Sistem Keamanan ATM (*Automated Teller Machine* / Anjungan Tunai Mandiri)

Roni Sambiangga [NIM: 13502025]

Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung
Jalan Ganesha No. 10, Bandung 40132
INDONESIA

Email: if12025@students.if.itb.ac.id

Abstrak

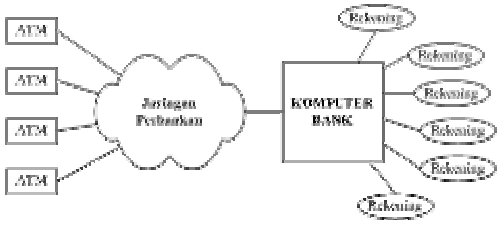
Pada makalah ini dibahas studi literatur mengenai sistem keamanan pada ATM (*automated teller machine* / anjungan tunai mandiri) yang meliputi pengamanan PIN (*personal identification number*) dan bentuk serangan pada keamanan ATM. Metode yang digunakan dalam pengamanan pada ATM adalah dengan penggunaan PIN untuk dapat melakukan akses dan transaksi melalui mesin ATM. Pengamanan PIN dilakukan dengan menggunakan proses kriptografi (enkripsi dan dekripsi) dengan menggunakan standar *Triple* DES (*data encryption standard*).

Penggunaan ATM tidak terlepas dari perlunya menjaga sistem keamanan pada ATM. Dalam dokumen ini dijelaskan penggunaan metode kriptografi DES dan *Triple* DES. Saat ini sudah terdapat berbagai ancaman yang menyerang keamanan dalam penggunaan ATM seperti *skimming*, *phishing*, dsb.

Kata kunci: ATM, *Automated Teller Machine*, *data encryption standard*, *phishing*

Pendahuluan

ATM (*Automated Teller Machine* / Anjungan Tunai Mandiri) merupakan sebuah perangkat komputerisasi yang digunakan oleh suatu lembaga keuangan (bank) dalam upaya menyediakan layanan transaksi keuangan (pengambilan uang) di tempat umum tanpa membutuhkan adanya pegawai bank (*teller*). Pada mulanya penyediaan ATM adalah untuk memudahkan layanan pengambilan uang dari tabungan nasabah, akan tetapi seiring dengan perkembangan teknologi dan kebutuhan akan peningkatan layanan kepada para nasabah, penggunaan ATM telah meluas tidak hanya sebatas pengambilan uang saja. Saat ini sudah memungkinkan bagi para nasabah untuk melakukan transfer (pemindahbukuan) uang, pembayaran, pengecekan saldo, dan transaksi keuangan lain sebagainya cukup dengan menggunakan ATM. Secara umum, teknologi pada ATM merupakan suatu bentuk jaringan komputer yang tersebar, yang dapat digambarkan (gambar 1) sebagai berikut:



Gambar 1 Jaringan ATM

Adanya proses transaksi (komunikasi) antarkomputer yang melalui sebuah jaringan yang luas, isu mengenai keamanan merupakan isu yang perlu diperhatikan secara khusus. Hal ini tentunya untuk menjamin proses transaksi dapat terjadi dengan baik dan benar. Teknik pengamanan yang dilakukan

adalah dengan penggunaan *personal identification number* (PIN) sehingga hanya orang tertentu saja yang dapat mengakses ataupun melakukan transaksi pada ATM. Untuk pengaksesan pada mesin ATM para nasabah akan memiliki kartu dengan pita magnetik atau sebuah chip yang berfungsi sebagai tempat penyimpanan data seperti nomor kartu, nomor PIN, dan data keamanan lainnya. Dalam sistem keamanan yang diterapkan pada ATM terdapat proses enkripsi data untuk menjaga keamanan data pribadi, seperti nomor PIN ataupun nomor kartu, dan juga untuk menjaga keamanan selama proses transaksi berlangsung (pada saat proses transaksi berlangsung terjadi komunikasi antara ATM dengan komputer bank yang melalui jaringan perbankan).

