

Déboguer les applications réseau lorsque tout est chiffré (1/13)

Stéphane Bortzmeyer
stephane+cdl@bortzmeyer.org

Capitole du Libre, 19 novembre 2022

Avant

Avant

- Rien n'était chiffré,

Avant

- Rien n'était chiffré,
- Les bisounours et les licornes gambadaient ensemble dans des lacs de confiture de groseille,

Avant

- Rien n'était chiffré,
- Les bisounours et les licornes gambadaient ensemble dans des lacs de confiture de groseille,
- On faisait confiance au réseau,

Avant

- Rien n'était chiffré,
- Les bisounours et les licornes gambadaient ensemble dans des lacs de confiture de groseille,
- On faisait confiance au réseau,
- Et on déboguait avec tcpdump / Wireshark,

Avant

- Rien n'était chiffré,
- Les bisounours et les licornes gambadaient ensemble dans des lacs de confiture de groseille,
- On faisait confiance au réseau,
- Et on déboguait avec tcpdump / Wireshark,
- Remarquables outils pour apprendre le réseau, d'ailleurs.

Depuis

Depuis

- Edward nous a prévenu que des méchants espionnaient,

Depuis

- Edward nous a prévenu que des méchants espionnaient,
- Même les jenairiencacher ont compris,

Depuis

- Edward nous a prévenu que des méchants espionnaient,
- Même les jenairiencacher ont compris,
- On chiffre tout, et à juste titre,

Depuis

- Edward nous a prévenu que des méchants espionnaient,
- Même les journalistes ont compris,
- On chiffre tout, et à juste titre,
- Les derniers bastions du non-chiffrement cèdent :
 - DNS avec DoT, DoH et DoQ,
 - La couche transport, avec QUIC.

Depuis

- Edward nous a prévenu que des méchants espionnaient,
- Même les jenairiencacher ont compris,
- On chiffre tout, et à juste titre,
- Les derniers bastions du non-chiffrement cèdent :
 - DNS avec DoT, DoH et DoQ,
 - La couche transport, avec QUIC.
- Tout ce qui n'est pas chiffré pourra être utilisé contre vous (RFC 8546 sur la *wire image*).

Alors, comment on fait ?

On peut lutter contre le chiffrement

On peut lutter contre le chiffrement

- Les gens qui réclament de la « visibilité »,

On peut lutter contre le chiffrement

- Les gens qui réclament de la « visibilité »,
- Les affaiblissements délibérés (comme le ETLS de l'ETSI),

On peut lutter contre le chiffrement

- Les gens qui réclament de la « visibilité »,
- Les affaiblissements délibérés,
- La diabolisation de DoH,

On peut lutter contre le chiffrement

- Les gens qui réclament de la « visibilité »,
- Les affaiblissements délibérés,
- La diabolisation de DoH,
- « Nous sommes pour le chiffrement, mais » (discours de l'Internet Watch Foundation),

On peut lutter contre le chiffrement

- Les gens qui réclament de la « visibilité »,
- Les affaiblissements délibérés,
- La diabolisation de DoH,
- « Nous sommes pour le chiffrement, mais »,
- Combat d'arrière-garde ?

On peut demander à l'application de donner ses clés

On peut demander à l'application de donner ses clés

- Rappel de cryptographie « hybride » : la cryptographie asymétrique ne sert qu'à l'échange de clés, on fait de la cryptographie symétrique après, avec cette clé de session,

On peut demander à l'application de donner ses clés

- Rappel de cryptographie « hybride » : la cryptographie asymétrique ne sert qu'à l'échange de clés, on fait de la cryptographie symétrique après, avec cette clé de session,
- L'application peut exporter cette clé, un logiciel d'analyse du trafic peut ensuite l'utiliser pour déchiffrer,

On peut demander à l'application de donner ses clés

- Rappel de cryptographie « hybride » : la cryptographie asymétrique ne sert qu'à l'échange de clés, on fait de la cryptographie symétrique après, avec cette clé de session,
- L'application peut exporter cette clé, un logiciel d'analyse du trafic peut ensuite l'utiliser pour déchiffrer,
- `SSL_CTX_set_keylog_callback` avec OpenSSL,

