REVIEW PAPER

"An Improved Rainbow Table Attack for Long Password"

Disajikan Sebagai Tugas Mata Kuliah Kriptoanalisis Pada

Program Studi Informatika Universitas Udayana

(Dosen Pengampu: I Komang Ari Mogi, S.Kom., M.Kom)

Disusun Oleh:

I Gusti Ngurah Bagus Pramana Putra (1808561030)

Lalu Muhamad Waisul Kuroni (1808561037)

PROGRAM STUDI INFORMATIKA

FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM

UNIVERSITAS UDAYANA

2021

Terdapat banyak aplikasi jaringan mengunakan metode kriptografi untuk melindungi data yang sensitif seperti komunikasi sosial, email, dan belanja online. Sebagian besar aplikasi tersebut sering digunakan untuk enkripsi yang diakui secara universal dan algoritma otentifikasi untuk meyakinkan pengguna bahwa layanan yang disediakan cukup aman. Dari pandangan teoritis, kekuatan keamanan yang tinggi dari algoritma kriptografi disebabkan oleh menemukan kunci/kata sandi yang tidak dapat diraih oleh kemampuan komputasi saat ini.

Keamanan dan pemulihan kata sandi menarik banyak perhatian para peneliti pada yang sangat tinggi. Pada penelitian pada artikel ini berfokus pada serangan secara offline yang berarti dapat menebak dan memeriksa kata sandi tanpa batasan waktu. Cara yang paling umum dari password cracking adalah brute force attack yang hanya mencari seluruh ruang kandidat yang memungkinkan untuk mengidentifikasikan kata sandi yang benar. Metode ini hampir merupakan opsi default di banyak perangkat lunak penghancur kata sandi yang terkenal saat ini. Attack brute force asli ditingkatan kemudian dengan menganalisis kemungkinan terjadi dalam kata sandi untuk mengurangi ukuran ruang pencarian. Yang menarik dari serangan brute force adalah pencarian ruang tumbuh secara eksponensial dengan Panjang kata sandi.

Pada satu set karakter dari semua symbol yang dengan Panjang password 10, ukuran totalnya adalah 9510 yang mana proses pembuatannya sangat memakan waktu. Mempertimbangkan fitur kata sandi yang dipilih manusia, untuk mencoba mengurangi ruang pencarian kata sandi lebih lanjut. Bagian ini dikumpulkan sebagai dictionary kata sandi untuk membuat protocol otentikasi popular. Itu efek pemulihan sebenarnya terletak pada penerapan dictionary kata sandi untuk membuat protocol otentikasi popular. efek pemulihan sebenarnya terletak pada penerapan dictionary untuk kata sandi. Bagian paling kritis dari penyerangan adalah dictionary kata sandi mendasarinya. Hasil penelitian menunjukan presentase passwordnya hanya bervariasi antara 17% dan 24%. pengalaman cracking kata sandi, peneliti jika melakukan pengingkatan keberhasilan cracking password yang lebih rumit. Untuk mengatasi masalah penyimpanan dictionary ini, table rainbow dianggap sebagai algoritma yang efisien dan praktis untuk pembalik kata sandi teks biasa dari hash.

Berikut hal yang dilakukan oleh peneliti.

1. Peneliti mengusulkan metode pembuatan kata sandi yang ditingkatkan berdasarkan dictionary generator dan rainbow table untuk pemulihan kata sandi yang lama dapat dilakukan serta meningkatkan tingkat keberhasilan penjelajahan untuk kata sandi yang mudah diingat manusia.
2. Peneliti secara rinci mendesain fungsi Kernel dalam pembuatan rainbow table dan secara hati-hati menangani transformasi rules yang memperoleh kata sandi baru dari generator dictionary dasar.
3. peneliti mengumpulkan generator dictionary dengan probabilitas kemunculan tinggi dalam kumpulan kata sandi praktis dan khususnya menyajikan yang sangat cocok untuk pengguna sandi-sandi cracking

