STUDI ALGORITMA ENKRIPSI PADA PROTOKOL *SECURE REAL TIME PROTOCOL*

Albert Raditya S – NIM : 13506077

Program Studi Teknik Informatika, Institut Teknologi Bandung
Jl. Ganesha 10, Bandung
E-mail : if16077@students.if.itb.ac.id

Abstrak

Seiring dengan berkembangnya zaman, teknologi semakin mempererat hubungan antar manusia. Kita tidak lagi perlu berhubungan secara langsung atau melalui tatap muka, kita dapat saling berhubungan satu dengan yang lainnya misalnya melalui instant messenger, email, dll. Kita-pun semakin sadar mengenai kebutuhan keamanan, dan kerahasiaan dari media tersebut. Karena kebutuhan itulah, SRTP sebuah metode pengembangan dari RTP dibutuhkan.

SRTP adalah sebuah protocol yang dikembangkan oleh kelompok kecil yang berasal dari CISCO dan Ericson dan dipublikasikan pada Maret 2004. SRTP – Secure Real-time Transport Protocol adalah pengembangan dari *protocol* RTP yang menyediakan fitur kerahasiaan melalui fasilitas enkripsi, autentikasi dan integritas pesan, dan *relay protection* untuk RTP traffic dan untuk mengontrol traffic untuk RTP. SRTP berfungsi untuk menjamin pengamanan pengiriman data khususnya multimedia file.

SRTP menggunakan Algoritma AES sebagai metode enkripsi dalam pengiriman data. Pada aplikasinya SRTP memiliki 2 buah mode, yaitu Segmented Integer Counter, dan AES di f8-mode. Selain itu SRTP juga dapat berjalan dengan mode null cipher. Mode ini adalah mode dimana pengiriman data tidak dilindungi dengan algoritma enkripsi.

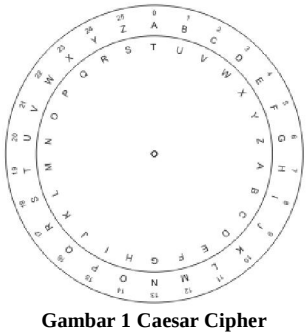
Dalam paper ini, penulis akan membahas mengenai perbandingan ketiga buah mode SRTP diatas. Penulis akan membandingkan terutama dua buah mode yang pertama baik dari segi implementasi, keamanan, kegunaan, dan kelemahan masing-masing mode tersebut.

Kata kunci: Secure Real-Time Protocol, *Advanced Encryption Standard*, *AES Segmented Integer Counter Mode, AES f8-mode, dan null cipher*.

I. PENDAHULUAN

Kita tahu bahwa manusia adalah makhluk sosial yang berarti manusia tidak dapat hidup tanpa orang lain. Oleh karena alasan tersebut, manusia berinteraksi dengan manusia lain. Seiring dengan berkembangnya zaman, kebutuhan untuk informasi, dan keamanan pengiriman informasi menjadi semakin penting. Kebutuhan ini juga semakin berkembang cepat, terlebih seiring perkembangan Teknologi Informasi seperti mobile phone, Internet, dll.

Salah satu cara untuk mengaplikasikan pertukaran informasi yang aman adalah menggunakan kriptografi. Karena kesadaran manusia atas pentingnya keamanan pertukaran informasi, Kriptografi sejak dahulu telah dikembangkan. Salah satu contoh algoritma kriptografi klasik yang cukup sering digunakan adalah Caesar Cipher.



Gambar 1 Caesar Cipher

Setelah ditemukannya komputer maka, algoritma kriptografi klasik mulai ditinggalkan, dan

kriptografer mulai beralih menggunakan algoritma kriptografi modern. Algoritma-algoritma Kriptografi modern yang sering digunakan adalah DES, AES, Blowfish, Serpent, GOST, dll.

II. LANDASAN TEORI

2.1 Kriptografi

Algoritma kriptografi klasik adalah algoritma yang digunakan untuk melakukan proses enkripsi dan dekripsi pesan di saat sebelum ditemukan komput

2.2 Algoritma Kriptografi Klasik

Algoritma kriptografi klasik adalah algoritma yang digunakan untuk melakukan proses enkripsi dan dekripsi pesan di saat sebelum ditemukan komputer.

