HTTP-related WG Report (IETF88)

株式会社レピダム 林 達也

HAYASHI, Tatsuya

lepidum Co. Ltd.

IETF88報告会 2013/12/20

Agenda

- 自己紹介
- 参加の背景・経緯
- rtcweb WG
- httpbis WG
- httpauth WG
- oauth WG
- etc
  - tsvarea (QUIC)
  - uta WG

IETF 88

- Vancouver, Canada
- November 3-8, 2013

自己紹介

- 名前
  - 林 達也 (@lef)
- 所属
  - 株式会社レピダム
    代表取締役
    - https://lepidum.co.jp/
  - OpenIDファウンデーション
    ジャパン プロデューサー
  - Identity Conference (#idcon)
  - Internet Society
    Japan Chapter
    プログラム委員(2013)
- 業務領域
  - 標準化支援
  - 認証・認可, アイデンティティ、プライバシー
  - ネットワーク技術
  - ソフトウェアセキュリティ, 脆弱性
  - プログラミング言語処理系

背景・経緯

- 「HTTP相互認証プロトコル」の標準化支援
  - httpauth WG(Sec Area)
    - https://tools.ietf.org/html/draft-oiwa-http-mutualauth
  - (独)産業技術総合研究所様の研究成果
    - https://www.rcis.aist.go.jp/special/MutualAuth/
- IETFや標準化との関わり
  - IETF76広島(November 8-13 2009)から
  - 主にHTTP/Webと認証を中心に
- いくつかの企業様向けに、標準化支援や最新動向のコンサルテーション等をしています

rtcweb WG (WebRTC)

- Real-time Communication Between Browsers
- ブラウザで音声や映像の**通信**を実現
  - 音声や映像でのコミュニケーションが目的のため、P2P通信まで規格に入っている
  - プラグインなし！
- ChromeやFirefoxで実装済み
- W3CとIETFで策定中
  - 3GPPも？

WebRTC

- Hello Firefox, this is Chrome calling!
  - http://blog.chromium.org/2013/02/hello-firefox-this-is-chrome-calling.html
- Hello Chrome, it's Firefox calling!
  - https://hacks.mozilla.org/2013/02/hello-chrome-its-firefox-calling/

Huge Spec(a part of...)

- Network Stack
  - ICE: Interactive Connectivity Establishment (RFC 5245)
    - STUN: Session Traversal Utilities for NAT (RFC 5389)
    - TURN: Traversal Using Relays around NAT (RFC 5766)
  - SDP: Session Description Protocol (RFC 4566)
  - DTLS: Datagram Transport Layer Security (RFC 6347)
  - SCTP: Stream Control Transport Protocol (RFC 4960)
  - SRTP: Secure Real-Time Transport Protocol (RFC 3711)
- VoiceEngine
  - Audio Codec
  - Jitter/packet loss concealment
  - Echo Cancellation
  - Noise reduction
  - Audio Capture (Hardware Access)
- VideoEngine
  - Video Codec
  - Jitter/packet loss concealment
  - Synchronization
  - Image Enhancement
  - Video Capture (Hardware Access)

Impact of WebRTC

- ブラウザそのものが通信の世界まで担う
- ブラウザのプラットフォーム化の最たるもの
- 実装と仕様策定の乖離がW3C的？
  - Running Codeはかなり先にいっているのに、決まってないことはまだ山積み！
  - MTIで延々と議論 → でもChrome/Firefoxは相互接続してる

rtcweb WG in IETF88

- 『コーデック戦争 (H.264 vs VP8) 終結か？』 (IETF報告会85より)
  - 大嘘でした…
- mandatory to implement (MTI)
  - Audio: G.711(STD.ITU-T RECMN G.711-ENGL 1989) and Opus(RFC 6716) → fixed!
  - Video:
  - H.264 vs VP8 Battle!!!
    - OpenH264公開 → Cisco "we pay MPEG-LA"
      - http://www.openh264.org/
    - → 決着せず…！
    - RFC3929: Alternative Decision Making Processes for Consensus-Blocked Decisions in the IETF で決着する案が出た
      - しかし…

httpbis WG

- Hypertext Transfer Protocol Bis
- HTTPを扱っているWG
  - 現在、HTTP/2.0を仕様策定中
  - 以前はHTTP/1.1の曖昧さを廃し、適切に仕様定義しなおすことを目指していた(1.1 はWGLC中！->まだ…)
- HTTP/2.0については頻繁にInterimを開催
  - 次回はJanuary 22-24 2014 Interim - Zurich CH

HTTP/1.1(bis) in IETF88

"Plan is to reach the RSE in January." !!!

