NTTソフトウェア

IETF報告会（86thオーランド）

セキュリティエリア関連状況

2013.4.18

NTTソフトウェア株式会社

菅野　哲

発表の流れ

- 自己紹介
  - 菅野って誰よ？
- IETF セキュリティエリア
  - どんなことをやっているところなの？
  - 最近のセキュリティエリアの動向
- IETF 86 セキュリティエリアおよび関連
  - SEC: PKIX, IPSECME, SAAG
  - Related: CFRG, Alternative PKI model BoF?
- まとめ
  - IETFに参加して感じたこと
  - 呼びかけ

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
- 主な業務
  - 暗号技術の調査～標準化＆OSS化
    - 主にCamelliaを中心に
    - CRYPTREC
      - リストガイドWG

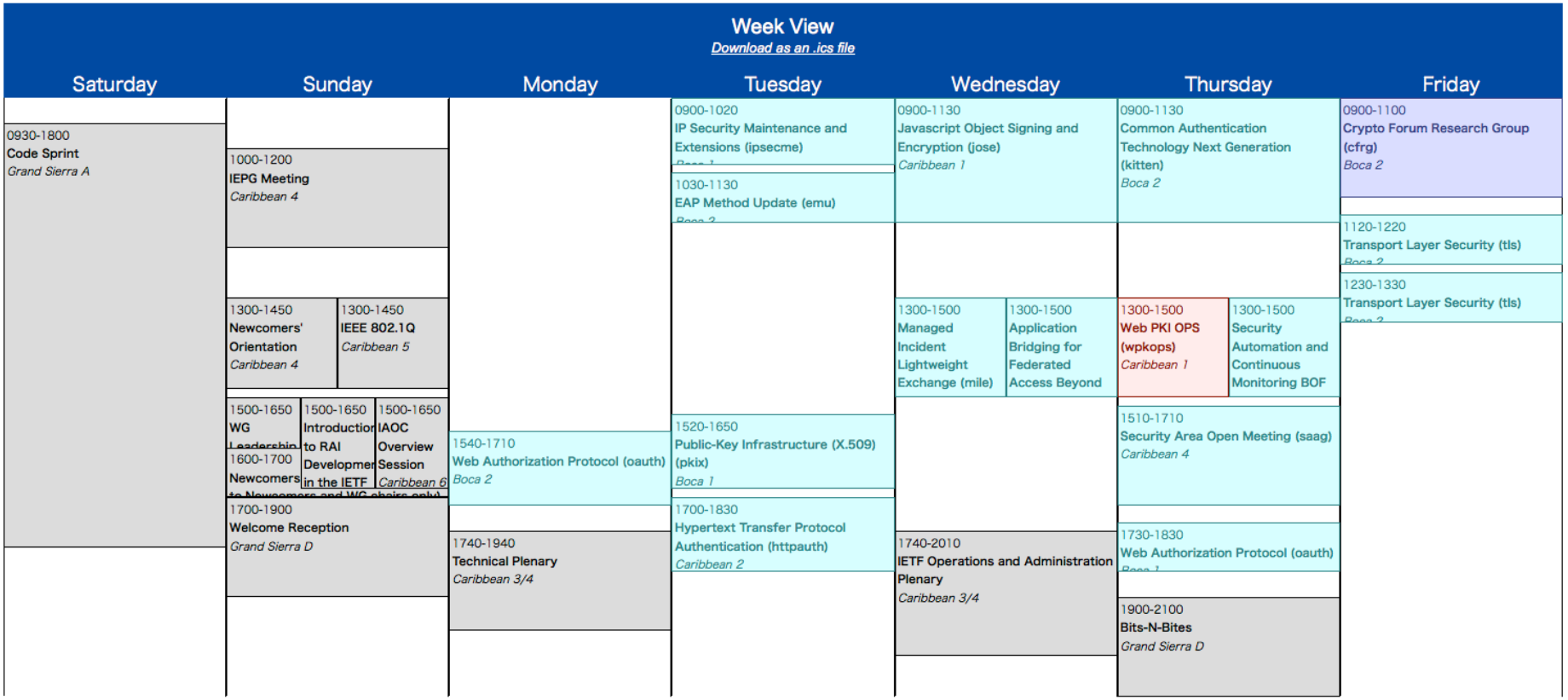
https://info.isl.ntt.co.jp/crypt/camellia/

