PENGAMANAN JARINGAN VoIP DENGAN MEMANFAATKAN ALGORITMA STREAM CIPHER A5

Satrio Ajie Wijaya [1)]

1) Jurusan Teknik Informatika ITB, Bandung, email: if14092@students.if.itb.ac.id

Abstract – *Voice over IP adalah suatu teknologi yang memungkinkan suatu percakapan jarak jauh melaui media internet. Data suara diubah menjadi kode digital dan dialirkan melaui jaringan, dalam hal ini adalah jaringan internet, dan bukan melalui jaringan PSTN biasa. Dalam melakukan pengiriman paket VoIP dibutuhkan suatu tenik pengamanan sehingga pembicaraan yang dilakukan melaui fasilitas VoIP tidak dapat disadap oleh orang yang tidak memiliki otoritas. Salah satu tekhnik pengamanan yang dapat dilakukan adalah dengan melakukan enkripsi untuk tiap paket data yang dikirim dalam hal ini adalah algoritma stream cipher A5.*

Kata Kunci*: VOIP, delay, A5*

1. PENDAHULUAN

Voice over IP atau yang lebih dikenal dengan VoIP adalah suatu teknologi yang mampu untuk melewatkan trafik suara, video, dan data dengan memanfaatkan suatu jaringan IP.

Ada beberapa keuntungan yang diperoleh dengan memanfaatkan VoIP jika dibandingkan dengan memanfaatkan jaringan telepon biasa. Dengan memanfatkan VoIP, biaya yang dikeluarkan untuk melakukan penggilan dan pembicaraan terutama pembicaraan jarak jauh dapat ditekan sampai 70% dari biaya yang dekeluarkan pada ketika melakukan pembicaraan dengan menggunakan telepon biasa yang menggunakan jaringan PSTN. Disamping hal tersebut, biaya pemeliharaan dapat ditekan seminimal mungkin dikarenakan adanya pemisahan *voice* dan *data network.*

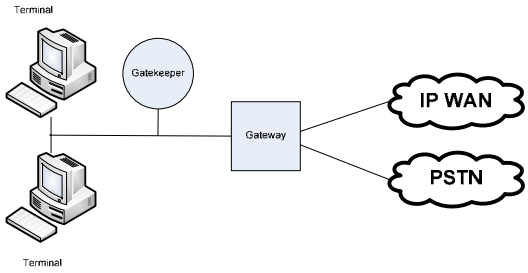
Namun, disamping keunggulannya yang dimiliki VoIP tersebut ada permasalahan yang dihadapi oleh para pengguna aplikasi terutama mengenai masalah keamanan. Paket suara yang dikirimkan dengan memanfaatkan aplikasi ini sangat riskan untuk disadap dan dimanipulasi oleh pihak yang tidak memiliki otoritas. Hal ini dikarenakan belum adanya suatu system pengamanan yang digunakan untuk melakukan pengiriman trafik suara tersebut.

Untuk mengatasi permasalah tersebut, salah satu solusi yang dapat ditempuh adalah dengan melakukan enkripsi terhadap paket data yang dikirimkan, dalam hal ini enkripsi dilakukan dengan memanfaatkan salah satu algoritma stream chipper yaitu algoritma A5 yang biasanya dimanfaatkan untuk melakukan enkripsi terhadap jaringan GSM di wilayah Amerika Serikat dan Eropa.

2. ARSITEKTUR VoIP

Ada 4 komponen utama yang digunakan dalam VoIP

- *Terminal*
- *Gateway*
- *Gatekeeper*
- *Multipoint Control Unit*



Gambar 1 Arsitektur VoIP

Terminal yang digunakan adalah berupa suatu personal computer atau alat lain yang dapat menjalankan aplikasi multimedia. Terminal tersebut digunakan untuk melakukan komunikasi dua arah secara real time.

Gateway digunakan untuk mmenghubunkan jaringan VoIP dengan jaringan non VoIP seperti jaringan PSTN yang digunakan pada telpon biasa. *Gateway* ini berfungsi untuk melakukan konversi dari jaringan VoIP ke jaringan PSTN, dan begitu pula sebaliknya. Akan tetapi, untuk jika jaringan VoIP tidak terhubung dengan jaringan PSTN maka *gateway* tidak dibutuhkan.

Gatekeeper berfungsi sebagai *local administrator* yang mengatur telefoni dalam jaringan VoIP dalam suatu wilayah. Biasanya untuk suatu jaringan LAN akan memiliki satu *gatekeeper.*

Multipoint Control Unit atau dikenal dengan MCU berguna untuk mengatur negosiasi antar terminal-terminal yang saing terhubung dengan jaringan VoIP. *Multipoint Control Unit* digunakan pada jaringan VoIP yang memiliki setidaknya 3 terminal ataau lebih.

