IETF88th Technical Plenary

IETF88 SECURITY AREA

SATORU KANNO, NTT SOFTWARE

DECEMBER 20, 2013

自己紹介

- **名前**
  - 菅野 哲（かんの さとる）
- **所属**
  - NTTソフトウェア
- **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
    - ✓ 世の中的にはCamellia標準化＆OSS

いきなりですが・・・

PRISM

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盛りだくさん

IETF88の率直な感想

- **一言で言うと・・・すごく暗号技術に注目がッ！**
  - 個人的にはテンション上がった！（おい
    - ✓ 肋骨を折ったし…
  - 他エリアでも暗号祭り！！
    - ✓ Application Area（◯◯ over TLS）

今回の報告

- **IETF88 Security Area Updateということで・・・**
  - Security Areaって？
  - Security AreaのWG動向
    - ✓ TLS WG
      - TLS BCP
      - TLS 1.3
      - New Stream cipher
    - ✓ SAAG
      - NIST Cryptography Standards Process Review
  - 暗号技術に注目した動向
    - ✓ 暗号アルゴリズムの見直す兆し

SECURITY AREA

- **Security Areaとは**
  - ビルディングブロックとしてのセキュアプロトコルを検討
    - ✓ TLS, IPsec, OAUTH, JOSEなど
  - 13WG+SAAG
    - ✓ PKIXが終了
- **Securityの関係があるWGs/RGs**
  - WGs: WEBSEC, HTTPBIS, PRECISE,WPKOPS
  - RGs: CFRG
- **IETF88における Security Area の活動状況**
  - 9WG, 1BoF, SAAG

IETF SECURITY AREでの流行語？

知ってたら参加者を気分！（おい

- **End-to-End Encryption**
  - 発信元−受信先で暗号化をして**中間からの覗きを防止**
- **Opportunistic Encryption**
  - 認証なしに**セキュアチャネル**を設定しちゃう行為
    - ✓ モチロンMITMには弱い！
  - みんなのココロの中に定義がある状態
- **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**
    - ✓ ◯SAとかN◯AとかNS◯
- **（Perfect）Forward Secrecy**
  - 雑に言うと…もし秘密鍵がバレても影響範囲を最小化できる
  - TLSでいうEphemeral Diffie-Hellmanなど

TLS

- **TLS WGとは・・・**
  - **TLS／DTLSに関する維持管理や仕様拡張**
- **今回のTLS WGは？**
  - 2013年11月5日16:10-18:40
  - 130人程度参加で大盛況！

TLS

Agenda

1. Administrvia (5 min) - Blue Sheets, Note Takers, etc.
2. Document Status and TLS related work (10 Min)
   DICE, HTTPbis & ALPN, Apps Area TLS BCP
3. ALPN (15 Min) - draft-ietf-tls-applayerprotoneg
4. TLS BCP (15 min) - draft-sheffer-tls-bcp
5. Updating Cipher Model (20 min)
   draft-gutmann-tls-encrypt-then-mac and AEAD
6. Stream Ciphers (20 min)
   ChaCHa - draft-agl-tls-chacha20poly1305
7. Hardware Considerations for TLS Key Generation (5 Min)
8. TLS 1.3 (60 min)

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

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

5

Non-NIST Approved !!

PFSを満たす鍵交換を推進！NIST以外の選択

TLS: STREAM CIPHER(1/3)

- **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(2/3)

- **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(3/3)

- **今のChaCha20って？**
  - 例：google.co.jp

標準化されていないけど実装済み

Informational: 0xc0 から始まる規則

（省略）

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

TLS: TLS 1.3(1/2)