On peut demander à l'application de donner ses clés

- Rappel de cryptographie « hybride » : la cryptographie asymétrique ne sert qu'à l'échange de clés, on fait de la cryptographie symétrique après, avec cette clé de session,
- L'application peut exporter cette clé, un logiciel d'analyse du trafic peut ensuite l'utiliser pour déchiffrer,
- `SSL_CTX_set_keylog_callback` avec OpenSSL,
- Wireshark sait relire ces clés (`tls.keylog_file: /tmp/mykeys` dans la configuration),

On peut demander à l'application de donner ses clés

- Rappel de cryptographie « hybride » : la cryptographie asymétrique ne sert qu'à l'échange de clés, on fait de la cryptographie symétrique après, avec cette clé de session,
- L'application peut exporter cette clé, un logiciel d'analyse du trafic peut ensuite l'utiliser pour déchiffrer,
- `SSL_CTX_set_keylog_callback` avec OpenSSL,
- Wireshark sait relire ces clés,
- Attention, c'est à l'application de faire ce qu'il faut, la bibliothèque TLS ne le fait pas (curl le fait mais pas openssl),

On peut demander à l'application de donner ses clés

- Rappel de cryptographie « hybride » : la cryptographie asymétrique ne sert qu'à l'échange de clés, on fait de la cryptographie symétrique après, avec cette clé de session,
- L'application peut exporter cette clé, un logiciel d'analyse du trafic peut ensuite l'utiliser pour déchiffrer,
- `SSL_CTX_set_keylog_callback` avec OpenSSL,
- Wireshark sait relire ces clés,
- Attention, c'est à l'application de faire ce qu'il faut, la bibliothèque TLS ne le fait pas (curl le fait mais pas openssl),
- Moyen le plus courant de le demander : la variable d'environnement `SSLKEYLOGFILE`.

Exemple de code Python

```
def write_keys(conn, keys):  
    keylogfile.write(keys.decode() + "\n")  
  
if os.environ["SSLKEYLOGFILE"]:  
    keylogfile = open(os.environ["SSLKEYLOGFILE"], "a")  
    context.set_keylog_callback(write_keys)
```

Dans Wireshark

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
9	0.024467	192.168.2.4	193.70.85.11	TCP	66	58052 → 1965 [ACK] Seq=324 Ack=1576 Win=64128 Len=0 TSval=3455568688 TSecr=65590872
10	0.024586	193.70.85.11	192.168.2.4	TCP	1514	1965 → 58052 [PSH, ACK] Seq=1576 Ack=324 Win=64896 Len=1448 TSval=3455568672 TSecr=3455568672
11	0.024588	192.168.2.4	193.70.85.11	TCP	66	58052 → 1965 [ACK] Seq=324 Ack=3024 Win=64128 Len=0 TSval=3455568688 TSecr=65590872
12	0.024710	193.70.85.11	192.168.2.4	TLSv1.3	1514	Certificate [TCP segment of a reassembled PDU]
13	0.024712	192.168.2.4	193.70.85.11	TCP	66	58052 → 1965 [ACK] Seq=324 Ack=4472 Win=64128 Len=0 TSval=3455568688 TSecr=65590872
14	0.030785	193.70.85.11	192.168.2.4	TLSv1.3	236	Certificate Verify, Finished
15	0.030789	192.168.2.4	193.70.85.11	TCP	66	58052 → 1965 [ACK] Seq=324 Ack=4642 Win=64128 Len=0 TSval=3455568694 TSecr=65590880
16	0.030958	192.168.2.4	193.70.85.11	TLSv1.3	176	Change Cipher Spec, Certificate, Finished
17	0.038802	193.70.85.11	192.168.2.4	TLSv1.3	169	New Session Ticket
18	0.038812	192.168.2.4	193.70.85.11	TLSv1.3	120	Application Data
19	0.048168	193.70.85.11	192.168.2.4	TLSv1.3	91	Application Data
20	0.049145	193.70.85.11	192.168.2.4	TLSv1.3	1514	Application Data, Application Data
21	0.049150	192.168.2.4	193.70.85.11	TCP	66	58052 → 1965 [ACK] Seq=488 Ack=6218 Win=64128 Len=0 TSval=3455568713 TSecr=65590898
22	0.049188	193.70.85.11	192.168.2.4	TLSv1.3	90	Alert (Level: Warning, Description: Close Notify)
23	0.049512	192.168.2.4	193.70.85.11	TLSv1.3	90	Alert (Level: Warning, Description: Close Notify)
24	0.049533	192.168.2.4	193.70.85.11	TCP	66	58052 → 1965 [FIN, ACK] Seq=512 Ack=6810 Win=64128 Len=0 TSval=3455568713 TSecr=65590898
25	0.057435	193.70.85.11	192.168.2.4	TCP	66	1965 → 58052 [RST] Seq=6010 Win=0 Len=0
26	0.057478	193.70.85.11	192.168.2.4	TCP	66	1965 → 58052 [RST] Seq=6010 Win=0 Len=0

