



InfoTekJar : Jurnal Nasional Informatika dan Teknologi Jaringan

ISSN (Print) 2540-7597 | ISSN (Online) 2540-7600



Available online at : <http://bit.ly/InfoTekJar>

Penerapan SMS Gateway untuk Kode Verifikasi

Rofa Very Andika

Universitas Sumatera Utara

KEYWORDS

Keamanan Komputer (*Software*); Data; SMS Gateway

CORRESPONDENCE

Phone:

E-mail: rofa.very@gmail.com

ABSTRACT

Kata sandi digunakan untuk memproteksi hal-hal yang sifatnya rahasia. Beberapa orang sudah membuat kata sandi dengan menggabungkan beberapa jenis karakter sehingga sulit untuk ditebak, tetapi jika sebuah sistem digabungkan dengan SMS kode verifikasi yang dikirim oleh sistem saat pengguna ingin masuk kedalam suatu sistem, maka suatu sistem akan lebih aman dibuka dan dijalankan dimanapun.

PENDAHULUAN

Salah satu metode pengamanan sistem informasi yang umum diketahui oleh banyak orang adalah *password* atau kata sandi, *Password* mempunyai peranan penting dalam pengamanan informasi-informasi yang sifatnya pribadi atau rahasia.

Dengan menggunakan *password* secara langsung untuk masuk kesuatu sistem, tidak menutup kemungkinan ada pihak lain yang coba mengetahui *password* dengan cara mensadap menggunakan berbagai macam cara, dan mencoba untuk masuk kedalam sistem yang kita gunakan. Jika itu terjadi, maka hal tersebut akan sangat merugikan kita jika sebagai pemegang *password* yang asli.

Dengan adanya tahap verifikasi *password* melalui SMS (*Short Message Service*) maka tahap keamanan akan naik satu tingkat lebih tinggi atau memperpanjang cara untuk masuk kedalam suatu sistem. Hal ini tentunya tidak akan memudahkan orang-orang yang tidak bertanggung jawab untuk melihat, merubah atau merusak data kita. Metode ini juga digunakan oleh perusahaan besar seperti *google mail(gmail)* untuk verifikasi kode masuk kedalam *electronic mail*.

PEMBAHASAN

Pada dasarnya ancaman datang dari seseorang yang mempunyai keinginan memperoleh akses ilegal ke dalam suatu jaringan komputer. Oleh karena itu, harus ditentukan siapa saja yang diperbolehkan mempunyai akses legal ke dalam sistem, dan

ancaman-ancaman yang dapat mereka timbulkan. Ada beberapa tujuan yang ingin dicapai oleh penyusup dan sangat berguna apabila dapat membedakan tujuan-tujuan tersebut pada saat merencanakan pembangunan suatu sistem informasi.

Beberapa tujuan para penyusup antara lain adalah :

1. Hanya ingin tahu sistem dan data yang ada pada suatu jaringan komputer yang dijadikan sasaran. Penyusup yang bertujuan seperti ini sering disebut dengan *The Curious*.
2. Membuat sistem jaringan menjadi down, atau mengubah tampilan situs *website*. Penyusup yang mempunyai tujuan seperti ini sering disebut sebagai *The Malicious*.
3. Berusaha untuk sumber daya di dalam sistem jaringan komputer untuk mempeoleh popularitas. Penyusup yang mempunyai tujuan seperti ini sering disebut sebagai *The Profil Malicious*.
4. Ingin tahu data apa saja yang ada didalam jaringan komputer untuk selanjutnya dimanfaatkan untuk mendapat uang. Penyusup seperti ini sering disebut sebagai *The Competition*.

