Department of CEE/ Computer Science

How Secure is your Password?

GPU Password Cracking

Alwin Villamor, Cassandra Sanchez, & Ebony Turner

Advisor: Dr. Melissa Danforth Assistant: Alfonso Puga

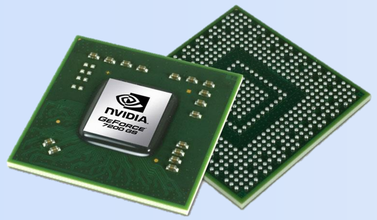
CSU Bakersfield

Chevron

Research Experience Vitalizing Science – University Program

Partial support for this work was provided by the National Science Foundation's Federal Cyber Service: Scholarship for Service (SFS) program under Award No. 1241636.

Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.



What are GPUs?

GPUs are single-chip processors primarily used to manage and/or provide the performance of video and graphics.

Why are GPUs used for cracking passwords?

GPUs are excellent at processing mathematical calculations and it has hundreds if not thousands of cores that can be used to compute multiple mathematical functions simultaneously. Basically, it is much faster to use a GPU for password cracking.

How password cracking works?

In our world of technology, there are two ways passwords are cracked. Either hackers try to crack your password by using simple logic or tools.

Methods:

Simple Logic	Tools
• Name Combinations • Hobbies • Important Years/ Numbers	• Dictionaries • Attacks • Rules

Simple logic hackers, may be a close friend or an associate, use personal/ public information already know about you to guess your password.

Dictionaries attacks scan through lists of preset words, phrases, and common passwords.

Brute-force attacks use every possible combination of letters, digits, and symbols to decrypt passwords.

Examples:

	Combinations	Possible Passwords
Password has 6 digits	10 x 10 x 10 x 10 x 10 x 10	1,000,000
Password has 6 symbols	32 x 32 x 32 x 32 x 32 x 32	1,073,741,824
Password has 6 letters (lowercase)	26 x 26 x 26 x 26 x 26 x 26	308,915,776
Password has 6 characters (lowercase, uppercase, digits, & symbols)	94 x 94 x 94 x 94 x 94 x 94	689,869,781,056

Time Trials

NVIDIA				
	MD5	SHA1	SHA256	SHA512
Dictionary Attack (large.dict)	3 mins	5 mins	8 mins	35 mins
Combo Attack (large.dict/ common_passwords.dict)	3 days 10 hrs	7 days 4 hrs	15 days 3 hrs	42 mins
a 6 (Word+Pattern)	2 yrs 28 days	4 yrs 319 days	9 yrs 360 days	> 10 yrs
a 7 (Pattern+Word)	1 yr 347 days	4 yrs 359 days	> 10 yrs	> 10 yrs

Using the multiple hash types, such as: MD5, SHA1, SHA256, & SHA512, we calculated the times differences between attacks and GPUs- NVIDIA & ATI/AMD.

Attacks:

- -a 0 (one dictionary attack)
- -a 1 (two dictionary attacks)
- -a 3 (brute force attack)
- -a 6 (Word + Pattern attack)
- -a 7 (Pattern + Word)

Rules:

- ?u : uppercase
- ?l : lowercase
- ?s : symbols
- ?d : digits
- ?a : all

Dictionaries:

- large.dict (7070 words)
- example.dict (129988 words)
- common_passwords.dict (3548 words)
- english_lower.dict (439833 words)
- combo2.dict (9025 words)
- combo3.dict (857375 words)

ATI/ AMD				
	MD5	SHA1	SHA256	SHA512
Dictionary Attack (large.dict)	10 secs	16 secs	28 secs	39 secs
Combo Attack (large.dict/ common_passwords.dict)	41 mins	1 hr 39 mins	3 hrs 45 mins	11 hrs 42 mins
a 6 (Word+Pattern)	11 days 14 hrs	5 yrs 145 days	28 days 5 hrs	265 days 2 hrs
a 7 (Pattern+Word)	8 days 20 hrs	22 days 9 hrs	82 days 22 hrs	132 days

Tips

What makes a weak password?

- Is typically 8 characters or less
- Has common password patterns
- Is relevant to previous password
- Contains some public/ personal information about yourself

Ex: Special Dates
Names
etc.

What makes a strong password ?

- Is longer than 8 characters
- Has multiple characters and/ or difficult phrases
- Is (in no relation) connected to you personal or publicly

14 Passwords Decrypted	42 Total Passwords	
example.dict •gogo •control •ferrari •pandora •kittykat •Password large.dict • nectarine • bowlnoodle combo3.dict/ example.dict •345qwerty combo2.dict/ english_lower.dict •@pplications english_lower.dict/ large.dict •phishfood common_passwords.dict •irishpanda	• bowlnoodle • irishpanda • trolltrolltroll • pandora • ferrari • control • gogo • nectarine • sudoku • password • phishfood • kittykat • jellyman • dix76Ta2zbp • sW@G_Daddy • LoLoLoLoL • Sux0.0nach • L0ck_me_7own • Ab_9287 • G_O_g_0 • 1sand_wich • @pplications • L33Th4x0r • Fos_U.BuLLdoGs	• LoGpass775 • twe20ntyb_ts • !axG@b#164Z:"dYMnfF0 • Ab3Zh3110 • Lag#Wth#f@k • j}#La74Def(m8!)! • X@rs790k • G_O_g_0_7X • what!I-had4BREAKFAST(: • \(._.)/?!.@# •@LLy*VRB453RBelongZU5 • (T%aP$:#Mo • 147HL25+kM72‖L • highway123 • HelloWorld • 345qwerty • Help-Me •YouKilledKenny • tagM1B1Hh

References

Hashcat*: http://hashcat.net/oclhashcat/*

GPU*: http://en.wikipedia.org/wiki/Graphics_processing_unit*

Password tips: *http://www.connectsafely.org/tips-to-create-and-manage-strong-passwords/*

Methods for password cracking: http://www.infosecisland.com/blogview/18538-Top-Ten-Password-Cracking-Methods.html