Hash innen!

Veres-Szentkirályi András (Silent Signal)

HWSW Free!
2017-04-25

Figyelem!

$$C_i = K_i \oplus P_i$$

Az előadást kriptográfusok számára a szövegben előforduló általánosítások és egyszerűsítések miatt csak laikus társaságában ajánljuk!

Egy fontos gondolat előszó helyett

„Anyone, from the most clueless amateur to the best cryptographer, can create an algorithm that he himself can't break."

– Bruce Schneier (1998. október 15.)
https://www.schneier.com/crypto-gram-9810.html#cipherdesign

Kiber

Megfelelő helyen és mennyiségben ízlés szerint:

- kiber
- kiber
- kiber
- kiber
- kiber
- kiber
- kiber

WTF hash

- AKA (message) digest
- kivonat, „fasírt”
- tetszőleges hosszú bemenet
- fix hosszú kimenet
- skatulyaelv érvényesül
  - n bit $\iff$ 2^n lehetőség
  - mindent leképezünk $\implies$ lesz ütközés

Hashtábla

- „asszociatív tömb”, szótár
- tartalom szerint címezhető tár
- naiv megoldás: $\mathcal{O}(n)$
- okos megoldás: $\mathcal{O}(\log n)$
- hash-sel tárolás: $\mathcal{O}(1)$
- elsődleges szempont: gyorsaság

Jelszavak

- **jelszót nem mentünk el könnyen visszaállítható formában**
- támadói modell: read-only DB hozzáférés
- extrém alacsony entrópia (tipikusan $< 64 bit$)
- elsődleges szempont: biztonság
  - confidentiality: ne lehessen jelszót előállítani
  - availability: a rendszer legyen elérhető

Integritás

- „történt-e nem kívánt adatmódosítás?”
- támadói modell: bitrot, kozmikus sugarak – CRC32
- támadói modell: rosszindulatú – lásd alább
- hálózati forgalomra: TLS, SSH, VPN
- tárolt adatokra: Git, BitTorrent
- digitális aláírásra: X.509, kriptopénz, e-számla
- ’90-es évek nosztalgiájának: AV
- elsődleges szempont: itt is biztonság
- de: magas entrópia, akár több GB méret

Hash függvények alkalmazási területei

Terület	Sebesség	Entrópia	Kimenet
Hashtábla	gyors	?	rövid
Jelszavak	lassú	alacsony	hosszú
Integritás	gyors	magas	hosszú

Jellemző támadási forma:

- Hashtábla: DoS web felől (JSON kulcsok)
- Jelszavak: brute force, szótár, reuse
- Integritás: hamisítás, megtévesztés

