NAMA	MONTANA GURNING
NIM	11S19017
TOPIK (WEEK 14)	NETWORKING AND INTERNET SECURITY

PROTOKOL

Protokol merupakan aturan yang berisi rangkaian langkah-langkah, yang melibatkan dua atau lebih orang, guna menyelesaikan suatu kegiatan. Adapun contoh dari protocol itu sendiri, yakni:

- Secure Socket Layer / SSL
- IPSec / Internet Protocol Security
- Kerberos
- Transport Layer Security / TLS

Security Socket Layer / SSL

- Protokol untuk browsing web secara aman (web security)
- Menggunakan komunikasi antar client dan server
- Dikembangkan oleh Netscape Communications (1994)
- Ada 2 versi, yakni : v2 dan v3 (v3 umumnya paling banyak digunakan)

TCP / IP (Transmission Control Protocol / Internet Protocol)

TCP/IP merupakan sebuah standard protocol guna menghubungkan komputer dan jaringan dengan jaringan yang lebih besar yaitu INTERNET. SSL akan beroperasi antara protocol komunikasi TCP/IP dan Aplikasi.

Lapisan (dan protocol) untuk browsing dengan SSL

Application (HTTP, FTP, Telnet)
Security (SSL)
Transport (TCP)
Network (IP)
Data Link (PPP)
Physical (modem, ADSL, cable TV)

Cara Kerja TCP/IP tanpa SSL

1. Kebanyakan transmisi pesan di internet dikirim sebagai kumpulan potongan pesan yang disebut PAKET
2. IP bertanggung jawab merutekan paket (komputer awal => komputer tujuan)
3. Pada sisi penerima, TCP memastikan paket sudah samapi, menyusun sesuai nomor urut, dan memastikan paket tiba tanpa perubahan
4. Jika paket ada perubahan / ada data yang hilang, maka TCP meminta kirim ulang

5. TCP/IP tidak memiliki pengaman komunikasi yang bagus (yang dikirimkan berupa plaintext)
6. TCP/IP tidak mengetahui pesan telah diubah oleh man-in-the-middle attack
7. SSL membangun hubungan yang aman atara 2 socket, sehingga pengiriman pesan antara 2 entitas dapat dijamin keamanannya / terjaga kerahasiaannya
8. SSL adalah protocol client-server, yang dimana web browser menjadi client dan website menjadi server
9. Client memulai komunikasi sedangkan server memberi respon terhadap permintaan client
10. Protokol SSL tidak dapat bekerja kalau tidak diaktifkan dahulu (biasanya klik tombol yang ada pada seb server) => pada browser bagian option

Komponen SSL

Antara client dengan server merupakan dua hal yang tidak saling mengenal

SSL disusun atas 2 subprotokol (layer), yakni:

1. SSL Hanshaking => Membangun koneksi (kanal) yang aman berkomunikasi
2. SSL Record => Menggunakan kanal yang sudah aman. Membungkus seluruh data yang dikirim selama koneksi

SSL Handshaking

- Subprotokol yang paling complex
- Tujuannya untuk memungkinkan server & client untuk saling melakukan autentikasi
- Client & server menentukan algo encrypt, Mac Algo, Crypto Key yang dipakai
- Digunakan sebelum melakukan pengiriman paket data
- Bila subprotokol sudah terbentuk, maka http:// akan berubah menjadi https://

HTTP vs HTTPS

- HTTP no encryption & no SSL
- HTTPS terdapat protocol Handshaking

SSL Record

Application
Fragment
Compress
Add MAC
Encrypt
Append SSL Record Header

- Pada sisi penerima, SSL Record melakukan proses berkebalikan. Mendeskripsi data yang diterima, mengontentikasinya (dgn MAC), men-decompresinya, lalu merakitnya
- Protokol SSL akan membuat komunikasi lebih lambat
- Maka ditambahkan piranti keras, seperti kartu PCI / Peripheral Component Interconnect yang dapat dipasang kedalam web server untuk memproses transaksi SSL lebih cepat sehingga mengurangi waktu pemrosesan

Computer server yang memiliki SSL biasanya mempunyai Digital Certificate, yang dikeluarkan oleh CA. Sertifikat dengan kunci public yang dimiliki oleh server. Sertifikat server dinamakan Sertifikat SSL.

