PENGAMANAN DATA MENGGUNAKAN OPENSSL PADA APLIKASI BERBASIS WEB

ANDOKO PRIYO DARMANTO
41505120034

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

PENGAMANAN DATA MENGGUNAKAN OPENSSL PADA APLIKASI BERBASIS WEB

Laporan Tugas Akhir

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Oleh:
ANDOKO PRIYO DARMANTO
41505120034

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

LEMBAR PERNYATAAN

Yang bertanda tangan dibawah ini:

NIM : 41505120034

Nama : ANDOKO PRIYO DARMANTO

Judul Skripsi : PENGAMANAN DATA MENGGUNAKAN OPENSSL PADA APLIKASI BERBASIS WEB

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

(ANDOKO PRIYO DARMANTO)

LEMBAR PERSETUJUAN

NIM : 41505120034

Nama : ANDOKO PRIYO DARMANTO

Judul Skripsi : PENGAMANAN DATA MENGGUNAKAN OPENSSL PADA APLIKASI BERBASIS WEB

SKRIPSI INI TELAH DIPERIKSA DAN DISETUJUI

JAKARTA, 10 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

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, terima kasih atas bantuan dan bimbingan serta waktunya dalam menyelesaikan tugas akhir ini.
2. Bapak, Ibu dan Adik tercinta yang telah mendukung penulis baik spirit maupun materi.
3. Para Dosen dan Staff administrasi Universitas Mercu Buana
4. Saudara dan Sahabatku terutama Angkatan VIII IT PKSM Universitas Mercu Buana, terima kasih atas kebersamaan serta kekompakannya selama ini

Serta pihak-pihak lain yang tidak dapat penulis sebutkan namanya satu persatu. Semoga Allah SWT membalas kebaikan dan selalu mencurahkan hidayah serta taufikNya, Amin.

Jakarta, Juni 2011

Penulis

DAFTAR ISI

Halaman

LEMBAR PERNYATAAN ……. i

LEMBAR PERSETUJUAN…..…… ii

KATA PENGANTAR …… iii

ABSTRACT ……..……. iv

ABSTRAKSI ..…… v

DAFTAR ISI ……... vi

DAFTAR GAMBAR ..…… x

DAFTAR TABEL …… xiii

BAB I PENDAHULUAN

1.1 Latar Belakang Masalah 1

1.2 Perumusan Masalah …...…….…… 2

1.3 Tujuan Penulisan …...…….…… 3

1.4 Batasan Masalah …….. 3

1.5 Metodologi Penelitian …….…….... 4

1.6 Sistematika Penulisan …… 4

BAB II LANDASAN TEORI

2.1 Pengertian Internet …….……... 6

2.2 *Secure Socket Layer* (SSL) ……..……..... 6

2.2.1 Cara Kerja *Secure Socket Layer* (SSL) …….. 7

2.2.2 Kriptografi ……. 8

2.2.3 Sertifikat …..……...……... 11

2.3 Apache *Web Server* .....……..……. 12

2.3.1 Struktur Konfigurasi ……..... 13

2.4 OpenSSL ……... 14

2.5 *HyperText Markup Language* (HTML) …….……... 15

2.6 PHP ……... 15
2.7 Pengertian Umum Rekayasa Perangkat Lunak …… 16
2.7.1 Pengertian *Unified Modeling Language* (UML) ……... 18
2.7.2 Diagram *Unified Modeling Language* (UML) …….. 18
2.8 Basis Data 22
2.8.1 Teknik *Entity Relationship Diagram* (ERD) …… 23