Algoritma kriptografi klasik dapat dibedakan menjadi dua metode yaitu:

1. Metode Subtitusi
   Metode dimana kata atau huruf yang ingin dienkripsi digantikan dengan huruf atau kata lain.
2. Metode Transposisi
   Metode dimana huruf atau kata yang ingin dienkripsi ditukar urutannya sehingga tidak mudah dimengerti oleh orang yang ingin

Kedua metode diatas sangat penting karena merupakan dasar yang akan diimplementasikan untuk algoritma kriptografi modern.

2.3 Algoritma Kriptografi Modern

Algoritma Kriptografi Modern merupakan algoritma kriptografi yang digunakan setelah komputer ditemukan. Berbeda dengan algoritma kriptografi klasik dimana objek enkripsi adalah huruf, di algoritma kriptografi modern terdapat 2 objek enkripsi yaitu bit , dan block (kumpulan bit).

Algoritma Kriptografi enkripsi dengan menggunakan objek bit disebut stream cipher. Sedangkan Algoritma kriptografi yang menggunakan blok sebagai objeknya disebut block cipher. Algoritma Stream cipher dapat dengan mudah dipecahkan seperti pada algoritma kriptografi klasik yaitu dengan teknik analisis frekuensi, dan teknik prakiraan.

Selain menggunakan objek yang kita enkripsi atau dekripsi, algoritma kriptografi modern juga memiliki beberapa metode untuk enkripsi, yaitu ECB - Electric Code Book, CBC - Cipher Block Chaing, CFB - Cipher Feedback, dan OFB - Output Feedback.

2.4 Advance Encryption Standard

Advanced Encrption Standar merupakan algoritma kriptografi modern yang menggantikan algoritma DES (Data Encryption Standard). Sebagai standard enkripsi kritografi simetri.

AES merupakan hasil sayembara pencarian algoritma kriptografi yang baru. Pada kenyatannya, AES menggunakan algoritma Rijndael yang diusulkan oleh Vincent Rijmen dan Joan Daemen. Sebenarnya ada fitur tambahan yang tidak diimplementasikan dari algoritma Rijndael yaitu penanganan untuk ukuran block dan ukuran key masukkan yang berlebihan.

AES memiliki 3 buah versi berdasarkan panjang kunci yaitu: AES128, AES192, dan AES256. Tetapi algoritma AES192 sangat jarang untuk digunakan, sehingga algoritma AES128 dan AES256, lebih lazim digunakan.

Algoritma Rijndael, secara garis besar terbagi menjadi 3 buah bagian, yaitu: AddRoundKey, putaran sebanyak Nr, dan Final Round.

AddRoundkey yaitu merupakan sebuah tahapan inisialisasi dari AES. Add roundkey melakukan operasi xor dengan key. Putaran sebanyak Nr -1 terdiri dari 4 buah proses sederhana yaitu: subbytes (subtitusi byte dengan menggunakan sbox), ShiftRows (pergeseran baris-baris array state secara wrapping), MixColumns (mengacak data di masing-masing kolom array state), AddRoundkey (melakukan SOR state sekarang dengan round key). Keempat Subproses diatas akan diulangi sebanyak Nr -1 kali. Proses yang terakhir terdiri dari 3 buah subprose yaitu subbytes, Shiftrows, dan addRoundKey.

2.5 Secure Real Time Protocol

Secure Real Time Protocol adalah sebuah profile dari Real-time Transport Protocol yang menyediakan layanan kerahasiaan, ontentikasi

pesan, dan reply protection terhadap RTP traffic dan terhadap control traffic untuk RTP.

SRTP menyediakan sebuah framework untuk proses enkripsi dan otentikasi RTP dan RTCP stream. SRTP mendefinisikan sebuah himpunan cryptographic transform, dan memperbolehkan transformasi baru yang akan diimplementasikan di masa depan. SRTP dapat mencapai throughput yang tinggi dan low packet envasion di lingkungan yang beragam.

