Penerapan Kombinatorial untuk Menghitung Kekuatan Sandi dari Serangan *Brute-Force*

[1]Fahziar Riesad Wutono - 13512012
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
[1]13512012@std.stei.itb.ac.id

***Abstract*—Saat ini sandi (*password)* digunakan untuk mengecek apakah seseorang berhak untuk mengakses suatu akun. Pemilihan sandi yang baik diperlukan agar orang yang tidak berhak sulit untuk menebak sandi yang digunakan untuk mengakses suatu akun. Sandi yang kuat adalah sandi yang memiliki jumlah kemungkinan yang banyak untuk membentuknya. Kekuatan sebuah sandi atau entropi dari sandi dapat diukur dengan menggunakan kombinatorial.**

***Index Terms*—Combinatoric, password, password strength, password entropy.**

I. PENDAHULUAN

Untuk mendapatkan suatu pelayanan di internet, terkadang seseorang harus membuat akun terlebih dahulu. Dengan mendaftar di penyedia e-mail, seseorang dapat berkirim pesan dengan orang dengan. Dengan mendaftar di layanan penyimpanan file, seseorang dapat menyimpan sebuah file di internet dan hanya mengizinkan orang tertentu saja yang dapat mengakses file tersebut.

Selain itu pengguna juga perlu membuat akun di komputer pribadinya untuk dapat menggunakan komputer tersebut. Akun ini digunakan oleh sistem operasi untuk mengidentifikasi pengguna. Sistem operasi Linux dan Windows mewajibkan penggunanya untuk membuat sebuah akun saat instalasi sistem operasi. Dengan melihat jenis akun pengguna, sistem operasi dapat menentukan apakah pengguna tersebut diizinkan untuk mengakses file, melakukan instalasi software atau memodifikasi konfigurasi dari sistem operasi.

Akun yang telah dibuat seseorang merupakan identitas ia di dunia digital. Karena merupakan identitas seseorang di dunia digital, pengecekan apakah pengakses akun adalah orang yang berhak. Tanpa pengecekan ini orang yang tidak berhak dapat mengakses akun seseorang di internet dan menggunakan akun tersebut untuk melakukan hal yang tidak bertanggung jawab.

Ada beberapa teknik untuk mengecek apakah pengakses akun adalah orang yang berhak dan mencegah orang yang tidak berhak untuk mengakses akun. Teknik tersebut antara lain dengan menggunakan sidik jari, pengelanan wajah (*face recognition)* dan dengan meminta sandi (*password)* dari pengguna.

Sidik jari setiap manusia berbeda. Dengan memanfaatkan perbedaan tersebut, sidik jari dapat dimanfaatkan untuk mengecek apakah seseorang adalah orang yang berhak untuk mengakses sebuah akun. Kelemahan teknik ini yaitu diperlukan *hardware* tambahan yaitu *fingerprint scanner*.

Teknik lainnya yaitu *face recognition*. Teknik ini dilakukan dengan memeriksa wajah pengguna. Untuk melakukan *face recognition* diperlukan komputer dengan kamera.

Teknik yang ketiga yaitu dengan menggunakan sandi. Saat membuat akun, pengguna diharuskan membuat sebuah sandi. Kemudian setiap kali pengguna akan mengakses akun pengguna diharuskan memasukkan kembali sandi yang ia buat saat membuat akun. Teknik ini paling praktis dibandingkan dua teknik sebelumnya. Teknik ini hanya memerlukan *keyboard* untuk memasukkan sandi.

Kelemahan dari teknik yang ketiga adalah pemilihan sandi oleh pengguna. Jika sandi yang digunakan lemah, orang lain dapat menebak sandi yang digunakan untuk mengakses akun. Oleh karena itu, pengguna harus memilih sandi yang kuat sehingga orang lain sulit untuk menebak sandi yang digunakan untuk mengakses akun.

II. PASSWORD CRACKING

Password Cracking adalah metode yang melibatkan berbagai teknik dan peralatan untuk menebak, menentukan dengan sebuah metode, atau memperoleh pasword untuk tujan mendapatkan akses ke sumber daya yang dilindungi [1]. Secara garis besar, *password cracking* terbagi menjadi dua, yaitu *offline attack* dan *online attack*.