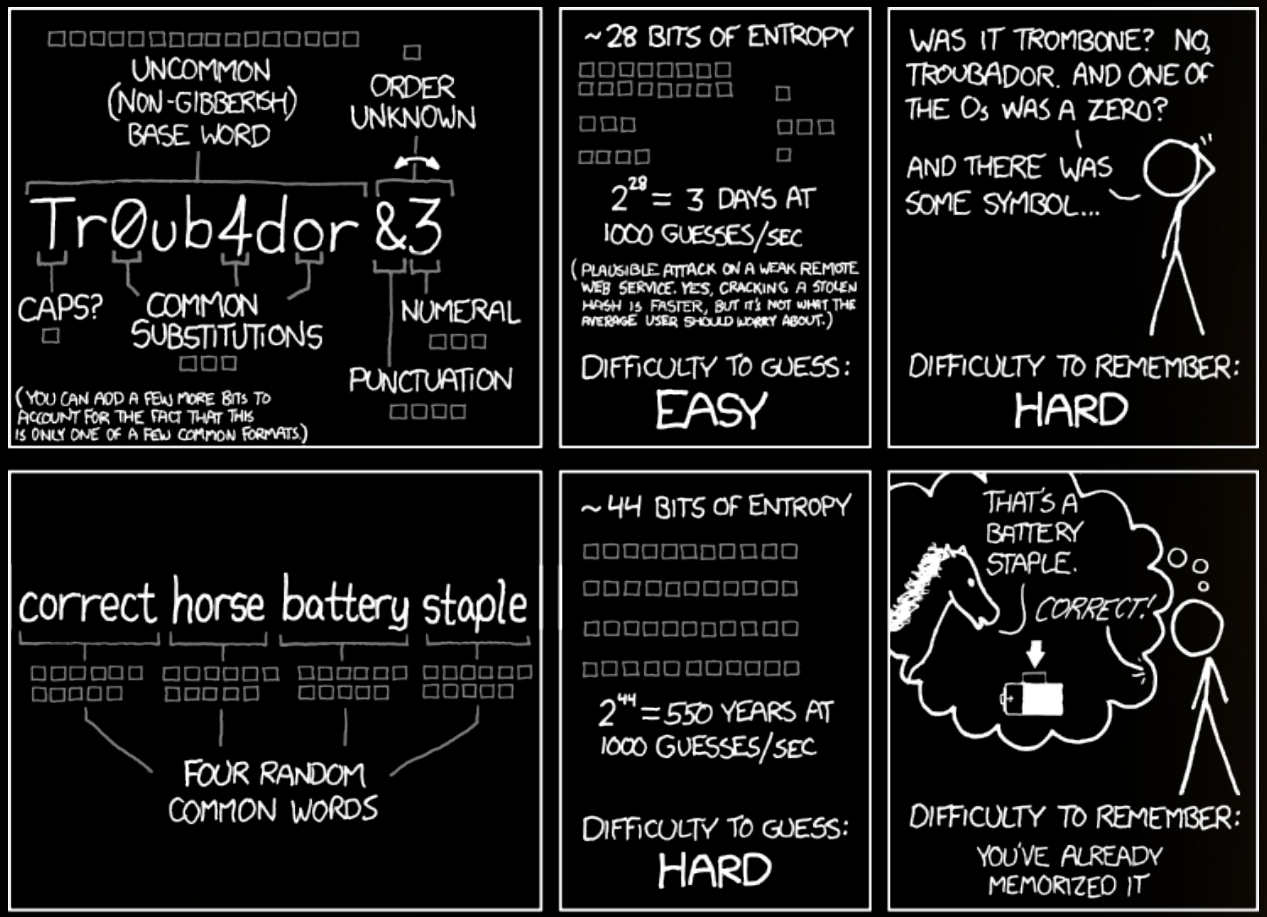
Nagyságrendek

- hasznos közelítés: $2^{10} \approx 10^3$
- $2^{128} \approx 10^{38}$
- Ötöslottó: $\binom{90}{5} \approx 5 \times 10^9$
- 1 év $\approx 3 \times 10^7$ s
- $10^9 \frac{\text{teszt}}{\text{s}} \implies$ teljes tér bejárása 10^{22} CPU-év
  - univerzum $13.799 \pm 0.021 \times 10^9$ éves
  - 5×10^9 év múlva a Nap vörös óriássá válik, és valószínűleg elnyeli a Földet

Entrópia

- „információtartalom”
- Példa: `https://linusakesson.net/scene/a-mind-is-born/`
  - PCM/WAV soundtrack: 26 MB
  - MP3 soundtrack: 2,2 MB
  - C64 executable: 256 bájt
- relevancia hash-elésnél: hányat kell próbálkozzak?

Jelszavak entrópiája (https://xkcd.com/936)



Hash mint „entrópiaforrás”

- csak alacsony entrópia bizonyítható
- black box: security by obscurity
- $RND() = H(P())$ ahol $P()$ kimenete megjósolható kiváló backdoor
  - gyakori tapasztalat: $P =$ `time(2)`
  - hardveres CSPRNG megbízhatósága?

Lavina-elv

- egy bit változik a bemeneten $\Longrightarrow$ bitek legalább fele változik a kimeneten
- fontos a statikus idejű összehasonlítás
  - vö. „short-circuit” kiértékelés, pl. `memcmp(3)`

```
if (md5($password) == $hash) {
  print "Allowed!\n";
}
```

```
> var_dump("615295194528097206937025831268l4" ==
  "615295194528097200000000000000000");
bool(true)
```

http://phpsadness.com/sad/47

Hardening: *salt*

- Rainbow tábla 101: tároljunk le egy nagy $H(x) \to x$ táblázatot jól megválasztott x értékekre (pl. szótár)
- ellentámadás: használjunk saltot
  - $H(p)$ helyett $(s, H(p, s))$ tárolása
  - password reuse és azonos jelszavak ellen véd
  - támadást jelentősen lassítja
  - salt reuse ellenben ront a hardening hatásfokán
- too much kool-aid: „pepper” $\to$ kerülendő!
  - kulcsok periodikus cseréje nem megoldható
  - további hardeningnek értelmesebb egy szimmetrikus titkosítás

