Enkripsi Protocol Kerberos

Mochamad Reza Akbar
NIM : 13507131

Program Studi Teknik Informatika, Institut Teknologi Bandung
Jl. Ganesha 10, Bandung
e-mail: if17131@students.if.itb.ac.id

ABSTRAK

Internet merupakan tempat yang tidak aman. Banyak protokol-protokol yang digunakan di internet yang tidak menyediakan keamanan. Banyak alat yang digunakan hacker-hacker jahat yang mencoba menyadap password dalam jaringan. Dengan kata lain, aplikasi mengirimkan password yang tidak terenkripsi melalui jaringan yang sangat rentan. Lebih parah lagi, aplikasi client/server yang lain percaya bahwa program klien berlaku jujur terhadap identitas user yang sedang dipakainya.

Beberapa situs mencoba menggunakan firewall untuk mengatasi masalah keamanan jaringan mereka. Sayangnya, firewall memiliki asumsi bahwa "orang-orang jahat" berada di luar, yang seringkali merupakan asumsi yang sangat buruk. Kejadian-kejadia yang membahayakan sering terjadi dari dalam. Firewall juga memiliki kelemahan yang signifikan bahwa firewall membatasi pengguna dalam menggunakan internet.

Untuk mengatasi masalah-masalah keamanan jaringan tersebut maka MIT(Massachusetts Institute of Technology) membuat Kerberos. Protokol Kerberos menggunakan kriptografi yang kuat sehingga klien dapat membuktikan identitas dirinya ke server dan juga sebaliknya melalui koneksi jaringan yang tidak aman. Setelah klien dan server membuktikan identitasnya menggunakan Kerberos, masing-masing dapat melakukan enkripsi terhadap komunikasi-komunikasi yang dilakukan untuk memastikan pripasi dan integritas data.

Kerberos secara mudah dapat didapat secara bebas atau gratis dari MIT, dibawah persetujuan copyright sangat mirip dengan penggunaan operating system dan X window system yang didapat secara bebas. MIT menyediakan Kerberos dalam bentuk source sehingga setiap orang yang ingin menggunakan Kerberos dapat melihat langsung kode yang ada dan meyakinkan bahwa kode tersebut dapat dipercaya. Sebagai tambahan, kepada siapa yang lebih mementingkan untuk mempercayai produk yang professional. Kerberos juga hadit sebagai product dari berbagai macam vendor.

Makalah ini memberikan penjelasan singkat mengenai Kerberos dan menjelaskan penggunaan enkripsi untuk mencapai tujuannya.

Kata kunci: Kerberos, kriptografi, enkripsi, otentikasi, protokol.

1. PENDAHULUAN

Semakin berkembangnya jaringan computer, semakin banyak pula pengaksesan jaringan yang dilakukan. Namun, semakin, dengan demikian semakin umum dilakukan berbagai jenis serangan yang muncul untuk mencuri data dalam jaringan tang tingkat keamanannya rawan. Hal ini memicu dikembangkannya enkripsi yang kuat yang dipasang dalam sebuah protocol jaringan untuk menghindari berbagai jenis serangan.

Maka muncullah sebuah protokol yang bernama Kerberos. Kerberos adalah keamanan jaringan komputer yang merujuk kepada sebuah protokol otentikasi yang dikembangkan oleh Massachusetts Institute of technology (MIT).

Kerberos adalah protokol otentikasi jaringan yang menyediakan otentikasi yang kuat bagi aplikasi klien dan server dengan menggunakan kriptografi kunci rahasia. Protokol ini dibuat oleh MIT yang merupakan bagian dari proyek Athena pada pertengahan 1980an. Mandat proyek Athena adalah untuk mengekplorasi bermacam-macam cara komputasi dan membangun basis pengetahuan yang diperlukan untuk strategi keputusan untuk jangka yang panjang agar bagaimana komputer-komputer siap dipakai di kurikulum MIT.

Protokol ini dinamakan Kerberos. Kerberos merupakan anjing berkepala tiga yang menjaga gerbang menuju Hades dalam mitologi yunani. Dapat juga dinamakan Cerberus menurut mitologi romawi.

