Serangan pada system keamanan ATM dengan kartu *magnetic stripe* dan solusi yang ditawarkan dengan penggunaan kartu *chip*

Rizkiana Novitasari

Program Studi Informatika
Institut Teknologi Bandung
Jalan Ganeca 10 Bandung 40132
E-mail : if17122@students.if.itb.ac.id

ABSTRAK

Kartu ATM yang umumnya dimiliki masyarakat saat ini adalah kartu berbasis *magnetic stripe*. Teknologi kartu magnetik ini secara *inheren* tidak aman karena kartu menyimpan data-data secara *plain* atau tanpa enkripsi sehingga dapat dibaca oleh alat pembaca (*magnetic stripe reader*) manapun. Sekali terbaca, maka dengan menggunakan perangkat *magnetic stripe writer*, kartu baru yang memiliki fungsi yang identik dengan kartu asli dapat dibuat dengan mudah (*kloning*).

Baru-baru ini, Indonesia digegerkan dengan tindak kejahatan yang dikenal dengan ATM *skimming*. Pelaku kejahatan memanfaatkan kelemahan dari kartu ATM berbasis *magnetic stripes* ini. Pelaku pemalsuan kartu melakukan teknik skimming untuk mencuri data-data kartu magnetik untuk selanjutnya dituliskan secara identik ke dalam kartu baru. Teknik skimming ini dilakukan dengan cara memasang *magnetic stripe reader* tambahan ke terminal ATM atau POS (*point of sales*) yang sah.

Saat ini, bank di Indonesia sedang didorong untuk mengganti kartu ATM yang ada, yang berbasis *magnetic stripes*, ke kartu ATM yang menggunakan *chip*. Kartu ini biasa dikenal dengan nama *smart card*, *chip card*, atau *integrated circuit card*.

Kata kunci: *magnetic stripe card*, *chip card*, *smart card*, pengolahan data, sistem pengamanan, serangan.

1. PENDAHULUAN

Kartu *magnetic stripe* adalah tipe kartu yang mampu menyimpan data dengan memodifikasi daya magnet dari partikel kecil magnetik berbasis besi pada pita dari material magnetik di kartu. *Magnetic stripe*, terkadang disebut **magstripe**, dibaca dengan kontak fisik dan menggesekkan lewat *reading head*. Kartu *magnetic stripe* umumnya digunakan pada kartu kredit, kartu identitas, dan tiket transportasi. Kartu *magnetic stripes* juga menganding sebuah *RFID tag*, alat *transponder*, dan/atau sebuah *microchip* yang biasanya digunakan untuk akses control kegiatan bisnis atau pembayaran elektronik.

Kartu ATM yang umumnya dimiliki masyarakat saat ini adalah kartu berbasis *magnetic stripe*. Baru-baru ini, Indonesia digegerkan dengan tindak kejahatan yang dikenal dengan ATM *skimming*. Pelaku kejahatan memanfaatkan kelemahan dari kartu ATM berbasis *magnetic stripes* ini. Pelaku pemalsuan kartu melakukan teknik *skimming* untuk mencuri data-data kartu magnetik untuk selanjutnya dituliskan secara identik ke dalam kartu baru.

Saat ini, bank di Indonesia sedang didorong untuk mengganti kartu ATM yang ada, yang berbasis *magnetic stripes*, ke kartu ATM yang menggunakan *chip*. Kartu ini biasa dikenal dengan nama *smart card*, *chip card*, atau *integrated circuit card*.

Smart card, *chip card*, atau *integrated circuit card* (ICC), adalah suatu kartu berukuran saku dengan sirkuit terintegrasi yang tertanam yang bisa memproses data. Hal ini mengimplikasikan kalau kartu *chip* bisa menerima input yang diproses, dengan aplikasi ICC, dan dikirimkan sebagai output. Ada dua kategori global dari ICC. Kartu memori yang mengandung hanya komponen penyimpanan memori *non-volatile*[1] dan mungkin beberapa logika keamanan yang spesifik. Kartu mikroprosessor yang mengandung memori *volatile* dan komponen mikroprosessor. Kartu ini terbuat dari plastik, secara umum *PVC*, tapi terkadang *ABS* atau polikarbonat. Kartu bisa memiliki hologram untuk menghindari pemalsuan. Menggunakan *chip card* juga merupakan bentuk dari otentikasi keamanan kuat untuk *single sign-on*[2] di dalam perusahaan dan organisasi besar.

2. PENDEFINISIAN MASALAH

Kondisi saat ini adalah kartu *magnetic stripes* yang sudah umum digunakan untuk implementasi kartu ATM.

---

[1] Memori yang tidak mudah hilang

[2] Properti kontrol akses dari sistem perangkat lunak multiple, berelasi, tapi independen.

Akan tetapi, kasus kejahatan pemalsuan kartu ATM yang terjadi membuat sistem keamanan di kartu *magnetic stripes* diragukan. Pelaku pemalsuan kartu melakukan teknik *skimming* untuk mencuri data-data kartu magnetik untuk selanjutnya dituliskan secara identik ke dalam kartu baru. Teknik *skimming* ini dilakukan dengan cara memasang *magnetic stripe reader* tambahan ke terminal ATM atau POS (*point of sales*) yang sah.

