

PASSWORD ATTACKS AND GENERATION STRATEGIES

Predrag Tasevski

Tartu University, Faculty of Mathematics and Computer Sciences, major: Master of Science in Cyber Security

May 21, 2011

Table of contents

Introduction

Methods

- Ad-hoc models

- Brute force

- Rainbow tables

Examples and tools

Comparison of input dictionary list

Test

Conclusion

INTRODUCTION

Password is a secret word or string of characters that is used for authentication in order to prove identity or gain access to a resource[Gill(1997)].

- ▶ Usage of password cracking tools
- ▶ Methods and approaches guessing the passwords
- ▶ Examples of leaks and generating password dictionaries
- ▶ Comparison of already cracked passwords from available password dictionaries and
- ▶ Test

METHODS

Password cracking is a method of guessing the attack.

Types of password cracking methods[Vines(2007)]:

- ▶ Dictionary
- ▶ Hybrid
- ▶ Brute force

Ad-hoc models

Dictionary attacks - colander rules

Example

Capitalization the first letter, adding three digits to the end, changing the letter 'a' to '@' etc.

Hybrid it adds simple numbers or symbols to the password attempt.

Brute force

Brute force are fraction of the total words that are made by users creating their passwords.

Brute force attacks methods:

- ▶ Pure brute force [Group(2010)]
- ▶ Letter frequency analysis attack [Stitson(2003)]
- ▶ Markov models [Shmatikov Arvind(2005)]
- ▶ Targeted brute force attacks [WEIR(2010b)]

Rainbow tables (1)

Rainbow tables are using the reduction functions to create multiple parallel chains within a single "rainbow" table.

- ▶ Increases the probability of a correct crack for a given table size, the use of multiple reduction functions also greatly increases the speed of look-ups [JeffXChen(2011)].
- ▶ Hash function [Oechslin(2003)], later on developed more powerfull tool RainbowCrack(including: LM hash, MD5, SHA1, and NTLM) [JeffXChen(2011)].
- ▶ Benefit is of using the tables over and over again after creating one [Gates(2011)].

Rainbow tables (2)

- ▶ Index value ranges from 0 to (key max-1) [Kuliukas(2006)].
- ▶ Three main functions: *IndexToPlain*, *PlainToHash*, and *HashToIndex* [Kuliukas(2006)].

Example

If the attacker was trying to brute force all seven character long words which contains only lower cases letters the key max would be 26^7 .

EXAMPLES AND TOOLS (1)

- ▶ On-line password cracking: THC Hydra and NCrack (run by very small input dictionaries) [WEIR(2010a)].
- ▶ Offline password cracking attacks:
 - ▶ John the Ripper [Group(2010)].
 - ▶ Cain & Able [Montoro(2011)].
 - ▶ L0phtcrack[L0pht Holdings(2009)].
 - ▶ Elcomsoft Distributed Password Recovery [Ltd(2011)].
 - ▶ AccessData Password Recovery Toolkit [AccessData(2011)].
 - ▶ TC Brute [IsNull(2010)].

EXAMPLES AND TOOLS (2)

Finding and creating input dictionaries.

Available:

- ▶ Skull Security [Bowes(2011)] by Ron Bowes.
- ▶ Facebook User Directory [Facebook(2011)].
- ▶ WikiGrabber command line tool that builds custom dictionaries by spidering/crawling [Wikipedia.org(2011)].
- ▶ Wiktionary <http://www.wiktionary.org/>.
- ▶ Python source code developed for password dictionary generator by Travis Altman [Altman(2010)].

EXAMPLES AND TOOLS (3)

- ▶ DRCrack

<https://sites.google.com/site/reusablesec2/drcrack>
dictionary based on rainbow table (Rcrack -
<http://www.project-rainbowcrack.com/>).

- ▶ Objectif Sécurité:

<https://www.objectif-securite.ch/en/index.php> open source applications using rainbow tables, for office documents or system passwords.

- ▶ Probabilities of passwords are calculated systematically from an existing list of plain-text passwords which measures the frequencies of certain patterns and the characters that are used [Weir(2010)].