HTTP/2.0

- Webの世界に起きる静かで大きな**変革**

- 目的
  - 環境を限定しないパフォーマンス改善
  - ネットワーク資源の効率的な使用
  - 現代的なセキュリティ要件および慣習の反映
  - いくつかの提案の中からGoogleのSPDYというプロトコルをスタートポイントに策定を開始

HTTP/1.1と2.0の違い

- HTTPヘッダーのバイナリ化
- HTTPヘッダーの効率化(圧縮)
- 多重化(Multiplexing)
- 優先制御(Prioritizing)
- 通信の開始方法
- TCPコネクションの利用方針
- etc...

HTTP/2.0 in IETF88 (1)

- Seattle Interim meeting summary
- Upgrade Mechanism
  - Alt-Svc
- Priority Levelling
- Frame Type
- HPACK

HTTP/2.0 in IETF88 (2)

- Security Area Joint Meeting
- ALPN review
- HPACK review (focus on CRIME)
- Encryption and HTTP/2
  - Opportunistic Encryption(日和見暗号)
    - http:// でのサーバ検証の有無
    - なにもしない / HTTP/2.0ではhttps必須に
- Accommodating Proxies

HTTP/2.0 after IETF88

- Moving forward on improving HTTP's security
  - http://lists.w3.org/Archives/Public/ietf-http-wg/2013OctDec/0625.html
- HTTP2はhttps必須に？
  - Chrome/Firefoxは平文なしと明言
  - IEは平文ありと明言

- https://twitter.com/mnot/status/400564763559620608
- PROXY問題/安全を盲信されないか？等の反対意見、等々

httpauth WG

- Hypertext Transport Protocol Authentication
- 現在の機能の不足や安全性等、課題の多いHTTPプロトコルの認証機構を、新しく安全にすることを目指す
  - TLSを用いる方法やHTMLのフォーム認証はスコープ外
- 新しい認証をExperimental RFCとして策定
  - 現在ある複数の提案を統合したり選んだりするのではなく相互にレビューする形
  - 仕様と実装とどっちが先かの問題を避ける
- BasicおよびDigestの国際化、Digestのアルゴリズム更新もスコープ
  - こちらはStandard Track RFCを目指す

httpauth WG in IETF88

- Report on Virtual Interim
- Basic: To merge basicauth-update and basicauth-enc
- Digest: Need review for draft-ietf-httpauth-digest-00
- HTTP Origin-Bound Authentication (HOBA)
- RESTful Authentication Pattern for the Hypertext Transport Protocol (RestAuth)
- Commonalities

oauth WG

- Web Authorization Protocol
  - Webで使われる認可の為のフレームワーク
  - RFC6749 "The OAuth 2.0 Authorization Framework"
  - RFC6750 "The OAuth 2.0 Authorization Framework: Bearer Token Usage"
- 現在は拡張仕様や周辺仕様との連携、トークンのフォーマット、周辺エンドポイント等の議論中
- 踏まえてRecharteringをする予定、なのですが…

oauth WG in IETF88

- Dynamic Client Registration
  - 継続して議論中
- Proof-of-Possession
  - 昔Holder of Key(HoK)と呼ばれていた提案
  - MAC Tokenとの連携
    - やはりBearerでないトークンへの需要は大きい
  - 継続して議論中
- Act-As and On-Behalf-Of Token
  - WS-Security, WS-Trustで実現していた機能をカバーしたい？

Info: OAuth2.0, OIDC & UMA Interop (revised)

- OAuth2.0, OIDC and UMA Interop event is co-sponsored by the MIT-KIT, the Internet Society (ISOC) and the Kantara Initiative.
  - https://kit.mit.edu/events/
  - https://elists.isoc.org/pipermail/oauth-interop/
  - https://elists.isoc.org/mailman/listinfo/oauth-interop

QUIC:"Quick UDP Internet Connections"