BAB III ANALISIS DAN PERANCANGAN

3.1 Analisis Permasalahan ……..... 25
3.2 Analisis Serangan terhadap Kemanan Data ……..... 25
3.2.1 Sniffing ……..... 25
3.2.2 Session Hijacking ……..... 27
3.2.3 Password …… 28
3.2.4 Kesalahan pengetikan *hypertext transport protokol secure* (HTTPS) ……. 28
3.3 Analisis *Secure Socket Layer* (SSL) …… 29
3.3.1 Analisis *Handshake Sequence* ……... 29
3.3.2 Analisis Protokol *Secure Socket Layer* (SSL) …… 32
3.3.3 Analisis *Mesage Authenticate Code* (MAC) ……. 39
3.4 Analisis *Web Server Apache* dan *Secure Socket Layer* (SSL) …… 39
3.5 Analisis *Virtual Host* ……... 41
3.6 Analisis Dampak Sistem ……. 41
3.7 Analisa Kebutuhan Implementasi *Secure Socket Layer* (SSL) ……... 42
3.7.1 Deskripsi Umum Sistem ……..... 43
3.7.2 Analisis Spesifikasi dan Kebutuhan Aplikasi 43
3.8 Perancangan *Secure Socket Layer* (SSL) …… 44
3.8.1 Kriptografi ……. 44
3.8.2 Sidik jari *(Thumbprint*) …….. 44
3.8.3 Sertifikat ……. 45
3.9 OpenSSL …….. 47

3.10 Perancangan Konfigurasi Jaringan ……... 48
3.11 Perancangan Program Aplikasi ……. 48
3.11.1 *Unified Modelling Language* (UML) ……..... 50
3.12 Perancangan Layar Aplikasi ……. 59
3.13 Perancangan Basis Data …… 61

BAB IV IMPLEMENTASI DAN PENGUJIAN

4.1 Spesifikasi Komputer dalam Implementasi dan Pengujian ……. 63
4.2 Batasan Implementasi ……... 63
4.3 Implementasi *Virtual Host* pada *Web Server* Apache ……... 64
4.4 Implementasi *Secure Socket Layer* (SSL) pada *Virtual Host Web Server* Apache ……... 65
4.5 Implementasi Sertifikat ……. 68
4.5.1 Sertifikat *Server* ……... 69
4.5.2 Sertifikat *Client* ……... 70
4.5.3 Sertifikat *Certificate Authority* (CA) ……... 71
4.5.4 Implementasi Sertifikat pada *Browser Client* …….. 74
4.6 Implementasi Antar Muka Aplikasi *Web Server* ..……..... 75
4.7 Pengujian ……... 77
4.7.1 Pengujian *Black Box* ……..……..... 77
4.7.2 Pengujian Keamanan *Security Socket Layer* (SSL) pada *Web Server* …….……..... 78
4.7.3 Pengujian *Log* …….. 83
4.7.4 Analisa Hasil Pengujian 84
4.7.5 *Troubleshooting* pada *Secure Socket Layer* (SSL) ……..... 85

