PENGGUNAAN KRIPTOGRAFI DALAM FIREWALL TO FIREWALL SYSTEM

Dimas Aditiya Nurahman 13508093

Program Studi Teknik Informatika Institut Teknologi Bandung
Jl.Ganesa 10, Bandung
e-mail: dimas_an@rocketmail.com

ABSTRAK

Makalah ini membahas sub pokok bab mengenai penerapan dari salah satu bahasan Algoritma dan Bilangan Bulat yaitu kriptografi. Kriptografi di sini akan dihubungakan dengan pengaplikasian atau penerapannya dalam pengamanan jaringan yang dikontrol melalui suatu sistem bernama firewall. Makalah ini akan mengulas sedikit tentang aplikasi-aplikasi penggunaan metode kriptografi dalam firewall.

Komunikasi TCP/IP dapat mengamankan suatu jaringan dengan bantuan dari kriptografi. Dengan penggunaan metode *encrypt message*, akses ke suatu jaringan dapat dikontrol sesuai dengan autentifikasi pengamanan yang diingnkan seperti adanya IP security. Protocol dan metode dari kriptografi dirancang untuk tujuan yang berbeda dalam pengaman data komunikasi, baik stanlone computer maupun computer yang terhubung dengan jaringan computer, seperti LAN, WAN, Internet, dan lain sebagainya. Contoh pengaplikasiannya adalah pada enkripsi *firewall-to-firewall*. Sistem ini pertama kali diaplikasikan pada firewall ANS InterLock. Saat ini, koneksi semacam ini disebut sebagai *Virtual Private Network* (VPN) yang dapat diimplementasikan menggunakan algoritma blowfish. Ia adalah "privat" karena menggunakan kriptografi. Ia menjadi privat secara "virtual" karena komunikasi privat tersebut mengalir melalui jaringan publik seperti internet. VPN muncul sebelum adanya konsep penggunaan firewall seperti sekarang ini, akan tetapi VPN kini mulai sering dijalankan pada firewall.

Kata kunci: Kriptografi, Firewall, VPN, Jaringan, algoritma, IP, Security .

1. PENDAHULUAN

Sebagaimana kita ketahui, segala hal pada masa modern ini menggunakan metode komunikasi dengan menggunakan sistem jaringan internet contohnya dalam *transfer and share* dokumen-dokumen penting dari perusahaan. Sistem jaringan ini terhubung secara global dan setiap orang dapat mengakses dengan cara-cara tertentu. Oleh karena itu, kita harus memperhatikan keamanan jaringan secara keseluruhan. Kita tidak dapat menjamin bahwa semua orang di "luar sana" adalah orang baik-baik, sehingga permasalahan keamanan jaringan ini merupakan hal yang harus mendapat perhatian yang lebih dari seorang administrator jaringan. Kita juga sebaiknya tidak selalu berpikir bahwa keamanan jaringan bukan hanya berhubungan dengan hacker atau cracker dari "luar sana" tetapi sering kali ancaman tersebut juga datang dari sisi jaringan internal kita sendiri.

Penjelasan di atas menunjukkan bahwa penggunaan firewall sangatlah penting. Untuk mengamankan jaringan salah satunya firewall dapat menggunakan bantuan dari kriptografi. Dalam kriptografi dikenal metode enkripsi dan dekripsi. Untuk penggunaannya sendiri, kedua metode di atas digunakan berdasarkan keperluan jaringan. Contohnya dalam penggunaan aplikasi firewall to firewall dapat digunakan algoritma enkripsi dan dekripsi *blowfish*.

Dengan adanya penjelasan dan pendeskripsian mengenai penggunaan kriptografi selain untuk menambah wawasan diharapkan baik pembaca maupun penulis makalah dapat terinspirasi untuk melakukan pengembangan hal-hal dalam metode kriptografi di bidang aplikasi jaringan. Selain itu penggunaan firewall dalam jaringan merupakan hal yang menjadi suatu keharusan, karena banyaknya *hacker* atau virus yang dapat menyerang jaringan, sehingga dapat membahayakan dokumen-dokumen penting yang bersifat *private.*

2. METODE

Ketika jaringan kita terhubung dengan sebuah WAN atau terhubung dengan Internet, maka kita harus mempertimbangkan masalah baik keamanan dari tiap-tiap komputer di dalam jaringan kita maupuan keamanan jaringan secara keseluruhan. Untuk dapat melakukan *control* terhadap jaringan yang kita buat, perlu adanya suatu metode, yaitu metode untuk mengamankan file-file

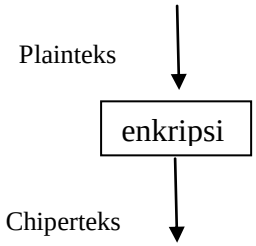
penting agar tidak dapat diakses oleh *user* yang tidak terautentifikasi oleh *author* dari jaringan.