Slow food, slow fashion, slow password hashing

- hogyan lassít a programozó? ciklussal!
- ésszel: HMAC használata „pucér” hash helyett
- PBKDF2: RFC-ben definiált, jó implementációk
  - WPA: salt=SSID, iter=4096, hash=HMAC-SHA-1
  - `https://tools.ietf.org/html/rfc2898`
- `crypt(3)` SHA-2 alapon: Linuxon default
  - `https://passlib.readthedocs.io/en/stable/lib/passlib.hash.sha256_crypt.html`
- bcrypt: régi de jó, blowfish alapú, BSD-n default
  - `https://passlib.readthedocs.io/en/stable/lib/passlib.hash.bcrypt.html`

GPU – egy kép felér ezer gépi szóval

#000	#FF0	#000
#000	#000	#FF0
#FF0	#FF0	#FF0

$$x' = \frac{x + \#\mathrm{F00}}{2}$$

#800	#F88	#800
#800	#800	#F88
#F88	#F88	#F88

jelszo	qwertz	1234
asdf	1988	titok
4321	Aa1!	函数

$$x' = H(x)$$

2 d 7 e 0 a	3 b 6 0 1 3	7 4 4 6 f f
f 2 8 7 4 0	6 d 2 a c a	e 1 e e 0 a
8 9 f a a 3	f 1 d e 6 5	2 f 1 e e 6

GPU – részletek

- skálázódó számítási kapacitás → RAM-ra lövünk
- Argon2 és scrypt direkt sok memóriát igényelnek
- előbbi PHC nyertes és sokan elemezték 2013 óta
  - `https://passlib.readthedocs.io/en/stable/lib/passlib.hash.argon2.html`
- utóbbi finomhangolása pilótavizsgás
  - `https://passlib.readthedocs.io/en/stable/lib/passlib.hash.scrypt.html`

Merkle-Damgård konstrukció

- MD5, SHA-1, SHA-2 ilyenek (SHA-3 viszont nem!)
- $H(a) = H(b) \implies \mathrm{H(a}\|c) = H(b\|c)$
  - ütközés esetén folytatható változatlanul az üzenet
- $H(k\|a)$ és b alapján előállítható $H(k\|a\|b)$
  - k titkos kulcs
  - $a =$ „utalj 50 Forintot Andrásnak”
  - $b =$ „közleménnyel Bélának”
  - ez ellen (is) véd a HMAC!

Hashfüggvények „megtörése”

- collision $\Longrightarrow$ 2^{nd} preimage $\Longrightarrow$ preimage
- preimage: adott y értékhez $H(x) = y$
- 2^{nd} preimage: adott x értékhez $H(x) = H(x')$
- collision: bármilyen x és x' amire $H(x) = H(x')$
- születésnapi támadás: $\sqrt{2^N}$ alsó korlát
  - ez alatt „megtörtük”
  - MD5
  - SHA-1

