MONSTERS IN THE MIDDLEBOXES

Luke Valenta

@lukevalenta

Systems Engineer, Cloudflare

Gabbi Fisher

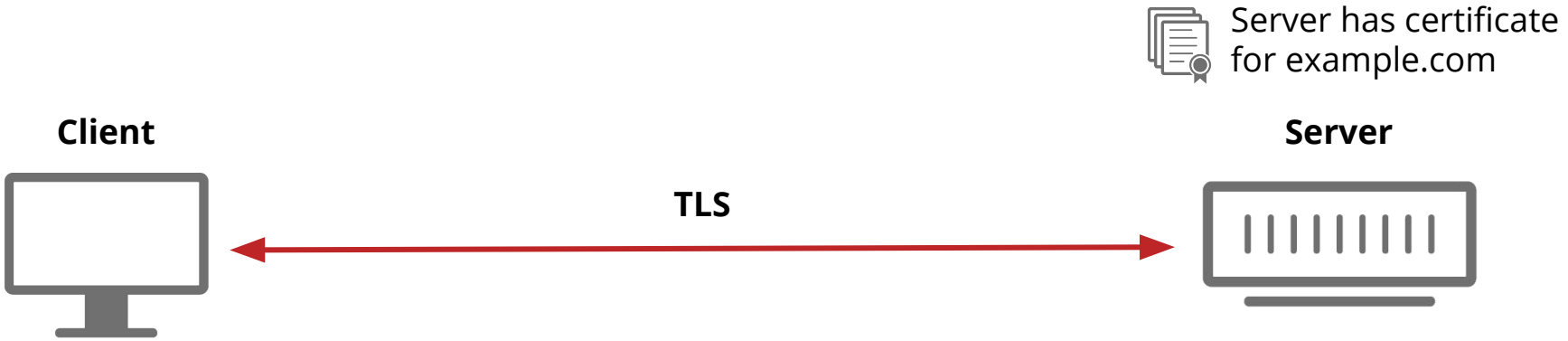
@gabbifish

Systems Engineer, Cloudflare

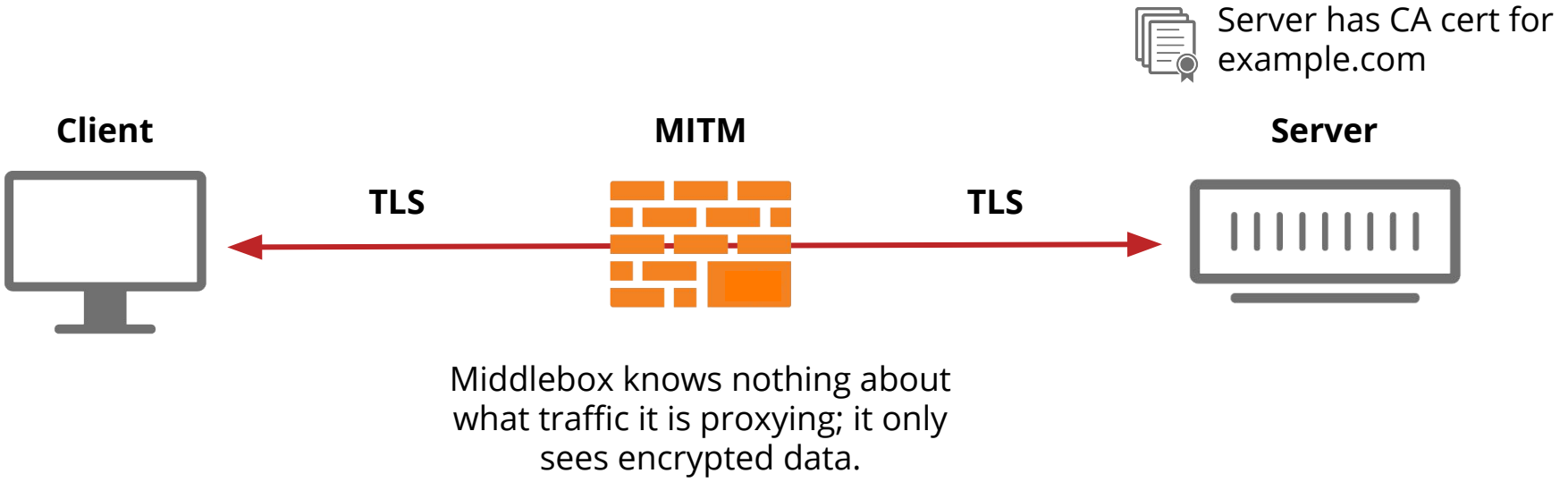
Outline

1. “HTTPS Interceptors and How to Find Them”: Common sources of MITM (Monsters in the Middle).
2. A technique for detecting HTTPS interception
3. Building tools for detecting Internet-scale HTTPS detection: MITMEngine and MALCOLM

