Peningkatan Keamanan Kunci Enkripsi Menggunakan Perubahan Kunci Berkala dan Akses Ganda

Christian (13207033)
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
qruz_tyan@students.itb.ac.id

***Abstrak*—Kombinasi penggunaan kunci publik dan kunci simetri di dalam pengamanan data atau informasi sudah menjadi aplikasi umum di dalam sistem pengamanan umum terhadap suatu aset atau suatu informasi dan fasilitas. Akan tetapi, tingkat keamanan ini hanya bertumpu pada algoritma enkripsi kunci simetri dan kunci publik yang digunakan beserta dengan kerumitan kunci publik dan kunci simetri yang digunakan itu sendiri. Semakin besarnya kapasitas *processing* dari CPU yang terus dikembangkan di dalam industri perancangan IC digital membuat serangan atau pemecahan kerahasiaan kunci dan algoritma yang digunakan pun tidak membutuhkan waktu yang lama sebagaimana kebutuhan waktu yang ekivalen untuk pemecahan kunci dan algoritma menggunakan kapasitas *processing* yang lebih rendah. Dengan adanya perubahan kunci secara berkala pada sistem yang disinkronisasi terhadap pengguna akan meningkatkan keamanan kunci dan data atau informasi yang dirahasiakan melalui algoritma dan kunci enkripsi tersebut dengan jalan membatasi rentang waktu keberlakuan suatu kunci terhadap suatu algoritma tertentu.**

***Index Terms*—Kunci Sinkronisasi, Kunci Publik, Kunci Simetri**

I. Latar Belakang

Di dalam perkembangan teknologi pengamanan dan autentifikasi identitas untuk akses suatu data atau fasilitas, semakin banyak usaha serangan terhadap keamanan kunci menggunakan berbagai macam peralatan berbasis algoritma pemecahan (dekripsi) kunci untuk suatu identitas tertentu dengan tujuan membuka akses terhadap data atau fasilitas yang diinginkan tersebut. Tentunya hal ini tergolong sedikit atau cenderung langka karena teknologi yang dibutuhkan merupakan teknologi intelijen sehingga jumlah serangan yang dapat terjadi pun sedikit. Akan tetapi, di dalam dunia intelijen internasional, hal ini sudah menjadi umum seiring dengan penggunaannya juga yang tidak terbatas pada suatu negara atau suatu fasilitas tertentu. Adapun teknologi yang digunakan di dalam pemecahan suatu kode atau kunci melibatkan algoritma-algoritma tertentu yang membutuhkan waktu dekripsi dalam rentang yang tidak pasti. Kondisi ini dapat menjadi suatu celah tersendiri untuk peningkatan keamanan data atau fasilitas yang diserang tersebut, yakni dengan membatasi keberlakuan kunci sesi atau masa aktif suatu kunci.

Adapun metode-metode pengamanan yang telah ada saat ini menerapkan tingkat kerumitan algoritma yang tinggi beserta dengan probabilitas kunci yang sangat besar untuk enkripsi data atau informasi yang bersifat rahasia. Akan tetapi, terpusatnya metode akses data atau informasi tersebut pada satu metode saja merupakan kelemahan tersendiri di dalam tingkat keamanannya karena kriptanalis akan terpusat pada satu metode tersebut dalam konteks homogenitas metode yang ada untuk setiap pihak yang memiliki akses terhadap sistem tersebut. Di sisi lain, dengan adanya pembedaan metode akses untuk pihak yang berbeda akan menjadi kekuatan di dalam sistem karena kriptanalis tidak memiliki pembanding yang banyak untuk setiap metode yang diserang olehnya.

II. Rumusan Masalah

Di dalam topik ini, penulis membagi permasalahan yang ada ke dalam beberapa hal utama, yakni:

- Bagaimana mengatur pergantian kunci untuk pembatasan masa aktif suatu kunci?
- Bagaimana menerapkan pergantian kunci ini di dalam mekanisme fisisnya?
- Apa kelemahan dan kelebihan dari sistem pembatasan masa aktif suatu kunci dengan pergantian kunci inis?

III. Metode Penelitian

Di dalam penyusunan makalah ini, penulis sepenuhnya melakukan studi literatur mengenai keamanan informasi dan manajemen kunci publik dan kunci simetri di dalam aplikasi terhadap fungsi sehari-hari yang ada di masyarakat umum dengan landasan kemungkinan adanya ekivalensi penggunaan metode yang sama untuk sistem keamanan rahasia.

