Kajian Perkembangan Teknologi ***Smart Card*** dari Segi Keamanan dan Implementasinya di Kehidupan Sehari-hari

Adhitya Agung Satria[1] (13502009), Gamma[2] (13502058), dan M. Yusuf Hamdan[3] (1350213)

Departemen Teknik Informatika
Institut Teknologi Bandung
Jalan Ganesha 10 Bandung 40132

E-mail : if12009@students.if.itb.ac.id[1], if21058@students.if.itb.ac.id[2], dan if12013@students.if.itb.ac.id[3]

Abstrak

Smart card adalah suatu penemuan di bidang IT yang telah mempermudah kehidupan manusia karena mempunyai banyak fungsi dan kemampuannya menyimpan data *cardholder*. Penggunaannya juga sudah mencakup banyak bidang, dari kesehatan, transportasi, dan keuangan. Perusahaan bisnis juga telah melihat potensi *smart card* ini dan telah mengembangkan berbagai jenis *smart card* . Seiring dengan kegunaannya, *smart card* mempunyai masalah yang penting untuk diperhatikan yaitu keamanannya. Dalam tulisan ini, penulis mencoba mengkaji perkembangan *smart card* dari jenisnya, komponen dan teknologi yang dipakai, masalah keamanannya, solusi strategis penanganannya, dan enkripsi yang sering dipakai dalam *smart card*.

Kata kunci: *smart card* , *microprocessor*, keamanan, enkripsi, kriptografi,

1. Pendahuluan

Perkembangan zaman menuntut manusia untuk mengembangkan berbagai macam teknologi untuk membantu meningkatkan kehidupannya. Pada tahun 1930-an, *plastic card* pertama kali diperkenalkan. Penggunaannya sendiri baru mulai terkenal pada tahun 1950-an. Kemudian kartu kredit yang termasuk *plastic card* , yang sekarang ini sudah menjadi gaya hidup di kebanyakan negara maju. Kartu kredit ini pertama kali dibuat oleh Bank of America pada tahun 1960. Banyak sekali kegunaan *plastic card* ini diantaranya sebagai identitas, untuk bepergian, mengakses gedung, mengambil dari bank, dan membayar barang belanjaan. Diperkenalkan juga berbagai macam dan bentuk *plastic card* tersebut.

Sudah banyak bukti aplikasi *plastic card* di berbagai negara. Jepang sendiri telah menggunakannya sebagai kartu pembayaran, kartu telepon, dan kartu bepergian. Di Afrika Selatan, orang menggunakannya untuk pembayaran dengan pencocokan sidik jari sebagai otentifikasi.

Plastic card yang pertama kali dibuat adalah berupa kartu bisnis biasa. Informasi yang terdapat di kartu tersebut seulit untuk di-*copy* tetapi masih dapat dibaca manusia. Adanya teknik *emboss* (memberi semacam relief huruf di kartu) memudahkan pertukaran informasi yang ada di kartu ke kertas karbon. Walaupun proses ini masih memerlukan *key-punch* dalam sistem terkomputerisasi.

Lalu muncul teknologi *magnetic stripe*. Teknologi ini memungkinkan seluruh proses sebelumnya yang manual menjadi lebih otomatis. Tetapi hal ini tidak menghilangkan fungsi kartu sebagai identitas dan sangat terhubung dengan pemegang kartu. Adanya tanda tangan dan foto juga sebagai salah satu cara otentifikasi, walaupun dinilai sangat tidak efektif.

2. Pendefinisian Masalah

Kondisi saat ini adalah diperlukannya suatu kartu yang bisa menyimpan lebih banyak data daripada kartu *magnetic stripe*. Data ini mulai dari data kesehatan, belanja, dan koleksi data lainnya.

Sejak pertama kali *plastic card* diperkenalkan, tingkat pengamanan selalu menjadi perhatian terpenting. Seberapa hebat keamanan kartu itu tersebut. Opini yang terbentuk di masyarakat adalah kartu yang mereka punya

melindungi gedung dan rekening bank mereka dari kejahatan dan teknologi keamanannya hanya diketahui oleh perusahaan keamanan. Opini ini benar tetapi, perkembangan yang terjadi adalah faktor manusia sebagai rantai terlemah dalam keamananan telah menimbulkan banyak pelanggaran yang akhirnya memperparah tingkat keamanan.

Hal ini terjadi ketika operator keamanan yang bersangkutan bermasalah dengan prosedur dan validasi. Merka secara sengaja mengabaikan proseur dan lebih suka melakukan jalan pintas untuk keamanan. Mereka tidak menyadari seberapa besar pengaruh tindakan mereka ke tingkat keamanan. Contoh: kartu dikembalikan sebelum tanda terima ditanda tangan atau bagian depan kartu tidak pernah diperiksa untuk identifikasi. Sistem keamanan sendiri mungkin juga bermasalah ketika membiarkan perilaku seperti ini tanpa ada tindak lanjut.

