IETF92 Update
Security Area
- 暗号技術を中心に -

2015年4月24日

菅野　哲（かんの　さとる）

この登壇者は何者・・・？

- **名前**
  - 菅野 哲（かんの さとる）
- **所属**
  - PKI48
    - 初代センター

- **その他の所属**
  - ISOC Japan Chapter（Program Committee）
  - MIT-KIT Japan Chapter
  - NTTソフトウェア

今回の話題は･･･

暗号技術に関連する動向

なぜ暗号技術の話を取り上げるのか？

IETF88において

Pervasive Surveillance

を大きく取り上げた

政府への不信感の高まり

PSの明確化！

暗号技術で対抗

IETF92での主な動きは・・・

楕円曲線の選定

TLSの利活用

CFRG

CFRG: RG Document Status

Document Status

- Approved for publication, in RFC Editor queue
  - draft-irtf-cfrg-chacha20-poly1305-10
- Sent to IRSG for review
  - draft-irtf-cfrg-dragonfly-06
- Accepted as CFRG draft
  - draft-irtf-cfrg-spake2-01
- Active, will be presented today
  - draft-irtf-cfrg-augpake-03: Augmented Password-Authenticated Key Exchange (AugPAKE)
- Expired, talking to editors
  - draft-irtf-cfrg-cipher-catalog-01: Ciphers in Use in the Internet
- Related work/possible work item
  - draft-hoffman-rfc6090bis-00: Fundamental Elliptic Curve Cryptography Algorithms

RFCが発行間近！！

CFRG: Agenda

```
WEDNESDAY, March 25, 2015. 13:00-15:00 CDT (2 hours)


Document status from Chairs                                  -  5 mins

Elliptic Curves for Security: draft-irtf-cfrg-curves-01
(Adam Langley)                                               - 10 mins

Elliptic Curves: next steps and discussions (chairs)         - 35 mins
-------------------------------------------------------------------

Scrypt [draft-josefsson-scrypt-kdf-02] (
-------------------------------------

Algebraic Eraser (Paul Gunnells)
-------------------------------------------------------------------

Hash-based Signatures [draft-xmss-00]
Andreas Huelsing                                             - 20 mins
-------------------------------------------------------------------

PAKE requirements document status (Dan Harkins)              -  5 mins

Augmented Password-Authenticated Key Exchange (AugPAKE):
draft-irtf-cfrg-augpake-03 (SeongHan Shin)                   - 15 mins

SIP Authentication using the EC-SRP5 Protocol:
draft-liu-sipcore-ec-srp-00 (Dr. Fuwen Liu)                  - 15 mins
```

ずっと議論していた
楕円曲線問題に決着ッ！？

CFRG: Elliptic Curves 関連（1/2）

Where we are – 1

- We have selected two curves
  - Curve25519 – already deployed in several places.
  - Goldilocks – offers good performance-security trade-off at higher security level (approx 224 bits).
- These curves (and I
  a deterministic pro
  input a prime *p* for
- http://www.ietf.or
  cfrg-curves-02.txt

定番なCurve25519と・・・

Curve448！

Where we are – 3

- We have submitted a short proposal to the NIST workshop as IETF/IRTF input.
- We have liaised with W3C.

選択結果を様々な組織に展開へ

CFRG: Elliptic Curves 関連（2/2）

Where we are going next – 2

- Some signature options (illustrative, not definitive):
  - ECDSA on the (twisted) Edwards form versions of the new curves.
    - Is that compliant with NI
    - Does that matter?
  - De-randomised ECDSA.
    - Avoids common failure r
    - Generate *r* for ECDSA by key.
    - OR generate *r* via PRF on augment ECDSA private

Where we are going next – 3

- Some signature options (illustrative, not definitive):
  - EdDSA [BDLSY'11]
    - Variant of Schnorr signature scheme, rather than DSA.
    - Uses derandomisation trick and a different verification equation.
    - Already deployed in OpenSSH.

鍵交換の次は署名に着手？！

楕円曲線がとことん好き♡ という方に朗報！

◆ 第92回IETF報告［第2弾］IETFにおける暗号技術に関する動向(楕円曲線)

NTTソフトウェア株式会社 菅野哲

第90回IETF報告(*1)において報告しました「Pervasive Surveillance（大規模な盗聴行為)」の対策として、暗号技術を用いたさまざまな提案がされました。今回の第92回IETFにおいても、最近の暗号技術に関する対策について検討が行われた、記念日的なIETF会合である第88回IETF(*2)から引き続き話題性があるようです。