- GoogleがChrome(Chromium)に新しく導入したプロトコル
- まだ概要やデザインドキュメント程度しか公開されていない
  - http://blog.chromium.org/2013/06/experimenting-with-quic.html
  - https://docs.google.com/a/chromium.org/document/d/1RNHkx_VvKWyWg6Lr8SZ-saqsQx7rFV-ev2jRFUoVD34
- 目的
  - TLSによく似た高セキュリティ
  - TCP Fast Open と TLS Snapstart を組み合わせたような(だいたい 0-RTTの)素早い接続
  - パケットロスを低減するパケット速度調整
  - 再送頻度を低減するパケットのエラー補正
  - TCP のHead-of-Lineブロッキング(先頭詰り)を回避するUDPトランスポート
  - モバイルクライアントのために再接続を削減する接続ID
  - 取り替え可能(pluggable)な輻輳制御メカニズム

QUICの中身

- 中身としてはUDP上でTCP+TLSに相当する機能を実現するプロトコルといっていいと思われる
- そのQUIC上ではSPDYを使うことが前提とされている
- 名前通り、TCPよりも早く通信をしたいというのが目標なのは明白
- このブログの著者欄には"RTT Reduction Ranger" (ラウンドトリップ時間を削減するレンジャー部隊)との肩書がついているように、RTTの短縮はかなり大きな重要なのは間違いない
- 仮にSPDYを前例とすれば、この後、標準化の提案がある可能性はそれなりに高いように思われる

Impact of QUIC

- TLSによくにた高いセキュリティ？
  - → DTLSですらなく新規？PKIは?
- SPDY必須が前提だが？
  - → HTTP/2.0が標準化され、QUICが標準化されたら?
- UDPを使うことでブラウザ(Userland)の世界に通信コンポーネントが移動？
  - →OSの機能を取り込んでいっている？
- ブラウザのプラットフォーム化！？

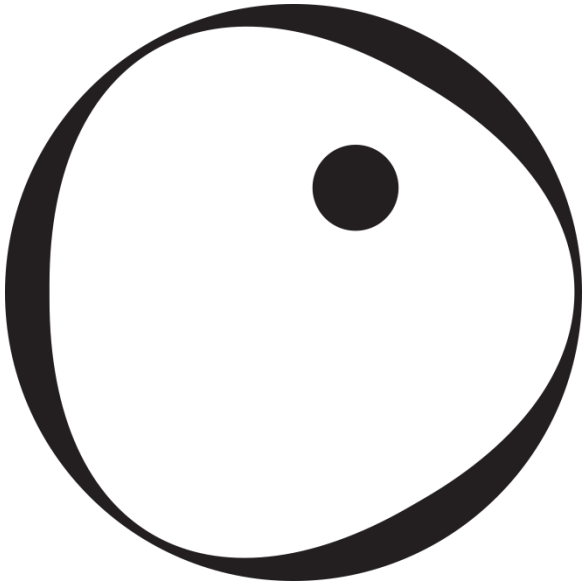
uta WG (After IETF88)

- Using TLS in Applications
- App Area New WG!
  - TLSを使用するための定義や仕様を更新して相互接続性を向上
  - 推奨されるTLSのバージョンや暗号スイート、暗号モード、拡張機能等のTLSクライアントとサーバのためのベストプラクティスを策定
  - SMTP, POP, IMAP, XMPP, そしてHTTP 1.1を代表的なアプリケーション上でTLSを使用するための定義を最新版に更新
  - クライアント/サーバ通信に加え、サーバ間のプロキシとの通信、ピアの適切な選択等も
  - TLS, DANEを始めとしたWGと連携

Conclusion

- Web/HTTPを中心に、App/RAI関係は一気に暗号通信の話に飲み込まれている感があります
  - CRIME Attack問題の辺りから、若干そういう空気はあったものの、やはりPRISMの影響は非常に大きいです
  - S/MIMEやSMTPという単語をこれほど聞いたIETFは始めて
  - TLSについての話題も非常に多かったように思います
- QUICのような時代背景にあわせた変革や、End to End暗号化の文脈を契機に、既存の仕組みに対する「やり直し」のチャンス？(その是非はさておき)
- Web/HTTP関連の話題は増える一方です
  - HTTP関連のWGを中心に軽くご紹介しましたが、他にも色々あって正直カバーしきれていません
  - もっと参加者や専門家が増えて欲しい
  - 皆様も是非！

Any Questions? / Please Feedback!



lepidum

https://lepidum.co.jp/

mailto:hayashi@lepidum.co.jp / twitter: @lef