* Frame 22: 657 bytes on wire (5256 bits), 657 bytes captured (5256 bits)
 * Ethernet II, Src: CZNICzsp_00:4c:9e (d8:58:d7:00:4c:9e), Dst: Micro-St_ab:01:3c (2c:f0:5d:ab:01:3c)
 * Internet Protocol Version 4, Src: 193.70.85.11, Dst: 192.168.2.4
 * Transmission Control Protocol, Src Port: 1965, Dst Port: 58052, Seq: 6218, Ack: 488, Len: 591
 * [2 Reassembled TCP Segments (1949 bytes): #20(1382), #22(567)]
 * Transport Layer Security
 * Data [1527 bytes]
 * Transport Layer Security

```

0000  23 20 53 74 c3 a9 70 68 61 6e 65 20 42 6f 72 74  # St...ph...ane Bort
0010  7a 6d 65 79 65 72 27 73 20 47 65 6d 69 6e 69 20  zmeyer's Gemini
0020  73 65 72 70 65 72 0a 0a 54 68 69 73 20 69 73 20  server... This is
0030  6f 6f 73 74 6c 79 20 61 6e 20 65 78 70 65 72 69  mostly a an experi
0040  6d 65 6e 74 61 6e 20 73 65 72 70 65 72 2e 20 59  mental's server. Y
0050  6f 75 20 7f 69 6c 6c 20 6e 6f 74 20 65 69 6e 64  ou will not find
0060  29 61 29 6c 6f 74 20 6f 0e 28 63 6f 6e 74 65 6e  a lot of conten
0070  74 2e 0a 0a 23 23 20 52 46 43 0a 0a 54 68 69 73  t...# R FC- This
0080  29 69 73 29 61 29 6d 69 72 72 6f 72 20 6f 6e 20  is a mirror of
0090  52 46 43 73 20 28 73 61 63 72 65 64 20 74 65 78  RFCs (sa cred tex
00a0  74 73 20 6f 6e 29 74 68 65 20 49 6e 74 65 72 6e  ts of the Intern
00b0  65 74 29 2e 0a 0a 3d 2e 20 67 65 6d 69 6e 69 3a  et)...-> gemini:
00c0  2f 2f 6f 65 6d 69 6e 69 2e 62 6f 72 74 7a 6d 65  //gemini..bortzme
00d0  79 65 72 2e 6f 72 6f 2f 72 6e 63 2d 6d 69 72 72  yer.org/rfc-mirr
00e0  6f 72 2f 72 6e 63 2d 69 6e 64 65 78 2e 6f 6d 69  or/rfc-1 ndex.gmi
00f0  29 49 6e 04 65 78 20 6f 6e 20 61 6c 6c 29 52 46  Index of all RF
0100  43 20 0a 0a 4f 72 20 79 6f 75 20 63 61 6e 20 63  C...Or y ou can c
0110  72 65 63 7a 65 20 61 6e 20 65 52 4c 29 7f 69 74  reate an URL wit
0120  58 20 74 68 65 29 52 46 43 20 6e 75 6d 62 65 72  n the RFC number
0130  20 6f 65 6d 69 6e 69 3a 2f 2f 6f 65 6d 69 6e 69  gemini: //gemini
  
```

On peut demander à l'application de dire ce qu'elle fait

On peut demander à l'application de dire ce qu'elle fait

- L'application peut aussi aider, en étant bavarde,

On peut demander à l'application de dire ce qu'elle fait

- L'application peut aussi aider, en étant bavarde,
- `curl --verbose` est un modèle, `curl --trace` (ou `--trace-ascii`) est encore plus détaillé,

On peut demander à l'application de dire ce qu'elle fait

- L'application peut aussi aider, en étant bavarde,
- `curl --verbose` est un modèle, `curl --trace` est encore plus détaillé,
- Firefox et ses *Web Developer Tools* aussi.