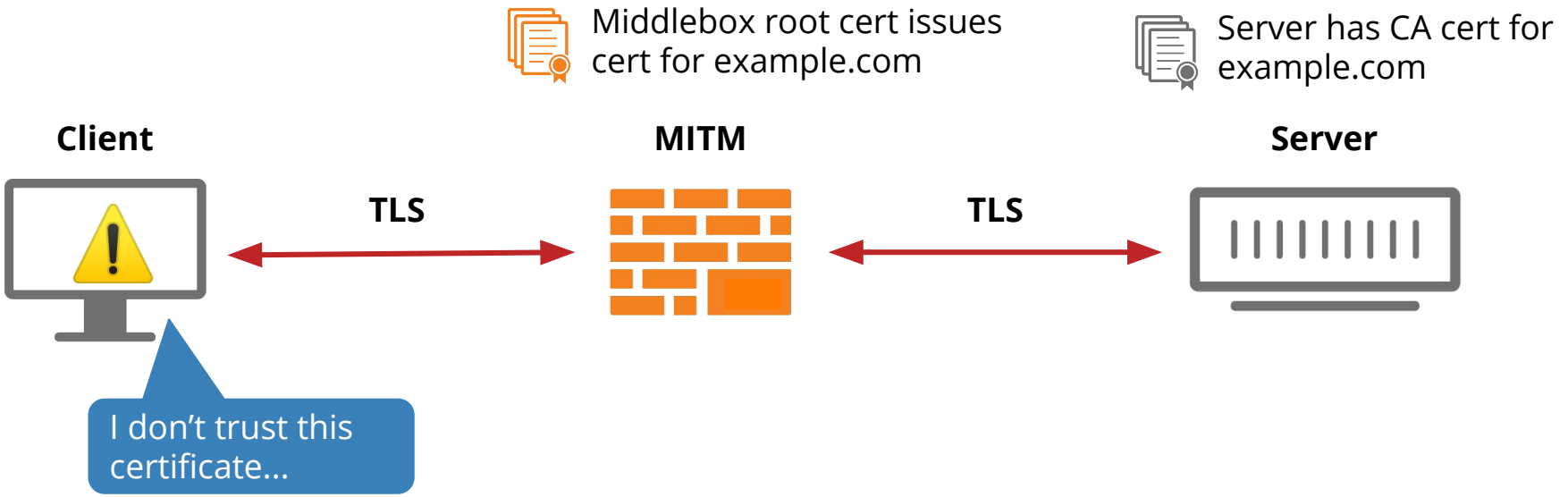
HTTPS Without Interception



HTTPS Without Interception



Attempting HTTPS Interception

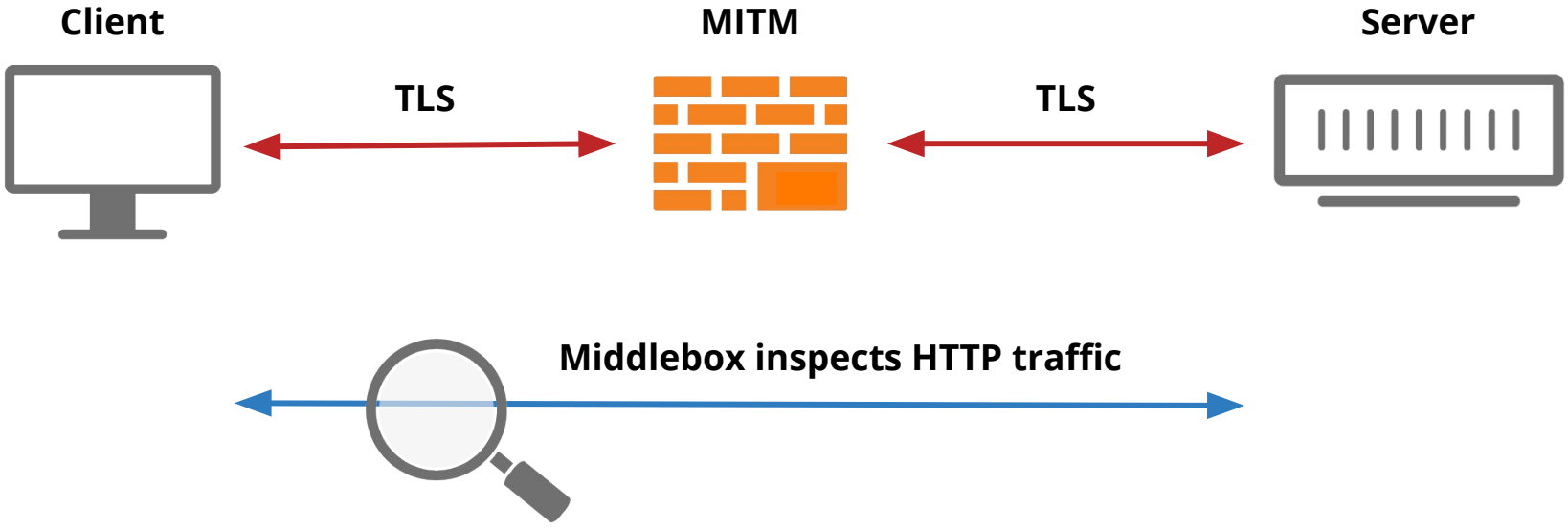


How HTTPS Interception Works

Interceptor installs new root cert

Middlebox root cert issues cert for example.com

Server has CA cert for example.com



Types of HTTPS Interception

Antivirus/Corporate/Government

- Detect malware
- Detect C&C traffic
- Detect exfiltration
- Anti-terrorism
- Censorship

Types of HTTPS Interception

Antivirus/Corporate/Government

- Detect malware
- Detect C&C traffic
- Detect exfiltration
- Anti-terrorism
- Censorship

Project Zero calls out Kaspersky AV for SSL interception practices

Using an SSL proxy that simplistically stored certificates, Kaspersky Anti-Virus left its users open to TLS certificate collisions.

