Sistem Keamanan

Definisi

Sistem keamanan adalah suatu sistem yang mengamankan sesuatu/aset yang berharga seperti informasi atau benda fisik.

Sidik jari

Salah satu poin dari suatu sistem keamanan adalah otentikasi pengguna. Otentikasi memungkinkan suatu sistem untuk menjaga agar hanya pengguna yang bersangkutan yang memiliki akses pada asetnya. Bentuk otentikasi yang umum diantaranya adalah kode personal seperti kata kunci (*password*) atau kombinasi angka (*Personal Identification Number*). Namun terdapat beberapa masalah pada metode ini seperti diketahuinya kode tersebut oleh pihak lain atau melupakan kodenya. Solusi dari cara ini adalah menggunakan otentikasi biometrik.

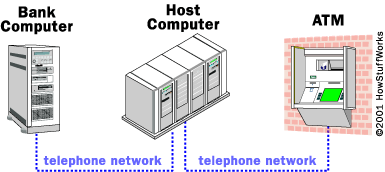
Otentikasi biometrik adalah sistem otentikasi yang memanfaatkan data dari bagian tubuh pengguna yang tidak berubah dan unik untuk setiap orang, seperti wajah, sidik jari, retina, *DNA*, dan lain-lain. Dengan menggunakan data biometrik, keamanan sistem akan jauh lebih tinggi karena informasi ini jauh lebih susah untuk dicuri oleh pihak lain, dan tidak bisa hilang kecuali pada kondisi ekstrem.

Mesin ATM

Salah satu aplikasi sistem keamanan yang tinggi diantaranya adalah pada bisnis perbankan. Bisnis perbankan melibatkan aset yang nilainya sangat besar. Kepercayaan pengguna terhadap bank tersebut juga faktor utama dari bisnis ini, sehingga sistem keamanan adalah faktor terpenting pada bidang ini.

Suatu sistem perpindahan dana secara elektronik memiliki tiga komponen utama: jaringan komunikasi, komputer, dan terminal. Jaringan komunikasi diamankan melalui metode enkripsi dan bentuk komunikasi yang sulit untuk disadap. Komputer (server) diamankan secara fisik dan sistem keamanan internal yang mencegah hacker untuk mengambil alih. Lalu terminal (ATM) juga diamankan secara fisik dan memiliki verifikasi pengguna untuk mencegah pencurian.

Mesin ATM (*Automated Teller Machine*) adalah pengganti teller bank yang bertugas untuk menjadi perantara antara pengguna dengan transaksi melalui bank. ATM pada dasarnya adalah komputer terminal yang berkomunikasi dengan server banknya melalui jaringan. Semua data dijaga dengan baik pada servernya. Dan pada umumnya ATM menggunakan two-factor authentication untuk dapat mengakses rekening penggunanya, yang biasanya menggunakan kartu ATM dan PIN. Bila otentikasi gagal biasanya ada mekanisme tertentu sesuai kebijakan banknya untuk mengamankan rekening pengguna.



Berikut adalah sistem keamanan ATM yang terdapat secara umum:

* On-Line PIN Validation

Melakukan validasi PIN dengan server pusat.

* Off-Line PIN Validation

Membandingkan PIN yang dimasukan dengan PIN referensi menggunakan suatu algoritma kriptografi tertentu. Tidak digunakan lagi karena respon sistem terlalu lambat.

* Hardware Security Module

Suatu module untuk melakukan proses kriptografi untuk menjaga privasi dari PIN. Module ini akan melakukan *key management* untuk melakukan enkripsi dan dekripsi PIN setiap kali dikirimkan pada jaringan.

Harga: Standar 3000 - 30k USD

Mesin ATM yang umum menggunakan beberapa jenis enkripsi standar: DES, Triple DES, dan AES.

* DES

DES mengenkripsi data dalam blok berukuran 64-bit dengan key berukuran 56-bit.

* Triple DES

Menggunakan metode enkripsi DES yang diulang sebanyak tiga kali.

* AES

AES mengenkripsi data dalam blok berukuran 128-bit, dan key dengan ukuran variatif antara 128, 192, atau 256-bit.

Referensi

[1] Biometrics Identification System, <http://www.technovelgy.com/ct/Technology-Article.asp?ArtNum=12>

[2] ATM Machine System, <https://www.quora.com/How-do-ATM-machines-work-internally>

[3] ATM Machine System, <https://www.quora.com/How-does-an-ATM-machine-work-1>

[4] Security of ATMs, <https://en.wikipedia.org/wiki/Security_of_automated_teller_machines>

[5] HSM Pricing, <https://wiki.opendnssec.org/display/DOCREF/HSM+Buyers%27+Guide>