IV. Sumber Data

Sumber kajian data yang penulis gunakan sepenuhnya berasal dari kajian literatur elektronik yang membahas manajemen kunci, baik kunci simetri maupun kunci

publik, beserta dengan sertifikasi suatu data.

V. TEORI DASAR

A. Kunci Sesi

Pada umumnya, kunci sesi sangat banyak dipakai di dalam autentifikasi fasilitas atau data-data yang bersifat rahasia dengan membatasi keberlakuan kunci yang digunakan pada sesi pengguna mengakses data atau fasilitas tersebut saja sehingga ketika pengguna akan mengakhiri sesi aktifnya saat itu, mesin atau komputer yang digunakan akan secara otomatis melakukan pergantian kunci yang disinkronisasikan dengan kunci akses pengguna dan sistem. Dengan demikian ketika pengguna akan melakukan akses kembali terhadap data atau fasilitas yang sama, sistem akan mendeteksi kunci yang berbeda yang digunakan pada pengaksesan data atau fasilitas tersebut. Hal ini diterapkan untuk peningkatan keamanan kunci yang digunakan tersebut. Akan tetapi, sistem ini memiliki kelemahan-kelemahan signifikan. Pada umumnya, sistem ini sudah dipakai di dalam pengamanan kunci atau PIN akses rekening bank di dalam mesin-mesin ATM (*Auto Teller Machine*). Sudah sangat banyak pencurian uang melalui pengaksesan kunci sesi dengan cara penggandaan kartu ATM yang telah digunakan secara tidak langsung. Hal ini dilakukan dengan perekaman fisis kartu yang telah digunakan sebelumnya pada mesin ATM yang telah digunakan ke dalam mesin lalu dimasukkan kartu yang masih kosong atau belum terkonfigurasi ke dalam mesin ATM yang sama sehingga kartu sebelumnya akan terduplikasi ke dalma kartu yang baru tersebut dan secara otomatis kartu yang baru tersebut akan memiliki kunci sesi yang baru yang telah dibuat oleh sistem bagi kartu ATM yang telah digunakan sebelumnya. Kondisi ini membuat pihak pengganda akan memiliki akses penuh terhadap rekening korban menggunakan kunci sesi yang didapatnya, sekalipun tentu saja, masih juga dibutuhkan PIN.

Kunci sesi pada dasarnya merupakan kunci simetri yang dimiliki oleh sistem dan pengguna. Kunci ini kemudian dienkripsi lagi menggunakan kunci publik. Kunci sesi digunakan umumnya untuk mengamankan suatu informasi atau pesan dengan metode Diffie-Hellman untuk transmisi kunci di dalam komunikasi antara sistem dengan pengguna atau dua pihak yang akan sama-sama menggunakan kunci sesi tersebut. Kunci ini kemudian akan dienkripsi menggunakan kunci publik yang akan mempersulit serangan terhadap kunci ini karena panjang kunci hasil enkripsi yang terbatas membuat kriptanalisis semakin sukar dilakukan.

B. Manajemen Kunci

Manajemen kunci perlu dilakukan mengacu pada prinsip penggunaan kunci yang harus terbatas atau memiliki daur hidup yang terbatas sehingga keamanan data yang dienkripsi menggunakan kunci tersebut pun semakin terjamin. Secara umum, daur hidup kunci terdiri dari:

- Pembangkitan kunci, yakni pembentukan kunci melalui algoritma tertentu atau secara manual oleh pengguna;
- Distribusi kunci, yakni fase pembagian kunci kepada pihak-pihak yang akan turut menggunakan kunci yang sama tersebut melalui protokol kriptografi tertentu;
- Penyimpanan kunci, yakni fase pengamanan kunci di dalam suatu media penyimpanan yang aman beserta dengan pengamanan tambahan di dalam media tersebut dengan menggunakan algoritma tertentu untuk memecah kunci atau mengambil nilai tertentu dari kunci secara acak;
- Penggunaan kunci, yakni penetapan suatu identitas tertentu pada kunci yang menjadi tanda dari fungsi penggunaan kunci tersebut atau klasifikasi kunci tersebut di dalam sistem yang menggunakan hirarki kunci;
- Perubahan kunci, yakni fase pengubahan kunci di dalam daur hidupnya untuk membatasi keberlakuannya untuk mencegah terjadinya *exhaustive search* dalam rentang waktu panjang atau lebih lama daripada masa aktif kunci yang bersangkutan;
- Penghancuran kunci, yakni fase pemusnahan kunci yang telah digunakan untuk kemudian diganti dengan kunci yang baru pada fase pembangkitan kunci berikutnya.