Penyalahgunaan lain yang mungkin terjadi karena teknologi yang dipakai sudah diketahui banyak orang. Sekarang ini, pengetahuan mengenai teknologi kartu sudah dapat diakses dengan mudah. Dengan sedikit pengetahuan tentang sistem keamanan, teknologi yang dipakai, dan kemampuan programming para penjahat dapat menghasilkan kartu tiruan atau transaksi kartu.

Memang harus diakui bahwa tidak ada sistem yang benar-benar aman. Selalu ada kesalahan, lubang yang tidak terdeteksi. Tetapi desainer sistem harus bisa meminimalisir kesalahan-kesalahan tersebut. Anehnya. sistem kartu di banyak negara termasuk Amerika Serikat, telah menganggap serangan/kejahatan yang dilakukan termasuk biaya yang sudah bisa diperkirakan dalam anggaran.

3. Arti dan Fungsi

Smart card sering disebut sebagai *chip card* atau *integrated circuit* (IC) *card* . Definisi *chip card* sendiri yaitu kategori umum yang mencakup *smart card* dan *memory card* . *Smart card* adalah *plastic card* yang mengandung *memory chip* dan *microprocessor*. Kartu ini bisa menambah, menghapus, mengubah informasi yang terkandung. Keunggulannya adalah *smart card* tidak perlu mengakses *database* di server karena sudah ada sebagian terkandung di kartu. Sedangkan *memory card* dipasangi *memory silicon* tanpa *microprocessor*.

Fungsi dasar suatu *smart card* adalah untuk mengidentifikasi *card holder* ke sistem komputer. *Cardholder* disini adalah pemilik asli kartu tersebut. Identifikasi ini menyangkut otentifikasi organisasi yang membuat kartu tersebut dan *cardholder* dan hak aksesnya..

Beberapa hal yang harus dipertimbangkan dalam metode identifikasi kartu adalah: apakah kartu dapat:

- Mengkonfirmasi identitas *cardholder* sebelum mengakses data
- Memberikan data untuk konfirmasi ke alat eksternal, sistem atau perorangan.
- Menyediakan data ke sistem tanpa pengecekan orang yang menggunakan.

Untuk itu harus didefinisikan tingkat keamanan yang diperlukan. Tingkat keamanan paling tinggi, sedang, atau hanya cukup untuk mengatasi pencuri amatir saja.

4. Kebutuhan Keamanan dan Pemodelan

Sebenarnya tujuan paling realistis bisa dilakukan oleh desainer sistem keamanan adalah untuk menjamin bahwa usaha yang dilakukan untuk menyerang sistem itu lebih mahal dari hasil yang akan didapat. Hal ini akan membuat orang menjadi tidak tertarik untuk menyerang sistemnya. Ada banyak cara untuk melakukannya, antara lain:

- Membatasi bagian sistem yang terpengaruh ketika diserang.harus ada pembagian sistem sehingga kehilangan satu data hanya memepengaruhi subsistem saja
- Membatasi *lifespan* suatu sistem. Hal ini bisa dicapai dengan cara mengurangi jangka waktu kunci dan data kritis lainnya.
- Membatasi jumlah resiko, dengan cara mengasosiasikan tingkat akses data di sistem dengan tingkat keamanan yang dipunyai di kartu
- Mengurangi motivasi penyerangan, dengan cara hanya berhubungan dengan komunitas orang-orang yang bisa dipercaya yang mempunyai sistem kontrol.

4.1. Kriteria

Dalam usaha untuk membuat sistem keamanan yang baik, tentu saja perlu suatu perencanaan. Lalu hal yang pertama kali dilakukan dalam perencanaan adalah menentukan kebutuhan dasar keamanan yang diperlukan. Karena keamanan bisa mempunyai arti yang berbeda bagi tiap orang. Tapi berikut ini adalah beberapa kriteria yang bisa dipilih untuk menentukan tingkat keamanan yang diperlukan:

a. *Safety*, meliputi tingkat keselamatan manusia dan tindakan yang dilakukan untuk tiap resiko yang mungkin terjadi.
b. *Nondelivery* yaitu resiko kehilangan data (transaksi) ketika terjadi komunikasi antar sistem. Perencanaan mekanisme deteksi resiko ini sangat penting.
c. *Accuracy*, berurusan kemungkinan kesalahan yang terjadi ketika penyimpanan dan pertukaran data.

