IETF88th Technical Plenary

PKI DAY 2014

IETFでのTLS関連の標準化動向

SATORU KANNO

MARCH 13, 2014

自己紹介

- **名前**
  - 菅野 哲（かんの さとる）
- **所属**
  - NTTソフトウェア 株式会社
- **その他の所属**
  - IPA（非常勤研究員）
  - ISOC Japan Chapter（Program Committee）
  - MIT-KIT Japan Chapter（窓口？）
- **主な活動**
  - 暗号技術に関係する色々なお仕事に従事（標準化～開発）
    - ✓ Camellia標準化＆OSSなど

本講演の目的

- **本講演のモチベーション**
  - IETFで起きている大きな動向を知ってほしい
  - 興味を持ってもらえたら嬉しい♪

- **対象は？**
  - IETFにおけるTLSに関する動向
    - ✓ TLS WG
    - ✓ CFRG
  - IETFにおける暗号技術に関する動向
    - ✓ Pervasive Surveillance対策
    - ✓ 新しい暗号技術に関する検討
    - ✓ IETFにおける暗号技術に関する動向
  - IETFにおけるPKI関連の動向

用語の準備(1/2)

知っておくと理解が深まるかもしれない？

- **Opportunistic Encryption**
  - 認証なしに**暗号通信**をおっ始める仕組み
  - IETFとして**未定義**なんだけれども言葉は一人歩き中！
  - Unauthenticated Encryptionと同一視されることもある
    - ✓ モチロンMITMには弱い！

- **Pervasive Surveillance**
  - 潤沢なリソースを持った組織が行う広範囲な**盗聴行為**
    - ✓ 某国の某組織
  - ✓ 最近のIETFでは，監視に対する技術が多く提案されている

- **(Perfect)Forward Secrecy**
  - 秘密鍵を使い捨てして解読される影響範囲を限定する仕組み
  - 用語としてはラフな定義もない？！
    - ✓ E.g., Ephemeral Diffie-Hellman

用語の準備(2/2)

知っておくと理解が深まるかもしれない？

- **WebPKI**
  - 雑に言うと，SSL/TLSで利用されるPKI関連技術
    - ✓ Certificate Pinning, Certificate Transparencyなど
- **SSL/TLSへの攻撃**
  - **BEAST, CRIME, TIME, Lucky Thirteenなど**
    - ✓ CBC
    - ✓ 通信で利用される圧縮方式
  - RC4への攻撃

IETFにおけるTLSに関する動向

IETFのTLSってどこで議論されてるの？

- **IETF TLS WGで議論されてる**
  - 1996年5月から存在しているWG
    - ✓ PKIX: 1995年10月開始
  - 粘り強くre-charterを繰り返し現在に至る
    - ✓ CBCの改修，RC4撤廃，（D）TLS1.3検討

- **WGの参加者たちの好物は？**
  - Pervasive Surveillance対策技術
  - TLS 1.3
  - Non-NIST approved algorithmの選択肢
  - Best Current Practice

SSL/TLSを雑におさらい

- **SSL/TLSって？**
  - Transport層での暗号通信路を実現する通信プロトコル
  - XXX over TLS とかでも利用

現状のSSL/TLSのおさらい

- **証明書関連**
  - クロス証明書関係でアカン時もある
    - 現在もMD2を利用したRoot証明書も現役
- **鍵関連**
  - 鍵生成で利用する素数がアカンパターン
    - ✓ Debianの擬似乱数生成
  - RSAの鍵交換（PKCS#1 v1.5という事実）
    - ✓ 既知の攻撃が存在
  - Forward Secrecyを実現するEphemeral な鍵交換でも・・・
    - ✓ 実装によっては1024bitな時が…
- **プロトコルの脆弱性**
  - SSL2.0というレガシーが使えてしまう状況
- **暗号技術の危殆化**
  - RC4

