RFC4270の話
&
組込み機器への影響

2008-07-03

PKI Day 2008

松下電工株式会社
福田尚弘

RFC4270の話

現状のサマリー

1. MD5、SHA-1攻撃は両方発見、MD5への攻撃はシビア
   →MD5への攻撃は現代のどのコンピュータ上でもありうる

2. SHA-1攻撃は現在複数コンピュータでも実現可能でない
   →攻撃の改良、またはムーアの法則で将来計算力が安くなれば可能

3. 一般のプロトコルは攻撃に影響されない方法をとっている
   →影響を受けるプロトコルはデジタル署名を使っている

4. 優れたハッシュアルゴリズムは影響を許容レベルに減衰
   →悪いアルゴリズムは2^L以下、脆弱の程度では攻撃対象

RFC4270の話
ハッシュアルゴリズムと攻撃

- **衝突攻撃**: 2^(L/2)
- **原像探索攻撃**:2^L
- **別原像探索攻撃**:2^L
  →**最も効果的な攻撃だが**…

(同一ハッシュの計算量的困難性)＆(メッセージが攻撃適性を持つ困難性)の両方の満足は困難

→ハッシュが一致してもそのメッセージビットがプロトコル構造に“そぐわな”ければ、現実の攻撃は困難

RFC4270の話

ハッシュアルゴリズムを使うプロトコルへの影響

	ハッシュの利用方法	衝突攻撃	可能性
1	否認防止付デジタル署名	影響	別紙
2	信頼できる第三者機関による証明書内のデジタル署名	影響	別紙
3	チャレンジレスポンスプロトコル		相手の秘密保持によるので困難
4	共有秘密鍵によるメッセージ認証		双方の秘密保持によるので困難
5	鍵導出関数		双方のランダム入力から乱数を入力するので困難（IETFの方法）
6	ミキシング関数 （ランダムにデータを混合する）		
7	完全性保護		

RFC4270の話
否認防止付デジタル署名

- 別原像探索攻撃で注文書を10$→1万$へ…

→2^L なのでほとんどありえない

- 人間がチェックする場合は確認可能

→ＥＤＩでは自動で行うので場合による

RFC4270の話

信頼できる第三者機関によるデジタル証明書

1) 公開鍵1つで異なる2つのIDをもつ証明書入手が可能…
→別人に成りすませる

2) 異なる2つの公開鍵の証明書も入手できる…
→意味があるか？

対策

- シリアル番号を推測不能にする
- IDにランダム要素を入れる
- 有効日時(Validity Date)を推測不能にする

Note:衝突攻撃は人間が読めない公開鍵などには効果がある、
しかし、人間にわかるIDなどがあると難しい

RFC4270の話
ブルース 対 ポール

ブルース

→最初から SHA-256 **を使い始めるべきである**

ポール

→プロトコルが衝突攻撃の影響を受けない限り
SHA-1 **を使うべきである**

組込機器への影響
どのくらい影響するか？

- モノによる…
  - 衝突耐性を要求するかしないか？
  - オープン、クローズ、ハイブリッド…
  - FIPSなど保証がなくなるので自前で保証必要
  - 商品価値に影響がでる（カタログベース）
  - 寿命が長い（10年以上）製品では影響
    →寿命内でFIPSの保証なくなるモノも…
    ＊組込機器もネット対応での保守に流れる
    （ファームアップデート）

組込機器への影響
どのくらい大変か？

- モノによる…
  - 現行の組込は「カツカツ」で動くもの
    ＊動的アップデートには倍のメモリ必要
  - 安全な移行の仕組みが求められる
    →ダウングレードアタック対策など
    →安全な仕組みも古い暗号アルゴリズムを使う？
    →アルゴリズムは軽量であるべき（電池駆動）
  - 移行に限らないが、安全性維持にはコストがかかる
    →H/Wの交換、互換維持問題

組込機器への影響
まとめ

- **衝突耐性を要求** & **衝突**(2^63 →2^40) **になれば危険**
- NIST**が**2010**年以降使ってよい**SHA-1**のアプリケーション**
  - HMAC (Hash-based Message Authentication Code)
  - KDF (Key Derivation Function)
  - RNG (Random Number Generator)
- **移行の仕組みの導入で変わること**
  - **保守のためのネット対応**
  - **リソース増** (CPU**能力、メモリ容量の**UP)
  - **互換･非互換の対応**

→コスト増と仕組みの複雑化が予想される

参考

[1] RFC2470
“Attacks on Cryptographic Hashes in Internet Protocols”,
P. Hoffman, VPN Consortium,
B. Schneier, Counterpane Internet Security,
November 2005
[2] Workshop Report: The First Cryptographic Hash Workshop, Oct. 31-Nov. 1, 2005, Shu-jen Chang, Morris Dworkin, NIST
http://csrc.nist.gov/groups/ST/hash/documents/HashWshop_2005_Report.pdf
[3] NIST's Policy on Hash Functions, March 15, 2006
http://csrc.nist.gov/groups/ST/hash/policy.html