**JURUSAN TEKNIK INFORMATIKA**

**FAKULTAS TEKNOLOGI INFORMASI**

**INSTITUT TEKNOLOGI SEPULUH NOPEMBER**

**USULAN TUGAS AKHIR**

# **IDENTITAS PENGUSUL**

**Nama** : **Dian Rahma Latifa Hayun**

**NRP** : **5109 100 113**

Dosen Wali : Diana Purwitasari, S.Kom, M.Sc.

1. **JUDUL TUGAS AKHIR**

**Mekanisme *One-Time-Password* untuk Mengamankan Password dari Serangan *Phishing***

1. **LATAR BELAKANG**

*Phishing* merupakan ancaman serius pada keamanan data pengguna dalam jaringan. Phishing merupakan jenis serangan dimana penyerang (*phiser*) mencoba untuk menipu pengguna dalam penyediaan informasi rahasia dari pengguna yang bersangkutan. Misalnya informasi akun bank pengguna, nomor kartu kredit, dan sebagainya. Untuk mendapat informasi yang diinginkan, pertama-tama penyerang mempersiapkan sebuah halaman situs web palsu yang menyerupai situs web yang asli. Alamat URL situs web palsu tersebut selanjutnya akan dikirimkan secara acak ke sejumlah besar pengguna melalui e-mail atau pesan singkat pada aplikasi-aplikasi *chatting.* Pengguna yang mengakses situs web tersebut selanjutnya akan diarahkan ke situs web palsu tersebut, dimana mereka akan diminta untuk memasukkan informasi pribadi atau informasi rahasia mereka. Meski dirasa proses untuk melakukan serangan ini susah, akan tetapi kini sudah ada “*phishing kits*” yang dapat membuat situs web palsu dalam waktu singkat.

Oleh karena itu diperlukan suatu upaya untuk melindungi informasi personal atau rahasia dari para pengguna. Adapun teknik-teknik yang telah diterapkan untuk mencegah serangan ini adalah sebagai berikut.

1. Teknik *List-based*

Adalah teknik yang menggunakan daftar alamat situs web yang telah terindikasi sebagai situs web palsu(*black list*) atau daftar alamat situs web yang aman dikunjungi (*white list*) untuk mencegah pengguna dari serangan ini. Kelemahan dari teknik ini adalah pada perkara cakupan, akurasi dan update dari daftar alamat situs web tersebut

1. Teknik *Heuristic-based*

Adalah teknik yang menggunakan beberapa kriteria tertentu untuk menentukan apakah sebuah situs web merupakan situs *phishing* atau bukan. Kelemahan dari mekanisme ini menurut Cranor adalah ketidakmampuannya dalam mendeteksi dan memblok semua situs phishing.

Berdasarkan pembahasan di atas, maka dibutuhkan metode yang menyelesaikan permasalahan tersebut dari akarnya. Yakni memastikan bahwasanya

Maka solusi yang ditawarkan adalah metode yang dapat mengautentikasi pengguna pada sebuah web.

1. **RUMUSAN MASALAH**

Berdasarkan latar belakang yang telah diuraikan diatas, terdapat beberapa permasalahan yang dapat dirumuskan sebagai berikut.

1. Bagaimana mengirimkan *One-Time Password*?
2. Bagaimana membangkitkan password?
3. Bagaimana menghubungkan server web dengan jaringan *instant messagging?*
4. **BATASAN MASALAH**

Batasan masalah dari aplikasi yang akan dibangun adalah sebagai berikut.

* + - 1. Bahasa pemrograman web yang digunakan adalah PHP
      2. Protokol yang digunakan untuk menghubungkan server web dengan *instant messaging* adalah protokol XMPP

1. **TUJUAN DAN MANFAAT TUGAS AKHIR**

Manfaat dari pembuatan tugas akhir ini adalah untuk memberikan keamanan kepada pengguna ketika melakukan proses login pada sebuah situs web dengan menggunakan mekanisme ­*One-Time-Password.* Aplikasi ini akan selalu membangkitkanpassword baru disetiap kali pengguna melakukan proses login. Sehingga dapat mencegah serangan phishingpassword.