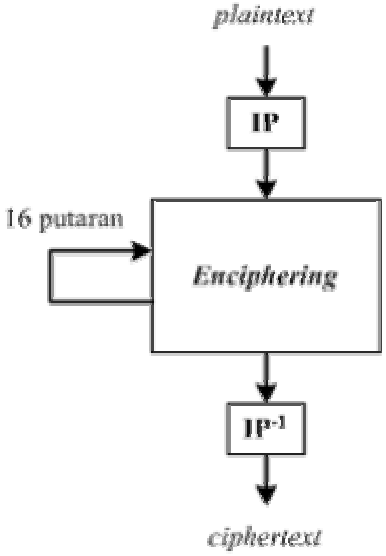
Untuk menjamin keamanan pada ATM digunakan metode enkripsi data dengan teknik *data encryption standard* (DES); yang kemudian dikembangkan menjadi *Triple DES* guna meningkatkan keamanan data.

Data Encryption Standard (DES)

Data Encryption Standard (DES) merupakan sebuah standar dalam sistem kriptografi dengan tipe dan mode algoritma simetri. Algoritma kriptografi yang digunakan pada DES – yang disebut sebagai *Data Encryption Algorithm* (DEA) – merupakan pemrosesan terhadap bit dalam bentuk *block cipher* (*cipher* blok). DES merupakan *cipher* blok dengan menggunakan blok 64-bit dan menggunakan kunci eksternal dengan panjang kunci sebesar 64 bit juga (sama dengan ukuran blok). Pada DES, proses enkripsi data (*plaintext*) menggunakan kunci internal atau upa-kunci (*sub-key*) sepanjang 56 bit yang dibangkitkan dari kunci eksternal. Prosedur yang dilakukan dengan algoritma DES adalah sebagai berikut:

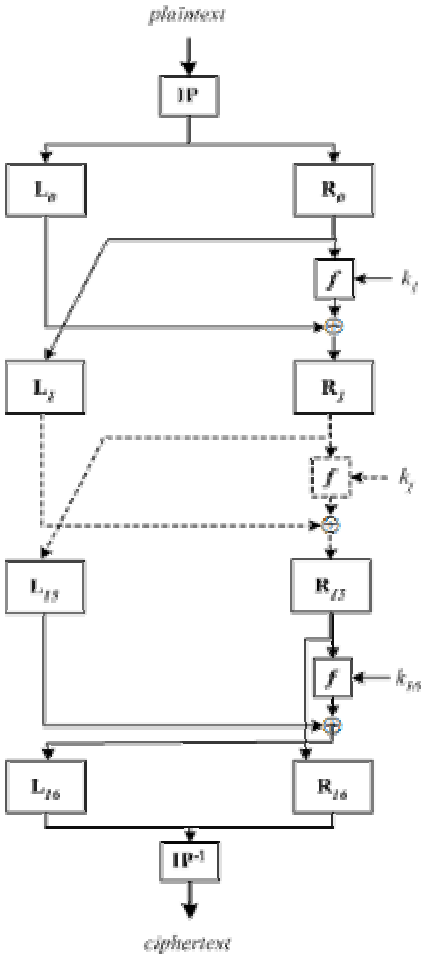
1. Blok *plaintext* dipermutasi dengan menggunakan matriks permutasi awal (*initial permutation*/IP)
2. Terhadap blok hasil permutasi awal tesebut dilakukan proses *enciphering* (enkripsi) dengan melakukan 16 putaran (*round*). Pada proses inilah digunakan kunci internal yang berbeda-beda untuk setiap putarannya.
3. Hasil dari proses *enciphering* tersebut akan dipermutasi dengan menggunakan matriks permutasi balikan (*invers initial permutation*/IP^{-1})

Skema dari proses dengan menggunakan algoritma DES dapat digambarkan (gambar 2) sebagai berikut:



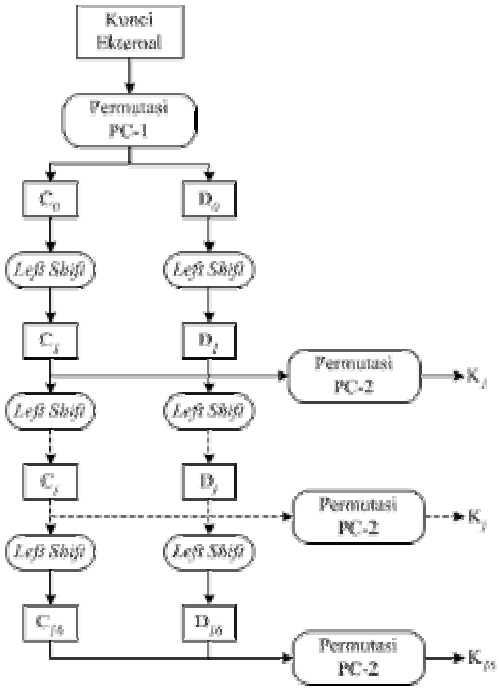
Gambar 2 Skema algoritma pada DES

Pada proses *enciphering*, setiap putarannya digunakan algoritma dengan model jaringan Feistel. Dengan demikian pada proses *enciphering* blok *plaintext* hasil permutasi awal akan dibagi menjadi dua bagian dengan ukuran masing-masing 32 bit. Di dalam jaringan Feistel inilah digunakan kunci internal terhadap fungsi transfromasi. Secara lengkap skema algoritma pada DES digambarkan pada gambar 3.



Gambar 3 Skema lengkap algoritma pada DES

Pada DES pembangkitan kunci dilakukan dengan menggunakan kunci eksternal yang diberikan sebelumnya. Proses pembangkitan kunci internal dilakukan dengan melakukan permutasi dan penggeseran bit ke kiri. Keseluruhan pembangkitan kunci internal dilakukan seperti pada gambar 4 berikut:



Gambar 4 Diagram pembangkitan kunci internal (sub-key) pada DES

Kunci internal yang telah dibangkitkan akan digunakan pada fungsi f dalam algoritma DES. Secara sistematis proses *enciphering* merupakan proses pada model jaringan Feistel yang dirumuskan sebagai berikut:

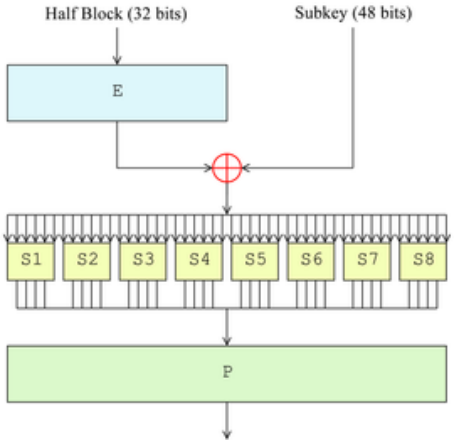
$$\mathbf{L_i = R_{i-1}}$$

$$\mathbf{R_i = L_{i-1} + f(R_{i-1}, K_i)}$$

Keterangan:

L = sub-blok kiri (*left*)
R = sub-blok kanan (*right*)
i = 1, 2, ..., *r*; *r* adalah jumlah putaran
K_i = kunci pada putaran ke-*i*
f = fungsi transformasi

Pada fungsi tranformasi algoritma DES dilakukan fungsi ekpansi (E), fungsi XOR, subtitusi (S), dan permutasi (P) terhadap vektor-vektor bit dari setiap sub-blok. Fungsi transformasi digambarkan pada diagram komputasi (gambar 5) berikut:



Gambar 5 Diagram komputasi fungsi pada DES

untuk proses *deciphering* (dekripsi) pada DES, operasi yang dilakukan merupakan kebalikan dari operasi yang dilakukan pada saat melakukan proses *ciphering*.

Penggunaan DES sebagai standar kriptografi (pengamanan) data masih diperdebatkan dan pada DES terdapat celah keamanan yang cukup fatal yaitu penggunaan kunci dengan ukuran 56 bit. Penggunaan kunci dengan jumlah kemungkinan yang cukup "sedikit" ini (2^{56} atau 72.057.594.037.927.936 kemungkinan) mengakibatkan rentan terhadap serangan keamanan. *Electronic Frontier Foundation* (EFE) pada tahun 1998 merancang dan membuat sebuah perangkat keras (DES *cracker*) dengan menggunakan metode *exhaustive search key* untuk memecahkan kunci pada DES dan diharapkan dapat berhasil menemukan kunci DES tersebut selama 5 hari. Setahun kemudian, penggunaan DES *cracker* dengan kolaborasi internet dapat menemukan kunci DES kurang dari 1 hari. Dikarenakan kelemahan tersebut kemudian dikembangkanlah DES sehingga menghasilkan standar yang disebut sebagai *Triple* DES.

