ISOC JAPAN CHAPTER IETF87 UPDATE MEETING SECURITY関連

—TLS WG, IRTF CFRG, 暗号技術の何か—

NTTソフトウェア株式会社
菅野 哲（かんの さとる）
kanno.satoru@po.ntts.co.jp

2013年9月5日

はじめに

- **IETF87 Security Areaでの動向から雰囲気を知ってもらいたい.**
  - Security Areaは怖くないです！
  - 少しでも興味を持ったら情報収集や活動をやってみてください！！

- **発表の流れ**
  - 自己紹介
    - この登壇者って誰よ？
  - おさらい
    - IETF Security Areaってどんなとこ？
  - IETF87 Security Area
    - どんな雰囲気だったの？
    - 今後注目しとけばいいことって何かしら？
      - TLS 1.3
      - ほとんどの人が気にしない暗号技術の動向
  - おまけ

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
  - たぶん9年目
- **主な活動**
  - 暗号技術関連のお仕事が中心
    - Camelliaという共通鍵暗号に関する標準化活動など
  - SNS
    - Twitter satorukanno
    - Facebook satoru.kanno
- **IETF初参加は？**
  - 72nd Dublin, Ireland

IETF SECURITY AREってどんなところ？

- **ミッション**
  - 意外性はなくセキュリティに関する技術を議論／検討
  - 有名なプロトコルだと…
    - TLS，IPsec
- **最近のSecurity Areaの大きな流れ**
  - 検討したプロトコルのメンテナンスなどがメイン
    - tls, ipsec, kitten etc.,
- **どのくらいのWGが存在するの？**
  - 13WG
    - 通信プロトコル，認証関連，関連する技術
    - http://datatracker.ietf.org/wg/
- Security Areaが関係あるWG等は？
  - CFRG（Crypt Forum Research Group）

IETF87 SECURITY AREAの雰囲気

IETF87 Security Areaとその周辺の大きな流れとしては・・・

PKIXが終了したので公開鍵暗号の話題が***減少***・・・
CBCやRC4関連等で*共通鍵暗号の話題* が***増加***！

JOSEでは暗号技術について活発に議論されているが・・・今回は割愛！！

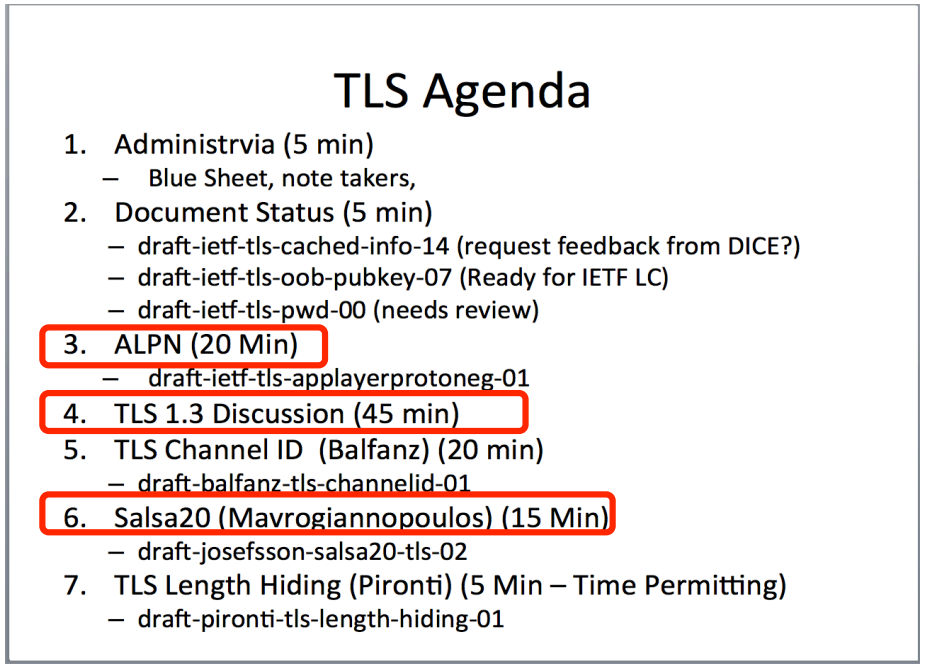
- **今回，取り上げるトピックスは・・・**
  - IETF Security Area
    - TLS WG
      - TLS 1.3に関連する話題
      - Stream Cipherに関する話題
  - IRTF CFRG
    - IETFでの暗号技術に関する動向
      - SM2
      - AESの代替アルゴリズムリスト
  - 上記以外で共有したい動向