By Chris Duckett | January 4, 2017 -- 01:25 GMT (17:25 PST) | Topic: Security

Blue Coat SSL Visibility Appliance contains multiple vulnerabilities

Vulnerability Note VU#498348

Original Release Date: 2015-05-29 | Last Revised: 2015-06-02

Kazakhstan government is now intercepting all HTTPS traffic

Kazakh government first wanted to intercept all HTTPS traffic way back in 2016, but they backed off after several lawsuits.

By Catalin Cimpanu for Zero Day | July 18, 2019 -- 19:38 GMT (12:38 PDT) | Topic: Security

Types of HTTPS Interception

Antivirus/Corporate/Government

- Detect malware
- Detect C&C traffic
- Detect exfiltration
- Anti-terrorism
- Censorship

Malware

- Inject ads
- Steal private data

Types of HTTPS Interception

Antivirus/Corporate/Government

Mac malware intercepts encrypted web traffic for ad injection

Posted: October 24, 2018 by Thomas Reed
Last updated: October 25, 2018

SEARCHAWESOME

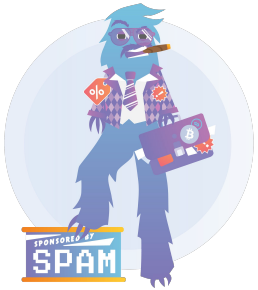
- Censorship

Alert (TA15-051A)

Lenovo Superfish Adware Vulnerable to HTTPS Spoofing

Original release date: February 20, 2015 | Last revised: September 30, 2016

Malware



- Inject ads
- Steal private data

Types of HTTPS Interception

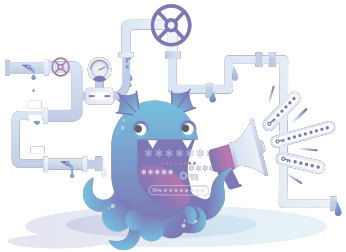
Antivirus/Corporate/Government

- Detect malware
- Detect C&C traffic
- Detect exfiltration
- Anti-terrorism
- Censorship

Malware

- Inject ads
- Steal private data

Leaky Proxies



- Product features
- Convenience

Types of HTTPS Interception

Antivirus/Corporate/Government

- Detect malware
- Detect C&C traffic
- Detect exfiltration
- Anti-terrorism
- Censorship

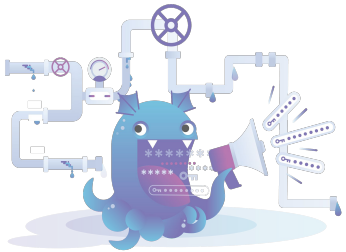
Vulnerability Report – CVE-2018-17612

Certificate Management Vulnerability in Sennheiser HeadSetup

Hans-Joachim Knobloch, André Domnick
Secorvo Security Consulting GmbH

Version 1.2
Date October 31, 2018

Leaky Proxies



- Product features
- Convenience

Types of HTTPS Interception

Antivirus/Corporate/Government

- Detect malware
- Detect C&C traffic
- Detect exfiltration
- Anti-terrorism
- Censorship

Vulnerability Report – CVE-2018-17612

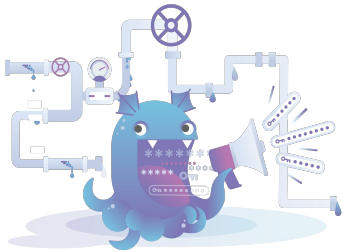
Certificate Management Vulnerability in Sennheiser HeadSetup

Hans-Joachim Knobloch, André Domnick
Secorvo Security Consulting GmbH

Version 1.2
Date October 31, 2018

As easy as guessing "SennheiserCC!" ¯_(ツ)_/¯

Leaky Proxies



- Product features
- Convenience

Types of HTTPS Interception

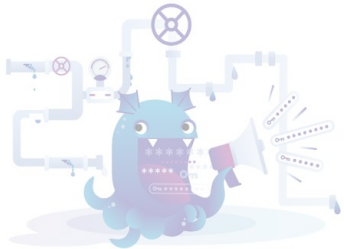
Antivirus/Corporate/Government

- Detect malware
- Detect C&C traffic
- Detect exfiltration
- Anti-terrorism
- Censorship

Malware

- Inject ads
- Steal private data

Leaky Proxies



- Product features
- Convenience

Reverse Proxies

- Security
- Performance
- Reliability

Types of HTTPS Interception

Antivirus/Corporate/Government

Incident report on memory leak caused by Cloudflare parser bug

23 Feb 2017 by John Graham-Cumming.

CLOUDTEST VULNERABILITY (CVE-2019-11011)

By Akamai InfoSec June 17, 2019 10:00 AM

0 Comments

Ticketbleed (CVE-2016-9244)

Ticketbleed is a software vulnerability in the TLS/SSL stack of F5 BIG-IP appliances allowing a remote attacker to extract up to 31 bytes of uninitialized memory at a time.