Pada *offline attack*, penyerang berusaha untuk mendapatkan akses ke *database* yang berisi password pengguna. Perlindungan terhadap *offline attack* tidak dapat dilakukan oleh pemilik akun melainkan oleh sistem milik penyedia layanan. *Offline attack* memerlukan cara yang lebih canggih dibandingkan dengan *online attack*. Namun, sekali penyerang berhasil, semua sandi yang digunakan pengguna untuk mengakses akun dapat diketahui oleh penyerang.

Pada *online attack* penyerang berusaha untuk

mendapatkan sandi pengguna dengan mencoba kemungkinan sandi yang digunakan oleh pengguna.

Ada beberapa metode yang digunakan oleh penyerang, antara lain *Smart Guesses, Dictionary Attacks, Brute Force Attacks* ,dan *Rainbow Tables*[2].

Pada *Smart Guesses*, penyerang mencoba mendapatkan sandi dengan memasukkan sandi yang paling umum digunakan orang. Contoh dari *Smart Guesses* yaitu penyerang mencoba memasukkan tanggal lahir sebagai sandi pengguna, atau menggunakan kata yang umum digunakan sebagai sandi oleh pengguna, misalnya kata "password" atau "qwerty".

Pada *Dictionary Attacks*, penyerang menggunakan sebuah kumpulan kata, misalnya kata pada kamus, dan mencoba setiap kata hingga sandi ditemukan. Proses ini dapat dilakukan secara otomatis oleh perangkat lunak.

Rainbow tables digunakan untuk melakukan *offline attacks* setelah penyerang mendapat akses *database* yang berisi sandi pengguna yang sudah di-*hash*. *Rainbow tables* berisi pasangan sandi dan nilai *hash* dari sandi tersebut.

Pada *Social Engineering*, penyerang menipu pengguna sehingga pengguna memberikan sandi yang digunakan untuk mengakses akun kepada pengguna. Salah satu caranya adalah membuat *website* palsu yang mirip dengan *website* aslinya sehingga pengguna tertipu dan memasukkan sandinya di *website* palsu tersebut.

Brute-Force attacks mirip dengan *dictionary attacks*, namun pada *brute-force attacks* tidak digunakan daftar kata untuk menebak sandi. Pada *brute-force attacks* mencoba semua kemungkinan susunan karakter yang mungkin untuk menjadi sandi. Makalah ini akan

III. KOMBINATORIAL

Kombinatorial merupakan bagian dari ilmu Matematika yang membahasa jumlah cara untuk mengurutkan beberapa buah objek. Dengan menggunakan kombinatorial, jumlah cara yang mungkin dapat dihitung tanpa harus mengenumerasi setiap kemungkinan.[3]

Dalam kombinatorial terdapat beberapa kaidah dasar untuk menghitung. Kaidah-kaidah tersebut antara lain kaidah penjumlahan dan kaidah perkalian

A. Kaidah Perkalian

Kaidah perkalian dilakukan jika ada 2 kejadian, kejadian pertama dengan p buah kemungkinan hasil dan kejadian kedua dengan q buah kemungkinan hasil dan dilakukan dan dilakukan dua buah percobaan. Jumlah kemungkinan hasil dapat dihitung dengan rumus:

$$total\ kemungkinan = p \times q \quad (1)$$

Rumus tersebut masih dapat diperluas. Jika ada buah kejadian, masing-masing memiliki P_1, P_2, P_3, ..., Pi buah kemungkinan hasil, maka jumlah kemungkinan hasil adalah:

$$total\ kemungkinan = P_1 \times P_2 \times P_3 \times ... \times P_n \quad (2)$$

B. Kaidah Penjumlahan

Kaidah penjumlahan dilakukan apabila ada 2 kejadian, kejadian pertama dengan p buah kemungkinan hasil dan q buah kemungkinan hasil dan dilakukan satu buah percobaan. Jumlah kemungkinan hasil dapat dihitung dengan rumus:

$$total\ kemungkinan = p + q \quad (3)$$

Rumus tersebut dapat diperluas jika ada n kejadian, masing-masing mempunyai jumlah kemungkinan hasil P1, P2, P3, .., Pi, maka total kemungkinan hasil yang mungkin adalah:

$$total\ kemungkinan = P_1 + P_2 + P_3 + \cdots + P_i \quad (4)$$

IV. CHARACTER SET

Character set adalah himpunan dari karakter yang mungkin untuk membentuk sebuah sandi[4]. *Character set* yang akan dibahas di makalah ini adalah *character space* yang dapat diketik dengan keyboard *qwerty*.