Triple DES

Triple DES merupakan varian pengembangan dari DES (*Data Encryption Standar*) – sebelumnya disebut sebagai "*multiple* DES" dikarenakan pada dasarnya *triple* DES hanyalah penggunaan DES secara berulang; dalam hal ini pengulangannya dilakukan tiga kali. *Triple* DES umumnya disebut juga dengan singkatan TDES atau dengan istilah 3DES. Secara umum *triple* DES dirumuskan sebagai berikut:

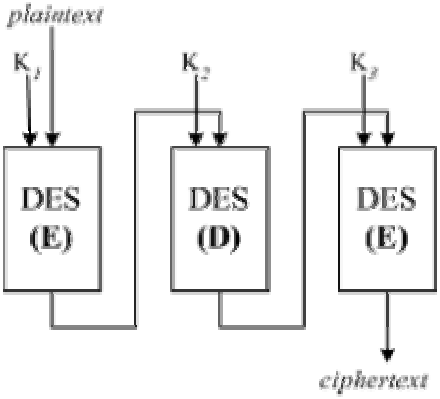
Enkripsi: $C = E_{K3}(E_{K2}(E_{K1}(P)))$

Dekripsi: $P = D_{K3}(D_{K2}(D_{K1}(C)))$

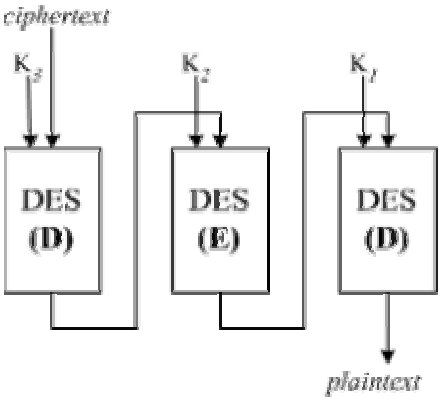
Keterangan:
P = *plaintext*
C = *ciphertext*
E = enkripsi
D = dekripsi
K*i* = kunci ke-*i*

Varian di atas umumnya disebut dengan mode EEE (dikarenakan menggunakan tiga kali proses enkripsi). Namun, kemudian dilakukan sebuah penyederhanaan terhadap varian tersebut sehingga melahirkan mode baru yang disebut sebagai EDE (enkripsi-dekripsi-enkripsi), dengan adanya penyisipan fungsi dekripsi. Penggunaan tiga kali DES pada *triple* DES diharapkan dapat meningkatkan keamanan dikarenakan juga adanya penggunaan kunci yang lebih panjang yaitu kunci dengan ukuran 168 bit (tiga kali ukuran DES, 56 bit). Pada penggunaan *triple* DES dengan mode EDE dapat dilakukan dengan menggunakan 3 kunci, 2 kunci ataupun hanya menggunakan 1 kunci.

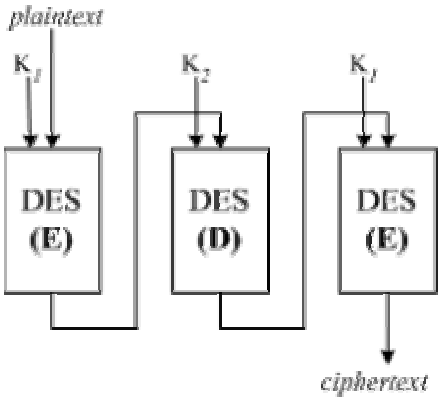
Skema model triple DES digambarkan sebagai berikut:



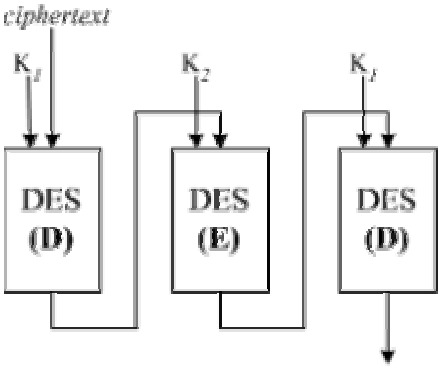
Gambar 6 *Triple* DES 3-kunci (enkripsi)



Gambar 7 *Triple* DES 3-kunci (dekripsi)



Gambar 8 *Triple* DES 2-kunci (enkripsi)



Gambar 9 *Triple* DES 2-kunci (dekripsi)

Penggunaan triple DES dengan 1 kunci merupakan bentuk penyederhanaan yang menggunakan kunci k = k1 = k2 = k3.