IETF TLS WG

- **TLS WGとは・・・**
  - **TLS／DTLSに関する維持管理や仕様拡張**

- **ここ最近のTLS WGは・・・**
  - 100人程度参加で大盛況！
  - TLS1.3 や ストリーム暗号の検討が盛ん

大どんでん返しが発生・・・

TLS BCP

- **何を検討するの？**
  - SSL/TLSへの攻撃の対処法や関連する仕様について複雑すぐる
    - ✓ 実装者が混乱してしまうのでBCPをまとめちゃおうというモチベ
- **いつから検討されてる？**
  - IETF88
- **どんなところを気にしながら検討が進んでる？**
  - 実装するCiphersuiteの数を絞りたい
    - ✓ 現在，Ciphersuiteが320個の定義済み
  - 利用する鍵交換アルゴリズム
    - ✓ PFSが必須か？
  - 暗号利用モード
    - ✓ AEAD
  - そもそものTLSのプロトコルバージョン
    - ✓ TLS1.2が推奨になりそう

TLS: BCP TLS(1/2)

Motivation

- Provide clear guidance to confused TLS implementers
  - Several outstanding vulnerabilities
  - Some require app-level mitigations
  - Conflicts: move av
    RC4?!
- Pervasive passive monitor
  important, motivation
- The BCP is based on exist
  current or near-future impl
  - Absolutely no new
    creativity to TLS 1
  - Which will obsolet

Suite数は320程度と膨大！

Approach

- A single ciphersuite (or a very small number of them), that:
  - A client should propose, along with its other ciphersuites
  - A server should accept, unless a stronger one is offered
- Plus a few more recommendations
  - 2048-bit RSA certificates
  - Disable fallback to SSLv3
  - Disable TLS-level compression
  - Possibly a word on session resumption

3

IETF88 TLS WG発表資料より

TLS: BCP TLS(2/2)

DH/ECDHEのEはEphemeralのE！

DHE vs. ECDHE

- Modular Diffie-Hellman widely available, much more than Elliptic Curve DH
- However:
  - 1024 DH is considered insecure, important client implementations will fail the handshake if presented with >1024 DH
  - We only have crypto agility with ECDH (negotiated curves)
- Recommendations, in priority order:
  - ECDH: Brainpool with a fallback to P-256 (expect P-256 to be the prevalent curve in use for a while)
  - Ephemeral DH-2048: TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
  - Ephemeral DH-1024

Non-NIST Approved !!

Current Practiceというより Future Practice…

TLS 1.3

- **いつから？**
  - IETF87からIETF89で議論（継続中）
  - ML上でも活発

- **どんなところを気にしている？（IETF89ではどんな感じに？）**
  - ハンドシェイクフロー
    - ✓ たたき台のI-Dが投稿！
    - ✓ New Handshake Flows for TLS 1.3
    - ✓ http://datatracker.ietf.org/doc/draft-rescorla-tls13-new-flows/
  - Ciphersuiteはどうする？
    - ✓ GCMのだけにしちゃおうぜ！
  - 圧縮はどうする？
    - ✓ 無効化しちゃおうぜ！
  - 鍵交換アルゴリズム
    - ✓ PFS な鍵交換

議論は始まったばかりなのでチャンスあり！

Non-NIST approved algorithm

- **なんで注目されてるの？**
  - アレな出来事が要因…
    - ✓ 例：Dual_EC_DRBG
    - ✓ （NISTは頑張ってるので悪者しないで…
- **んじゃ，どんなアルゴリズムがあるの？**
  - 共通鍵暗号: Camellia（おい
  - ストリーム暗号： Salsa20 or ChaCha20
  - Elliptic Curve: Brainpool, Curve25519, BN?

厳選された選択肢を増やすのは好ましい！

TLS: STREAM CIPHER(1/4)

- **SSL/TLSにはRC4というストリーム暗号がある**
- **何故だかIETFの人たちはストリーム暗号が大好き♡**

参考情報：1秒あたりのスループット

某アルゴリズムより4倍程度高速！

Algorisms	16 bytes	64 bytes	256 bytes	1024 bytes	8192 bytes
RC4	515377.40k	639651.63k	686025.38k	704258.05k	711376.90k
Camellia128	121727.59k	154398.87k	166057.22k	169401.34k	170527.40k

※ 菅野PCで測定

でもね・・・

今は…モノ凄く弱いんです… orz…

TLS: STREAM CIPHER(2/4)

- **RC4の後継ストリーム暗号 ChaCha20**
  - Salsa20の亜種でDan J. Bernstein により設計
  - Poly1305と組合せてAEADを構成

