Analisa Kombinasional Pembuatan Password dan Kemungkinan Menjebolnya

Erwin 13511065
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
erwin.huang@std.itb.ac.id

Abstrak*—Makalah ini membahas mengenai pembuatan password dan beberapa upaya dalam pemjebolan password. Teknik - teknik dalam membuat password yang kuat, kombinasi - kombinasi karakter yang umum digunakan untuk membuat password, dan beberapa analisis tentang pembobolan password, serta upaya sistem mengatasi penjebolan password juga dibahas dalam makalah ini. Makalah ini bertujuan untuk memotivasi pembaca agar membuat password yang kuat yang susah untuk dijebol para hacker / cracker karena dewasa ini masih banyak sekali orang yang membuat password yang mudah ditebak oleh para pihak yang tidak bertanggung jawab.

***Kata Kunci*—Kombinasi, password, penjebolan, brute force**

I. PENDAHULUAN

Pada saat ini, password sudah banyak digunakan dalam kehidupan sehari-hari. Mulai dari jaringan sosial seperti facebook, twitter, sampai pada jaringan bisnis seperti e-bay. Password yang dibuat oleh seseorang biasanya berhubungan dengan hal-hal yang mudah diingat oleh orang tersebut. Pentingnya privasi seseorang mengakibatkan munculnya sistem-sistem untuk memproteksi privasi dari pengguna. Bersamaan dengan itu. Muncul juga usaha-usaha untuk menjebol password orang lain untuk kepentingan sendiri maupun kepentingan organisasi tertentu. Berikut akan dibahas seputar pembuatan password dan usaha-usaha untuk menjebolnya.

II. PASSWORD DAN PEMBUATANNYA

Password terdiri dari 2 kata yaitu pass dan word. Pass berarti lewat dan word berarti kata. Jika digabung, password berarti kata yang diperlukan untuk membuka sesuatu. Password menurut kamus adalah sekumpulan karakter yang dipilih pengguan atau administrator sistem dan digunakan untuk mengautentikasi pengguna ketika ia masuk, demi mencegahh akses yang tidak diinginkan ke dalam akunnya.Password digunakan untuk memverifikasi identitas seseorang yang memakai jasa tertentu bersama sejumlah orang lain yang juga memakai jasa yang sama. Jika password yang digunakan telah sesuai, maka sistem akan memperbolehkan akses seseorang terhadap data yang diinginkannya.

Pembuatan password biasanya disesuaikan dengan ketentuan – ketentuan dari tempat seseorang membuat password tersebut. Ketentuan tersebut misalnya password harus berupa angka, alfanumerik, case sensitive, dll. Berdasarkan ketentuan tersebut, maka kekuatan dari password yang dibuat seseorang dapat ditentukan.

Kombinasi password yang dapat dibuat oleh seseorang adalah jumlah karakter yang mungkin digunakan pangkat panjang password. Misalnya jika ditentukan password dengan panjang 4 karakter dan hanya boleh menggunakan angka, maka jumlah kombinasi yang mungkin adalah 10^4 = 10000.

Password yang kuat dapat dibentuk dengan memanfaatkan semua batasan – batasan yang diberikan oleh sistem tempat seseorang membuat password (menyertakan semua jenis karakter yang diperbolehkan dan panjang password lebih besar dari hasil rata-rata panjang minimum dan panjang maksimum yang diperbolehkan sistem). Dengan demikian, password seseorang tersebut akan semakin kuat. Misalnya password dengan 4 karakter case sensitive. Jika seseorang membuat password dengan hanya menggunakan huruf kecil / huruf kapital saja, maka jumlah kombinasinya adalah 26^4 = 456976. Jika seseorang membuat password dengan menggunakan huruf besar dan huruf kecil sekaligus, maka jumlah kombinasinya adalah 52^4 = 7311616. Jumlah kombinasi tersebut tentunya jauh lebih besar dibanding dengan pembuatan password dengan cara yang pertama.

Agar password lebih kuat, karakter-karakter simbol seperti ,@#$ dapat ditambahakan ke dalam password. Password dengan tambahan simbol biasanya sangat susah untuk ditebak. Peluang menebak password yang dilengkapi simbol – simbol unik hampir mendekati nol.

III. UPAYA PENJEBOLAN PASSWORD

Upaya penjebolan password biasanya dilakukan dengan tujuan untuk mempeoleh informasi – informasi sensitif seseorang maupun sekelompok orang untuk kepentingan yang menjebol password ataupun organisasinya. Sebuah password akan lebih mudah dijebol apabila kekuatan password tersebut lemah. Pembahsan tentang kuat-lemahnya password dapat dilihat pada bagian II.

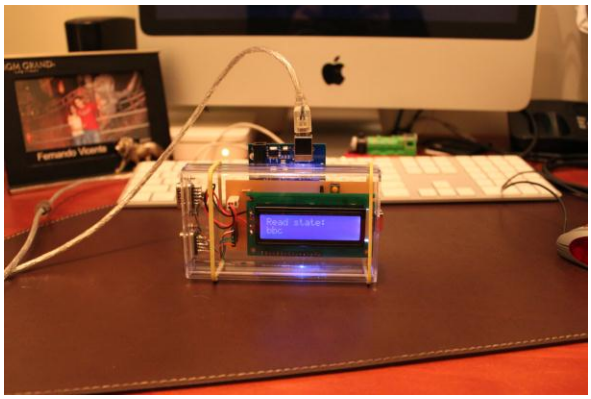
Cara yang paling sering digunakan untuk menjebol password adalah dengan menebak. Tebakan – tebakan yang dilakukan biasanya adalah sekelompok kata tertentu yang sering digunakan kebanyakan orang dalam membuat password. Berikut adalah beberapa password yang paling sering digunakan di internet versi Oktober 2012 berdasarkan Splash Data (sebuah pengembang software manajemen password) :

1. Password
2. 123456
3. 12345678
4. abc123
5. qwerty
6. monkey
7. letmein
8. dragon
9. 111111
10. baseball

Password yang telah terdaftar di atas sangat tidak dianjurkan untuk dipakai karena para pembobol password dapat dengan mudah menebaknya dan tingkat kekuatan password di atas sangat rendah.

