TLS 1.3 draft 23 ハンズオン

2018.2.14

山本和彦
@kazu_yamamoto

ブラウザで TLS 1.3 接続してみる

- サーバ
  - `https://mew.org/`
- Firefox Nightly
  - `https://mew.org/`
  - 錠前 → ">" → "More Information"
- Chrome Canary
  - `chrome://flags#tls13-variant` -> Draft 23
  - 再起動
  - "..." ボタン → Devtool → Security
  - `https://mew.org/`

Haskell TLS クライアントを使ってみる

- `tls-simpleclient`
  - `https://mew.org/~kazu/proj/tls13-handson/`
  - この勉強会の後には消します
- マニュアル
  - `https://github.com/vincenthz/hs-tls/issues/167`
- 基本的な使い方

```
% tls-simpleclient host [port]
```

- ファイアウォール機能に注意！
- 以後、以下のオプションを指定しているとします
  - `-O <file>`　HTMLの出力先
  - `--http1.1`　HTTP/1.1 で "GET /" を送る
  - `--no-valid`　サーバ認証を省略する

フルハンドシェイク

```
% tls-simpleclient -g x25519 mew.org
groups = [X25519], keyshare = [X25519]
TLS 1.3: AES128GCM-SHA256 SHA256
NewSessionTicket received: lifetime = 86400 sec
```

HRR(Hello Retry Request)

```
% tls-simpleclient mew.org
groups = [X448,X25519,P256], keyshare = [X448]
Retrying client hello...
groups = [X25519], keyshare = [X25519]
TLS 1.3: AES128GCM-SHA256 SHA256
NewSessionTicket received: lifetime = 86400 sec
```

PSK(PreShared Key)

```
% tls-simpleclient --session mew.org
groups = [X448,X25519,P256], keyshare = [X448]
Retrying client hello...
groups = [X25519], keyshare = [X25519]
TLS 1.3: AES128GCM-SHA256 SHA256
NewSessionTicket received: lifetime = 86400 sec

Resuming the session...
groups = [X25519], keyshare = [X25519]
TLS 1.3: AES128GCM-SHA256 SHA256
PSK[0] is used
NewSessionTicket received: lifetime = 86400 sec
```

0RTT(Round Trip Time)

```
% cat early-data.txt
GET / HTTP/1.1
Host: mew.org

% tls-simpleclient --session \
    -Z early-data.txt mew.org
groups = [X448,X25519,P256], keyshare = [X448]
Retrying client hello...
groups = [X25519], keyshare = [X25519]
TLS 1.3: AES128GCM-SHA256 SHA256
NewSessionTicket received: lifetime = 86400 sec

Resuming the session...
groups = [X25519], keyshare = [X25519]
Sending 0RTT data...
TLS 1.3: AES128GCM-SHA256 SHA256
PSK[0] is used
0RTT data is accepted
NewSessionTicket received: lifetime = 86400 sec
```

TLS 1.3 draft 23 公開サーバ

- `enabled.tls13.com` (BoringSSL)
- `www.tls13.facebook.com` (fizz)
- `tls13.crypto.mozilla.org` (NSS)

picotlsをビルドする

```
% git clone https://github.com/h2o/picotls
% cd picotls
% git submodule init
% git submodule update
% cmake .
% make
% ls cli
cli
```

picotls クライアント

- フルハンドシェイク

```
% cli mew.org 443
```

- HRR

```
% cli -n mew.org 443
```

- PSK

```
% rm ticket
% cli -s ticket mew.org 443
% cli -s ticket mew.org 443
```

- 0RTT

```
% rm ticket
% cli -s ticket mew.org 443
% cat early-data.txt - | cli -s ticket mew.org 443
```

さらに進むには

- Haskell TLS の `tls-simpleserver`
  - `https://github.com/vincenthz/hs-tls/issues/167`
- picotls のサーバ
  - `http://d.hatena.ne.jp/kazu-yamamoto/20180214`
- OpenSSL
  - `http://d.hatena.ne.jp/kazu-yamamoto/20170530`
- BoringSSL
  - `http://d.hatena.ne.jp/kazu-yamamoto/20171205`
- NSS
  - `http://d.hatena.ne.jp/kazu-yamamoto/20170207`
- Wireshark
  - `https://www.wireshark.org/download/automated/`