Protokol Kerberos menggunakan enkripsi kriptografi yang kuat, sehingga klien dapat membuktikan identitasnya ke server dan juga sebaliknya dalam koneksi jaringan yang tidak aman. Enkripsi kriptografi yang digunakan adalah enkripsi Data Encrytion Standard (DES).

Data Encryption Stantard (DES) adalah metode enkripsi data yang luas digunakan dengan menggunakan kunci private rahasia yang dipercaya sangat susah untuk dipecahkan. Terdapat sebanyak 72.000.000.000.000.000 (72×10^{15}) atau lebih kemungkinan kunci enkripsi yang mungkin dapat digunakan. Untuk setiap pesan yang diberikan, kunci didapat secara acak dari sekian banyak kemungkinan kunci angka. Seperti metode-metode kriptografi kunci pribadi yang lain, pengirim dan penerima pesan harus tahu dan menggunakan kunci pribadi yang sama.

DES dikembangkan oleh National Bureau of Standards dengan bantuan National Security Agency. Enkripsi ini sengaja dibuat untuk menyediakan metode standar untuk pengamanan pesan rahasia dan data yang dianggap rahasia. IBM menciptakan draf algoritma awal, yang dinamakan LUCIFER. DES secara resmi menjadi standar resmi pada November 1976.

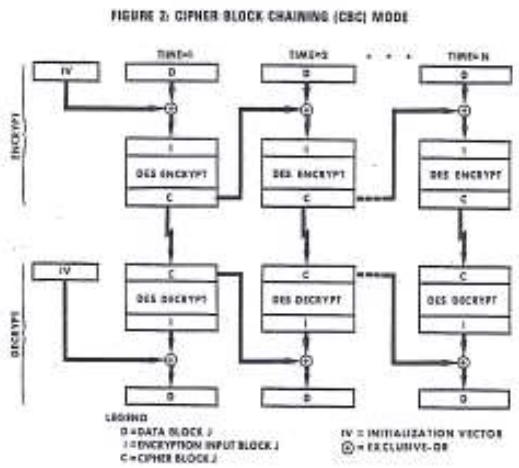
2. Protokol Kerberos Version 4

2.1 Enkripsi

Basis algoritma enkripsi yang digunakan di protokol Kerberos versi ini adalah Data Encryption Standard (DES) dari Intsitute of Standards and Technology (NIST). DES merupakan enkripsi blok cipher yang beroperasi menggunakan 64-bit blok.

Mode enkripsi standar yang digunakan DES adalah Electronic Code Book (ECB). Mode ECB adalah mode yang tidak digunakan dalam Kerberos, karena tidak efisien ketika digunakan dalam blok-blok data. Ketika terjadi pengulangan data yang dienkripsi dengan menggunakan ECB, maka penyadap akan dapat mengenali blok ciphertext yang identik. Meskipun tidak langsung diketahui hasil dekripsi data, hal ini dapat mengakibatkan resiko yang sangat besar untuk para kriptoanalisis.

FIPS 81 menetapkan mode Cipher Block Chaining (CBC) dalam Kerberos untuk meringankan masalah ini. Enkripsi blok Ciphertek yang sebelumnya di XOR-kan dengan plaintek yang akan dienkripsi selanjutnya, sehingga aliran blok data yang dienkripsi dapat tertutupi. Untuk enkripsi blok pertama kunci enkripsi digunakan untuk menghasilkan Initialization Vector (IV), yang nantinya kana digunakan sebagai blok ciphertek yang akan di XOR-kan dengan blok plaintek yang pertama. Akan tetapi mde CBC ini tidak dapat memberikan jaminan terhadap apa yang diharapkan Kerberos. Jika blok ciphertek dimodifikasi atau dirubah, error satu blok plaintek yang telah didekripsi akan membuat error blok setelahnya. Untuk mengecek integritas data enkripsi maka akan ditambahkan pada plaintek sebelum enkripsi dan mengenkripsinya sebagai bagian dari palintek dengan menggunakan integritas checksum.