Dari deskripsi di atas, dapat dirumuskan beberapa masalah sebagai berikut :

1. Mekanisme pengamanan kartu *magnetic stripes* sudah tidak bisa dipercaya lagi karena informasi pada kartu *magnetic stripes* bisa dambil dengan mudahnya oleh oknum pelaku kejahatan.
2. Apabila pengamanan data pada ingin ditingkatkan dibutuhkan mekanisme pengamanan data yang lebih baik lagi.
3. Apabila pengamanan data pada ingin ditingkatkan, dibutuhkan *device* yang lebih canggih yang mampu memfasilitasi mekanisme pengamanan yang lebih baik.

Bank di Indonesia sendiri sudah didorong untuk mengganti pemakaian kartu ATM yang berbasis *magnetic stripes* menjadi kartu berbasis *chip*. Hal ini menimbulkan beberapa rumusan masalah baru yaitu :

1. Mekanisme apa yang dimiliki oleh kartu chip sehingga bisa dipercaya untuk menggantikan kartu *magnetic stripes*.
2. Bagaimana mekanisme pengamanan data pada kartu *chip* bisa dikatakan lebih baik dari kartu *magnetic stripes*.

3. ANALISIS

3.1 KRIPTOGRAFI PADA *MAGNETIC CARD*

3.1.1 Overview *Magnetic Card*

Kartu *magnetic stripe* adalah tipe kartu yang mampu menyimpan data dengan memodifikasi daya magnet dari partikel kecil magnetik berbasis besi pada pita dari material magnetik di kartu. *Magnetic stripe*, terkadang disebut **magstripe**, dibaca dengan kontak fisik dan menggesekkan lewat *reading head*. Kartu *magnetic stripe* umumnya digunakan pada kartu kredit, kartu identitas, dan tiket transportasi. Kartu *magnetic stripes* juga menganding sebuah *RFID tag*, alat *transponder*, dan/atau sebuah *microchip* yang biasanya digunakan untuk akses control kegiatan bisnis atau pembayaran elektronik.

Magnetic Stripe sangat serupa dengan VCR atau teknologi *floppy disk*. Ia menggunakan material magnetik untuk menyimpan data. Perbedaan antara VCR dan teknologi *magnetic stripe* adalah *magnetic stripe* dicetak pada kertas atau plastik, dan menyimpan data bukannya suara atau gambar. Kartu *magnetic stripes* didesain untuk bisa ditangani secara langsung dan sering digunakan untuk membaca secara penggesekan manual. Dua faktor paling esensial yang mempengaruhi perekaman magnetik dan proses *replay* adalah diarahkan ke partisi medium dan kecepatan *travelling* dari medium.

3.1.2 Tipe dan Komponen Magnetic Card

Magnetic stripes memiliki dua versi, versi kartu kredit normal dan *high-coercivity* (**HiCo**) *version*. Versi **HiCo** meningkatkan keandalan dengan mengurangi kemungkinan data dihapus atau rusak secara tidak sengaja *Coercivity* didefinisikan sebagai kekuatan dari pembalikan *flux* dari magnet, atau dengan kata lain perlawanan dari *demagnetization*[3] material. Ini adalah karakteristik yang paling penting untuk menentukan jenis material untuk digunakan sebagai *stripe*. Ketika sebuah magnet di demagnetasi pada *magnetic stripe*, data yang di-*encode* hilang atau berubah. Oleh karena itu, semakin tinggi *coercivity* dari material, semakin tinggi peluang dari *magnetic stripe* menjadi rusak. Bagaimanapun, semakin tinggi *coercivity* dari material, semakin mahal kartunya.

Magnetic stripe pada umunya sebuah kolom dari magnet kecil. Data yang dimasukkan di-*encode* ke media dengan menyesuaikan polaritas dari magnet. Untuk melakukan ini, seorang pembaca harus mendeteksi perubahan dipolaritas pada magnet. Perubahan dari polaritas dari magnet ke magnet disebut pembalikan *flux*. Apabila r*eader* mendeteksi perubahan, hal ini menandakan sebuah nilai biner "1" atau "0".

Ada dua reader yang beroperasi, yang melalui penggesekan atau pemasukan kartu.\

3.1.3 Pengolahan data pada *Magnetic Stripe*

Setiap karakter yang di-e*ncode* di *stripe* terbuat dari sejumlah bit. Polaritas dari parikel magnetik di *stripe* diubah untuk mendefinisikan setiap bit. Beberapa skema ada untuk menentukan apakah setiap bit adalah satu atau nol, skema yang paling umum digunakan adalah **F2F**

[3] Proses membuat bahan bermagnet menjadi kehilangan kemagnetannya. Salah satu cara yang banyak diterapkan adalah dengan menempatkan bahan yang bersangkutan dengan medan magnet yang kuat,

(atau *aiken biphase*) dan **MFM** (*modified frequency modulation*).

Standar **ISO/IEC 7811** menspesifikasikan *encoding* F2F. Di *encoding* ini, setiap bit memiliki panjang fisikal yang sama di *stripe*-nya. Keberadaan atau ketidakberadaan dari polaritas berubah di tengah dari pendiktean bit baik bernilai 0 atau 1.

