Peluang dan Kombinasi pada Penjebolan Password

Biolardi Yoshogi 13509035[1]
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
vsio@students.itb.ac.id[1]

Abstract*—Makalah ini membahas mengenai analisis dalam menjebol password yang baik disadari maupun tidak disadari menggunakan aplikasi kombinasional dari struktur diskrit. Adapun metode yang digunakan untuk menjebol password adalah dengan cara brute force. Ada baiknya untuk mengetahui seberapa sulit untuk menjebol password menggunakan brute force dengan mengetahui jumlah kombinasi yang memungkinkan dan menggunakan hasil yang didapat pada jumlah kombinasi untuk menghitung peluang untuk menjebol password. Makalah ini juga bertujuan untuk memberi motivasi berupa keputusasaan untuk mencoba menjebol password orang lain.

***Kata Kunci*— brute force, kombinatorial, password, permutasi,**

I. PENDAHULUAN

Zaman sekarang, banyak hal yang merupakan hak masing-masing dilindungi oleh password. Password telah banyak digunakan dalam kebutuhan perlindungan akun termasuk harta. Dengan hal tersebut, orang merasa aman bahwa haknya dilindungi dari orang yang tidak berhak menyentuh haknya. Akan tetapi, tentu saja masih ada orang yang mencoba menjebolnya karena alasan tertentu. Berikut ini, akan dibahas beberapa hal mengenai password dan hal-hal yang ilmiah mengenai password.

II. PASSWORD

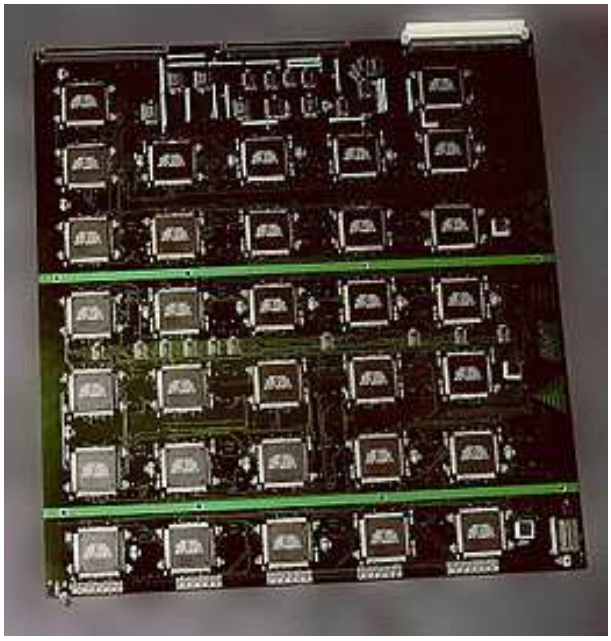
Kata sandi (Inggris: password atau passphrase) adalah kumpulan karakter atau string yang digunakan oleh pengguna jaringan atau sebuah sistem operasi yang mendukung banyak pengguna (multiuser) untuk memverifikasi identitas dirinya kepada sistem keamanan yang dimiliki oleh jaringan atau sistem tersebut. Sistem keamanan akan membandingkan kode-kode yang dimasukkan oleh pengguna (yang terdiri atas nama pengguna/user name dan password) dengan daftar atau basis data yang disimpan oleh sistem keamanan sistem atau jaringan tersebut (dengan menggunakan metode autentikasi tertentu, seperti halnya kriptografi, hash atau lainnya). Jika kode yang dibandingkan cocok, maka sistem keamanan akan mengizinkan akses kepada pengguna tersebut terhadap layanan dan sumber daya yang terdapat di dalam jaringan atau sistem tersebut, sesuai dengan level keamanan yang dimiliki oleh pengguna tersebut. Idealnya, kata kunci merupakan gabungan dari karakter teks alfabet (A-Z, a-z), angka (0-9), tanda baca (!?,.=-) atau karakter lainnya yang tidak dapat (atau susah) ditebak oleh para intruder sistem atau jaringan. Meskipun begitu, banyak pengguna yang menggunakan kata sandi yang berupa kata-kata yang mudah diingat, seperti halnya yang terdapat dalam kamus, ensiklopedia (seperti nama tokoh, dan lainnya), atau yang mudah ditebak oleh intruder sistem.[1]