Malware

- Inject ads
- Steal private data

Reverse Proxies

- Security
- Performance
- Reliability

Types of HTTPS Interception

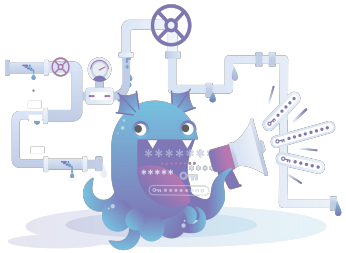
Antivirus/Corporate/Government

- Detect malware
- Detect C&C traffic
- Detect exfiltration
- Anti-terrorism
- Censorship

Malware

- Inject ads
- Steal private data

Leaky Proxies

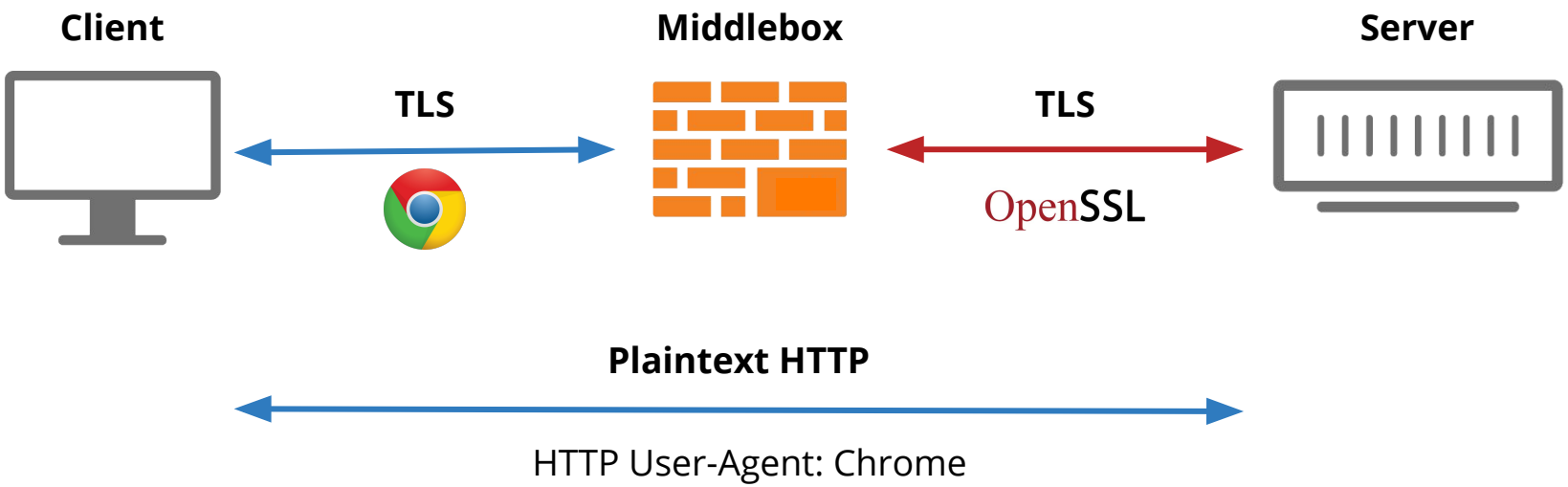


- Product features
- Convenience

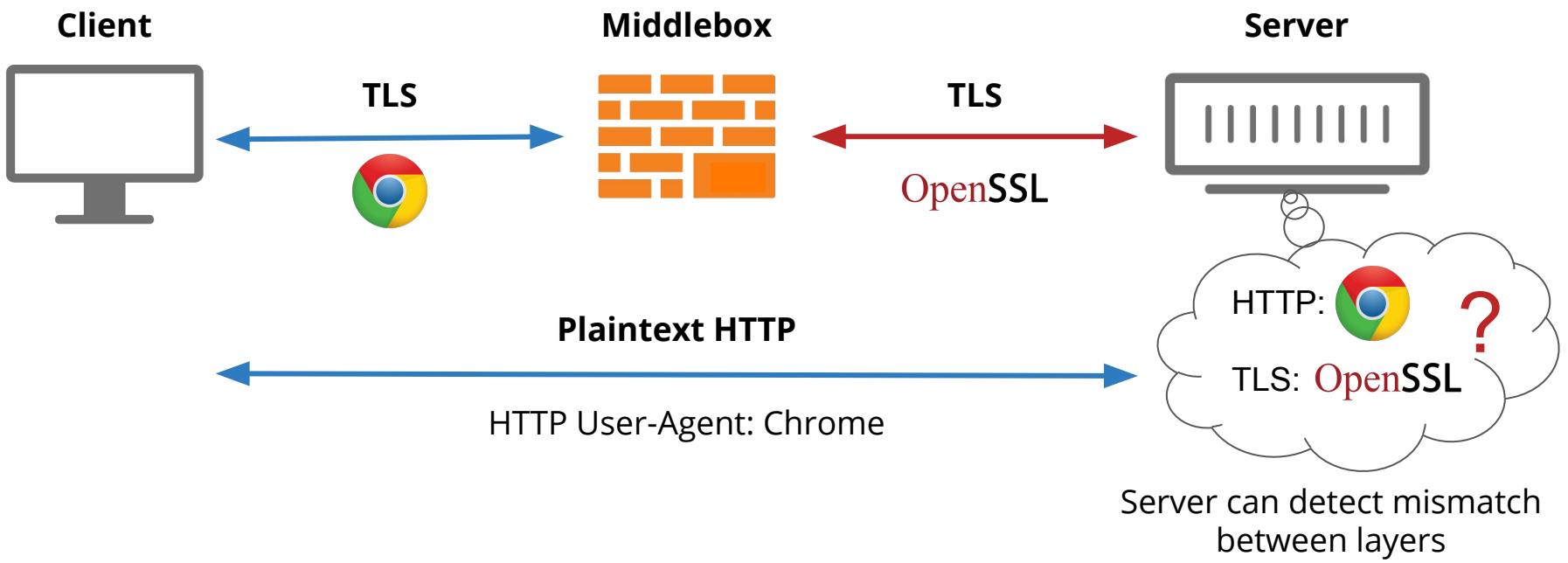
Reverse Proxies

- Security
- Performance
- Reliability

Detecting HTTPS Interception [Durumeric et al., 2017]