Pengaruhnya tergantung dari jenis data yang bersangkutan.

d. *Data Integrity*, mengatur integritas data yang disimpan dari pengubahan data baik yang sengaja maupun tidak. Pengubahan ini kemungkinan besar akan terjadi. Oleh karena itu, sistem harus bisa menananganinya dengan baik.
e. *Confidentiality*, menangani keamanan kerahasiaan informasi yang terkandung baik di kartu dan sistem yang berhubungan dengannya. Kebocoran yang terjadi mungkin karena kesalahan logic sistemnya atau ada kelemahan dalam sistem yang akhirnya disalahgunakan.
f. *Impersonation*, resiko yang terjadi jika ada orang yang tidak mempunyai hak akses tetapi menggunakan kartu tersebut.
g. *Repudiation*, harus ada meknisme pembuktian bahwa suatu transaksi terjadi dengan menggunakan kartu ayng bersangkutan. Mekanisme ini biasanya dilakukan dengan digital signature menggunakan kriptografi kunci publik.

4.2. Model

Sistem keamanan sendiri bisa dimodelkan tingkat keamanannya berdasarkan proses yang dialami oleh suatu data yaitu *Storage*, *Transmission*, dan *Use*.

4.2.1. Storage

Jika suatu data harus bisa diakses secara *offline* dan harus portable, maka sebaiknya disimpan di *smart card* . Sebaliknya data lainnya lebih baik disimpan di komputer dan *smart card* dapat digunakan untuk mengaksesnya. Data dibuat agar tidak dapat dimengerti oleh orang lain dengan enkripsi. Data juga harus dicek apakah tidak terjadi perubahan yang tidak diinginkan atau kesalahan baik fungsi dan operasi di sistem

4.2.2. Transmission

Proses pengiriman data juga harus dicek untuk menjaga tidak adanya perubahan baik sengaja atau tidak. Pengecekan ini biasanya dilakukan dengan *cyclic redundancy check* (CRC), *transaction counter*, dan *message authentication check* (MAC).

4.2.3. Use

Harus ada pengecekan untuk menjamin bahwa orang yang menggunakan adalah *cardholder* sebenarnya. Ada berbagai macam cara antara lain:

- Tanda tangan dan foto digunakan untuk pengecekan secara manual untuk kondisi dimana terjadi komunikasi tatap muka
- Teknik menggunakan *Personal Identification Number* (PIN). Walaupun mempunyai banyak keterbatasan, teknik ini mempunyai catatan yang baik karena teknik ini mudah diimplementasikan dan diterima dengan baik oleh konsumen..
- Teknik menggunakan pengecekan biometris untuk tingkat keamanan yang lebih baik.

5. Tipe dan Karakteristik

Smart card dapat dikelompokan berdasarkan:

- *Function*, yang merupakan perbedaan paling mendasar antara *memory card* dan *microprocessor card*
- *Access mechanism*, yaitu contact dan contactless
- *Physical characteristic*, dilihat dari ukuran dan bentuk

Berikut ini adalah macam-macam jenis *smart card* yang ada:

5.1. Memory Card

Smart card yang paling sederhana. Kartu ini hanya mengandung *memory circuit* yang dapat diakses melalui kontak dengan *synchronous protocol*. Dalam *memory* itu terdapat *protected area* yang hanya bisa diakses jika menerima kode keamanan tertentu. Ada juga pembatasan jika ada aplikasi luar yang ingin mengakses *memory* .

Ada juga beberapa jenis *memory card* yang menyediakan layanan otentifikasi. Ukuran data yang bisa disimpan di dalamnya tidak terlalu besar, sekitar 100 bits – 10 kb. Kartu ini banyak digunakan untuk aplikasi *accounting* seperti kartu telepon, *transportation card* dan *vending card* .

5.2. Microprocessor Card

Smart card ini mempunyai *memory* circuit dan *microprocessor* dalam satu *chip*. Semua akses ke kartu akan melalui *microprocessor*. Datanya sendiri baru bisa diakses jika telah melewati semacam *security logic*.

Terdapat sebuah interface untuk I/O yang bisa mempunyai bentuk yang berbeda antar kartu. Dari segi keamanan, *microprocessor* bisa dibilang sulit untuk dipalsukan.

Perkembangannya sekarang ini adalah *microprocessor* diganti dengan *State change*. Hal ini dilakukan karena *microprocessor* sudah tidak terbatas dalam hal kecepatan dan kapasitas memori. *State change* berisi *Programmable Gate Array* (PGA) yang berukuran lebih kecil dan dapat mengemulasikan fungsi *microprocessor* dengan kecepatan yang lebih baik.

Sekarang ini, kartu ini juga diberi kemampuan untuk melakukan kriptografi seperti *memory-adddress srambling*, *auto-detection hacking*, *power-circuit manipulation*, dan *electron microscopy*.