Secara garis besar ada 4 buah *Character set* yang dapat diketik dengan menggunakan keyboard *qwerty*:

A. Upper Case Characters

Himpunan *Upper Case Characters* berisi huruf kapital yang terdapat di *keyboard qwerty*. Himpunan *Upper Case Characters* dapat dituliskan:

U = {A, B, C, D, E, F, G, H, I, J, K, L, M, N, O, P, Q, R, S, T, U, V, W, X, Y, Z}

Kardinalitas dari himpunan *Upper Case Characters* adalah 26.

B. Lower Case Characters

Himpunan *Lower Case Characters* berisi huruf kecil yang terdapat di *keyboard qwerty*. Himpunan *lower case characteris* dapat dituliskan:

L = {a, b, c, d, e,f g, h, i, j, k, l, m, o, p, q, r, s, t, u, v, w, x ,y z}

Kardinalitas dari himpunan *lower case characters* adalah 26.

C. Angka

Angka (*numbers*) berisi angka yang terdapat pada *keyboard qwery*. Himpunan angka dapat dituliskan:

N = {1, 2, 3, 4, 5, 6, 7, 8, 9, 0}

Kardinalitas dari himpunan angka adalah 10.

D. Simbol

Simbol (*symbols)* adalah karakter yang tidak terdapat di himpunan *uppercase letters*, *lowercase letters*, dan angka[4]. Himpunan simbol terdiri dari:

S = {`, ~, !, @, #, $, %, ^, & ,*, (,), _, -, =, +, |, \,], }, {, [, ‘, “, ;, :, ?, /, >, ., <, ,, }

Dalam makalah ini, yang termasuk ke dalam himpunan simbol hanyalah simbol yang terdapat pada *keyboard qwerty*. Hal ini dipilih karena penggunaan simbol yang terdapat pada *keyboard qwerty* dalam sandi lebih mudah dilakukan pengguna dibandingkan dengan menggunakan simbol yang tidak terdapat di *keyboard qwerty*. Simbol-simbol lain tersebut dapat dimasukkan ke dalam himpunan simbol jika sandi mengandung simbol lain tersebut. Simbol-simbol lain tersebut dapat diakses dengan menggunaka program *character map* di Windows.

Dalam makalah ini, kardinalitas himpunan simbol adalah 33. Kardinalitas himpunan simbol dapat berubah jika simbol-simbol dari program *character map* di Windows dimasukkan ke dalam himpunan simbol.

IV. MENGHITUNG KEAMANAN SANDI DARI SERANGAN BRUTE FORCE

Secara umum, keamanan dari sandi ditentukan oleh beberapa faktor, yaitu panjang dari sandi tersebut, karakter apa saja yang ada di dalam sandi tersebut, dan tingkat keacakan dari sandi tersebut. Sandi dikatakan acak apabila sulit untuk diprediksi sehingga mempersulit *Smart Guesses*.

Agar sandi aman dari serangan *Brute-Force*, sandi harus sulit diperoleh dengan menggunakan teknik *Brute-Force*. Pada teknik *Brute-Force*, semua kombinasi yang mungkin untuk membentuk sandi dicoba. Agar sandi semakin sulit ditebak dengan *Brute-Force*, kemungkinan kombinasi sandi haruslah banyak. Dengan kemungkinan kombinasi yang banyak, teknik *brute-force* akan membutuhkan waktu yang lama serta sumber daya yang besar untuk memperoleh sandi. Bila kemungkinan kombinasi sandi sangat banyak, ada kemungkinan penyerang kekurangan waktu atau sumber daya sehingga sandi gagal didapatkan oleh penyerang.

Jumlah kombinasi yang mungkin dari sebuah sandi dapat dihitung dengan menggunakan kombinatorial. Kaidah perkalian berbunyi:

$$total\ kemungkinan = P_1 \times P_2 \times P_3 \times ... \times P_n \quad (2)$$

P_1, P_2, P_3, .. P_n adalah jumlah karakter yang mungkin untuk karakter ke 1, 2, 3, .., n. Hasil perkalian dari hasil dari P_1, P_2, P_3, .. P_n adalah jumlah kombinasi yang mungkin untuk membentuk sebuah sandi.