Detecting HTTPS Interception [Durumeric et al., 2017]



Identifying HTTP and TLS Clients

HTTP

Parse User Agent Header

```
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/75.0.3770.100 Safari/537.36
```

Identifying HTTP and TLS Clients

HTTP

Parse User Agent Header

```
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/75.0.3770.100 Safari/537.36
```

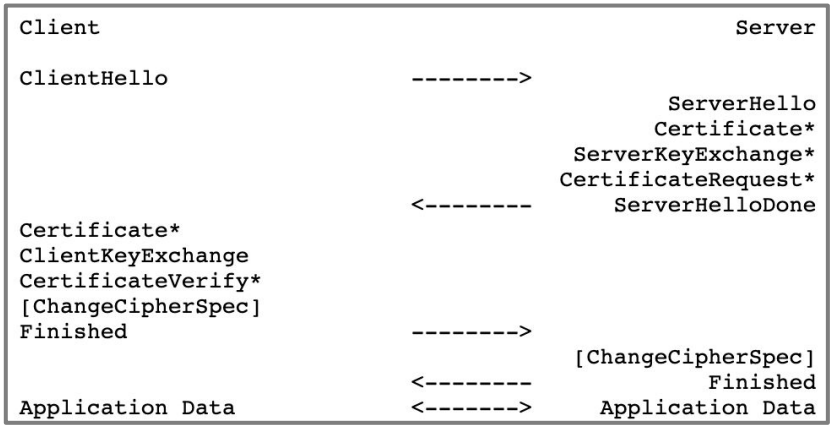
TLS

No identifying field is present in the protocol. Instead, use known techniques for fingerprinting browsers based on TLS Client Hello.

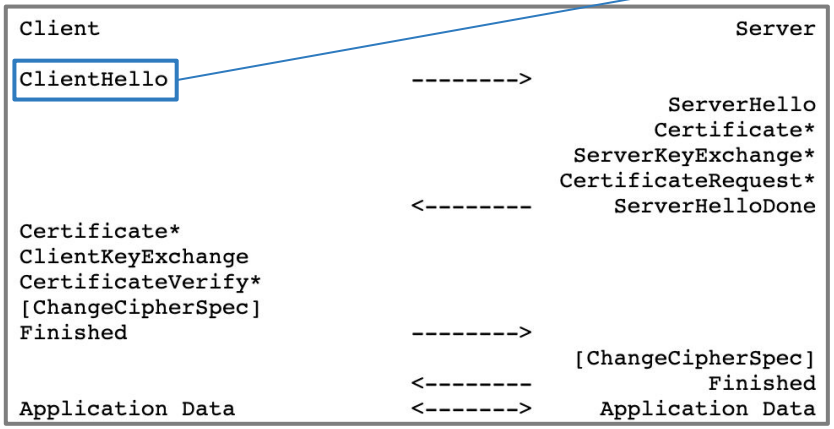
TLS Client Hello Fingerprinting

- [Ristić; 2009] HTTP client fingerprinting using SSL handshake analysis.
- [Majkowski; 2012] SSL fingerprinting for p0f.
- [Brotherston; 2015] TLS Fingerprinting: Smarter Defending & Stealthier Attacking.
- [Anderson et al.; 2016] Classifying Encrypted Traffic with TLS-Aware Telemetry
- [Durumeric et al.; 2017] The Security Impact of HTTPS Interception.
- [Althouse, Atkinson, Atkins; 2017]. TLS Fingerprinting with JA3 and JA3S.
- [Anderson, McGrew; 2019]. TLS Fingerprinting in the Real World.
- [Frolov, Wustrow; 2019]. TLS Fingerprint.

TLS Handshake (RFC 5246)

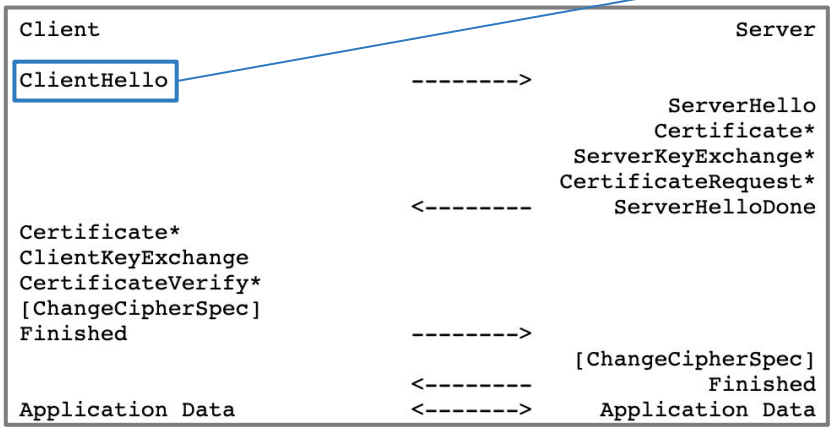


TLS Handshake (RFC 5246)




```
struct {
    ProtocolVersion client_version;
    Random random;
    SessionID session_id;
    CipherSuite cipher_suites<2..2^16-2>;
    CompressionMethod compression_methods<1..2^8-1>;
    select (extensions_present) {
        case false:
            struct {};
        case true:
            Extension extensions<0..2^16-1>;
    };
} ClientHello;
```

