SSL in Bro 2.3

Johanna Amann
International Computer Science Institute

johanna@icir.org
http://www.icir.org/johanna
Outline

New features of the Bro SSL/TLS analyzer

TLS protocol basics

Detecting Heartbleed with Bro
Bro SSL and X509 events
(in random order)
Bro SSL and X509 events (in random order)

<table>
<thead>
<tr>
<th>client_hello</th>
<th>ssl_stapled_ocsp</th>
<th>ssl_change_cipher_spec</th>
</tr>
</thead>
<tbody>
<tr>
<td>server_hello</td>
<td>ssl_encrypted_data</td>
<td>x509_extension</td>
</tr>
<tr>
<td>ssl_session_ticket_handshake</td>
<td>ssl_dh_server_params</td>
<td>x509_ext_basic_constraints</td>
</tr>
<tr>
<td>ssl_established</td>
<td>ssl_change_cipher_spec</td>
<td>x509_ext_subject_alternative_name</td>
</tr>
<tr>
<td>x509_certificate</td>
<td>ssl_handshake_message</td>
<td>ssl_extension_elliptic_curves</td>
</tr>
<tr>
<td>ssl_extension</td>
<td>ssl_encrypted_data</td>
<td>ssl_extension_application_layer_protocol_negotiation</td>
</tr>
<tr>
<td>ssl_alert</td>
<td>ssl_extension_ec_point_formats</td>
<td>ssl_extension_server_name</td>
</tr>
<tr>
<td></td>
<td>ssl_server_curve</td>
<td></td>
</tr>
</tbody>
</table>
Bro SSL and X509 events
(in random order)

**Event** `ssl_stapled_ocsp`:
Bro 2.3 also supports OCSP verification.

Support stapled OCSP (Online Certificate Status Protocol) messages.
Bro SSL and X509 events
(in random order)

Event x509_* (Certificates):

More information in the records (e.g., about cryptographic key material).

Extension parsing (basic constraints, subject alternative name and presence).

Easier certificate validation, more information (e.g., full validated and built chain).
Bro SSL and X509 events
(in random order)

More detailed parsing of cipher use:

- **ssl_dh_server_params**: Diffie Hellman key information
- **Elliptic Curve support and choices.**
Bro SSL and X509 events
(in random order)

More detailed SSL extension parsing:
E.g., ALPN (Application Layer Protocol Negotiation).
Used to negotiate SPDY and HTTP/2.
Bro SSL and X509 events
(in random order)

More generic events:
Handshake messages, heartbeats, encrypted data.
Bro SSL and X509 events
(in random order)

Also:

StartSSL support (SMTP & POP3)
Much more robust.
SSL Protocol Basics

• Record based protocol

• Records do not have to map to TCP packets

• Record header is never encrypted, only payload is (after the handshake is done)
SSL Protocol Basics

- Record based protocol
- Records do not have to map to TCP packets
- Record header is never encrypted, only payload (after the handshake is done)

<table>
<thead>
<tr>
<th>Type</th>
<th>Version</th>
<th>Length</th>
<th>Payload</th>
</tr>
</thead>
</table>

Common record types:
- Change Cipher Spec
- Alert
- Handshake
- Application Data
SSL Protocol Basics

- Record based protocol
- Records do not have to map to TCP packets
- Record header is never encrypted, only payload is (after the handshake is done)
Basic SSL Handshake

Client

Client hello

Server hello

Certificate

(Client Key Exchange)

(Server Key Exchg)

Change Cipher Spec

Finished

Change Cipher Spec

Finished

Encrypted application data

Server
Basic SSL Handshake

Client hello
(extensions)

Client Key Exchange
Change Cipher Spec
Finished

Encrypted application data

Server hello
(extensions)
Certificate
(Server Key Exchg)

x509_* events
ssl_handshake_message

Change Cipher Spec
Finished

ssl_change_cipher_spec
ssl_encrypted_data
HOW THE HEARTBLEED BUG WORKS:

SERVER, ARE YOU STILL THERE?
IF SO, REPLY "POTATO" (6 LETTERS).

