APTIKOM
ASOSIASI PERGURUAN TINGGI INFORMATIKA DAN KOMPUTER

MODUL PJJ

Mata Ajar

STRATEGI DAN IMPLEMENTASI E-COMMERCE

Topik Bahasan

SISTEM KEAMANAN KOMUNIKASI DALAM ELECTRONIC COMMERCE

Versi

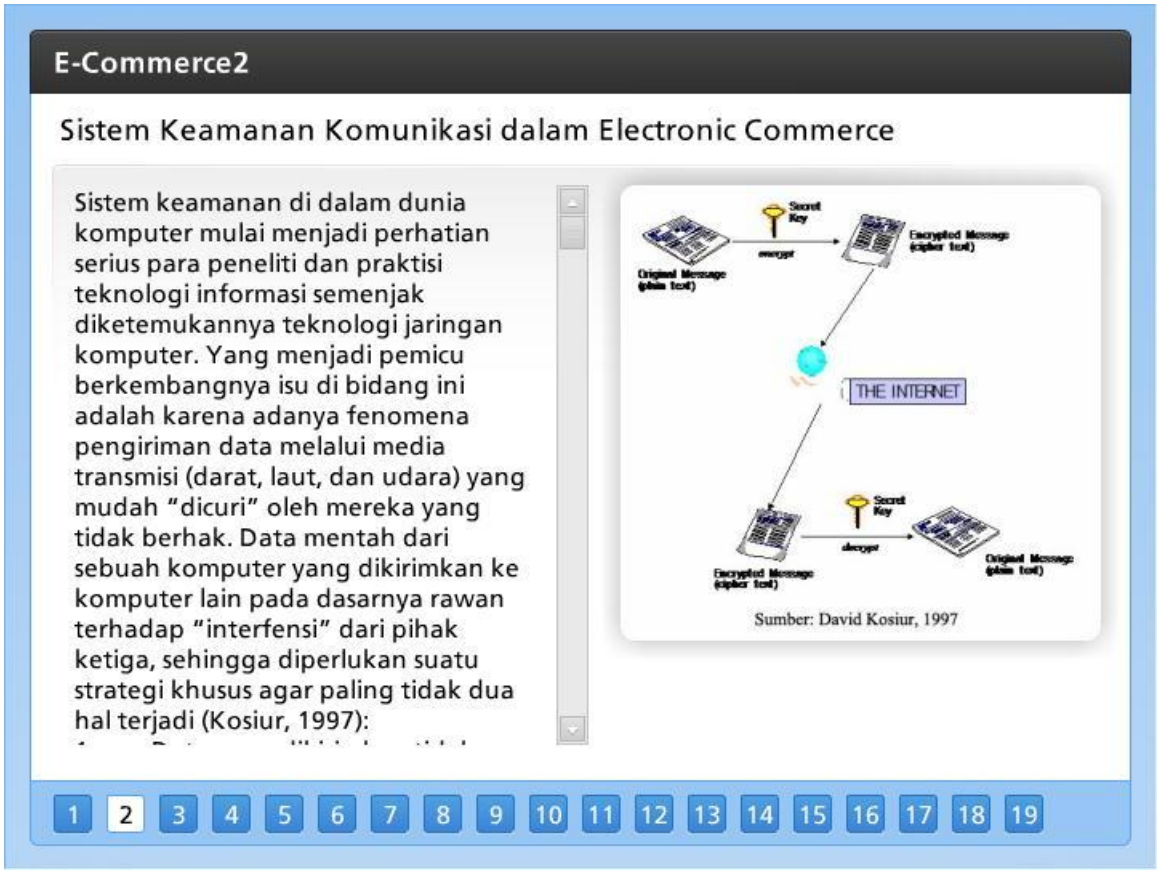
2013/1.0

Nama File

SDIE-8A-SistemKeamanan.pdf

Referensi Pembelajaran

8-A



Sistem keamanan di dalam dunia komputer mulai menjadi perhatian serius para peneliti dan praktisi teknologi informasi semenjak diketemukannya teknologi jaringan komputer. Yang menjadi pemicu berkembangnya isu di bidang ini adalah karena adanya fenomena pengiriman data melalui media transmisi (darat, laut, dan udara) yang mudah "dicuri" oleh mereka yang tidak berhak. Data mentah dari sebuah komputer yang dikirimkan ke komputer lain pada dasarnya rawan terhadap "interfensi" dari pihak ketiga, sehingga diperlukan suatu strategi khusus agar paling tidak dua hal terjadi (Kosiur, 1997):

1. Data yang dikirimkan tidak dapat secara "fisik" diambil oleh pihak lain yang tidak berhak; atau
2. Data yang dikirimkan dapat "diambil secara fisik", namun yang bersangkutan tidak dapat membacanya.

Secara prinsip, pencapaian obyektif kedua lebih mudah dibandingkan dengan yang pertama, karena untuk dapat memproteksi data secara fisik memerlukan teknologi dan biaya yang teramat besar. Prinsip yang kedua sebenarnya sudah

lama berkembang dalam dunia ilmu pengetahuan pada umumnya, yaitu ketika diperkenalkan ilmu sandi (menyamarkan data asli atau data yang sebenarnya ke dalam bentuk lain dengan menggunakan metoda pemetaan tertentu), seperti yang diajarkan di kalangan kepanduan (pramuka) atau militer. Di dalam dunia komputer, teknik penyadian tersebut dinamakan sebagai encryption dan decryption. Encryption adalah proses pengkodean data mentah menjadi data samaran dengan teknik pemetaan tertentu, sementara decryption adalah proses pemetaan kembali dari data samaran menjadi data aslinya. Mekanisme penyandian yang terjadi di dalam dunia internet adalah sebagai berikut.