III. BRUTE FORCE:

Serangan brute-force 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 analisa 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]

Ada juga teknologi yang berkembang untuk melakukan Brute Force secara otomatis:



(Sumber: http://upload.wikimedia.org/wikipedia/commons/thumb/b/bd/Board300.jpg/260px-Board300.jpg)

IV. Motivasi Orang Menjebol Password:

1. Ingin menggunakan akun orang lain dengan tujuan tertentu seperti iseng, penyalahgunaaan baik tingkat usil hingga tingkat kriminal
2. Lupa password.
3. Tidak ada fitur lupa password di situs di mana akunnya terdaftar
4. Lupa jawaban dari pertanyaan kunci (umumnya diimplementasikan dalam situs e-mail)

V. Hambatan Menjebol Password:

Berikut ini bebepara hambatan yang mempersulit untuk melakukan brute force pada password.

1. Jumlah karakter dan input yang cukup banyak. Jumlah karakter bisa mencapai 256 huruf dan inputnya pun bisa mencapat 256. Jika menggunakan rumus yang tercantum di sini, maka cukup besar sekali jika password yang dicoba dijebol memiliki jumlah input maksimum.
2. Karakter aneh yang tidak tercantum dalam keyboard sehingga menyulitkan untuk mengetik karakter tersebut. Dapat menggunakan aplikasi Character Map (untuk OS Window), namun mengklik dan meng-copy-nya berulang-ulang tentu saja tidak seefisien mengetik keyboard.
3. Situs yang diproteksi oleh sistem anti-gagal-masuk. Sistem ini menyulitkan untuk penerapan brute force karena jika dalam hitungan tertentu gagal masuk, maka akan ada konsekuensi yang membuat brute force menjadi lebih tidak efisien (Contoh: Tidak bisa masuk selama waktu tertentu, ban IP, ditambahkan sistem proteksi Captcha).
4. Sistem Captcha. Jika menggunakan Bot (Contohnya dengan script VB), maka akan lebih menyulitkan karena bot zaman sekarang masih kesulitan untuk membaca citra subjektif manusia.

VI. DATA STATISTIK

Contoh-contoh kombinasi di dalam password yang diambil dari 10.000 email Hotmail yang dijebol:[3]

1. 123456 - 64
2. 123456789 - 18
3. alejandra - 11
4. 111111 - 10
5. alberto - 9
6. tequiero - 9
7. alejandro - 9
8. 12345678 - 9
9. 1234567 - 8
10. estrella - 7
11. iloveyou - 7
12. daniel - 7
13. 000000 - 7
14. roberto - 7
15. 654321 - 6
16. bonita - 6
17. sebastian - 6
18. beatriz - 6
19. mariposa - 5
20. america - 5

Berikut ini panjang password yang umumnya digunakan:[3]

- 1 chars – 2 – 0 %
- 2 chars – 4 – 0 %

- 3 chars – 4 – 0 %
- 4 chars – 31 – 0 %
- 5 chars – 49 – 1 %
- 6 chars – 1946 – 22 %
- 7 chars – 1254 – 14 %
- 8 chars – 1838 – 21 %
- 9 chars – 1091 – 12 %
- 10 chars – 772 – 9 %
- 11 chars – 527 – 6 %
- 12 chars – 431 – 5 %
- 13 chars – 290 – 3 %
- 14 chars – 219 – 2 %
- 15 chars – 157 – 2 %
- 16 chars – 190 – 2 %
- 17 chars – 56 – 1 %
- 18 chars – 17 – 0 %
- 19 chars – 7 – 0 %
- 20 chars – 14 – 0 %
- 21 chars – 10 – 0 %
- 22 chars – 8 – 0 %
- 23 chars – 3 – 0 %
- 24 chars – 3 – 0 %
- 25 chars – 3 – 0 %
- 26 chars – 0 – 0 %
- 27 chars – 3 – 0 %
- 28 chars – 0 – 0 %
- 29 chars – 1 – 0 %
- 30 chars – 1 – 0 %