VI. PERANCANGAN DAN IMPLEMENTASI

A. Sistem Manajemen Kunci Berkala

Pada dasarnya sudah sangat banyak aplikasi manajemen kunci di dalam implementasi nyata, seperti pada pengamanan *account* bank menggunakan kartu ATM yang membutuhkan PIN sebagai kode aksesnya. Akan tetapi, daur hidup kunci yang digunakan terbatas pada periode pengaksesan ATM oleh pengguna di mesin ATM atau periode terjadinya akses data pengguna menggunakan kartu ATM pengguna tersebut. Apabila pengguna tidak mengakses ATM dalam jangka waktu panjang, kriptanalis pun memiliki waktu yang panjang juga untuk melakukan kriptanalisis dan memecahkan kunci untuk pengaksesan *account* pengguna yang diserang.

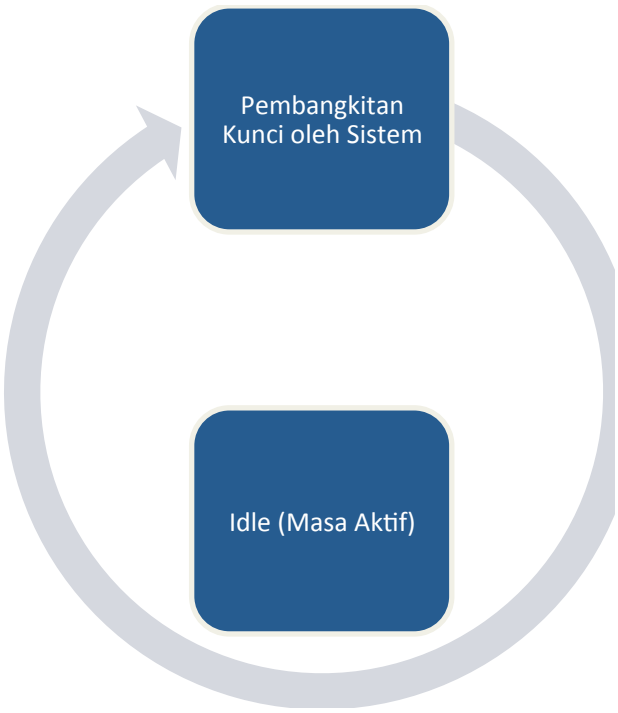
Kelemahan ini dapat ditangani dengan membatasi masa aktif kunci yang bersangkutan bukan pada periode pengaksesan *account* itu oelh kartu pengguna, tetapi berdasarkan pada rentang waktu yang berjalan sehingga dibutuhkan kunci yang berbeda-beda per periode masa aktif kunci tersebut untuk mengakses *account* pengguna. Adapun kunci yang dimaksud merupakan kunci simetri yang dibangkitkan oleh sistem. Prinsip ini sangat berguna untuk diaplikasikan pada pengamanan *account* bank melalui akses kartu ATM dan kunci akses suatu ruangan menggunakan kartu akses tertentu karena umumnya

serangan terhadap akses terhadap suatu ruangan atau fasilitas berkaitan erat dengan aset atau perihal penting di dalam fasilitas atau ruangan tersebut sehingga serangan harus dilakukan terhadap sistem atau terhadap mesin akses di lokasi yang menjadi tempat ruangan atau fasilitas itu terletak.

Di dalam metode ini, pihak yang memiliki hak akses dibagi ke dalam dua kelompok, yakni administrator utama dan pihak-pihak yang diberi hak khusus untuk pengaksesan sistem yang dituju.

Pengamanan kunci sesi utama yang merupakan kunci simetri utama terdiri dari tiga tingkat pemakaian kunci, yakni kunci sesi menggunakan kunci simetri, kunci privat untuk enkripsi kunci sesi, dan kunci pribadi pengguna yang menjadi kunci algoritma pengacakan kunci privat sebelumnya. Perubahan yang dilakukan oleh sistem yaitu pembangkitan kunci simetri secara berkesinambungan per satuan waktu yang dispesifikasikan terhadap sistem tersebut. Sistem secara keseluruhan dapat digambarkan sebagai berikut.

