PKIの事故から学ぶDNSSECの必要性
～WebPKIの状況～

NTTソフトウェア株式会社
菅野 哲（かんの さとる）

2013年5月29日

はじめに

- 標準化活動を行っている情報セキュリティ／暗号技術な人の観点からWebPKIの現状を考える

- DigiNotar事件などのPKIに関連する動向を共有し，証明書の不正発行・偽造問題から気づきを得たい
  - PKIを利用しているから安全という認識を変える！？

本発表でのポイント

- 安全だと信じているWebPKIって脆弱かも？！
- 実はWebPKIはドメイン名に深く依存している？！
- 証明書の不正発行・偽造問題に対する脅威とコスト
- 安全な生活インフラはなくなってしまうの？

SSL/TLSにおけるWebPKIの状況

- ざっくりとPKI周辺の状況をまとめて言うと・・・
  - 生活インフラと言っても良いくらい利用されている
    - 重要な情報を送受信する時には必須
      - SSL/TLSサーバ
      - コードサイニング… etc.,
  - 生活インフラだけど***Weak point*** が多く存在する
    - Weak pointがあり魅力的なターゲット
  - 事件が多く発生しても根本的な対策が打たれない
    - Comodo事件，DigiNotar事件
      - 攻撃者にとっての有益なUse Case（成功事例）になりうる

WebPKIは攻撃者にとって狙い目！

WebPKIにおける ***Weak point*** は？

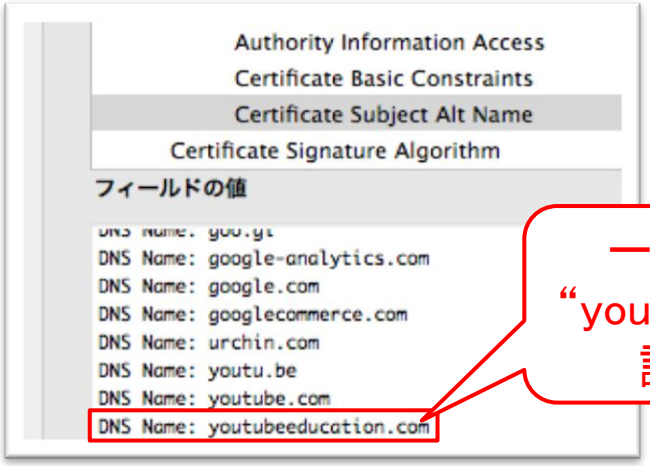
- 証明書のSubject Nameの体系
  - WebPKIの認証局は階層的なドメイン名空間と不一致
    - 認証局であれば，どのドメイン名に対する証明書を発行可
    - どんなドメイン名の証明書を発行できるので・・・
      - どんな攻撃に対しても全てのPKIの信頼点は守られている
      - 1つでも認証局が陥落すると全てのドメイン名が危険に晒される
- 危殆化した暗号アルゴリズム
  - 証明書ストアに危殆化したハッシュ関数や短い鍵長の証明書**まだ**格納されている
  - 証明書偽造に関する技術の向上
    - MD5: Wang（2004）; Stevens（2007）; Flame（2012）
      - 計算コスト: Stevens PS3を200台で1日； Flame 大量の計算機能力 or 未知の探索手法

個人・組織から国家レベル

- 標準化仕様と現実のギャップ
  - そもそもWebPKIはRFC5280から逸脱している！？
    - Certificate Path Construction, Constraints, Extended Key Usageが異なる
  - 相互運用性の欠如等を導く

もう少しドメインとWebPKI関係を考えてみる…

- ドメイン名とPKIのどちらも階層構造で管理されている
  - Webでの利用を考えると*構造は似ていても似て非なるもの*
    - 認証局はドメインに対して制約なく発行できるので，
    - WebPKIのあるべき論であれば，両者の構造は一致させる必要がある
- Unified Communications Certificateという仕組み
  - 1つのサーバ証明書で複数ホストを利用可能にする技術
    - 証明書の管理は楽だが・・・パッと見でドメインの所有者を判別できない
      - 不正な証明書の発行依頼が行われると意図しないドメインに対する証明書も．．．