IETF セキュリティエリアってどんなところ？

- ミッション
  - セキュリティに関する技術を議論／検討
    - 有名どころだと・・・
      - TLS, IPsec, SSH
- どのくらいWGがあるの？
  - 12WG
    - 新規: HTTPAUTH, 統合: KITTEN + KRB-WG => KITTEN
    - IETF85（12WG => 12 WG）
- 最近のSecurity Area内の動向
  - プロトコルのメンテナンスを行っているWGが多い
    - TLS, IPSECME, PKIX, …
- Security Areaが関係あるWG等は？
  - WEBSEC, HTTPBIS, KARP＆SIDR, PRECISE, WPKOPS
  - CFRG（Crypt Forum Research Group）

IETF86 セキュリティエリアWG

- セキュリティエリアWG スケジュール



IETF86: PKIX

- PKIX WGとは
  - インターネットでのPKI技術に関する仕様を検討
- 参加者数
  - 45名程度
- 注目ポイント！
  - IETF86のミーティングで終了という方向
    - 1995年に始まってから，ついに最終回か！？
      - WGを継続させるような大きな議題もなかった
    - 今後，議論したい時はWG MLを利用する

IETF86: PKIX

- IETF86 PKIXの議題は以下のとおり

PKIX Agenda for 86th IETF in Orlando

- Status and Direction
  - Document Status Overview, Stefan Santesson
  - Direction of the working group , Sean Turner
- WG documents
  - Enrollment over Secure Transport, Max Pritikin
- Related Specifications
  - Authentication Context Extension, Stefan Santesson

http://www.ietf.org/proceedings/86/slides/slides-86-pkix-0.pdf

IETF86: PKIX

- 今回のPKIXは？
  - IETF86までに発行されたRFC
    - RFC 6818
      - Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
    - RFC 6844
      - DNS Certification Authority Authorization (CAA) Resource Record
  - 今回の議題
    - Enrollment over Secure Transport
      - クライアント証明書などの証明書入手のためのプロトコル
      - http://tools.ietf.org/html/draft-pritikin-est-02/
    - Authentication Context Extension
      - SAMLを用いた認証連携時にユーザー証明書に付随する情報を伝達するための証明書拡張
      - http://aaa-sec.com/_temp/draft-santesson-auth-context-extension-04.txt

IETF86: IPSECME

- IETF86 IPSECMEの議題は以下のとおり

Today's agenda (1 of 2)

- **Auto Discovery VPN Problem Statement and Requirements** - draft-ietf-ipsecme-ad-vpn-problem - 15 mins
- **A TCP transport for the Internet Key Exchange** - draft-ietf-ipsecme-ike-tcp - 20 m
- **Additional Diffie-Hellman Tests for IKEv2** draft-ietf-ipsecme-dh-checks - 5 mins
- **Signature Authentication in IKEv2** - draft-kivinen-ipsecme-signature-auth - 10 mins

Today's agenda (2 of 2)

- **More Raw Public Keys for IKEv2** - draft-kivinen-ipsecme-oob-pubkey - 5 mins
- **Cryptographic Algorithm Implementation Requirements and Usage Guidance for ESP and AH** - Not-quite-submitted draft - 15 mins
- **Gateway discovery and addressing** - draft-mglt-ipsecme-security-gateway-discovery and draft-mglt-ipsecme-alternate-outer-address - 5 mins
- **Simple VPN solution using Multi-point Security Association** - draft-yamaya-ipsecme-mpsa - 5 mins
- *If time permits*: draft-gundavelli-ipsecme-3gpp-ims-options - 5 mins

http://www.ietf.org/proceedings/86/slides/slides-86-ipsecme-0.pdf

IETF86: IPSECME

- 個人的に気になった議題は・・・
  - Additional Diffie-Hellman Tests for IKEv2
    - http://tools.ietf.org/html/draft-ietf-ipsecme-dh-checks
    - DH鍵交換を使用する場合, Menezesの攻撃に対する対策するためにDH公開鍵の検証が必要
    - 論点:
      - 検証失敗時にどのように応答するかで議論
        - » 検証失敗のメッセージを送付 or 無視
        - » 引き続きCFRGでの議論へ
  - Signature Authentication in IKEv2
    - http://tools.ietf.org/html/draft-kivinen-ipsecme-signature-auth
    - IKEv2の署名方式の自由度を広げることを目的とし，ECDSAを実現する
    - 論点
      - ECDSAの利用に関する大きな反対もなく議論継続
      - ADからRSA-PSSをサポートすべきとコメントあり