Adapun tujuan yang ingin adalah membuat mekanisme pengamanan password dari serangan phishing,sehingga dapat menyelamatkan data privasi atau rahasia pengguna.

1. **DASAR TEORI**
   1. **XMPP**
      1. **Deskripsi XMPP(Extenxible Messaging and Presence Protocol)**

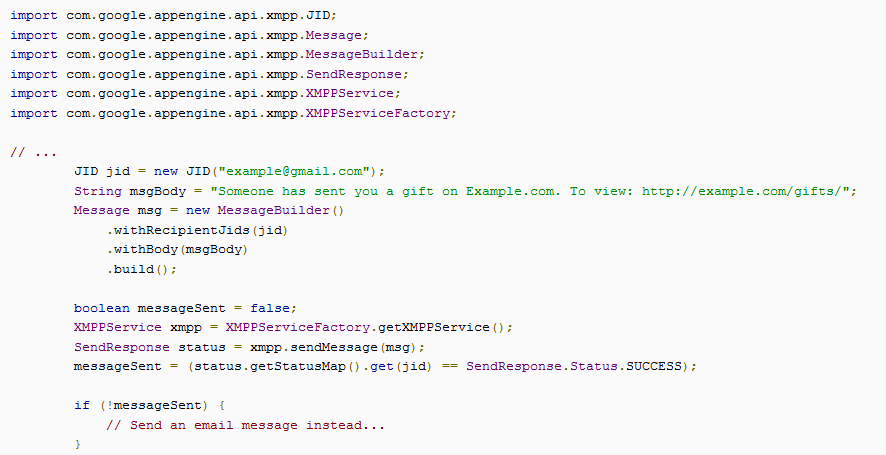
XMPP merupakan teknologi terbuka untuk *instant messaging,* chat dengan banyak pihak, suara dan *video call,* kolaborasi *midleware* sederhana, kesatuan konten, dan menyamaratakan routing dari data XML. XMPP pada awalnya dikembangkan oleh komunitas *open-source* Jabber untuk menyediakan layanan *instant messaging* yang aman, terbuka, bebas dari spam, dan terdesentralisasi[1].

* + 1. **Arsitektur XMPP**

Arsitektur sederhana XMPP terdiri dari klien dan server. Dimana setiap klien mengimplementasikan bentuk dari protokol khusus klien.Sedangkan server, dia sebagai penyedia layanan routing antar klien yang sedang berkomunikas. *Library* XMPP dapat dijumpai dalam bahasa C, C#, Java,Phyton dan beberapa bahasa lainnya.

* + 1. **Protokol XMPP**

XMPP adalah protokol yang relatif sederhana yang terjadi melalui soket TCP menggunakan pesan XML. Komunikasi asinkronus terjadi pada data XML. Suatu data XML merupakan pembungkus yang mengenkapsulasi pertukaran data yang terjadi pada 2 entitas. Dibawah ini merupakan contoh implementasi XMPP dengan menggunakan bahasa java, pada kasus seorang klien hendak mengirimkan pesan singkat.