Gambar 6-1 Diagram proses pengamanan kunci di dalam sistem per satuan waktu tetap



Gambar 6-2 Diagram daur hidup kunci yang dibangkitkan sistem

Dengan demikian, maka sistem akan secara berkesinambungan membangkitkan kunci simetri baru di setiap satuan waktunya. Karena pengamanan ini melibatkan bukan hanya kunci privat untuk melakukan dekripsi kunci simetri utama, maka parameter waktu pun ikut dienkripsi bersamaan dengan kunci simetri utama menggunakan kunci publik oleh sistem dengan parameter waktu terlebih dahulu dienkripsi menggunakan kunci sinkronisasi dari algoritma Diffie-Hellman di dalam sistem yang langsung disinkronisasi dengan kartu pengguna.

Secara keseluruhan, ketika pengguna melakukan akses pada mesin autentifikasi fasilitas atau ruangan menggunakan kartu aksesnya, pengguna harus memasukkan PIN atau kunci pribadinya untuk mendekripsi kunci privat pada kartu. Setelah itu, kunci privat ini akan digunakan untuk mendekripsi kunci simetri atau kunci sesi utama dan kunci sinkronisasi pada kartu. Kunci sinkronisasi ini kemudian akan diuji kesamaannya dengan kunci sinkronisasi pada sistem sesuai dengan identitas pengguna yang ditangkap oleh sistem melalui kunci pribadi di awal input, yakni PIN pengguna.

Gambar 6-3 Diagram proses di dalam sistem ketika *user* melakukan akses melalui kartu akses

Tentu saja pengecekan kunci sesi terhadap catatan waktu membutuhkan adanya *database* secara khusus yang menyimpan *record* seluruh kunci dan data waktu akses oleh pengguna. Ini bertentangan dengan pentingnya penghapusan kunci yang telah habis masa aktifnya sehingga dibutuhkan pengujian atau pengecekan waktu dan kunci sesi dalam metode lain.

Berkenaan dengan hal tersebut, dapat digunakan algoritma Diffie-Hellman untuk pembangkitan sebuah

kunci untuk enkripsi catatan waktu di pihak sistem dan di kartu pengguna. Proses ini pun terjadi pada saat pengaksesan fasilitas, ruangan, atau sistem oleh pengguna melalui kartu aksesnya. Kunci inilah yang dimaksud di dalam kunci sinkronisasi di dalam gambar 6-3.

Di pihak sistem utama, algoritma pembangkitan kunci sesi harus melibatkan parameter waktu proses ketika pembangkitan itu dilaksanakan. Hal ini dimaksudkan untuk meningkatkan kompleksitas algoritma sehingga nilai saat itu akan bergantung pada nilai di satuan waktu sebelumnya.

Pada dasarnya kekuatan utama mekanisme dan manajemen kunci di dalam metode ini bukan terletak pada pemakaian kartu akses untuk pengaksesan sistem utama, melainkan pada mekanisme akses fasilitas atau ruangan yang dituju di dalam sistem tersebut yang terdiri dari dua metode, yakni penggunaan kartu dan akses secara langsung di lokasi. Di dalam akses langsung di lokasi, hanya dibutuhkan kunci sesi sebagai input tunggal terhadap sistem. Kunci inilah yang berubah-ubah terhadap waktu dan pengaksesan metode ini hanya dapat dilakukan oleh administrator utama.

B. Spesifikasi Sistem dan Perangkat

Dengan metode pengamanan seperti ini, dibutuhkan perangkat keras yang mendukung, yakni *processor* dengan kecepatan tinggi, yakni *processor* yang kuat untuk memroses ketiga tahapan pengujian kunci akses pada kartu dengan cepat. Selain itu, Alat pembaca kartu yang menerapkan metode *scanning* kartu secara statik, yakni dengan kartu diletakkan pada mesin tersebut, bukan melalui penggesekan kartu sebagaimana diterapkan pada mesin gesek kartu. Hal ini dikarenakan sistem harus melakukan pengujian secara berbalasan antara mesin *scanning* yang terhubung pada sistem pusat dengan kartu akses yang diperiksa oleh sistem dalam beberapa tahap proses. Selain mesin *scanning* kartu, dibutuhkan juga *keypad* numerik atau alfabetis untuk menjadi media input kunci pribadi pengguna sesuai kartu aksesnya (atau PIN).