TLS WG

- **TLSやDTLSに関する維持管理することが目的**
  - 最終日（金曜日）なのに**100人**程度の参加者

- **TLS WG Agenda**
  - TLS 1.3がメインの議題！
    - ALPNも含めれば***65分間***も議論…
  - Stream Cipherの追加に向けた提案
    - Salsa20

HTTP2.0なども関係している！
詳細は林さんが話すハズ！



TLS Agenda

1. Administrvia (5 min)
   - Blue Sheet, note takers,
2. Document Status (5 min)
   - draft-ietf-tls-cached-info-14 (request feedback from DICE?)
   - draft-ietf-tls-oob-pubkey-07 (Ready for IETF LC)
   - draft-ietf-tls-pwd-00 (needs review)
3. ALPN (20 Min)
   - draft-ietf-tls-applayerprotoneg-01
4. TLS 1.3 Discussion (45 min)
5. TLS Channel ID (Balfanz) (20 min)
   - draft-balfanz-tls-channelid-01
6. Salsa20 (Mavrogiannopoulos) (15 Min)
   - draft-josefsson-salsa20-tls-02
7. TLS Length Hiding (Pironti) (5 Min – Time Permitting)
   - draft-pironti-tls-length-hiding-01

TLS WG: TLS 1.3

- **結果： TLS 1.3をItemにするの？**
  - TLS1.3の標準化を行うことに**60人**程度の賛同あり
    - WGとして取り扱う議題になった！

TLS WGでの議論風景

TLS WG: TLS 1.3

ブラウザ等でTLS 1.2の実装が浸透してきたところで次の手を考えるのは良いタイミング！

- 注目すべきトッピックス

  主に既存のTLSで問題になっていることに対する解決策

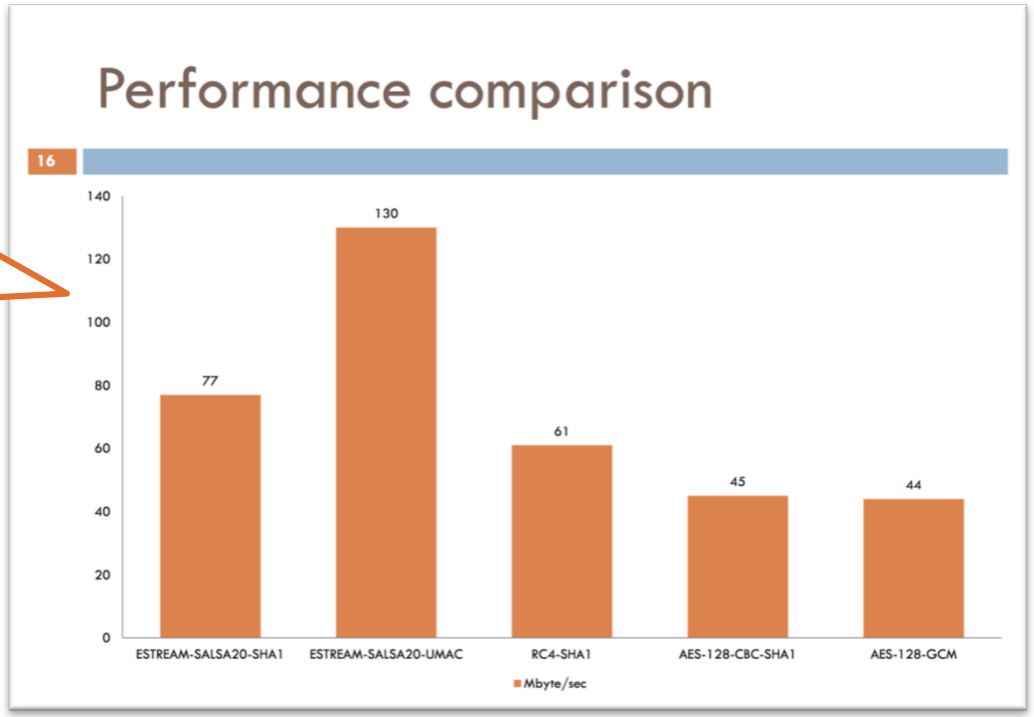
  - Handshakeでのネゴシエーション情報の保護を実現したい
    - Passive/Activeな攻撃者に対して情報保護
  - Cross-Protocol Attack Resistance を改善したい
    - ServerKeyExchangeでのデジタル署名がHandshake全体でないのが原因
      - A cross-protocol attack on the TLS protocol. ACM Conference on Computer and Communications Security 2012
        - Nikos Mavrogiannopoulos, Frederik Vercauteren, Vesselin Velichkov, Bart Preneel
  - CiphersuiteをAEADにする
    - CBCを捨ててAEAD（GCM，CCM？）に移行する
    - CFRGで標準化が進められているOCBモードが有力？！
  - Ciphersuiteの取り扱い
    - TLSのバージョンごとにSuiteを定義する
    - RC4やCBCに関するSuiteを削除する
    - 脆弱性が発見された際の代替アルゴリズムを用意する
    - MTIなCiphersuiteを追加する