Berbicara mengenai pengamanan suatu system, maka erat hubungannya dengan kriptografi. Kriptografi adalah ilmu sekaligus seni untuk menjaga kerahasiaan pesan (data atau informasi) dengan cara menyamarkannya (to crypt artinya menyamar) menjadi bentuk tersandi yang tidak mempunyai makna. . Kriptografi modern menggunkan disiplin matematika, ilmu komputer, dan rekayasa. Bila kerahasiaan suatu informasi menjadi sangat penting, maka hal seperti ini sangat dibutuhkan.

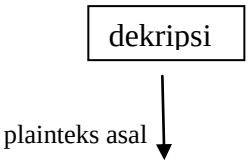
Tanpa kiat sadari hal-hal dalam kehiduapn kita sehari-hari menggunakan prinsip kriptografi. Mulai dari transaksi di mesin ATM, transaksi di di bank, transaksi dengan kartu kredit, ,percakapan memalui telepon genggam, *e-commece* melalui intenet, login situs jejaring social, sampai mengaktifkan peluru kendali pun menggunakan kriptografi. Kriptologi merupakan gabungan dari ilmu kriptografi dan analisis sandi. kriptografi merupakan teknik untuk mengamankan data dari sisi kerahasian (confidentiality), keabsahan pengirim/penerima (authentication), keaslian data (integrity) dan pertanggungjawaban telah mengirim/menerima (nonrepudiation).

Kriptografi menjadi sangat penting kareana menjadi dasar dari konsep pengamanan system pada jaringan, Sehingga masalah keamanan firewall dan jaringan pada computer tidaklah lepas dari kriptografi. Sehingga bila kita dapat membuktikan keamanan algoritma kriptografi terhadap sebuah analisis sandi, kita masih harus berhadapan dengan banyak analisis sandi lainnya. masalah ini yang harus dihadapi adalah bagaimana merancang algoritma kriptografi yang dapat diimplementasikan secara efisien pada berbagai platform perangkat lunak dan perangkat keras.

Dasar enkripsi cukup sederhana. Pengirim menjalankan fungsi enkripsi pada pesan ***plaintext (plaintext*** artinya teks jelas yang dapat dimengerti)**,** ***ciphertext(chipertext,*** artinya teks tersandi) yang dihasilkan kemudian dikirimkan lewat jaringan, dan penerima menjalankan fungsi dekripsi **(*decryption*)** untuk mendapatkan ***plaintext*** semula. Dekripsi membalikkan pesan menjadi pesan yang dapat dibaca kembali.



.



Gambar 1. Diagram alur proses kriptografi

Proses ini hanya dapat dilakukan oleh orang yang menggunakan metode yang sesuai. Proses enkripsi/dekripsi tergantung pada kunci (*key*) rahasia yang hanya diketahui oleh pengirim dan penerima. Semakin rumit algoritma kriptografi yang digunakan, semakin sulit pula untuk para hacker, cracker yang ingin membobol *security system* yang digunakan, sehingga komunikasi data antara pengirim dan penerima aman.

Kriptografi pada dsarnya digunakan untuk menjamin privasi: mencegah informasi menyebar kepada pihak yang tidak terautentifikasi secara legal untuk mengakses file yang ada pada jaringan. Oleh karena itu kriptografi memiliki hal-hal yang sanagt berkaitan erat pokok yaitu privasi, *authentification* (memverifikasi identitas pengguna) dan integritas (memastikan bahwa pesan belum diubah). Kriptografi pada firewall digunakan untuk mencegah ancaman dari *user* yang tidak berhak untuk memasuki komunikasi atau jaringan, sehingga kerahasiaan data dapat dilindungi. Secara garis besar, kriptografi digunakan untuk mengirim dan menerima pesan. Kriptografi pada dasarnya berpatokan pada kunci yang secara selektif telah disebar pada komputer-komputer yang berada dalam satu jaringan dan digunakan untuk memroses suatu pesan.