Jenis karakter yang umumnya digunakan:[3]

- 3,713 = 42 %; Hanya mengandung ‘a’ sampai ‘z’.
  Contoh : iloveyou
- 291 = 3 %; mengandung ‘a’ sampai ‘z’ dan ‘A’ sampai ‘Z’.
  Contoh: ILoveYou
- 1707 = 19 %; numerik: mengandung hanya angka ‘0’ sampai ‘9’.
  Contoh: 123456
- 2655 = 30 %; campuran ‘a’ sampai ‘z’, ‘A’ sampai ‘Z’, dan ‘0’ sampai ‘9’.
  Contoh: Iloveyou12
- 565 = 6 %; campuran alpabet, angka, dan karakter aneh.
  Contoh: 1Love You$%@

Statistik dari sumber lainnya dengan skala lebih global:[4]

Password Popularity - Top 20

Rank	Password	Number of Users with Password (absolute)
1	123456	290731
2	12345	79078
3	123456789	76790
4	Password	61958
5	iloveyou	51622
6	princess	35231
7	rockyou	22588
8	1234567	21726
9	12345678	20553
10	abc123	17542

Rank	Password	Number of Users with Password (absolute)
11	Nicole	17168
12	Daniel	16409
13	babygirl	16094
14	monkey	15294
15	Jessica	15162
16	Lovely	14950
17	michael	14898
18	Ashley	14329
19	654321	13984
20	Qwerty	13856

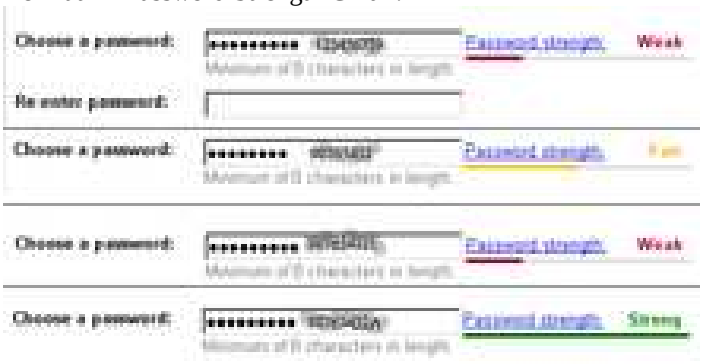
(Sumber: http://i.zdnet.com/blogs/imperva_passwords_popularity_rockyou_breach.jpg)

Dari statistik di atas, bisa dikatakan bahwa password yang umum meningkatkan peluang untuk menjebol password secara drastos.

VII. MINIMALISASI PENJEBOLAN

Password Strength adalah pengukuran keefektifan password untuk dapat bertahan dari jebolan berupa tebakan dan brute force.[5]

Berikut ini Password Strength Gmail.



(Sumber: http://upload.wikimedia.org/wikipedia/en/thumb/3/39/PassWord_Strength.png/220px-PassWord_Strength.png)

VIII. PEMBAHASAN

$C = I^L$

C : Jumlah Permutasi
I : Jumlah semua karakter yang sah digunakan
L : Jumlah maksimum input password

$P = 1/(C)$

P : Peluang untuk menjebol password

$P = I^{-L}$

Dengan menggunakan rumus tersebut, akan diuji peluang-peluang yang akan terjadi dengan parameter yang berbeda.

Contoh Penggunaan dalam kasus:

1. Misal jumlah semua karakter yang sah digunakan hanya alpabet yang artinya ada 26 karakter dan tidak *case-censitive*. Misalkan maksimum input password adalah 8 input. Hasilnya ada 208,827,064,576 susunan. Untuk peluangnya, diambil dari jumlah susunan tadi: 1/208.827.064.576; Dalam desimalnya menghasilkan 4.78865 x 10^{-12}.

2. Misal jumlah semua karakter yang sah digunakan hanya alpabet yang artinya ada 26 karakter dan *case-censitive* yang berarti ada 52 karakter yang harus ditangani. Misalkan maksimum input password adalah 8 input. Hasilnya ada 53,459,728,531,456 susunan. Untuk peluangnya, diambil dari jumlah susunan tadi: 1/53,459,728,531,456; Dalam desimalnya menghasilkan 1,870566 x 10^{-14}.