TLS WG: SALSA20

- **RC4はお亡くなりになったし，AEADが使えるCiphersuiteってTLS1.2以降だよね？　TLSプロトコルへの攻撃だってあるじゃん？**
  - Stream Cipherが必要だよね！って感じでSalsa20が提案

- ***疑惑の性能比較*でSalsa20採用に向けた本質的な議論が未 orz…**
  - 次回以降のCFRGで…

・測定環境がない．．．
・どの実装で比較したの？
・この数値は妥当なの？



- **CRYPTREC暗号リストにも…**
  - **KCipher-2**がある！

TLS WG:参考情報

IETFの動きに関連する参考情報として．．．

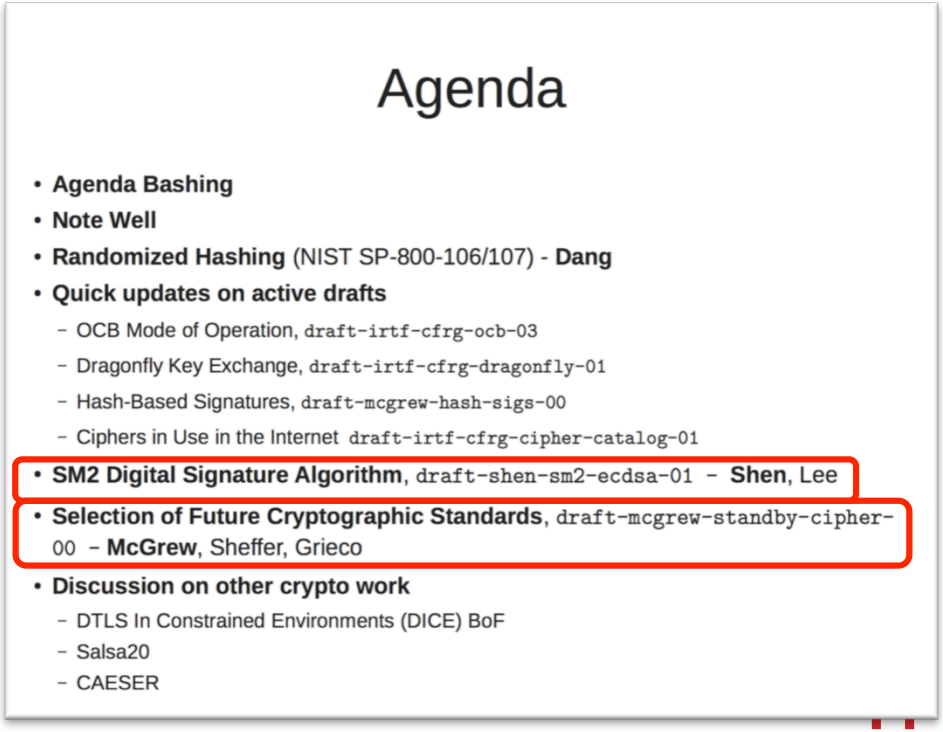
- **ALPN**
  - ALPNとは，TLSにおけるネゴシエーションに関する拡張
  - Googleが主導して色々な環境に実装
    - *.google.comのサーバでは実際に動作
    - OpenSSLにパッチ投稿済み
    - NSSにも投稿済み
      - Chrome Canaryでも動作可能
        - 送信するデータ量を削減するためにCiphersuiteを厳選
          - 利用可能なのはAES, RC4, 3DES

Camellia関連のSuiteが削除（＞＜

- **RC4の取り扱いに関する動向**
  - HTTP2.0方面でRC4を無効化しようぜ？という動きもあった！？
  - RC4ってダメじゃね？という声に応えてIETF87後にDraftが投稿
    - Prohibiting RC4 Cipher Suites
      - https://datatracker.ietf.org/doc/draft-popov-tls-prohibiting-rc4/?include_text=1
    - **TLSだけでRC4が使われているワケではない**
      - 例えば，Kerberos v5，SSHなどあるけど･･･どうするの？