Menyangkut keamanan dalam penggunaan triple DES, masih memungkinkan terjadi penyerangan dengan menggunakan sekitar 2^{32} *known-plaintexts*, 2^{113} langkah, 2^{90} pemecahan DES, dan 2^{88} kapasitas memori. Tentu saja untuk melakukan hal tersebut akan membutuhkan biaya yang sangat besar.

Saat ini, penggunaan triple DES sudah mulai ditinggalkan dikarenakan kehadiran standar baru yang disebut sebagai *Advanced Encryption Standard* (AES). Salah satu kelebihan yang dimiliki oleh AES adalah kecepatan dalam melakukan proses. AES dapat melakukan proses enam kali lebih cepat jika dibandingkan dengan *triple* DES untuk kapasistas pemrosesan yang sama. Akan tetapi penggunaan *triple* DES masih cukup banyak dijumpai dikarenakan butuhnya biaya yang cukup besar untuk beralih ke teknologi yang baru. Selain itu, jika dibandingkan dengan AES, penerapan *triple* DES dirasakan lebih cocok untuk penerapan pada perangkat keras, seperti pada sistem jaringan komunikasi, perangkat jaringan VPN, ataupun pada ATM.

Pengamanan Pada ATM

Pada sistem keamanan ATM umumnya menggunakan nomor PIN dengan kombinasi empat angka. Proses pembuatan nomor PIN tersebut menggunakan perhitungan sebagai berikut:

1. Ambil lima digit terakhir dari nomor rekening
2. Gabungkan kelima angka tersebut dengan 11 digit data validasi (data validasi diciptakan sendiri)
3. Keenambelas angka tersebut merupakan data yang menjadi data masukan untuk algoritma DES. Pada pemrosesan dengan algoritma DES digunakan kunci berukuran 16 digit yang kemudian disebut sebagai “kunci PIN”.
4. Dari hasil pemrosesan dengan DES diambil 4 digit pertama kemudian diubah ke dalam bentuk desimal – penggunaan DES akan menghasilkan bilangan dengan satuan heksadesimal. Empat digit tersebut kemudian disebut sebagai “PIN alami”.
5. Dari PIN alami tersebut kemudian ditambahkan dengan 4 digit yang disebut sebagai *offset* sehingga menghasilkan nomor PIN yang akan digunakan oleh nasabah.

Sebagai contoh:

- Misalkan nomor rekening nasabah adalah *4506602100091715*
- Lima digit terakhir adalah *91715*
- Data validasi adalah *88070123456*
- Masukan untuk algoritma DES adalah *8807012345691715*
- "Kunci PIN" untuk algoritma DES adalah *FEFEFEFEFEFEFEFE*
- Hasil dari algoritma DES adalah *A2CE126C69AEC82D*
- "PIN alami" (empat digit pertama) adalah *0224*
- Nilai *offset* adalah *6565*
- Nomor PIN nasabah adalah *6789*

Pada kartu ATM (ataupun kartu kredit) yang dimiliki oleh nasabah terdapat pita magnetik – umumnya sering disebut sebagai lapisan ke-dua (*track 2*) pita magnetik – yang digunakan untuk menyimpan data rahasia terkait dengan data-data keamanan seperti nomor rekening, nomor kartu, nomor PIN, dan lain sebagainya.

Serangan Pada Keamanan ATM

Penggunaan teknik enkripsi (kriptografi) tidak selalu menjamin seratus persen pada sistem keamanan ATM. Berbagai kejahatan atau kecurangan terhadap sistem keamanan ATM tidaklah sedikit. Kejahatan yang terjadi mulai dari tindakan yang cukup sederhana, seperti pencopetan, penodongan, ataupun perampokan, sampai penggunaan teknologi yang cukup canggih yaitu penggunaan teknologi untuk mengetahui nomor rekening, PIN nasabah, ataupun melakukan duplikasi data keamanan nasabah. Berikut akan dijelaskan beberapa ancaman keamanan pada penggunaan ATM.

Pencurian uang

Salah satu bentuk paling sederhana dalam melakukan kecurangan di ATM adalah dengan mencuri uang hasil pengambilan yang dilakukan oleh nasabah. Tentunya pencurian di sini bukan dengan menodong nasabah setelah melakukan transaksi melainkan menggunakan alat "penyimpan" uang yang ditempelkan pada mesin ATM (gambar 10).