5.3. Contact Card

Kartu ini merupakan versi awal dari *smart card* yang beredar di Eropa. Kartu ini adalah *smart card* yang mempunyai *contact chip*. Kartu ini harus dimasukkan ke *reader* untuk melakukan transaksi atau menyampaikan informasi dari kartu ke *reader*. Kekurangannya adalah:

- Titik *contact*-nya dapat rusak karena sering digunakan, *reader* yang jelek, atau tergesek di kantong
- Ujung *microcircuit* dapat rusak jika kartu bengkok atau ditekan terlalu keras
- Mudah diserang melalui titik *contact* kartu
- Kerusakan yang terjadi di alat *contact reader* yang merupakan alat mekanis karena pemakaian yang tidak baik atau karena serangan fisik

5.4. Contactless Card

Kartu ini adalah jenis *smart card* yang menggunakan frekuensi radio (RF) untuk bertukar informasi. Jadi kartu ini tidak perlu kontak fisik ke *reader/terminal* untuk bertukar informasi. Kartu ini mengandung *microcircuit* yang tertutup di dalam kartu, sehingga kartu ini hanya perlu didekatkan dengan *reader* tanpa kontak langsung untuk bertukar informasi.

Kontak antar kartu dan *reader* tergantung pada kepekaan *reader*. Banyak dipakai untuk transaksi yang menekankan pada unsur kecepatan, terutama di industri transportasi.

Kelebihannya adalah:
- Lebih dapat diandalkan
- Maintenance lebih sedikit daripada *contact card*
- *Lifespan*-nya lebih lama daripada *contact card*

Sedangkan kekurangannya antara lain:
- Tidak cocok untuk pertukaran data yang besar
- Ukurannya lebih besar daripada contact *card* dan belum ada ukuran standar
- Jumlah manufaktur pembuat sedikit sehingga jenis kartunya terbatas
- Harganya relative lebih mahal daripada contact *card*

5.5. Hybrid Card

Smart card yang menggunakan dua teknologi yang ada di *contact card* dan *contactless card* . Sehingga terdapat alat *contact* dan antena dalam satu kartu. Kartunya sendiri ada yang menggunakan satu *microprocesor* dan ada juga yang menggunakan dua *microprocessor*. Kartu jenis ini dibuat untuk membuat pengguna bisa memakai kartunya di banyak aplikasi.

Ada pula istilah *combi card* yang sejenis dengan *hybrid card* tapi membutuhkan suatu alat yang dinamakan *pouch* untuk mengubah fungsi *contact card* menjadi *contactless card* . Dan alat *contact*-nya adalah antena yang terdapat dari *pouch* sedangkan media transmisi yang digunakan adalah gelombang radio.

Tingkat keamanan *hybrid card* lebih baik daripada *combi card* karena gelombang radio sangat mudah untuk disusupi dan hal ini akan mengurangi tingkat keamanan kartu.

5.6. Subscriber Identity Module (SIM) Card

Smart card kecil dan dapat diprogram berisi kunci identitas *subscriber* ke layanan selular. Kunci ini digunakan untuk identitas ke *digital mobile service* dan jenis layanan yang dipakai. SIM *card* ini bisa dipasang permanent ke teleponnya atau yang removable. SIM ini berguna untuk kunci keamanan yang dipakai oleh jaringan GSM.

5.7. Removable User Identity Modul (R-UIM) Card

Smart card yang fungsinya sama dengan SIM *card* tetapi untuk telepon dengan teknologi CDMA. Kartu ini memungkinkan komunikasi antar kedua jaringan.

5.8. Universal subscriber Identity Module (USIM) Card

Pengembangan dari SIM *card* yang akan digunakan di teknologi jaringan 3G. kartu ini akan dimasukan di peralatan 3G dan digunakan untuk otentifikasi jaringan dan fungsi lainnya

6. Komponen

Pembahasan komponen akan dibagi berdasarkan komponen-komponen dasar *smart card*

6.1.Carrier

Material dasar yang digunakan untuk pembuatan *smart card* adalah *polyvinyl chloride* (PVC) atau *thermoplastic* sejenis. Bahan ini digunakan karena murah dan dapat di-*emboss*. Bahan lain yang dapat digunakan adalah *Acrylonitrile butadiene styrene* (ABS) yang lebih tahan suhu tinggi, *Polycarbonate* yang digunakan untuk kartu *mobile-telephone*, dan *Polyethylene terephthalate* (PETP) yang banyak digunakan di Jepang karena fleksibel dan ringan. Kriteria dalam pemilihan bahan adalah reliabilitasnya yang tahan lama/tidak mudah rusak dan tahan panas lebih baik

6.2. Chip

Kompenen utama kartu yaitu IC yang dipasang di dalam kartu. Isi *chip* ini bisa teridiri dari *memory* , *microprocessor* atau PGA *chip*.

