Monthly Research

数学者の暗号破りに見る「暗号の強さ」の重要性

Fourteenforty Research Institute, Inc.
株式会社 フォティーンフォティ技術研究所
http://www.fourteenforty.jp

Ver2.00.01

背景：暗号破りがフォーカスされた事件

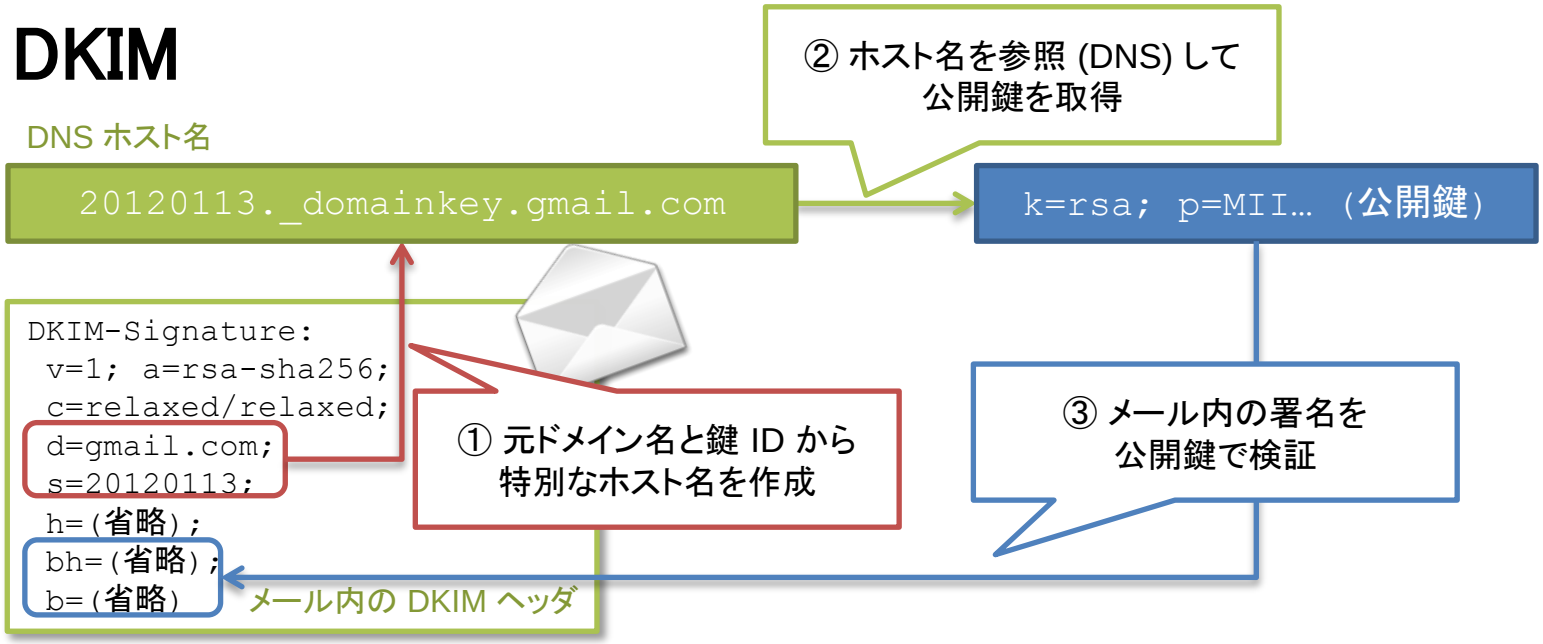
- WIRED のニュース・インタビューより[1]
- 数学者 Zachary Harris が、Google から届いたメールの送信元証明（DKIM）に弱い電子署名方式が使われていることに気がついた
  - この署名鍵を破ることで、Google 創業者のメールに見せかけた偽のメールを Google の CEO 宛に送ることに成功した
  - 彼はクラウドコンピューティングの力を借りることによって個人では現実的ではないと思われていた解読を実現した

[1] http://www.wired.com/threatlevel/2012/10/dkim-vulnerability-widespread/all/ (原文)
http://wired.jp/2012/10/27/dkim-vulnerability-widespread/ (日本語抄訳)