Cara lain yang juga sering digunakan adalah brute force. Brute force adalah sebuah pendekatan secara langsung dalam memecahkan suatu masalah. Brute force menggunakan algoritma yang simpel yaitu mencoba semua kemungkinan yang ada. Cara ini biasanya digunakan pada scope karakter password yang tidak terlalu besar (misalnya adalah password dengan karakter angka).

Contoh hardware brute force :



Contoh brute force untuk menjebol password angka dengan panjang password maksimal 4 karakter :

1. 10
2. 10^2
3. 10^3
4. 10^4

Dengan demikian, maksimal dibutuhkann 10 + 100 + 1000 + 10000 = 11110 kali uji coba untuk mendapatkan password tersebut. Jumlah ini adalah kecil dan hanya memerlukan waktu yang singkat jika dilakukan brute force dengan menggunakan software.

Berikut adalah jumlah yang dibutuhkan untuk menjebol password yang terdiri dari karakter huruf case insensitive dengan panjang karakter 1-7 :

1. 26
2. 1352
3. 52728
4. 1827904
5. 59406880
6. 1853494656
7. 56222671232

Untuk password yang lebih standar yang terdiri dari karakter alfanumerik case sensitif dengan panjang karakter 8 :

1. 62
2. 62^2
3. 62^3
4. 62^4
5. 62^5
6. 62^6
7. 62^7
8. 62^8

Jika hasil di atas dijumlah, maka dibutuhkan waktu yang sangat lama (lebih dari jutaan tahun) untuk memecahkan password tersebut meskipun telah digunakan bantuan software. Hasil ini menunjukkan bahwa password akan semakin susah dijebol jika menggunakan semua jenis karakter yang diperbolehkan oleh sistem tempat membuat password. Software – software brute force biasanya dilengkapi dengan batasan – batasan tertentu agar scope pencarian tidak terlalu besar (misalnya dengan hanya mengecek semua karakter huruf kecil pada panjang karakter tertentu ataupun hanya mengecek karakter anngka untuk panjang karakter tertentu). Oleh karena itu, password yang hanya menggunakan 1 jenis karakter saja sangat tinggi peluangnya untuk dapat dijebol dengan menggunakan algoritma brute force.

IV. UPAYA SISTEM UNTUK MENGATASI BRUTE FORCE

Seperti yang telah tertulis pada bab sebelumnya, password dengan karakter angka sangat mudah di-crack dengan menggunakan brute force. Ini menjadi ancaman yang serius pada sistem yang menerapkan angka sebagai karakter satu-satunya dalam password (contohnya pin atm bank). Untuk mengatasi hal tersebut, dilakukan beberapa pendekatan, antara lain :

1. Pemblokiran
   Cara ini tergolong sangat efektif untuk mengatasi pemjebolan password pada sistem atm bank. Setelah beberapa kali mengalami kegagalan masukan password, maka kartu atm secara otomatis diblokir dan hanya bisa direset ulang passwordnya oleh pemilik asli kartu tersebut di bank yang bersangkutan.

2. Captcha
   Captcha adalah suatu gambar yang mengisyaratkan input tertentu kepada user dengan gambar. Captcha biasanya menggunakan gambar yang dimengerti manusia tetapi tidak dimengerti oleh program (mislanya huruf yang terlihat agak kacau dilengkapi dengan coretan-coretan). Cara ini juga tergolong efektif menangani brute force di internet karena software brute force sulit untuk menganalisa gambar captcha. Selain itu, jika terjadi kesalahan input password, captcha juga akan berganti. Ini akan menyebabkan brute force semakin susah untuk dilakukan (Brute force yang dilakukan manual oleh cracker akan sangat lama dan jika dilakukan software, tidak dapat menangani captcha).

3. Pemblokiran IP address
   Cara ini juga efektif untuk menangani brute force di internet karena setelah beberapa kali mengalami kegagalan, IP address orang yang menggunakan brute force akan terblokir untuk waktu tertentu. Dengan demikian, brute force semakin sulit untuk dilakukan (brute force mencoba banyak sekali kemungkinan yang mengakibatkan pemblokiran secara terus – menerus)

V. KESIMPULAN

Password yang kuat adalah password yang menyertakan semua jenis karakter yang diperbolehkan sistem untuk digunakan dengan panjang karakter diatas rata-rata (lebih besar dari (panjang minimum + panjang maksimum) / 2).

Brute force efektif untuk lingkup password yang tidak terlalu besar (jenis karakter dan panjang yang minim).

REFERENCES

[1] http://dictionary.reference.com/browse/password
Tanggal akses 17 Desember 2012 17:04:33

[2] http://www.dailymail.co.uk/sciencetech/article-2223197/Revealed-The-common-passwords-used-online-year-password-STILL-tops-list.html
Tanggal akses 17 Desember 2012 17:44:02

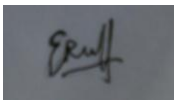
[3] http://www.zdnet.com/brute-force-attacks-beyond-password-basics-7000001740/
Tanggal akses 18 Desember 2012 20:01:29

[4] http://www.ittelkom.ac.id/staf/zka/Materi%20Desain%20Analisis%20Algoritma/M07Algoritma%20Brute%20Force.pdf
Tanggal akses 18 Desember 2012 21:14:49

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, 19 Desember 2012



Erwin 13511065