User Meg wants these 6 letters: POTATO. User
Meg wants pages about "girl games". Unlock
user records with master key 513909657335.

User Meg wants these 6 letters: POTATO.
User Meg wants pages about "girl games". Unlock
user records with master key 513909657335.

POTATO

SERVER, ARE YOU STILL THERE?
IF SO, REPLY "BIRD" (4 LETTERS).

User Meg wants these 6 letters: P recovered.
User Meg wants pages about "girl games". Unlock
user records with master key 513909657335.

User Meg wants these 6 letters: P recovered.
User Meg wants pages about "girl games". Unlock
user records with master key 513909657335.

SERVER, ARE YOU STILL THERE?
IF SO, REPLY "HAT" (500 LETTERS).

User Meg wants these 500 letters: HAT. Lucas
requests the "missed connections" page. User
administration wants to set server's master key to "1493508534".

User Meg wants these 500 letters: HAT. Lucas
requests the "missed connections" page. User
administration wants to set server's master key to "1493508534".

BIRD

HMM...

SERVER, ARE YOU STILL THERE?
IF SO, REPLY "BIRD" (500 LETTERS).

User Meg wants these 500 letters: HAT. Lucas
requests the "missed connections" page. User
administration wants to set server's master key to "1493508534".

User Meg wants these 500 letters: HAT. Lucas
requests the "missed connections" page. User
administration wants to set server's master key to "1493508534".

User Meg wants these 500 letters: HAT. Lucas
requests the "missed connections" page. User
administration wants to set server's master key to "1493508534".

Source: http://xkcd.com/1354/
Heartbeats

- Type
- Length
- Heartbeat Data
- Padding
Heartbeats

Record Header

Payload

Type | Version | Length | Type | Length | Heartbeat Data | Padding

Heartbeats
Heartbleed - Sample

Request:
- Type: Heartbeat
- Version: TLS 1.2
- Length: 20
- Payload:
  - Type: Request
  - Length: 60,000
  - Heartbeat Data: 1 byte
  - Padding: 16 bytes

Response:
- Type: Heartbeat
- Version: TLS 1.2
- Length: 60,019
- Payload:
  - Type: Response
  - Length: 60,000
  - Heartbeat Data: 60,000 bytes
  - Padding: 16 bytes

20 Bytes

60,019 Bytes
Detection before encryption

Check inner and outer length field.
Outer length = inner length + 1 + 2 + 16
Detection before encryption

Bro triggers a notice when it detects a exploit.
A second notice is triggered when it succeeds (if the client sends a reply).

Check inner and outer length field.
Outer length = inner length + 1 + 2 + 16
Detection before encryption

Check heartbeat length.
Minimal legal length is 19 Bytes.
Detection before encryption

Furthermore:
All heartbeats before encryption are dubious.

Give notice when Bro determines session encryption has not started yet.
Detection after encryption

Request:
- Type: Heartbeat
- Version: TLS1.2
- Length: 25
- Encrypted payload: 25

Response:
- Type: Heartbeat
- Version: TLS1.2
- Length: 60,000
- Encrypted payload: 60,000

Bro tracks request/response pairs.