CFRG

- **CFRGはネットワークやIETFで使用される暗号技術について議論および検討を行うリサーチグループ**
  - IETFで利用する暗号アルゴリズムが対象
- **今回のCFRGは全てのItemを議論できず尻切れとんぼ…**
  - 比較的時間を費やして議題を報告
    - SM2
    - Future Crypto Standards



Agenda

- **Agenda Bashing**
- **Note Well**
- **Randomized Hashing** (NIST SP-800-106/107) - **Dang**
- **Quick updates on active drafts**
  - OCB Mode of Operation, `draft-irtf-cfrg-ocb-03`
  - Dragonfly Key Exchange, `draft-irtf-cfrg-dragonfly-01`
  - Hash-Based Signatures, `draft-mcgrew-hash-sigs-00`
  - Ciphers in Use in the Internet `draft-irtf-cfrg-cipher-catalog-01`
- **SM2 Digital Signature Algorithm**, `draft-shen-sm2-ecdsa-01` – **Shen**, Lee
- **Selection of Future Cryptographic Standards**, `draft-mcgrew-standby-cipher-00` – **McGrew**, Sheffer, Grieco
- **Discussion on other crypto work**
  - DTLS In Constrained Environments (DICE) BoF
  - Salsa20
  - CAESER

CFRG: SM2 DIGITAL SIGNATURE ALGORITHM

そもそもSM2って何よ？

- **中国のデジタル署名アルゴリズム**
  - 中国で広く利用されているから標準化したいというモチベーション
  - Standard TrackでRFC化を目指す！
    - Informationalでね！と諭される

- **そもそもSM2って世界で評価されているの？**
  - 今まで中国語でしか情報がなかったけど英語ページを作成
  - 査読付き学会に採択された実績はないみたい
  - OIDなども存在していない…
  - でも，***中国国内での利用実績***は多いらしい！

やるべき課題は多そうだけど. . .

コミュニティへの貢献は大事！

発表者はSecurity Areaで***活発に活動***しているので
参加者たちの暖かい雰囲気で進行することができていた！

CFRG: SELECTION OF FUTURE CIPHER STANDARDS

- **現在，IETFで標準化されているセキュアプロトコルはAESに非常に依存している！**
  - AESに問題がないと信じる理由がない
    - AESの代替アルゴリズムリストが必要！！

- **AESの代替アルゴリズムに求められる評価基準（案）**

(AES) Evalutation Criteria

- Security
- Computational efficiency
- Memory requirements
- Hardware and software suitability
- Simplicity
- Flexibility
- Licensing requirements; it should be available worldwide on a royalty-free basis.

<u>個人的に思った問題点：</u>

・CFRGだけでは
マンパワーが不足する.

・誰もが納得する評価基準
としての線引きが難しい？

CFRG: その他

- **Dragonfly Key Exchange**
  - パスワードやパスフレーズを用いた離散対数ベースの鍵交換プロトコル
  - 様々なところに積極的に提案している
    - 例えば，IEEE 802.15.9
    - 気づくと・・・みなさんの活動エリアでも提案されるかも・・・
  - Draft
    - http://tools.ietf.org/html/draft-irtf-cfrg-dragonfly-01