Gambar 10 Alat "penyimpan" uang

Alat yang digunakan dalam metode ini adalah sebuah "duplikat" tempat keluarnya uang pada mesin ATM. Dengan demikian nasabah yang akan melakukan transaksi tidak mencurigai perangkap tersebut. Saat nasabah melakukan transaksi tentunya diharapkan uang akan keluar dari mesin ATM. Namun, dikarenakan uang tersebut disimpan di perangkap tersebut, seolah-olah proses yang terjadi adalah mesin ATM kehabisan uang, sudah tidak ada lagi lebar uang yang tersisa di dalam mesin ATM tersebut. Setelah merasa proses transaksi gagal maka nasabah (sang korban) meninggalkan mesin ATM dan tak lama setelah itu dang pelaku kejahatan mengambil "tabungan"-nya di ATM tersebut.

Pencurian kartu

Proses pencurian kartu yang dimaksud di sini adalah dengan menggunakan alat yang "ditanamkan" ke dalam mesin ATM yaitu pada lubang/slot untuk memasukkan kartu ATM (gambar 11). Fungsi alat tersebut adalah seolah-olah mengakibatkan situasi dimana kartu "tertelan" oleh mesin ATM sehingga nasabah tidak sadar bahwa sebenarnya kartu ATM miliknya telah dicuri.

Gambar 11 Alat untuk "menelan" kartu ATM

Pada saat nasabah (sang korban) kebingungan dengan situasi tersebut, sang pelaku kejahatan seolah-olah datang untuk membantu dan meminta nasabah tersebut untuk memasukkan nomor PIN kembali dengan dalih untuk memastikan proses di ATM tersebut; secara diam-diam pelaku kejahatan mengintip nomor PIN nasabah. Dikarenakan kartu ATM tidak dapat terselamatkan nasabah tersebut dianjurkan untuk melapor ke pihak yang terkait. Setelah nasabah pergi sang pelaku kejahatan dapat melakukan transaksi dengan kartu yang "disimpan" di mesin ATM dan ia juga mengetahui nomor PIN kartu tesebut.

Dengan menggunakan metode pencurian kartu tersebut, tentunya hal yang menjadi perhatian utama bagi pelaku kejahatan adalah mengenai nomor PIN dari kartu ATM tersebut agar dapat digunakan. Bila menggunakan cara yang telah disebutkan sebelumnya tentunya dapat menimbulkan kecurigaan bagi sang korban. Oleh karena itu, terdapat beberapa teknik lain yang digunakan untuk mendapatkan nomor PIN dari nasabah yang menjadi korban kejahatan tersebut, yaitu:

- Penggunaan kamera tersembunyi

  Teknik ini merupakan teknik yang sederhana. Dengan menempatkan posisi kamera di tempat yang strategis dan tersembunyi dengan baik, pelaku kejahatan dapat dengan mudah melihat nomor PIN yang dimasukkan oleh nasabah (sang korban).

Gambar 12 Penggunaan kamera tersembunyi

- Penggunaan tombol-kunci palsu

  Pada teknik ini digunakan tombol-kunci (*keypad*) palsu yang berfungsi untuk mengirimkan nomor PIN yang ditekan oleh nasabah kepada pelaku kejahatan. Nasabah tidak menyadari bahwa tombol-kunci yang ditekan tersebut merupakan media untuk mengirimkan nomor PIN kartu ATM tersebut karena penampilan dari tombol-kunci seolah-olah merupakan bagian dari mesin ATM.

Gambar 13 Tombol-kunci palsu

- Penyadapan nomor PIN

  Penyadapan nomor PIN menyerupai dengan metode yang digunakan dengan tombol-kunci palsu. Hanya saja bedanya pada penyadapan nomor PIN dilakukan dengan mengakses data yang disimpan di dalam mesin ATM. Pada saat nasabah memasukkan nomor PIN-nya di mesin ATM saat itu juga data tersebut tersimpan secara elektronik (digital) pada alat

pencatatan data elektronik di mesin ATM tersebut. Dengan melakukan penyadapan terhadap akses data tersebut maka dapat diambil data-data penting yang disimpan di dalam mesin ATM tersebut salah satunya adalah nomor PIN nasabah.

Skimming

Metode *skimming* dapat dipahami sebagai metode "penyaringan" data pada kartu ATM nasabah. Untuk kasus kejahatan dengan metode skimming digunakan alat yang disebut sebagi "*skimer*" (gambar 14). Fungsi alat ini adalah untuk "menyaring" data-data yang terdapat di dalam kartu ATM nasabah.