3.1.4 Teknik Kriptografi pada *Magnetic Card*

Algoritma enkripsi yang digunakan adalah DES dengan mode ECB. Karena DES bekerja dengan mengenkripsikan blok 64-bit, maka PIN yang hanya terdiri dari 4 angka (32 bit) harus ditambah dengan *padding bits* sehingga panjangnya menjadi 64 bit. *Padding bits* yang ditambahkan berbeda-beda untuk setiap PIN, bergantung pada informasi tambahan pada setiap kartu ATM-nya. Algoritma DES yang digunakan dalam sistem keamanan ATM masih membuka peluang bagi *cryptanalyst* untuk melakukan *cryptanalysis* terhadap sistem tersebut. Dengan mengetahui data pada *magnetic stripe* sebuah ATM, seorang *cryptanalys* dapat menebak empat digit PIN yang dipakai oleh nasabah pengguna ATM menggunakan teori probabilitas.

3.1.5 Kelebihan & kekurangan dari penggunaan teknologi *magnetic stripes*

Kelebihan *magnetic stripe* termasuk :

- Data bisa dimodifikasi atau ditulis ulang
- Kapasitas data tinggi di relasi ke kode bar
- Menambah kemanan sejak hal ini bukan dalam bentuk yang bisa dibaca manusia
- Kebal terhadap kontaminasi dari kotoran, air, minyak, kelembaban , dll.
- Tidak ada komponen bergerak, secara fisik kuat.
- Standar yang terbangun dengan baik
- Tidak habis dibutuhkan untuk menulis atau menulis ulang.

Beberapa kekurangan dari penggunaan *magnetic stripe card* :

- Tidak bekerja pada jarak, sehingga membutuhkan kontak yang dekat ke reader
- Data bisa rusak dengan tersesat pada *field magnetic*
- Bentuk yang tidak bisa dibaca manusia bisa kekurangan di beberapa aplikasi

3.2. KRIPTOGRAFI PADA *CHIP CARD*

3.2.1 Overview *Chip Card*

Chip card adalah kartu plastik yang berukuran sama dengan kartu kredit yang di dalamnya terdapat *chip* silikon yang disebut *microcontroller*. *Chip* merupakan *integrated circuit* yang terdiri dari prosesor dan memori. *Chip*, seperti layaknya CPU (*Central Processing Unit*) di komputer, bertugas melaksanakan perintah dan menyediakan *power* ke *Chip card* . *Chip card* mempunyai kemampuan untuk memproses dan menginterpretasikan data, serta menyimpan data tersebut secara aman. Apalagi dengan perkembangan algoritma kriptografi, data yang disimpan akan dienkripsi terlebih dahulu, sehingga tidak mudah dibaca oleh pihak yang tidak berwenang/berhak. Hal ini akan mempersulit pemalsuan *chip card*. Ukuran dan dimensi *chip card* menurut ISO7816 adalah :

1. Dimensi kartu, yaitu panjang 87,6mm, lebar 53,98mm dan tebal 0,76mm.
2. Kartu terbuat dari PVC (*Polyvynl Chloride*) atau PVCA (*Polyvynl Chloride Acetate*).

3.2.1 Tipe dan Komponen *Chip Card*

Secara umum ada 3 jenis memori **[ISO7816-95]** yang digunakan:

1. **ROM** (*Read Only Memory*), berfungsi untuk menyimpan program utama dan sifatnya permanen.
2. **RAM** (*Random Access Memory*), berfungsi untuk menyimpan data sementara ketika proses sedang berjalan atau hasil penghitungan selama mengeksekusi perintah.
3. **EEPROM** (*Electrically Erasable Programmable Read Only Memory*), berfungsi untuk menyimpan program dan data yang sewaktu-waktu bisa diubah.

3.2.1 Pengolahan data pada *Chip Card*

Chip card, disebut juga *tamper resistant security devices*, adalah suatu teknologi *chip VLSI* yang berfungsi bukan hanya untuk menyimpan data tetapi dapat memproses suatu informasi dan mengontrol secara internal suatu algoritma kriptografi sehingga cocok digunakan untuk pengecekan identitas dan mengembangkan suatu sistim keamanan secara logika dan elektronik. Kartu kredit modern pada dasarnya mempunyai tiga elemen, yaitu ***processing power***, ***data storage elemen***, dan ***input/output data***. *Processing power* akan didukung oleh *chip* mikroprosesor, *storage element* oleh *chip* memori, dan I/O data melalui kontak metal yang terdapat dalam lapisan atas kartu. Hal tersebut berlangsung dengan cara memasukkan kartu ke dalam slot unit pembaca/menulis (read/write) sehingga komunikasi data akan mengalir antara kartu dengan unit pembacanya.

Aplikasi *Chip card* telah banyak digunakan pada saat ini, seperti untuk kepentingan transaksi keuangan, *medical record* untuk si pemegang kartu, telephone kartu, dan lain sebagainya. Tetapi hal yang perlu diperhatikan dengan berkembangpesatnya penggunaan *Chip card* ini adalah

faktor keamanan. Proses identifikasi atau otentifikasi sangat diperlukan agar informasi yang ada dalam kartu tidak bisa diubah atau dipakai oleh pihak yang tidak berhak.

