OTENTIKASI BERBASIS CHALLENGE / RESPONSE PADA APLIKASI BERBASIS INTERNET

AGUS MUHAMMAD RAMDAN
41505120059

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS MERCU BUANA
JAKARTA
2011

OTENTIKASI BERBASIS CHALLENGE / RESPONSE PADA APLIKASI BERBASIS INTERNET

Laporan Tugas Akhir

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Oleh:
AGUS MUHAMMAD RAMDAN
41505120059

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS MERCU BUANA
JAKARTA
2011

DAFTAR GAMBAR

Halaman

1.	GAMBAR 2.1.	Diagram Blok Kritografi Modern	10
2.	GAMBAR 2.2.	Fungsi Hash Satu Arah	12
3.	GAMBAR 2.3.	Klasifikasi Jenis Diagaram UML	17
4.	GAMBAR 3.1.	Pengiriman Password (P) Dalam Bentuk Plainteks	22
5.	GAMBAR 3.2.	Pengirim Password (P) Dalam Bentuk Keluaran Fungsi Hash	22
6.	GAMBAR 3.3.	Verifikasi Password Yang Dikirm Dalam Bentuk Message Digest	23
7.	GAMBAR 3.4.	Verifikasi Password Yang Dikirm Dalam Bentuk Digest	24
8.	GAMBAR 3.5.	Replay Attack Pada Pengiriman Password	24
9.	GAMBAR 3.6.	Skema Otentikasi Dengan Memanfatkan Nonce	25
10.	GAMBAR 3.7.	Verifikasi Password Dengan Menggunakan Nonce	26
11.	GAMBAR 3.8.	Use Case	31
12.	GAMBAR 3.9.	Activity Diagram	34
13.	GAMBAR 3.10.	Pendaftaran Sequence Diagram	35
14.	GAMBAR 3.11.	Login Sequence Diagram	35
15.	GAMBAR 3.12.	Ganti Password Sequence Diagram	36
16.	GAMBAR 3.13.	Transaksi/Aksi Sequence Diagram	37
17.	GAMBAR 3.14.	Kelas Diagram	39

18.	GAMBAR 3.15.	Kelas Diagram	40
19.	GAMBAR 3.16.	Register Pengguna	44
20.	GAMBAR 3.17.	Permintaan Challenge	44
21.	GAMBAR 3.18.	Challenge Login Form	45
22.	GAMBAR 3.19.	Challenge Transaksi/Aksi Form	45
23.	GAMBAR 3.20.	Otentikasi Berhasil Transaksi/Aksi Form	46
24.	GAMBAR 3.21.	Otentikasi Gagal Transaksi/Aksi Form	46
25.	GAMBAR 3.19.	Ganti Password	47
26.	GAMBAR 3.20.	Token Password	47
27.	GAMBAR 4.1	Layar-Layar Pada Saat Pendaftaran Pengguna	55
28.	GAMBAR 4.2.	Layar-Layar Pada Saat Login	55
29.	GAMBAR 4.3	Layar-Layar Pada Saat Transaksi	56
30.	GAMBAR 4.4	Layar-Layar Pada Saat Ganti Password	49
31.	GAMBAR 4.5.	Token Desktop	50
32.	GAMBAR 4.6.	Hasil Junit	57

DAFTAR ISI

LEMBAR PERNYATAAN ..... **i**
LEMBAR PERSETUJUAN ..... **ii**
KATA PENGANTAR ..... **iii**
ABSTRACTION ..... **v**
ABSTRAKSI ..... **vi**
DAFTAR ISI ..... **vii**
DAFTAR GAMBAR ..... **x**
DAFTAR TABEL ..... **xii**
BAB I PENDAHULUAN **1**
1.1. Latar Belakang 1
1.2. Perumusan Masalah 3
1.3. Maksud Dan Tujuan 3
1.4. Batasan Masalah Penelitian 3
1.5. Metodologi Penelitian 3
1.6. Sistematika Penulisan 4
BAB II LANDASAN TEORI **5**
2.1. Keamanan Komputer (Computer Security) 5
2.2. Konsep Dasar Kriptograpi 9
2.2.1. Kriptograpi (Crytpgraphy) 9
2.2.2. Fungsi Hash 10
2.2.3. Message Auntentication Code (MAC) 12
2.2.4. Tanda Tangan Digital (Digital Signature) 13
2.2.5. Pembangkit Bilangan Acak Semu (PBAS) 14
2.3. Konsep Otentikasi 14
2.3.1. Password 15
2.3.2. One-Time Password(OTP) 15
2.3.3. Challenge / Response 15

2.4. Unified Modeling Language (UML) 15
2.4.1. Use Case Diagram 17
2.4.2. Activity Diagram 19
2.4.3. Sequence Diagram 20
2.4.4. Class Diagram..... 15
BAB III ANALISIS DAN PERANCANGAN 21
3.1. Analisis Permasalahan 21
3.1.1. Analisis Serangan Pasif..... 22
3.1.2. Analisis Serangan Aktif 24
3.1.3. Analisis Otentikasi Challenge Resposne..... 25
3.1.3. Replay Attacks pada CookieStore Session..... 25
3.2. Analisis Token..... 27
3.3. Analisa Kebutuhan Pembangunan Aplikasi..... 29
3.3.1. Deskripsi Umum Sistem 29
3.3.2. Analisis Spesifikasi dan Kebutuhan Aplikasi..... 29
3.3.3. Use case Model..... 31
3.3.4. Activity Diagaram..... 34
3.3.5. Sequennce Diagaram..... 34
3.3.6. Analisa Kelas 38
3.4. Perancangan Kelas..... 39
3.4.1. Diagram Perancangan Kelas..... 39
3.4.2. Perancangan Database..... 42
3.4.3. Perancangan Modul 43
3.5. Perancangan Antar Muka..... 44
3.5.1. Web App 44
3.5.2. Token Desktop..... 47
BAB IV IMPLEMENTASI DAN PENGUJIAN..... 49
4.1. Lingkungan Implementasi..... 49
4.2. Implementasi Kelas..... 49
4.3. Implementasi Modul..... 54
4.4. Implementasi Antar Muka..... 54
4.5. Pengujian Aplikasi..... 57

