BRUTE FORCE PASSWORD CRACKING DENGAN MENGGUNAKAN GRAPHIC PROCESSING POWER

Himawan Pramaditya
Fakultas Teknologi Informasi Universitas Merdeka Malang
h.pramaditya@gmail.com

Abstract

Password created to secure something against access from unauthorized persons. The longer the password created increasingly long and complex with a view to improving safety. Graphic processing unit can be used as a suitable medium to guess a password combinations quickly. This was due to a combination of password guessing process is in accordance with the architecture of a graphics processing unit that typically consist of hundreds or thousands of simple processing cores per unit. With the rapid development of technology in the field of processing power, a process that used to guess a password might take decades can now be done in just a matter of hours.

Keywords : GPU, password cracking, brute force, security

1. PENDAHULUAN

Dewasa ini perkembangan teknologi informasi terutama di bidang processing unit sangatlah pesat dibanding dengan beberapa tahun silam. Masih ada diingatan kita semua bahwa beberapa tahun yang lalu komputer dan laptop kita masih dibekali dengan processor ber inti tunggal yang berkecepatan hanya pada hitungan puluhan hingga ratusan megahertz. Namun sekarang tidak aneh jika kita menemui sebuah processor yang memiliki lebih dari satu inti yang tiap-tiap intinya berkecepatan beberapa gigahertz.

Salah satu cabang *processing power* yang mengalami peningkatan yang amat pesat adalah di bidang *Graphic Processing Unit* (GPU). Berbeda dengan unit CPU pada umumnya yang dibekali dengan beberapa core namun setiap corenya dirancang untuk mampu menangani berbagai instruksi yang panjang dan rumit, GPU didesain khusus untuk menangani proses rendering grafis dimana mereka hanya dituntut untuk melakukan instruksi sederhana berulang-ulang namun dengan kecepatan yang amat tinggi.

Oleh karena tipikal beban kerja yang seperti itu, seringkali GPU hanya dibekali dengan processing core sederhana namun dalam jumlah yang amat banyak mulai ratusan hingga ribuan core per unitnya.

Pengolahan rendering grafis yang bersifat sederhana dan repetitif ternyata sangat cocok digunakan untuk menebak kombinasi password secara *brute force* yang sederhana dan hanya membutuhkan kecepatan.

Sesuai dengan latar belakang yang telah disampaikan di atas maka perumusan masalah yang dibahas adalah bagaimana cara menggunakan GPU sebagai produk yang sesuai untuk tugas pembobolan password.

Tujuan penelitian ini adalah untuk mengukur kemampuan dan keefektifan sebuah graphic processing unit dalam menebak suatu kombinasi password melalui metode *brute force*.

Password

Password adalah sandi atau kata rahasia berupa string karakter tertentu yang digunakan untuk meng-otentikasi seseorang untuk membuktikan bahwa dirinya berhak untuk mendapatkan akses terhadap sesuatu yang harus dirahasiakan dari mereka yang tidak memiliki akses.

Password atau sandi telah digunakan sejak zaman kuno. Bahkan oleh sejarawan kuno yunani Polybius dijelaskan bahwa sistem password telah digunakan pada sistem militer kekaisaran romawi.

Meskipun terdiri dari kata -word, namun bukan berarti sebuah password harus terdiri dari sebuah kata-kata, namun dapat juga berupa susnan karakter yang sulit untuk ditebak. Password kadang dapat terdiri dari beberapa suku kata sehingga bisa disebut dengan passphrase. Beberapa bentuk lain menggunakan serangkaian angka-angka seperti pada mesin ATM yang disebut dengan *passcode*. Password umumnya cukup pendek untuk dapat dengan mudah diingat dan diketik.

Kebanyakan organisasi menentukan kebijakan password yang berbeda-beda pada komposisi dan penggunaan password, biasanya dalam hal panjang karakter minimum, kategori yang diperlukan (misalnya huruf besar dan kecil, angka, dan karakter khusus), dan unsur-unsur yang dilarang (misalnya namanya sendiri, tanggal lahir, alamat , nomor telepon).

Password telah digunakan dengan komputer sejak awal masa komputasi. CTSS MIT, salah satu sistem sharing pertama di dunia yang diperkenalkan pada tahun 1961 memiliki perintah LOGIN yang meminta password pengguna. Pada saat user mengetikkan PASSWORD, sistem mematikan mekanisme pencetakan, sehingga pengguna dapat mengetikkan password dengan privasi. Pada awal 1970-an, Robert Morris menemukan gagasan untuk menyimpan password login dalam bentuk hash sebagai bagian dari sistem operasi Unix . Sistem ini didasarkan pada simulasi terhadap mesin kriptografi Hagelin rotor, dan pertama kali muncul dalam Edisi 6 Unix pada tahun 1974 .