WG itemに採用

Performance

Intel Xeon E5-2690@2.9GHz with Hyper-Threading and Turbo Boost disabled

AES-128-GCM, AES-NI disabled	131 MB/s
AES-128-GCM, AES-NI enabled	892 MB/s
ChaCha20+Poly1305	427 MB/s
ChaCha20+Poly1305, -march=native	560 MB/s

ARM Cortex-A9@1.2GHz

AES-128-GCM	25 MB/s
ChaCha20+Poly1305	92 MB/s

TLS: STREAM CIPHER(3/4)

- **IETF89・・・**
  - IETF88でWG itemに選択！からの評価依頼
    - ⇒ IETF88ではノリノリだったのに一転・・・

参加者からの声
- ✓ そもそもストリーム暗号いるの？
- ✓ DTLSでストリーム暗号使えなくない？
- ✓ CTRモードでOKじゃね？

⇒ ちゃぶ台をひっくり返し過ぎ！！

裏で誰かが暗躍してそうな雰囲気…

TLS: STREAM CIPHER(4/4)

- **そんな状況なのに・・・**
  - 例：google.co.jp

標準化されていないけど実装済み

Informational: 0xc0 から始まってるのでは・・・

https://www.ssllabs.com/ssltest/

唐突ですが・・・

Pervasive Surveillance

って気になっている人？

PRISMとは

- **2007年から運営されていた通信監視プログラム**
  - 2013年6月6日 ワシントンポスト等で報道

- **対象は？**
  - 9つのWebサービス
    - ✓ So.cl（Microsoft），Google，Yahoo，Facebook，Apple，AOL，Skype，YouTube，PalTalk

- **何を収集してたの？**
  - E-mail，文書，写真，利用記録などシビレる情報

Pervasive Surveillance対策

いくつか対策技術として存在している

- **(Perfect) Forward Secrecy**
  - Internet Infrastructure Review（IIR）Vol.22に記事！
  - http://www.iij.ad.jp/company/development/report/iir/022.html
- **Opportunistic Encryption (OE)**
  - 有名どころだとSTARTTLS
  - Client-to-Client, Client-to-ServerなOEがない？
- **Unauthenticated Encryption**
  - 認証せずにEndpointとの暗号化を実行

監視者のコストを増加させようというアプローチ

IETFで人気なTLSさん

- **DTLS In Constrained Environments (DICE)**
  - http://datatracker.ietf.org/wg/dice/charter/
- **Constrained RESTful Environments(CORE)**
  - http://datatracker.ietf.org/wg/core/charter/
- **Using TLS in Applications (UTA)**
  - http://datatracker.ietf.org/wg/uta/charter/

Applications Areaでの利用が活発化している！

DTLSを必要としている傾向がある

IETFにおける暗号技術に関する動向

CFRGにおける動向（TLSな文脈で）

- **Stream Cipher**
  - ChaCha20 + Poly1305
  - KCipher-2 (CRYPTREC的な意味で)

夢破れた感じ

- **暗号化関連**
  - Encrypt-then-MAC for TLS and DTLS
  - Authenticated Encryption with Replay prOtection (AERO)
    - ✓ https://datatracker.ietf.org/doc/draft-mcgrew-aero/