2.1 Sejarah Kriptografi

Paling awal dikenal penggunaan kriptografi adalah beberapa ciphertext diukir di atas batu di Mesir, tapi ini mungkin telah dilakukan untuk melek geli pengamat. The next oldest is bakery recipes from Mesopotamia. Tertua berikutnya adalah roti resep dari Mesopotamia.

Kriptografi klasik menggunakan chipper klasik jenis chipper transisiyang mengatur ulang huruf-huruf dalam pesan ('hello world' menjadi 'ehlol owrdl' dalam skema penataan ulang sederhana), dan substitusi chipper yang secara matematis menggantikan huruf atau kelompok huruf dengan kombinasi menurut suku/kelompok huruf (misalnya, 'terbang sekaligus' menjadi 'gmz bu podf' dengan mengganti setiap huruf dengan satu berikut dalam abjad Latin). Versi sederhana yang ditawarkan baik sedikit kerahasiaan dari giat lawan, dan masih dilakukan.

Sandi substitusi chipper awal adalah Caesar chiper, di mana setiap huruf pada plaintext digantikan oleh sebuah huruf beberapa jumlah posisi tetap lebih lanjut dalam alfabet. Chipper ini dinamakan setelah Julius Caesar yang ditemukan telah menggunakannya, dengan pergeseran 3 kode enkripsi, untuk berkomunikasi dengan para jenderal selama kampanye militer,

Berikut adalah potongan algoritma enkripsi yang digunakan dalam Caesar chipper yang dapat menjadi dasar sebagai pengembangan untuk algoritma autentifikasi jaringan.

```
/* Program enkripsi file dengan Caesar cipher */
#include <stdio.h>
main(int argc, char *argv[])
{
FILE *Fin, *Fout;
char p, c;
int k;
Fin = fopen(argv[1], "rb");
if (Fin == NULL)
printf("Kesalahan dalam membuka %s sebagai berkas
masukan/n", argv[1]);
Fout = fopen(argv[2], "wb");
printf("\nEnkripsi %s menjadi %s ...\n", argv[1],
argv[2]);
printf("\n");
printf("k : ");
scanf("%d", &k);
while ((p = getc(Fin)) != EOF)
{
c = (p + k) % 256;
putc(c, Fout);
}
fclose(Fin);
fclose(Fout);
}
```

```
/* Program dekripsi file dengan Caesar cipher */
#include <stdio.h>
main(int argc, char *argv[])
{
FILE *Fin, *Fout;
char p, c;
int n, i, k;
Fin = fopen(argv[1], "rb");
if (Fin == NULL)
printf("Kesalahan dalam membuka %s sebagai berkas
masukan/n", argv[1]);
Fout = fopen(argv[2], "wb");
printf("\nDekripsi %s menjadi %s ...\n", argv[1],
argv[2]);
printf("\n");
printf("k : ");
scanf("%d", &k);
while ((c = getc(Fin)) != EOF)
{
p = (c - k) % 256;
putc(p, Fout);
}
fclose(Fin);
fclose(Fout);
}
```

Pengembangan komputer digital dan elektronik setelah Perang Dunia II memungkinkan sandi jauh lebih kompleks. Dimana kerahasiaan pesan saat itu sangatlah penting Selain itu, komputer memungkinkan untuk enkripsi data apapun representable dalam format biner. tidak seperti cipher klasik yang hanya teks terenkripsi bahasa tertulis; ini masih baru dan signifikan.

Penelitian akademik kriptografi relatif baru, tetapi baru dimulai pada pertengahan 1970-an. Belakangan ini, IBM personil merancang algoritma yang menjadi Federal (yaitu, US) Data Encryption Standard; Whitfield Diffie dan Martin Hellman menerbitkan persetujuan kunci algoritma mereka, dan RSA algoritma diterbitkan pada Martin Gardner 's Scientific American kolom.. Sejak itu, kriptografi telah menjadi alat yang digunakan secara luas dalam komunikasi, jaringan komputer, dan keamanan komputer secara umum.