Analisa Sistem

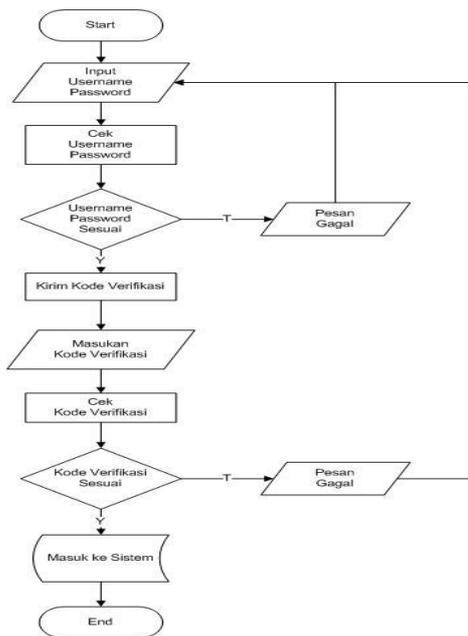
Salah satu cara klasik untuk menjaga suatu sistem agar orang lain tidak mudah masuk kedalam sistem dengan cara menggunakan verifikasi kode yang dikirim melalui *SMS Gateway*. Yang mana sistem mengirim kode verifikasi ke ponsel pemegang akun yang sudah didaftarkan. Dengan cara tersebut maka yang berhasil masuk kedalam suatu sistem hanya orang pemegang akun dan ponsel itu saja.

Tahap pertama untuk membangun sebuah sistem yang diperlukan adalah alur dari sistem yang akan dibangun atau biasa disebut dengan *flowchart*.

Flowchart atau Diagram alir merupakan sebuah diagram dengan simbol-simbol grafis yang menyatakan aliran algoritma atau proses yang menampilkan langkah-langkah yang disimbolkan dalam bentuk kotak, beserta urutannya dengan menghubungkan masing-masing langkah tersebut menggunakan tanda panah. Diagram ini biasanya memberikan solusi selangkah demi selangkah untuk penyelesaian masalah yang ada di dalam proses atau algoritma tersebut.

Kegunaan dari *flowchart* adalah :

- Untuk mendesign program.
- Untuk menentukan alur dan cara kerja dari program tersebut.
- Untuk mempresentasikan program.



Gambar 1. *Flowchart* Login kedalam Sistem

Dalam contoh kasus ini disarankan untuk kode verifikasi menggunakan kode acak setiap transaksinya. Sangat tidak disarankan jika menggunakan kode statik atau tetap, karena akan mudah dihafal atau dilihat oleh orang lain. Berikut contoh penggalan kode secara acak dari bahasa pemrograman pascal.

```

procedure TKodeVerifikasi.SetKode;
begin
  Randomize;
  scapcha:=IntToStr(Random(10000));
end;
    
```

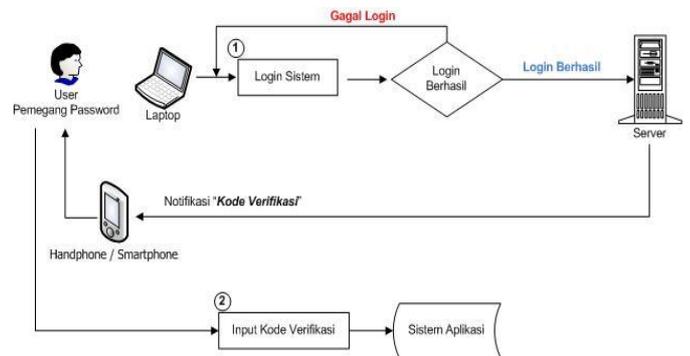
Gambar 2. Penggalan kode verifikasi secara acak

Penjelasan Kode :

- Sistem akan mengacak maksimal 4 digit angka.

- Sistem bisa saja mengeluarkan angka dari 1-9999.

Dengan cara ini, kode verifikasi akan selalu berubah setiap transaksinya. Dan akan menyulitkan orang lain untuk menghafalnya.

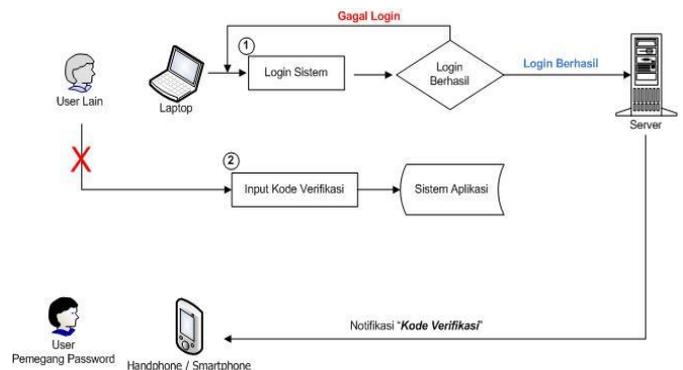


Gambar 3. Skema pengiriman kode dan berhasil login

Penjelasan Gambar 3, Skema pengiriman kode dan berhasil login:

User pemegang akun asli melakukan *login* kedalam sistem

- Jika *User* berhasil *login*, maka sistem akan melakukan pengacakan kode (kode verifikasi).
- Setelah itu sistem akan mengirimkan kode tersebut ke ponsel si *User* yang sudah terdaftar didalam *database*.
- *User* memasukkan kode yang dikirim melalui sms.
- Jika kode tersebut sesuai dengan daftar data yang ada didalam *database*, maka *user* akan berhasil masuk kedalam sistem.