Exploit succeeded when a response is sent.
Detection after encryption

Some exploit tools craft heartbeat packets that are smaller than the allowed minimum.
Detection in Bro

```
min_lengths_tls11[|min_lengths_tls11|] = [cipher=/{AES_256_GCM_SHA384/}, $min_length=43];
min_lengths_tls11[|min_lengths_tls11|] = [cipher=/{AES_128_GCM_SHA256/}, $min_length=43];
min_lengths_tls11[|min_lengths_tls11|] = [cipher=/{AES_256_CBC_SHA384/}, $min_length=96];
min_lengths_tls11[|min_lengths_tls11|] = [cipher=/{AES_256_CBC_SHA256/}, $min_length=80];
min_lengths_tls11[|min_lengths_tls11|] = [cipher=/{AES_128_CBC_SHA256/}, $min_length=80];
min_lengths_tls11[|min_lengths_tls11|] = [cipher=/{AES_128_CBC_SHA/}, $min_length=64];
min_lengths_tls11[|min_lengths_tls11|] = [cipher=/{3DES_EDE_CBC_SHA/}, $min_length=48];
min_lengths_tls11[|min_lengths_tls11|] = [cipher=/{SEED_CBC_SHA/}, $min_length=64];
min_lengths_tls11[|min_lengths_tls11|] = [cipher=/{IDEA_CBC_SHA/}, $min_length=48];
min_lengths_tls11[|min_lengths_tls11|] = [cipher=/{DES_CBC_SHA/}, $min_length=48];
min_lengths_tls11[|min_lengths_tls11|] = [cipher=/{DES40_CBC_SHA/}, $min_length=48];
min_lengths_tls11[|min_lengths_tls11|] = [cipher=/{RC4_128_SHA/}, $min_length=39];
min_lengths_tls11[|min_lengths_tls11|] = [cipher=/{RC4_128_MD5/}, $min_length=35];
min_lengths_tls11[|min_lengths_tls11|] = [cipher=/{RC4_40_MD5/}, $min_length=35];
min_lengths_tls11[|min_lengths_tls11|] = [cipher=/{RC2_CBC_40_MDS/}, $min_length=48];
min_lengths[|min_lengths|] = [cipher=/{256_CBC_SHA/}, $min_length=48];
min_lengths[|min_lengths|] = [cipher=/{128_CBC_SHA/}, $min_length=48];
min_lengths[|min_lengths|] = [cipher=/{3DES_EDE_CBC_SHA/}, $min_length=40];
min_lengths[|min_lengths|] = [cipher=/{SEED_CBC_SHA/}, $min_length=48];
min_lengths[|min_lengths|] = [cipher=/{IDEA_CBC_SHA/}, $min_length=48];
min_lengths[|min_lengths|] = [cipher=/{DES_CBC_SHA/}, $min_length=48];
min_lengths[|min_lengths|] = [cipher=/{DES40_CBC_SHA/}, $min_length=48];
min_lengths[|min_lengths|] = [cipher=/{RC4_128_SHA/}, $min_length=39];
min_lengths[|min_lengths|] = [cipher=/{RC4_128_MD5/}, $min_length=35];
min_lengths[|min_lengths|] = [cipher=/{RC4_40_MD5/}, $min_length=35];
min_lengths[|min_lengths|] = [cipher=/{RC2_CBC_40_MDS/}, $min_length=48];
```
Detection before encryption

Odd behavior:

• Heartbeats before application data

• Heartbeats within first 60 seconds
Heartbleed detection

238 lines, including empty lines and comments

@load policy/protocols/ssl/heartbleed

Embedded devices, etc. will not be patched for a long time.
Collection Setup

Sites running Bro
  add SSL data collection script
  SSL traffic identified using DPD

Result: 2 log files
  uploaded to ICSI on rotation
  not kept on local machine

collection script distributed via Git

ICSI has no access to raw data
# Notary - collected features

<table>
<thead>
<tr>
<th>Available ciphers</th>
<th>Timestamp</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Analyzer Error</td>
<td>Packet loss</td>
<td>Hash(client session ID)</td>
</tr>
<tr>
<td>Client &amp; Server TLS extensions</td>
<td>Selected cipher</td>
<td>Hash(client IP, server IP)</td>
</tr>
<tr>
<td>Content length</td>
<td>Server certificates</td>
<td>Hash(server session ID)</td>
</tr>
<tr>
<td>Connection history</td>
<td>Server IP</td>
<td>Ticket lifetime hint</td>
</tr>
<tr>
<td>Duration</td>
<td>Server Name Indication</td>
<td></td>
</tr>
<tr>
<td>Feature</td>
<td>Analyzer Error</td>
<td>Packet loss</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>---------------------------</td>
<td>----------------------</td>
</tr>
<tr>
<td>Available ciphers</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Client &amp; Server TLS extensions</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Timestamp</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Version</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Content length</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Server certificates</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Connection history</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Server IP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Duration</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Server Name Indication</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Available ciphers</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Analyzer Error</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Client &amp; Server TLS extensions</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Content length</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Connection history</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Duration</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Timestamp</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Packet loss</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Selected cipher</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hash(client session ID)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hash(client IP, server IP)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hash(server session ID)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Server certificates</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Server IP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ticket lifetime hint</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Server Name Indication</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Heartbeat supported if client and server acknowledge support in extension.
Notary - collected features

About 40% of servers supported the extension from Jan to March.

