

Tugas EL-695
Keamanan Sistem Informasi

Aspek Keamanan Komunikasi Multimedia H.323

Herry Sitepu
23200048

Program Magister Teknik Sistem Komputer
Jurusan Teknik Elektro
Fakultas Teknologi Industri
Institut Teknologi Bandung
2001

Aspek Keamanan Komunikasi Multimedia H.323

H.323 merupakan standar yang dibuat oleh ITU-T untuk komunikasi multimedia. Pada mulanya H.323 ditujukan untuk aplikasi komunikasi multimedia yang berbasis LAN (*Local Area Network*), namun dalam perkembangannya H.323 juga mempunyai interface ke jaringan lainnya sehingga menjadikannya teknologi yang independent terhadap jaringan yang digunakannya. Banyak perusahaan yang mensupport H.323 dan teknologi tersebut juga telah banyak digunakan pada jaringan komputer saat ini. Hal tersebut membuat H.323 menjadi standar komunikasi multimedia masa depan.

Versi terakhir protokol H.323 tersebut menawarkan banyak fasilitas seperti keamanan, fast-call set-up, servis tambahan dan data support. H.235 adalah standar untuk sistem keamanan bagi H.323 yang memberikan fitur-fitur seperti *authentication*, *integrity*, *privacy*, dan *non-repudiation*.

1. Pendahuluan

H.323 merupakan standar yang dikeluarkan oleh ITU-T (International Telecommunication Union) untuk sistem komunikasi multimedia berbasis paket melalui jaringan yang tidak memberikan jaminan QoS (Quality of Service) seperti jaringan IP. H.235 adalah protokol keamanan bagi H.323 yang memberikan beberapa servis keamanan seperti Authentication, Access control, Non-repudiation, Confidentiality and Integrity bagi keempat channel H.323 (RAS, H.225.0, H.245, dan RTP).

Bab 2 memberikan gambaran mengenai arsitektur protokol H.323. Bagian 2.1 memberikan penekanan terhadap cara pembentukan komunikasi H.323. Arsitektur dasar dari H.323 dan elemen-elemen yang terlibat didalamnya akan dijelaskan pada bagian 2.2. Akhirnya pada bagian 2.3 akan diberikan contoh H.323 call.

Bab 3 menjelaskan dan menganalisa kebutuhan keamanan pada sistem H.323. Pada bab tersebut juga akan dibahas beberapa skenario yang mungkin terjadi dalam komunikasi H.323.

Bab 4 akan memperkenalkan beberapa pilihan keamanan yang ditawarkan oleh H.235, yaitu protokol utama yang menangani isu keamanan dalam sistem H.323

Kemudian akan dibahas pula bagaimana menggunakan pilihan-pilihan tersebut untuk mengamankan H.323 call. Bagian 4.3 akan membahas mengenai analisa mengenai keuntungan dan kerugian berbagai pilihan keamanan yang ada pada H.235 dan sejauh mana H.235 bisa menangani kebutuhan H.323. Pada bagian 4.4 juga dibahas secara singkat mengenai non-repudiation pada H.323.

Bab 5 akan menjelaskan isu-isu yang berhubungan dengan Legal Interception dalam jaringan IP. Beberapa solusi yang mungkin serta kelemahan penggunaan mekanisme legal interception pada lingkungan H.323 juga akan dibahas di bab ini.

2. Sistem H.323 secara singkat

Standar H.323 memberikan fondasi bagi komunikasi audio, video, dan data melalui jaringan IP, termasuk Internet. Setiap produk multimedia yang dibuat oleh berbagai vendor yang mengikuti standar H.323 bisa saling berinteroperasi, sehingga user bisa berkomunikasi tanpa menghawatirkan masalah kompatibiliti.

H.323 bisa digunakan untuk terminal dengan kemampuan audio saja dan juga bisa digunakan pada terminal yang memiliki kemampuan video. H.323 bisa digunakan dalam point-to-point call dan juga bisa digunakan dalam aplikasi multipoint conference. H.323 juga mengatur masalah call control, multimedia management, bandwidth management dan juga interface antar LAN dan interface ke jaringan lainnya (jaringan PSTN, ATM, ISDN, dll).

2.1 Standar-standar H.323

Bagian-bagian sistem H.323 mencakup H.225.0 untuk connection establishment, H.245 untuk control, RTP/RTCP dan audio/video codec, codec tersebut adalah audio codec (G.711, G.723.1, dan G.728) dan video codec (H.261, H.263) yang melakukan kompresi dan dekompresi terhadap media stream. H.235 untuk keamanan, H.246 untuk interoperability dengan circuit switched services dan H.450 untuk servis-servis tambahan. H.323 adalah standar yang memayungi banyak standar-standar ITU lain, yaitu:

Video H.261, H.263 (optional)

Audio G.711, G.722, G.728, G.723, G.729 (mandatory)

Call Signaling H.225.0 (mandatory)

Call Control H.245 (mandatory)

Multipoint H.323 (optional)

Data T.120 (optional)

Security H.235 (optional)

Supplementary Services H.450 (optional)

CS services H.246 (optional)

H.225

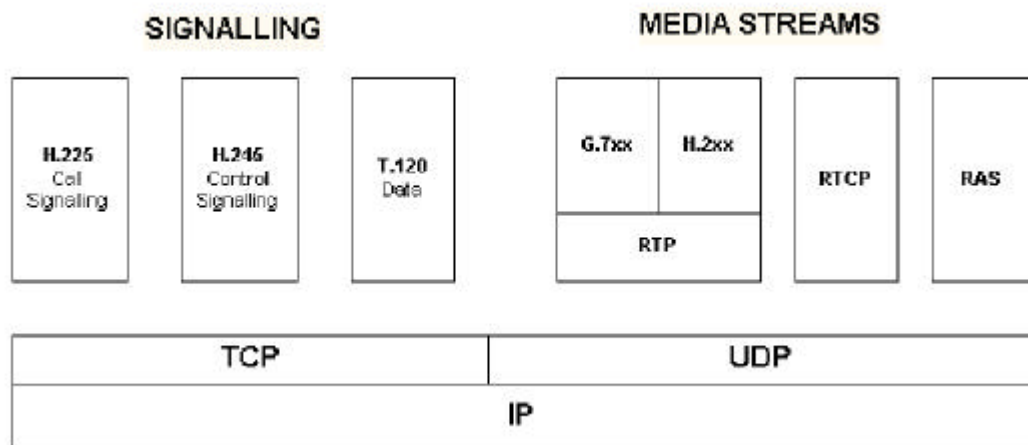
Protokol ini menentukan gatekeeper message (RAS) yang mengatur registration, admision dan status. Call set-up dan termination message dilakukan dengan menggunakan Q.931. H.225 juga menjelaskan penggunaan RTP (Real Time Transport Protocol) sebagai transport bagi stream media.