Gambar 4. Skema pengiriman kode dan gagal login

Penjelasan Gambar 4, Skema pengiriman kode dan gagal login:

- *User* lain mencoba melakukan *login* kedalam sistem. Menggunakan *username* dan *password* asli milik *user* asli (pemegang akun asli).
- Jika *User* lain tersebut berhasil *login*, maka sistem akan melakukan pengacakan kode (kode verifikasi).
- Setelah itu sistem akan mengirimkan kode tersebut ke ponsel si *User* asli (pemegang akun asli) yang sudah terdaftar didalam *database*.
- Karena *user* lain tidak mendapatkan kode verifikasi yang dikirim oleh sistem, maka otomatis *user* tersebut tidak akan bisa masuk kedalam sistem.

Kelebihan dan Kelemahan Sistem

gratis-via-web-dengan-php-dan-mysql/

Kelebihan :

- Sistem akan lebih aman dari pihak lain, yang sengaja menggunakan *software* tertentu untuk mensadap *username* dan *password*.
- *User* atau pengguna akan memiliki rasa aman, karena hanya dia yang memegang ponsel untuk verifikasi data.
- Memperpanjang alur / cara kerja, jika ada seseorang yang ingin masuk kedalam sistem tersebut.
- Pengamanan berlapis akan sangat penting untuk menjaga data-data dari orang yang tidak bertanggung jawab.

Kekurangan :

- Ponsel si pemegang akun harus dipastikan hidup saat ingin login kedalam sistem.
- Pengecekan berkala pada sisi modem sipengirim pesan kode verifikasi.

Kesimpulan dan Saran

3.1 Kesimpulan

Inti dari keamanan komputer adalah melindungi komputer baik itu dari sisi *hardware*, *software* ataupun jaringannya dengan tujuan mengamankan informasi yang berada di dalamnya. Mencegah terjadinya suatu serangan terhadap sistem. Dengan demikian kita perlu memperhatikan desain dari sistem, aplikasi yang dipakai pengguna. Ketiga faktor tersebut merupakan cara yang baik untuk mencegah terjadinya kebocoran sistem, serangan, dan lain-lain.

Password digunakan untuk memproteksi hal-hal yang sifatnya rahasia. Beberapa orang sudah membuat *password* dengan menggabungkan beberapa jenis karakter sehingga sulit untuk ditebak. Tetapi jika hanya dengan menggunakan *username* dan *password* kemungkinan orang lain masih bisa mengetahuinya, dengan cara menanamkan beberapa *software* yang memang di rancang untuk mensadap *username* dan *password*. Hal ini dapat dicegah dengan memperpanjang suatu alur sistem dengan menggunakan SMS kode verifikasi jika *username* dan *password* sesuai dengan daftar data. Dengan hal itu informasi tidak mudah dilihat, rusak dan manipulasi oleh orang-orang tertentu dengan masuk kedalam sistem. Hanya pengguna yang terdaftar sesuai dengan nomor ponsel yang bisa masuk kedalam sistem.

3.2 Saran

Setelah melakukan kajian, ada beberapa hal yang disarankan untuk penelitian selanjutnya :

- Penggabungan metode enkripsi untuk penggunaan kode verifikasi.
- Perhitungan kecepatan modem sms gateway ataupun sistem untuk melakukan pengiriman sms disaat banyak yang melakukan *login* secara bersamaan.
- Penerapan metode antrian yang harus diperhitungkan.

4. Referensi

- [1] https://id.wikipedia.org/wiki/Diagram_alir
- [2] https://id.wikipedia.org/wiki/Keamanan_komputer
- [3] <http://lppm3.bsi.ac.id/jurnal/index.php/biangmatika/article/viewFile/12/13>
- [4] <http://blog.rosihanari.net/membuat-sendiri-kirim-sms->