Central Processing Unit

Menurut Wikipedia Central Processing Unit atau lazim disebut processor adalah perangkat keras Komputer Yang memahami Dan melaksanakan perintah Dan Data Bahasa Dari perangkat Lunak. Istilah Lain, pemroses / prosesor (processor), sering digunakan untuk menyebut CPU. Adapun mikroprosesor adalah CPU Yang diproduksi Dalam, sirkuit Terpadu, seringkali Dalam, sebuah paket Negara sirkuit Terpadu-Tunggal. Sejak pertengahan 1970-an years, mikroprosesor sirkuit Terpadu-Tunggal inisial telah digunakan UMUM Dan menjadi ASPEK Penting Dalam, penerapan CPU.

CPU berfungsi seperti kalkulator, hanya saja CPU jauh lebih kuat daya pemrosesannya. Fungsi utama dari CPU adalah melakukan operasi aritmatika dan logika terhadap data yang diambil dari memori atau dari informasi yang dimasukkan melalui beberapa perangkat keras, seperti papan tombol, pemindai, tuas kontrol, maupun tetikus. CPU dikontrol menggunakan sekumpulan instruksi perangkat lunak komputer. Perangkat lunak tersebut dapat dijalankan oleh CPU dengan membacanya dari media penyimpan, seperti cakram keras, disket, cakram padat, maupun pita perekam. Instruksi-instruksi tersebut kemudian disimpan terlebih dahulu pada memori fisik (MAA), yang mana setiap instruksi akan diberi alamat unik yang disebut alamat memori. Selanjutnya, CPU dapat mengakses data-data pada MAA dengan menentukan alamat data yang dikehendaki.

Saat sebuah program dieksekusi, data mengalir dari RAM ke sebuah unit yang disebut dengan bus, yang menghubungkan antara CPU dengan MAA. Data kemudian didekode dengan menggunakan unit proses yang disebut sebagai pendekoder instruksi yang sanggup menerjemahkan instruksi. Data kemudian berjalan ke unit aritmatika dan logika (ALU) yang melakukan kalkulasi dan perbandingan. Data bisa jadi disimpan sementara oleh ALU dalam sebuah lokasi memori yang disebut dengan register supaya dapat diambil kembali dengan cepat untuk diolah. ALU dapat melakukan operasi-operasi tertentu, meliputi penjumlahan, perkalian, pengurangan, pengujian kondisi terhadap data dalam register, hingga mengirimkan hasil pemrosesannya kembali ke memori fisik, media penyimpan, atau register apabila akan mengolah hasil pemrosesan lagi. Selama proses ini terjadi, sebuah unit dalam CPU yang disebut dengan penghitung program akan memantau instruksi yang sukses dijalankan supaya instruksi tersebut dapat dieksekusi dengan urutan yang benar dan sesuai.

Graphic Processing Unit

Menurut Wikipedia *Graphics processing unit* atau GPU (atau biasa juga disebut visual processing unit atau VPU) adalah sebuah prossesor khusus untuk untuk bagian grafis dari microprocessor. Alat ini digunakan di sistem benam, telepon genggam, komputer pribadi, workstation, dan konsol game. GPU Modern sangat efisien dalam memanipulasi komputer grafis dan struktur paralel, membuatnya lebih efektif dari fungsi umum CPU yang digunakan untuk bebagai perhitungan algoritma. Pada komputer pribadi (PC), GPU biasanya terdapat di video card atau di motherboard. Sebagian lain dari komputer desktop dan notebook mempunyai GPU yang terintegrasi, yang biasanya jauh lebih lambat kemampuannya daripada yang menggunakan *video card discrete.*

Brute Force

Menurut Wikipedia Serangan brutal (bahasa Inggris: *Brute-force attack*) adalah sebuah teknik serangan terhadap sebuah sistem keamanan komputer yang menggunakan percobaan terhadap semua kunci yang mungkin. Pendekatan ini pada awalnya merujuk pada sebuah program komputer yang mengandalkan kekuatan pemrosesan komputer dibandingkan kecerdasan manusia. Sebagai contoh, untuk menyelesaikan sebuah persamaan kuadrat seperti $x^2+7x-44=0$, di mana x adalah sebuah integer, dengan menggunakan teknik serangan *brute-force*, penggunanya hanya dituntut untuk membuat program yang mencoba semua nilai integer yang mungkin untuk persamaan tersebut hingga nilai x sebagai jawabannya muncul. Istilah brute force sendiri dipopulerkan oleh Kenneth Thompson, dengan mottonya: "*When in doubt, use brute-force*" (jika ragu, gunakan *brute-force*).