SRTP pada kenyataannya hanya mengenkripsi payload (Audio atau video) untuk kerahasiaan. Algoritma Autentikasi melindungi integritas dari seluruh paket RTP Packet. SRTP MKI (Master Key Identification) akan mengidentifikasikan kunci master mana yang digunakan untuk mendapatkan session keys yang sekarang ini digunakkan dalam proses enkripsi dan dekripsi. Walau kadang tidak digunakkan, sebuah MKI yang typical berukuran 4 byte dan digunakkan di system yang membutuhkan multiple key exchange.

SRTP adalah sebuah protocol keamanan internet yang efisien dan singkat, berjalan dengan baik, dan telah tercapai layanan interoperability yang baik. Namun, SRTP kekurangan protocol untuk bertukar kunci yang lebih diterima.

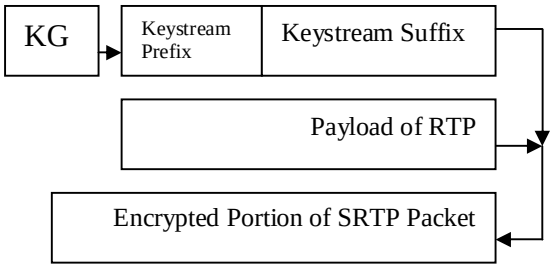
Setiap SRTP stream membutuhkan baik pengirim amupun penerima untuk menjaga informasi status cryptographic, yang bernama “cryptograpic context”.. SRTP membutuhkan dua buah jenis kunci yaitu master key dan session key. Session key artinya kunci yang secara langsung digunakan dalam cryptographic transform. Master key adalah sebuah bilangan random bit string.

III ANALISIS

3.1 AES di Secured Real-time Transfer Protocol

Transformasi Enkripsi yang didefinisikan di SRTP memetakan paket indeks dan mengubah kunci rahasia menjadi keystream segment SRTP. Setiapa keystream segment mengenkripsi sebuah RTP.
Proses untuk mengenkripsi sebuah paket terdiri dari:

- Menghasilkan keystream segment sesuai dengan paket
- Bitwise keystream segment XOR dengan payload dari Paket RTP untuk menghasilkan Bagian yang terenkripsi dari SRTP paket.



Gambar 2. Rancangan Umum AES pada SRTP

3.2 AES dalam mode Segmented Integer

Untuk memulai memahami kita mulai dengan dengan plainteks M, kunci K, dan sebuah counter ctr,dimana ctr adalah n bit string. C adalah hasil XOR dari M dan bit pertama M akan di pad sehingga

$$EK(ctr) \| EK(ctr + 1) \| EK(ctr + 2)\|..$$

Sedangkan untuk mendekripsi diakukakn hal yang sama sengan enkripsi tetapu M dan C diubah urutannya

Untuk scenario yang penggunaanya dianjurkan nonce akan diawali dengan 0 dan menghasilkan string ctr sebanyak 128 bit yang encode number nonce 2^{64}(atau nonce dianggap sebagai 64 bit binary number) Number dari nonce diincrement setiap enkripsi. Biasanya nilau C juga ditransmut bersama string yang mengencode nonce.

Secara konsepsual, Counter Mode terdiri atas mengenkripsi successive integers. Setiap paket dienkripsi dengan keystream segment yang berbeda, yang dapat dihitung dengan cara berikut ini

Inklusi dari SSRC memperbolehkan kita untuk menggunakan sebuah kunci yang sama untuk melindungi distinct SRTP streams didialam RTP session yang sama

Untuk SRTCP , SSRC dari setiap header pertama dari compound packet harus di gunakan, 31 bit I akan menjadi SRTCP index dan K_e , k_s akan digantikan dengan SRTCP Encryption key dan salt.