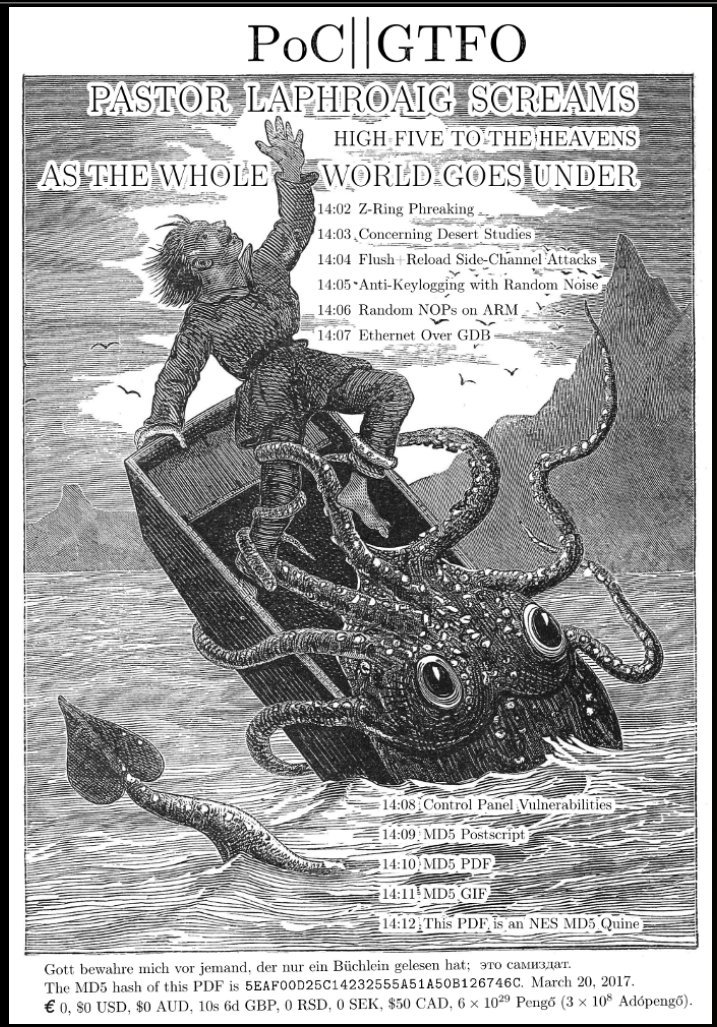
MD5 támadások: USA elnökválasztás (2007. november)

- https://www.win.tue.nl/hashclash/Nostradamus/
- „Predicting the winner of the 2008 US Presidential Elections using a Sony PlayStation 3”
- előre publikált MD5 hash
- PDF minden jelöltre egyező értékkel
- 1 PlayStation 3 $\approx$ 30 PC erre a feladatra

MD5 támadások: farkas a bárányok között (2015)

- https://blog.silentsignal.eu/2015/06/10/poisonous-md5-wolves-among-the-sheep/
- jól viselkedő EXE bekerül MD5 fehérlistába
- rosszul viselkedő EXE azonos MD5 értékkel
- https://github.com/silentsignal/sheep-wolf
  - FireEye
  - REDACTED (network forensics appliance)
  - REDACTED (next-generation AV)
  - Panda Adaptive Defense 360
  - REDACTED (malware analysis sandbox)
  - REDACTED (malware analysis sandbox Virustotal API)
  - Malware whitelists (and blacklists) of Tenable Nessus

MD5 támadások: PoC||GTFO (2017. március)



MD5 támadások: PoC||GTFO (2017. március)

Gott bewahre mich vor jemand, der nur ein Büchlein gelesen hat; это самиздат.
The MD5 hash of this PDF is `5EAF00D25C14232555A51A50B126746C`. March 20, 2017.
€ 0, $0 USD, $0 AUD, 10s 6d GBP, 0 RSD, 0 SEK, $50 CAD, 6×10^{29} Pengő (3×10^{8} Adópengő).

```
$ md5sum pocorgtfo14.pdf
5eaf00d25c14232555a51a50b126746c
```