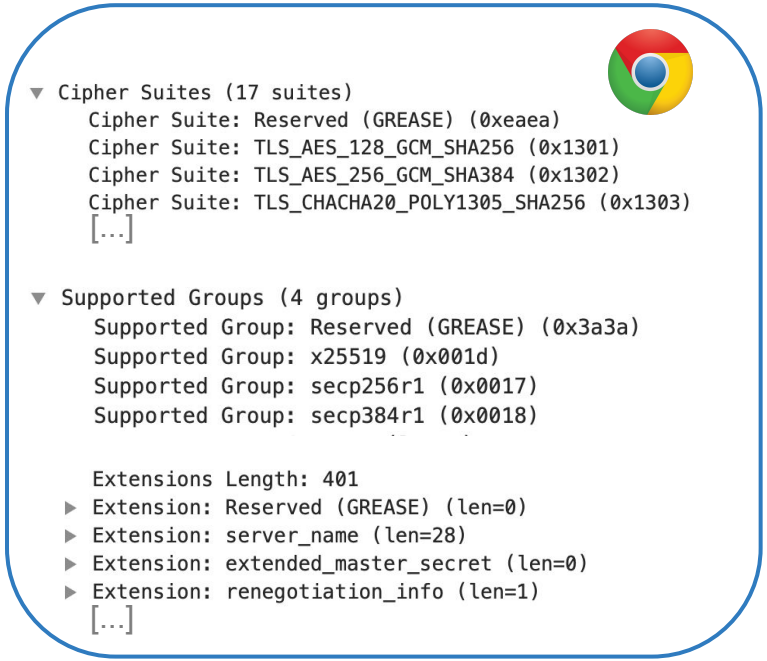
TLS Handshake (RFC 5246)

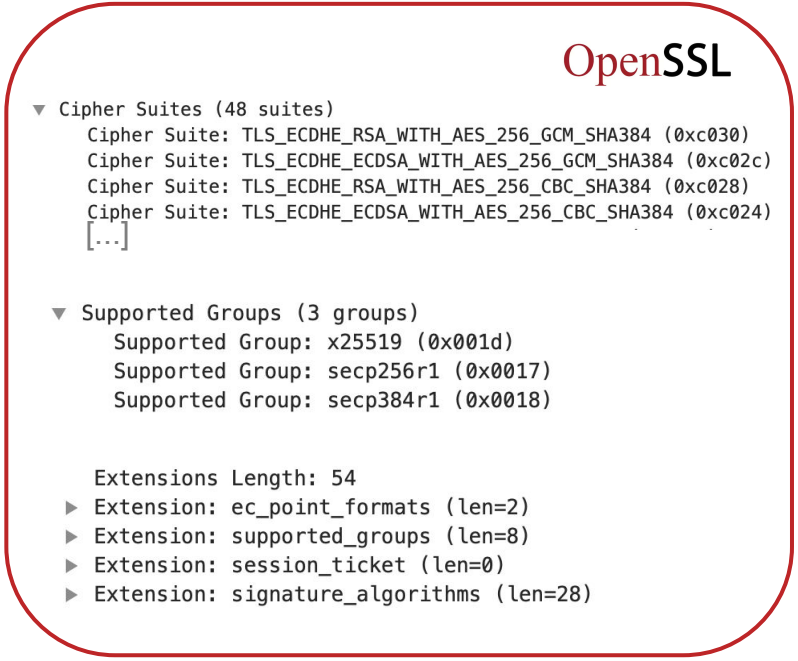



```
struct {
    ProtocolVersion client_version;
    Random random;
    SessionID session_id;
    CipherSuite cipher_suites<2..2^16-2>;
    CompressionMethod compression_methods<1..2^8-1>;
    select (extensions_present) {
        case false:
            struct {};
        case true:
            Extension extensions<0..2^16-1>;
    };
} ClientHello;
```

TLS libraries tend to keep these fields the same!