3.2.1 Tipe Kriptografi pada Chip Card

Otentikasi Kartu kredit modern.

Proses otentikasi antara *Chip card* (*prover*) dengan perangkat penerima (*verifier*) dilaksanakan di tempat transaksi, langsung seperti di bank atau pasar swalayan. Proses identifikasi secara kriptografi dari kedua unit ini disebut *card (node) authentication*.

Dengan perangkat perantara ini, perangkat penerima akan memverifikasi otentikasi dari *Chip card* kemudian *Chip card* akan membuktikan identitasnya terhadap perangkat *verifier*. Sehingga hal ini akan memberikan suatu proses otentikasi yang saling mendukung untuk keamanan yang berlapis terhadap sistem informasi. Perbedaan prinsip secara rinci antara ketiga metoda otentikasi tersebut membutuhkan diskusi tersendiri tetapi tabel di bawah ini akan memberikan gambaran dasar secara umum dari setiap metoda otentifikasi Kartu kredit modern ditinjau dari prosedur yang harus dilakukan.

Tabel 1
Perbandingan Prosedur Otentikasi Kartu kredit modern

No	Karakteristik	**Algoritma Satu Kunci Simetris**	**Algoritma Kunci Publik Asimetris**	**Algoritma Berbasis Zero Knowledge**
1.	Persamaan Enkripsi	$Y'=E_K(Z)$	$Y \equiv Z^d \pmod n$	$T \equiv r^v \pmod n$
2	Persamaan Dekripsi	$Z' = D_K(Y')$	$Z' \equiv Y^e \pmod n$	$T = J^d t^v \pmod n$
3	Jumlah pemakaian kunci	Satu kunci (K)	Dua kunci (d dan n)	Satu kunci (B)
4	Perlu Random Generator	Ya	Tidak	Tidak
5	Pemakaian memori chip	Lebih besar	Lebih besar	Lebih kecil
6	Komunikasi	Rumit	Rumit	Sederhana
7	Tingkat keamanan sistem	Sedang	Tinggi	Tinggi
8	Penanganan thd. trouble	Mudah,Cepat	Rumit	Rumit
9	Algoritma /Chiper	Sederhana	Sulit	Sulit
10	Kerumitan realisasi	Rendah	Sedang	Sedang
11	Waktu proses	Cepat	Sedang	Lebih lama
12	Perlu akses ke Card Issuer's Master Key	Ya	tidak	tidak

3.2.1 Kelebihan & kekurangan dari penggunaan *Chip Card*

Keuntungan menggunakan *Chip card* :

1. Lebih handal daripada *kartu magnetik* (kartu magnetik)

Kehandalan dari *Chip card* disebabkan oleh proteksi terhadap keamanan data yang disimpan. Keamanannya tidak hanya tergantung pada *chip*, namun juga keseluruhan system termasuk aplikasi serta proses pembuatan dari *Chip card* itu sendiri. *Chip* menjamin keamanan data yang disimpan di dalam *Chip card* disebabkan adanya mekanisme enkripsi sehingga tidak mudah dibaca oleh pihak yang tidak berwenang. Untuk membuat aplikasi *Chip card* juga perlu rancangan *security* terhadap aplikasi itu sendiri, misalnya aplikasi dibuat agar hanya pihak yang berwenang yang dapat menggunakan *Chip card* dan aplikasi yang ada di dalamnya. Selain keamanan chip dan aplikasi, keamanan terhadap proses pembuatan *Chip card* ,terutama pembuatan Mikroprosesor juga perlu dipertimbangkan. Kebanyakan dari perusahaan pembuat *chip* menyembunyikan detail dari rangkaian mikroprosesor, tidak terkecuali pada *customer*-nya.Dalam hal ini ada 3 fase, yaitu *designed-in security*, kontrol terhadap informasi dan proses pembuatan dan pemasaran . *Designed-in security* meliputi perancangan dari chip mikroprosesor. Kontrol terhadap informasi meliputi bagaimana informasi yang rahasia disimpan. Sedangkan proses pembuatan dan pemasaran lebih banyak memperhatikan aspek keamanan dari *chip* tersebut, misalnya tempat penyimpanan yang aman.

2. Lebih banyak menyimpan informasi daripada *kartu magnetik*.

Kapasitas memori dari *Chip card* lebih besar dibanding kartu magnetik. Kartu magnetik hanya memiliki memori sebesar 140 *byte* yang hanya cukup untuk menyimpan kode PIN dan data untuk *login* ke dalam *server-based system*. Oleh karena itu, transaksi lebih banyak dilakukan secara *on-line*. Sedangkan *Chip card* mempunyai ukuran memory bermacam-macam, misalnya :

- 1 Kbyte (CP1 dari ASE(Alladin *Chip card* Environment))
- 2 Kbyte (CC1 dari ASE(Alladin *Chip card* Environment))
- 22 Kbyte (JavaCard)

- 31 Kbyte(MSC0402 dari Motorola). Selain berisi informasi, *Chip card* juga berisi sistem operasi yang mengendalikan seluruh proses yang terjadi di *Chip card* .