2.2. Firewall

Firewall adalah alat yang digunakan untuk mencegah orang luar memperoleh akses ke suatu jaringan. Firewall terdiri dari kombinasi antara perangkat lunak (software) dan perangkat keras (hardware). Firewall menyortir alamat yang masuk ke dalam jaringan kemudian memblokir alamat yang tidak sasuai. Penyortiran ini dapat dilakukan menggunakan pengaman kriptografi.

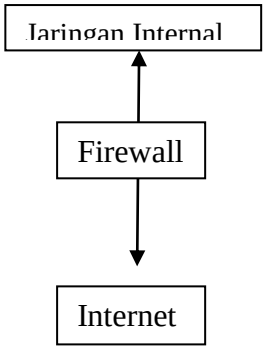
Firewall bekerja dengan mengamati paket IP yang melewatinya. Berdasarkan konfigurasi dari firewall, akses

dapat diatur berdasarkan IP address, port, dan arah informasi.

Untuk memahami bagaimana firewall bekerja, hal pertama adalah berkaitan dengan pemeriksaan prosedur penggunaan IP *address* sebagai suatu index. Dimana IP *address* ini menjadi index autentifikasi secara global di internet, baik *address* yang static maupun dinamik.

1). IP alamat statis adalah alamat yang permanent, yang merupakan alamat dari suatu mesin yang selalu dihubungkan ke Internet. Ada berbagai kelas dari alamat IP statis. Satu kelas dapat ditemukan dengan query. Kelas itu merupakan mesin tertinggi yang terhubung dengan jaringan, seperti domain dari server, Web server, dan root-level mesin, yang sudah terdaftar sebagai hostname pada database InterNIC.
2). IP address dinamis adalah alamat IP yang selalu berubah-ubah yang berfungsi sebagai koneksi ke jaringan. IP dinamis sering digunkan ISP untuk melakukan dial-up akses pada waktu dial up node, yang berfungsi menetapkan alamat IP yang selalu berbeda.

Singkatnya skema sederhana firewall ditunjukkan melalui gambar 2.



Gambar 2. Skema alur jalannya Firewall

Lalu, Bagaimana proses hubungan antara firewall sendiri dengan kriptografi? Dalam firewall dikenal istilah Intrusion Detection Systems(IDS). IDS ini membantu sistem informasi untuk mempersiapkan diri dan menghadapi ‘serangan’. IDS menyaring koneksi yang masuk ini dengan mengumpulkan informasidari berbagai system dan network source yang bervariasi, kemudian menganalisa informasi untuk mengatasi masalah sekuriti yang mungkin terjadi. Autentifikasi user dan password masih dibutuhkan untuk penggunaan, proteksi, dan organisasi, program anti-virus, file permission yang sesuai, semua sistem audit yang masih dipakai, dan network practice keseluruhan serta kebijakan masih selalu dibutuhkan. Proses sebaliknya, untuk mengubah ciphertext menjadi plaintext, disebut dekripsi (decryption). Jadi metode pengamanan yang ada pada firewall menggunakan prinsip ilmu kriptografi

2.3. Prinsip Algoritma Blowfish

Firewall jenis lain yang bekerja di internet adalah enkripsi *firewall-to-firewall*. Sistem ini pertama kali diaplikasikan pada firewall ANS InterLock. Saat ini, koneksi semacam ini disebut sebagai *Virtual Private Network* (VPN). Sebenarnya konsep VPN sendiri dapat diterapkan dengan beberapa cara, namun pada sub bab ini hanya akan dibahas mengenai penggunaan dengan metode enkripsi dekripsi blowfish.

Blowfish merupakan algoritma kunci simetrik cipher blok yang dirancang pada tahun 1993 oleh Bruce Schneier untuk menggantikan DES. Pada saat itu algoritma untuk men-enkripsi suatu pesan sangat banyak, akan tetapi penggunaannya sangat terbatas untuk publik, hal ini dikarenakan adnya hak paten dan lisensi untuk setiap algoritma yang digunakan. Schneier menyatakan bahwa blowfish bebas paten dan akan berada pada domain publik. Pernyataan Schneier sebagai penemu algoritma blowfish tersebut membuka gerbang baru dunia kriptografi untuk dapat terjun dan berkembang di publik, khususnya bagi masyarakat yang membutuhkan algoritma kriptografi yang cepat, kuat, dan tidak terhalang oleh lisensi.