TLS Fingerprinting based on Client Hello





HTTPS Interception Detection Process

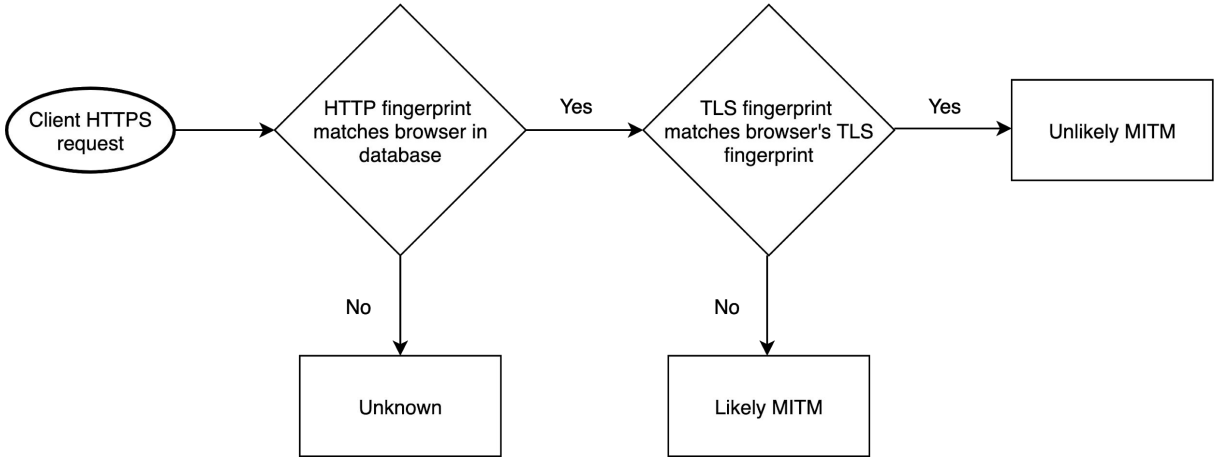
HTTPS Interception Detection Process

1. Build database of HTTP and TLS browser fingerprints

HTTPS Interception Detection Process

1. Build database of HTTP and TLS browser fingerprints

2. Check HTTP and TLS fingerprints of incoming requests against database



MITMEngine:
HTTPS Interception Detection Library

Open sourced at https://github.com/cloudflare/mitmengine. PRs welcome!

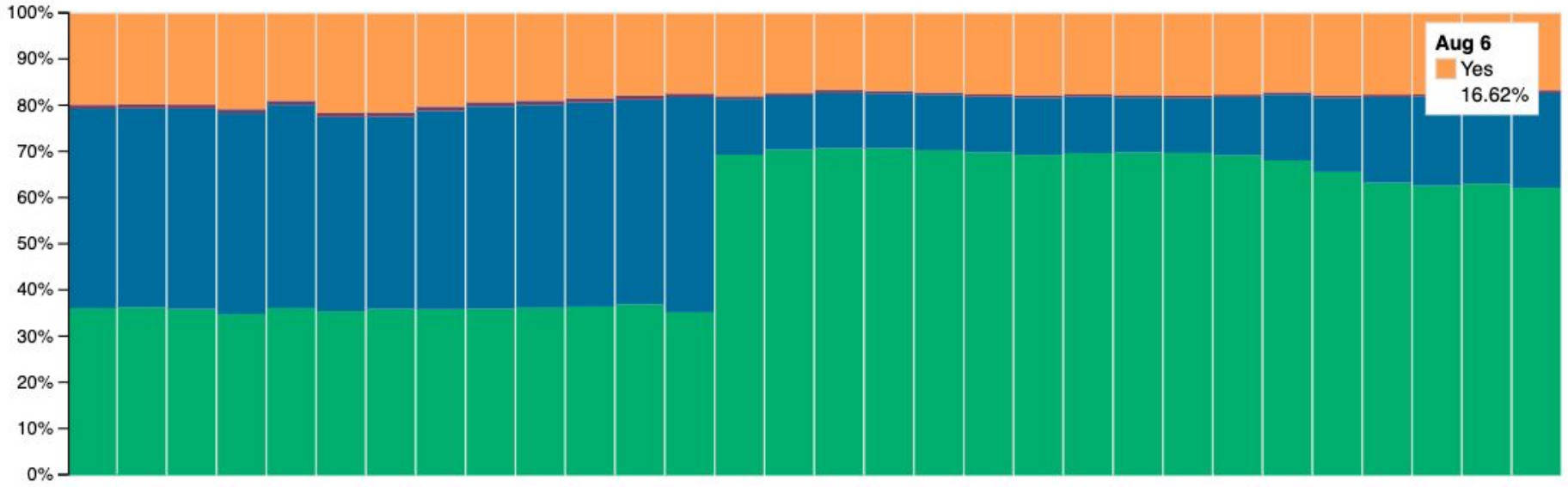
- Goal #1: **Maintainability**
  - Fingerprints quickly go stale with browser updates
  - Time-consuming to generate new fingerprints manually
  - Goal is to automatically generate ground truth fingerprints from Cloudflare's network
- Goal #2: **Flexibility**
  - Currently support a flexible fingerprint format to model a variety of browser behavior
  - Plan to add support for other TLS fingerprint formats (JA3, tlsfingerprint.io)
- Goal #3: **Performance**
  - The system should be fast enough to deploy at scale
  - Currently deployed on a 5% sample of Cloudflare TLS requests

