ANALISIS DAN IMPLEMENTASI KRIPTOSISTEM HIBRID UNTUK PENGAMANAN FAT FILE SYSTEM DI TINGKAT WINDOWS DRIVER

Alexander R Sirait[1], Maman Abdurohman[2], Dr. Mochammad Zuliansyah[3]

[1]Teknik Informatika, Fakultas Teknik Informatika, Universitas Telkom

Abstrak

Pengamanan data dalam sistem komputer memerlukan adanya usaha menjaga kerahasiaan dan keamanan data. Salah satu cara menjaga kerahasiaan data adalah dengan menggunakan kriptografi yang bertujuan untuk menghindari penggunaan data oleh pihak yang tidak berhak. FAT merupakan file system yang paling sering digunakan di sistem operasi Windows dan dapat diakses di berbagai platform lainnya. Di tingkat driver Windows, dapat ditambahkan lapisan untuk mengamankan data di media fisik secara background (transparan). Lapisan ini diimplementasikan sebagai non- plug & play device driver pada Windows.
Alasan pemilihan kriptosistem hibrid ditujukan untuk pengamanan data yang [cukup] kuat dan mempermudah key-management sehingga tidak merepotkan berbagai user dalam mengamankan data masing-masing. Kriptosistem hibrid ini terdiri dari asymmetric cryptograph menggunakan algoritma RSA, dan symmetric cryptograph menggunakan algoritma RC6. Panjang key dapat disesuaikan dengan kemampuan/spesifikasi hardware sistem komputer yang digunakan. Penyesuaian ini dilakukan agar pengamanan data yang terjadi secara transparan tidak menimbulkan penurunan kinerja sistem yang signifikan.

Kata Kunci : windows driver, kriptosistem hibrid, RC6, RSA, FAT file system

Abstract

Data storage on computer system needs an effort to keep data secrecy and safety. One of the alternatives is to secure data using cryptography. Cryptography is a discipline that studies about how to keep a data secretly to avoid unauthorized access. FAT file system is very often used in Windows operating-system and can be accessed across many other platforms. At Windows driver level, one layer can be added to secure data on physical media transparently (background-operated). This layer is implemented as non- plug & play device driver on Windows platform.
The reason of using hybrid cryptosystem is to ensure powerful [enough] data security and simplify key-management so that users will conveniently secure their respective data. This hybrid cryptosystem consists of asymmetric cryptograph with RSA algorithm, and symmetric cryptograph with RC6 algorithm. Key length can be adjusted to measure up to computer hardware specification. This adjustment is needed to maintain seamlessly (less user awareness) data encryption/decryption and avoid significant computer performance degradation.

Keywords : windows driver, hybrid cryptosystem, RC6, RSA, FAT file system

1. Pendahuluan

1.1 Latar belakang

Berbagai macam cara dan alternatif telah dikembangkan untuk menangani masalah keamanan dan kerahasiaan data. Salah satunya adalah kriptografi. Dengan menggunakan kriptografi, data asli (*plaintext*) akan diubah ke dalam bentuk data sandi (*ciphertext*), kemudian data sandi tersebut dapat dikembalikan ke bentuk data asli hanya bisa dengan menggunakan kunci (*key*) tertentu yang hanya dimiliki oleh pihak yang sah. Tentunya hal ini menyebabkan pihak lain yang tidak memiliki kunci tidak dapat mengerti data yang sebenarnya sehingga kerahasiaan data dapat terjaga.

Pengguna komputer pada umumnya melupakan [atau tidak tahu] melakukan pengamanan data di dalam komputernya. Hal ini dapat disebabkan oleh cukup sulitnya menentukan kunci dengan panjang tertentu yang beragam untuk berbagai jenis data (*file*) yang dimiliki, dan juga oleh karena [kemalasan] user harus berinteraksi dengan sebuah aplikasi pengamanan data setiap kali melakukan enkripsi/dekripsi. Otomasi pengamanan data secara transparan dapat menjadi solusi untuk mempermudah pengamanan data di media penyimpanan kapasitas besar (*mass storage media*).

Ada dua skema penggunaan kunci di dalam kriptografi. Skema pertama adalah *asymmetric cryptography*, yaitu menggunakan dua buah kunci berbeda. Salah satu kunci disebut *public key* dan yang lainnya adalah *private key*. *Public key* digunakan pada proses enkripsi dan dapat diketahui oleh pihak-pihak yang memerlukan (tidak dirahasiakan). *Private key* digunakan pada proses dekripsi dan hanya diketahui oleh pihak tertentu (dirahasiakan). Skema kedua adalah *symmetric cryptography*, yaitu menggunakan satu kunci rahasia. *Secret key* yang sama akan digunakan pada proses enkripsi dan proses dekripsi, dan isi kunci harus dirahasiakan. Saat ini telah banyak terdapat berbagai algoritma kriptografi untuk *Asymmetric Cryptosystem* dan *Symmetric Cryptosystem*. Kriptosistem adalah sistem yang menggunakan suatu algoritma kriptografi untuk mentransformasikan plaintext menjadi ciphertext menggunakan kunci-kunci (*keys*) tertentu dalam suatu fungsionalitas terpadu dalam rangka pengamanan data. Pada Tugas Akhir ini, algoritma yang digunakan untuk *asymmetric cryptosystem* adalah algoritma RSA dan untuk *symmetric cryptosystem* adalah algoritma RC6. Pengamanan data menggunakan *symmetric cryptosystem*, dan pengamanan *key* menggunakan *asymmetric cryptosystem*. Kriptosistem hibrid (kombinasi dua kriptosistem) ini diharapkan dapat memberikan pengamanan data sekaligus mempermudah *key-management*.