H.245

Protokol ini mengatur masalah conference control dan capability exchange messages. Capability exchange dibutuhkan agar kedua pihak (atau semua oihak) yang ikut dalam suatu conference bisa membuat persetujuan mengenai media stream apa yang akan digunakan serta berbagai parameter call control lainnya.

H.235

Protokol ini menangani aspek keamanan dan autentikasi bagi channel-channel H.323. Protokol ini akan dibahas lebih lanjut pada bab empat dan bab lima. Media stream dikirimkan dengan menggunakan transport RTP/RTCP. RTP membawa media stream dan RTCP membawa informasi status dan kontrol. Signaling dikirimkan dengan menggunakan reliable transport, yaitu TCP. Gambar 1 dibawah ini memperlihatkan hubungan antara protokol-protokol H.323 dengan protokol RTP/RTCP dan protokol TCP.



Gambar 1. Protokol-protokol H.323 dalam hubungannya dengan protokol transport pada model OSI.

2.2 Arsitektur H.323

Komponen-komponen sistem H.323 adalah Terminal, Gateway, Gatekeeper, Multipoint Controller (MC), Multipoint Processor (MP) dan Multipoint Control Unit

(MCU). Control message dan prosedur-prosedur H.323 digunakan oleh komponen-komponen tersebut untuk saling berkomunikasi.

Setiap terminal minimal memiliki kemampuan audio, sementara video atau data bersifat optional, dalam suatu conference yang bisa berupa point-to-point conference maupun multipoint conference. Gatekeeper bertanggung jawab untuk masalah admission control dan address translation services. MC, MP, dan MCU merupakan komponen yang menangani multipoint conference. Gambar 2 berikut memberikan gambaran dari elemen-elemen yang merupakan bagian dari sistem H.323.

Gatekeeper

Sebuah gatekeeper bertindak sebagai titik pusat bagi semua call didalam zonanya dan menyediakan call control service bagi endpoint yang sudah terdaftar. Sebuah zone H.323 adalah kumpulan terminal, MCU dan gateway yang dimanage oleh sebuah gatekeeper. Gatekeeper bersifat optional dalam sistem H.323, tapi bila gatekeeper tersebut ada maka gatekeeper tersebut menangani fungsi-fungsi call control yang penting seperti: address translation (dari nama alias LAN bagi terminal dan gateway ke alamat IP), admission control dan bandwidth control. Signaling antara masing-masing terminal dan gatekeeper dilakukan melalui koneksi TCP menurut spesifikasi RAS. Fungsi optional pada gatekeeper adalah autorisasi, manajemen bandwidth, servis tambahan seperti billing, directory service dan call management service.

Gateway

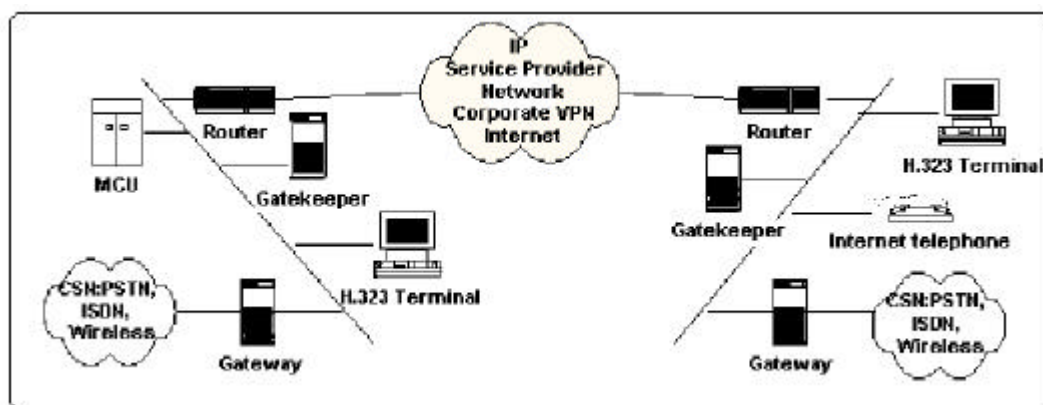
Gateway adalah elemen yang bersifat optional dalam sebuah H.323 conference. Gateway menjadi jembatan ke jaringan yang berbeda (seperti PSTN) dan melakukan konversi signaling dan media dari satu jaringan ke jaringan yang lainnya. Gateway menyediakan fasilitas interworking antara jaringan circuit switched dan jaringan berbasis paket yang menggunakan Q.931 untuk call setup dan call termination.

H.323 Terminal

Sebuah terminal H.323 adalah client endpoint yang mensupport komunikasi dua arah secara real time dengan elemen H.323 lainnya. Sebuah terminal minimal harus mensupport voice (audio codec), signaling (Q.931, H.245, RAS) dan RTP/RTCP (untuk penomoran paket audio dan video).

Jika dalam sebuah sistem H.323 terdapat sebuah gatekeeper, maka terminal H.323 akan berusaha menemukan gatekeeper tersebut untuk selanjutnya mendaftarkan

dirinya sebelum memulai conference. Untuk menemukan dan menentukan alamat transport RAS dari sebuah gatekeeper maka sebuah terminal harus melakukan gatekeeper discovery. Terminal H.323 di rumah yang menggunakan akses dial-up ke ISP tidak usah mendaftarkan diri ke gatekeeper, namun terminal dalam sebuah jaringan korporat mungkin harus dikonfigurasi untuk mendaftarkan dirinya ke gatekeeper pada saat power up.



Gambar 2, Sistem H.323 beserta komponen-komponennya

MCU

Multipoint Control Unit (MCU) mensupport conference antara tiga atau lebih end-point. Sebuah MCU terdiri dari sebuah Multipoint Controller (MC), dan dengan beberapa atau tanpa Multipoint Processor (MP).

MC menangani negosiasi H.245 antar semua terminal untuk menentukan kapabiliti yang dimiliki oleh semua terminal untuk memproses audio dan video. MC juga mengontrol resource yang ada pada sebuah conference dengan menentukan audio dan video stream mana yang merupakan multicast (bila ada). MP menangani media stream. MP melakukan mixing, switching, dan pemrosesan audio, video, dan atau data. MP bisa stand-alone atau terintegrasi kedalam sebuah gateway, gatekeeper, atau terminal.

2.3 H.323 call

Untuk membentuk conference H.323 secara point-to-point maka pertama-tama harus dibuat dahulu koneksi TCP. Pertama-tama harus bentuk dahulu channel Q.931 di port yang sudah diketahui disisi terminal yang menerima call. Call setup message kemudian dipertukarkan seperti yang ditentukan oleh H.225. Jika terminal yang menerima call ternyata menerima call tersebut maka alamat IP dan port pada terminal tersebut yang digunakan untuk mendengarkan koneksi H.245 kemudian dikirimkan ke terminal yang mengawali call dengan menggunakan channel Q.931.