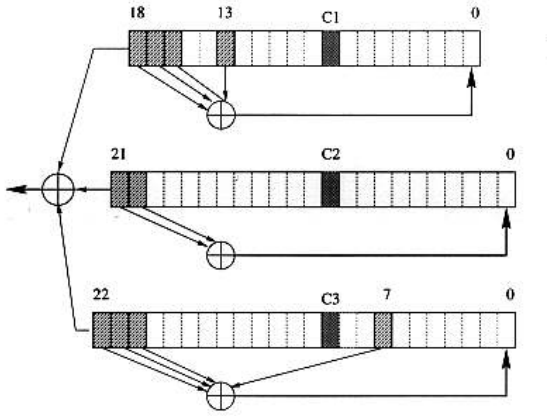
Gateway, *gatekeeper*, dan *Multipoint Control Units* secara logik merupakan suatu perangkat yang saling berdiri sendiri. Tetapi secara fisik dapat diimplementasikan sebagai satu perangkat

3. ALGORITMA A5

Algoritma A5 adalah algoritma stream chipper yang digunakan untuk melakukan dekripsi dan enkripsi pada jarinagan GSM (*Group Special Mobile)* untuk wilayah Amerika Serikat dan Eropa.

Paket data yang berisi pembicaraan jaringan GSM aka dikirimkan tiap 4,6 mili detik dengan panjang paket sebesar 228 bit. Untuk tiap satu pembicaraan tersebut akan memiliki satu *session key*.

Algoritma A5 terdiri atas 3 *linear feedback shift register* (LFSR) yang memiliki panjang 19,22, dan 23 bit.



Gambar 2 LFSR algoritma A5

Tiap bit yang berada pada posisi paling kanan pada tiap-tiap LFSR diberi nama sebagai bit ke-0.

Untuk LFSR pertama, ketukan dikenakan pada bit ke-13, ke-16, ke 17, dank ke-18. Untuk LFSR ke-2, ketukan dikenakan pada bit ke-20 dan ke-21. Untuk LFSR ke-3 ketukan dikenakan pada bit ke -7 , ke-20, ke-21, dank ke-22.

Pada tiap satu *clocked*, tiap bit-bit ketukan yang dimiliki oleh masing-masing LFSR dilakenakan operasi XOR. Hasil operasi tersebut akan disimpan pada bit ke-0 untuk tiap LFSR.

4. ANCAMAN KEAMANAN VoIP

Ada beberapa ancaman terhadap keamann VoIP, yaitu ancaman terhadap perangkat jaringan VoIP dan terhadap pengguna aplikasi VoIP. Ancamaan terhadap perangkat jaringan VoIP dapat berupa perusakan terhadap perangkat jaringan tersebut. Hal ini dapat diatasi dengan melakukan pengamanan terhadap perangkat jaringan tersebut secara fisik. Ancaman terhadap pengguna dapat berupa kegiatan *eavesdropping* dan pencurian identitas pengguna layanan VoIP.

Dari dua hal tersebut, ancaman terhadap pengguna jaringan VoIP merupakan ancaman yang harus memperoleh tindakan yang serius, karena menyangkut keamanan data dan paket suara yang dikirimkan melalui jaringan.

Salah satu hal yang mendapat perhatian penting adalah kegiatan *eavesdropping* terhadap paket suara yang dikirimkan melalui jaringan VoIP. Kegiatan ini dapat dilakukan dengan memanfaatkan ARP *sniffing* terhadap jaringan yang dilalui oleh paket suara VoIP tersebut. Dengan memanfaatkan teknik ARP *sniffing* , penyerang dapat mencuri paket data yang sedang dikirim dari dari terminal pengirim ke terminal penerima .Hal ini tentunya akan sangat merugikan pengguna layanan ini jika pembicaraan yang sedang dilakukan dapat didengar oleh pihak yang tidak bertanggung jawab.

5. PENERAPAN ALGORITMA A5 PADA JARINGAN VOIP

Untuk mengatasi permasalah *eavesdropping* yang dilakukan oleh pihak yang tidak bertanggung jawab, salah satu kegiatan yang dapat dilakukan adalah dengan melakukan kegiatan enkripsi terhadap paket suara yang dikirim melalui jaringan VoIP tersebut. Salah satu enkripsi yang dapat dilakukan adalah dengan memanfaatkan algoritma stream chipper A5.

Penganamanan dilakukan dengan memanfaatkan algoritma stream chipper A5 dikarenakan paket suara yang dikirim melalui jaringan VoIP berupa paket datagram yang lebih mementingkan pengiriman data yang *real time* dengan keterlambatan data yang relative kecil.

Secara garis besar paket VoIP berupa paket-paket *RTP datagram* yang memiliki panjang sekitar lebih dari 40 byte. Untuk tiap paket *RTP datagram* terdiri dari *IP header, UDP header, RTP header,* dan *RTP payload* yang merupakan data suara yang akan dikirimkan.

