標準化の一側面
-- IETFにおけるPKIの状況 --

富士ゼロックス株式会社
システム要素技術研究所
稲田 龍
<Ryu.Inada@fujixerox.co.jp>

概要

- RFC 5280 (RFC 3280の後継)が2008年5月に公開
  - PKIのインターネットでの利用のプロファイルが更新
  - PKIのインフラストラクチャとしての利用には決着がついたのか?
    - 新たな暗号・ハッシュアルゴリズムの利用は?
- そもそもPKIの応用はどうなっているの?
- IETFのSecurity Area全体としては、アルゴリズム独立が大きな問題となっている
  - 各WGがそれなりに対応を急いでいる……が、古いプロトコルほど問題を抱えている

IETFとは?

- Internet Engineering Task Force
  - インターネットで利用する各種プロトコルを標準化
  - The Internet Engineering Task Force (IETF) is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. It is open to any interested individual. The IETF Mission Statement is documented in RFC 3935.

  - http://www.ietf.org/overview.htmlの冒頭を抜粋(下線は筆者による追加)

PKIの基盤技術

- 主にSecurity Area PKIX-WGで議論
  - 基本は証明書/CRLのフォーマットの議論
    - RFC 5280により終了。
    - ただしECC/SHA-2系の暗号アルゴリズムの移行に関しては継続中。
  - PKIアプリケーションの利用に欠かせない基盤技術系の議論が行われている

応用技術

- PKIをどうプロトコルに応用するか?
- プロトコルの一部として利用するにはどうするのか?

- やはり暗号アルゴリズムの変更が大きな話題に……

PKIXでの主要な話題

- 証明書のフォーマット
  - RFC 5280としてRFC化
    - ECCを証明書で使えるようにするための検討が続いている
- 証明書の認証
  - OCSP v2
    - SHA-1からの脱却の検討が始まっている
  - SCVP
- 証明書の管理
  - TAM (Trust Anchor Management)
  - WebDAVでの管理
- アルゴリズム移行
  - 後ほどパネルでも話題に

PKIX

- RFC 3279bis/RFC 4055bis
  - ECC関連のアルゴリズムID/パラメータの設定に関してのI-D
  - RFC 3279bis
    - 多くの細かな修正が入っている
    - NISTのFIPS 180-3がRFC化のスケジュールに間に合いそうなく(NIST Tim Polk氏)、FIPS 180-2を参照することとなった
  - RFC 4055bis
    - 修正点は2箇所のみ、あとはTypo

PKIX - ASN.1 Update

- 70th よりWGアイテム

- I-D
  - Paul Hoffman氏とJim Schaad氏が作成
  - PKIX-WGがレビューを行なう

- 従来のモジュールの再利用可能･ASN-1コンパイラの利用が可能
  - OpenSSL/Crypt APIの様に直接暗号APIを用いるものは再利用できない。
- 通信路上を流れるデータには新旧で差異はない

- アクションアイテム
  - 市販、フリーのASN.1コンパイラで新モジュールが使えるかのテストが必要

PKIX - TAM

- 69th IETFでBoF開催
  - 新WGにせず、PKIX-WGで扱う

- 要件仕様
  - 管理対象、用語、TAに関連したデータにスコープを拡大
  - TrustAnchorInfo vs. ValidationPolicy
    - TrustAnchorInfoは、TA管理の主要なデータを保持
    - ValidationPolicyは、TA管理に必要な追加データを保持

PKIX - TAM

- Request/Reply Protocol vs. Directory
  - Microsoft Stefan Satesson氏の説明
  - Directoryを用いたTA管理のモデルの説明
    - X.500におけるトラディショナルな方式
    - Active Directoryなどで既に多く使われている
  - 要求仕様I-DはRequest/Reply Protocolを前提としているところが多い
    - 両モデルがあることを明記すべき
    - 両モデルの必要性を明記すべき

PKIX - PRQP

- 70th にてExperimental RFCとして扱うことが合意

- AIAなどの情報の伝播が可能
- OpenCAで実装済み

- PKIXの範疇を超えるがP2Pを使ったPEACHもある

PKIX – Wildcards in DNS Names

- Microsoft Stefan Satesson氏の提案

- いわゆるワイルドカード証明書の扱いについて
  - 主要なプラットフォームで動作する(IEでも動くようになった)
  - メジャーな認証局から取得可能
- 問題点
  - Name Constraintの問題
    - 通常の証明書と同様に扱う
  - IDNにおけるワイルドカードの扱い
    - ノーアイデア
- 提案内容
  - Informational RFC
  - 3280bisに修正

  ワイルドカード証明書を認める方向にすべき

- 意見多数
  - RFC 2818 (HTTP Over TLS)ではワイルドカード証明書をOKとしている(Tim Polk)
  - ブラウザがワイルドカードを含んだ名前の解釈に関してのInformational RFCを書くべき(Phillip Hallam-Baker)
  - RFC 3779（X.509 Extensions for IP Addresses and AS Identifiers）に従う(Steve Kent)

- MLでの議論

TLS

- TLS 1.2がほぼ固まった。
  - 新しい乱数発生器
  - 新しい暗号アルゴリズム(日本からはCameriaが提案されている)
- 安全性を考え、暗号の強度に関しての考察が始まっている
  - DESの禁止
  - この動きで証明書で提供する公開鍵の鍵長を制限する動きもある
    - 512 bit RSAの禁止の動き
- 脆弱性を考慮し、プロトコルのダウングレードを制限する動きもある
  - SSLv2は禁止にしたいという動きがあるが……

S/MIME

- 安全性を考え、暗号の強度に関しての考察が始まっている
  - DESの禁止
  - この動きで証明書で提供する公開鍵の鍵長を制限する動きもある
    - 512 bit RSAの禁止の動き
- IDB暗号の利用が話題に上がっている

LTANS

- 一段落が着きクローズ予定
  - 欧州にてサービスが開始

IPsec

- 主流はShared Secretでの運用
  - 証明書を利用したIPsecのプロファイルI-Dが期限切れのまま

ご清聴ありがとうございました

リファレンスなど

- IETF
  - http://www.ietf.otg/
- IETF Security Area
  - http://www.ietf.org/html.charters/wg-dir.html#Security%20Area
- PKIX-WG
  - http://www.ietf.org/html.charters/pkix-charter.html
- TLS-WG
  - http://www.ietf.org/html.charters/tls-charter.html
- S/MIME WG
  - http://www.ietf.org/html.charters/smime-charter.html
- IPsec WG
- LTANS WG
  - http://www.ietf.org/html.charters/ltans-charter.html

リファレンスなど

- IPA (情報処理推進機構 : 情報セキュリティ)
  - http://www.ipa.go.jp/security/index.html
- IPAのPKI関連技術情報
  - http://www.ipa.go.jp/security/pki/pki.html

- JNSA
  - http://www.jnsa.org/

商標権の表示

- Windowsは米国マイクロソフト社の登録商標です。