- **徐々にTLS1.3の検討が立ち上がる**

Rough time allocation

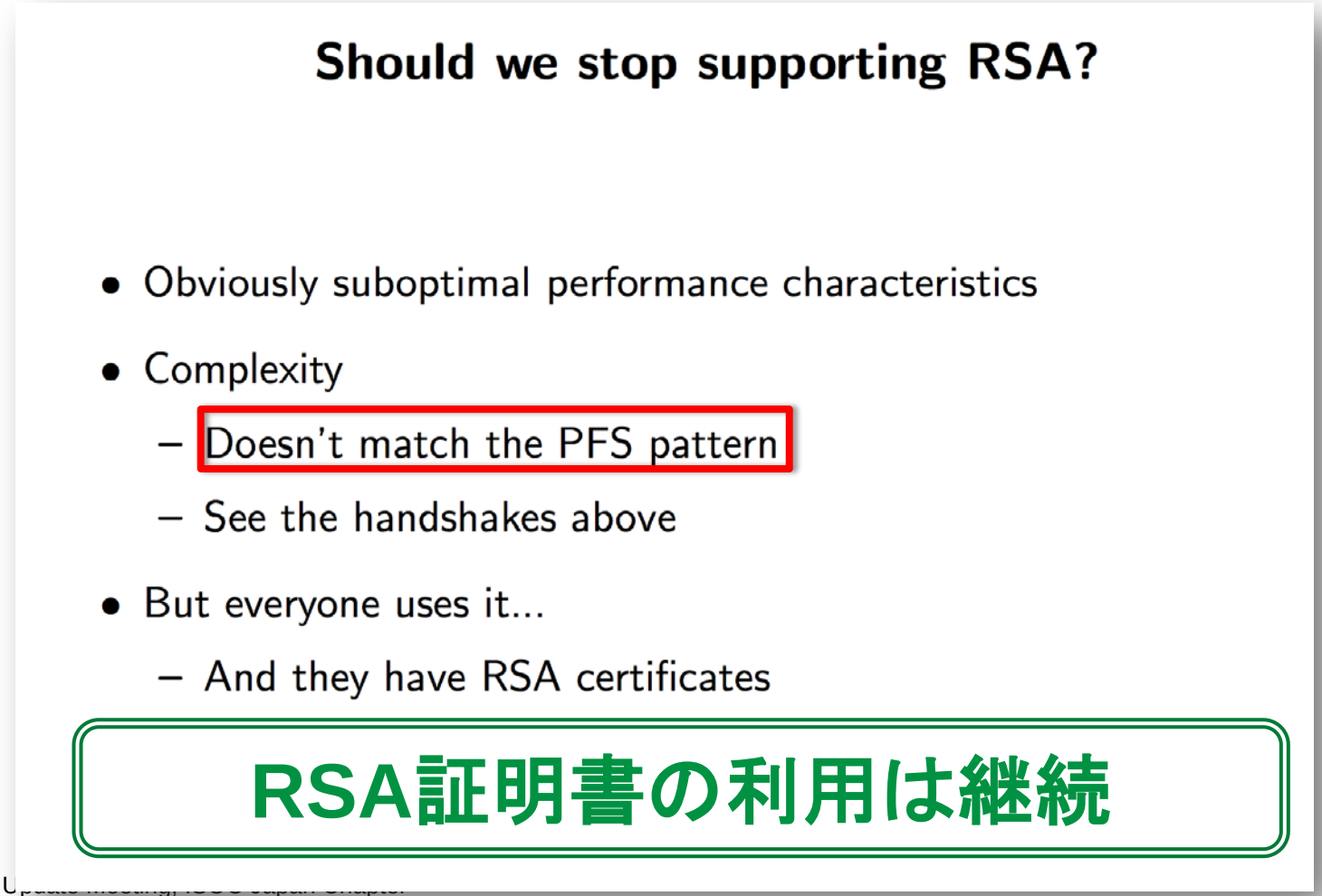
Time	Topic
30	New handshake flows
7	Should we allow renegotiation
7	Should we stop supporting RSA?
7	Should we get rid of resumption?
7	Random sizes
2	Other?

Handshake flowコンペの動きも…

やりたいことや課題を洗い出し中

TLS: TLS 1.3(2/2)

- **疑惑のRSAのサポート止めちゃう？話**
  - TLSからRSAを排除するのか？と勘違いされた



SAAG

- **SAAGとは・・・**
  - Security Areaの全体会合
  - Invited Talkで情報交換や情報共有

SAAG

agenda

- Security Area WG Reports, <10 mins
- Security Related BOFs, 3 mins
- Other Security-Related WGs, 7 mins
- Invited Presentation
  - NIST crypto standards process update – Tim Polk, 15 mins
  - Session Security Envelope – Bob Moskowitz, 15 mins
  - Protecting Encapsulation with Encryptin – Dino and Roger, 15 mins
  - Opportunistic encryption: then and now – Paul Wouters, 15 mins
- Time for perpass-overflow stuff (if need be)
- Open Mike

一連のNSAに起因する話題…

SAAG: NIST CRYPTOGRAPHY STANDARDS PROCESS REVIEW

使用中止

- SP800-90A: Dual_EC_DRBGにバックドア！？
  - 標準化した要員にNSAの人が…

Process Review & Update

- Document and publish NIST process
- Invite public comment on NIST process
- Independent evaluation to review the process ands to suggest improvements
- NIST will update process as necessary to:
  - Maximize openness and transparency
  - Support the development of the most secure, trustworthy guidance practicable

NISTの仕様策定プロセスの透明化！

IETFでの暗号技術に関する予想

- **既存技術の見直し**
  - レガシーな暗号技術の移行促進
    - ✓ RSA PKCS#1 v1.5は**安全ではない**けど…
- **Pervasive Surveillance対策に注力！**
  - 暗号技術利用に関する見直し
    - ✓ Perfect Forward Secrecy (PFS)
    - ✓ Opportunistic Encryption
- **新しい暗号プリミティブの発生**
  - Privacy Protection Protocol ?
  - Pairing Based Cryptography ?

IETF89

- **Date**
  - March 2 - 7, 2014
- **Location**
  - London, England
- **URL**
  - http://www.ietf.org/meeting/89/index.html

IETF Meeting Registration System

Attendance List

IETF 89

London, England

March 2-7, 2014

Last updated Tuesday, December 10, 2013 at 20:06:37 PST

116 Registrations
0 On Site

問合せ先

- **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'*)

参考情報

- **IETF88**
  - http://www.ietf.org/meeting/88/
- **IETF88 Agenda**
  - https://datatracker.ietf.org/meeting/88/agenda.html
- **IETF88 Meeting Material**
  - https://datatracker.ietf.org/meeting/88/materials.html#sec

BEER TALKの宣伝？！

今回のIETFで話題になった

アレな話題は…

Beer Talkで取り扱われr