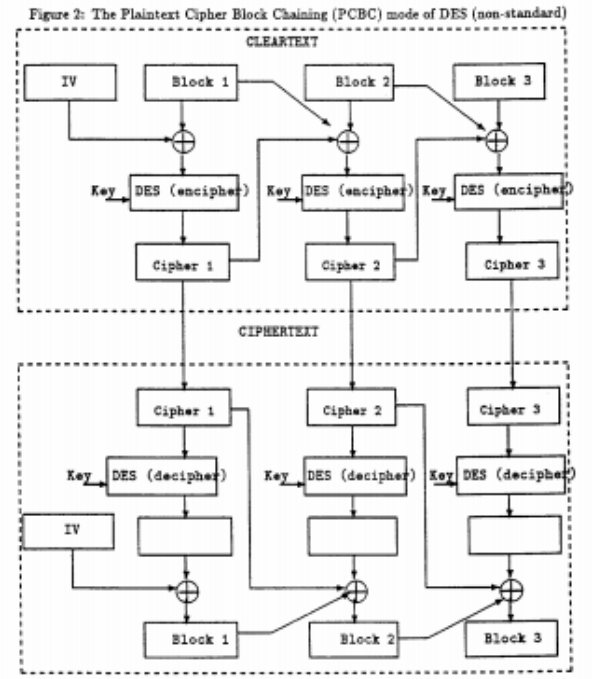
Gambar 1 - Mode Cipher Block Chaining dalam DES

Mode CBC dapat dijelaskan sebagai gambar 1 diatas. Pesan yang akan dienkripsi dibagi menjadi blok-blok. Dalam enkripsi CBC, masukan blok pertama yang telah dibagi akan di XOR-kan dengan 64bit initializing vector (IV),i.e.,(I1,I2,...,I64)=(IV1⊕D1,IV2⊕D2,...,IV64⊕D64). Blok input akan diproses dengan alat DES melakukan enkripsi state dan hasil keluaran blok akan menjadi ciphertek, i.e., (C1,C2,... ,C64) = (01,02,.. ,064). Ciphertek pertama ini akan di XOR-kan denga blok plaintek yang kedua untuk menghasilkan blok masukan DES yang kedua i.e., (I1,I2,...,I64) = (C1⊕D1,C2⊕D2,...,C64⊕64). I dan D disini menunjuk ke blok yang kedua. Blok masukan yang kedua akan diproses dengan alat DES state enkripsi untuk menghasilkan blok ciphertek yang kedua. Proses enkripsi ini akan terus berjalan sampai sukses hingga menghasilkan sebuah ciphertek sebagai hasil dari enkripsi data plaintek.

Dalam dekripsi CBC, blok ciphertek pertama dari enkripsi pesan digunakan sebagai blok input dan diproses hingga alat DES di state dekripsi, i.e., (I1,I2,…,I64)=(C1,C2,…,C64). Hasil dari blok keluaran, yang sama dengan blok input yang benar selama enkripsi

DES berlangsung, akan diXOR-kan dengan IV (harus sama dengan IV yang digunakan saat enkripsi) untuk menghasilkan blok plaintek yang pertama, i.e.,(D1,D2,…,D64)=(O1⊕IV1,O2⊕IV2,...,O64⊕IV64). Blok ciphertek yang kedua akan digunakan sebagai blok input dan diproses secara DES dengan state dekripsi dan hasil blok keluaran di XOR-kan dengan blok cipher pertama. Untuk menghasilkan blok plaintek yang kedua, i.e., (D1,D2,...,D64) = (O1⊕C1,02⊕C2,...,064⊕C64). Diingatkan lagi bahwa D dan O menunt=juk ke blok kedua. Proses dekripsi CBC terus berlanjut seperti barusan hingga blok cipher terakhir berhasil di dekripsi. Ciphertek merepresentasikan sebagian blok data harus di dekripsi secara spesifik untuk aplikasi.