Terminal yang mengawali call kemudian membentuk channel H.245 dengan membuka koneksi TCP dengan menggunakan alamat dan port yang sudah diperoleh sebelumnya. Saat ini channel Q.931 sudah tidak dibutuhkan lagi dan sudah bisa ditutup.

Channel H.245 kemudian digunakan oleh kedua entiti untuk bertukar audio/video capability dan kemudian melakukan penentuan master-slave. Akhirnya ketika data transfer sudah lengkap maka channel H.245 bisa digunakan untuk mengakhiri call. Gambar 3 adalah contoh H.323 call signaling yang digunakan dalam proses call establishment. Kedua endpoint dalam komunikasi tersebut didaftarkan ke Gatekeeper yang sama dan menggunakan Direct Call Signaling. Conference point-to-point pada sistem H.323 membutuhkan lima fase yang dijelaskan secara singkat berikut ini:

Fase A: Call Setup

Call setup dilakukan dengan menggunakan H.225 (Q.931, RAS) call control message. RAS message digunakan jika terdapat sebuah gatekeeper dalam sebuah sistem H.323, bila tidak ada maka yang digunakan hanyalah Q.931. Jika tidak ada gatekeeper maka kedua endpoint bisa berkomunikasi secara langsung. Endpoint 1 (EP1) (calling endpoint) mengirimkan Setup message ke Call Signalling Channel TSAP Identifier pada Endpoint 2 (EP2). Endpoint 2 meresponnya dengan Connect message yang berisi H.245 Control Channel Transport Address untuk digunakan dalam signaling H.245.

Jika terdapat sebuah gatekeeper dalam sistem maka kita memiliki beberapa kemungkinan konfigurasi karena masing-masing endpoint bisa saja terdaftar pada gatekeeper yang sama atau pada gatekeeper yang berbeda, atau mungkin saja satu endpoint terdaftar pada sebuah gatekeeper dan endpoint yang lainnya tidak terdaftar pada gatekeeper manapun. Gatekeeper juga bisa saja bekerja dalam mode Direct Call Signaling atau Routed Call Signaling. Gambar 3 memperlihatkan Sebuah contoh call establishment yang sukses. Kedua endpoint terdaftar pada gatekeeper yang sama dan menggunakan Direct Call Signaling.

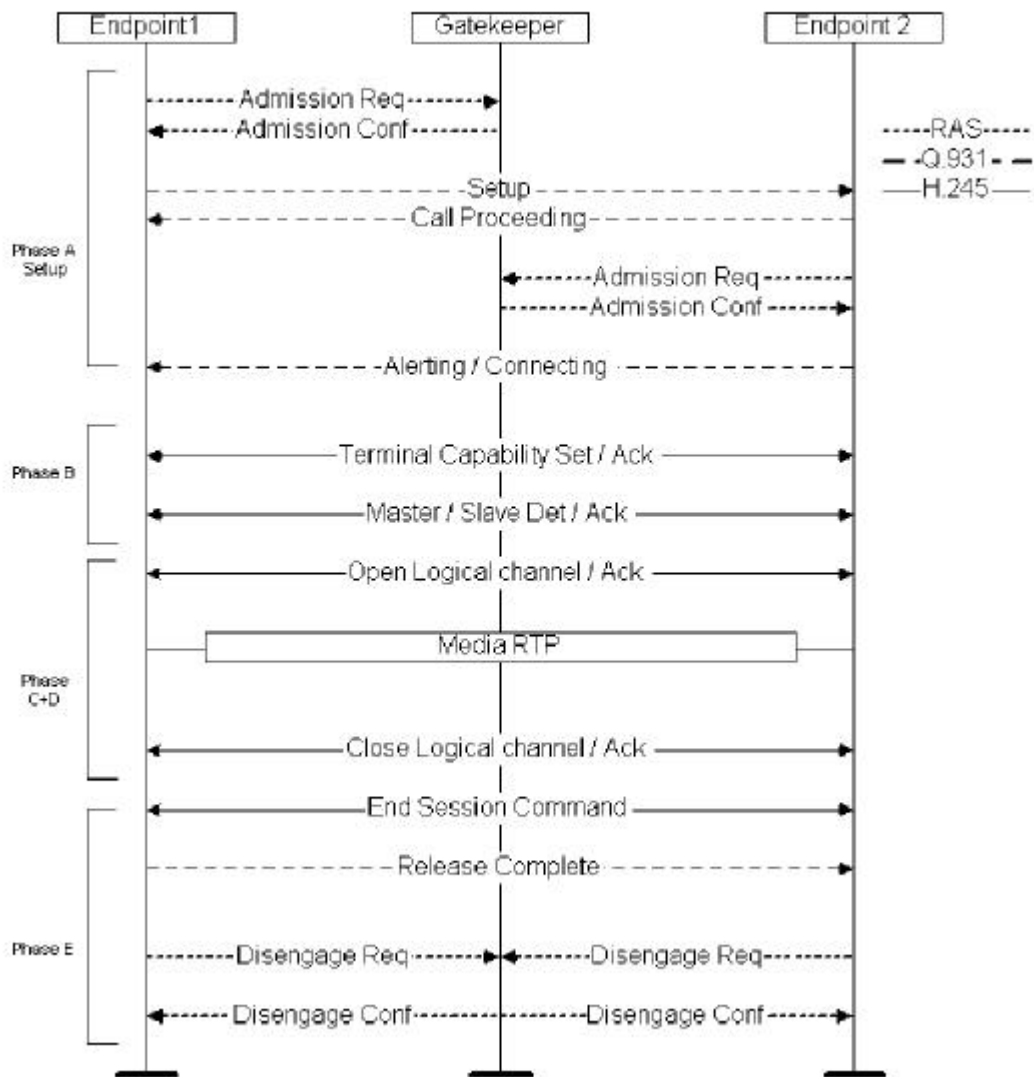
EP1 mengawali pertukaran ARQ/ACF (Admission Request/Admission Confirm) dengan gatekeeper yang kemudian membalasnya dengan Call Signaling Channel Transport Address dari EP 2 dalam message ACF. EP1 kemudian menggunakan alamat tersebut untuk mengirimkan message setup ke EP2 dengan harapan bahwa EP2 akan menerima call dan melakukan pertukaran ARQ/ACF dengan gatekeeper. EP2 menjawabnya dengan Connect message yang didalamnya berisi H.245 Control Channel Transport Address untuk digunakan dalam signaling H.245. Ketika call harus disetup

melalui gateway atau sebuah MCU, maka call setup antara gateway atau MCU dan endpoint mirip seperti endpoint-to-endpoint call setup yang telah dibahas diatas.