Dasar-dasar rainbow table attack

$$S_i = X_{i1} \xrightarrow{f} X_{i2} \xrightarrow{f} \ldots\ldots\ldots \xrightarrow{f} X_{it} = E_i$$

Faktanya, untuk meningkatkan cakupan kunci di ruang kunci saat rantai ini dibuat, pengurangan fungsi r pada setiap kolom rantai berbeda pula dengan fungsi f. jika fungsi ini di setiap kolom direkatkan dengan warna yang berbeda. Karenanya mereka dinamai rantai Rainbow/ rainbow chains.

$$C_0 \xrightarrow{f} Y_1 \xrightarrow{f} Y_2 \xrightarrow{f} \ldots \xrightarrow{f} Y_s = E_j.$$

Rantai di atas akan kembali dari titik awal S_j sampai menemukan kunci $k=X_{i(t-s)}=f^{t-s-l}(S_j)$. yang diinginkan, sandi yang benar ini mungkin tidak ada di rantai yang cocok. Fenomena ini dihasilkan dari Y_1 bertepatan dengan rantai di table tetapi rantai rainbow yang cocok ini tidak mengandung sandi yang benar. Ini kasus yang bisa disebut dengan alarm palsu.

- **Ciri-ciri kata sandi yang Panjang**

  Alasan yang mendasarinya adalah bahwa kata sandi yang dipilih manusia harus mudah diingat. Kebanyakan kata sandi yang panjang ini terdiri dari kata-kata yang bermakna, angka, dan huruf penggabungan Keyboard.

- **Generator dictionary dan pola komposisi**

  Setelah mengetahui prinsip konstruksi kata sandi yang panjang, maka kita harus menemukan dictionary generator untuk menghasilkan pattern . Untuk mengumpulkan

generator dan mengurai pola komposisinya serta untuk menjamin kemunculannya probabilitas tinggi dalam kata sandi praktis, ada beberapa sumber generator, sebagai berikut :

a. hasil statistik dari dataset password praktis. Analisis kata sandi yang dirilis dari semua forum jaringan, social aplikasi dan seterusnya untuk mendapatkan pola kata sandi dan generator.
b. Model MarNov menghasilkan string
c. Elemen dasar dari bahasa tertentu. karena komponen kata sandi dari setiap pengguna selalu berasal bahasa tertentu, elemen fundamental ini adalah generator dictionary kata sandi yang populer.

- **Mengubah aturan generator**
    a. **Aturan 1**. Pengalihan kasus. aturan ini memungkinkan generator untuk beralih antara huruf kecil dan huruf besar. Tentu saja hanya berlaku untuk alfabet.
    b. **Aturan 2**. substitusi khusus. aturan ini memberikan substitusi untuk beberapa huruf khusus. Misalnya, IO "adalah diganti dengan I0 "sedangkan Ie" diubah menjadi I3 "dan seterusnya.
    c. **Aturan 3**. seluruh kebalikannya. aturan ini memungkinkan generator muncul dalam bentuk kebalikannya. Misalnya, kata Iwell "diubah menjadi Illew"

Implementasi dan analisis

- **Generator**. Untuk tujuan cracking kata sandi yang berasal dari bahasa Cina, peneliti memilih grup generator dictionary dengan tiga kinds: suku kata fonetik, angka dan symbol.
- **Pola Komposisi**. peneliti menetapkan pola komposisi sebagai PNS, yang berarti kata sandi terdiri dari satu phonetic, angka dan satu simbol khusus.
- **Mengubah Pattern**. perhatikan bahwa aturan transformasi dikonfigurasikan sesuai dengan generator.untuk phonetic suku kata, peneliti memberi aturan pergeseran huruf hanya untuk huruf awal.
- **Komentar**. Selain itu, jika kita memperluas rainbow table dengan melibatkan lebih banyak tabel rainbow, maka tingkat kesuksesan dapat ditingkatkan lebih lanjut.