Rainbow Tables: Hybrids and Sub-keyspaces

James Nobis (quel)

http://www.freerainbowtables.com

Passwords^11, 2011

Overview

- Personal bio
- Background information
- RTI2 file format
- Hybrids and Sub-keyspaces

Personal bio

- What is freerainbowtables.com?
- How much money do you make?
- Who is this guy?
  - Official day job title: Senior System Administrator / Developer
  - *nix - Linux, OpenBSD, NetBSD
  - coder in several languages
  - amateur crypto hobbyist
  - Bachelor of Science in Computer Science
  - not in the sec industry

Background Information

- Generic TMTO for ciphers and hashes
  - Time-Memory TradeOff
- Probabilistic - not a lookup table
  - md5_loweralpha#1-10

$$keySpace = 146813779479510 \approx 2^{47.061}$$
$$lookupTableStorage \approx 2^{47.061} * 16 \approx 2136\,TiB$$
$$RTIStorage \approx 280\,GiB$$
$$RTI2Storage \approx 112\,GiB$$
$$RTSuccess \gtrapprox 99.905\%$$

- See my talk from Passwords^10 for full background[1]

RTI2 file format

- initial design and implementation by
  - PowerBlade - Martin Jørgensen[2]
- format header design by
  - Sc00bz - Steve Thomas[3]
- format change to have prefix indexes and data in 1 file
- storing parameters in the header and not the filename
- variable length data chains - start and end point
- data chains are ceiled to the next byte
  - project-rainbowcrack.com's rtc took this approach as well [4]
- full bit packing is for a later minor revision
- header also adds support for per position charsets
  - including per position hybrid charsets

Performance Comparison

[quel@paranoia] cat hashes.txt
2c678f2e67902fb8294e15f6d44cc3e1
b172647b25385aef84620de9b5d194ad

[quel@paranoia] ./rcracki_mt -t 3 -l hashes.txt -o results.txt
/mnt/rainbow_tables/freerainbowtables/md5/md5_loweralpha#1-
10_?/*.rti

md5_loweralpha#1-10_1_40000x67108864_distrrtgen[p][i]_04.rti:
plaintext of 2c678f2e67902fb8294e15f6d44cc3e1 is kpcjdbsdr

md5_loweralpha#1-10_1_40000x67108864_distrrtgen[p][i]_17.rti:
plaintext of b172647b25385aef84620de9b5d194ad is lytoyswacd

Performance Comparison 2

plaintext found:	2 of 2 (100.00%)
total disk access time:	590.79 s
total cryptanalysis time:	99.76 s
total pre-calculation time:	385.65 s
total chain walk step:	3199760004
total false alarm:	55469
total chain walk step due to false alarm:	814610518
plaintext found:	2 of 2 (100.00%)
total disk access time:	378.32 s
total cryptanalysis time:	101.09 s
total pre-calculation time:	385.69 s
total chain walk step:	3199760004
total false alarm:	55379
total chain walk step due to false alarm:	813259824

Hybrids

- hybrids? Why do we need them?
- first attempt
- hybrid2

Hybrids? Part 1

- all-space#1-7 lm/halflmchall
- alpha-numeric-space#1-8
- alpha-space#1-9
- lm-frt-cp437-850#1-7
- loweralpha-numeric-space#1-8
- loweralpha-numeric-symbol32-space#1-7
- loweralpha-numeric-symbol32-space#1-8
- loweralpha-space#1-9
- loweralpha#1-10
- mixalpha-numeric-all-space#1-6
- mixalpha-numeric-all-space#1-7
- mixalpha-numeric-space#1-7
- mixalpha-numeric-space#1-8
- mixalpha-numeric#1-7
- mixalpha-numeric#1-8
- numeric#1-12

Hybrids? Part 2

- keySpaces from 2^36.230 to 2^47.754
- RTI on disk sizes from 1.8 GiB to 530 GiB
- some new sets at 2^48.889 are 773 GiB RTI - 395 GiB RTI2
- generation about 61 days for clients on the high end
- Should we settle for less than 99.9% success?
- Should we just ignore everything but GPUs?
- Why settle for less?!

Hybrids - first attempt

- keyspace bias
- allowed only 2 character sets
- first character set of fixed length
- second at the end of variable length
- example: md5_hybrid(loweralpha#7-7,numeric#1-3)
  - [a-z]{7}[0-9]{1,3}
  - cracks testing1, testing12, testing123

Hybrid2 Part 1

- each character set is a sub-keyspace
- code is complete and deployed for CPUs
- code is nearly complete for GPUs
- next up ntlm [A-Z][a-z]{5}[a-z0-9]{2}[0-9]{1,3}[1]
  - yes that's length 9, 10, or 11!
  - at 99.9% success
  - complements existing sets like ntlm_mixalpha-numeric#1-8
- good corporate password statistics are needed
- Per seems to have some data ;)
- give us feedback on what tablesets to do

Hybrid2 Part 2

- full implementation allows multiple charsets per sub-keyspace
- lets just look at hybrid2 with 1 charset per sub-keyspace first
- [A-Z][a-z]{5}[a-z0-9]{2}[0-9]{1,3}

$$\begin{aligned} \text{keySpace} &= 26 * 11,881,376 * 1296 * 1110 \\ &= 444,393,878,722,560 \approx 2^{48.6588} \end{aligned}$$