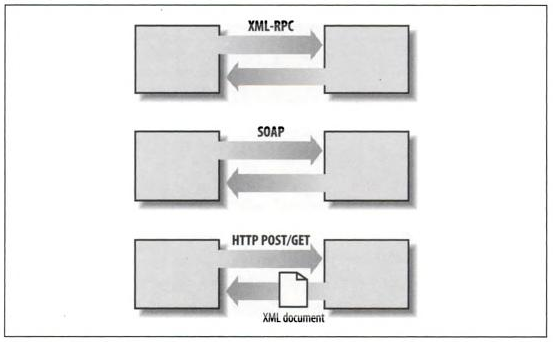
****

Gambar 1. Contoh program dengan XMPP

* 1. **Web Service**
     1. **Deskripsi Web Service**

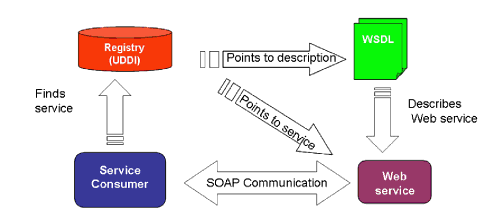
Web service didefinisikan sebagai sebuah aplikasi yang dapat diakses oleh aplikasi lain melalui suatu web. Definisi lain menurut UDDI adalah sebuah aplikasi bisnis modular yang mandiri yang bisa diakses melalui koneksi internet dan memiliki antarmuka. Dengan kata lain web service merupakan web yang memberikan layanan aplikasi yang dapat digunakan bersama dan memiliki antarmuka publik yang dapat diakses melalui internet[2].

Suatu web service dapat berinteraksi secara langsung dengan aplikasi lain dengan menggunakan bahasa XML, untuk saling bertukar pesan melalui protokol untuk internet. Ada beberapa alternatif untuk pesan XML yang digunakan. Yang pertama bisa menggunakan XML-Remote Procedure Call(XML-RPC), kemudian SOAP, lalu HTTP Get/Post.



Gambar 2. Pesan XML untuk Web Services

Terdapat tiga properti berbeda yang dapat diidetifikasi untuk layanan dan web services. Ketiga properti tersebut adalah.

* + - * 1. Deskripsi fungsional, mengandung deskripsi formal tentang apa yang dapat dilakukan oleh sebuah servis.
        2. Deskripsi Perilaku, fokus pada bagaimana fungsionalitas dari sebuah sistem dapat dipenuhi dan bagaimana servis yang dibangum mampu untuk berkomunikasi dengan aplikasi lain.
        3. Deskripsi non-fungsional, berisi kendala apa saja yang dihadapi dari kedua properti yang sebelumnya dijelaskan.

Gambar 3. Proses penggunaan web services

1. **RINGKASAN TUGAS AKHIR**

Pada tugas akhir ini akan dibangun sebuah aplikasi yang secara umum memiliki fungsi untuk mengautentikasi pengguna yang akan log in pada sebuah situs web. Ancaman serangan phishing pada kata sandi masih menjadi hal berbahaya. Oleh karena itu aplikasi berbasis web yang akan dibangun ini merupakan terobosan untuk mencegah terjadinya serangan phishing pada kata sandi dengan menggunakan sistem *One Time Password*[5]*.*

Aplikasi ini akan bekerja pada dua proses, yakni proses registrasi dan proses login. Pada proses login, aplikasi ini bertujuan untuk mengeliminasi penggunaan kata sandi yang tetap untuk mengakses sebuah situs web, sehingga skenario baru yang diajukan adalah sebagai berikut.

Mulai

Registrasi reguler tanpa penggunaan password

Input akun IM &informasi autentikasi

Validasi akun IM pengguna

Akhir

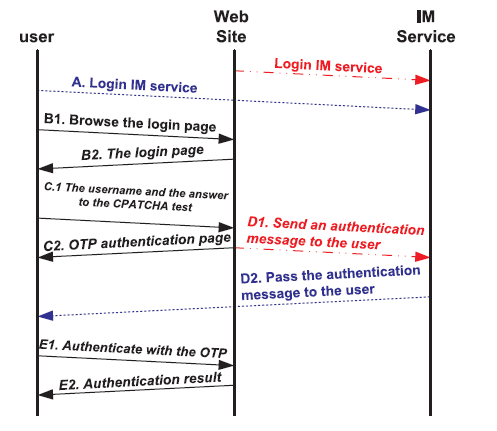
Gambar 4. Modifikasi proses register pengguna

Pengguna diminta untuk menginputkan nama pengguna tanpa password. Selanjutnya pengguna meng-inputkan akun *Instant Messaging(IM)* dan informasi autentikasi. Pengguna harus memasukkan akun IM yang didukung oleh situs web yang bersangkutan. Informasi autentikasi merupakan jawaban dari *security question.* Kemudian sistem melakukan validasi, dengan terlebih dahulu memunculkan tes CAPTCHA untuk memastikan bahwa yang melakukan proses registrasi adalah manusia bukan robot.