これ以外で気になる動向（1/2）

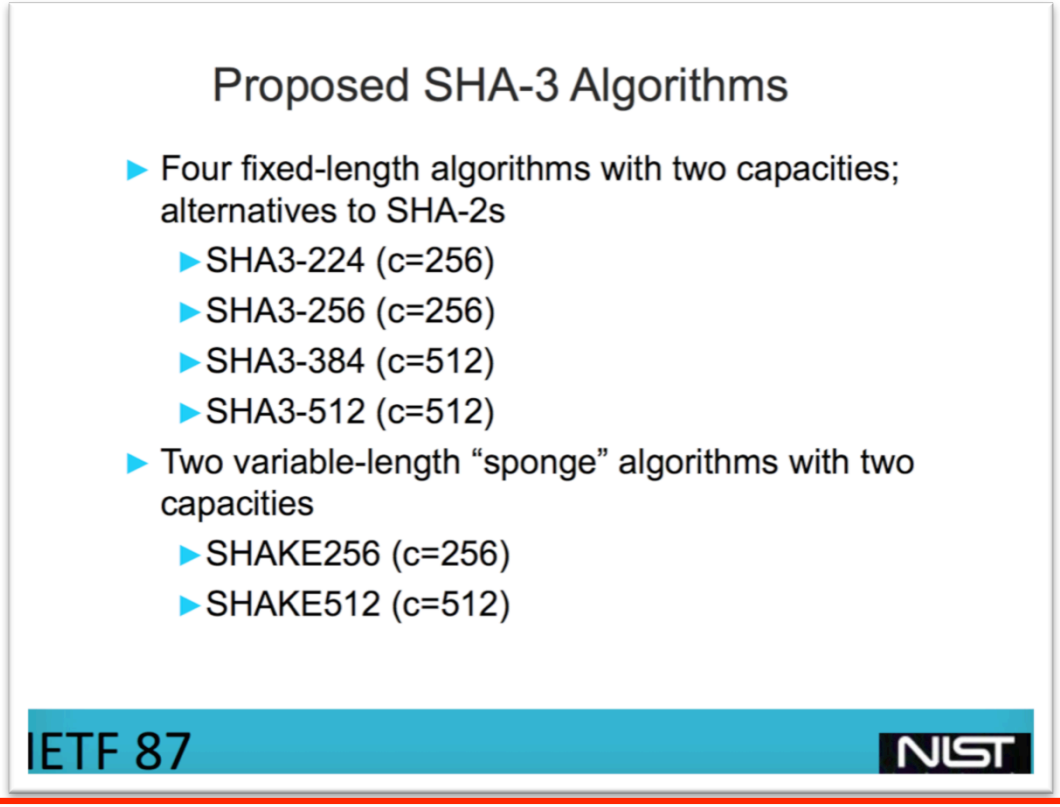
- **Elliptic Curve Cryptography（ECC）の標準化が活発化？！**
  - Brainpool Curveを利用したI-DやRFCが増加！
    - 例としては・・・
      - RFC 6954
      - Using the Elliptic Curve Cryptography (ECC) Brainpool Curves for the Internet Key Exchange Protocol Version 2 (IKEv2)

- **DTLSを利用しようという機運が高まっている？！**
  - M2Mなどの制約条件が厳しい環境下での利用ニーズの拡大？
  - BoF/WG
    - DTLS In Constrained Environments (DICE) BoF
    - Constrained RESTful Environments（CORE）
    - Light-Weight Implementation Guidance（LWIG）

- **DNSSEC/DANEと既存プロトコルの組合せ技！？**
  - SMTPやS/MIMEなどのメール関連技術と組合せて補完して，より安全性を高めようとする流れ

これ以外で気になる動向（2/2）

- **SHA-3の動向**
  - “FIPS 202 SHA-3 Permutation-Based Hash Standard”として発行される予定



SHA-3を利用して実現したい将来的なターゲット：
擬似乱数関数，ストリーム暗号，認証付き暗号など・・

IETF88に参加してはどうでしょうか？

IETF 88 - Vancouver, BC, Canada

November 3-8, 2013

Meeting Venue:
Hyatt Regency Vancouver
655 Burrard Street
Vancouver, BC, Canada V6C 2R7
Tel: +

IETF Meeting Registration System

Attendance List

IETF 88

Vancouver, BC, Canada

November 3-8, 2013

Last updated Tuesday, September 03, 2013 at 19:40:07 PDT

202 registrations:

現在，日本からの
登録者は8名！

http://www.ietf.org/meeting/88/index.html

でも･･･IETFの参加方法がわからんし･･･

ISOC JPにIETFの歩き方ってのがあるんです♪

IETF

IETFの歩き方

初心者の方がIETFとは？何かを知るために参考になるURLを記載しております。

Internet Week2012: T8 インターネットの決めごと（標準、ポリシー、慣習）の作り方を学ぼう

インターネットのプロトコルおよび技術規格策定団体およびそのプロセスの紹介　by 川島　正伸 (NECアクセステクニカ株式会社)さん

IETF TAO

IETFでは初心者の為にTAO（心得）を作成しています。以前はRFC4677の様にそれ自身をRFCにしていましたが、RFC6722によりWebページにて公表する様になりました。

- 現在TAOは英語のみではなく各国語で翻訳されています。
- 日本語のページはこちら

Copyright (C) 2002-2010 ISOC Japan Chapter

Powered by FreeStyleWiki3.6.4 with Perl5.014002

http://www.isoc.jp/wiki.cgi?page=IETF

要望などはアンケートに書いてもらえると助かります！

おわり