Fase B: Initial communication and capability exchange

Setelah kedua sisi bertukaran call setup message, maka kedua EP harus membentuk H.245 Control Channel, yang akan digunakan untuk melakukan capability exchange dan media channel establishment.

Capability pada endpoint system dipertukarkan dengan mengirimkan message H.245 terminalCapabilitySet .



Gambar 3. H.323 call signaling

Prosedur penentuan master slave digunakan untuk menentukan MC mana yang aktif dalam conference apabila kedua endpoint mempunyai MC capability. Penentuan master slave dilakukan dengan mengirimkan message `MasterSlaveDetermination` atau `MasterSlaveDeterminationAck`.

Fase C: Establishment of audio-visual communication

H.245 digunakan untuk membuka logical channel bagi berbagai aliran informasi. Seperti yang tampak pada Gambar 1, audio dan video stream yang dikirimkan saat logical channel setup dalam H.245, dikirimkan dengan menggunakan protokol transport yang unreliable (UDP) dan komunikasi data dikirimkan dengan menggunakan protokol transport yang reliable (TCP). Message `openLogicalChannelAck` akan menerima balasan alamat transport yang sudah ditetapkan oleh endpoint penerima pada logical channel tersebut. Channel pengirim harus mengirimkan aliran informasi dengan menggunakan logical channel ke alamat transport tersebut.

Fase D: Call services

Terdapat beberapa call service yang termasuk kedalam spesifikasi H.323 seperti perubahan bandwidth, status dan ad hoc conferencing.

Call bandwidth mula-mula dinegosiasikan dan diberikan oleh gatekeeper pada saat fase call setup. Saat kapanpun selama call, EP atau gatekeeper bisa meminta pengurangan atau penambahan call bandwidth. Jika perubahan menghasilkan bit rate yang melebihi call bandwidth saat ini maka EP harus meminta perubahan call bandwidth dari gatekeepernya. Perubahan bandwidth akan bermanfaat saat suatu endpoint ingin mengurangi bandwidth untuk suatu periode waktu tertentu sehingga bisa memberikan space bandwidth untuk call lainnya.

Dalam contoh pada Gambar 3 EP1 meminta perubahan bandwidth dengan menggunakan message `Bandwidth Change Request (BRQ)` kepada gatekeeper. Gatekeeper akan menjawabnya dengan mengirimkan `Bandwidth Change Confirm (BCF)`.

Ketika call bandwidth sudah mencukupi kebutuhan tersebut maka EP1 akan menutup logical channel sebelumnya dan kemudian membuka logical channel baru dengan bit rate yang baru, yaitu dengan mengirimkan message `closeLogicalChannel` dan `openLogicalChannel` ke EP2. EP2 kemudian meminta perubahan bandwidth ke gatekeepernya dan kemudian EP2 ke EP1 dengan `openLogicalChannelAck`.

Fase E: Call Termination

Dalam contoh call pada Gambar 3, ketika salah satu EP ingin mengakhiri call maka endpoint tersebut pertama-tama akan menutup semua logical channel bagi video, data dan audio. Kemudian endpoint tersebut mengirimkan endSessionCommand dalam H.245 control channel. Apabila jawaban dari endpoint yang lain telah diterima maka endpoint tersebut akan menutup H.245 control channel. Jika call signaling (Q.931) masih terbuka, maka channel tersebut ditutup dengan menggunakan message ReleaseComplete.

Karena gatekeeper ada dalam sistem, maka gatekeeper harus diberitahukan untuk membebaskan bandwidth dan EP harus diputuskan dari gatekeeper dengan menggunakan message Disengage Request. Gatekeeper kemudian menjawabnya dengan Disengage Confirm. Maka call diakhiri.

3. Aspek Keamanan sistem H.323

3.1 Kebutuhan Keamanan pada H.323

H.323 mencakup banyak protokol dan melibatkan banyak elemen, sehingga isu keamanan didalamnya menjadi cukup kompleks. Ada beberapa kebutuhan keamanan yang umum yang harus dipenuhi – authentication, integrity, confidentiality, non-repudiation dan availability.

3.1.1 Authentication

Setiap user atau mesin yang terlibat dalam sebuah conference call haruslah bisa diautentikasi bahwa ia adalah sebagaimana yang diakuinya. Hal ini merupakan kebutuhan yang sangat penting dalam H.323. tanpa autentikasi maka siapapun atau mesin apapun bisa berpura-pura menjadi orang lain dan ikut dalam sebuah conference call, sehingga tidak bisa dijamin lagi masalah integritas atau non-repudiation.

Tidak hanya endpoint yang harus diautentikasi tapi juga gateway, gatekeeper, dan MCU. MCU dianggap sebagai elemen yang dipercaya ditengah-tengah dua buah atau lebih endpoint. Hal tersebut sangat bergantung pada model trust yang dipercaya atau tidak dipercaya oleh endpoint terhadap “trusted element” tersebut. Akan tetapi jika semua “trusted element” telah diautentikasi maka kita bisa lebih lagi menjamin keamanan.

Autentikasi bisa terjadi pada level end user atau hanya pada level fisik. Autentikasi juga harus dilindungi dari replay attack, confidentiality dan memiliki ketahanan terhadap man-in-the-middle attack.

3.1.2 Integrity

Semua message signaling dan media stream yang dikirimkan oleh berbagai elemen tidak boleh dirusak, karena Cracker akan berusaha melakukan perusakan terhadap informasi yang dikirimkan antara dua entiti A dan B. Sebagai contoh, cracker tersebut bisa saja mengubah kunci enkripsi yang dikirimkan A ke B pada saat sesi tertentu. Sekarang B akan melakukan enkripsi dengan menggunakan kunci yang salah dan data bisa didekripsi oleh hacker sementara A dan B tetap bisa melakukan enkripsi terhadap data dengan menggunakan kunci yang sebenarnya, dengan cara ini A tidak akan menyadarinya dan akan meneruskan percakapannya. Jadi sangatlah penting untuk menerapkan integrity dalam H.323.

3.1.3 Privacy and Confidentiality

Jaringan komunikasi bisa saja di sadap dan kita harus bisa memastikan bahwa semua data yang dikirimkan bisa disembunyikan dari para penyadap. Yang harus dibuat rahasia bukan saja data media stream, tapi juga data signaling. Jadi kita harus menggunakan teknik enkripsi-dekripsi untuk menyembunyikan data dari para penyadap. Jika data paket yang telah dienkripsi di tengah jalan ternyata disadap oleh seseorang maka ia tidak bisa melihat informasi didalamnya tanpa mengetahui algoritma enkripsi yang digunakan dan kunci yang digunakan dalam algoritma tersebut.

3.1.4 Non-repudiation

Non-repudiation adalah suatu mekanisme yang memastikan bahwa seseorang yang ikut dalam sebuah call conference tidak bisa menyangkalinya. Non-repudiation bersifat dua arah, artinya disisi yang lain service provider juga tidak bisa menuntut seseorang untuk membayar biaya call yang ternyata tidak pernah dilakukan oleh orang tersebut.