Heartbeat supported if client and server acknowledge support in extension

Client & Server TLS extensions
Content length
Connection history
Duration

Selected cipher
Server certificates
Server IP
Server Name Indication

Hash(client session ID)
Hash(client IP, server IP)
Hash(server session ID)
Hash(server session ID)
Ticket lifetime hint

Analyzer Error
Packet loss
Timestamp
Version
Restamp
About 40% of servers supported the extension from Jan to March.

About 40% of servers supported the extension from Jan to March.
About 40% of servers supported the extension from Jan to March.

Heartbeat supported if client and server acknowledge support in extension

• Google started disabling Heartbeat on March 27th
  …more than a week before public disclosure

• Akamai started disabling it on April 3rd
  4 days before disclosure.
Exploit attempts - LBL

Day

Number of scan attempts

04-08  04-09  04-10  04-11  04-12  04-13  04-14  04-15  04-16  04-17  04-18  04-19  04-20  04-21  04-22  04-23  04-24  04-25  04-26  04-27  04-28  04-29  04-30

04-04  04-05  04-06  04-07  04-08  04-09  04-10  04-11  04-12  04-13  04-14  04-15  04-16  04-17  04-18  04-19  04-20  04-21  04-22  04-23  04-24  04-25  04-26  04-27  04-28  04-29  04-30

100
200
300
Exploit attempts - LBL

No prior exploitation
## Exploit types - LBL

<table>
<thead>
<tr>
<th>Type</th>
<th>Sources</th>
<th>Dests.</th>
<th>Conns.</th>
</tr>
</thead>
<tbody>
<tr>
<td>(1) Cleartext attacks</td>
<td>254</td>
<td>179</td>
<td>701</td>
</tr>
<tr>
<td>(2) Successful cleartext attacks</td>
<td>4</td>
<td>10</td>
<td>26</td>
</tr>
<tr>
<td>(3) Short heartbeat</td>
<td>2</td>
<td>8</td>
<td>78</td>
</tr>
<tr>
<td>(4) Heartbeat before data</td>
<td>51</td>
<td>121</td>
<td>3,571</td>
</tr>
<tr>
<td>(5) Heartbeat within first minute</td>
<td>1</td>
<td>1</td>
<td>71</td>
</tr>
<tr>
<td>(6) Successful attack after encryption</td>
<td>5</td>
<td>6</td>
<td>77</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>300</strong></td>
<td><strong>203</strong></td>
<td><strong>4,266</strong></td>
</tr>
</tbody>
</table>
### Exploit types - LBL

<table>
<thead>
<tr>
<th>Type</th>
<th>Sources</th>
<th>Dests.</th>
<th>Conns.</th>
</tr>
</thead>
<tbody>
<tr>
<td>(1) Cleartext attacks</td>
<td>254</td>
<td>179</td>
<td>701</td>
</tr>
<tr>
<td>(2) Successful cleartext attacks</td>
<td>4</td>
<td>10</td>
<td>26</td>
</tr>
<tr>
<td>(3) Short heartbeat</td>
<td>2</td>
<td>8</td>
<td>78</td>
</tr>
<tr>
<td>(4) Heartbeat before data</td>
<td>51</td>
<td>121</td>
<td>3,571</td>
</tr>
<tr>
<td>(5) Heartbeat within first minute</td>
<td>1</td>
<td>1</td>
<td>71</td>
</tr>
</tbody>
</table>

**Total** 300  203  4,266

Very low number of successful attacks due to aggressive blocking of incoming scans.
Certificate changes

Number of IPs with same certificate vs Day

- **April**
- **March**
Evolution of cipher suites
Summary

• Many SSL changes in Bro 2.3.

• Exercise tomorrow will show possible uses.

• Bro has very comprehensive detection of Heartbleed …which will stay interesting for quite a while.

• Notary: http://notary.icsi.berkeley.edu
  We are looking for more sources.