C. Kelemahan dan Kelebihan

Metode manajemen kunci demikian memiliki beberapa kelemahan dan kelebihan yang memegang peranan kuat. Jika ditinjau dari fungsionalitas metode ini, implementasi nyata hanya terbatas pada beberapa aplikasi saja, yakni aplikasi-aplikasi sistem yang menggunakan suatu sistem utama dengan kartu akses untuk setiap penggunanya. Metode manajemen kunci ini tidak dapat digunakan pada aplikasi perangkat lunak yang hanya membutuhkan *password* atau kata kunci rahasia tertentu untuk pengaksesan data atau informasi di dalamnya karena metode ini melibatkan dua tempat penyimpanan data, yakni sistem itu sendiri dan kartu akses yang dimiliki oleh pengguna. Selain itu, metode ini pun tidak dapat dipergunakan untuk sistem yang tidak *online* setiap saatnya, yakni sistem yang hanya aktif pada saat pengaksesan atau sistem yang memiliki periode keaktifannya terbatas. Hal ini dikarenakan algoritma pembangkitan kunci sesi melibatkan parameter waktu pembangkitan tersebut.

Di samping kelemahan dari sistem ini yang memegang peranan di dalam implementasi metode ini, metode ini memiliki keunggulan yang cukup signifikan, yakni metode pengaksesan langsung yang terbatas hanya pada administrator yang mengetahui perubahan kunci sesinya saja. Hal ini sejalan dengan banyaknya kasus serangan kriptanalis terhadap sistem pengaksesan menggunakan kode akses di lokasi peralatan pengaksesan tersebut. Dengan adanya perubahan kunci secara terus-menerus tersebut maka kriptanalis hanya memiliki waktu pemecahan kode sesi yang berlaku di rentang waktu keberlakuan kunci sesi tersebut saja. Inilah yang menjadi keunggulan utamanya, karena pembangkitan kunci dapat diatur untuk berada di rentang waktu yang sempit sehingga setiap usaha penyerangan akan berbenturan dengan kondisi adanya perubahan kunci secara terus menerus di saat usaha penyerangan dilakukan. Hal ini juga sejalan tingkat kerumitan algoritma yang diterapkan pada sistem untuk pengaksesan melalui kartu akses oleh pengguna. Penyerangan kriptanalis dengan menggunakan akses kartu harus melalui tiga tahap analisis, yakni penentuan kunci pribadi (PIN) pengguna yang berbeda-beda untuk setiap kartunya sekalipun satu tujuan pengaksesan yang digunakan untuk mendekripsi kunci privat yang akan digunakan berikutnya, kunci privat yang akan digunakan untuk dekripsi kunci sesi yang adalah kunci simetri utama untuk akses yang diinginkan, dan kriptanalisis untuk kunci sinkronisasi yang selaras dengan karakteristik unik dari kunci pribadi pertama, yakni kunci yang sepenuhnya hanya diketahui oleh pengguna kartu spesifik.

IV. KESIMPULAN

Keamanan akses suatu sistem, fasilitas, atau ruangan bertumpu pada kunci akses terhadap sistem tersebut yang juga bergantung pada tingkat kerumitan algoritma enkripsi informasi pengaksesan sistem atau fasilitas tersebut. Peningkatan keamanan terhadap sistem yang bersangkutan dapat dilakukan dengan penggandaan metode akses sistem untuk perbedaan pihak-pihak yang mengaksesnya untuk mempersempit ruang lingkup analisis oleh kriptanalis di dalam penyerangan kriptografinya dan perubahan kunci akses sistem secara berkala per satuan waktu sehingga diharapkan kunci akan sudah berubah sebelum kriptanalisis di dalam penyerangan kriptografi berhasil dilakukan terhadap sistem ini. Hal ini dapat diperkuat dengan penerapan hirarki kunci untuk menambah kerumitan sistem secara keseluruhan dalam rangka mencegah keberhasilan serangan oleh kriptanalis di dalam waktu yang sangat singkat tersebut.

REFERENCES

[1] http://en.wikipedia.org/wiki/Symmetric_key_management, "Symmetric Key Management", diakses tanggal 7 Mei 2011.

[2] http://en.wikipedia.org/wiki/Key_management, "Key Management", diakses tanggal 7 Mei 2011.

[3] http://en.wikipedia.org/wiki/Public_key_certificate, "Public Key Certificate", diakses tanggal 7 Mei 2011.

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 11 Mei 2011

Christian (13207033)