Trinity College Dublin
Coláiste na Tríonóide, Baile Átha Cliath
The University of Dublin

Scalable Computing

Practical assignment 4 - Break more hashes

Ashutosh Sharma (18304203)
sharmaas@tcd.ie

Date 1/11/2018

CPU's vs GPU's

Q. Which one is better?

Ans. Depends on the computational task.

CPU: https://i.ebayimg.com/images/a/(KGrHqYOKocE35g,etHUBOB)iz3wT!~~/s-l640.jpg
GPU: https://rs3.sinahk.net/cap/3/2018/08/21/f/fcfe797313d866e8f9453121b3420aa5.jpg

Explanation:

Why use GPU’s instead of CPU’s for hash cracking?

- CPU’s are slow at cracking hashes because they have limited cores mostly 4-8 cores. A CPU core is faster at solving a problem which cannot be further subdivided into small tasks than GPU but still, it is a single core.

- GPU’s has 1000s of cores. Each GPU’s single core is slower than CPU’s single core but still, GPU has 1000s of cores. A hashing problem can be divided and run in parallel on all the GPU cores. Thus GPU’s are faster than CPU’s.

More on CPU’s vs GPU’s

	Comparison	
	CPU i7-9700K*	GPU 2080 Ti**
Clock speed	3.60 GHz to 4.90 GHz	1.65 GHz
Cores	8 Cores and 8 Threads	3584 Cuda Cores

* : https://ark.intel.com/products/186604/Intel-Core-i7-9700K-Processor-12M-Cache-up-to-4-90-GHz-
** : https://www.nvidia.com/en-us/geforce/graphics-cards/rtx-2080-ti/

Methodology

2000 — hashes to crack

Q1. Type of hash formats?

- No clue? Don't worry "**JohnTheRipper**" helps!

Q2. Which wordlist to use?

- Used most common wordlist from the internet i.e. "**Rockyou**".

Q3. Which hash cracking tool to use?

- Depends which tool works. Example: hashcat does not support argon2 but JTR does.

https://avatars2.githubusercontent.com/u/1268598?s=400&v=4
https://www.google.ie/url?sa=i&source=images&cd=&ved=2ahUKEwiQisSk6rHeAhVL_qQKHeZJB0kQjRx6BAgBEAU&url=https%3A%2F%2Fwww.zdnet.com%2Farticle%2Fhashcat-password-cracker-goes-open-source%2F&psig=AOvVaw275bDETIjfBzFnPhqNlL2r&ust=1541114832875725

Methodology

1. Crack some hashes of easier format like “**descrypt**”/ “**MD5**” using “**rockyou**” wordlist.

2. Attempt few “**brute-force**” attacks on “**descrypt**”. Like

   a) Digit of length 1-5

   b) Lowercase alphabets 1-5

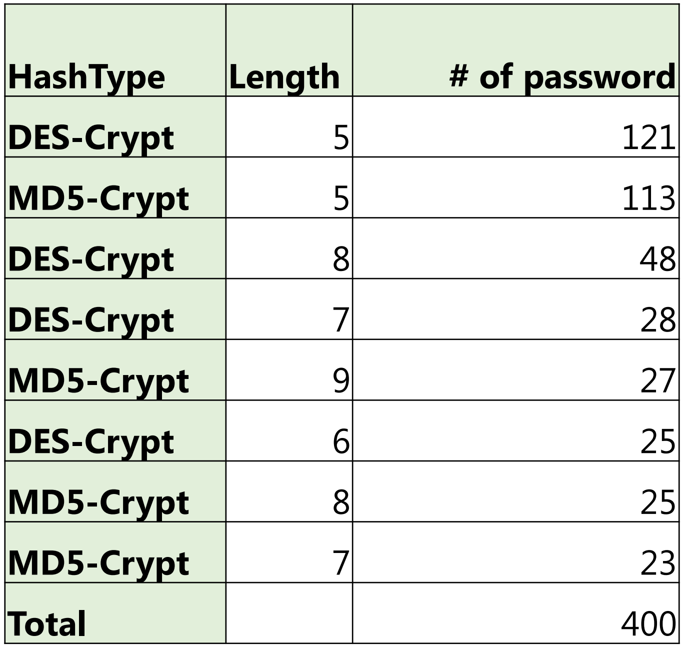
   c) Alpha Numeric 1-5

   d) Lowercase alphabets 5-8 for a short duration

Contd.

- The “**rockyou”** and “**Bruteforce**” attack sessions provided 400 passwords out of 700 (MD5 and descrypt).
- Next step, analyze the password to find the pattern. As there was a hint that assignment contains 3 kinds of passwords.
  1. Type 1 : Rockyou
  2. Type 2 and Type 3 : Unknowns

Finding Pattern



HashType	Length	# of password
DES-Crypt	5	121
MD5-Crypt	5	113
DES-Crypt	8	48
DES-Crypt	7	28
MD5-Crypt	9	27
DES-Crypt	6	25
MD5-Crypt	8	25
MD5-Crypt	7	23
Total		400

- The table provided the intuition about the potential password pattern.
- Maximum passwords were of length 5 and 8

Deep dive the 5 and 8 length passwords to find the pattern:

Hash Format	password	Length
DES-Crypt	aphuw	5
DES-Crypt	azohz	5
DES-Crypt	beequ	5
DES-Crypt	chahy	5
DES-Crypt	aerae	5
DES-Crypt	aeshu	5
DES-Crypt	ahbei	5
DES-Crypt	ahche	5
DES-Crypt	ahfoj	5
DES-Crypt	ahnoh	5
DES-Crypt	ahnoo	5
DES-Crypt	ahrei	5
DES-Crypt	aijoz	5

Hash Format	password	Length	Right 4 char	Right 4 char
DES-Crypt	fuckadam	8	fuck	adam
DES-Crypt	sexymama	8	sexy	mama
DES-Crypt	pullsums	8	pull	sums
DES-Crypt	soccerma	8	socc	erma
DES-Crypt	solibabe	8	soli	babe
DES-Crypt	tavonias	8	tavo	nias
DES-Crypt	valenzon	8	vale	nzon
DES-Crypt	cpatrick	8	cpat	rick
DES-Crypt	ashaunti	8	asha	unti
DES-Crypt	shellyma	8	shel	lyma
DES-Crypt	amirasyu	8	amir	asyu
DES-Crypt	hottiemn	8	hott	iemn
DES-Crypt	karlitat	8	karl	itat

Key Insights:

1. GPU’s are more efficient but instances are costly ☹.
2. More efficient to run JTR in parallel on CPU while running hashcat on GPU.
3. Argon 2 does not supports GPU side ways attacks. Thus hashcat does not supports this format and it is kind of useless to try to crack argon2 using GPU.
4. Argon2 was the strongest hash formats out of the given hash formats.

Limitations

1. Hashcat didn’t support the given PBKDF2 format. JTR OpenCL mode was a better alternative approach.
2. Argon2 super difficult hash algorithm to crack.
3. The assignment was very time-consuming.

Any questions?

Trinity College Dublin
Coláiste na Tríonóide, Baile Átha Cliath
The University of Dublin

Thank You