認証のための暗号：電子署名

- 電子署名:
  事実上“秘密鍵”を持っている人だけが生成することのできる
  情報(“署名”)を、それに対応する“公開鍵”を用いて検証するモデル
  - 電子署名が付与されている文書を第三者が改ざんした場合には
    “署名”が無効になるため、改ざんされたことがはっきり分かる
    (改ざんの防止)
  - 数学的な性質を用いて、文章やデータが特定の個人、
    法人やコンピュータから発信されたことを極めて高い確率で
    証明することができる(なりすましの阻止)

DKIM



- DKIM (DomainKeys Identified Mail) は
  メールの送信元 (ドメイン) を電子署名を用いて証明する仕組み
  - 送信元が指定する特殊なホスト名から “公開鍵” を取得する
  - メール内にある “署名” を取得した “公開鍵” を用いて検証する
  - 検証に成功した場合、極めて高い確率で
    送信元が正しいことを保証することができる

電子署名に利用される方式：RSA

- 公開鍵暗号や電子署名の方式
  - ある整数を、それ以上分解できない整数（素数）の組み合わせに分解する（素因数分解）ことが難しいことを利用する
    → 素因数分解を行うことができるなら RSA を破ることができる
  - RSA においては、2 つの素数 を掛けあわせた数を“公開鍵”とし、“秘密鍵”は 2 つの素数から計算される特別な数とする
- 幅広い利用
  - インターネット上の暗号通信（SSL/TLS）を行ったり、なりすましを防止したりする（DKIM 等）ためなどに広く用いられている
  - インターネットの世界の暗号はこの暗号に守られているといっても過言ではない

RSA：解読手法

$$x^2 - y^2 = (x + y)(x - y)$$

- 因数分解を行えば“公開鍵”から“秘密鍵”を導き出せる
- 最近は“平方差法”を基本とした因数分解が主流
  - 左辺の値が分解したい数の（0 以外の）倍数になる適切な x と y の組み合わせを見つければ、因数分解の公式によって元の数の因数を計算することができる
  - この因数から RSA の秘密鍵を復元することができる
- “平方差”の適切な組み合わせを見つけるために複雑な数学理論とアルゴリズムが開発された
  - 複数多項式二次ふるい法（MPQS）
  - 一般数体ふるい法（GNFS）

RSA：解読の歴史

- 素因数分解 / 因数分解技術の向上とコンピュータの計算能力の向上とともに解読されてきた
- RSA-100 (330 ビット)
  - 1991年4月1日
- RSA-129 (426 ビット)
  - 1994年4月
- RSA-155 (512 ビット)
  - 1999年8月22日
- RSA-768 (232 桁)
  - 2009年12月12日

RSA：鍵の長さと解読の危険

- RSA の強度は、(他に致命的な誤り[1] がない限り)
  公開鍵を生成するために用いる 2 つの素数の大きさに依存する
  - 近年では 155 桁以上の素数を 2 つ用いる (1024 ビット以上)
- 逆にいえば、小さな素数を用いて構築されている
  RSA 暗号は弱いということがいえる
  - 現在では、2048 ビット以上の鍵が推奨されている
  - Zach Harris の暗号破りは、この “短い” RSA 鍵が
    比較的容易に破れてしまうことを利用している

[1] http://www.atmarkit.co.jp/news/200805/20/openssl.html

Z.H. の暗号破り : DKIM の弱い RSA 鍵

- Zach Harris 氏は、Google から届いた (DKIM で送信元が証明される) メールを見て、証明に用いている鍵の長さが短いことに気がついた
  - RSA アルゴリズムの 512 ビット鍵
- さらに他のサービス等の DKIM 鍵などを見て、一部において非常に短い RSA 鍵が使われていることを発見
  - 384 ビット、512 ビット、768 ビット
  - 一般的には 1024 ビットないと十分な安全性を確保できない
- 既存のソフトウェア (CADO-NFS) とクラウドコンピューティングサービス (Amazon EC2) を用いて Google の RSA 鍵を因数分解した
  - 結果として、Zach は (修正されるまで一時的に) 送信元を Google と偽ったメールを誰にでも送信できるようになった