6.2.1. Micoprosessor

Kebanyakan *smart card* mempunyai 8-bit *microprocessor*, dengan desain Motorola 6805 atau Intel 8051 denga *clock speed* tertinggi 5 MHz.. Tetapi sudah ada *microprocessor* 16-bit dan mungkin kedepannya makin banyak yang lebih cepat. RISC *microcontroller* banyak digunakan di *smart card* untuk aplikasi yang perlu kecepatan proses daripada *multifunctions*.

6.2.2. Memory

Memory memakan tempat terbesar di IC *smart card* . *Memory* ini dibagi menjadi 5 area berdasarkan tipe *semiconduktor memory* yang dipakai:
- *Read-only memory* (ROM), yang berisi program permanen yang harus ada dalam kartu, yang disebut mask.

- *Programmable* ROM (PROM) digunakan untuk me-*load* nomor seri kartu dan nilai permanent lain
- *Flash memory*, sebagai tempoat program tambahan.
- E^2PROM, merupakan bagian terbesar *memory* untuk *data storage*
- *Random Access Memory* (RAM), digunakan untuk tempat penyimpanan data sementara ketika kartu sedang dipakai
- *Ferro-electric* RAM (FRAM), RAM yang bisa menyimpan data *nonvolatile*.

Komposisi tiap bagian *memory* tergantung dari penggunaan kartu yang dipakai

6.2.3. Coprocessor

Bagian *chip* yang dibuat untuk melakukan operasi aritmatika dalam fungsi kriptografi sepertri enkripsi DES atau RSA.

6.2.4.Memory Management.

Digunakan untuk mengontol *memory* dan menyediakan proteksi *hardware* dari akses yang tidak valid. Proteksi ini menggunakan metode hirarki *file* data.

6.2.5. I/O

Microprocessor smart card menggunakan *single bidirectional serial input-output interface*. Metode ini sesuai dengan standar ISO 7816-3 tentang protokol komunikasi.

6.3. Contact

Contact card mempunyai kurang lebih delapan titik kontak. Posisi dan desainnya disesuaikan dengan ISO 7816-2. Walaupun begitu masih banyak orang terutama di Perancis, yang menggunakan desain posisi transisi (pojok kiri atas). *Contact* ini dibuat dari emas atau bahan berkonduksi lainnya. Kontak ini dihubungkan dengan *chip* dengan kabel yang sangat tipis.

6.4. Antenna

Contactless card menggunakan sinyal dengan frekuensi radio (RF) sebagai media transmisi I/O. antena sehingga antena dipasang di kartu sebagai *coil*. Antena juga berfungsi untuk mendapatkan energi dari RF, selain baterai yang ada di kartu.

Sinyal yang digunakan mempunyai frekuensi 135 kHz atau 13,56 MHz. Jika menggunakan frekuensi yang rendah, energi yang diperluakan rendah dan bisa mencapai jangkauan 1m, tapi kecepatan transfer data rendah. Sedangkan jika menggunakan frekuensi tinggi, maka akan memakan energi lebih tinggi, tapi kecepatan transfernya tinggi.

6.5. Mask

Mask adalah program permanaen yang ada di ROM, sering disebut sebagai OS *smart card*. Perbedaannya dengan OS PC pada umumnya adlah Mask melakukan fungsi aplikasi seperti mengurangi nilai, membandingkan tanda tangan digital dan pola yang ada. Jenis *smart card* sendiri tergantung dari *mask* yang ada walaupun menggunakan *microprocessor* yang sama. *Mask* diprogram ketika pertama kali *chip* dibuat, sehingga keamanannya tergantung proses manufakturnya.

7. Teknologi

7.1. Sejarah

Pembuat pertama kali teknologi awal *smart card* adalah orang Jepang bernama Kunitaka Arimura pada tahun 1970. Dia mematenkan ciptaannya yang hanya terbatas penggunaannya hanya di Jepang saja. Dan pembuatannya harus dengan lisensi Arimura.

Pada tahun 1974-1976, Rolang Moreno di Perancis membuat hak paten beberapa aspek fungsional *smart card* dan menjual lisensinya ke perusahaan bernama Bull dan perusahaan lain. Lalu Bull mengembangkan aspek *microprocessor* di *smart card* dan memegang lisensi teknologi yang berhubungan dengan *microprocessor smart card* .

Sementara itu, Innovatron, perusahaan milik Moreno, berusaha menempuh jalur hukum dan kebijakan agresif untuk melisensikan *smart card* di dunia sehingga membatasi jumlah perusahaan yang mengembangkan teknologi ini. Tetapi hak paten paling penting tentang *smart card* telah kadaluarsa di tahun 1996.