IP HEADER	UDP HEADER	RTP HEADER	RTP PAYLOAD
20 bytes	8 bytes	12 bytes	n bytes

Gambar 3 *RTP datagram*

Enkripsi A5 tidak dilakukan pada keseluruhan paket,

tetapi hanya terhdap bagian *RTP payload* saja. *RTP payload* tersebut merupakan data suara yang akan dikirim. Hal ini dilakukan dengan tujuan untuk mempermudah ketika melakukan pembacaan paket oleh terminal penerima paket . Disamping itu, dengan melakukan pengenkripsian hanya pada bagian *RTP payload* saja maka tidak dibutuhkan pengembangan arsitektur VoIP yang baru. Arsitektur dan perangkat VoIP yang digunakan dapat memanfaatkan perangkat dan arsitektur yang sudah ada. Perubahan dibutuhkan pada bagian *application layer* baik pada sisi terminal penerima dan terminal pengirim. Hal ini dikarenakan , pada bagian tersebut kegiatan pengenkripsian dan pendekripsian terhadap *RTP payload* dilakukan.

Pengenkripsian dan pendekripsian dilakukan pada *application layer*. Pengenkripsian dilakukan pada pada *application layer* yang terdapat pada terminal pengirim dan pendekripsian dilakukan pada *application layer* milik terminal penerima.

Sebelum data suara dikirim dengan memanfaatkan datagram, data suara tersebut dipecah-pecah menjadi paket-paket kecil. Ketika dilakukan pembentukan bagian *RTP payload* pada paket *RTP datagram,* bagian tersebut terlebih dahulu akan dienkripsi dengan memanfaatkan algoritma enkripsi *stream chipper* A5. Setelah bagian *RTP payload* tersebut dienkripsi, bagian tersebut kemudian akan dienkapsulasi dengan *RTP header*, *UDP header*, dan terakhir *IP header* sehingga terbentuk paket *RTP datagram* yang lengkap.

Paket yang telah terenkripsi tersebut dikirimkan melalui jarinagan VoIP. Jika antara terminal pengirim dengan terminal penerima terhubung dengan jaringan PSTN, maka penysuaian dapat dilakukan pada bagian *gateway* atau pada terminal yang terhubung dengan jaringan PSTN. Jika penyesuaian dilakukan pada bagian *gateway*, maka dibutuhkan suatu *gateway* yang mampu untuk melakukan dekripsi dan enkripsi terhadap paket data yang dikirim. Namun, hal ini tentunya akan membahayakan terhadap paket data yang dikirimkan setelah melalui *gateway* tersebut karena enkripsi dilakukan pada hanya sampai *gateway* saja. Jika penyesuaian dilakukan pada terminal yang terhubung dengan jaringan PSTN maka dibutuhkan terminal yang mampu melakukan proses enkripsi dan dekripsi. Apabila antara terminal pengirim dan terminal penerima hanya dihubungkan dengan jaringan WAN saja,pendekripsian data hanya dilakukan pada sisi terminal saja.

Setelah paket *RTP datagram* diterima oleh terminal penerima, maka paket tersebut diambil bagian *RTP payload*-nya untuk kemudian di dekripsi dengan memanfaatkan algoritma dekripsi A5. *RTP payload* yang telah didekripsi tersebut kemudian akan digabungakan menjadi data suara utuh. Data suara yang telah digabungkan tersebut kemudian akan didengar oleh terminal penerima sebagai suatu pesan suara.

Ada beberapa kesulitan yang akan muncul ketika menerapkan algoritma *stream chipper* A5 pada paket data suara milik VoIP. Kesulitan tersebut muncul karena perbedaan antara karaktereistik antara paket data pada jaringan GSM dengan paket data milik jaringan VoIP. Untuk tiap paket data pada jaringan GSM memiliki panjan sebesar 228 bit sedangkan panjang paket untuk tiap satu packet data VoIP memiliki panjang yang berbeda dari pada paket data milik jaringan GSM.

Karena yang mengalami proses enkripsi dan dekripsi hanya dikenakan pada bagian *RTP payload* saja, maka yang patut diperhatikan dalam mekanisme pengenkripsian dan pendekripsian paket data VoIP hanya pada bagian panjang data yang dimiliki oleh bagian *RTP payload* saja. Jika panjang data yang dimiliki oleh *RTP payload* setara dengan panjang paket data milik jaringan GSM, yaitu sebesar 228 bit tentunya teknik pengenkripsian dan pendekripsian data tidak akan mengalami perubahan. Akan tetapi, jika panjang data pada bagian *RTP payload* lebih besar atau lebih kecil maka dibutuhkan penyesuaian terhadap teknik pengenkripsian dan pendekripsian Penyesuaian tersebut dapat dilakukan dengan menambahkan dummy bit untuk tiap tahapan enkripsi bagian *RTP payload.*

4. HASIL PEMBAHASAN

4.1 Kelebihan Pemanfaatan Algoritma A5 pada Jaringan VoIP

Dengan memanfaatkan algoritma A5 maka tingkat keamanan terhadap paket data yang dikirim melalui jaringan VoIP dapat ditingkatkan. Hal ini disebabkan karena paket-paket data yang dikirimkan adalah paket-paket yang telah terenkripsi dengan memanfaatkan algoritma A5. Hal ini tentunya akan mempersulit tindakan *eavesdropping* yang mungkin dilakukan terhadap jaringan VoIP.