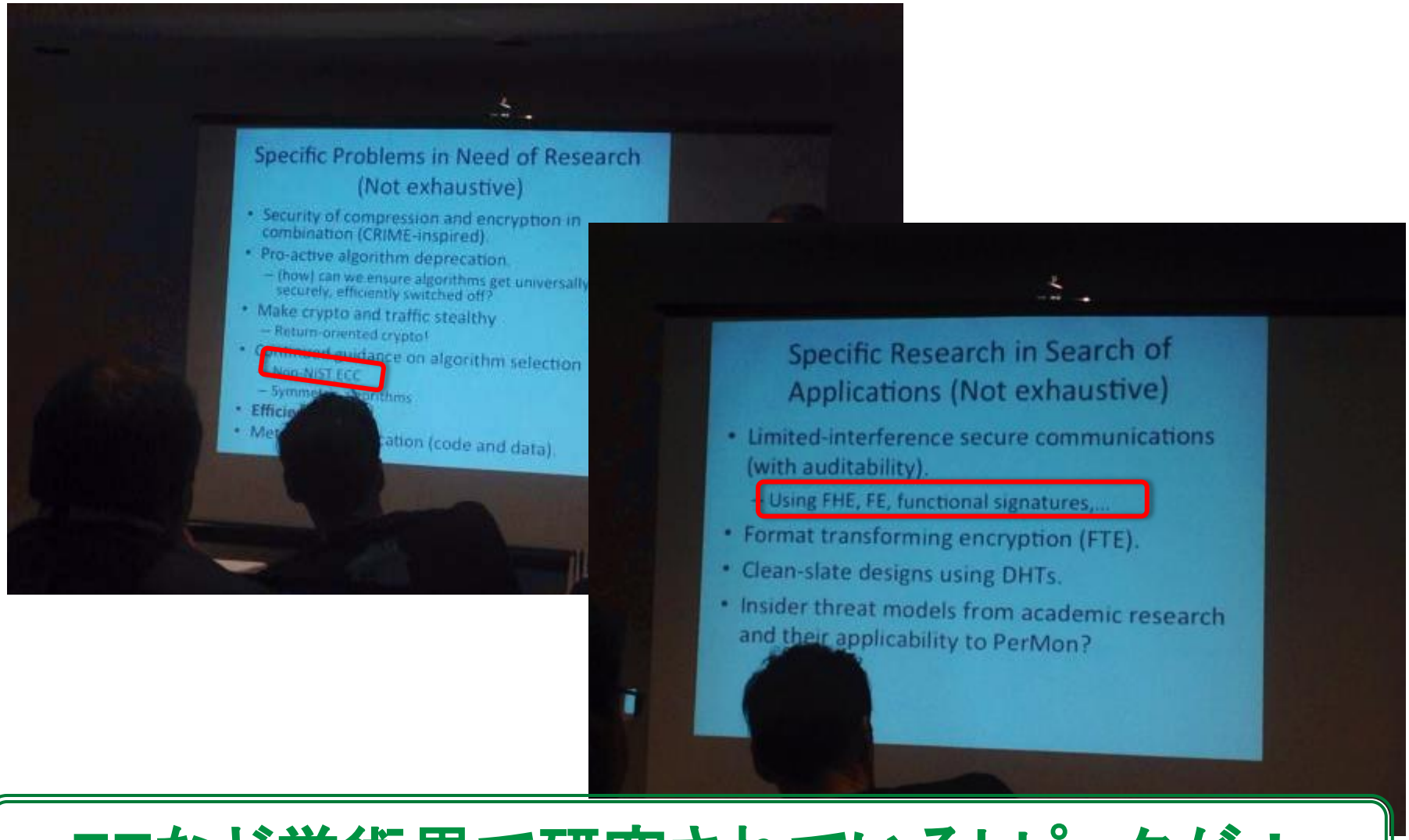
- **Safe Elliptic Curve**

UC Berkeleyの学生が提案

  - **Additional Elliptic Curves for IETF protocols**
    - ✓ https://datatracker.ietf.org/doc/draft-ladd-safecurves/
  - Non-NIST approved Curveを採用する動き

- **安全な鍵交換アルゴリズムの検討への動き**
  - IETF89前くらいからMLでアツイ議論
  - MQVの名前も…

CFRGにおける動向（IETF89）



FEなど学術界で研究されているトピックが！

IETFにおけるPKI関連の動向

IETFにおけるPKI relatedな動向

- **PKIX ➡ 終了**
- **Web PKI OPS (WPKOPS)**
  - https://datatracker.ietf.org/wg/wpkops/charter/
- **Web Security (WEBSEC)**
  - http://datatracker.ietf.org/wg/websec/charter/
- **Public Notary Transparency (TRANS)**
  - https://datatracker.ietf.org/wg/trans/charter/

IETFでPKI屋さんの出番ですよ！ ハヨ！

まとめ

- **IETFでのTLS関連の動向を共有**
  - みんなの興味はSurveillance対策
    - ✓ TLS WGでの動向
    - ✓ CFRGでの暗号技術に関する動向

- **IETFのような標準化団体でPKI屋さん不足**
  - WPKOPSやTRANSがあるのに・・・

CONTACT

- **E-mail**
  - kanno.satoru@po.ntts.co.jp
- **SNS**
  - Twitter (satorukanno)
  - Facebook (satoru.kanno)
  - Linkedin

お気軽にご連絡ください！(*'ω'*)