3.2 Analisis keamanan AES CTR Mode

Ketika menggunakan AES-CTR mode akan menghasilkan kerahasiaan yang tinggi. Sayangnya, sangat mudah untuk salah mempergunakan counter mode. Ketika counter block values digunakan dari satu paket dengan kunci yang sama, key stream yang sama akan digunakan untuk mengenkripsi kedua paket, maka jaminan kerahasiaan terhindar/
the same key stream will be used to encrypt both packets, then the confidentiality
Ketika dua plainteks yang berbeda dienkripsi dengan satu keystream yang sama dan ketika hal tersebut terjadi serangan

(P1 XOR K1) XOR (Q1 XOR K1) = P1 XOR Q1
(P2 XOR K2) XOR (Q2 XOR K2) = P2 XOR Q2
(P3 XOR K3) XOR (Q3 XOR K3) = P3 XOR Q3

Ketika orang yang ingin menddengarkan pembicaraan kita tersebut mendapatkan kedua plaintext tersebut di xor bersama, maka akan dengan mudah dapat di pecah dan mendapatkan plaintextnya. Jadim menggunakan sebuah keystream untuk mengenkripsi dua buah plainteks akan memperlihatkan plainteks tersebut. Maka jangan menggunakan AES CTR dengan kunci yang static.

Selain itu kita juga membutuhkan perhatian yang special untuk pencegahan penggunaan kembali counter block value dengan static key selama penggunaannya.

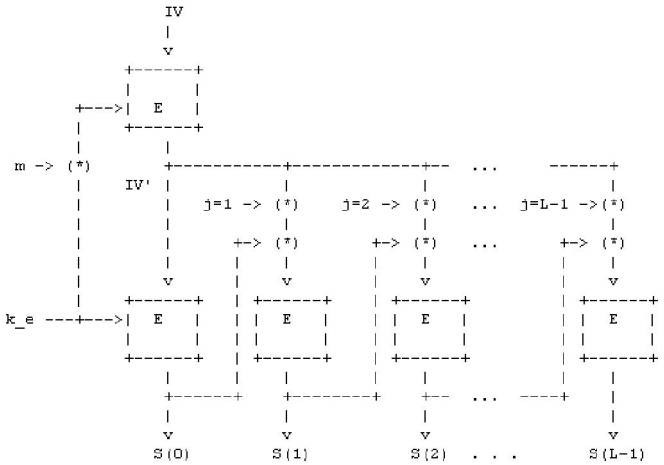
Supaya aman, implementasi ESP harus menggunakan kunci yang baru untuk digunakan dalam AES CTR. Internet Key Exchange protocol dapat dipergunakan untuk mendapatkan kunci yang baru. IKE juga dapat dipergunakan untuk mendapatkan nonce yang ada di bagian pertama dari security association.

Implementasi ESP yang memperbolehkan penggunaan sebuah kunci yang sama untuk enkripsi outbound traffic dam dekripsi incoming traffic dengan peer yang sama harus bisa memastikan bahwa nilai NONCE keduanya berbeda

3.3 AES f8-mode

AES mode ini dipergunakkan untuk mengenkripsi UMTS (Universal Mobile Telecommunication System). Untuk High Level, F8-Mode merupakan variasi dari Ouput Feedback Mode dengan elaborasi dari inisialisasi dan feedback function. Jika pada normal OFB, intinya terdiri dari block cipher

Berikut adalah gambar struktur AES dalam mode F8:



Gambar 2 AES F8 Mode (* menandakan XOR)

Dari diagram diatas kita dapat melihat keseluruhan kerja dari AES dalam fungsi f8.

Penghasilan Keystream

Untuk Key stream S(0) ||... || S(L-1) sebagai N-bit pesan akan didefinisikan dengan
Setting

IV' = E(k_e XOR m,IV)

Dan j = 0, 1, …..L-1. Dimana L = N/ n_b (difloorkan keatas). Perhatikan bahwa kita tidak menggunakan langsung IV. Kita menyerahkannya ke E dengan kunci lain untul menghasilkan nilai yang tersamrkan untuk mencegah Eavesdropper untuk mengetahui input dan output pairs.

Peran internal counter j adalah untuk menghindari siklus short keystream. Hasil kunci yang tersamarkan m sebagai berikut

$$m = k\_s \,||\, 0x555..5,$$

sender tidak perlu menghasilkan 2^{32} block, yang mana cukup untuk menghasilkan 2^{39} block.