BAB V KESIMPULAN DAN SARAN

5.1 Kesimpulan ……..…… 87
5.2 Saran …… 88

DAFTAR PUSTAKA ……. 89
LAMPIRAN ……. 91

DAFTAR GAMBAR

Halaman

1. GAMBAR 2.1. GAMBARAN UMUM CARA KERJA SSL [SUMBER: IETF 108] ..…… 7
2. GAMBAR 2.2. ALGORITMA SIMETRIS [SUMBER: DONY ARIYUS 108] ……. 9
3. GAMBAR 2.3 ALGORITMA ASIMETRIS [SUMBER: DONY ARIYUS 109] …….. 10
4. GAMBAR 2.4 ALGORITMA HIBRIDA [SUMBER:P.K.YUEN 656] …….. 11
5. GAMBAR 2.5 HIRARKI SERTIFIKAT [SUMBER: STEPHEN THOMAS 34] ……... 12
6. GAMBAR 2.6 PERINGKAT PENGGUNAAN WEB SERVER DARI NETCRAFT.COM …… 13
7. GAMBAR 2.7 STRUKTUR BERKAS HTTPD.CONF [SUMBER: RALF S. ENGELSCHALL 65] …… 14
8. GAMBAR 2.8 KONSEP KERJA PHP [SUMBER: WWW.PHP.NET] …….. 16
9. GAMBAR 2.9 TAHAPAN REKAYASA PERANGKAT LUNAK [SUMBER: ROGER. S. PRESSMAN 21] …….. 17
10. GAMBAR 2.10 MODEL PEMBELIAN TIKET [SUMBER: ADI NUGROHO 51] …….. 19
11. GAMBAR 2.11 CLASS DIAGRAM [SUMBER: ADI NUGROHO 110] …….. 20
12. GAMBAR 2.12 COMPONENT DIAGRAM [SUMBER: ADI NUGROHO 200] …….. 21
13. GAMBAR 2.13 DEPLOYMENT DIAGRAM [SUMBER: ADI NUGROHO 210] …… 21
14. GAMBAR 2.14 ISTILAH DALAM DATABASE [SUMBER: THOMAS M. CONNOLLY 24] ……. 23
15. GAMBAR 2.15 ONE TO ONE RELATIONSHIP [SUMBER: THOMAS M. CONNOLLY 156] ... …… 23
16. GAMBAR 2.16 ONE TO MANY RELATIONSHIP [SUMBER: THOMAS M. CONNOLLY 157] …… 24
17. GAMBAR 2.17 MANY TO MANY RELATIONSHIP [SUMBER: THOMAS M. CONNOLLY 158] …… 24
18. GAMBAR 3.1. HASIL PENCARIAN PADA SITUS WWW.GOOGLE.COM ……. 26
19. GAMBAR 3.2. HASIL PENYADAPAN PROGRAM CAIN & ABEL.……... 26
20. GAMBAR 3.3. SESSION HIJACKING …….. 28
21. GAMBAR 3.4. PROSES HANDSHAKE SEQUENCE [SUMBER: IETF 22] …….. 31
22. GAMBAR 3.5. KOMPONEN PROTOKOL SSL [SUMBER: STEPHEN THOMAS 69] .. 33
23. GAMBAR 3.6. STRUKTUR HANDSHAKE MESSAGE [SUMBER: STEPHEN THOMAS 75] …… 34
24. GAMBAR 3.7. STRUKTUR RECORD MESSAGE [SUMBER: STEPHEN THOMAS

70] ……. 37
25. GAMBAR 3.8. STRUKTUR PESAN PROTOKOL SSL …… 38
26. GAMBAR 3.9 ARSITEKTUR APACHE WEB SERVER …… 40
27. GAMBAR. 3.10 PROSES PEMBUATAN SIDIK JARI DIGITAL …… 45
28. GAMBAR 3.11 SERTIFIKAT X.509 …… 46
29. GAMBAR 3.12 SERTIFIKAT PAYPAL …… 46
30. GAMBAR 3.13 GAMBARAN UMUM APLIKASI …… 49
31. GAMBAR 3.14 USE CASE DIAGRAM …… 50
32. GAMBAR 3.15 ACTIVITY DIAGRAM ……. 53
33. GAMBAR 3.16 ACTIVITY DIAGRAM SSL HANDSHAKE 1 …… 54
34. GAMBAR 3.17 ACTIVITY DIAGRAM SSL HANDSHAKE 2 …… 55
35. GAMBAR 3.18 CLASS DIAGRAM …… 56
36. GAMBAR 3.19 STATECHART DIAGRAM ……... 57
37. GAMBAR 3.20 DEPLOYMENT DIAGRAM ……. 58
38. GAMBAR 3.21 DIAGRAM COMPONENT ……... 58
39. GAMBAR 3.22 LAYAR UTAMA ……... 59
40. GAMBAR 3.23 RANCANGAN LAYAR MENU UTAMA ……... 60
41. GAMBAR 3.24 RANCANGAN LAYAR UTAMA PENGGUNA ……. 62
42. GAMBAR 4.1. KONFIGURASI BERKAS VHOST.CONF ……... 64
43. GAMBAR 4.2. KONFIGURASI BERKAS SSL.CONF …….. 66
44. GAMBAR 4.3 PEMBUATAN PRIVATE KEY SERVER ……. 69
45. GAMBAR 4.4. PEMBUATAN BERKAS SERVER.CSR …….. 70
46. GAMBAR 4.5. SERTIFIKAT ERROR …… 70
47. GAMBAR 4.6 PEMBUATAN SERTIFIKAT CLIENT ……. 71
48. GAMBAR 4.7. PEMBUATAN SERTIFIKAT CERTIFICATE AUTHORITY (CA) …… 72
49. GAMBAR 4.8. ERROR VERIFIKASI PADA SERTIFIKAT SERVER ……. 73
50. GAMBAR 4.9 ERROR MESSAGE CLIENT AUTHENTICATION ……. 74
51. GAMBAR 4.10 SERTIFIKAT INTERNET EXPLORER (IE) …… 75
52. GAMBAR 4.11 IMPLEMENTASI TAMPILAN HALAMAN UTAMA …… 75
53. GAMBAR 4.12 IMPLEMENTASI TAMPILAN HALAMAN REGISTER ……... 76
54. GAMBAR 4.13 IMPLEMENTASI TAMPILAN HALAMAN DOKUMEN ……. 76
55. GAMBAR 4.14 IMPLEMENTASI TAMPILAN HALAMAN LIHAT DOKUMEN ……. 77
56. GAMBAR 4.15 CAPTURING HTTPS …… 79
57. GAMBAR 4.16 PENCARIAN KATA “JAKARTA SELATAN” ……... 80
58. GAMBAR 4.17 PREFERENCES SSL APLIKASI WIRESHARK ……. 81
59. GAMBAR 4.18 HASIL REKAM SSL DENGAN APLIKASI WIRESHARK ……... 81