Katakanlah dua orang yang berbeda lokasi ingin melakukan pertukaran dokumen melalui internet. Is pengirim dan is penerima masing-masing memiliki sebuah "kunci" (misalnya sebuah "password") yang akan dipergunakan sebagai variabel dalam melakukan pemetaan. Berdasarkan rumus atau formula pemetaan tertentu (misalnya rumus matematika sederhana), teks dokumen asli akan diacak atau dienkripsi menjadi sebuah teks yang baru (cipher text). Teks yang "tidak dapat dibaca" ini kemudian barulah dikirimkan ke penerima melalui jalur internet. Untuk dapat membacanya, is penerima akan menggunakan "kunci" yang sama untuk mendekripsikan pesan yang ada. Dengan adanya mekanisme ini, is pengirim dan is penerima dapat melakukan komunikasi secara aman tanpa rasa takut pesannya terbaca oleh mereka yang mencurinya sepanjang jalur komunikasi.

Sumber: David Kosiur, 1997

Kelemahan dari sistem ini adalah sebagai berikut:

- Karena kunci yang dipergunakan sama, berarti masing-masing orang harus memiliki kunci yang berbeda jika ingin berkomunikasi dengan orang lain, yang tentu saja akan sangat repot mengingatnya;
- Jika secara kebetulan dua atau lebih orang memiliki kunci yang sama, maka yang bersangkutan dapat mencuri dan mendeskripsikan pesan orang lain; dan
- Masalah autentifikasi juga akan menjadi isu utama, karena si penerima belum tentu yakin bahwa si pengirim adalah orang yang sesungguhnya, karena

mungkin saja orang lain yang secara sengaja mengetahui kunci enkripsi si pengirim mencoba mengirimkan dokumen atas nama orang lain.

Sumber: David Kosiur, 1997

Terlepas dari kekurangan-kekurangan di atas, mekanisme "symmetric encryption" ini masih cukup baik dipergunakan untuk sebuah jaringan komputer sederhana, dimana data atau informasi yang dikirim tidak memiliki tingkat kerahasiaan yang tinggi. Aplikasinya dalam dunia internet atau E-Commerce misalnya dipergunakan untuk pengiriman dokumen-dokumen standar (brosur, pengumuman, dsb.) baik melalui email maupun attachment. Mekanisme penyandian lainnya yang lebih baik adalah dengan menggunakan metode "public-key cryptography" seperti yang digambarkan di berikut ini. Dalam sistem ini, setiap orang yang akan melakukan komunikasi via internet akan diberikan sebuah kunci (disebut sebagai "public key") yang diketahui oleh semua orang secara terbuka. Jika seseorang ingin mengirimkan sebuah pesan, maka yang bersangkutan diharapkan untuk terlebih dahulu melihat daftar public key (kunci publik) dan mencari tahu kunci publik si penerima.

Kunci inilah yang akan menjadi variabel enkripsi terhadap dokumen atau teks asli tersebut, sebelum dokumen samaran (acak) yang ada dikirimkan melalui internet. Pesan ini baru akan dapat dideskripsikan dengan sebuah "private key" yang hanya diketahui oleh si penerima. Tanpa adanya "private key" tersebut, mustahil seseorang dapat melakukan deskripsi terhadap pesan atau dokumen yang ada. Dengan kata lain, setiap orang yang ingin berkomunikasi akan memiliki sepasang kunci:

1. Kunci yang diketahui oleh umum (public key) dan
2. Kunci yang hanya diketahui secara pribadi (private key).

Dengan adanya sistem semacam ini, maka kekurangan-kekurangan pada metoda "symmetric encryption" dapat teratasi:

- Setiap orang hanya perlu mengingat kunci pribadinya, karena kunci untuk berkomunikasi ke orang-orang lain dapat dengan mudah ditemukan pada daftar kunci;
- Algoritma pemetaan bekerja berdasarkan pasangan kunci, sehingga walaupun seseorang memiliki salah satu kunci yang sama, namun jika pasangan kuncinya berbeda, tidak akan dapat dipergunakan untuk mendeskripsikan pesan orang lain; dan
- Dengan sendirinya problem autentifikasi akan terselesaikan karena yang bersangkutan pasti akan menggunakan kunci yang benar (bukan kunci orang lain) agar dapat dibaca oleh mereka yang memiliki pasangan kuncinya.

Mekanisme penyandian di atas biasa pula dipergunakan dalam dunia E-Commerce untuk menjaga kerahasiaan sebuah data, misalnya:

- Data nomor kartu kredit yang hanya boleh diketahui oleh si pengirim dan bank atau lembaga keuangan tertentu;
- Nomor identifikasi pengguna (user id) dan password yang hanya boleh diketahui oleh konsumen dan perusahaan penyedia jasa E-Commerce;
- Mengirimkan daftar pelanggan beserta rincian profilnya yang secara prinsip merupakan milik perusahaan yang tidak boleh dilihat para saingan bisnis;
- Melakukan download dokumen atau produk digital lainnya yang hanya dapat dibaca oleh mereka yang secara sah telah membeli; dan lain sebagainya.

Satu-satunya kelemahan sistem ini adalah implementasinya secara teknis yang memakan waktu cukup lama untuk melakukan pengkodean dengan kunci publik. Berbagai teknik baru telah diperkenalkan di dunia pengamanan data sebagai alternatif untuk melakukan komunikasi secara lebih cepat sekaligus aman.