Z.H. の暗号破り : クラウドコンピューティング

- クラウドコンピューティング
  - ネットワークを通じて使う分だけコンピュータ（および処理能力）を利用する最近流行している利用形態
  - これを利用することで、個人でもスーパーコンピュータ並の処理能力を一時的に借りることが可能になった
- Harris 氏のインタビューより…
  - 512 ビットの RSA 鍵を 72 時間以内で解読
    （Zach 曰く: “384 ビットだったら手元のノートパソコンでも 1 日で解読できただろう”）
  - 利用料金の合計は 70 ドル程度
    （ここから、性能の高いコンピュータを 2～4 台借りたものと推測される）

RSA：解読実験

- Zach Harris 氏が見つけた中で最も短い長さ（384-bit）の OpenSSL 鍵を生成し、秘密鍵を破棄、公開鍵だけから秘密鍵を復元する
  - OS： Arch Linux (x86_64)
  - CPU： Core i7 3612QM（ノート PC 用）
  - メモリ： 8GB
  - ソフト： CADO-NFS 1.1[1]
- 解読実験結果（19 時間 30 分 26 秒）
  - 因数分解： 19 時間 30 分 25 秒
  - 秘密鍵の再生成（Python）： 1 秒
- 512-bit（Harris 氏が破ったものとほぼ同じ強度）であったとしても 2 ヶ月以内（クラウドコンピューティングなし）で解読可能と推測される

[1] http://cado-nfs.gforge.inria.fr/

鍵の重要性：鍵長

- RSA: 2048 ビット以上が推奨される（電子政府推奨暗号リストより）
  - 1024 ビットでも現状解読は難しいが、
    時代の変化に伴って相対的に弱くなることを考慮すべき
  - Microsoft Windows は最近のアップデートで、
    1024 ビット未満の弱い鍵をブロックするようになった[1]
- 同等の安全性を担保する：暗号方式が違えば鍵の強度は違う[2]
  - 共通鍵暗号：　108 ビット前後（具体的な暗号によって異なる）
  - RSA/DSA：　2048 ビット
  - ECDSA：　206 ビット
  - 実際に（具体的な）鍵の長さを規定する場合には
    暗号方式も考慮することが必要

[1] https://blogs.technet.com/b/jpsecurity/archive/2012/07/30/3511493.aspx
[2] http://jp.fujitsu.com/group/labs/downloads/techinfo/technote/crypto/eccvsrsa-20100820.pdf

鍵の重要性：使われうる場面

- SSL/TLS（インターネット上の暗号化通信）
  - サイト証明書
- SSH（シェルログイン）
  - 公開鍵認証
  - ホスト鍵
- Windows ログイン
  - ユーザー証明書
- …

まとめ

- Zach Harris 氏が破ったのは、RSA の “弱い” 鍵だった
  - 鍵が長ければこのような解読が行われる危険性は少なくなる
- 重要な認証においては鍵の長さをチェックしてみよう
  - Google のような大企業でさえミスがある

主要参考文献

- WIRED 英語版
  “Google の採用メールがネットのセキュリティホールを暴き出すまで”
  (http://www.wired.com/threatlevel/2012/10/dkim-vulnerability-widespread/all/)
  (日本語版抄訳: http://wired.jp/2012/10/27/dkim-vulnerability-widespread/)
- CADO-NFS メーリングリスト “Thanks”
  (http://lists.gforge.inria.fr/pipermail/cado-nfs-discuss/2012-October/000098.html)
- 立教大学理学部 “数体ふるい法による素因数分解”
  (http://www.rkmath.rikkyo.ac.jp/~kida/nfs_intro.pdf)
- 英語版 Wikipedia “RSA numbers”
  (https://en.wikipedia.org/wiki/RSA_numbers)

リンク

- CRYPTREC “電子政府推奨暗号リスト”
  (http://www.cryptrec.go.jp/list.html)
- IPA/NISC “電子政府推奨暗号の利用方法に関するガイドブック”
  (http://www.cryptrec.go.jp/report/c07_guide_final.pdf)