Teknik yang paling banyak digunakan untuk memecahkan password, kunci, kode atau kombinasi. Cara kerja metode ini sangat sederhana yaitu mencoba semua kombinasi yang mungkin.

Sebuah password dapat dibongkar dengan menggunakan program yang disebut sebagai password cracker. Program *password cracker* adalah program yang mencoba membuka sebuah password yang telah terenkripsi dengan menggunakan sebuah algoritma tertentu dengan cara mencoba semua kemungkinan. Teknik ini sangatlah sederhana, tapi efektivitasnya luar biasa, dan tidak ada satu pun sistem yang aman dari serangan ini, meski teknik ini memakan waktu yang sangat lama, khususnya untuk password yang rumit.

Namun ini tidak berarti bahwa password cracker membutuhkan *decrypt*. Pada prakteknya, mereka kebayakan tidak melakukan itu. Umumnya, kita tidak dapat melakukan *decrypt* password-password yang sudah terenkripsi dengan algoritma yang kuat. Proses-proses enkripsi modern kebanyakan hanya memberikan satu jalan, di mana tidak ada proses pengembalian enkripsi. Namun, anda menggunakan tool-tool simulasi yang mempekerjakan algoritma yang sama yang digunakan untuk mengenkripsi password orisinal. Tool-tool tersebut membentuk analisis komparatif. Program *password cracker* tidak lain adalah mesin-mesin ulet. Ia akan mencoba kata demi kata dalam kecepatan tinggi. Mereka menganut "Azaz Keberuntungan", dengan harapan bahwa pada kesempatan tertentu mereka akan menemukan kata atau kalimat yang cocok. Teori ini mungkin tepat mengena pada anda yang terbiasa membuat password asal-asalan. Dan memang pada kenyataannya, password-password yang baik sulit untuk ditembus oleh program *password cracker*.

2. METODE PENELITIAN

Untuk melakukan penelitian mengenai password cracking dengan menggunakan graphic processing unit dibutuhkan beberapa hal antara lain:

a. Data mengenai kemampuan proses beberapa *Graphic Card* yang sekarang tersedia di pasaran
b. Data mengenai kemampuan proses beberapa CPU yang sekarang tersedia di pasaran sebagai data pembanding.
c. Data mengenai harga setiap komponen baik GPU maupun CPU yang sekarang dijual di pasaran.
d. Data mengenai panjang password yang saat ini umum digunakan sebagi standar keamanan minimal.
e. Data mengenai algoritma enkripsi password yang menjadi standar keamanan baku.
e. Aplikasi untuk mensimulasikan aktifitas *password cracking* yang menggunakan kemampuan proses dari sebuah GPU

3. HASIL DAN PEMBAHASAN

Mencoba menjebol proteksi password secara manual mungkin terlihat seperti upaya yang bodoh, terutama jika Anda sedang berhadapan dengan password yang panjang.

Serangan *brute-force* bergantung pada probabilitas. Semakin panjang password, semakin banyak password yang ada untuk memeriksa. Hal ini bergantung pada teori permutasi, yang merupakan susunan angka dalam urutan tertentu. Jadi pikirkan password sebagai anagram. Jika diberi huruf a, b, dan c, berapa banyak susunan memerintahkan berbeda bisa Anda buat? Dengan hanya tiga huruf, dapat dibuat satu set enam permutasi dari himpunan {a, b, c}, yaitu [a, b, c], [a, c, b], [b, a, c], [b, c, a], [c, a, b], dan [c, b, a].

Namun pada kemungkinan password sederhana. Pengulangan diperbolehkan, sehingga rumus untuk jumlah kemungkinan password **p** untuk ditebak adalah $\mathbf{p} = \mathbf{x}^{\mathbf{n}}$ dimana **x** adalah

jumlah karakter mungkin. Dan **n** adalah panjang password.

Jadi pada perhitungan jumlah kemungkinan password yang ada untuk karakter abjad adalah:

Jenis Kombinasi Abjad	Jumlah kemungkinan Password		
	2 Karakter	4 Karakter	6 Karakter
Abjad kecil	676	456976	308915776
Abjad kecil dan besar	2704	7311616	19770609664
Abjad kecil, besar dan angka	3844	14776336	56800235584
Seluruh karakter ASCII	8836	78074896	689869781056

Seperti yang terlihat, pada enam karakter saja, sudah mendapatkan jumlah kombinasi dalam hitungan miliaran jika dimasukkan huruf kecil dan huruf besar. Jika termasuk karakter khusus dan nomor (semua karakter ASCII), maka akan ditemukan bahwa jumlah calon password meledak menjadi lebih dari tiga-perempat triliun. Dan jangan lupa bahwa jika tidak diketahui panjang password, harus dicari semua kemungkinan kombinasi dari password karakter tunggal dengan panjang yang dipilih.