4.5.1. Pengujian hasil Token 57
4.5.2. Test Token Simulasi 57
4.5.3. Test Token pada Aplikasi WEB 61
4.5.4. PenggujianPerformance Aplikasi 68
4.5.5. Analisa Hasil Pengujian 69
BAB V KESIMPULAN DAN SARAN 71
5.1. Kesimpulan..... 71
5.2. Masukan Dan Saran 72
DAFTAR PUSTAKA..... 73
LAMPIRAN 75

DAFTAR TABEL

Halaman

1.	TABEL 2.1	Jenis Diagaram Resmi UML	16
2.	TABEL 2.2	Notasi use case diagram	18
3.	TABEL 3.1	Pemetaan Atribut Kelas Menjadi Kolom Pada Tabel TBL_NONCE_TOKEN	42
4.	TABEL 3.1	Pemetaan Atribut Kelas Menjadi Kolom Pada Tabel TBL_MT_USER	43
5.	TABEL 4.1	Daftar Implementasi Modul	54
6.	TABEL 4.2	Pengujian Performansi Tanpa Database	68
7.	TABEL 4.3	Pengujian Performansi Dengan Database	69

KATA PENGANTAR

Puji syukur Alhamdulillah kehadirat Allah SWT yang telah melimpahkan segala rahmat dan karuniaNya, sehingga penulis dapat menyelesaikan laporan tugas akhir yang merupakan salah satu persyaratan untuk menyelesaikan program studi strata satu (S1) pada Jurusan Teknik Informatika Universitas Mercu Buana.

Penulis menyadari bahwa laporan tugas akhir ini masih jauh dari sempurna. Karena itu, kritik dan saran akan senantiasa penulis terima dengan senang hati.

Dengan segala keterbatasan, penulis menyadari pula bahwa laporan tugas akhir ini takkan terwujud tanpa bantuan, bimbingan, dan dorongan dari berbagai pihak. Untuk itu, dengan segala kerendahan hati, penulis menyampaikan ucapan terima kasih kepada:

1. Bapak Abdusy Syarif, ST., MT, selaku pembimbing tugas akhir pada Jurusan Teknik Informatika Universitas Mercu Buana.
2. Ibu Ida Nurhaida ST., MT, selaku Koordinator tugas akhir pada Jurusan Teknik Informatika Universitas Mercu Buana.
3. Ibu Devi Fitrianah, S.Kom., MTI selaku kepala program studi Teknik Informatika pada Jurusan Teknik Informatika Universitas Mercu Buana.
4. Bapak dan Ibu tercinta yang telah mendukung penulis baik spirit maupun materi.
5. Isteriku tercinta yang selalu memberikan spirit maupun materi untuk terus meyelesaikan tugas akhir ini
6. Anak-anakku yang lucu-lucu yang sering hadir menemani saat mengerjakan tugas akhir ini.
7. Sahabatku Andoko yang selalu mengingatkan kami untuk menyelesaikan tugas akhir ini tepat waktu.

8. Saudara dan sahabat-sahabatku terutama Kawan-kawan Angkatan 2006 yang telah memberikan dukungan moral untuk terus meyelesaikan tugas akhir ini

Semoga Allah SWT membalas kebaikan dan selalu mencurahkan hidayah serta taufikNya, Amin.

Jakarta, 1 Juni 2011

Penulis

LEMBAR PERNYATAAN

Yang bertanda tangan dibawah ini:

NIM : 41505120059

Nama : AGUS MUHAMMAD RAMDAN

Judul Skripsi : OTENTIKASI BERBASIS CHALLENGE / RESPONSE PADA APLIKASI BERBASIS INTERNET

Menyatakan bahwa skripsi tersebut diatas adalah hasil karya saya sendiri dan bukan plagiat. Apabila ternyata ditemukan didalam laporan skripsi saya terdapat unsur plagiat, maka saya siap untuk mendapatkan sanksi akademik yang terkait dengan hal tersebut.

Jakarta, 10 Juni 2011

(Agus Muhammad Ramdan)

LEMBAR PERSETUJUAN

NIM : 41505120059

Nama : AGUS MUHAMMAD RAMDAN

Judul Skripsi : OTENTIKASI BERBASIS CHALLENGE / RESPONSE PADA APLIKASI BERBASIS INTERNET

SKRIPSI INI TELAH DIPERIKSA DAN DISETUJUI

JAKARTA, 1 JUNI 2011

Abdusy Syarif, ST., MT
Pembimbing

Ida Nurhaida ST., M.T
Koord. Tugas Akhir Teknik Informatika

Devi Fitrianah, S.Kom., MTI
KaProdi Teknik Informatika