3. Lebih sulit untuk ditiru daripada *kartu magnetic*

Kartu magnetik mempunyai pita magnetik pada permukaaannya. Peng-*copy*-an terhadap kartu magnetik dilakukan dengan meng-*copy* pita magnetik tersebut ke kartu lain. Pada *Chip card* peng-*copy*-an terhadap kartu sulit dilakukan, ini disebabkan karena setiap kartu memiliki nomor seri yang unik, tidak ada 2 buah kartu yang memiliki nomor seri yang sama. Jika pengaman dari kartu dilakukan dengan menghitung hash dari nomor seri kartu, maka peng-*copy*-an kartu tidak mungkin dilakukan. Selain itu juga disebabkan karena proteksi terhadap data dengan menggunakan *secret code*, sehingga data tidak dapat dibaca tanpa mengetahui *secret code*-nya.

4. Dapat digunakan kembali

Setelah nilai yang tertulis di dalam *Chip card* , misalnya jumlah pulsa/uang habis,*Chip card* dapat di'isi' ulang dengan menuliskan nilai tertentu ke dalamnya. Ini bisa dilakukan selama kondisi *Chip card* masih baik, misalnya tidak terdapat kerusakan pada chip. Berbeda dengan kartu magnetik, setelah nilai yang ada di dalamnya habis, maka kartu tersebut tidak dapat digunakan kembali.

5. Dapat melakukan banyak fungsi di berbagai area industri

Walapun kartu magnetik telah banyak dimanfaatkan di berbagai sektor, misalnya sektor perbankan dan sektor telekomunikasi, tetapi fungsi yang dapat dilakukan terbatas atau disebut *single function*. Misalnya sebagai kartu kredit untuk melakukan fungsi kredit. Karena keistimewaan yang dimiliki oleh *Chip card* , yaitu dalam hal kapasitas simpan dan kemampuan untuk melakukan proses, *Chip card* menawarkan skema *multi-function*, yaitu satu kartu untuk berbagai layanan. *Chip card* banyak dimanfaatkan misalnya di sektor telekomunikasi, misalnya SIM *card* pada layanan GSM. SIM selain sebagai kartu telepon dengan sistem *Pre-paid* juga akan dikembangkan layanan untuk kredit, jadi semacam ATM pribadi. Di samping itu *Chip card* telah dimanfaatkan di sektor lain, seperti sektor keuangan, transportasi, dan kesehatan.

6. Selalu mengalami evolusi (sesuai dengan perkembangan chip komputer dan memori).

Chip card mempunyai standar mikroprosesor 8-bit, namun saat ini mulai dikembangkan mikroprosesor 32-bit yang mempunyai keuntungan, yaitu memungkinkan melakukan pemrograman dengan menggunakan bahasa tingkat tinggi dan meningkatkan kekuatan komputasi untuk fungsi matematika yang kompleks yang tidak mungkin dilakukan pada mikroprosesor 8-bit. Peningkatan kekuatan komputasi ini akan mempercepat jalannya program dan waktu transaksi. Dan yang paling penting, peningkatan MIPS (*million instruction per second*) memungkinkan industri *Chip card* memanfaatkan kemajuan teknologi biometri dan kriptografi. Selain perkembangan mikroprosesor, perkembangan memori merupakan faktor penting dalam perkembangan *Chip card* . Misalnya proses pembuatan memori menggunakan 0.8 micron menghasilkan memori dengan ukuran 23K ROM, 8K EEPROM dan 384 byte RAM. Dengan makin kecilnya satuan yang digunakan, misal 0.28 *microm*, makin kecil pula ukuran *die* (unit terkecil di dalam memori). Ini menyebabkan kapasitas memori di dalam *chip* tersebut menjadi semakin besar.

Kekurangan menggunakan *Chip card* :

a. Serangan Secara Logika

Semua kunci pada *Chip card* disimpan dalam *Electrically Erasable Programmable Read Only Memory* (EEPROM), dan pada kenyataannya operasi tulis ke EEPROM dapat dipengaruhi oleh tegangan dan temperatur yang tidak biasa, informasi dapat terperangkap dengan menaikkan atau menurunkan tegangan yang diberikan ke *microcontroller* .

Sebagai contoh, serangan yang terkenal yaitu *microcontroller* PIC16C84 akan membersihkan *security bit controller* dengan menghapus memori dengan cara menaikkan tegangan VCC ke VPP-0,5V. Sebagai contoh yang lain adalah serangan terhadap DS5000 *security processor*. Penurunan tegangan kadang-kadang dapat membongkar keamanan kunci tanpa menghapus data rahasia. Tegangan rendah dapat memfasilitasi serangan lain, seperti *analogue random generator* digunakan untuk membuat kunci kriptografi akan mengeluarkan keluaran hampir semuanya angka 1 ketika pemberian tegangan direndahkan.

Untuk alasan-alasan tersebut, beberapa *security processors* mengimplementasikan sensor yang akan mengeluarkan tanda peringatan ketika ada perubahan lingkungan. Bagaimanapun juga, jenis sensor ini selalu mengeluarkan tanda peringatan yang salah akibat dari munculnya fluktuasi ketika *Chip card* diaktifkan dan ketika *Chip card* menstabilkan diri. Oleh sebab itu skema ini tidak biasa digunakan.