3.1.5 Availability

Conference call service harus bisa diakses saat dibutuhkan dengan delay yang wajar. Dengan kata lain harus ada mekanisme untuk meminimisasi ancaman Denial of Service (DOS attack). Perusahaan yang menyediakan service harus bisa memastikan level availability tertentu, jika tidak maka ia tidak bisa mendapatkan banyak user. Masalahnya DOS attack ini pada umumnya sangat sulit untuk diatasi.

3.2 Beberapa skenario dalam H.323

Pada bagian ini akan dibahas beberapa trust model dan skenario, analisa ancaman yang mungkin terjadi dan mendiskusikan mekanisme keamanan apa saja yang dibutuhkan untuk mengamankan H.323 call. Bagian ini akan lebih dikonsentrasikan pada authentication, integrity dan confidentiality. Pada bagian yang lain akan dibahas mengenai isu non-repudiation.

3.2.1 *Basic point to point call*

Dalam skenario ini, elemen yang terlibat adalah terminal dan gatekeeper (lihat Gambar 4.). Apabila diasumsikan bahwa tidak ada hubungan trust yang sudah dibuat sebelumnya antar kedua elemen maka dibutuhkan autentikasi untuk memverifikasi endpoint-endpoint. Autentikasi dapat dilakukan pada saat call establishment atau saat pertukaran awal message dalam call control H.245 channel. Pembentukan call antara terminal ke terminal dilakukan dengan menggunakan Q.931. Ketika ada gatekeeper, seperti pada gambar, maka digunakanlah RAS antar gatekeeper untuk berkomunikasi dengan endpoint sehingga gatekeeper bisa memfasilitasi manajemen endpoint. Selain itu gatekeeper bisa menerima permintaan servis dari terminal yang terhubung kepadanya. Metode autentikasi yang digunakan bisa berbasis enkripsi simetrik atau berbasis subscription.

Metode autentikasi berbasis subscription harus dilakukan pada saat ada hubungan dengan terminal atau gatekeeper. Hal tersebut bertujuan untuk membuktikan bahwa orang yang ikut dalam call adalah dia yang sebenarnya, sehingga trust relationship antar dua entiti bisa dibangun. Selanjutnya bisa digunakan metode enkripsi simetrik untuk melakukan autentikasi terhadap message flow selanjutnya.

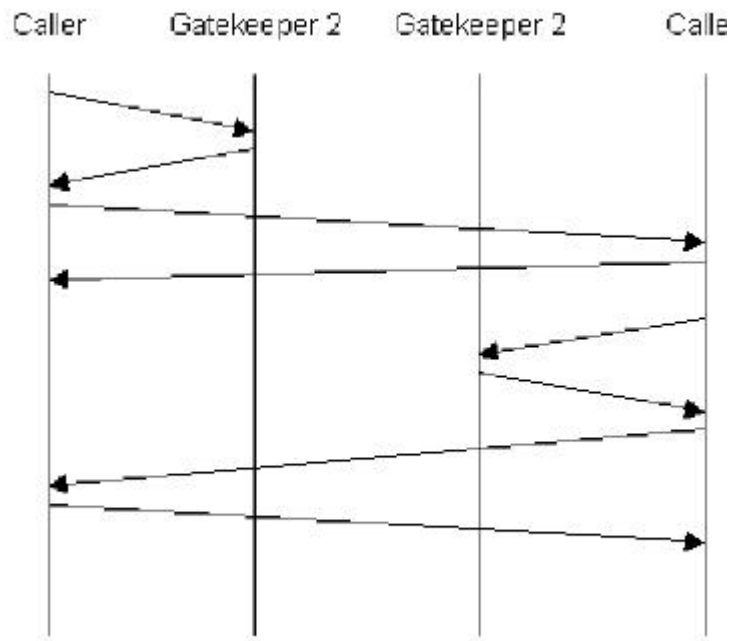
Semua signalling message dan media stream data punya potensi disadap dan dirusak, sehingga mekanisme keamanan seperti digital signature atau enkripsi bisa digunakan untuk memberikan integrity dan confidentiality. Message yang harus dienkripsi adalah Q.931, RAS, H.245, dan RTP.

Karena message dari protokol yang berbeda dijalankan secara berurutan, misalnya message untuk mensetup conference call harus mendahului call control message dan kemudian diikuti dengan media stream, sehingga algoritma dan key dapat dinegosiasikan dan didistribusikan dalam message yang telah datang sebelumnya. Kita akan melihat bagaimana hal tersebut sebenarnya dilakukan dengan menggunakan H.235.

3.2.2 *Multipoint Call*

Dalam multipoint conference call digunakan MCU (Multipoint Control Unit), yang biasanya terdiri dari MC (Multipoint Controller) dan MP (Multipoint Processor). MP digunakan untuk mendistribusikan data pada multipoint conference, prosesnya bisa dilakukan tersentralisasi atau terdesentralisasi. MC digunakan dalam conference control, prosesnya selalu dilakukan terpusat tanpa menghiraukan cara distribusi data yang digunakan.

Dalam skenario ini, call establishment selalu dilakukan melalui MCU. End point yang ingin ikut dalam conference call harus diautentikasi dahulu oleh MCU agar bisa diterima dalam call tersebut.



Gambar 4 Komunikasi melalui gatekeeper

Algoritma enkripsi dan kunci juga harus selalu dikomunikasikan dari MCU ke endpoint. Jadi multipoint conference call memiliki kebutuhan keamanan yang mirip dengan point-to-point call. Perbedaannya adalah masalah trust relationship antar elemen yang harus dibangun melalui MCU.

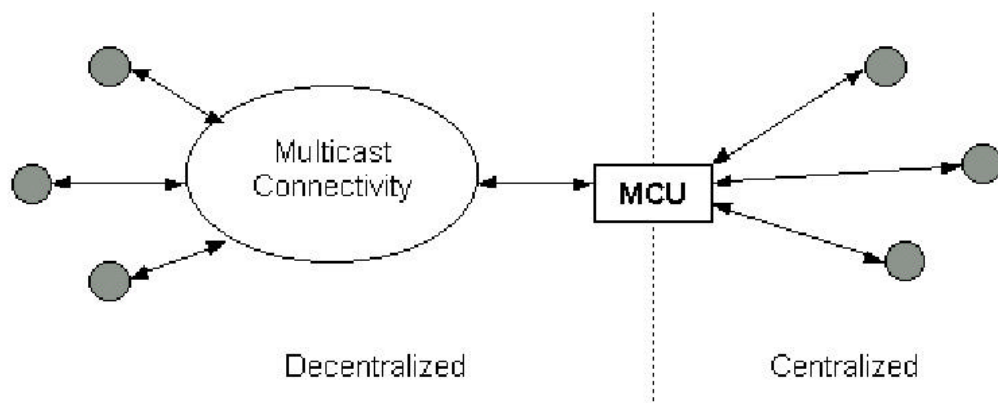
3.2.3 *Penggunaan Gateway*

Dalam situasi yang sebenarnya, dua atau lebih terminal yang terlibat dalam conference call bisa saja jauh terpisah secara fisik. Terminal-terminal tersebut dapat