60. GAMBAR 4.19 CAIN & ABEL SNIFER DAN MODE ARP ……. 82
61. GAMBAR 4.20 HASIL APR-HTTPS …….. 83
62. GAMBAR 4.21 LOG SSL_ERROR.TXT …… 84
63. GAMBAR 4.22 LOG SSL_ACCESS.TXT ……... 85

DAFTAR TABEL

Halaman

1. TABEL 2.1 NOTASI PADA ACTIVITY DIAGRAM [SUMBER: ADI NUGROHO 61]……. 19
2. TABEL 2.2 NOTASI PADA STATECHART DIAGRAM [SUMBER: ADI NUGROHO 188]…… 20
3. TABEL 3.1. DAFTAR PESAN HANDSHAKE SEQUENCE [SUMBER: STEPHEN THOMAS 76] ……... 30
4. TABEL 3.2. DAFTAR NILAI DARI HANDSHAKE PROTOCOL [SUMBER: STEPHEN THOMAS 76] …… 34
5. TABEL 3.3. DAFTAR FATAL ALERT [SUMBER: STEPHEN THOMAS 73] …….. 36
6. TABEL 3.4. DAFTAR STRUKTUR RECORD MESSAGE [SUMBER: STEPHEN THOMAS 70] ……... 38
7. TABEL 3.5. DAFTAR STRUKTUR DISTINGUISHED NAMES [SUMBER: RALF S. ENGELSCHALL 9] ……. 47
8. TABEL 3.6. STRUKTUR TABEL MENU REGISTER ……. 60
9. TABEL 3.7. STRUKTUR TABEL MENU DOKUMEN …… 60
10. TABEL 3.8. STRUKTUR TABEL BUAT DOKUMEN BARU ……. 60
11. TABEL 3.9. STRUKTUR TABEL MENU DOKUMEN …… 61
12. TABEL 3.10. TABEL DATA PENGGUNA …….. 61
13. TABEL 3.11. TABEL DATA PROYEK ……. 62
14. TABLE 4.1. DAFTAR KONFIGURASI VHOST.CONF [SUMBER: RALF S. ENGELSCHALL] …… 65
15. TABEL 4.2. DAFTAR KONFIGURASI SSL.CONF [SUMBER: RALF S. ENGELSCHALL] …… 67
16. TABEL 4.3. KONFIGURASI SECURE SOCKET LAYER (SSL) [SUMBER: RALF S. ENGELSCHALL] …… 68