Gambar 14 *Skimer*, alat "penyaring" data pada kartu ATM

Penempatan *skimer* diletakkan di sekitar mesin ATM sehingga seolah-olah alat tersebut merupakan bagian dari mesin ATM. Cara kerja alat ini adalah dengan menyalin data-data yang ada di dalam pita magnetik kartu ATM pada saat digesekan di alat tersebut. Setelah data di dalam kartu ATM disalin maka pelaku kejahatan dapat melakukan duplikasi kartu ATM dan melakukan transaksi pengambilan uang di ATM layaknya seorang nasabah.

Phishing

Phising merupakan bentuk kejahatan dengan manggunakan teknik rekayasa sosial. Pada penggunaan teknik ini sang pelaku kejahatan mencoba untuk mencari tahu dan mengambil data-data pribadi nasabah dengan memposisikan dirinya sebagai seseorang ataupun lembaga yang dapat dipercaya dalam melakukan transaksi ataupun komunikasi secara elektronik. Umumnya penggunaan teknik penipuan ini dilakukan dengan menggunakan media internet, email, ataupun telepon. Pelaku akan mengaku sebagai orang yang dapat dipercaya dalam melaksanakan suatu kegiatan atau transaksi tertentu. Pada bentuk penyerangan menggunakan ATM umumnya saat ini adalah dengan menggunakan fasilitas transfer yang sudah dapat dilakukan melalui mesin ATM. Dengan menggunakan nomor rekening tujuan tertentu maka proses transfer dilakukan dan pada saat itu juga data-data nasabah dapat diketahui oleh pelaku kejahatan. Dalam proses komunikasi dengan menggunakan jaringan komputer tentunya dibutuhkan informasi mengenai pengirim dan penerima. Dengan menempatkan diri sebagai penerima, sang pelaku kejahatan tentunya dapat mengetahui data-data mengenai sang pengirim, dalam hal ini adalah nasabah (sang korban). Dengan menggunakan metode ini, pelaku kejahatan akan mengetahui data-data dari nasabah terutama terkait dengan rekening, alamat, ataupun data-data lain yang terkait.

Teknik phishing yang dilakukan dengan media ATM adalah untuk mengetahui data-data yang terdapat di dalam pita magnetik (*track 2*) karena pada pita magnetic tersebut tersimpan data-data rekening ataupun finansial nasabah diantaranya adalah *card verification value* (CVV) dan *card validation code* (CVC). Kedua data tersebut merupakan data yang digunakan oleh Visa dan MasterCard yang merupakan data untuk melakukan transaksi. Dengan mendapatkan data-data tersebut, sang pelaku dapat membuat duplikat kartu dan menggunakan kartu tersebut dalam melakukan transaksi sehari-hari tanpa perlu pusing memikirkan saldo yang mencukupi atau tidak. Seandainya kartu tersebut sudah tidak bisa dipakai lagi, maka yang dilakukan adalah menggunakan kartu lain milik nasabah yang lainnya.

Umumnya bentuk serangan dengan teknik *phishing* saat ini cukup banyak terjadi pada media internet, salah satunya pada bidang perbankan dengan adanya layanan *internet banking*. Melalui layanan ini nasabah dapat melakukan transaksi perbankan seperti transfer dana, pembayaran, dan lain sebagainya. Penggunaan teknik dengan media internet umumnya dilakukan terhadap pengguna layanan keuangan. Untuk layanan-layanan tertentu yang tersedia dengan menggunakan media internet dibutuhkan

data-data pribadi dari pengguna. Sebagai contoh adalah untuk kegiatan bisnis sebutlah tranfser dana. Dengan adanya layanan secara *online* tentunya akan mempermudah nasabah dalam menjalankan transaksinya. Nasabah tidak perlu lagi harus datang ke bank hanya untuk melakukan transaksi transfer dana. Pada kesempatan inilah seorang *phisher* (pelaku *phishing*) menjalankan aksinya. Dengan membuat sebuah halaman web yang menyerupai dengan halaman web dari pihak perbankan, *phisher* menyamar dan berlaku layaknya pihak perbankan tersebut. Untuk melakukan proses transaksi tentunya membutuhkan data-data pribadi meliputi nomor rekening, nomor identitas, nomor kontak, dan lain sebagainya. Tentunya dengan tidak menaruh rasa curiga, nasabah memberikan data-data yang memang "dibutuhkan" tersebut. Dengan demikian, sang *phisher* telah mendapatkan "ikan" yang dicarinya. Secara tidak langsung, phisher telah memiliki data-data yang dibutuhkan untuk mengetahui keuntungan apa saja yang kira-kira bisa dia dapatkan dari sang korban.