berada pada jaringan yang berbeda dengan protokol yang berbeda. Jadi dalam kasus ini dibutuhkan gateway. Untuk mengatasi kebutuhan tersebut maka terdapat berbagai protokol yang menghubungkan jaringan PSTN (Public Switched Telephone Network) dengan jaringan IP atau antara jaringan IP dengan LAN. Selain itu terdapat pula gateway seperti firewall dan proxy yang bisa digunakan oleh jaringan korporat atau jaringan kampus untuk melindungi jaringan internalnya dari serangan orang luar. Bagaimanakah aspek keamanan yang ada bila terdapat gateway dalam sistem. Pertanyaan pertama yang perlu kita jawab adalah apakah kita akan membutuhkan hop-by-hop security atau end-to-end security.

Jika yang dibutuhkan adalah end-to-end security maka semua gateway dan MCU sepanjang jalur komunikasi harus diautentikasi, dan privacy dapat dijamin jika semua elemen telah terbukti terlindungi dari serangan man-in-the-middle-attack.

Jika yang dibutuhkan hanyalah hop-by-hop security maka kita hanya dapat memastikan keamanan komunikasi antar elemen yang berdekatan satu dengan yang lainnya sepanjang jalur komunikasi, sementara itu komunikasi yang jauh dari gateway dianggap tidak aman. Isu lainnya yang terjadi dalam skenario ini adalah ketika channel H245 yang telah dienkripsi tersebut melewati firewall atau proxy. Firewall atau proxy harus melakukan dekripsi, mengubahnya, dan melakukan enkripsi kembali protokol. Isu tersebut menjadi sangat penting karena protokol H.245 membawa informasi nomor port yang telah ditentukan secara dinamik.



Gambar 5. Komunikasi multipoint

3.3 Non-repudiation

Seperti telah disebutkan sebelumnya bahwa non-repudiation mencegah seseorang menyangkali bahwa dirinya pernah ikut dalam sebuah conference call. Dan pada saat yang bersamaan kita juga harus melindungi end user agar tidak dituntut oleh service

provider untuk membayar call yang tidak pernah diikutinya. Aspek pada H.323 ini belum banyak dipelajari secara ekstensif untuk melihat beberapa beberapa solusi potensial. Karena aspek tersebut banyak berhubungan dengan accountability maka salah satu solusi dapat dihubungkan dengan sistem AAA (Authentication, Authorization, and Accounting). Berikut ini adalah pengantar singkat sistem AAA, diskusi yang lebih mendalam terhadap solusi yang mungkin bagi syarat keamanan dalam H.323 akan dibahas pada bab berikutnya. AAA merupakan singkatan *Authentication, Authorization, and Accounting*.

≪≪ Authentication adalah bagaimana memverifikasi identitas yang diakui oleh seseorang.

≪≪ Authorization adalah bagaimana menentukan apakah hak tertentu bisa diberikan pada seseorang. Sebagai contoh hak tersebut bisa berupa akses ke suatu resource.

≪≪ Accounting adalah bagaimana mengumpulkan data-data mengenai konsumsi resource yang bertujuan untuk melakukan analisa trend, perencanaan kapasitas, billing, auditing, dan alokasi biaya.

Proposal untuk protokol dan sistem AAA sedang dikembangkan oleh IETF, yaitu oleh *AAA working group*. Tujuan *AAA working group* adalah untuk menentukan satu protokol yang mengimplementasikan authentication, authorization and accounting dan seumum mungkin agar bisa digunakan untuk banyak aplikasi.

Biasanya user mempunyai *home organization*, atau *home domain*, dimana dia memiliki perjanjian servis. Home organization ini memberikan servis ditempat dimana user tersebut biasanya berada. Ketika user berpindah tempat dan ingin mengakses servis tersebut, sementara dia telah berada di *foreign domain* (organisasi yang bukan merupakan *home domain* nya), maka dibutuhkan suatu mekanisme untuk mengautentikasi user dan memberi otorisasi untuk menggunakan resource tersebut. Accounting adalah mekanisme yang menangani masalah billing, sehingga accounting membutuhkan syarat non-repudiation.

4. Mengamankan H.323

Saat ini H.235 merupakan rekomendasi utama yang mencakup isu-isu keamanan H.323. Rekomendasi ini menjelaskan perbaikan pada kerangka kerja H.3xx-Series Recommendation agar memasukkan servis keamanan seperti Authentication dan Privacy (enkripsi data). Protokol tersebut menjelaskan bagaimana infrastruktur keamanan dan teknik privacy tertentu yang bisa digunakan oleh H.3xx-Series pada terminal multimedia. Jadi pada bab ini kita akan lebih berfokus pada rekomendasi H.235 beserta dengan berbagai aspek yang menyertainya.

4.1 Implementasi dan pilihan keamanan H.235

H.235 menyediakan pilihan keamanan sebagai berikut:

4.1.1 Authentication

Authentication adalah mekanisme untuk menentukan identitas endpoint yang ikut dalam sebuah conference. Authentication tersebut bisa digunakan pada level user atau pada level mesin. Dalam H.235, authentication dapat diperoleh dengan dua metode utama- berbasis enkripsi simetrik yang tidak membutuhkan kontak awal antar entiti; atau autentikasi berbasis subscription, yang mensyaratkan kedua bagian memiliki password atau sertifikat yang digunakan bersama. Sebenarnya ada pilihan ketiga untuk memperoleh authentication, yaitu dengan menggunakan protokol keamanan yang terpisah seperti TLS atau IPSEC. Paper ini tidak membahas masalah TLS dan IPSEC.

Dengan menggunakan metode yang pertama maka kita bisa memberikan authentication penuh di level user. Hal ini berbeda dengan cara kedua yaitu dengan menggunakan kunci rahasia bersama yang telah dibangkitkan sebelumnya dan algoritma yang telah disetujui untuk melakukan autentikasi komunikasi yang akan dilakukan bahwa endpoint adalah dirinya yang telah diautentikasi sebelumnya.