Jika pengguna lulus dalam test CAPTCHA maka langkah berikutnya yang akan dilakukan adalah sebagai berikut:

1. Mengirim halaman validasi akun IM kepada pengguna. Pada halaman tersebut memuat informasi akun IM yang akan digunakan, string acak (session), serta kolom pengisian one time password yang dikirim ke akun IM pengguna.
2. Apabila akun IM pengguna adalah akun baru bagi website tersebut, maka sistem akan meminta ijin untuk menambahkan akun pengguna, kemudian pengguna menyetujui akun sistem, dan sebaliknya.
3. Setelah akun IM disetujui oleh kedua pihak, situs web akan mengirim pesan validasi akun melalui layanan IM yang telah dirancang. Pesan tersebut memuat session (t) dan sebuah *one-time-password* p.
4. Kemudian pengguna melakukan verifikasi pengirim pesan tersebut dengan membandingkan session yang dikirim dan akun pengirim dengan yang muncul di halaman validasi.

Adapun pada proses kedua yakni proses login, akan dilakukan skenario seperti yag terlihat pada gambar 5 dibawah ini.



Gambar 5. Proses login pengguna

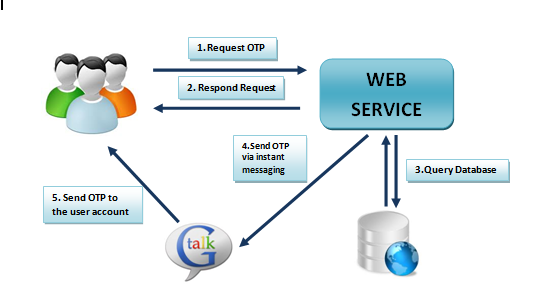
Sesuai skenario pada gambar di atas, pada proses login terdapat 5 langkah yang dilakukan:

1. Pengguna login terlebih dahulu ke akun IM yang dimiliki.
2. Pengguna melakukan proses login di halaman login dari situs web dimana halaman login memuat kolom pengisian nama akun pengguna dan tes CAPTCHA.
3. Pengguna memasukkan nama pengguna dan jawaban atas tes CAPTCHA yang diberikan. Jika pengguna lolos dalam test CAPTCHA situs web akan menampilkan halaman yang memuat kolom bagi pengguna untuk memasukkan OTP yang dikirim oleh situs web. Halaman tersebut juga memuat session t dan IP address yang digunakan pengguna untuk konek ke internet.
4. Jika nama akun pengguna valid, sistem akan memeriksa akun IM pengguna kemudian mengirimkan pesan autentikasi ke akun tersebut, serta OTP-nya.
5. Langkah terakhir, pengguna memasukkan OTP yang dikirim oleh sistem dan masuk ke halaman pengguna.

Maka secara garis besar, fitur-fitur yang terdapat pada aplikasi yang akan dibangun ini adalah sebagai berikut.

1. Menyediakan tes CAPTCHA untuk mengidentifikasi bahwa pengguna yang melakukan proses login bukanlah robot.
2. Mampu membangkitkan *One Time Password(*OTP*)* yang akan digunakan oleh pengguna pada saat login.
3. Dapat mengirimkan OTP kepada pengguna melalui pesan singkat pada aplikasi *chatting.*

Aplikasi ini akan menggunakan sistem klien-server, sehingga membutuhkan oneksi internet agar klien dapat mengakses situs web, aktif pada aplikasi *chat,* dan agar dapat melakukan interaksi dengan *database server.* Secara umum arsitektur klien-server ditunjukkan pada gambar 6 dibawah ini.



