ADOPSI ENKRIPSI JEFFERSON WHEEL PADA PROTOKOL ONE-TIME PASSWORD AUTHENTICATION UNTUK PENCEGAHAN SNIFFING PADA PASSWORD E-MAIL

Vega Valentine[1], Anne Yuliyanti[2], Bertalya[3]
[1,2,3] Fakultas Teknologi Informasi dan Ilmu Komputer
Universitas Gunadarma
Jalan Margonda Raya, Pondok Cina No.100, Depok, 16424
email:[1,2]{slaved_jepun,anneyuliyanti}@student.gunadarma.ac.id,[3] bertalya@staff.gunadarma.ac.id

ABSTRAKS

Pencurian password melalui sniffing merupakan teknik pencurian password yang relatif sulit diketahui user karena penyerangan dilakukan terhadap protokol dan langsung menyadap informasi akun dari server. Untuk itu diperlukan suatu metode pencegahan untuk melindungi username dan password user dari serangan para sniffer. Pada penelitian ini kami mengusulkan metode pencegahan sniffing dengan menggunakan teknik one-time password yang telah dikembangkan dengan nama One-Time Password Authentication (OTPA) dan disisipi teknik enkripsi yang mengadopsi teknik Jefferson wheel.

Kata kunci: enkripsi Jefferson wheel, One-Time Password Authentication, sniffing

1. LATAR BELAKANG

Banyak metode yang sering digunakan oleh *hacker* untuk dapat mengetahui *username* dan *password* dari sebuah akun (*account*). Akun yang dimaksud di sini dapat berupa akun apa saja, seperti akun *email*, akun jejaring sosial, akun *messenger*, dan lain sebagainya. Namun, akun yang sering dijadikan sasaran para *hacker* adalah akun *email*.

Adanya pemikiran bahwa akun *email* menjadi dasar atau acuan untuk memiliki akun lain seperti *messenger* juga jejaring sosial membuat *hacker* selalu mengincar *username* serta *password* dari akun *email*.

Salah satu cara yang digunakan *hacker* untuk mengetahui informasi akun seseorang adalah *sniffing*. *Sniffing* atau dalam konteks pencurian *password* sering disebut *password sniffing* adalah suatu teknik pencurian *password* dengan bantuan perangkat lunak untuk mengambil informasi *remote login* seperti *username* dan *password*[Wang, 2009]. Teknik *sniffing* relatif sulit diketahui *user* karena penyerangan dilakukan terhadap protokol dan langsung menyadap informasi akun dari *server*. Seringkali diketahui adanya *sniffer* setelah *password* serta informasi akun lainnya telah tercuri (Anonim, 2005).

Password sniffing atau disebut juga *Eavesdropping* merupakan salah satu metode pencurian *password* yang membutuhkan perangkat lunak untuk membantu *sniffer* menyadap informasi *login user* yang dituju [Brud, 2009]. Ada beberapa program yang disebut packet *sniffer* yang sering digunakan untuk melakukan pencurian *password*. Misalnya TCPdump, WireShark, atau Cain & Abel *packet sniffer*.

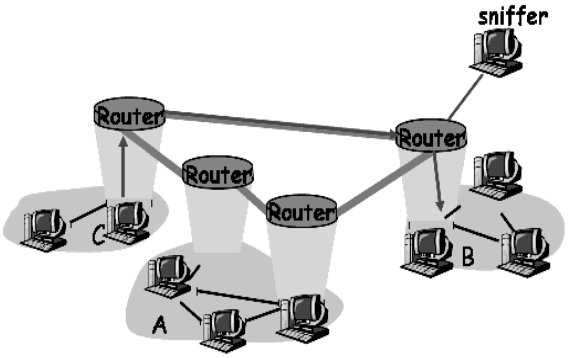
Pada awalnya program-program *sniffer* seperti ini digunakan dengan tujuan yang positif, yaitu untuk mempertahankan jaringan dan sistem agar dapat bekerja normal. Jaringan *sniffers* digambarkan seperti terlihat pada Gambar 1. Normalnya, *sniffer* digunakan sebagai asisten manajemen jaringan untuk memonitor dan sebagai fitur analisis yang dapat membantu memecahkan masalah jaringan, mendeteksi intrusi, kontrol atau pengawasan lalu lintas jaringan konten. Tetapi, fitur tersebut juga dapat digunakan oleh *hacker* sebagai alat mengintai untuk masuk ke komputer lain (Anonim, 2010).