COMPARISON OF INPUT DICTIONARY LIST [Bowes(2011)]

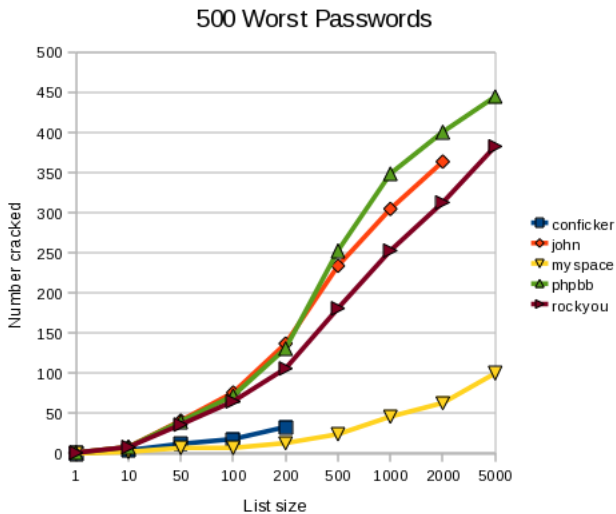


Figure: 500 worst passwords

Elitehackers-(zf05.txt) & Hak5 [Bowes(2011)]

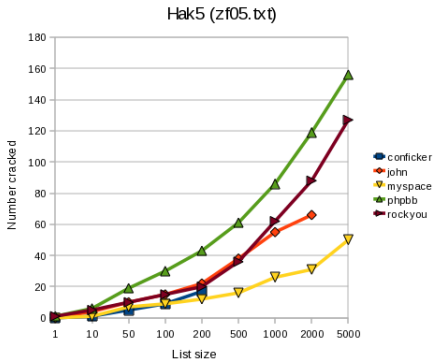
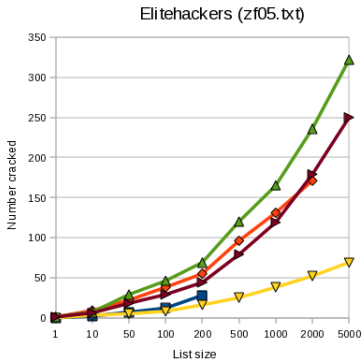


Figure: Elitehackers-(zf05.txt) & Hak5

Faithwriters [Bowes(2011)]

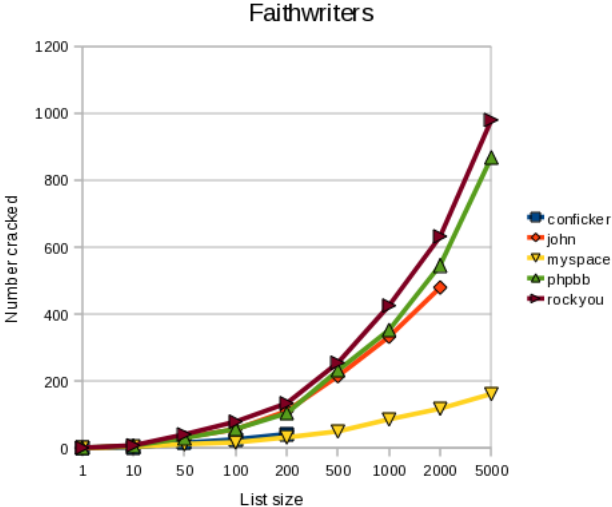


Figure: Faithwriters

Phpbb & Rockyou [Bowes(2011)]

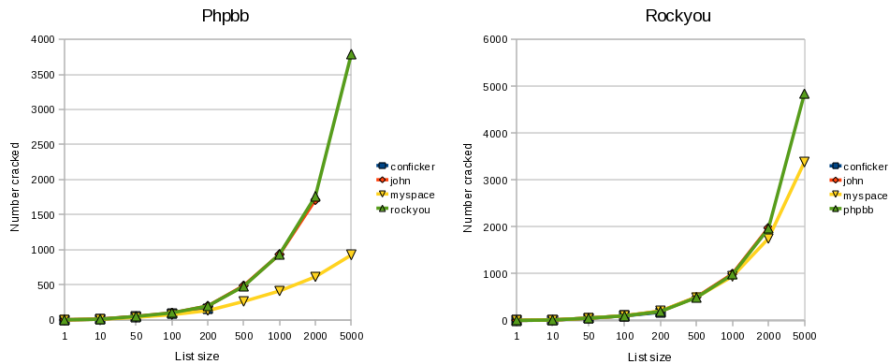


Figure: phpbbs & rockyou

TEST

- ▶ First approach is with the tools John the Ripper and Cain & Able.
 - ▶ System hash password file were tested of performing password cracking with an input dictionaries and different character password strength with different methods.
- ▶ Second approach is with the tool TC Brute where two virtual drives were encrypted with different passwords by the TrueCrypt application.
 - ▶ Brute force method performed with different input password dictionaries and different password strength.

Proof.

Test with TC Brute, two simulations.