Serangan-serangan baru terhadap kriptosistem kunci publik pada alat *tamperproof* muncul untuk mengetahui nilai eksponen pribadi (r) yang disimpan dalam *Chip card* . Eksponen pribadi (r) digunakan untuk membuat kunci privat, oleh sebab itu tidak boleh diketahui oleh pihak lain. Membuka alat *tamperproof* yang tertutup seperti *Chip card* dengan melakukan *external physical effect* (contoh : pengionan atau radiasi *microwave*), memungkinkan seseorang dapat menghasilkan kesalahan bit nilai eksponen pribadi pada lokasi bit sembarang di alat *tamperproof*. Kesalahan dalam lokasi bit sembarang tidak mempengaruhi kode itu sendiri, sebagai contoh program tidak *crash*, dan hanya beberapa nilai operasi yang terkena akibat. Contoh serangan untuk mengetahui nilai r adalah : serangan terhadap skema RSA.

Secara garis besar serangan terhadap skema RSA bekerja sebagai berikut berlaku **n=pq** adalah produk dari dua bilangan p dan q di RSA, **e adalah eksponen yang**

diketahui secara umum dan d adalah eksponen pribadi yang disimpan di dalam alat *tamperproof*. **M adalah sebuah *plaintext***, maka pesan yang terenkripsinya atau ***ciphertext* adalah C = p e mod n**.

Ditunjukkan representasi biner dari eksponen pribadi sebagai

$$\mathbf{r = r\ (t\text{-}1)|\ r\ (t\text{-}2)|\ \ldots\ |\ r\ (I)\ |\ \ldots\ |\ r\ (1)\ |\ r\ (0),}$$

dimana r (I) bernilai 1 atau 0, adalah bit ke I, t adalah jumlah bit d, dan x|y menunjukkan sambungan x dan y. Lebih jauh, ditunjukkan

$$\mathbf{C(0)= C,\ C(1) = C\ 2\ mod\ n,}$$
$$\mathbf{C(2) = C\ (2\text{^}2)\ mod\ n,\ \ldots,}$$
$$\mathbf{C(t\text{-}1) = C\ 2\text{^}(t\text{-}1).}$$

Diberikan C dan r, *plaintext* M dapat diekspresikan sebagai

$$\mathbf{M = (\ (\ C(t\text{-}1)\ d(t\text{-}1))\ (\ C(t\text{-}2)\ d(t\text{-}2))\ \ldots\ (\ C(I)\ r(I))\ \ldots\ (\ C(1)\ r(1))\ (\ C(0)\ r(0))\ mod\ n.}$$

Pada awalnya penyerang secara sembarang memilih suatu *plaintext* (M) dan menghitung *ciphertext* dari M (C). Misalkan salah satu bit dalam representasi biner d berubah dari 1 ke 0 atau sebaliknya, dan posisi bit yang salah bisa dimana saja. Kemudian *Chip card* diminta untuk mendeskripsikan C. Asumsi bahwa r(I) berubah menjadi komplemen r(I)', kemudian *output* dari alat akan menjadi

$$\mathbf{M' = (\ C(t\text{-}1)r(t\text{-}1)\ )\ (\ C(t\text{-}2)\ \ (t\text{-}2)\ )\ \ldots\ (\ C(I)r(I)'\ )\ \ldots\ (\ C(1)r(1)\ )\ (\ C(0)r(0)\ )\ mod\ n.}$$

Sejak penyerang memiliki M dan M', penyerang dapat menghitung M'/M = C(I)r(I)'/ C(I)r(I) mod n. Tentu saja, jika memiliki M/M' = 1/ C(I) mod n, maka r(I)=1, dan jika M'/M = C(I) mod n, maka r(I)=0. Penyerang dapat menghitung sebelumnya C(I) dan 1/C(I) mod n untuk I = 0,1,…, t-1, dan membandingkan M'/M mod n untuk setiap nilai I dalam menentukan satu bit d. Penyerang menentukan proses di atas berulang-ulang menggunakan pasangan *plaintext*/*ciphertext* yang sama sampai penyerang menemukan cukup informasi untuk memperoleh r.

b. Serangan Secara Fisik

Serangan fisik ini ditujukan bagi sirkuit *chip Chip card* . Sebelum serangan jenis ini dilakukan, sirkut *chip* harus dipindahkan dari bagian plastik *Chip card* . Setelah *chip* berhasil diambil, *chip* dapat diperiksa dan diserang secara langsung. Contoh serangan fisik yang lain adalah menghapus *security block bit* dengan memfokuskan sinar UV pada EEPROM, penyelidikan operasi sirkuit dengan menggunakan jarum mikro, atau menggunakan mikroskop laser pemotong untuk memeriksa *chip* dan sebagainya. Bagaimanapun juga, serangan ini hanya berlaku pada laboratorium yang canggih karena untuk melakukan serangan membutuhkan biaya yang tinggi.