Namun pengamanan ini tentunya hanya berlaku untuk melakukakan pengamanan terhadap isi tiap-tiap paket yang dikirimkan saja. Ancaman lain seperti pencurian paket yang dilakukan oleh pihak yang tidak memiliki otoritas terhadap paket tentunya masih dapat dilakukan.

4.2 Kekurangan Pemanfaatan Algoritma A5 pada Jaringan VoIP

Permasalahan yang dapat muncul yang disebabkan karena penggunaan algoritma *stream chipper* A5 pada jaringan VoIP dapat dibedakan menjadi dua bagian

1. Permasalahan terhadap sistem VoIP
2. Permaslahan terhadap algoritma A5

Salah satu permaslahan penting yang menjadi permasalahan sistem VoIP adalah mengenai permasalahan *delay* paket VoIP yang dikirimkan melalui jaringan VoIP tersebut. Hal ini dikarenakan permaslahan *delay* pengeiriman paket akan mempengaruhi kualiatas suara yang diterima oleh terminal penerima paket.

Ada beberapa delay yang mungkin terjadi pada pengiriman paket data yaitu berupa *delay* yang terjadi akibat transmisi (*propagation delay)*, *delay* akibat proses peletakan bit ke dalam *circuit(serialization delay)*, *delay* yang terjadi pada saat proses paketisasi digital (*packetization delay)*, *delay* akibat menunggu paket samapi dilayani (*queuing delay)*, *delay* akibat adanya buffer untuk mengatasi *jitter(jitter delay)*, dan *delay* yang terjadi ketika proses *coding*, *compression*, *decompression*, serta *decoding (processing delay).* Dengan melakukan penambahan proses yaitu proses penenkripsian dan pendekripsian pada masing-masing terminal, waktu yang dibutuhkan untuk melakukan pengiriman satu paket data secara otomastis akan meningkat. Hal tentunya akan mengakibatkan penurunan terhadap kualitas suara yang dihasilkan.

Disamping permasalahan pada sistem VoIP, permasalahan lain yang mungkin muncul adalah permasalahan mengenai kelemahan yang dimiliki oleh algoritma *stream chipper* A5. Algoritma A5 memiliki beberapa kelemahan yang dapat digunakan untuk melakukan kriptoanalisis terhadap paket data yang dikirimkan. Usaha *eavesdropping* masih dapat dilakukan terhadap paket data yang dikirim melalui jaringan VoIP meskipun akan membutuhkan waktu tambahan untuk melakukan kriptoanalisis terhadap paket data yang dikirim tersebut.

5. KESIMPULAN

Untuk menjaga keamanan paket data VoIP dapat dilakukkan dengan melakukan enkripsi terhadap paket data tersebut. Salah satu algoritma yang dapat digunakan untuk melakukan enkripsi adalah dengan memanfaatkan algoritma enkripsi *stream chipper* A5. Dengan memanfaatkan teknik enkripsi ini, keamanan paket data yang dikirim dapat ditingkatkan sehingga mempersulit kegiatan *eavesdropping* terhadap paket data tersebut. Akan tetapi, tindakan pengenkripsian ini tidak dapat menjamin ancaman kemanan lainnya, seperti pencurian terhadap paket VoIP tersebut. Disamping hal tersebut, kekurangan yang muncul adalah *delay* paket akan semakin meningkat yang berkibat pada menurunnya kualitas suara yang dihasilkan sistem oleh VoIP tersebut. Kelemahan yang dimiliki oleh algoritma A5 juga dapat menjadi celah keamanan yang dapat dieksploit untuk melakukan kegiatan kriptoanalisis terhadap paket data.

DAFTAR REFERENSI

[1] Munir, Rinaldi, *Kriptografi*, Program Studi Teknik Informatika STEI ITB, 2006.

[2] Iskandarsyah, M., *Dasar-Dasar Jaringan VoIP*, IlmuKomputer, 2003.

[3] J. Downey, John, *Understanding VoIP Packet Sizing and Traffic Enginering*, Cisco System, 2005.

[3] http://cryptome.org/a51-bsw.htm.

[4] http:// www.gsm-security.net/faq/gsm-a5-broken-security.shtml