Ada beberapa cara untuk melakukan pertukaran kunci rahasia yang digunakan dalam H.235, cara tersebut digunakan juga untuk pertukaran media session key untuk enkripsi. Cara tersebut akan dibahas secara singkat diakhir bagian ini. Misalkan kita mengambil proses autentikasi endpoint-gatekeeper sebagai contoh. Dengan mekanisme gatekeeper harus mempunyai hubungan kriptografik dengan end-point sehingga bisa memastikan bahwa endpoint tertentu yang telah terdaftar sebelumnya adalah endpoint yang sama dengan endpoint yang mengirimkan RAS message. Pertukaran Diffie-Hellman harus terjadi bersamaan dengan message GRQ dan GCF dan kunci rahasia bersama digunakan pada message RRQ/URQ berikutnya dari terminal ke gatekeeper.

Pada autentikasi berbasis subscription kita mengasumsikan bahwa setiap endpoint telah mempunyai identifier yang unik. Metode ini mempunyai tiga variasi, yaitu:

☞ Password-based dengan menggunakan enkripsi simetrik

Gambar 6 memperlihatkan format token dan pertukaran message untuk melakukan autentikasi jenis ini. Protokol ini berbasis 5.2.1 dari ISO/IEC 9798-2. Diasumsikan bahwa identifier dan passwordnya dipertukarkan pada saat subscription. Panjang kunci enkripsi adalah N octet (ditandai oleh AlgorithmID), dan dibentuk sebagai berikut:

?? Jika panjang password = N, Kunci = password;

?? Jika panjang password < N, maka kunci dipadding dengan nol;

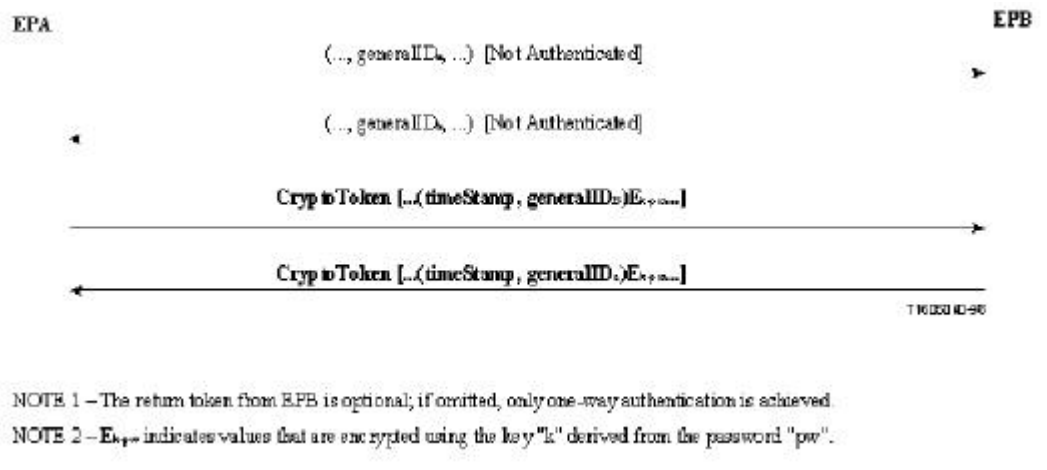
?? Jika panjang password > N, maka N octet pertama ditetapkan sebagai kunci, octet N +M dari password kemudian di-XOR dengan octet Mmod(N) (untuk semua octet diatas N). Jadi “kelebihan” octet pada password secara berulang di folded back dan di-XOR kembali dengan kunci.

≠≠ Password dengan hashing

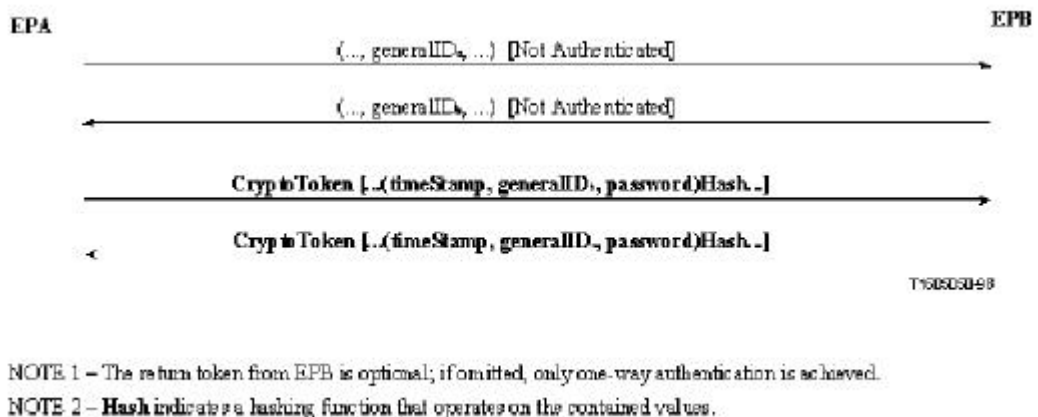
Gambar 7 memperlihatkan format token dan pertukaran message yang diperlukan untuk melakukan autentikasi jenis ini. Protokol ini berbasis 5.2.1 dari ISO/IEC 9798-4. Diasumsikan identifier dan passwordnya di pertukarkan pada saat subscription.

≠≠ Certificate-based dengan signatures

Certificate adalah data tertentu yang berhubungan dengan keamanan yang dikeluarkan oleh lembaga tertentu yang dipercaya. Certificate digunakan untuk memberikan integrity pada data dan autentikasi terhadap asalnya data tersebut. Untuk otorisasi dengan menggunakan public key certificate maka endpoint diharuskan memberikan digital signature dengan menggunakan public key-nya.

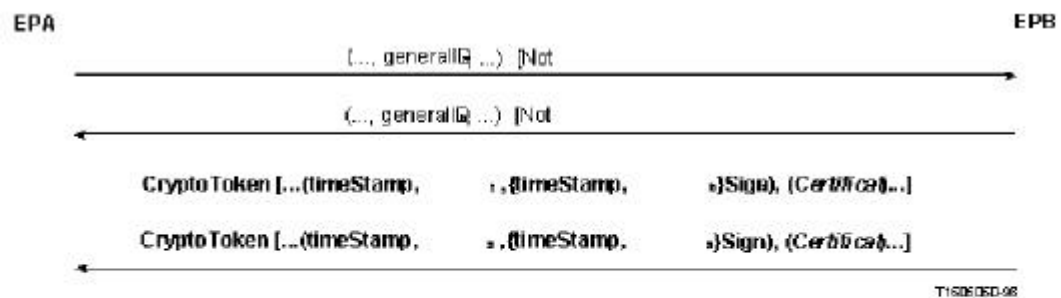


Gambar 6.



Gambar 7

Gambar 8 memperlihatkan format token dan pertukaran message yang diperlukan untuk melakukan autentikasi dengan metode certificate-based. Protokol ini berbasis 5.2.1 dari ISO/IEC 9798-3. Diasumsikan bahwa identifier dan certificate diassign/dipertukarkan saat subscription.