- reduction function applied per sub-keyspace
- effectively apply IndexToPlain to [A-Z], then [a-z]{5} , concatenate, and continue
- limited to only the final charset having variable length

Sub-keyspaces Part 1

- per position charsets of different lengths
- multiple charsets per position
- allows the table set to be ordered for faster attacks
- possibilities get fairly interesting

Sub-keyspaces Part 2

- Sc00bz tells us that for keyspaces like Omni6 to encode the key space with the sub-keyspaces increasing to keep consistent with the RC reduction function. This is so that converting an index to a password can search for the most likely sub-keyspace to least likely. [2]

Sub-keyspaces Part 3 - Omni6 [4] a tribute to Sc00bz

*****

******

MMMMMMM

Mnnnnnnn

maaaaaaaa

000000000

0000000000

00000000000

000000000000

maaaa0000

maaaaa000

maaaaaa00

maaaaaaa0

maaaaa0000

maaaaaa000

$*$ – 95 characters: space through ~

M – 62 characters: A-Z, a-z, and 0-9

m – 52 characters: A-Z and a-z

n – 36 characters: a-z and 0-9

a – 26 characters: a-z

0 – 10 characters: 0-9

Sub-keyspaces Part 4 - Omni6 a tribute to Sc00bz

- encoded for RC reduction function use

000000000	2^29.897	1.65 MiB
*****	2^32.849	12.97 MiB
0000000000	2^33.219	0
00000000000	2^36.541	217.59 MiB
maaaa0000	2^37.790	470.48 MiB
******	2^39.419	1.42 GiB
000000000000	2^39.863	1.94 GiB
maaaaan00	2^41.016	4.36 GiB
MMMMMMM	2^41.679	7.00 GiB
Mnnnnnnn	2^42.144	9.65 GiB
maaaaaaan	2^43.773	32.44 GiB
maaaaan000	2^44.338	47.98 GiB
total	2^45.506	105.69 GiB

Sub-keyspaces Part 5 - Omni6 a tribute to Sc00bz

add(numeric#9-9,
mixalpha-numeric-all-space#5-5,
numeric#10-11,
hybrid2(mixalpha#1-1,loweralpha#4-4,numeric#4-4),
mixalpha-numeric-all-space#6-6,
numeric#12-12,
hybrid2(mixalpha#1-1,loweralpha#5-5,loweralpha-numeric#1-1,numeric#2-2),
mixalpha-numeric#7-7,
hybrid2(mixalpha-numeric#1-1,loweralpha-numeric#7-7),
hybrid2(mixalpha#1-1,loweralpha#7-7,loweralpha-numeric#1-1),
hybrid2(mixalpha#1-1,loweralpha#5-5,loweralpha-numeric#1-1,numeric#3-3))

433 characters

Contact information

- James Nobis (quel)
- quel@quelrod.net
- http://www.freerainbowtables.com
- GPG
  - pub 4096R/8B429E16 2010-02-05
  - 934B 3013 6826 BF6B BE93 750A 8081 124C 8B42 9E16
  - uid James Nobis quel@quelrod.net
  - sub 4096g/0312862A 2010-02-05
  - sub 4096R/A35ECB2E 2010-02-05
  - sub 4096R/F7C0F683 2010-11-25

FRT Links

- http://www.freerainbowtables.com
- http://gitorious.org/freerainbowtables-applications
- http://rcracki.sourceforge.net
- http://www.tbhost.eu
- http://boinc.freerainbowtables.com/distrrtgen
- http://boinc.berkeley.edu

Non-FRT Links

- http://www.cryptohaze.com
- http://www.project-rainbowcrack.com
- http://ophcrack.sourceforge.net
- http://www.iacr.org
- http://eprint.iacr.org/complete
- http://www.acm.org

References

- [Nobis, 2010] James Nobis. "Rainbow Tables Past, Present, and Future." Passwords^10. 2010. Web. 09 Dec. 2010. http://insomnia.quelrod.net/docs/passwords_10_frt.pdf http://ftp.ii.uib.no/pub/passwords10/James_Nobis_at_Passwords10.m
- [PowerBlade, 2009] PowerBlade, Martin Jørgensen. "RTI2 file format." FRT. 2009. Web. 11 Nov. 2010. http://www.freerainbowtables.com/phpBB3/topic1217.html.
- [Sc00bz, 2010] Sc00bz, Steve Thomas. "RTI2 header format." FRT. 2010. Web. 28 May. 2011. http://freerainbowtables.com/phpBB3/post16006.html#p16006.
- [RainbowCrack Project, 2011] RainbowCrack Project. "Rainbow Table File Format". RainbowCrack Project. 2011. Web. 28 May. 2011. http://project-rainbowcrack.com/file_format.htm.

References 2

- [FRT, 2011] "next table to generate." FRT. 2011. Web. 23 Apr. 2011. http://www.freerainbowtables.com/phpBB3/topic2559-30.html
- [Sc00bz, 2010] Sc00bz, Steve Thomas. "RTI2 header format." FRT. 2010. Web. 28 May. 2011. http://freerainbowtables.com/phpBB3/post16018.html#p16018
- [Sc00bz, 2011] Sc00bz, Steve Thomas. "Omni." TOBTU. 2011. Web. 28 May. 2011. http://www.tobtu.com
- [Sc00bz, 2011] Sc00bz, Steve Thomas. "Advanced Rainbow Table Calculator." TOBTU. 2011. Web. 28 May. 2011. http://www.tobtu.com/rtcalc.php.

Licensing