「SSL/TLSの基礎と最新動向」を受講して

#seccamp 2015 @elliptic_shiho

自己紹介

- 緑川志穂(@elliptic_shiho)
- Crypto, Binary, CTF, …
- 今回のseccampでは低レイヤートラックを中心に取りました

講義概要

- AES_128_GCMやHMAC-SHA256等の実際に利用されている暗号技術の一部をワークショップ的にNode.jsを使って実装する
- SSL/TLSのハンドシェイク処理を学び、Node.jsを使って通信をしてみる
- TLS 1.3とそれ以前との違いを学ぶ

良かった/楽しかった

- ワークショップ形式でTLSで利用されている独特とも言える暗号化方式についての理解をすることができた。

  - 同時にNode.jsの暗号ライブラリの利用法を学ぶことが出来た。

良かった/楽しかった

- 普段Wiresharkで解析したり眺めるだけのパケットだったTLSの通信を深く掘り下げて読む良い機会だった。
  - 普段何気なく使っている基盤をきちんと知ることが出来た。

良かった/楽しかった

- 最新規格であるTLS1.3をTLS1.2との対比を通じて学ぶことができた。
  - TLS1.2の問題点とそれをどのようにしてTLS1.3で解決しているかを学べた。
  - 逆にTLS1.3になったから出てきた脆弱性についても知ることが出来た。

講義を終えて

- 普通に楽しかった
  - Node.jsを触ったことが殆ど無くて少し苦戦した..
    - 事前課題をしっかりやり込むべき

講義を終えて

- 普通に調べたら入手がかなり大変な資料やニッチな情報もあり、4時間とは思えない濃さだった。
  - スライドだけでも非常に有用な資料だと思うので興味のある方は見てみると良いかもしれない

ありがとうございました