# II

metodOlogi penelitian

## Tempat dan Waktu Penelitian

Penelitian ini dilakukan di Jurusan Matematika Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Lampung. Waktu penelitian dilakukan pada semester genap tahun ajaran 2010-2011.

## Obyek Penelitian

Obyek dari penelitian ini adalah masalah keamanan proses autentikasi pada suatu aplikasi atau sistem (studi kasus: aplikasi Ujian *Online* Jurusan Matematika FMIPA Universitas Lampung. Proses autentikasi akan menjadi sangat rentan terhadap serangan *sniffer* jaringan (*replay attack*) ketika *user* menggunakan *password* yang sama (*password* statis) untuk masuk ke-dalam suatu sistem. Sehingga dalam hal ini diperlukan suatu cara *alternatif* untuk mengamankan proses autentikasi agar informasi penting yang dimiliki *user* tidak jatuh ke tangan pihak-pihak yang tidak berwenang.

Penggunaan metode autentikasi *one time password* adalah salah satu alternatif untuk menangani masalah keamanan proses autentikasi aplikasi atau sistem tersebut. Ada beberapa alasan mengapa penulis menggunakan metode keamanan tersebut pada proses autentikasi adalah sebagai berikut:

1. Dapat menangani tindakan *replay attack*, hal ini dikarenakan pada proses autentikasi, *password* yang sebenarnya tidak di lewatkan pada jaringan sehingga *password* sebenarnya menjadi lebih aman.
2. Password yang dihasilkan berupa *one time password* selalu berubah-ubah dan hanya bisa digunakan untuk sekali proses *login* saja. Sehingga jika seseorang mendapatkan, OTP tersebut tidak akan bisa digunakan kembali dalam proses *login* berikutnya.
3. Tidak ada informasi rahasia yang disimpan sehingga jika seseorang berusaha mencari data yang tersimpan hal tersebut menjadi tidak berguna.
4. Metode autentikasi OTP menggunakan fungsi hash dalam pembuatan sebuah *password*, sehingga akan sangat sulit untuk membalikkan fungsi tersebut.

## Tahapan Penelitian

Tahapan penelitian yang dilakukan dalam penelitian ini mengacu kepada model pengembangan aplikasi yang digunakan, yaitu model *waterfall* dimana terdapat lima (5) proses tahap pengerjaan penelitian ini sebagai berikut:

1. Analisis Kebutuhan

Pada tahapan ini dilakukan pencarian sebuah masalah, solusi penyelesaian dan studi referensi. Adapun masalah penelitian ini adalah ketika *user* atau *admin* melakukan *login*, sebuah paket atau data *login* yang dikirim menuju ke *server* telah dibelokkan arah oleh *sniffer*, sehingga paket harus melalui *sniffer* untuk sampai kepada *server*. Gambar 3.1 menunjukkan data *login* *admin* dan *user* yang tertangkap aplikasi Cain & Abel oleh *sniffer*.



Gambar 3.1 Data *Login* yang Tertangkap

Setelah data *login* tertangkap, kemudian *sniffer* dengan segera menggunakan salah satu dari data *login* tersebut untuk masuk ke aplikasi Ujian *Online*. Dalam hal ini data *login* yang akan dimasukkan oleh *sniffer* adalah data *login* dengan nilai *Username* “**rajha**” dan *Password* “**rahasia123**”.



Gambar 3.2 Data *Login* yang Di-*input* *Sniffer*

Ternyata dengan data *login* tersebut *sniffer* dapat dengan sukses masuk ke halaman *admin* yang dapat dilihat pada Gambar 3.3.



Gambar 3.3 *Sniffer* Sukses Masuk ke Halaman *Admin*

Metode autentikasi *one time password* (OTPA) dibuat untuk mengatasi masalah tersebut. Setelah suatu *password* dipakai, maka *password* yang sama tidak dapat dipakai untuk kedua kalinya.

Mengingat masalah dari penelitian ini adalah tentang keamanan sistem autentikasi, studi kepustakaan dilakukan dengan cara mengumpulkan referensi atau data-data melalui buku-buku komputer, jurnal ilmiah dan situs *website* yang berhubungan dengan keamanan sistem informasi (khususnya pada proses autentikasi sistem dengan metode *one time password*) dan pengembangan aplikasi berbasis *mobile* dengan J2ME (khususnya *token software*). Referensi atau data-data yang telah terkumpul di sortir sesuai dengan bidang pembahasan.

1. Desain Aplikasi/Sistem

Pada tahap ini dilakukan perancangan solusi berdasarkan analisis kebutuhan. Ada dua (2) tahap perancangan yang dilakukan, yaitu:

1. Perancangan aplikasi *Mobile Token* yang akan digunakan sebagai *password/*PIN generator ketika *user* ingin masuk ke aplikasi Ujian *Online*.
2. Perancangan pengembangan pada bagian proses autentikasi aplikasi Ujian *Online* Jurusan Matematika FMIPA Universitas Lampung. Dengan kata lain tahap perancangan ini khususnya dilakukan dengan memodifikasi metode autentikasi yang ada menjadi metode autentikasi *One Time Password* (OTPA).