Sesuai dengan opini Moreno, aspek paling penting *smart card* adalah fungsi kontrol akses ke informasi yang terkandung dalam *smart card* dengan teknik *password* atau fungsi internal lainnya untuk menjaga keamanan informasi. Fungsi ini akan membuat *chip logic* makin sulit tapi akan menyederhanakan kerja sistem lain yang berhubungan terkait dengan enkripsi dan manajemen kunci.

Terdapat bermacam-macam jenis teknologi yang digunakan dalam *smart card* , antara lain:

7.2. Standard

Beberapa organisasi memperkenalkan standar untuk agar saling kompatibel dan dapat dipakai secara umum, diantaranya:

- ISO 7816 yang mendefinisikan *contact card*
- EMV (Europay, Master*card* , Visa) hasil kerjasama tiga perusahaan kartu kredit untuk mengembangkan ISO 7816 dengan menambahkan fungsi yang berhubungan dengan bank lebih detail
- ETSI (European Telecommunication Standard Institute) berisi standar pemakaian *smart card* publik dan sistem telepon selular.

7.3. Hybrid

Smart card mempunyai banyak teknologi agar dapat digunakan secara umum. Contoh: *smart card* yang

menggunakan teknologi *magnetic stripe*. Hal yang harus diperhatikan adalah adanya faktor keamanannya dan prioritas penggunaan teknologi yang ada tergantung situasi dan kondisi .

7.4. PCMCIA Card

Teknologi ini dipicu oleh perkembangan laptop yang menginginkan adanya portable *memory* dan *interface card* yang berukuran lebih kecil dan terstandarisasi. Sehingga *Personal Computer Memory Card Industry Association* (PCMCIA) mengeluarkan tiga standar pembuatan *memory card* kecil dan hardisk dengan tebal 10,5 mm.

7.5. Barcoding

Teknologi ini banyak dipakai karena produksinya murah dan banyak *reader* yang mendukung. Tetapi tingkat keamanannya kurang baik. *Barcode* ini menggunakan *infra red* dan hanya bersifat *read-only.*

7.6. Radio Frequency Identification (RFID)

RFID digunakan untuk kontrol akses, lalulintas, dan aplikasi industri lainnya. Tag di alatnya, yang mempunyai berbagai macam bentuk, mempunyaii antena. Jika dekat dengan *reader*, antena ini akan membangkitkan tenga untuk menyalakan *circuit* di *tag* dan mentransmisikan *ID number* ke *tag*. Sebagian besar RFID juga bersifat *read-only*.

8. Serangan dan Manajemen Resiko

8.1. Sumber Serangan

Sumber-sumber serangan yang mungkin dilakukan adalah dari:

a. *Normal cardholder*, yang berusaha mencoba melakukan hal-hal yang tidak sesuai dengan prosedur sistem. Serangan ini lebih bersifat tidak sengaja karena ketidaktahuan pemegang kartu.
b. *Careless cardholder*, yang sering menghilangkan atau merusak kartu atau mesin terminal. Serangan ini juga bersifat tidak sengaja
c. *Malicious cardholder*, yang mempunyai akses terbesar ke sistem, atau menyediakan kartu dan kode untuk analisis.
d. *Insider*, biasanya adalah karyawan perusahaan yang mengeluarkan kartu yang mempunyai kesempatan menyalin, menganalisis atau mencuri data untuk diberikan ke orang lain.
e. *Outsider*, yang mempunyai akses ke sistem.
f. *Card thieves*, pencuri kartu yang telah mendapatkan beberapa informasi penting untuk menggunakan kartu yang didapat.
g. *Criminal gangs*, yang secara berkelompok dan sitematis mendapatkan banyak kartu dan akses ke sistem sehingga bisa menciptakan rekening dan bisnis palsu
h. Kelompok yang paling berbahaya adalah orang-orang yang berusaha untuk menghancurkan sistem yang ada apapun resiko dan biaya yang diperlukan karen alasan pribadi.

8.2. Bahaya Serangan

Tingkat bahaya serangan bisa dikelompokan menjadi:

a. *Grade* I, dimana serangan ini mengakibatkan bahaya kematian
b. *Grade* II, dimana serangannya membahayakan kelangsungan hidup perusahaan/bisnis
c. *Grade* III, dimana serangan mengakibatkan kerusakan yang cukup parah dan biaya kompensasi tambahan
d. *Grade* IV, dimana serangan mengakibtakan tambahan kerja dan keterlambatan
e. *Grade* V, dimana serangan hanya berupa gangguan kecil

8.3. Faktor Penyebab Serangan

Penyebab masalah keamanan sering terjadi karena:

- Masalah *hardware*
- Masalah *software*
- Masalah jaringan komunikasi
- Kesalahan prosedur
- Serangan untuk mengeksploitasi penyebab masalah keamanan lainnya

8.4. Manajemen Resiko

Setelah mengetahui sumber serangan, penyebab masalah, dan tingkat serangan keamanan, kita harus merencanakan tindakan apa yang harus dilakukan. Hal pertama yang harus dilakukan adalah fokus pada masalah yang mempunyai probabilitas kejadian dan nilai tertinggi. Masalah inilah yang akan menyebabkan kerugian terbesar dan memerlukan usaha yang besar untuk diperbaiki. Selanjutnya, melihat biaya yang harus dikeluarkan untuk membuat solusi keamanannya. Desainer sistem keamanan harus yakin bahwa biaya implementasi solusi lebih murah dari kerugian yang mungkin diderita. Jika sebaliknya, maka implementasi solusi tersebut bisa dibilang sia-sia.