Tetapi, perancang Kerberos menginginkan proses enkripsi dan pengecekan dapat dilakukan dalam sekali jalan. Karena dengan melakukan dua kali proses, yaitu enkripsi dan pengecekan akan menghabiskan biaya yang lebih untuk performa yang ada. Criteria desain yang mereka inginkan adalah tidak terlalu mengharapkan bantuan enkripsi hardware DES secara spesifikasi. Mereka hanya berharap kepada implementasi software algoritma enkripsi. Sebagai hasilnya, mereka tidak membatasi penggunana mode operasi standar yang dilakukan. Maka mereka menemukan mode enkripsi yang alinyang disebut mode Plaintext Cipher Block Chaining (PCBC) yang melakukan operasi XOR antara blok plaintek sebelumnya dengan blok plaintek yang akan dienkripsi dan dengan blok ciphertek yang telah dienkripsi sebelumnya. Sebagai hasil dari penggunaan mode enkripsi PCBC ini, error yang terjadi di salah satu blok ciphertek akan mengakibatkan erro terhadap seluruh blok plaintek yang telah dienkripsi. Dengan menggunakan mode ini, maka pengecekan checksum dapat ditiadakan.



Gambar 2 – Mode Plaintext Cipher Block Chaining (PCBC) dalam DES

Proses mode Enkripsi dan dekripsi Plaintek Cipher Block Chaining (PCBC) hampir sama dengan proses yang dilakukan CBC. Perbedaan terjadi ketika blok masukan enkripsi DES, akan diXOR-kan kembali dengan plaintek sebelumnya (untuk blok pertama hanya dilakukan sekali dengan IV). Sedangkan pada saat dekripsi, hasil dekripsi DES dekripsi blok pertama setelah diXOR-kan dengan IV akan menghasilkan blok palintek dan blok tersebut akan digunakan untuk melakukan XOR dengan hasil XOR hasil dekripsi masukan DES dekripsi dengan blok ciphertek sebelumnya sehingga menghasilkan blok palintek yang kedua.

Tetapi penggunaan mode PCBC ini juga memiliki ketidakefisienan yang berbeda: penukaran dua blok ciphertek dapat menghancurkan plaintek hasil dekripsi yang dilakukan.

2.2 Checksums Kriptografi

Dalam penambahan dalam enkripsi untuk mengurung dan menjaga keamanan pesan, dobel algoritma checksum dapat digunakan sebagai opsi aplikasi protokol untuk mendapatkan kepastian integritas data dengan cost yang kecil. Algoritma ini dimodifikasi dari Jueneman. Checksum dikomputasi denganmenggunakan kunci sesi yang dipakasi sebagai bibit. Tetapi, checksum protokol

yang sekarang tidak dienkripsi ketika ditransmisikan, meninggalkan kunci sesi terekspos memungkinkan terjadi ketika algoritma tersebut dibalik. Jika checksum telah dienkripsi, peyadap akan tahu bagaimana menemukan kunci sesi dengan menggunakan kriptoanalisis dalam bibit-bibit checksum.

2.3 Kriptoanalis

Protokol Kerberos dan implementasi yang ada didalamnya dirancang dengan asumsi bahwa sistem kriptografi yang dibuat adalah aman. Sangat kecil sekali analisis kriptografi yang dilakukan untuk menyerang sistem. Dengan system keamanan kriptografi yang ada dimungkinkan masih ada kriptoanalis yang mencoba untuk menyerang keamanan meskipun sangat jarang sekali.

2.4. Aplikasi Protokol

2.4.1 Servis Otentikasi

Untuk mendapatkan tiket yang akan diserahkan untuk mendapatkan kayanan, klien mengirimkan pesan ke KDC, yang berisi nama, instance dan realm, waktu hari host klien, lama waktu tiket berlaku dan nama layanan dan instance alasan untuk mendapatkan tiket.

KDC melakukan pembacaan catatan dari klien dan server secara berurut, membuat tiket dan mengorganisir credential information, mengenkripsi tiket dengan menggunakan kunci klien dan mengembalikan data yang telah dienkripsi tersebut bersama dengan beberapa pengaturan informasi plaintek kepada klien.

Tiket berisi nama klienm alamat host klien, kunci sesi, lama waktu tiket berlaku dan nama server, instance dan realm. Credential information berisi informasi yang berupa salinan kunci sesi yang berada di tiket, nama server, instance dan realm, lama waktu tiket berlaku, nomor versi kunci dari kunci pribadi server digunakan untuk membuat tiket, panjang tiket dan waktu hari di KDC.