IETF86: IPSECME

- Cryptographic Algorithm Implementation Requirements and Usage Guidance for ESP and AH
  - ESPおよびAHで使用される暗号アルゴリズムの要件および利用のためのガイドライン
  - 現在のDraftでの暗号アルゴリズムの推奨リスト（抜粋）
    - Authenticated Encryption
      - » AES-GCM（SHOUD+），AES-CCM（MAY）
    - Encryption Algorithm
      - » NULL（MUST），AES-128-CBC（MUST）[RFC3602]
      - » MAY AES-CTR（MAY），TripleDES-CBC（MAY）
      - » DES-CBC（ SHOULD NOT+ ）
  - 論点
    - アルゴリズムの多様性や安全性に関するSectionを追加
    - 5年毎に暗号アルゴリズムの安全性評価を行うかの議論
      - » 結論は出ず・・・

IETF86: SAAG

- Security Areaの全体会合

agenda

- WG Reports, <10 mins
- Security Related BOFs, 10 mins
- Invited Presentation
  - NIST SHA-3 Update - 15 minutes (Quynh Dang)
  - iSchedule/DKIM - 5 minutes (Cyrus Daboo)
  - SSH BCP - 15 minutes (Tatu Ylonen)
  - W3C Web Crypto API Update - 30 minutes (Ryan Sleevi)
- Open Mike

- 最近・・・ネタ不足感がある
  - RC4の話題が飛び入りで入ることを期待したが．．．

http://www.ietf.org/proceedings/86/slides/slides-86-saag-4.pdf

IETF86: SAAG

- 招待プレゼンの概要
  - NIST SHA-3 Update
    - NISTとしてSHA-3（Keccak）はSHA-2と共存
    - KeccakがWinnerになった理由
      - 高い安全性を実現
      - ハードウェア実装時に高性能
      - SHA-2とは異なる設計思想
  - iSchedule/DKIM
    - Internet Calendar Scheduling Protocol (iSchedule)を定義
    - カレンダー情報等は異なるドメイン間での情報交換が前提
      - ドメイン認証技術 => DKIM採用
    - APP Areaの識者からコメント
      - XMPP WGやJOSE WGを参考にしつつ，セキュリティ専門家のレビュが必須
    - Draft
      - https://datatracker.ietf.org/doc/draft-desruisseaux-ischedule/

IETF86: SAAG

- SSH BCP
  - SSH user keyやkerberosを用いた自動化アクセスに対する管理や監査の推奨されるポリシーの必要性を整理
    - セキュリティエリアで議論する必要があるのか？などの声も
  - Draft
    - https://datatracker.ietf.org/doc/draft-ylonen-sshkeybcp/

- W3C Web Crypto API Update
  - Web Crypto APIの背景や現在の進行状況等が報告
    - Web Crypto API:
      - » 主にブラウザ上で動作するJavaScriptアプリケーションで暗号化や復号，署名，検証，鍵交換等のためのAPI仕様

IETF86: CFRG

- CFRGとは？
  - 暗号技術に関する評価／議論を行う場
- IETF86 CFRGの議題は以下のとおり

Agenda

- JOSE Security Presentation by Jim Schaad
  - discussion
- Discussion on adoption of OCB draft
- Status of Crypt catalog draft
- Hash based signatures (David McGrew)
- Recent developments (Paul Hoffmann)