Seperti yang sudah dibahas di bagian sebelumnya, *Character set* adalah kumpulan karakter yang dapat membentuk sebuah sandi. Dalam hal ini, berarti huruf pertama adalah himpunan bagian dari *Character set* Begitu pula dengan huruf-huruf selanjutnya. Huruf ke 2, 3, dan seterusnya hingga huruf ke n adalah himpunan bagian dari *Character set*. Karena setiap karakter dari sandi adalah himpunan bagian dari *Character set*, maka jumlah karakter yang mungkin untuk menjadi sebuah karakter di sandi adalah kardinalitas dari *Character set* yang digunakan di sandi. Hal ini dapat ditulis menjadi:

$$P = |C| \quad (5)$$

Di sini, C adalah *Character set* yang membentuk sandi.

Dalam sebuah sandi, *Character set* yang digunakan untuk membentuk sebuah sandi sama untuk setiap karakter dalam sandi. Persamaan matematikanya yaitu:

$$P_1 = P_2 = P_3 = \cdots = P_n \quad (6)$$

Sehinga total dari seluruh kombinasi yang mungkin untuk membentuk sandi adalah kardinalitas dari *Character set* dipangkatkan dengan panjang karakter sandi. Dalam persamaan matematika ditulis:

$$\begin{aligned} total\ kemungkinan &= P_1 \times P_2 \times P_3 \times ... \times P_n \\ &= P \times P \times P \times ... \times p \\ &= P^n \end{aligned} \quad (7)$$

Dengan P adalah kardinalitas dari *character set* yang digunakan di sandi dan n adalah panjang dari sandi.

Seperti yang telah dituliskan pada bagian sebelumnya, *Character set* secara umum terdiri dari himpunan *uppercase character, lowercase character,* angka dan simbol. Sebuah sandi mungkin saja mengandung dua atau lebih *character set.* Misal pada sandi passw0rd, sandi tersebut mengandung 2 *character set*, yaitu *character set lowercase letter* dan *character set* angka. Karena sandi menggunakan *character set uppercase letter* dan angka, maka seluruh karakter yang mungkin menjadi bagian dari sandi adalah gabungan dari *character set lowercase letter* dan *character set* angka.

Secara umum himpunan karakter yang mungkin untuk menjadi bagian dari sandi adalah gabungan dari seluruh *character set* yang digunakan dalam sandi. Hal ini dapat ditulis menjadi

$$C = \bigcup_{i=1}^{N} A_i \quad (8)$$

Dalam persamaan ini, A1, A2, A3, ..., Ai adalah *character set* yang digunakan di dalam sandi dan N adalah jumlah *character set* yang digunakan dalam sandi.

Jika ada beberapa *character set* dalam sandi, maka P dalam persamaan 7 adalah kardinalitas dari gabungan seluruh karakter set pada sandi. Dalam persamaan matematika ditulis:

$$P = |C| = \left| \bigcup_{i=1}^{N} A_i \right| \quad (9)$$

V. Penulisan Kekuatan Sandi

Kekuatan sandi dari serangan *brute-force* ditentukan oleh jumlah kombinasi karakter yang mungkin untuk membentuk sandi tersebut. Semakin besar jumlah kombinasi yang mungkin, semakin kuat pula sandi tersebut dari serangan *brute-force*.

Kekuatan dari sandi dapat ditulis dengan menuliskan banyaknya kombinasi yang mungkin. Namun, cara ini kurang nyaman untuk digunakan. Sebuah sandi yang kuat setidaknya mengandung 1.208.925.819.614.629.174.706.176 kemungkinan[4]. Cara ini memakan banyak tempat. Selain itu, pengguna tidak memerlukan secara tepat berapa banyaknya kombinasi yang mungkin untuk membentuk sandi yang ia gunakan. Yang mereka butuhkan hanyalah gambaran secara umum apakah sandi yang ia pilih sudah cukup kuat atau belum.

Ada cara lain untuk menuliskan kekuatan sandi ke pengguna. Cara tersebut diantaranya dengan mengkategorikan sandi ke dalam beberapa kategori, misalnya kategori lemah, sedang dan kuat, dan dengan menuliskan dalam bentuk logaritma.

A. *Membagi Sandi Menjadi Beberapa Kategori*

Cara pertama untuk menuliskan kekuatan sandi adalah dengan membagi sandi ke beberapa kategori. Cara melakukannya sederhana. Pertama tentukan terlebih dahulu batas-batas jumlah kombinasi hitung terlebih dahulu jumlah kombinasi yang mungkin untuk membentuk sandi dengan menggunakan cara yang telah dibahas di bagian IV.