Harus diberi catatan bahwa tiket itu sendiri untuk tidak dienkripsi bersama dengan credentials information. Tiket biasanya dikirimkan melalui jaringan dari klien ke server dan jika tiket dienkripsi dengan menggunakan kunci pribadi, kunci sesi akan terkandung dengan aman sejak pelepasan atau pengiriman.

2.4.2 Client to Server

Setelah mendapatkan tiket dan credential information, klien membuat sebuat otenticator (yang mengandung nama klien, alamat host klien, dan lama waktu berlaku, yang digunakan untuk melawan pengulangan informasi. Semua yang terkandung dienkripsi dengan menggunakan kunci sesi) dan mengirimkan tiket, otenticator dan jika memungkinkan informasi aplikasi protokol ke aplikasi server.

Server mendekripsi dan menverifikasi tiket menggunakan kunci pribadi yang ada. Jika berhasil diverifikasi, maka digunakan kunci sesi untuk mendekripsi otenticator dan memverifikasi informasi tanpa pengulangan.

Pencapaian otentikasi yang diinginkan dari klien ke server adalah: jika klien membutuhkan otentikasi dari server ketika server membalas, server dapat menggunakan kunci sesi untuk membangkitkan balasan untuk membuktikan bahwa ini dapat diakses dengan kunci sesi. Hal ini melayani otentikasi server kepada klien, sejak kita asumsikan bahwa hanya server yang benar yang tahu kunci pribadi dan yang dapat mendekripsi tiket dan mendapatkan kunci sesi.

2.4.3 Ticket-Granting Service

Terdapat layanan special yang disediakan KDC yang merupakan bagian yang penting dalam layanan di Kerberos, tapi harus langsung mengakses ke basis data KDC. Layanan ini, diberi nama “Ticket-Granting Service” (TGS) yang dapat mengghasilkan tiket-tiket yang baru tanpa membutuhkan kunci pribadi yang dimiliki klien (yang nantinya harus membutuhkan workstation klien untuk menyiapkan atau mengulang request password klien).

Ketika user melakukan login, software workstation melakukan request tiket untuk TGS, dengan menggunakan protokol layanan otentikasi yang normal. User memasukkan passwordnya (ketika proses login), dan ini digunakan untuk mendekripsi respon. Tikiet dan credential akan disimpan di cache workstation. Lama waktu berlaku tiket dan kunci sesi disimpan di workstation dan memberikan waktu yang sangat singkat bagi penyadap dan penggangu yang mungkin menyerang.

Ketika tiket dibutuhkan untuk penambahan layanan, workstation klien menggunakan protocol klien-server standar untuk mengirimkan TGS tiket dam otentikator bersama dengan waktu berlaku klien, request waktu berlaku dan nama layanan yang membutuhkan tiket tertentu untuk melakukan TGS. TGS menggunakan kunci pribadinya (yang dapat diambil dari basisdata) untuk melakukan dekripsi tiket, untuk menverifikasi otentikator dan memenuhi request dengan membuat tiker yang baru dan mengontrol credential. Sebagai protokol layanan otentikasi, credential dan tiket dienkripsi (tapi dari kunci

sesi dari tiket TGS, bukan dari kunci pribadi klien) dan dikembalikan ke klien, yang nantinya akan di dekripsi dan menyimpan tiket dan credential di cache.

2.4.4 Intefgrity-protected messages

Pesan protokol "KRB_PRIV" digunakan ketika klien dan server menginginkan untuk melakukan verifikasi integritas dan keamanan dari pesan pribadi.

Pesan mengandung data user, beberapa informasi control, alamat jaringan pengirim dan waktu hari host pengirim, dienkripsi (dengan menggunakan mode PCBC DES) dengan menggunakan kunci sesi. Dalam pengenkripsian, perusakan pesan atau ketidakcocokan informasi control mengidentikasisan bahwa pesan telah dimodifikasi atau pesan sudah tidak asli.

3. Planned Version 5 changes

Proyek Athena merencanakan untuk dapat bantuan dalam hal melakukan enkripsi dengan menggunakan tipe enkripsi yang berbeda-beda dalam pesan protokol very yang kelima. Para perancang hanya dapat mengimplementasikan terbatas hanya versi DES. Berharap aka nada perancang-perancang yang lain dapat memberikan tipe enkripsi yang berbeda selainyang telah diimplementasikan (DES).