Proses dari penggunaan metode blowfish itu sendiri ialah dengan memperhatikan jenis-jenis serangan yang dapat membahayakan data atau jaringan, lalu menganalisis metode pengamanan, yang kemudian dari analisis tersebut metode atau pelayanan system apa yang diterapkan dengan memperhatikan efektifitas penggunaan pelayanan yang diterapkan. Metode tersebut menerapkan mekanisme kriptografi pada model OSI. Berdasarkan sumber, algoritma blowfish cukup efektif untuk digunakan dalam system keamanan dalam konsep firewall to firewall atau VPN. Blowfish adalah algoritma kriptografi kunci simetrik cipher blok dengan panjang blok tetap sepanjang 64 bit. Algortima tersebut juga menerapkan teknik kunci yang berukuran sembarang. Ukuran kunci yang dapat diterima oleh blowfish adalah antara 32 hingga 448 bit, dengan ukuran standar sebesar 128 bit. Blowfish memanfaatkan teknik pemanipulasian bit dan teknik pemutaran ulang dan pergiliran kunci yang dilakukan sebanyak 16 kali. Keefektifan blowfish dilihat dengan perhitungan panjang kunci/*key encrypt message.*

Algoritma utama terbagi menjadi dua sub-algoritma utama, yaitu bagian ekspansi kunci dan bagian enkripsi-dekripsi data. Berikut merupakan contoh potongan algoritma *encipher* dan *decipher* dalam bahasa C.

```
void Blowfish_encipher(unsigned long *xl, unsigned
long *xr)
{
  unsigned long  Xl;
  unsigned long  Xr;
  unsigned long  temp;
  short          i;

  Xl = *xl;
  Xr = *xr;

  for (i = 0; i < N; ++i) {
    Xl = Xl ^ P[i];
    Xr = F(Xl) ^ Xr;

    temp = Xl;
    Xl = Xr;
    Xr = temp;
  }

  temp = Xl;
  Xl = Xr;
  Xr = temp;

  Xr = Xr ^ P[N];
  Xl = Xl ^ P[N + 1];

  *xl = Xl;
  *xr = Xr;
}
void Blowfish_decipher(unsigned long *xl, unsigned
long *xr)
{
  unsigned long  Xl;
  unsigned long  Xr;
  unsigned long  temp;
  short          i;

  Xl = *xl;
  Xr = *xr;

  for (i = N + 1; i > 1; --i) {
    Xl = Xl ^ P[i];
    Xr = F(Xl) ^ Xr;

    /* Exchange Xl and Xr */
    temp = Xl;
    Xl = Xr;
    Xr = temp;
  }

  /* Exchange Xl and Xr */
  temp = Xl;
  Xl = Xr;
  Xr = temp;

  Xr = Xr ^ P[1];
  Xl = Xl ^ P[0];
  *xl = Xl;
  *xr = Xr;
}
```

2.4. Penggunaan IPSec

Pada bagian sub bab ini akan dijelaskan konsep *security* yang juga diterapkan pada firewall dalam hubungannya dengan IP *address* yang digunakan oleh *user*. IPsec ini ddapat digunakan juga sebagai aplikasi dari firewall to firewall *system* atau VPN selain penggunaan konsep algoritma blowfish keamanan IP ini dikenal dikenal dengan IP Security (IPsec) dan telah menjadi standarisasi keamanan internet. Di sini tidak begitu banyak dijelaskan konsep IPsec karena penggunaan atau aplikasi yang diterapkan untuk firewall to firewall tidaklah banyak.

IPsec didesain untuk melindungi komunikasi dengan cara menggunakan TCP/IP. Protocol IPsec dikembangkan oleh IETF, dan IPsec memberikan layanan terhadap privacy dan autentifikasi menggunakan algoritma kriptografi modern. Untuk melindungi IP datagram, data ditransformasikan menggunakan algoritma enkripsi. Ada dua tipe umum dari dasar IPsec:

1). Authentication Header (AH)
Adalah protocol dokumen yang meliputi format paket dan isu umum yang berhubungan dengan penggunaan AH untuk pengesahan paket.