http://www.ietf.org/proceedings/86/slides/slides-86-cfrg-0.pdf

IETF86: CFRG

- 各議題の動向
  - JOSE Security
    - JOSE WGで暗号技術に関するサポートを受けるため
    - RSA-PSSをサポートすべきでは？というコメントあり
      - キーパーソンからWebアプリ等の現状を確認するとの回答
  - Discussion on adoption of OCB draft
    - 暗号利用モード Offset CodeBook (OCB)モードの仕様
    - MLでOCBに関する特許で盛り上がる
  - Status of Crypt catalog draft
    - IETFで利用される暗号アルゴリズムのカタログ
    - 特にコメントおよび議論なし
  - Hash based signatures
    - 量子コンピュータに対する安全性を持つ，Merkle木を利用した署名方式
    - Merkle木に対する効率的なメモリ管理の特許が存在するとコメント
  - Recent Developments
    - 不正なDH鍵の検証について，検証失敗時の返答に関する議論
    - IPSECMEからの継続した議論だったが結論は出なかった．．．

IETF86: CFRG

- 暗号技術の利用や新たな技術の流れを知りたい時に役立つかも？！

- 関連するI-Ds
  - お役立ち関連
    - Selection of Future Cryptographic Standards
      - AESの代替アルゴリズムどうしようか？
    - Crypto Catalog
  - 暗号技術
    - ZSS Short Signature Scheme
      - ペアリングを用いた暗号技術
    - Hash based signatures
    - OCB mode

Camelliaはどうだ？！

楕円曲線暗号関連が今後の柱に・・・？！

IETF86: Alternative PKI Model BoF?

- 形式
  - 非公式 BoF
- 目的
  - 現在のPKIは色々問題があり，新たなPKIのモデルや仕組みが必要なのでは？
- 興味深いテーマなのに…ちょっと残念
  - 参加者募集が86attendees ML
  - Bits-n-Bytesの裏番組
  - 事前に議題や資料公開もなし

IETF86: Alternative PKI Model BoF?

- 参加者数
  - 25人程度
- 論点など
  - 議論のターゲット
    - 産業的な側面および技術的な側面からのアプローチ
  - ユーザから見たCAの透明性
    - 証明書が正しいものかどうか判定しにくい
      - 不正な証明書の検知に役立つCertificate Transparencyのような仕組みが必要
  - CAと監査費用に関するコストモデル
    - ブラウザに格納されている証明書を発行しているCA
      - 毎年監査を受けるために高額な費用を出費
    - ユーザから支払われるセキュリティに対する対価が見合わない
      - 監査に対する負担とのバランスが難しい
    - 持続的なPKIを実現するにはコストモデルの再考が必須！
  - PKI関連のインシデント対応
    - 不正な証明書発行時におけるCAでのインシデント対応が不十分

参加して感じたこと

- IETF86は日本からの若手参加が増加？！
  - もしかして大学からの参戦があったから？
  - でも・・・セキュリティエリアじゃない・・・
    - セキュリティエリアにも若い息吹をッ
- 暗号技術に関する脅威には興味なし？
  - IETF開催期にRC4への攻撃が発表！
    - 話題としてキーワードが出る程度. . .
  - RC4はTLSなどで利用されておりインパクト大
    - RC4を利用しているプロトコルは多い => 対応必須では？
  - 事実としてGoogle, Facebookなどが通信で利用
    - 暗号通信中のCookieを復元されると厄介
  - 参考: RC4への攻撃
    - Full Plaintext Recovery Attack on Broadcast RC4
      - http://fse2013.spms.ntu.edu.sg/slides/Slides05_2.pdf
      - FSE2013において五十部-渡邉-大東-森井により発表
    - 概要
      - 同一の平文を異なる多数の暗号鍵で暗号化した場合，平文が復元できる攻撃

終わりに

- IETF86 セキュリティエリア関連状況として概要を報告
  - PKIX, SAAG, CFRG, Alternative PKI model BoF?

おまけ

- IETF 87はベルリンですよ！
  - http://www.ietf.org/meeting/87

IETF 87 - Berlin, Germany

July 28 - August 2, 2013

Meeting Venue:
InterContinental Berlin
Budapester Str. 2, 10787
Berlin, Germany
Tel: +49 30 26020

IETF Meetings start Monday morning and run through Friday afternoon (13:30), with late scheduling changes. Newcomers' training and technical tutorials take place the previous Sunday afternoon. Participants should plan their travel accordingly.

Please note that new information is being added to this page continually; please check back here for the most up-to-date information about IETF 87.

Any questions, comments are welcome!