Hosts Found
443	273,140
10443	262,724
1106	47,654
3391	36,719
4433	17,874
12346	15,334
12446	9,388
12681	1,368
Σ	664,201

 **78.42%** of hosts evaluated

We Identified Five DTLS Services



Preferred Key Exchange Methods: ECDHE & RSA

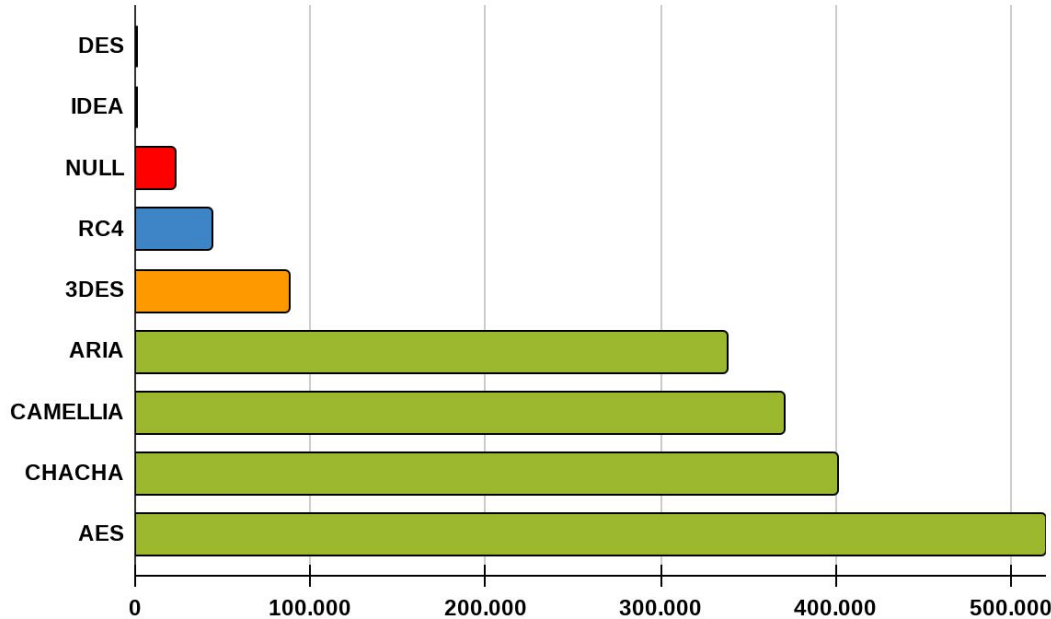


28 Bleichenbacher vulnerabilities

0 Invalid Curve vulnerabilities

0 Logjam & Freak vulnerabilities

Forbidden and Weak Encryption Algorithms Supported



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

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

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

¹Ruhr University Bochum
²Technology Innovation Institute
³Paderborn University



@nerinola1



nurullah.erinola@rub.de



<https://github.com/tls-attacker/TLS-Scanner>