2). Encapsulating Security Payload (ESP)
Adalah dokumen yang meliputi format paket dan isu umum yang berhubungan dengan penggunaan dari ESP untuk paket enkripsi dan autentikasi.

Untuk mengimplementasikan 2 jenis tipe di atas dibutuhkan algoritma AH dan ESP. Dibutuhkan dukungan untuk protokol IPsec, dan dukungan kernel untuk algoritma enkripsi dan hash yang akan digunakan oleh AH atau ESP. Berikut merupakan contoh potongan algoritma Hash untuk AH dan ESP

```
Initialize variables:
h0 = 0x67452301
h1 = 0xEFCDAB89
h2 = 0x98BADCFE
h3 = 0x10325476
h4 = 0xC3D2E1F0
   Initialize hash value for this chunk:
   a = h0
   b = h1
   c = h2
   d = h3
   e = h4
   Main loop:
   for i from 0 to 79
      if 0 = i = 19 then
         f = (b and c) or ((not b) and d)
         k = 0x5A827999
      else if 20 = i = 39
         f = b xor c xor d
```

```
        k = 0x6ED9EBA1
    else if 40 = i = 59
        f = (b and c) or (b and d) or (c and d)
        k = 0x8F1BBCDC
    else if 60 = i = 79
        f = b xor c xor d
        k = 0xCA62C1D6
    temp = (a leftrotate 5) + f + e + k + w[i]
    e = d
    d = c
    c = b leftrotate 30
    b = a
    a = temp
Add this chunk's hash to result so far:
h0 = h0 + a
h1 = h1 + b
h2 = h2 + c
h3 = h3 + d
h4 = h4 + e
```

IV. KESIMPULAN

Dewasa ini, sistem penggunaan internet atau jaringan sudahlah sangat marak digunakan di kalangan publik. Proses *transfer and share* pada dokumen-dokumen penting perusahaan menggunakan aplikasi jaringan ini. Dan karena terkoneksi dengan internet, jaringan ini dapat diakses secara global atau universal. Hal ini menyebabkan timbulnya ancaman dari orang-orang yang tidak berhak atau tidak terautentifikasi untuk dapat mengakses dokumen tersebut. Oleh karena itu dibutuhkan suatu sistem pengaman yaitu firewall sebagai penghalang agar *user* yang tidak terautentifikasi tidak dapat masuk ke dalam jaringan.

Firewall merupakan salah satu dari aplikasi dalam penggunaan metode kriptografi. Firewall yang merupakan sistem pengamanan pada jaringan komputer menggunakan suatu ”kode” sebagai autentifikasi dari jaringan luar yang ingin masuk. Kode ini merupakan kombinasi algoritma-algoritma dari kriptografi. Semakin rumit algoritma yang digunakan, semakin susah pula bagi para *hacker* atau *cracker* untuk dapat ”membobol” jaringan tersebut.

Pada dasarnya metode kriptografi yang digunakan pada firewall memiliki prinsip dasar yang sama dengan kriptografi awal. Yaitu menggunakan proses enkripsi dan dekripsi pada *message* yang ingin dirahgasiakan atau sebagai kode *login* ke suatu jaringan. Metode ini contohnya digunakan pada konsep firewall to firewall atau lebih dikenal dengan VPN, dimana algoritma yang digunakan adalah algoritma blowfish yang dapat memproses pemilihan pelayanan system pengamanan dari kasus *hacker* atau *cracker* yang masuk secara tidak legal.

REFERENSI

[1] Munir, Rinaldi, *Diktat Kuliah IF2151 Matematika Diskrit Edisi Keempat*, Departemen Teknik Informatika Institut Teknologi Bandung, 2004

[2] http://en.wikipedia.org/wiki/Cryptography
Tanggal Akses 18 Desember 2009
Pukul 20.55

[3] http://kunamix.multiply.com/journal/item/19
Tanggal Akses 17 Desember 2009
Pukul 22.55

[4] http://en.wikipedia.org/wiki/SHA_hash_functions
Tanggal Akses 17 Desember 2009
Pukul 22.55

[5] http://id.wikipedia.org/wiki/Blowfish
Tanggal Akses 17 Desember 2009
Pukul 21.40

[6]http://opensource.telkomspeedy.com/wiki/index.php/Konsep_IPSec
Tanggal Akses 17 Desember 2009
Pukul 21.00