i. Dumb Mouse

Dumb mouse adalah *reader* pintar yang kecil, murah, dapat membaca *Chip card* yang sesuai dengan standar **ISO 7816-3** dan mungkin juga jenis lain (termasuk *Chip card* memori maupun *Chip card* dengan *microcontroller*), dan menggunakan port serial komputer. *Chip card* mengeluarkan beberapa data jika mereka di *reset* atau dimasukkan ke alat pembaca. Ini disebut "*answer to reset*" atau **ATR. ATR** akan memberitahukan informasi mengenai pembuat *Chip card* (*issuer*) tersebut dan protokol yang seharusnya digunakan untuk berkomunikasi. Untuk menyandikan *byte* dapat menggunakan "*direct convention*" yaitu langsung mengkomplemenkan *bit* atau "*inverse convention*" yaitu *bit* dibalik dan dibaca dari belakang. Protokol yang biasa digunakan disebut T=0 yaitu protokol paling sederhana dan T=1 yaitu protokol lebih kompleks dan memiliki lapisan jaringan tambahan.

Contoh serangan yang dapat dilakukan :

1. **Pengujian jenis *Chip card*** : *Chip card* magnetik atau *Chip card* dengan *microcontroller*.
2. **Lihat dalam ATR** : tentukan teknik penyandiannya dan protokol yang digunakan.
3. **Menebak instruksi** yang digunakan, ada beberapa cara :
   - Coba semua kemungkinan. *Dumb mouse* beroperasi pada 9600 *baud* sehingga walaupun banyak *Chip card* , *dumb mouse* dapat bekerja dua kali lebih cepat. Hal ini berbahaya, karena seseorang dapat mengeksekusi instruksi yang merusak, mengkosongkan atau mem-*block Chip card* .
   - Melakukan *eavesdrop* pada komunikasi sesungguhnya dengan menggunakan alat *login*. Alat *login* dapat terlihat sebagai perpanjangan kawat antara *Chip card* dan terminal. Setiap *byte* yang dikirim dari atau ke *Chip card* dapat diawasi dan membantu untuk mengerti perintah dan protokol. Kesulitan yang ada adalah jika terminal beroperasi dengan kecepatan *baud* yang tidak sesuai standar dan jika terminal menggunakan detektor logam maka penggunaan *Chip card* dengan kawat (alat untuk *login*) tidak mungkin dilakukan.
   - Cari manual. Cara yang paling mudah. Tetapi membutuhkan biaya dan terkadang spesifikasi *Chip card* tidak disebarluaskan ke masyarakat.

4. **Dengan menggunakan spesifikasi terminal** dapat mengetahui beberapa perintah. Dengan perintah ini dapat memilih *file*, dapat membaca data dalam *file*, dapat memperoleh informasi rahasia dan dapat membaca informasi transaksi.

c. Serangan Pertukaran Pesan Melalui Jaringan Komputer

Berdasarkan bagaimana cara dan posisi seseorang mendapatkan pesan-pesan dalam saluran komunikasi, penyerangan dapat dikategorikan menjadi:

1. ***Sniffing***: secara harafiah berarti mengendus, tentunya dalam hal ini yang diendus adalah pesan (baik yang belum ataupun sudah dienkripsi) dalam suatu saluran komunikasi. Hal ini umum terjadi pada saluran publik yang tidak aman. Sang pengendus dapat merekap pembicaraan yang terjadi.
2. ***Replay attack****:* Jika seseorang bisa merekam pesan-pesan *handshake* (persiapan komunikasi), ia mungkin dapat mengulang pesan-pesan yang telah direkamnya untuk menipu salah satu pihak.
3. ***Spoofing****:* Penyerang – misalnya C – bisa menyamar menjadi A. Semua orang dibuat percaya bahwa C adalah A. Penyerang berusaha meyakinkan pihak-pihak lain bahwa tak ada salah dengan komunikasi yang dilakukan, padahal komunikasi itu dilakukan dengan sang penipu/penyerang. Contohnya jika orang memasukkan PIN ke dalam *Card Acceptance Device* (CAD) – yang benar-benar dibuat seperti CAD asli – tentu sang penipu bisa mendapatkan PIN pemilik *Chip card* . Pemilik *Chip card* tidak tahu bahwa telah terjadi kejahatan.
4. ***Man-in-the-middle****:* Jika *spoofing* terkadang hanya menipu satu pihak, maka dalam skenario ini, saat A hendak berkomunikasi dengan B, C di mata A seolah-olah adalah B, dan C dapat pula menipu B sehingga C seolah-olah adalah A. C dapat berkuasa penuh atas jalur komunikasi ini, dan bisa membuat berita fitnah. Kabel koaksial yang sering digunakan pada jaringan sangat rentan terhadap serangan *vampire tap*, yakni perangkat keras sederhana yang bisa menembus bagian dalam kabel koaksial sehingga dapat mengambil data yang mengalir tanpa perlu memutuskan komunikasi data yang sedang berjalan. Seseorang dengan *vampire tap* dan komputer jinjing dapat melakukan serangan pada bagian apa saja dari kabel koaksial.

Penyerang juga bisa mendapatkan kunci dengan cara yang lebih tradisional, yakni dengan melakukan penyiksaan, pemerasan, ancaman, atau bisa juga dengan menyogok seseorang yang memiliki kunci itu. Ini adalah cara yang paling ampuh untuk mendapat kunci.