本稿では、第92回IETFにおけるセキュリティ関連の報告のうち、セキュリティエリアでの技術的な動向に大きく影響すると予想されるIRTF（Internet Research Task Force)にある暗号のグループであるCFRG（Crypto Forum Research Group)で議論された「新しい楕円曲線の動向」について報告したいと思います。

(*1) https://www.nic.ad.jp/ja/mailmagazine/backnumber/2014/vol1225.html
(*2) https://www.nic.ad.jp/ja/mailmagazine/backnumber/2013/vol1152.html

https://www.nic.ad.jp/ja/mailmagazine/backnumber/2015/vol1299.html

UTA WG

UTA WG

- UTA（Using TLS in Applications）WGとは？
  - TLSプロトコルによりアプリケーションのプロトコルを保護する
  - **アプリケーションエリア**のWG

- **主に議論しているアイテムは・・・**
  - ***TLS Attacks and BCP***

UTA WG: Agenda

Agenda UTA IETF92

15:20 – 15:40: Note Well and status update

15:40 – 16:10: Deployable Enhanced Email Privacy (DEEP)

16:10 – 16:30: Open discussion

UTA WG: 主要Draftのステータス

- Summarizing Known Attacks on Transport Layer Security (TLS) and Datagram TLS (DTLS)
  - ***RFC 7457***として***2015年2月***に発行
- Recommendations for Secure Use of TLS and DTLS
  - ***RFC-EDITOR***のステータス

UTA WGの主なミッションが完了！

SAAG

SAAG: Agenda

agenda

1. WG/BoF Reports and administrivia (10 mins)
2. Status on PM
3. Invited/offered talks
    1. Joe Bonneau (30 mins)
    2. AGL/QUIC (15 mins)
    3. NSEC5, DNSSEC Authenticated Denial of Existence (10 mins)
    4. Darkmail (20 mins)
4. open-mic (40 mins)

https://www.ietf.org/proceedings/92/slides/slides-92-saag-0.pdf

SAAG: Pervasive Monitoring

Update on PM Drafts

- Lots of work is happening across many WGs related to PM, thank you all for your work!
  - IPsecMe, UTA, TLS,
- Drafts/RFCs specific to PM:
  - RFC7258 Pervassive Monitoring is an Attack, May 2014
  - Confidentiality in the Face of Pervasive Surveillance: A Threat Model and Problem Statement, draft-iab-privsec-confidentiality-threat
  - Effects of Ubiquitous Encryption, draft-mm-wg-effect-encrypt
    - Call for contributions/comments/text
- What to do next?

SAAG: Ubiquitous Encryption（Draft）

Network Working Group
Internet-Draft
Intended status: Informational
Expires: September 8, 2015

K. Moriarty
EMC Corporation
A. Morton
AT&T Labs
March 7, 201

Effect of Ubiquitous Encryption
draft-mm-wg-effect-encrypt-01

協力者
大募集中！

Abstract

Increased use of encryption will impact operations for security and network management causing a shift in how these functions are performed. In some cases, new methods to both monitor and protect data will evolve. In more drastic circumstances, the ability to monitor may be eliminated. This draft includes a collection of current security and network management functions that may be impacted by the shift to increased use of encryption. This draft does not attempt to solve these problems, but rather document the current state to assist in the development of alternate options to achieve the intended purpose of the documented practices.

http://www.ietf.org/id/draft-mm-wg-effect-encrypt-01.txt

TLS WG

TLS WG: Agenda

盛りだくさん！

殆どのitemを残してセッション終了！！

https://www.ietf.org/proceedings/92/slides/slides-92-tls-1.pdf

TLS WG: TLS MTI

Mandatory to Implement Cipher Suites

- Symmetric Ciphers

  MUST AES-GCM 128
  [SHOULD ChaCha20-Poly1305]*

- Hash

  MUST SHA-256

- Key Agreement

  MUST ECDH with P-256
  [SHOULD ECDH with 25519]*

- Signature

  MUST RSA
  MUST ECDSA with P-256

MTI != MTU

暗号な人的にはMTIに関する議論が知りたかった・・・

https://www.ietf.org/proceedings/92/slides/slides-92-tls-0.pdf

まとめ

- 新しい楕円曲線を選ぶぜ！問題に決着！
  - 今回のCFRGで確定されたTLSで使われるアレ
    - Curve25519とCurve448に確定
  - 他WGでの検討にも影響があるかも？
- Pervasive Surveillance関連の議論は継続中
  - Threat Model や Ubiquitous Encryption
- TLS 1.3のステータス
  - 一進一退の攻防を繰り広げている

- 個人的に感じた 今後の懸念・・・
  - いつまで続くの暗号通信ブーム？！
  - ちゃんと進むのかな？ TLS 1.3

連絡先

- **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！