Dari masalah-masalah penggunaan PCBC diatas, para perancang Kerberos dapat memutuskan untuk menggunakan mode CBC DES dengan menggabungkan metode terseut dengan checksum data untuk memberikan integritas data dan kerahasiaan data. Penggunaan algoritma checksum masih dalam perdebatan. Sehingga penggunaan algoritma tersebut tidak dapat menimbulkan interaksi yang negative terhadap DES.

Para perancang juga masih mencari kriptografi checksum yang lebih baik dari checksum dobel (yang belum memberikan bukti analitis). Ode checksum DES CBC memiliki property-properti yang lebih baik dalam pembelajaran, tapi secara komputasional masih lebih mahal dibandingkan checksum dobel. Para perancang mengidelakan komputasional checksum yang murah yang juga dapat menjamin keamanan.

Dengan berkembangnya zaman dan ilmu pengetahuan diharapkan perkembangan alat keamanan seperti protokol akan dapat cepat berkembang karena kejahatan data pun semakin lama akan semakin berkembang. Perkembangan versi 5 atau selanjutnya diharapkan akan semakin meningkatkan keamanan dan integritas data agar jaringan yang terjadi tidak ada yang dapat merusak sistem jaringan yang terjadi.

4. KESIMPULAN

Enkripsi yang dilakukan di protokol Kerberos ini terbilang cukup aman dengan susahnya pernyadap atau kriptoanalis untuk menyerang protokol ini. Meskipun jaringan yang dipakai adalah jaringan yang tidak aman sekalipun. Pengguanaan Kerberos dapat diimplementasikan di sebuah file sistem yang terdistribusi yang sangat membutuhkan keamanan data dan integritasnya.

Jaringan yang tidak aman seperti internet dapat menjadi aman dengan penggunaan protokol-protokol yang menjamin keamanan dan integritas data yang ada. Penggunaan enkripsi merupakan salah satu cara pengamanan yang dilakukan agar koneksi yang terjadi antara klien dan server dapat berjalan lancar.

Makalah ini mendiskusikan masalah enkripsi yang digunakan pada protokol Kerberos dan keputusan dalam mendesain dan rasional keputusan pada beberapa penggunaan enkripsi. perlu diingatkan pada beberapa implementasi dan protokol yang kurang efisien dan menyarankan agar perubahan-perubahan yang terjadi dapat mengurangi permasalahan-permasalahan pada protokol di versi selanjutnya.

Kerberos telah sukse mencapai tujuan atau goal dengan menggunakan software enkripsi dengan membatasi penggunaan kebutuhan data yang harus dienkripsi untuk basis protokol otentikasi dan memperbolehkan aplikasi-aplikasi untuk memiliki level integritas dan privasi kriptografi.

REFERENSI

[1] The Use of Encryption in Kerberos for Network Authentication,http://dsnd.csie.nctu.edu.tw/research/crypto/HTML/PDF/C89/35.pdf.

[2] Kerberos: The network Authentication protocol, http://web.mit.edu/Kerberos/.

[3] FIPS Pub 81 – DES Modes of Operation, http://www.umich.edu/~x509/ssleay/fip81/fip81.html.

[4] Kenneth Paul Birman, Reliable Distributed System, Springer-Verlag, March 2005.

[5] Chapter 1 introduction to Kerberos, http://h71000.www7.hp.com/doc/83final/ba554_90008/ch01.html

[6] Data Encryption Standard, http://www.laynetworks.com/users/webs/des.htm

[7] National Bureu of Standards. DES Modes of Operation. *Federal Information Processing Standars Publication*, 46, 1977.

[8] National Bureu of Standards. DES Modes of Operation. *Federal Information Processing Standars Publication*, 81, 1980.

[9] Roger M. Needham and M. D. Schoroeder. Using Encryption for Authentication in Large Networks of Computers. *Communications of the acm*, 21(12):993-999, DEC 78

[10] Steven P. Miller, B. Clifford Neuman, Jeffrey I. Schiller, and Jerome H. Saltzer. Section E.2.1: Kerberos Authentication and Autorization System. *Project Athena Technical plan*, December 1987