4. PERBANDINGAN KEAMANAN PADA *MAGNETIC CARD* DAN *CHIP CARD*

Fitur keamanan	Kartu Chip	Kartu Magnetic Stripe
Enkripsi dalam komunikasi data	Kartu chip dan terminal mempertukarkan data yang telah dienkripsi.	Kartu chip dan terminal mempertukarkan data *plain*.
Kerahasiaan data yang tersimpan dalam kartu	Data dilindungi dengan mekanisme akses kontrol atau dengan enkripsi.	Semua data disimpan di kartu dalam bentuk *plain*
Otentikasi	Terminal melakukan otentikasi terhadap kartu dengan menggunakan mekanisme *static data authentication* (SDA) atau *dynamic data authentication* (DDA). Data yang diperlukan untuk otentikasi dilindungi oleh mekanisme akses kontrol.	Terminal melakukan otentikasi terhadap kartu dengan cara membaca data-data dalam *magnetic stripe*. Data-data ini tidak dilindungi dengan mekanisme akses kontrol.
	Mekanisme otentikasi timbal balik dapat dilakukan, yaitu terminal mengotentikasi kartu dan kartu mengotentikasi terminal.	Tidak memungkinkan mekanisme otentikasi timbal-balik.
Non repudiasi	Mekanisme non-repudiasi dapat dilakukan karena terdapat data-data (kunci) yang dilindungi oleh mekanisme akses kontrol. Mekanisme biasanya berbasis *asymmetric encryption*.	Tidak terdapat mekanisme non-repudiasi karena kartu tidak memiliki mekanisme akses kontrol.
Transaksi secara *offline*	Dalam transaksi *offline*, terminal tetap dapat melakukan otentikasi terhadap kartu (dengan SDA atau DDA) dan memeriksa integritas data otentikasi.	Terminal tidak dapat memastikan integritas data otentikasi.

IV. KESIMPULAN

Penggunaan sistem *magnetic stripe card* pada kartu ATM sebelumnya telah dirasa cukup untuk menangani segala penyimpanan data, pengambilan data, dan pengamanan data. Akan tetapi seiring dengan perkembangan teknologi, sistem yang dimiliki oleh *magnetic stripe card* sudah dirasa tidak bisa menangani kasus tindak kejahatan yang menyerang sistem keamanan kartu magnetic stripe.

Perbaikan sistem kartu ATM dengan menggunakan kartu *chip* dinilai bisa menangani kelemahan yang dimiliki oleh kartu *magnetic stripes*. Dalam kondisi sekarang, penggunaan kartu chip untuk menggantikan kartu magnetic stripes dirasa cukup untuk menangani kasus penyerangan yang terjadi.

Namun demikian, harus disadari bahwa teknologi tidak akan berhenti berkembang sekarang. Akan ada, nantinya, teknik-teknik penyerangan yang lebih canggih yang mungkin akan bisa membobol sistem keamanan yang dimiliki kartu *chip*.

Oleh karena itu, kita tidak bisa langsung puas saja dengan penggunaan kartu chip. Inovasi-inovasi baru dibutuhkan untuk memperkuat keamanan dalam hal penyimpanan data rahasia untuk aplikasi-aplikasi tertentu seperti kartu ATM.

Ketika tindak kejahatan untuk mencuri data semakin canggih, inovasi untuk mengamankan data harus semakin canggih pula.

REFERENSI

[1] Munir, Rinaldi. "Kriptografi dalam kehidupan sehari-hari",2004, halaman 5-7.

[2] Priyandono,Bambang. "Authentication temper resistean security devices pada kartu kredit modern menggunakan metoda algoritma kunci simetris",2004, halaman 4-5 dan 14-15.

[3] Priyandono,Bambang. "tinjauan smart card untuk pengamanan database di sekolah berbasis komputer",2004, halaman 3-6 dan 10-14.

[4] *Magnetic Stripe Card* http://en.wikipedia.org/wiki/Magnetic_stripe_card (diakses pada tanggal 22 Maret pukul 17.00 WIB)

[5] *Introduction to Magnetic Stripe & Other Card Technologies*. http://www.hightechaid.com/tech/card/intro_ms.htm (diakses pada tanggal 22 Maret pukul 17.00 WIB)

[6] *Layout of data in magnetic stripes card* http://www.topbits.com/layout-of-data-on-magnetic-stripe-cards.html (diakses pada tanggal 22 Maret pukul 17.00 WIB

[7] *Magnetic Stripes* http://cobweb.ecn.purdue.edu/~tanchoco/MHE/ADC-is/Magnetic/main.shtml (diakses pada tanggal 22 Maret pukul 17.00 WIB)

[8] Kartu Pintar http://id.wikipedia.org/wiki/Kartu_pintar (diakses pada tanggal 22 Maret pukul 17.00 WIB)

[9] *Smart card* http://en.wikipedia.org/wiki/Smart_card (diakses pada tanggal 22 Maret pukul 17.00 WIB).

[10] Meng-*encode* kartu smart card http://www.evolis.com/ind/content/view/full/1189 (diakses pada tanggal 22 Maret pukul 17.00 WIB).