3. Misal jumlah semua karakter yang sah digunakan hanya angka numerik yang artinya ada 10. Misalkan maksimum input password adalah 8 input. Hasilnya ada 100,000,000 susunan. Untuk peluangnya, diambil dari jumlah susunan tadi: 1/100,000,000; Dalam desimalnya menghasilkan 1.00 x 10^{-8}.

4. Misal jumlah semua karakter yang sah digunakan hanya angka numerik yang artinya ada 16 yang merupakan basis 16. Misalkan maksimum input password adalah 8 input. Hasilnya ada 4,294,967,296 susunan. Untuk peluangnya, diambil dari jumlah susunan tadi: 1/4,294,967,296; Dalam desimalnya menghasilkan 0,00000000023283064.

5. Misal jumlah semua karakter yang sah digunakan hanya angka numerik yang artinya ada 10. Misalkan maksimum input password adalah 256 input. Hasilnya ada 10^{256} susunan. Untuk peluangnya, diambil dari jumlah susunan tadi: $1/10^{256}$; Dalam desimalnya menghasilkan 1,00 x 10^{256}.

6. (Agak di luar tapi agak masuk dikit) Misal dalam ujian isian, jumlah semua karakter yang sah digunakan asumsi ada yang artinya ada 100. Misalkan diwajibkan menulis 50 karakter. Hasilnya ada 10^{100} susunan. Untuk peluangnya, diambil dari jumlah susunan tadi: $1/10^{100}$. Dalam desimalnya menghasilkan 1,00 x 10^{100}. Dengan kata lain, dibutuhkan peluang sebesar $1/10^{100}$ agar jawaban yang ditulis pada satu soal isian itu benar. Jika ada 20 soal dan dihitung peluang berapa soal tersebut benar semua, maka: $10^{100x20} = 10^{2000}$.

7. (Agak di luar tapi agak masuk dikit) Misal dalam ujian pilihan ganda, jumlah pilihan ada 5. Karena pilihan ganda, maka input hanya 1 tetapi soal ada 50. Hasilnya ada 5^{1x50} atau 5^{50} atau $8{,}881784197001252323 \times 10^{34}$ susunan. Untuk peluangnya, diambil dari jumlah susunan tadi: $1/8{,}881784197001252323 \times 10^{34}$. Dalam desimalnya menghasilkan $1{,}125899906842624 \times 10^{-35}$. Dengan kata lain, dibutuhkan peluang sebesar $1/8{,}881784197001252323 \times 10^{34}$ agar semua jawaban yang dipilih dalam ujian pilihan ganda benar semua.

IX. KESIMPULAN

- Untuk menjebol akun seseorang dengan cara brute force sangatlah tidak mudah (berdasarkan subjektivitas) karena banyaknya kombinasi karakter yang memungkinkan disertai adanya hambatan dari sistem keamanan situs jika input password tidak benar.

- Dalam kehidupan seharui-hari, kita sering dihadapkan pada hal-hal bersifat peluang dan kombinasional baik hal tersebut disadari maupun tidak disadari. Kasus penjebolan password adalah kasus dari ribuan hingga miliaran kejadian yang melibatkan peluang baik yang disadari maupun yang tidak disadari.

REFERENCES

[1] Wikipedia. 2010. http://id.wikipedia.org/wiki/Password Waktu akses: 17 des 2010 Pukul 9:24

[2] Wikipedia. 2010. http://id.wikipedia.org/wiki/Serangan_brute-force Waktu akses: 17 des 2010 Pukul 9:27

[3] Acunetix, 2010. http://www.acunetix.com/blog/news/statistics-from-10000-leaked-hotmail-passwords/# Waktu akses: 17 des 2010 Pukul 10:57

[4] Zdnet, 2010. http://www.zdnet.com/blog/security/and-the-most-popular-password-is/5325?tag=rbxccnbzd1

Waktu akses: 17 des 2010 Pukul 11:00
[5] Wikipedia, 2010.
http://en.wikipedia.org/wiki/Password_strength
Waktu akses: 17 des 2010 Pukul 11:16