Keunggulan dari cara ini yaitu kekuatan dari sandi dituliskan dengan cara yang sederhana. Pada cara ini kekuatan dari sandi hanya dituliskan dengan kata "kuat", "sedang" atau "lemah". Pengguna awam akan langsung mengetahui bahwasannya sandi yang ia gunakan lemah.

B. *Menuliskan dalam Bentuk Logaritma*

Cara menuliskan kekuatan sandi yang kedua adalah dengan menuliskan banyaknya kombinasi sandi dalam bentuk logaritmanya. Cara ini dapat menuliskan kekuatan dari sandi dengan lebih detil dibandingkan dengan cara pertama.

Untuk menghitung kekuatan sandi dalam logaritma dapat digunakan persamaan[4]:

$$strength = \log_2 x \quad (10)$$

Di sini, x adalah banyaknya kombinasi yang mungkin untuk membentuk sandi. Nilai x didapat dari persamaan (9). Jika persamaan (9) disubtitusi ke persamaan (10) maka persamaan (10) akan menjadi:

$$strength = \log_2 \left| \bigcup_{i=1}^{N} A_i \right| \quad (11)$$

Satuan dari *strength* di sini adalah bits.

Jika bahasa pemrograman yang digunakan tidak terdapat fungsi untuk menghitung logaritma dari dua namun terdapat untuk menghitung ln, maka persamaan (11) dapat dihitung dengan menggunakan persamaan[4]:

$$strength = \frac{\ln|\cup_{i=1}^{N} A_i|}{\ln 2} \quad (12)$$

V. Kesimpulan

Ada beberapa cara untuk mengecek apakah pengakses akun adalah orang yang berhak. Salah satu caranya adalah dengan menggunakan sandi. Sandi yang dipilih pengguna harus kuat sehingga aman dari berbagai serangan untuk mendapatkan sandi. Salah satu serangan untuk mendapatkan sandi adalah serangan *brute-force.*

Pada serangan *brute-force*, penyerang mencoba satu-persatu kombinasi yang mungkin untuk mendapatkan sandi. Serangan dengan menggunakan *brute*-force semakin sulit jika jumlah kombinasi sandi yang mungkin semakin banyak. Sandi semakin kuat terhadap serangan *brute-force* seiring dengan semakin banyaknya cara membentuk sandi.

Kekuatan sandi atau entropi dari sandi terhadap serangan *brute-force* dapat dihitung dengan menggunakan kombinatorial. Dengan kombinatorial, menghitung banyaknya sandi yang mungkin dibentuk dari *character set* dapat dilakukan tanpa harus mengenumerasi satu-persatu semua kemungkinan.

VII. Ucapan Terima Kasih

Puji syukur saya kepada Allah SWT karena berkat rahmat-Nya lah makalah ini dapat saya selesaikan. Terima kasih penulis ucapkan kepada orang tua dari penuls karena berkat dukungan dari mereka penulis dapat menyelesaikan makalah ini. Penulis juga menyampaikan terima kasih kepada Ibu Harlili dan Bapak Rinaldi, dosen mata kuliah IF2120 Matematika Diskrit, yang telah mengajarkan dasar-dasar kombinatorial dan himpunan kepada penulis yang menjadi dasar teori dari makalah ini. Tidak lupa penulis juga mengucapkan terima kasih kepada teman-teman HMIF 2012 yang telah menjadi teman untuk saling berbagi ilmu.

REFERENSI

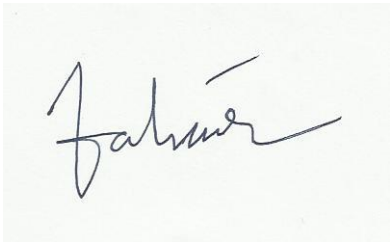
[1] Mark Burnett, “Perfect Passwords”, Rockland:Syngress Publishings, 2006, pp. 12
[2] Mark Burnett, “Perfect Passwords”, Rockland:Syngress Publishings, 2006, pp. 15-19
[3] Rinaldi Munir, “Diktat Kuliah IF2120 Matematika Diskrit”, Bandung:ITB, 2006, pp. VI 1 – VI 6
[4] blog.webernetz.net/2013/07/30/password-strengthentropy-characters-vs-words/ diakses tanggal 14 Desemeber 2013

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 27 November 2013

ttd



Fahziar Riesad Wutono - 13512012