CONCLUSION

- ▶ Methods and techniques can conduct password cracking:
 - ▶ on-line or
 - ▶ offline environment
- ▶ Tools that can guess the passwords.
- ▶ Input dictionaries with different languages.
- ▶ Passwords must be both reasonable and functional for the end user as well as strong enough for the intended purpose.
- ▶ To insure for the potential needs of: preventing password cracking, information security audit, password recovery, security policy, etc.

THANKS AND QUESTIONS

THANKS AND QUESTIONS?

predrag@ut.ee



AccessData.

Password recovery toolkit® (prtk®), 2011.

URL [http:](http://accessdata.com/products/forensic-investigation/decryption#passwordrecoverytoolkit)

[//accessdata.com/products/forensic-investigation/decryption#passwordrecoverytoolkit.](http://accessdata.com/products/forensic-investigation/decryption#passwordrecoverytoolkit)



Travis Altman.

Password dictionary generator.

<http://travisaltman.com/>, 2010.

URL [http:](http://travisaltman.com/password-dictionary-generator/)

[//travisaltman.com/password-dictionary-generator/.](http://travisaltman.com/password-dictionary-generator/)



Ron Bowes.

Passwords, January 2011.

URL [http:](http://www.skullsecurity.org/wiki/index.php/Passwords)

[//www.skullsecurity.org/wiki/index.php/Passwords.](http://www.skullsecurity.org/wiki/index.php/Passwords)



Facebook.

Facebook user directory.

<https://www.facebook.com/directory/>, 2011.

URL [https://www.facebook.com/directory/.](https://www.facebook.com/directory/)



Chris Gates.

Tutorial: Rainbow tables and rainbowcrack.

Tutorial, 2011.

URL

<http://www.ethicalhacker.net/content/view/94/24/>.



N.S. Gill.

The roman military system, 1997.

URL http://ancienthistory.about.com/library/bl/bl_text_polybius6.htm.



The OpenWall Group.

John the ripper password cracker.

<http://www.openwall.com/>, 2010.

URL <http://www.openwall.com/>.

Openwall Project - Information Security software for open environments.



IsNull.

Tcbrute, July 2010.

URL http://securityvision.ch/index.php?option=com_content&view=article&id=51&Itemid=58.



JeffXChen.

Rainbow table, April 2011.

URL https://secure.wikimedia.org/wikipedia/en/wiki/Rainbow_table.



Kestas Chris Kuliukas.

How rainbow tables work.

kestas.kuliukas.com; Kestas home page, 2006.

URL <http://kestas.kuliukas.com/RainbowTables/>.



LLC L0pht Holdings.

L0phtcrack password auditor.

L0phtCrack Password Auditor, 2009.

URL <http://www.l0phtcrack.com/>.



ElcomSoft Co. Ltd.

Elcomsoft products, 2011.

URL <http://www.elcomsoft.com/products.html>.



Massimiliano Montoro.

oxid.it web site.

oxid.it web site, 2011.

URL <http://www.oxid.it/index.html>.



Philippe Oechslin.

Making a faster cryptanalytic time-memory trade-off, 2003.

URL http://lasecwww.epfl.ch/php_code/publications/search.php?ref=0ech03.



Narayanan Vitaly Shmatikov Arvind.

Fast dictionary attacks on passwords using timespace.

Technical report, The University of Texas at Austin, 2005.



L. Stitson.

Intro to cryptography notes, 7 2003.

URL http://www.stanford.edu/~stinson/crypto/S3995/class_3.txt.



Russell Dean Vines.

Ethical hacking tools and techniques: Password cracking.

searchsecuritychannel.techtarget.com, 2007.

URL http://searchsecuritychannel.techtarget.com/generic/0,295582,sid97_gci1236496_mem1,00.html?ShortReg=1&mbxConv=searchSecurityChannel_RegActivate_Submit&.



CHARLES MATTHEW WEIR.

Using Probabilistic Techniques To Aid In Password Cracking Attacks.

PhD thesis, The Florida State University, 2010a.



CHARLES MATTHEW WEIR.

Middlechild password cracker.

Reusable Security Tools:

<https://sites.google.com/site/reusablesec/Home/password-cracking-tools/middle-child>, 2010b.

URL <https://sites.google.com/site/reusablesec/Home/password-cracking-tools/middle-child>.



Matt; Sudhir Aggarwal; Breno de Medeiros; Bill Glodek Weir.
Password cracking using probabilistic context-free grammars.

Technical report, Internet Security Seminar, 2010.



Wikipedia.org.

Web crawler.

Wikimedia.org;, 2011.

URL https://secure.wikimedia.org/wikipedia/en/wiki/Web_crawler.