Namun, seiring perkembangan teknologi, perangkat lunak seperti ini mulai dikembangkan untuk kegunaan yang negatif, yaitu untuk mengambil data dan informasi rahasia *user* yang tidak terenkripsi selama berlalu-lalang dalam jaringan. Selain itu, beberapa penggunaan negatif *sniffer* yang merugikan untuk keamanan jaringan antara lain:

a. Penangkapan sandi, yang merupakan alasan utama untuk sebagian besar penggunaan alat *sniffing* secara ilegal
b. Menangkap informasi transaksi khusus dan bersifat pribadi, seperti *username*, kredit ID, rekening, dan *password*
c. Merekam *email* atau pesan instan dan melanjutkan isinya
d. Beberapa *sniffers* bahkan dapat mengubah informasi target sistem komputer dan menyebabkan kerusakan
e. Merusak keamanan jaringan untuk mendapatkan otoritas akses yang lebih tinggi.

Untuk menanggulangi atau mencegah penyerangan *sniffer* terhadap suatu jaringan, ada beberapa cara yang bisa ditempuh, yaitu: (Anonim, 2010).

1. Penggunaan *switch* sebagai pengganti *Hub* dapat menon-aktifkan program *sniffer*.
2. Enkripsi data dapat mengurangi efek *sniffer* terhadap informasi pribadi
3. *One-Time Password* untuk mengecoh *sniffer* mengambil informasi yang tidak signifikan
4. Menolak *modus promiscuous* agar program *sniffer* tidak dapat dijalankan.



Gambar 1. *Network Sniffing* (Wang, 2009)

Adanya teknik-teknik pencurian *password* dan informasi rahasia akun tentu saja meresahkan bagi pemilik akun. Dengan adanya aksi-aksi *hacker* seperti ini tentu dibutuhkan pula upaya pencegahan agar tidak ada satu informasipun yang dapat diketahui oleh pihak-pihak yang tidak ber-kepentingan, sehingga akun yang dimiliki akan aman terjaga kerahasiaannya.

Pada penelitian ini kami mengusulkan metode pencegahan *sniffing* dengan menggunakan teknik *One-Time Password* dan disisipi teknik enkripsi yang mengadopsi teknik *Jefferson wheel*.

2. METODE PENCEGAHAN SNIFFING

Metode pencegahan *sniffing* menggunakan cara *One-Time Password* yang telah dikembangkan dengan nama *One-Time Password Authentication* (*OTPA*). Teknik *One-Time Password* bertujuan untuk mengecoh *sniffer* mengambil informasi yang bukan sebenarnya. Kemudian metode ini disisipkan teknik enkripsi mengadopsi teknik *Jefferson wheel*.untuk mengubah data password yang sebenarnya menjadi data yang tidak dimengerti. Metode ini diilustrasikan seperti pada Gambar 2.

2.1. One-Time Password

One-Time Password (OTP) adalah sebuah *password* yang hanya berlaku untuk sesi login tunggal atau transaksi tunggal (Wang, 2009).

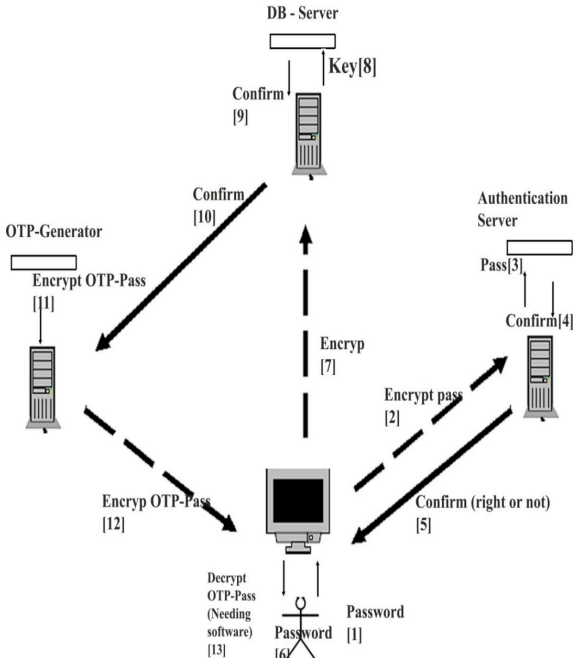
Secara umum, algoritma dari OTP dibuat secara *random*. Namun terdapat tiga pendekatan utama dalam proses *generate* OTP, yaitu: (Wang, 2009)