IV Formation

Pengaturan formasi IV memiliki tujuan untuk memperbolehkan implicit header Authentication atau sering disebut sebagai IHA.

IV untuk SRTP pada 128 Bit Blocks AES f8-mode akan dihasilkan dengan cara sebagai berikut:

IV = 0x00 || M || PT || SEQ || TS || SSRC || ROC

M, PT, SEQ, TS,SSRC akan diambil dari RTP Header.ROC datang dari Cryptographic context. Keberadaan SSRC sebagai bagian dari IV memperbolehkan AES-f8 mode untuk dipergunakan ketika kunci stream dipergunakan oleh multiple stream dalam RTP session yang sama

3.4 Perbandingan Counter Mode dan F8 Mode

Seperti yang telah dijelaskan diatas perbedaan signifikan yang ada adalah ketika penggunaan Master key pada kedua mode untuk mengenkripsi dua buah plainteks pada saat RTP session yang sama.

Pada Counter Mode, Karena tidak ada penanganan terhadap hal tersebut maka jika ada eavesdropper, plainteks yang ada akan dengan mudah dikeahui oleh eavesdropper tersebut.

Berbeda halnya dengan mode f8. F8 mode banyak melakukan modifikasi terhadap IV sehingga ketika kita melakukan enkripsi hasil yang dihasilkan tidak dengan mudah dienkripsi

Jika kita mengamati AES f8-mode tidak ada threshold yang menjamin keamanan sekuat yang dilakukan pada AES CM. AES F8 modemenggunakan above bound sebagai pembatas dengan kemanan yang cukup terhadap kekurangan yang ada.

3.5 Null Cipher

Null cipher merupakan salah satu mode enkripsi yang dapat dipilih pada SRTP. Mode ini digunakanjika user tidak menginginkan adanya enkripsi pada pesan yang dikirim.

Prosesnya dengan mengambil plainteks sebagai ciphertext.

IV KESIMPULAN

Penggunaan kriptografi dalam jaringan komputer sudah menjadi hal yang biasa. AES merupakan salah satu metode yang diimplementasikan sebagai pengamanan dalam salah satu bagian dari hal tersebut.

Untuk menambah kesulitan dalam mendapatkan pesan yang ada pada SRTP, maka pengiriman pesan pada SRTP dapat dilakukan dengan beberapa mode dari AES.

Mode-mode ini berguna untuk mengenkripsi pesan dengan mode yang berbeda sehingga eavesdropper tidak dengan mudah menebak mode yang digunakan dan sehingga eavesdropper tidak dengan mudah memecahkan dan mendapatkan plainteks yang dia ingin curi.

Dari mode-mode yang ada, menurut penulis yang paling baik adalah mode Counter Mode. Walaupun Counter mode memiliki kelemahan tetapi hasil enkripsi yang dihasilkan cukup kuat sehingga susah dipecahkan. Dan hasil keamanannya terjamin.

V USULAN PERBAIKAN TERHADAP COUNTER MODE

Perbaikan yang Penulis usulkan terhadap Counter mode adalah, ketika mengenkripsi dua buah plainteks pada saat session yang sama maka hal ini tidak boleh dilakukan

Jika hal ini terjadi maka pesan yang pertama masuk akan dienkripsi terlebih dahulu barulah mengenkripsi yang kedua sehingga key yang digunakan tidak sama. Sehingga eavesdropper tidak dengan mudah memecahkannya/

DAFTAR PUSTAKA

Munir, Ir. Rinaldi, M.T. Diktat Kuliah IF5054 Kriptografi. Teknik Informatika ITB, 2006
http://tools.ietf.org/html/rfc3711
http://www.faqs.org/rfcs/rfc3686.html
http://www.wikipedia.org

http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf/
http://www.mindspeed.com/web/download/download.jsp?docId=22980
http://www.rfc-editor.org/rfc/rfc4568.txt
http://danada.rice.iit.edu/voip/Roundtable-presos/IIT-End-to-End-VoIPSec-tm.pdf