Nama : Kadek Vincky Sedana (1808561071)

I Kadek Aldy Oka Ardita (1808561091)

Mata Kuliah : Kriptoanalisis

Review Paper

Enhanced Dictionary Based Rainbow Table

Tujuan utama dalam meningkatkan pemulihan kata sandi adalah untuk memenuhi tantangan yang semakin meningkat dari data pembuktian yang dilindungi kata sandi. Memanfaatkan pendekatan hybrid dari teknik brute force dan pendekatan tabel yang dihitung sebelumnya terbukti menjadi cara yang hemat biaya untuk memulihkan kata sandi. Di sisi lain, terlihat bahwa manusia tergoda untuk memilih password yang mudah diingat. Kata sandi tersebut dapat didasarkan pada kombinasi urutan tombol umum pada tata letak keyboard, kata-kata kamus, dan kombinasi kata-kata kamus. Oleh karena itu, dengan mempertimbangkan sifat manusia dan kecenderungannya dalam pemilihan kata sandi, dan memasukkan pengetahuan tersebut ke dalam desain metode pemulihan kata sandi baru akan meningkatkan kinerja secara signifikan.

Enhanced Rainbow Table

Dalam hal ini, penulis mengusulkan desain tabel pelangi yang ditingkatkan dengan algoritme penyortiran baru. Pembaruan pertama terletak pada teknik pembuatan rantai. Alih-alih menggunakan kumpulan teks biasa sebagai nilai awal, penulis secara sistematis memilih kumpulan unik yang jauh lebih kecil. Penulis memilih teks biasa dan menghitung nilai hash yang sesuai. Penulis membiarkan nilai hash yang dihasilkan h.tabel pelangi berbasis kamus yang disempurnakan.

Tabel pelangi yang ditingkatkan. Ada total 161 karakter seperti itu dan penulis berasumsi bahwa karakter ascii yang tidak dapat dicetak ini tidak membentuk salah satu dari kumpulan karakter sandi karena tidak ditemukan pada keyboard. Penulis memasukkan sejumlah karakter khusus ini ke dalam kata sandi yang disimpan. Cara memasukkan karakter khusus ini dengan memberikan informasi tentang posisi asli kata sandi setelah tabel diurutkan. Konsekuensinya, karakter khusus yang disisipkan ini akan menghabiskan ruang penyimpanan. Penulis mengilustrasikan dalam peningkatan ruang penyimpanan minimal dan juga secara signifikan lebih rendah daripada persyaratan penyimpanan tabel pelangi asli. Keuntungan dari algoritma pengurutan ini adalah kata sandi dalam tabel sekarang dapat diurutkan dan dengan demikian pencarian kata sandi dapat dioptimalkan. Kecukupan karakter khusus yang tersedia untuk digunakan dalam penyortiran, persyaratan penyimpanan, dan tingkat keberhasilan pemulihan kata sandi juga dievaluasi.

Design Of Dictionary Based Enhanced Rainbow Table

Dalam tabel pelangi yang ditingkatkan, sandi dibuat berdasarkan fungsi hashing dan pengurangan. Oleh karena itu, pembuatannya sangat acak dan sebagian besar kata sandi mungkin berisi karakter khusus di tempat acak dan kata-kata non-kamus. Sebagian besar pengguna juga perlu mencatat kata sandi dan menyimpannya secara terpisah untuk mencegah mereka melupakan kata sandi mereka sendiri untuk akses selanjutnya. Pendekatan sederhana adalah dengan melakukan serangan kamus terlebih dahulu dan kemudian pemulihan kata sandi tabel pelangi jika serangan kamus gagal. Namun, kebutuhan overhead komputasi dan penyimpanan akan tinggi. Alih-alih dalam makalah ini penulis mengusulkan pendekatan baru untuk memasukkan kata sandi umum ke dalam tabel. Metode paling sederhana untuk membuat tabel pelangi berbasis kamus yang disempurnakan adalah dengan menghasilkan kata-kata kamus yang dimutasi sebagai kolom awal kata sandi. Sebagai gantinya, penulis mengusulkan agar fungsi reduksi pertama menghasilkan kata-kata kamus yang dimutasi di kolom virtual pertama, dalam tabel pelangi yang ditingkatkan, akan dapat dipulihkan. Namun, dalam kasus ini, kemungkinan jumlah kata-kata kamus permutasi yang dihasilkan pertama kali dibatasi oleh jumlah rantai dalam tabel. Kecepatan pemulihan juga dapat mengganggu password tersebut karena mereka termasuk dalam kolom virtual pertama. Karenanya, rantai pelangi awal ini terdiri dari tiga kata sandi di atas..

Metode Konstruksi Rantai

Penulis mengusulkan 2 metode konstruksi rantai sedemikian rupa sehingga mereka menyertakan kata sandi yang diinginkan. Penulis kemudian memberikan analisis dari kedua metode dalam hal kelayakan dan upaya komputasi yang diharapkan diperlukan.

1. Metode 1: hitung semua kemungkinan nilai Pi - Aj. Kemudian, pertimbangkan semua kemungkinan rantai yang bisa dibentuk. Untuk setiap rantai, uji apakah hasil rantai tersebut berbeda fungsi reduksi. Jika demikian, kita telah menemukan rantai yang dibutuhkan; jika tidak, lanjutkan pengujian yang tersisa sampai menemukan rantai seperti itu
2. Metode 2: hitung semua kemungkinan nilai Pi - Aj. Ambil salah satu yang memiliki frekuensi kemunculan terendah. Tautan itu akan menjadi bagian yang dihasilkan rantai. Untuk tautan berikutnya, kita memilih tautan yang berbeda dari semua tautan sebelumnya dalam rantai dan terjadi pada frekuensi yang lebih rendah. Langkah ini diulangi hingga kita memiliki rantai yang diinginkan atau kkita mencapai titik di mana kita tidak dapat menambahkan tautan lagi. Dalam kasus terakhir, kita mundur ke proses sebelumnya dan memilih tautan lain sebagai gantinya, sampai rantai yang diinginkan diperoleh.

Kesimpulan

Dalam makalah ini, penulis mempresentasikan desain baru dari tabel pelangi berbasis kamus yang disempurnakan. Penulis kemudian mengusulkan dua metode baru konstruksi rantai. Penulis menganalisis dan membuktikan kelayakan metode yang diusulkan. Penulis juga menganalisis kemungkinan menghasilkan rantai yang diinginkan dalam skenario spesifik dari

ukuran ruang sandi yang berbeda dan dalam kasus umum ruang sandi n, dan upaya komputasi yang diharapkan diperlukan menggunakan masing-masing metode. Hasil analisis menunjukkan bahwa metode enhanced dictionary based rainbow table yang diusulkan merupakan pendekatan baru yang menjanjikan untuk memulihkan kata sandi secara efisien dengan mempertimbangkan penggunaan kata sandi umum (dapat diingat oleh manusia) dan kata sandi yang dibuat secara acak pada saat yang bersamaan.