a. Berdasarkan "*time-synchronization*" antara autentikasi *server-client* yang menyediakan *password* (OTP akan bersifat valid bila dalam peride waktu yang singkat).
b. Berdasarkan "*mathematical algorithm*" yang memungkinkan generalisasi suatu *password* baru berdasarkan *password* sebelumnya.
c. Berdasarkan "*mathematical algorithm"*, *password* baru didasari oleh suatu tantangan (misalnya : penetapan nilai suatu *password* secara random akan ditentukan oleh *server* atau detail transaksinya).

Berdasarkan teori ini, telah dibangun sebuah pengembangan protokol autentikasi yang menggunakan OTP, disebut OTPA (*One-Time Password Authentication*) (Yulianti, 2010). Protokol OTPA akan dijelaskan lebih lanjut pada bagian implementasi.

2.2. *One-Time Password Authentication*

Protokol *One-Time Password Authentication* (*OTPA*) adalah sebuah protokol autentikasi dengan menggunakan teknik *one-time password* untuk pengamanan pengiriman informasi *login user* (Yulianti, 2008).



Gambar 2. *One-Time Password Authentication (OTPA) Protocol*

Prosedur protokol OTPA ini adalah sebagai berikut:

- *User* memasukkan informasi *login*-nya yaitu *username* dan *password*, kemudian mendapat konfirmasi apakah informasi yang dikirim sesuai atau tidak.

- Jika informasi sesuai, user kemudian harus memasukkan informasi tambahan yang disebut '*security key*', sesuai dengan data yang tersimpan pada *database server*. Sekali lagi dilakukan pemeriksaan validitas informasi yang disebut '*security key checking*'
  - *Security key* diperoleh dari jawaban *security question* yang diisikan oleh user pada saat membuat *account email*
- Jika hasil '*security key checking*' valid, maka *server* akan men-*generate* OTP untuk sesi *login user* tersebut
- User memperoleh OTP-nya, OTP ini yang kemudian akan digunakan untuk mengakses internet melalui sistem yang digunakan.

2.3. Enkripsi Adopsi *Jefferson Wheel*

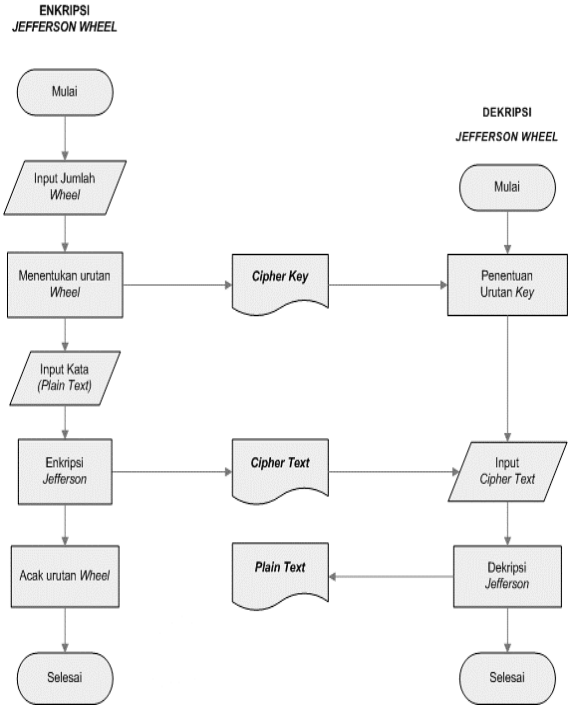
Jefferson Wheel adalah alat yang diciptakan Thomas Jefferson untuk melakukan enkripsi dan dekripsi pada masa revolusi Amerika (Brud, 2009). Pada masa itu, teknik enkripsi *Jefferson* digunakan untuk melindungi kerahasiaan pesan diplomatis kenegaraan Amerika.