一見，Googleが所有していそうもない
“youtubeeducation.com”などが含まれる．
認証局はどうやって確認するの？

PKIに対する攻撃手口

- PKIに対する攻撃手法を大別すると・・・・
  - システムの脆弱性を活用
    - Comodo
      - フロントサーバに存在していた既知の脆弱性を突いて潜入
        - DLLの解析を行うなどでID&PWが知られたりしたが…
    - DigiNotar
      - 認証局機能を乗っ取られて不正なSSLサーバ証明書が発行
        - EVSSL向けCAを含む，少なくとも6つ（疑わしいのも含めると30！！）
      - ***DNS改ざん***により偽SSL/TLSサーバに誘導
  - 暗号技術の脆弱性を活用
    - Flame
      - 危殆化したハッシュ関数（MD5）に対する選択プレフィクス衝突攻撃
      - 証明書の拡張フィールドをうまく利用して辻褄合わせ
    - 脆弱鍵（Vulnerable Repeated Keys）
      - 擬似乱数生成器の脆弱性(エントロピー不足)
      - 運用的な問題としてデフォルトの鍵を利用する
  - 参考情報
    - PKI Day 2012（http://www.jnsa.org/seminar/pki-day/2012/）
      - 「サイバー攻撃ツールとしての公開鍵証明書の役割～信頼の起点にカモフラージュされた攻撃の起点～」／神田 雅透 氏
      - 「公開鍵の多くが意図せず他のサイトと秘密鍵を共有している問題～いつのまにか他人と秘密鍵を共有してませんか？～」／須賀 祐治 氏

対策に関する動向

- 各団体における安全なWebPKIの実現に向けた取り組み
  - **IETF**
    - wpkops（Web PKI operations） WG
      - Trust model，失効処理，TLSに関する運用
    - certrans（Certificate Transparency）BoF
      - 証明書発行の透明性をどう実現するか？
    - Alternative PKI model side BoF
      - IETF86thで開催されたPKIモデル代替モデルについて有志により議論
  - **NIST**
    - CA Workshop
      - Workshop on Improving Trust in the Online Marketplace（2013年4月開催）
        - http://www.nist.gov/itl/csd/ct/ca_workshop.cfm
        - 現在のWebPKIに関する検討； DNSSECによりWebPKIを補強する流れ？！
  - **CA/Browser Forum**
    - Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates v1.0（2012.7～）
      - WebTrust for CAの後継規格
    - Network and Certificate System Security Requirements v.1.0（2013.1～）
      - WebTrust for CA，ETSI 101 456，ETSI TS 102 042
      - セキュリティ要件，権限管理，監視，脆弱性管理

DNSSECなどの技術が大きく取り上げられた！

これさえやっておけば大丈夫！という対策なし！
でも検討は徐々に行われている

今後も証明書の偽造は発生しうるか？

- 気持ち的には発生してほしくないが・・・

YESかなぁ…

- 理由として・・・
  - WebPKIの攻撃成功した際の利得が大きい！
  - 事件に対する根本的な対策としての決定打がない
  - 安価に証明書発行を行っているところが増加
    - 全部がダメとは言わないが運用や監査などのコストカットされ…

例えば・・・

WebPKIだけで対策しようとせず他のプロトコルを効果的に併用！

DNSSECによりDNSハイジャック等の脅威を削減！

まとめ

- 安全だと信じているWebPKIって脆弱かも？！
  - 冷静に考えるとWebPKIは脆い
    - WebPKIとドメイン名空間の乖離
      - 実際のところDNSという技術への依存関係が強い
    - 暗号アルゴリズムの危殆化
      - 暗号アルゴリズムの移行は進んでいるけど，危殆化したままという箇所は狙いどころ！
  - 案外，泥船的なところも・・・

- 証明書の不正発行・偽造問題に対する脅威とコスト
  - どんな偽造証明書をターゲットにするかで大変さは変化
    - 個人・組織レベルでPS3を用いて証明書の偽造
    - 国家レベルの計算機パワーや未知の探索手法
  - 証明書の不正発行だけでなくDNSハイジャックと併用で影響度アップ！
    - DigiNotar事件

- 安全な生活インフラはなくなってしまうの？
  - もしかしたらPKI単体ではツライ・・・
    - 例えばDNSSECをPKIと併用し，お互いを補強する必要があるのでは？