Adapun *tools* yang digunakan dalam tahap perancangan aplikasi atau sistem ini adalah sebagai berikut:

1. Diagram *Use Case* untuk menjelaskan interaksi antara *user* dengan aplikasi yang dibuat.
2. Diagram *Activity* untuk menggambarkan berbagai alir aktivitas dalam sistem yang sedang dirancang, bagaimana masing-masing alir berawal, *decision* yang mungkin terjadi, dan bagaimana mereka berakhir.
3. Diagram *Sequence* untuk menggambarkan interaksi antar objek di dalam dan di sekitar sistem berupa *message* yang digambarkan terhadap waktu.
4. Diagram *Class* untuk menampilkan struktur dari sebuah sistem.
5. Penulisan Program

Pada tahap ini dilakukan dua (2) tahap penulisan program berdasarkan desain aplikasi/sistem yang telah dilakukan sebagai berikut:

* 1. Penulisan Program Aplikasi *Mobile Token*

Pembuatan aplikasi *Mobile Token* menggunakan bahasa pemrograman J2ME, Notepad++ sebagai *source code editor*, dan Sun Java™ Wireless Toolkit 2.5 sebagai emulator *handphone*. Adapun fungsi-fungsi yang terdapat pada aplikasi *Mobile Token*, yaitu:

1. Fungsi Pembuatan *Secret Code*

*Secret Code* dihasilkan oleh fungsi hash MD5 dimana string yang di input pada fungsi tersebut adalah angka acak sepanjang 20 karakter. Inisialisasi *Secret Code* harus dilakukan dan dimasukkan ke *database* aplikasi Ujian *Online* agar proses autentikasi dapat berjalan dengan baik.

1. Fungsi Pembangkitan PIN *Login*

PIN dibangkitkan menggunakan algoritma OTPA dengan mode *Challenge Response* (CR). PINini digunakan untuk proses *login* agar masuk ke dalam aplikasi Ujian *Online*.

1. Fungsi Pembangkitan PIN Ujian

PIN dibangkitkan menggunakan algoritma OTPA dengan mode *Response* *Only* (RO). PINini digunakan untuk proses memulai ujian.

* 1. Penulisan Program Aplikasi Ujian *Online*

Penulisan program aplikasi Ujian *Online* tidak dilakukan dari awal, dengan kata lain aplikasi tersebut sudah ada sebelumnya. Hanya saja akan dilakukan modifikasi pada proses autentikasi. Aplikasi tersebut dikerjakan menggunakan IDE Macromedia Dreamweaver 8.0 sebagai editor atau *application developer* dan MYSQL sebagai basis data-nya.

1. Pengujian Program

Pada tahap ini dilakukan pengujian dengan metode *black box* dimana pengujian difokuskan pada spesifikasi fungsional aplikasi.

Ada dua (2) fase pengujian yang dilakukan, yaitu:

* 1. Pengujian Aplikasi *Mobile Token*

Setelah *project* aplikasi di *deploy* aplikasi *Mobile Token* diuji dengan cara menginstall aplikasi tersebut ke beberapa *handphone* yang berbeda. Hal ini dilakukan untuk mendapatkan pemetaan spesifikasi *handphone* yang *compatible* dengan aplikasi tersebut.

* 1. Pengujian Aplikasi Ujian *Online*

Setelah pengujian aplikasi *Mobile Token* dilakukan, berikutnya adalah pengujian aplikasi Ujian *Online*. Fokus utama dari pengujian ini adalah keberhasilan proses autentikasi pada aplikasi Ujian *Online* ketika aplikasi tersebut diintegrasikan dengan aplikasi *Mobile Token* yang telah terinstal pada *handphone*. Pengujian dilakukan dengan cara beberapa *user* melakukan proses *login* ke aplikasi Ujian *Online* secara bersamaan menggunakan *handphone* yang telah terinstall aplikasi *Mobile Token* sebelumnya.

1. Penerapan Program

Pada tahap ini dilakukan instalasi aplikasi *Mobile Token* pada *handphone* setiap *user* dan instalasi aplikasi Ujian *Online* pada sebuah *server* lokal. Setelah tahapan ini dilakukan dan tidak ada perubahan lagi, maka secara keseluruhan tahap penelitian dan pengembangan perangkat lunak selesai.

## Proses Alur Kerja Autentikasi *One Time Password* (OTPA)

Adapun alur kerja yang terjadi saat proses autentikasi berjalan pada kedua sisi, yaitu pada sisi *Mobile Token* dilakukan pembangkitan sebuah *password/*PIN dan *password/*PIN yang dihasilkan kemudian dibandingkan dengan *password/*PIN yang dihasilkan aplikasi Ujian O*nline.* Jika ternyata kedua *password/*PIN sama maka proses *login* sukses sebaliknya jika berbeda maka proses *login* ditolak.



Gambar 3.4 Proses Dasar Autentikasi *One Time Password* Mode RO



Gambar 3.5 Proses Dasar Autentikasi *One Time Password* Mode CR



Gambar 3.6 Konsep Kerja OTPA Mode CR (*Menu* *Login*)



Gambar 3.7 Konsep Kerja OTPA Mode RO (*Menu* Ujian)