Untuk mengetes kemampuan memecahkan sebuah password, diperlukan aplikasi untuk mencobanya. Dalam percobaan ini dapat digunakan software WinZIP dan WinRAR karena dapat dicoba untuk menebak password sebanyak-banyaknya tanpa ada batasan kesalahan menebak.

Sebagai pembanding akan dicoba untuk melakukan proses password cracking menggunakan tenaga CPU. Hasil yang didapatkan dengan menggunakan prosesor intel i5-2500k Sandy Bridge yang dijual dipasaran dengan harga sekitar US$ 200 adalah seperti berikut:

Jenis Kompresi dan Enkripsi	Password/Detik
C: - E: Zip 2.0	28 357 311
C: - E: AES 128	9715
C: - E: AES 256	9713
C: Zip E: Zip 2.0	28 492 733
C: Zip E: AES 128	9733
C: Zip E: AES 256	9760

Dengan kecepatan sekitar 28 juta password per detik maka lama waktu yang dibutuhkan untuk memecahkan password adalah:

Jenis Kombinasi	4 Karakter	6 Karakter	8 Karakter	12 Karakter
Abjad Kecil	instan	11 detik	2 jam	112 thn
Abjad Kecil dan Besar	instan	12 menit	22 hari	451345 thn
Seluruh Karakter ASCII	3 detik	7 jam	8 tahun	701193345 thn

Sekarang hasil tersebut akan dibandingkan dengan hasil *brute-force* password dengan menggunakan GPU *GeForce* GTX 460 dengan harga jual yang kurang lebih sama dengan processor intel i5-2500k yaitu pada rentang harga sekitar US$ 200. Untuk mengoptimalkan penggunaan processing power dari GPU tersebut kita menggunakan aplikasi penebak password yang didesain dengan paralelisme tinggi yaitu **Accent Password Recovery**:

Jenis Kompresi dan Enkripsi	Password/Detik
C: Zip E: Zip 2.0	516 096 000
C: Zip E: AES 128	166 800
C: Zip E: AES 256	156 138

Disana dapat dilihat lompatan performa yang sangat signifikan dari 28 juta password per detik menjadi lebih dari 500 juta password per detik. Dengan jumlah password per detik setinggi itu, maka password dapat dipecahkan dalam waktu seperti berikut:

Jenis Kombinasi	4 Karakter	6 Karakter	8 Karakter	12 Karakter
Abjad Kecil	instan	instan	7 menit	5,2 thn
Abjad Kecil dan Besar	instan	instan	23 jam	24918 thn
Seluruh Karakter ASCII	instan	20 menit	161 hari	38711625 thn

Hasil diatas seperti diatas adalah hasil dari percobaan dengan menggunakan GPU level menengah dengan harga 2 jutaan saja. Apabila kita menggunakan platform seperti intel z68 yang mampu untuk mengakomodasi 4 buah GPU secara bersamaan dan menggunakan GPU kelas high end maka angka tadi dapat meningkat berlipat-lipat hingga hitungan 5 milyar password per detiknya. Bahkan ada sebuah mesin dengan nama White Pixel yang mampu memecahkan hingga 28,6 milyar password per detiknya.

Dengan adanya kemampuan bagi sebuah alat untuk menebak hingga milyaran password per detik maka password dengan panjang dibawah 8 karakter sudah tidak aman lagi karena dapat dipecahkan dalam hitungan menit atau bahkan detik saja.

4. KESIMPULAN

1. Peningkatan kemampuan proses dari mikroprosesor dari waktu ke waktu berdampak langsung pada semakin rendahnya tingkat keamanan password.
2. Dengan adanya sistem mikroprosesor yang mampu menghasilkan milyaran kombinasi password per detik dituntut untuk mencari suatu bentuk pengamanan lain

5. REFERENSI

[1] http://en.wikipedia.org/wiki/cpu

[2] http://en.wikipedia.org/wiki/gpu

[3] http://en.wikipedia.org/wiki/brute-force_attack

[4] http://www.tomshardware.com/reviews/password-recovery-gpu.2945.html

[5] http://blog.zorinaq.com/?e=42

[6] http://www.engadget.com/2010/08/16/gpus-democratize-brute-force-password-hacking/

[7] http://hackaday.com/2010/09/27/gpu-processing-and-password-cracking/