MALCOLM: HTTPS Interception on Cloudflare's Network

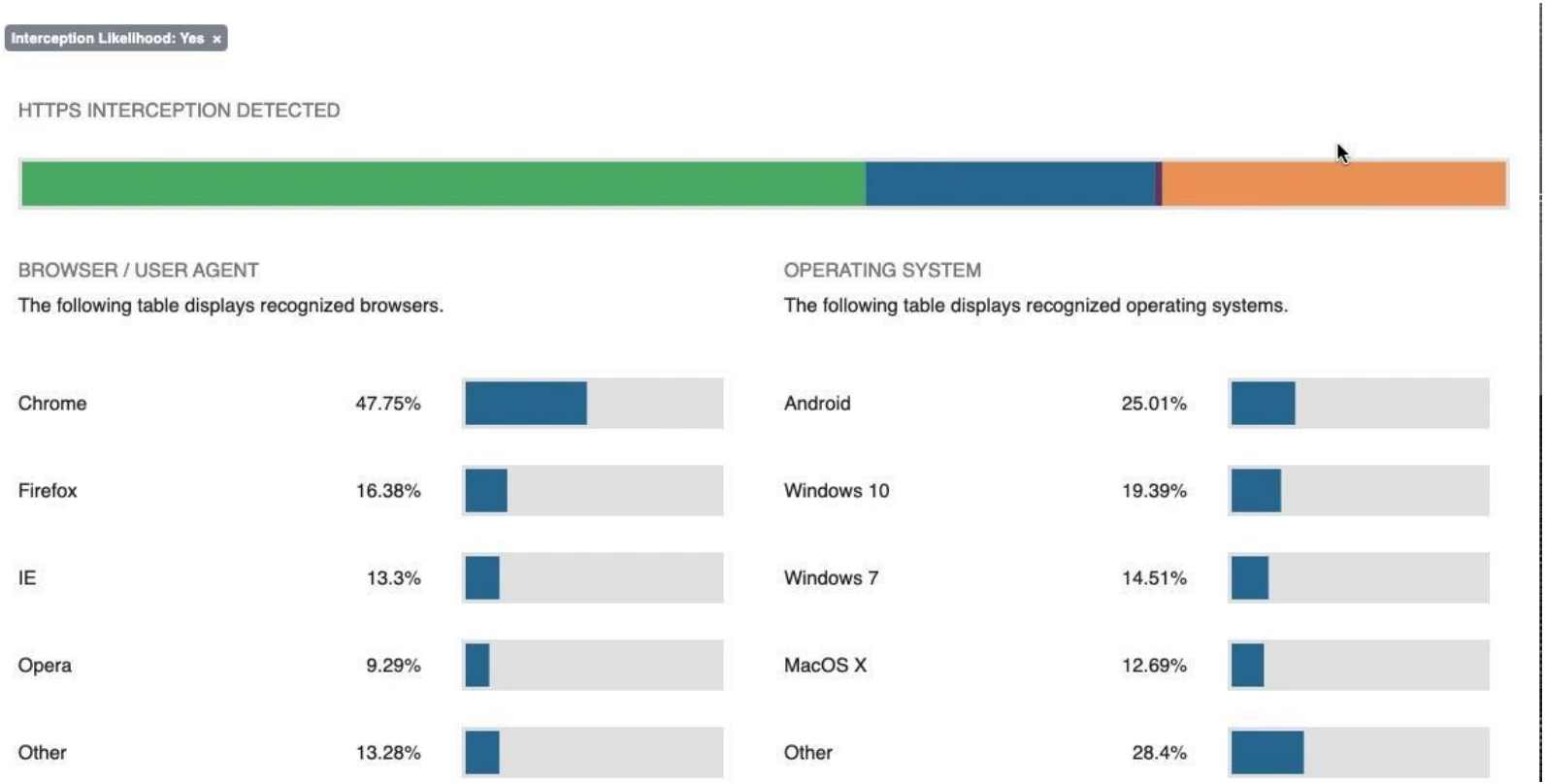
Public dashboard located at https://malcolm.cloudflare.com.

- Provides insight into HTTPS Interception observed by Cloudflare
- Powered by MITMEngine
- Allows for filtering by OS, browser, HTTPS interception tool, etc.

MALCOLM: HTTPS Interception Analytics



MALCOLM: HTTPS Interception Analytics



Takeaways / Sound Bytes

TLS-terminating middleboxes pose serious threats to network security

Heuristics based on HTTP and TLS fingerprints can be effective at detecting HTTPS interception

Our new open source tool and public dashboard provide insight into the state of HTTPS interception on the Internet

- https://github.com/cloudflare/mitmengine
- https://malcolm.cloudflare.com

Thank you!
@gabbifish
@lukevalenta

References

- [Ristić; 2009] HTTP client fingerprinting using SSL handshake analysis. https://blog.ivanristic.com/2009/06/http-client-fingerprinting-using-ssl-handshake-analysis.html
- [Majkowski; 2012] SSL fingerprinting for p0f. https://idea.popcount.org/2012-06-17-ssl-fingerprinting-for-p0f
- [Brotherston; 2015] TLS Fingerprinting: Smarter Defending & Stealthier Attacking. https://blog.squarelemon.com/tls-fingerprinting/
- [Anderson et al.; 2016] Classifying Encrypted Traffic with TLS-Aware Telemetry. https://resources.sei.cmu.edu/library/asset-view.cfm?assetID=449962
- [Durumeric et al.; 2017] The Security Impact of HTTPS Interception. https://jhalderm.com/pub/papers/interception-ndss17.pdf
- [Althouse, Atkinson, Atkins; 2017]. TLS Fingerprinting with JA3 and JA3S. https://engineering.salesforce.com/tls-fingerprinting-with-ja3-and-ja3s-247362855967
- [Frolov, Wustrow; 2019]. TLS Fingerprint. Tlsfingerprint.io
- [Anderson, McGrew; 2019]. TLS Fingerprinting in the Real World. https://blogs.cisco.com/security/tls-fingerprinting-in-the-real-world
- [Raman et al.; 2019] Kazakhstan's HTTPS Interception. https://censoredplanet.org/kazakhstan

Questions and Answers

Q: **Can’t middleware simply mimic browsers?**
A: The signatures of popular browsers are constanting changing, and mimicking the signatures would require the middleware to actually support all of the protocols and features of the browser (which would be great!).

Q: **Does this work for TLS 1.3?**
A: TLS 1.3 client hellos can be fingerprinted just the same as TLS 1.2 client hellos, since the record and handshake formats are kept the same.