Cipher Jefferson melakukan enkripsi dengan menggunakan prinsip substitusi abjad tunggal, dimana satu karakter *plaintext* digantikan dengan satu karakter lain menggunakan Disk Jefferson (Gambar 3). Hal ini dilakukan sampai semua karakter pada *plaintext* sudah berganti menjadi karakter-karakter yang terlihat acak dan tidak beraturan, disebut *ciphertext*. Proses inilah yang selanjutnya disebut sebagai satu tahap enkripsi.

Gambar 3. *Jefferson Disk*

Langkah-langkah enkripsi dan dekripsi *Jefferson wheel* dapat dilihat pada algoritma yang diilustrasikan pada gambar 4.

Pada tahun 1923-1942, enkripsi Jefferson dikembangkan oleh US Army dalam bentuk mesin enkripsi M-94. Penggunaan teknik enkripsi ini oleh pihak tentara Amerika Serikat menjadi bukti bahwa enkripsi Jefferson merupakan enkripsi yang *powerful*. Hal ini juga dikarenakan teknik dekripsinya yang memerlukan pencarian secara *exhaustive search* sehingga tidak akan dapat terpecahkan dengan mudah begitu saja.



Gambar 4. Algoritma Adopsi *Jefferson Wheel Cipher*

Pada tahun 1923-1942, enkripsi Jefferson dikembangkan oleh US Army dalam bentuk mesin enkripsi M-94. Penggunaan teknik enkripsi ini oleh pihak tentara Amerika Serikat menjadi bukti bahwa enkripsi Jefferson merupakan enkripsi yang *powerful*. Hal ini juga dikarenakan teknik dekripsinya yang memerlukan pencarian secara *exhaustive search* sehingga tidak akan dapat terpecahkan dengan mudah begitu saja.

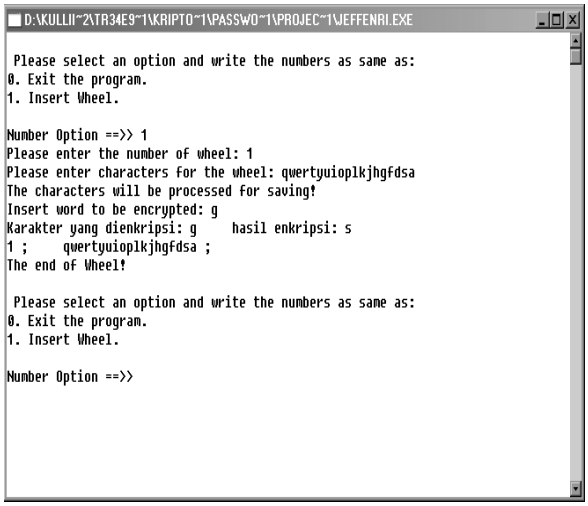
3. IMPLEMENTASI ADOPSI ENKRIPSI JEFFERSON WHEEL PADA PROTOKOL OTPA

Peran enkripsi *Jefferson Wheel* di sini adalah untuk melindungi data informasi *login* pada protokol OTPA, seperti *password* asli, *security key*, serta OTP untuk tiap *sesi login user*. Pada gambar 4,

 ISSN: 1907-5022

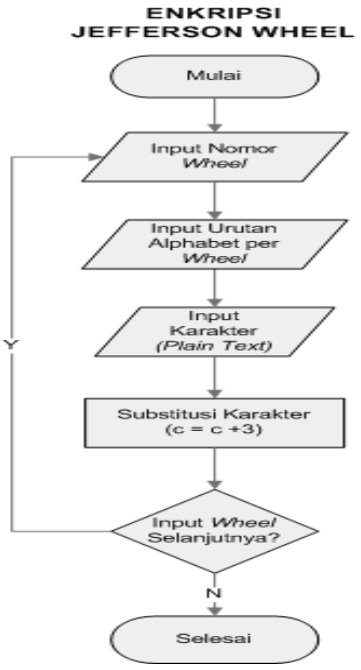
enkripsi ini akan diaplikasikan untuk langkah (2), (5), (7), (10), dan (12).