9. Enkripsi

Ketika berurusan dengan keamanan data, dalam hal ini informasi yang terkandung di *smart card* , harus ada teknik pembuktian bahwa identitas orang yang memakai *smart card* itu valid.

Sistem pengamanan yang digunakan di *smart card* adalah sistem kunci simetris dan sistem kunci publik. Metode/algoritma yang banyak digunakan di sistem kunci simetri adalah *Data Encryption Standard* (DES). Sedangkan algoritma yang digunakan di sistem kunci publik adalah RSA. Berikut ini disajikan algoritma DES dan RSA secara singkat

9.1. DES

Algoritma simetri menggunakan kunci yang sama untuk enkripsi dan dekripsi. DES adalah algoritma kriptografi yang disebut sebagai algoritma modern pertama yang dipakai untuk keperluan komersial dengan detail implementasi yang lengkap dan terbuka

Algoritma ini pertama kali diperkenalkan di Amerika Serikat dan telah disetujui oleh National Bereau of Standard (NBS) setelah diuji oleh National Security Agency (NSA). Algoritma ini sendiri dikembangkan dalam sebuah riset yang dipimpin oleh W.L. Tuchman pada tahun 1972 di IBM.

Desain algoritma DES sangat terkait dengan dua konsep utama dalam algoritma yaitu *product cipher* dan algoritma Lucifer (diciptakan oleh Horst Feistel). Maksud dari *product cipher* adalah menciptakan fungsi enkripsi kompleks dengan cara menggabungkan beberapa operasi enkripsi dasar sederhana yang saling melengkapi. Sehingga keduanya melibatkan operasi bolak-balik yang berulang. Operasi dasarnya termasuk transposisi, translasi, operasi aritmatika, substitusi, dan transformasi linier. DES sendiri termasuk golongan *cipher block* karena algoritma ini beroperasi pada *plaintext/ciphertext* dalam bentuk blok bit yang panjangnya sudah ditentukan.

DES sendiri beroperasi pada blok dengan ukuran 64 bit. DES mengenkripsikan *plaintext* menjadi *cipherteks* dengan menggunakan *internal key* atau *subkey* berukuran 56 bit. *Internal key* dibangkitkan dari *external key* yang panjangnya 64 bit.

Skema global dari algoritma DES[1)] adalah sebagai berikut:

1. Blok plaintext dipermutasi dengan matriks initial permutation atau IP
2. Hasil permutasi awal kemudian di-*encipher* sebanyak 16 kali (16 putaran). Setiap putaran menggunakan kunci internal yang berbeda.
3. Hasil *encipher* kemudian dipermutasi dengan matriks invers initial permutation atau IP-1 menjadi blok *ciphertext*.

Skema DES sangat tergantung pada kerahasiaan kunci. Oleh karena itu, terdapat dua situasi terkait dengan *smart card* , yaitu:

- Ketika kunci dapat didistribusikan dan disimpan secara terpisah dan aman
- Ketika kunci dipertukarkan antara dua sistem yang telah saling mengotentifikasikan diri dan pertukaran tersebut tidak berlanjut di luar transaksi atau *session* pertukaran lain.

DES sering kali digunakan untuk melindungi data dari *eavesdropping*. ketika transmisi pertukaran. Triple-DES adalah proses enkripsi data asli dengan melakukan algoritma DES tiga kali. Hasilnya meningkatkan efektivitas kunci dan kekuatan enkripsi.

Dilihat dari segi banyak perhitungan yang dilakukakan, DES itu lebih sederhana daripada RSA. Algoritma DES sendiri telah tersedia di *hardware* dan beberapa *chip smart card*. Tetapi adanya kunci khusus yang harus diketahui oleh kartu dan alat dekripsi *reader*, membuat algoritma ini tidak cocok untuk otentifikasi kartu di sistem terbuka karena alasan efektivitas.

9.2. RSA

Sistem kunci asimetris menggunakan kunci yang berbeda untuk enkripsi dan dekripsi.kunci yang boleh diketahui adalah kunci publik. Sedangkan kunci yang harus tetap dijaga kerahasiaannya adalah kunci privat.

