ATTACK AND OPTIMIZING SECURITY MANAGEMENT ON ATM MACHINES USING DES (Data Encryption Standard)

Abstrak

This paper aims to describe the attack and optimization of security management on ATM machines using the DES (Data Encryption Standard) method.

ATM is a device that is often used by many people and almost all people who have savings in the bank. Then needed adequate and guaranteed security so that users are comfortable using it. The security used in securing data access privacy on ATM machines is the Data Encryption Standard (DES) method.

DES is a standard in cryptographic systems with the type and mode of the symmetry algorithm. self-protection and resilience for the ATM system is very important and fundamental, then the effectiveness of the DES method is very important.

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)[1]. Awalnya ATM disediakan untuk memudahkan layanan pengambilan uang dari tabungan nasabah, namun seiring dengan perkembangan teknologi dan kebutuhan akan peningkatan layanan kepada para nasabah, maka 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 yang digunakan pada ATM merupakan suatu bentuk jaringan komputer yang tersebar saling menyebar.[2]

Adanya proses transaksi (komunikasi) antarkomputer yang melalui sebuah jaringan yang luas, oleh sebab itu keamanan merupakan isu yang perlu diperhatikan secara khusus. Hal ini tentunya proses transaksi lebih terjamin dan dapat terjadi dengan baik dan benar.

Teknik pengamanan yang digunakan yaitu 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)[1]. 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).

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.[3]

ISI

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 decimal 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 pengguna.

Serangan Pada Keamanan ATM

Penggunaan teknik enkripsi (kriptografi) tidak selalu menjamin seratus persen pada sistem keamanan ATM[4]. 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

- 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. 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.

- 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.
  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.

- 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.

- 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. [5]

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.

REFERENSI

[1] R. Sambiangga, “Sistem Keamanan ATM (Automated Teller Machine / Anjungan Tunai Mandiri),” *Tek. Inform. Sekol. Tek. Elektro dan Inform. Inst. Teknol. Bandung Jalan Ganesha No. 10, Bandung 40132 Indones.*, pp. 1–10, 2014.

[2] N. A. P, K. Y. F, G. V. D, K. Y. V, and S. A. V, “Aggregation Process for Implementation of Application Security Management Based on Risk Assessment,” pp. 98–101, 2018.

[3] T. Wang and Y. Chen, “IPDAC : An Integrated IP Address Management Framework for Telecommunication Management Networks,” *2019 20th Asia-Pacific Netw. Oper. Manag. Symp.*, pp. 1–4, 2019.

[4] C. Porretti, D. Kolev, and R. Lahaije, “The Security Management Platform,” 2016, doi: 10.1109/ARES.2016.50.

[5] L. Slipachuk, “The Process of the Critical Infrastructure Cyber Security Management using the Integrated System of the National Cyber Security Sector Management in Ukraine,” *2019 3rd Int. Conf. Adv. Inf. Commun. Technol.*, pp. 451–454, 2019.