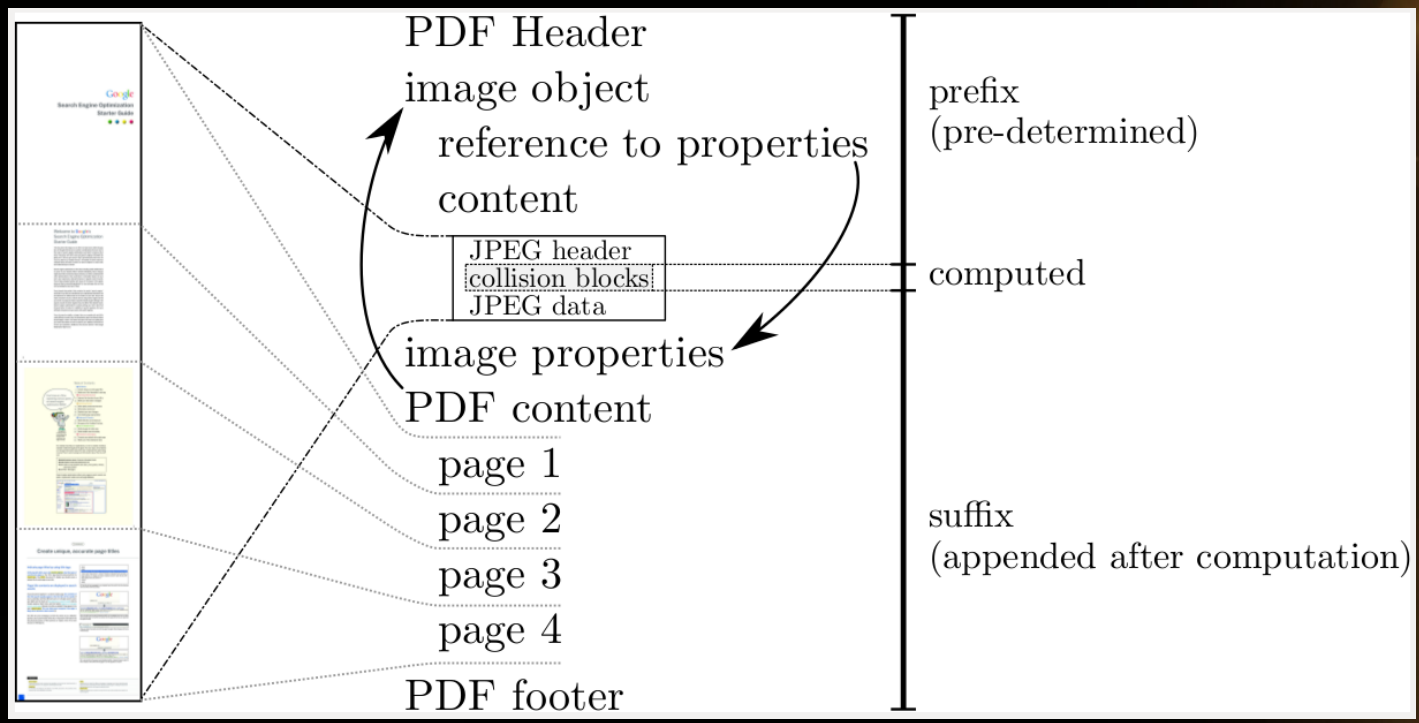
- És emellett még egyszerre egy NES ROM, ami szintén kiírja ugyanezt!
- `https://www.alchemistowl.org/pocorgtfo/pocorgtfo14.pdf`

SHAppening (2015. október)

- első valóban bemutatott támadás
  - korábbiak mind elméletiek maradtak, mert drága lett volna megvalósítani
  - egy hasonló megoldás akkortájt 2000 USD
- még nem teljes ütközés
  - az 75 és 120 ezer dollár között lett volna
  - bőven belefér nagyobb szervezeti büdzsébe

SHA-1 támadás: shattered (2017. február)

- PDF fejlécet követő JPEG: `https://shattered.it/`
- 110 GPU-év + 6500 CPU-év (vs. 12×10^9 GPU-év)



. . . de!

- nem minden formátum támadható ugyanannyira
  - PDF, JPEG, GIF belső lehetőségei segítőkészek
  - TCP specifikáció: „be conservative in what you do, be liberal in what you accept from others”
  - biztonság: legyünk csak konzervatívak megbízhatatlan forrásból származó adatokkal
- friss példa az égetőbb problémákra: FlexiSpy hack
  - default (`test:test`), hardcoded (`tcpip123`), reused (`*:tcpip123`), stored in plain & stolen (DC)
- kripto kód közvetlen környezete jobban támadható
  - `http://www.daemonology.net/blog/2008-12-18-AWS-signature-version-1-is-insecure.html`
  - `http://buhera.blog.hu/2013/07/08/andropokalipszis`
  - `https://pwnaccelerator.github.io/2016/signal-part1.html`

Köszönöm a figyelmet!

Facebook

vsza@silentsignal.hu

web

e-mail

SILENT SIGNAL
VÉSZJELZÉS HELYETT...

WWW.SILENTSIGNAL.HU