Bahaya yang ditimbulkan dari tindak kriminal *phishing* ini tidak hanya merugikan secara teknologi saja tetapi juga dapat berdampak ke lingkungan sosial. Kerugian utama tentunya akan dialami oleh pihak perbankan karena dengan tindak kriminal tersebut selain menghilangkan aset dan kekayaan juga mengakibatkan kehilangan kepercayaan publik. Secara damapak sosial, tentunya tindak *phishing* ini sangat mempengaruhi terutama terkait dengan keamanan pribadi (privasi). Oleh karenanya, peningkatan keamanan data menjadi perhatian utama dalam menangani kasus ini.

PIN Block Attack

Serangan terhadap keamanan ATM saat ini salah satunya adalah "*Personal Identification Number* (PIN) *block*". Serangan ini mengakibatkan para nasabah tidak bisa menggunakan kartu ATM untuk melakukan transaksi melalui mesin ATM. Bentuk penyerangan PIN *block* dilakukan terhadap data PIN yang terenkripsi. Tentunya penyerangan ini dilakukan terhadap jaringan yang terhubung antara mesin ATM dengan jaringan perbankan. Para *hacker* menyerang *server* yang terhubung dalam jaringan dan mengambil blok-blok PIN yang terisi dengan data-data yang telah terenkripsi – data mengenai nomor kartu, nomor rekening, dan nomor PIN serta jumlah dana transaksi. Selain itu, para pencuri juga mencuri kunci yang digunakan untuk melakukan enkripsi data-data tersebut. Dengan demikian juga memungkinkan bagi para pencuri tersebut untuk membuka data-data tersebut sehingga mengetahui nomor-nomor penting salahsatunya adalah nomor PIN nasabah. Dengan mengetahui data-data tersebut maka para pencuri tersebut bisa saja membuat duplikat kartu-kartu ATM dan melakukan penarikan tunai dari mesin-mesin ATM yang tersedia.

Pada jaringan ATM digunakan blok 64-bit untuk melakukan enkripsi terhadap PIN untuk melakukan proses transaksi dan menjamin keamanan dalam jaringan perbankan yang digunakan. Jaringan perbankan yang luas haruslah menjamin keamanan pengiriman data. Dikarenakan dalam perjalanan di dalam jaringan data tersebut harus melewati simpul-simpul (*nodes*) jaringan yang berbeda-beda maka data tersebut akan mengalami proses enkripsi dan pengaturan yang berulang-ulang dan hal ini memicu adanya celah keamanan terhadap data-data tersebut.

Kesimpulan

Dari hasil studi literatur mengenai sistem keamanan pada ATM (*Automated Teller Machine* / Anjungan Tunai Mandiri) didapatkan bahwa untuk keamanan ATM masih menggunakan metode kriptografi *Triple* DES. Selain itu cukup banyak serangan yang dapat mengancam keamanan pada ATM. Tentunya dalam menangani serangan tersebut merupakan tanggung ajwab bersama dari pihak perbankan maupun para nasabah. Untuk peningkatan keamanan data dalam jaringan perbankan dibutuhkan pengembangan dan penelitian lebih lanjut khususnya dalam bidang kriptografi sebagai salah satu cabang ilmu yang memperdalam bidang pengamanan data digital.

Daftar Referensi

APACS. *Card Fraud: the facts 2002*. United Kingdom. 2002

Bond, Michael. *Understanding Security APIs*. University of Cambridge. 2004.

Bond, Mike dan Piotr Zielinski. *Decimalisation Table Attacks for PIN Cracking*. University of Cambridge. 2003.

Istnick, Anna C. dan Emilio Caligaris. *ATM Fraud and Security*. DIEBOLD. Amerika Serikat. 2003.

Litan, Avivah. *Criminals Exploit Consumer Bank Account and ATM System Weaknesses*. Gartner. 2005.

Steel, Graham. *Formal Analysis of PIN Block Attacks*. University of Edinburgh. Scotland. 2006.

Vellani, Karim H. dan Mark Batterson. *Security Solutions for ATM*. Threat Analysis Group. 2003.