Gambar 6. Arsitektur Aplikasi

Dari gambar 9 diatas dapat dijelaskan sebagai berikut :

1. Klien mengirim permintaan OTP dengan memasukkan nama pengguna apabila sudah terdaftar.
2. Aplikasi mengirimkan respon .
3. Aplikasi melakukan query nama pengguna pada *database*untuk menemukan akun *instant messaging* dari pengguna yang bersangkutan.
4. Apabila ditemukan, maka aplikasi akan mengirimkan OTP melalui *instant messaging.*
5. OTP tersebut langsung dikirimkan kepada akun pengguna.
6. **METODOLOGI**
7. Penyusunan Proposal Tugas Akhir

Pada tahap ini penulis menyusun proposal tugas akhir sebagai langkah awal dalam pengerjaan tugas akhir. Pada proposal ini penulis menggagas penulisan tugas akhir untuk mengimplementasikan konsep *One-Time-Password* untuk mencegah serangan phishing pada kata sandi

1. Studi Literatur

Pada tahapan ini akan dilakukan studi literatur mengenai cara yang digunakan untuk membuat aplikasi.

1. Implementasi

Implementasi merupakan tahap untuk merancang dan membangun aplikasi.

1. Pengujian dan Evaluasi

Pada tahap ini dilakukan uji coba terhadap aplikasi yang telah dibuat.Tujuan uji coba perangkat lunak adalah untuk menemukan kesalahan-kesalahan (*bug*) sedini mungkin sehingga dapat diperbaiki sesegera mungkin.

1. Penyusunan Buku Tugas Akhir

Tahap terakhir merupakan penyusunan laporan yang memuat dokumentasi mengenai pembuatan serta hasil dari implementasi perancangan dan pembuatan aplikasi yang telah dibuat. Secara garis besar, buku laporan tugas akhir ini terdiri atas beberapa bagian yaitu:

1. Pendahuluan
   1. Latar Belakang
   2. Permasalahan
   3. Batasan Tugas Akhir
   4. Tujuan
   5. Metodologi
   6. Sistematika Penulisan
2. Tinjauan Pustaka
3. Desain dan Implementasi
4. Uji Coba dan Evaluasi
5. Kesimpulan dan Saran
6. Daftar Pustaka
7. **JADWAL KEGIATAN TUGAS AKHIR**

Tugas akhir ini diharapkan bisa dikerjakan menurut jadwal sebagai berikut:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| No. | Kegiatan | Bulan | | | | | | |
| September | | Oktober | | Nopember | | Desember |
| 1 | Penyusunan Proposal Tugas Akhir |  | |  | |  | |  |
| 2 | Studi Literatur |  |  |  | |  | |  |
| 3 | Implementasi |  | |  |  |  | |  |
| 4 | Pengujian dan Evaluasi |  | |  | |  | |  |
| 5 | Penyusunan Buku Tugas Akhir |  | |  | |  |  |  |

1. **DAFTAR PUSTAKA**

[1] http://xmpp.org/about-xmpp/technology-overview/

[2] Alonso, Gustavo, 2004. *Web Service: Concepts, Architecturesand Applications.* Jerman: Springer

[3] Cerami, Ethan, 2002. *Web Services Essensials,* Amerika Serikat: O’Reilly

[4] Fensel, Dieter, 2011. *Semantic Web Services,* Jerman: Springer

[5] Chun Yin Huang, Shang Pin Ma, Kuan-Ta Chen, 2011. *Using One Time Password to Prevent Password Phishing Attacks,* Journal of Network and Computer Application, 22 Februari 2011, 1292-1301

**LEMBAR PENGESAHAN**

###### **Surabaya, 10 Oktober 2012**

Menyetujui,

Pembimbing II

Baskoro Adi Pratomo S.Kom, M.Kom

NIP :

Pembimbing I

Waskitho Wibisono, S.Kom, M.Eng, Ph.D

NIP : 19741022 200003 1 001