Firefox nous aide

The screenshot shows the Firefox Developer Tools interface with the Network tab selected. The browser's address bar displays `localhost:5681/inbox`. The Network tab shows a list of requests:

Status	Met...	Domain	File	Initiator	Type	Transferred	Size
202	POST	localhost:...	inbox	document	plain	142 B	5 B
404	GET	localhost:...	favicon.ico	FaviconLoad...	html	cached	207 B

The selected request (202) is expanded to show its details:

- Filter Headers:**
 - Scheme: http
 - Host: localhost:5681
 - Filename: /inbox
- Address:** 127.0.0.1:5681
- Status:** 202
- Version:** HTTP/1.1
- Transferred:** 142 B (5 B size)
- Referrer Policy:** strict-origin-when-cross-origin
- Request Priority:** Highest
- Response Headers (137 B):**
 - content-length: 5
 - content-type: text/plain; charset=utf-8
 - date: Tue, 15 Nov 2022 09:39:19 GMT
 - server: hypercorn-h11

Encore mieux si c'est normalisé

Encore mieux si c'est normalisé

- Les solutions précédentes sont pour examen par un humain, et sont spécifiques à une application,

Encore mieux si c'est normalisé

- Les solutions précédentes sont pour examen par un humain, et sont spécifiques à une application,
- Il y a un format normalisé pour exporter dans un fichier le dialogue, qlog (créé à l'origine pour QUIC).

Encore mieux si c'est normalisé

- Les solutions précédentes sont pour examen par un humain, et sont spécifiques à une application,
- Il y a un format normalisé pour exporter dans un fichier le dialogue, qlog.
- qlog est un format abstrait, qui peut se retrouver instancié en, par exemple, JSON.

Encore mieux si c'est normalisé

- Les solutions précédentes sont pour examen par un humain, et sont spécifiques à une application,
- Il y a un format normalisé pour exporter dans un fichier le dialogue, qlog.
- qlog est un format abstrait, qui peut se retrouver instancié en, par exemple, JSON.
- qlog est générique et peut s'appliquer à plusieurs protocoles.

Et avec une brosse à dents connectée ?

Et avec une brosse à dents connectée ?

- Comment savoir ce que votre brosse à dents raconte à son maître ?

Et avec une brosse à dents connectée ?

- Comment savoir ce que votre brosse à dents raconte à son maître ?
- (Ça a été utilisé comme argument anti-DoH.)

Et avec une brosse à dents connectée ?

- Comment savoir ce que votre brosse à dents raconte à son maître ?
- (Ça a été utilisé comme argument anti-DoH.)
- Le fond du problème est plutôt le logiciel privé.

En résumé

En résumé

- Wireshark reste super, mais il faut aussi enseigner / pratiquer le débogage par la coopération de l'application,

En résumé

- Wireshark reste super, mais il faut aussi enseigner / pratiquer le débogage par la coopération de l'application,
- Toute application réseau devrait fournir des outils de débogage du trafic,

En résumé

- Wireshark reste super, mais il faut aussi enseigner / pratiquer le débogage par la coopération de l'application,
- Toute application réseau devrait fournir des outils de débogage du trafic,
- Il faut évidemment exiger du logiciel libre,

En résumé

- Wireshark reste super, mais il faut aussi enseigner / pratiquer le débogage par la coopération de l'application,
- Toute application réseau devrait fournir des outils de débogage du trafic,
- Il faut évidemment exiger du logiciel libre,
- Car sinon, on ne peut pas avoir confiance, même si le logiciel privateur produit une trace.