NO SERTIFIKAT SLL => YOUR CONNECTION IS NOT SECURE

Apabila terjadi hal seperti diatas, maka koneksi kita dengan server tidaklah aman

Transport Layer Security / TLS

- 1996, Netscape Communications Corp mengajukan SSL ke IETF / Internet Engineering Task Force untuk melakukan standarisasi
- Hasilnya adalah TLS. DIjelaskan di dalam RFC 2246
- TLS merupakan SSL versi 3.1 dan first implementation tahun 1999
- Format record TLS sama dengan Format record SSL
- Mirip SSL versi 3
- Perbedaannya terdapat pada: nomor versi, MACnya, pseurandom functionnya, alert code, dan beberapa komputasi kriptografinya

Rangkuman:

Protocol adalah sekumpulan peraturan atau perjanjian yang menentukan format dan transimi data**.** Layer di sebuah computer akan berkomunikasi dengan layer di computer yang lain. Peraturan dan perjanjian yang di pergunakan dalam komunikasi ini sering di sebut dengan protocol layer. SSL / Secure Socket Layer merupakan sebuah protocol yang digunakan untuk browsing web secara aman (web security). SSL sendiri terdiri dari dua sublayer, yakni: SSL Handshaking dan SSL Record. TLS / Transport Layer Security merupakan penerus dari SSL (Secure Socket Layer) yang menyediakan komunikasi yang aman antara server dan client. Koneksi yang dihasilkan dari TLS dijamin aman karena menggunakan symmetric cryptography yang digunakan untuk melakukan enkripsi setiap data penting yang dikirimkan. Kunci dibuat secara unik saat setiap koneksi terjadi dan didasarkan pada kerahasiaan bersama yang sudah dinegosiasikan diawal.

1. **What services are provided by the SSL Record Protocol?**

   • Confidentiality: The Handshake Protocol defines a shared secret key that is used for conventional encryption of SSL payloads.

   • Message Integrity: The Handshake Protocol also defines a shared secret key that is used to form a message authentication code (MAC).

2. **What steps are involved in the SSL Record Protocol transmission?**

- Application Data
- Fragmentation
- Compress
- Add MAC
- Append SSL Record Header

Record Protocol mengambil pesan aplikasi yang akan ditransmisikan, kemudian melakukan fragmen data ke dalam blok untuk dikelola. Selanjutnya melakukan kompresi data yang biasanya opsional. Kemudian menerapkan MAC, mengenkripsi, menambahkan header, dan mentransmisikan unit yang dihasilkan dalam segmen TCP. Data yang diterima didekripsi, diverifikasi, didekompresi, dan dipasang kembali dan kemudian dikirim ke pengguna tingkat yang lebih tinggi.

3. **What is the purpose of HTTPS?**

HTTPS mempunyai protocol Handshaking. S pada HTTPS adalah singkatan dari "Secure". Ini adalah versi aman dari standar HTTP browser web, digunakan ketika berkomunikasi dengan situs web. HTTPS jauh lebih aman daripada HTTP. Ketika kita terhubung ke server yang diamankan HTTPS, maka akan secara otomatis mengarahkan kita ke HTTPS browser web untuk memeriksa sertifikat keamanan situs web dan memverifikasi bahwa itu dikeluarkan oleh otoritas sertifikat yang sah. Sebagai contoh, jika kita mengunjungi "https://bank.com" di bilah alamat browser web kita, maka akan benar-benar terhubung ke situs web bank kita. Perusahaan yang mengeluarkan sertifikat keamanan menjamin mereka. Sayangnya, otoritas sertifikat terkadang mengeluarkan sertifikat buruk dan sistem rusak. Meskipun tidak sempurna, HTTPS masih jauh lebih aman daripada HTTP.