Angriffe gegen kryptografische Hash-Funktionen (SHA1, MD5)

mrmcd11b, 2. - 4. September, Darmdstadt
von Hanno Böck, http://www.hboeck.de/

Kryptografische Hash-Funktionen

- Erzeugt aus beliebigen Eingaben eine Ausgabe mit fester Länge
- Kollissionsresistenz: Es soll schwierig sein, zwei Eingaben mit der gleichen Ausgabe zu finden, d.h. keine unterschiedlichen a und b mit H(a)=H(b)
- Es soll nicht möglich sein, zu einer bekannten Eingabe eine weitere Eingabe mit gleichem Hash zu finden (Preimage-Attack)

Einsatz

- Signaturen: Es wird ein Hash einer Nachricht erzeugt und nur dieser signiert
- Verifikation von Downloads
- Schutz von Passwörtern (/etc/shadow)
- Baustein in komplexeren kryptografischen Konstruktionen (RSA-PSS)

Angriffe gegen MD5

- August 2004: Kollission für MD5 gefunden (Xiaoyun Wang, Dengguo Feng, Xuejia Lai und Hongbo Yu)
- Ebenfalls Kollissionen für MD4, SHA0, RIPEMD, HAVAL-128

Angriffe gegen SHA1

- Theoretischer Angriff im Februar 2005 mit einer Komplexität von 2^69
- Verbesserung des Angriffs auf 2^63 im August 2005
- 2^63 ist mit Großrechnern realistisch erreichbar

Was bedeutet Kollission?

- Aufgrund des Designs von MD5 und SHA1 ermöglicht eine bekannte Kollission die Erzeugung von beliebig vielen weiteren Kollissionen
- Es besteht die Möglichkeit, gezielt Dokumente mit gleichem Hash zu erzeugen, wenn es möglich ist, im Dokument ignorierbare Bytes zu integrieren (PostScript, gz)

Angriffe

- Sie erhalten einen Vertrag, signieren diesen und es existiert ein vollkommen unterschiedliches Dokument, für das anschließend die Signatur ebenfalls gilt
- Angriff auf Signaturen von Paketsystemen, jemand erstellt eine präparierte Version eines Pakets und jubelt gezielt (bspw. durch Arpspoofing) bestimmten Personen modifizierte Pakete mit Backdoors unter

Beispiel MD5

Julius. Caesar
Via Appia 1
Rome, The Roman Empire

May, 22, 2005

Order:

Alice Falbala is given full access to all confidential and secret information about GAUL.

Sincerely,

Julius Caesar

Julius. Caesar
Via Appia 1
Rome, The Roman Empire

May, 22, 2005

To Whom it May Concern:

Alice Falbala fulfilled all the requirements of the Roman Empire intern position. She was excellent at translating roman into her gaul native language, learned very rapidly, and worked with considerable independence and confidence.

Her basic work habits such as punctuality, interpersonal deportment, communication skills, and completing assigned and self-determined goals were all excellent.

I recommend Alice for challenging positions in which creativity, reliability, and language skills are required.

I highly recommend hiring her. If you'd like to discuss her attributes in more detail, please don't hesitate to contact me.

Sincerely,

Julius Caesar

Konsequenzen

- Es gibt vielfältige Szenarien, in denen Kollissionen in Hash-Funktionen Systeme kompromittieren
- Preimage-Attacken (Erzeugung eines Dokuments mit gleichem Hash zu vorgegebenem Dokument) bisher nicht möglich, jedoch deuten die bisherigen Angriffe möglicherweise auf weitere Schwächen hin
- Verwendung von MD5 und SHA1 beenden

Einsatz von MD5 und SHA1

- Selbst neueste SSL-Versionen verwenden nur SHA1
- SSH verwendet SHA1
- portage (Gentoo) verwendet MD5
- shadow verwendet MD5
- TCG 1.2 verwendet SHA1
- GPG verwendet per Default SHA1

Alternativen

- SHA2-Familie (SHA224, SHA256, SHA512), vom NIST standardisiert
- Neue Ansätze: Whirlpool, Tiger
- Möglichkeit, mehrere HASH-Funktionen aneinanderzuhängen, bspw. H(a)=sha512(a),whirlpool(a),tiger(a)
- Workshop des NIST im Oktober

Implementation

- shash, mhash (http://mhash.sourceforge.net/)
- shash, Commandline-Tool:
  shash -a WHIRLPOOL [filename]
- mhash, Library für diverse Programmiersprachen,
  Beispiel PHP:
  $hash = mhash(MHASH_SHA256, $input);

Links / Quellen

- http://www.cryptolabs.org/hash/ - mehrere Artikel zum Thema
- http://www.schneier.com/blog/ - Blog von Bruce Schneier, aktuelle Entwicklungen
- http://www.cits.rub.de/MD5Collisions/ - Postscript-Dateien mit gleichem MD5-Hash
- http://www.infosec.sdu.edu.cn/people/wangxiaoyun.htm - Papers von Xiaoyun Wang

Links / Alternativen

- http://www.cs.technion.ac.il/~biham/Reports/Tiger
- http://paginas.terra.com.br/informatica/paulobarreto/WhirlpoolPage.html
- http://csrc.nist.gov/publications/fips/ - Standards des NIST (SHA2)
- http://mhash.sourceforge.net/ - freie Implementierung aller relevanten HASH-Funktionen

Fragen?

Folien unter
http://www.hboeck.de/