Algoritma asimetris yang banyak digunakan adalah algoritma RSA. Algoritma ini dibuat oleh tiga orang peneliti di Massachussets Institute of Technology (MIT) pada tahun 1976. Nama RSA sendiri diambil dari inisial nama penemunya yaitu Ron (R)ivest, Adi (S)hamir, dan Leonard (A)dleman.

Keamanan algoritma RSA terletak pada sulitnya memfaktorkan bilangan yang besar menjadi faktor-faktor prima. Pemfaktoran dilakukan untuk memperoleh pasangan kunci privat-publik. Berikut ini adalah algoritma RSA[2)]:

9.2.1. Pembangkitan kunci

Kunci dibangkitkan dengan langkah sebagai berikut:

1. Bangkitkan dua bilangan prima besar berbeda, p dan q, yang sama jumlah digitnya.
2. Hitung $n = pq$ (1)
3. Hitung $\varphi = (p - 1)(q - 1)$. (2)
4. Pilih bilangan integer acak e, $1 < e < \varphi$, sedemikian sehingga $\gcd(e, \varphi) = 1$. (3)
5. Gunakan perhitungan untuk mendapatkan satu lagi bilangan integer d, $1 < d < \varphi$, sedemikian sehingga $ed \equiv 1 \pmod{\varphi}$. (4)

Maka kunci publiknya adalah (n,e) dan kunci privatnya adalaah d. nilai e disebut *encryption exponent* dan nilai d disebut *decryption exponent*. Sedangkan n disebut *modulus*.

Contoh kasus: B mengenkripsikan pesan ke A dan mendekripsikannya

9.2.2. Proses Enkripsi

Maka ketika enkripsi, B harus melakukan langkah-langkah sebagai berikut:

1. Dapatkan kunci pblik A (n,e)
2. Ubah bentuk pesan menjadi bilangan intger m, dengan $0 < m < n-1$.
3. Hitung $c = m^e \bmod n$ (5)
4. Kirim *ciphertext* c ke A

9.2.3. Proses Dekripsi

Untuk mengambil pesan m dari *ciphertext* c, A dapat menggunakan kunci privat d untuk dengan perhitungan

$$m = c^d \pmod{n.} \quad (6)$$

1) Munir, Renaldi. *Diktat Kuliah Kriptografi*. Hal. 106

2) Menezes,A. dkk. *Handbook of Applied Cryptography*.Hal. 286

Bentuk perhitungan aritmatika ini sangat lambat jika dijalankan di *byte-oriented processor*. Terutama 8-bit *microprocessor* yang terdapat di banyak *smart card* . Sehingga walaupun RSA menyediakan fungsi otentifikasi dan enkripsi, dalam sistem *smart card*, algoritma ini hanya digunakan untuk mengotentifikasi pengahasil pesan, pembuktian bahwa data belum diubah sejak tanda tangan dibangkitkan, dan enkripsi kunci.

Walaupun begitu kemampuannya mendistribusikan satu kunci secara publik dan kunci lainnya tetap rahasaia dalam kartu/*host system* membuatnya sering dipakai di open system.

10. Kesimpulan

Perkembangan smart card sebagai alat Bantu dalam pertukaran data semakin banyak aplikasinya, seiring dengan hal tersebut, muncul masalah baru yuang dihadapi yaitu keamanan. Kebutuhan keamanan untuk otentifikasi, kerahasiaan data, dan integritas data harus dipertimbangkan secara terpisah. Otentifikasi dapat dilakukan dengan algoritma sistem simetri atau asimetri. Data yang disimpan dalam kartu dapat dikatakan rahasia jika dilindungi oleh *chip* yang cocok dan mekanisme kontrol akses. Jika data/informasi perlu ditransmisi keluar, maka perlu dienkripsi menggunakan DES atau algoritma asimetri lainnya. Integritas data dapat dijamin dengan menggunakan standar MAC.

Referensi

[1] Hendry, Mike. 1997. *Smart card Security and Application*. London:Artech House.

[2] Munir, Renaldi. 2005. *Diktat Kuliah Kriptografi*. Bandung:Departemen Teknik Informatika, ITB

[3] Gartner. 2004. *Gartner Glossary of Information Technology*, Gartner Inc.

[4] Menezes,A. dkk. 1996. *Handbook of Applied Cryptography*. CRC Press.

[5] Frank, J.N. 1996. *Smart Cards Meet Biometrics. Card Technology*. Card Technology.

[6] Glass, A. S. 1991. *Why Would Secure Cards Be Smart?" Smart Card 2000 Conferece Proceedings*. Amsterdam.

[7] Mondex International. 1995. *Mondex: Security by Design*. London

[8] Scheneir, B. 1995. *Applied Cryptography: Protocols, Algorithms, dan Source Code in C*. New York: Wiley