1.2 Perumusan masalah

Pada Tugas Akhir ini, terdapat beberapa masalah yang dirumuskan sebagai berikut:

1. Bagaimana mengimplementasikan kriptosistem hibrid pada tingkat *driver* Windows untuk mengamankan data secara transparan (tidak disadari oleh user).
2. Bagaimana mengoptimalkan implementasi (baik di tingkat *driver* maupun di aplikasi GUI) supaya pengamanan data berlangsung [cukup] cepat, tanpa mengalami penurunan kinerja sistem komputer yang signifikan.
3. Bagaimana menguji fungsi *hybrid cryptosystem* ditinjau dari kemampuan driver melakukan pengamanan data, efisiensi *key-management*, dan kinerja komputer ketika digunakan oleh beberapa aplikasi pada saat yang bersamaan.

1.3 Tujuan

Berdasarkan rumusan masalah di atas, maka tujuan dari Tugas Akhir yang diharapkan adalah sebagai berikut:

1. Melakukan implementasi di tingkat *driver* pada sistem operasi Windows versi 5 untuk menerapkan kriptosistem hibrid.
2. Melakukan optimalisasi perangkat lunak untuk memperoleh pengamanan data yang dapat berjalan [cukup] cepat di berbagai spesifikasi *hardware* PC.
3. Melakukan pengujian pengamanan data dari kriptosistem hibrid, serta pemilihan panjang *key* yang efisien guna menghindari penurunan kinerja komputer yang signifikan.

1.4 Batasan Masalah

Batasan masalah pada Tugas Akhir ini adalah sebagai berikut :

1. Spesifikasi *hardware* setidaknya prosesor 1 GHz, RAM 128 MB, *harddisk* 4200 rpm tanpa *bad sector*, usb 2.0 *hi-speed media storage*. Spesifikasi sistem operasi setidaknya Windows XP *service pack* 2 dengan semua *device driver* terinstall dengan baik.
2. Tidak mempermasalahkan penggunaan bersama aplikasi lain yang memakai *disk-access/file-filter driver* tertentu, misal aplikasi *antithreat*, aplikasi *backup*, DBMS dan sebagainya, berhubungan masalah kompabilitas.
3. *Drive* instalasi sistem operasi (*host drive*, biasanya *drive* C) dipisahkan dari *drive* lain yang akan diamankan datanya, sehingga tidak mengamankan data pada *host drive*.
4. Default *storage format* adalah *FAT file system* (FAT12, FAT16, FAT32).
5. Tidak membahas *fault-tolerance* pengamanan data terhadap kondisi seperti *hardware failure*, *power lost*, *threat attack*, *accident/disaster*, *misuse*, dan lain-lain.

1.5 Metodologi Penyelesaian Masalah

Metode yang digunakan dalam penyelesaian Tugas Akhir adalah menggunakan metode studi pustaka atau studi literatur, dan analisis dengan langkah kerja sebagai berikut :

1. Studi Literatur :
   a. Pencarian referensi

Mencari referensi dan sumber-sumber lain berhubungan dengan algoritma RC6, algoritma RSA, *key-management*, arsitektur *Windows driver*, *FAT file system*, dan optimalisasi sistem.

b. Pendalaman materi
Mempelajari dan memahami materi yang berhubungan dengan konsep *hybrid cryptosystem* dan *key-management*.

2. Melakukan analisis terhadap referensi-referensi yang diperoleh guna mendefinisikan masalah dan penyelesaian masalah yang tepat.
3. Melakukan perancangan perangkat lunak berdasarkan analisis sebelumnya untuk mendapatkan fungsionalitas-fungsionalitas yang bisa menyelesaikan masalah.
4. Implementasi dan optimalisasi perangkat lunak guna menerapkan kriptosistem hibrid pada *FAT file system* yang meliputi:
   a. Perencanaan
   Pada tahapan ini dilakukan untuk melakukan analisis tentang struktur *FAT file system* dan pemodelan *Windows driver*.
   b. Analisis
   Pada tahapan ini dilakukan untuk menentukan batasan dan kemampuan fungsionalitas perangkat lunak yang perlu diimplementasikan.
   c. Perancangan
   Pada tahapan ini dijelaskan mengenai rancangan gambaran umum *Windows driver* dan aplikasi GUI yang kompatibel terhadap berbagai macam spesifikasi komputer.
   d. Implementasi
   Mengimplementasikan perangkat lunak yang telah dirancang sebelumnya dan melakukan optimalisasi lebih lanjut.
   e. Testing
   Melakukan pengetesan perangkat lunak yang dibuat, dengan konfigurasi yang berbeda-beda.
5. Melakukan pengujian terhadap skenario pengamanan data pada kriptosistem hibrid, serta analisis kinerja komputer dan efisiensi panjang *key* ketika melakukan pengamanan data.
6. Penyusunan laporan dalam bentuk tertulis sebagai buku Tugas Akhir.

