STRINT workshop

中島 博敬 / @nunnun

http://www.w3.org/People/Hiro

Keio University
1858
CALAMVS
GLADIO
FORTIOR

自己紹介

- **なかじま ひろたか**
- 慶應義塾大学 政策・メディア研究科 後期博士課程

  慶應義塾 湘南藤沢ITC
- https://github.com/nunnun / @nunnun
- 研究トピック
  - モバイルインターネット
  - MPTCP, SCTP, QUIC, HTTP/2, WebSocket, WebRTC
  - ガジェット

STRINT workshop

- IETF 88(バンクーバー)での動きをうけて、
  Pervasive Monitoringにどう対応するかがトピック
- IETF 89開催前(2月28日/3月1日)に開催
- IAB と W3C の共同ワークショップ
- 66のポジションペーパ/i-dが提出され、100名程度
  参加

Threats

- PMで行われている攻撃手法を正しく区分
  - Passive Attacker
  - Active Attacker
    - 協力者
      - 一時的な秘密鍵の漏洩(Static Key Exfilatration)
      - 動的な秘密鍵の漏洩(Dynamic Key Exfilatration)
      - コンテンツの漏洩(Content exfilatration)

http://down.dsg.cs.tcd.ie/strint-slides/s1-threat.pdf

COMSEC

- いかに既存の安全な手法の利用を増やすか
  - HTTPS

    Captive Portal, モバイルアプリ
  - SIP

    End-to-end暗号とかはあまり機能していない

    WebRTCはどうやら安全そう
  - XMPP

    IM Observatory, 他のIMは安全なの？
  - RADIUS

Policy

- 世論はSurveillanceに肯定的

  既にあらゆるところで監視されているので諦めている

- Monitoringの商業的な成功、規制当局の容認、Patriot Act

  など法的な裏付け

- GCHQ, Yahooの事例

- 技術とPolitics両方からのアプローチが必要

  OECD Privacy Framework, 国連のデジタルプライバシー

  権など

Opportunistic Keying

- DNSでKey Discovery
- 既存技術でどの程度Opportunistic keyingが用いられているか
- Opportunistic Keyingですべてが解決とはならない
- トランスポート層でOEをする: TCPCrypt

  Password-Authenticated Key Exchangeの利用
- HTTP/2におけるTLS for HTTP:// URL

  Explicit Proxy問題

Metadata

- metadataとは何か
- metadataの漏洩方法: ブラウザのリクエストなど
- e2eにおけるmetadataの保護
- metadata surveillanceから保護

  Aggregation, Contraflow, MultiPath

Deployment

- 安全なプロトコルはe2e暗号の使用が前提

  しかし現実は異なる。

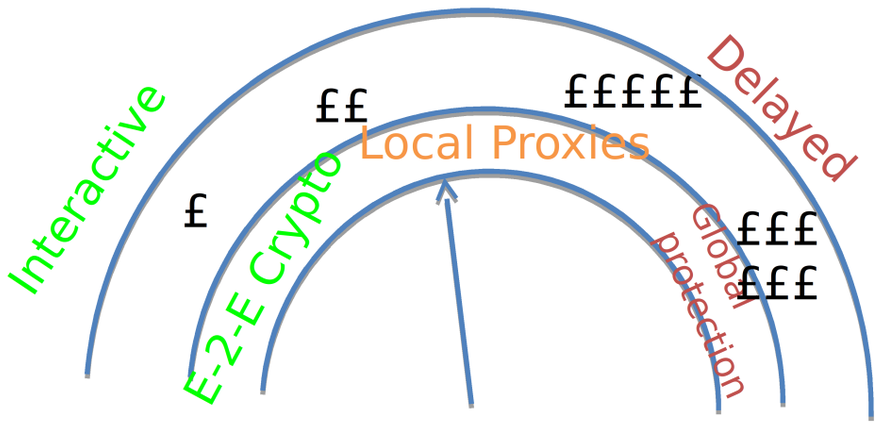
- metadata量

  e2e > local proxy > global

- 適切なリスク評価を

- Functional Signature, Encryption, 準同型暗号の

  活用



Sneakometer

Keio University
1858
CALAMVS
GLADIO
FORTIOR

その他

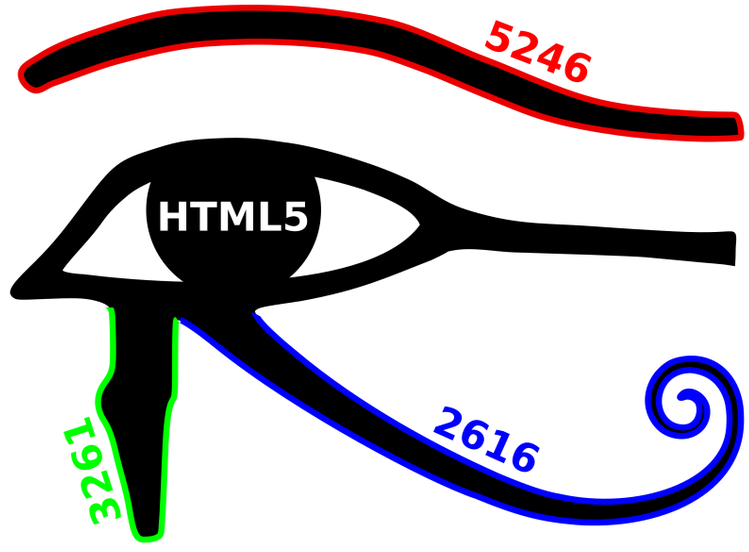
- セキュアなUI

  ValidではないSSL証明書使用時のUI・UI標準化の困難さ

- BetterCrypto.org : Gamificationの有用性

- Terminology
  - metadata -> envelop data, traffic analysis
  - Opportunistic Encryption -> Keying

- W3C Security IG / Privacy IG



Strengthening the Internet Against Pervasive Monitoring

London, 28 Feb – 1 Mar 2014

https://www.w3.org/2014/strint

Question?

hiro@awa.sfc.keio.ac.jp

http://www.w3.org/People/Hiro

@nunnun

Keio University
1858
CALAMVS
GLADIO
FORTIOR