Adopsi enkripsi *Jefferson Wheel* telah diaplikasikan ke dalam bentuk program dengan menggunakan bahasa pemrograman C++ (Gambar 5).



Gambar 5. Tampilan Program *Jefferson* dengan Turbo C++

Program ini merupakan adopsi enkripsi Jefferson karena dalam urutan alfabet tiap *disk/wheel* bisa disesuaikan dengan kebutuhan *user*. Alur program enkripsi ini pun berbeda dengan algoritma asli enkripsi *Jefferson Wheel*, seperti terlihat pada Gambar 6.



Gambar 6. Alur Program Adopsi *Jefferson Wheel*

Pada protokol OTPA, enkripsi *Jefferson Wheel* digunakan untuk melindungi data informasi *login* seperti *password* asli, *security key*, serta OTP untuk tiap *sesi login user*.

- Untuk melindungi *password* asli, dilakukan enkripsi *Jefferson Wheel* untuk pengiriman *password* dari user ke *server* untuk penanganan autentikasi (gambar 2 langkah (2)).
- Dilakukan enkripsi *Jefferson Wheel* pula untuk konfirmasi validitas *password* serta pengiriman *security question* untuk memperoleh *security key* dari *server* ke *user* untuk penanganan autentikasi (gambar 2 langkah (5)).
- Untuk melindungi *security key*, dilakukan enkripsi *Jefferson Wheel* untuk pengiriman *password* dari *user* ke *server* penyimpanan *database user* (gambar 2 langkah (7)).
- Dilakukan pula enkripsi *Jefferson Wheel* untuk pengiriman konfirmasi hasil *security key checking* dari *server* ke OTP Generator (gambar 2 langkah (10)).
- Untuk melindungi OTP yang akan digunakan *user* untuk mengakses internet, dilakukan enkripsi *Jefferson Wheel* untuk pengiriman OTP dari OTP Generator ke *user* (gambar 2 langkah (12)).
- Setelah proses di atas, user mendapatkan OTP untuk dapat digunakan mengakses sistem maupun internet tanpa kekhawatiran pencurian *password* oleh *sniffer*, karena *sniffer* tidak akan berhasil *login* dengan *password* OTP yang sama.

4 PENUTUP

Upaya pencurian password atau lebih dikenal dengan istilah password sniffing sampai saat ini menjadi permasalahan yang meresahkan para *user* pemilik akun. Akun *email* menjadi sangat rentan terhadap serangan *sniffer* karena akun email merupakan acuan untuk membuat akun lainnya.

Enkripsi *Jefferson Wheel* dapat diaplikasikan untuk melengkapi protokol OTPA sebagai metode pertahanan terhadap pencurian *password* melalui *sniffing*.

Metode ini dapat diimplementasikan pada organisasi atau institusi yang dilengkapi dengan fasilitas *email* khusus maupun akses jaringan internet. Penggunaan protokol OTPA yang dilengkapi dengan enkripsi adopsi *Jefferson wheel* ini sangat bermanfaat bagi *user*, sehingga *user* dapat mengakses akunnya tanpa kekhawatiran penyerangan dari *sniffer*.

PUSTAKA

Anonim. (2005). *Fortified SSH: A Cost Effective Way to Safeguard Your Network*. Technical Paper. September. 2005.

Bruff, (2009). D. *Thomas Jefferson's Wheel Cipher*.

Anonim. (2010). *Network Sniffer & Packet Sniffer*. http://www.colasoft.com/resources/ network-sniffer.php

Pamuji, T. *Cipher Jefferson.* Program Studi Teknik Informatika, Institut Teknologi Bandung.

Wang, J. (2009). *Computer Network Security Theory and Practice.*

Yuliyanti, A. & Vega V. (2008) *Modified Authentication Using One-Time Password to Support Web Services Security*. Universitas Gunadarma.