1.6 Sistematika Penulisan

Tugas Akhir ini disusun dengan sistematika sebagai berikut :

BAB I PENDAHULUAN
Bab ini meliputi latar belakang, perumusan masalah, tujuan, batasan masalah, metodologi penyelesaian masalah, serta sistematika penulisan.

BAB II DASAR TEORI
Bab ini memuat berbagai dasar teori yang mendukung dan mendasari materi Tugas Akhir ini.

BAB III ANALISIS KEBUTUHAN DAN PERANCANGAN SISTEM

Bab ini memuat tentang analisis kebutuhan dan perancangan perangkat lunak sebagai alat bantu dalam proses penyelesaian masalah.

BAB IV IMPLEMENTASI DAN PENGUJIAN SISTEM

Bab ini memuat tentang pengujian terhadap skenario pengamanan data, serta analisis kinerja dan panjang *key*.

BAB V KESIMPULAN DAN SARAN

Bab ini berisi kesimpulan-kesimpulan dari Tugas Akhir serta saran-saran untuk pengembangan selanjutnya.

5. Kesimpulan dan Saran

5.1 Kesimpulan

1. Implementasi di tingkat *driver* sudah berhasil dijalankan.
2. Perubahan panjang *key* RC6 [hampir] tidak memberikan perbedaan kinerja sehingga dikatakan sangat kecil pengaruhnya terhadap kinerja *driver* dalam mengerjakan fungsi enkripsi/dekripsi.
3. Panjang *key* RSA yang berbeda dapat menurunkan kinerja pada saat pembangkitan pasangan *key* RSA (semakin panjang *key* RSA semakin lama waktu pembangkitan *key*). Namun tidak berpengaruh terhadap kinerja *driver* dalam mengerjakan fungsi enkripsi/dekripsi.
4. Kinerja cipher RC6 jauh lebih baik daripada cipher RSA, sehingga tepat jika RSA hanya digunakan dalam *key-management* pada kriptosistem hibrid.
5. Panjang *key* RSA dapat disesuaikan dengan spesifikasi *hardware* user.
6. Aplikasi dan *driver* Windows yang dibuat pada Tugas Akhir ini dapat digunakan untuk pengamanan data yang belum tersedia pada *FAT file system*.

5.2 Saran

1. Penggabungan dua atau lebih algoritma simetris.
2. Penggunaan stream cipher.
3. Pengujian kriptanalisis terhadap kriptosistem hibrid.

Daftar Pustaka

[1] Alfan, Diki. "Enkripsi Data Dengan Algoritma Kriptografi Kunci Simetris". 2001

[2] Barreto, Paulo S. L. M., and Rijmen, Vincent. "The WHIRLPOOL Hashing Function". May 2003

[3] Dr. Dobbs Journal. "Developing Device Driver on Windows XP with Service Pack 2". March 2004

[4] James L. Massey, Gurgen H. Khachatrian, Melsik K. Kuregian. "Candidates Algorithm for the Advanced Encryption Standard (AES)". Cylink Corporation. June 1998

[5] Kurniawan, Yusuf Ir., MT. "Kriptografi. Keamanan Internet dan Jaringan Komunikasi". Bandung: Penerbit Informatika. 2004

[6] MSDN Professional. "Microsoft Windows NT Device Driver Kit (DDK)". Microsoft Publisher. 2004

[7] Microsoft Corp. "MSDN Journal 2004 DVD". Redmond. 2004

[8] Nasution, Hendrianto. "Algoritma Kriptografi Block Chiper CAST-256 untuk Penyandian Data". Bandung: STT Telkom. 2000

[9] NESSIE editors. "Performance of Optimized Implementations of the NESSIE Primitives". 2003

[10] PKCS editors, Public Key-based Cryptography Standards (PKCS#1 v2.1), RSA Security, Inc. 2002

[11] R.J.Anderson. "Robustness Principles for Public Key Protocols". Verlag. 2001

[12] RC6 Blockcipher, Primitive Specification & Supporting Documentation, RSA Security, Inc. 2000

[13] Russinovich Mark E., Solomon David A. " Microsoft Windows Internals, Fourth Edition: Microsoft Windows Server 2003, Windows XP, and Windows 2000". Microsoft Press. December 2004

[14] Schneier, Bruce. "Applied Cryptography 2nd Editon". New York: Addison-Wesley. 2001

[15] Stallings, William. "Cryptography and Network Security. Principles and Practice 2nd Edition". New Jersey: Prentice Hall. 1999

[16] Çetin Kaya Koç, High-Speed RSA Implementation, RSA Security, Inc.