NOTE 1 – The return token from EPB is optional; if omitted, only one-way authentication is

NOTE 2 – A "payment" type certificate may be optionally included by the EPA

NOTE 3 – Sign indicates a signing function (from associated certificate) performed on the contained

Gambar 8.

4.1.2 Integrity

H.235 menggunakan mekanisme kriptografik dengan hash function untuk melindungi integritas isi paket. Yang dienkrpsi hanyalah nilai checksum dari paket, dan bukan seluruh data payload. Hal ini bertujuan untuk mengurangi processing load untuk melakukan enkripsi.

4.1.3 Privacy and confidentiality

Rekomendasi H.235 memberikan pilihan untuk menggunakan beberapa mekanisme enkripsi. Tanpa mengetahui algoritma enkripsi dan juga kunci enkripsi yang digunakan maka orang yang tidak berwenang tidak akan bisa melihat isi informasi sehingga isi data bisa dirahasiakan (confidentiality). Dalam memilih algoritma enkripsi yang akan digunakan maka pertimbangan yang harus diambil merupakan *trade-off* antara masalah prioritas antara level keamanan yang dingin dicapai dan kompleksitas perhitungan enkripsi. Jadi sebetulnya pertimbangan pemilihan algoritma enkripsi lebih difokuskan kepada kebutuhan keamanan dari sistem itu sendiri.

4.1.4 Pertukaran kunci

Hal ini adalah bagian penting lainnya dalam rekomendasi H.235. Pertukaran kunci adalah inti yang sangat penting dalam autentikasi dan enkripsi untuk mendapatkan integrity dan privacy dari komunikasi. Ada tiga kategori pertukaran kunci yang digunakan di H.235:

≡≡ Out-of-band

Pertukaran kunci dengan menggunakan cara ini bisa dilakukan dengan melalui e-mail atau diberitahukan melalui telepon. Prosesnya dilakukan diluar protokol H.323. Jika ada hubungan langsung seperti LAN maka metode ini dianggap yang paling aman. Tapi jika tidak maka kunci dikirimkan melalui channel yang tidak aman seperti e-mail atau jalur telepon sehingga bisa saja ditengah jalan kunci tersebut disadap.

≡≡ Diffie-Hellman

Pertukaran kunci dengan metode ini akan menghasilkan kunci rahasia dan algoritma bersama yang dipilih diakhir prosesnya. Jika metode ini menghasilkan kunci yang lemah untuk algoritma tertentu maka kedua sisi yang berkomunikasi harus memutuskan hubungannya dahulu dan kemudian membentuk hubungan yang baru dengan kunci yang baru pula.

≡≡ Oakley dan ISAKMP

Oakley key Determination Protocol menggunakan teknik Diffie-Hellman yang telah dimodifikasi dalam membentuk session key pada Internet host dan router. Cara ini bisa saja digunakan bersama dengan ISAKMP (*Internet Security Association and Key Management Protocol*). ISAKMP adalah metode pertukaran key yang digunakan di Internet.

4.2 Menerapkan H.235 pada H.323

4.2.1 Keamanan dalam call establishment

Dua aspek yang penting dalam masalah kewanamanan pada saat fase call establishment, yaitu call authentication dan call authorization. Call connection channel harus dilakukan dengan menggunakan TLS untuk TSAP (message Q.931) dan menggunakan IPSEC untuk message RAS. Sebagai contoh jika kita menggunakan IPSEC, maka sebelum message RAS pertama dikirimkan dari endpoint ke gatekeeper, maka daemon ISAKMP/Oakley pada endpoint akan melakukan negosiasi security service yang akan digunakan pada paket yang melalui well-known port milik RAS channel. Setelah negosiasi selesai maka RAS channel dapat bekerja sama seperti kondisi jika channelnya belum diamankan.

Jika ada gatekeeper dalam topologi maka endpoint harus mengautentikasi dirinya sendiri ke gatekeeper melalui protokol RAS. Hal ini bisa dilakukan dengan menggunakan metode autentikasi yang telah dijelaskan pada bagian 4.1.1. Setelah call authentication, kedua entiti yang terlibat dalam call harus menegosiasikan mode secure yang digunakannya untuk call control channel.

Endpoint H.323 yang menerima message SETUP dengan *h245SecurityCapability* harus menjawab dengan *h245SecurityMode* didalam message CONNECT. Jika endpoint tersebut tidak memiliki capability seperti yang dinegosiasikan maka terminal tersebut bisa menolak koneksi dengan mengirimkan *Release Complete* dengan kode kesalahan *SecurityDenied*. Jika terminal yang mengawali call menerima message CONNECT dari terminal yang menerima call tetapi tidak memiliki security mode yang disetujui oleh terminal itu maka ia bisa mengakhiri call dengan *Release Complete* dengan kode kesalahan *SecurityDenied*.

Jika calling terminal menerima message CONNECT tanpa security capability maka ia bisa memutuskan call dengan *Release Complete* dengan kode kesalahan *undefinedReason*. Jika calling terminal menerima *h245Security mode*, maka ia akan membuka dan menjalankan channel H.245 dalam mode secure yang telah disepakati. Jika terjadi kesalahan dalam mensetup H.245 ke mode secure seperti dalam proses diatas maka akan menghasilkan protocol error dan koneksi akan segera diakhiri.

4.2.2 Keamanan Call Control

Autentikasi dan negosiasi keamanan harus terjadi setelah mode aman untuk fase call establishment selesai dibentuk dan siap untuk melakukan pertukaran message H.245 berikutnya. Kunci harus dipertukarkan agar bisa mengaktifkan enkripsi untuk integrity dan privacy.

Setelah H.245 bekerja dalam secure mode, mirip dengan H.225, maka negosiasi harus dilakukan untuk menentukan security mode yang akan digunakan untuk media stream. Algoritma enkripsi dan kunci enkripsi harus dipertukarkan diantara kedua terminal dan hal ini bisa dilakukan dengan berbasis per logical channel, sehingga beragam media channel bisa dienkrpsi dengan menggunakan mekanisme yang berbeda. Misalnya dalam multipoint conference yang terpusat, maka kunci yang berbeda bisa digunakan untuk stream data ke masing-masing endpoint.

Informasi capability dipertukarkan diantara endpoint dengan menggunakan message H.245. Kumpulan capability ini bisa berisi definisi, yang menyatakan parameter keamanan dan enkripsi. Setiap algoritma enkripsi yang digunakan bersamaan dengan

media codec tertentu akan memberikan definisi capability yang baru. Sama seperti capability yang lain, endpoint bisa mensuplai codec yang telah dienkripsi pada saat pertukaran. Setelah pertukaran capability selesai dilakukan, maka endpoint bisa membuka logical channel yang aman untuk media sama seperti yang dilakukan dalam kondisi yang tidak aman. H.245 master-slave digunakan untuk menentukan master entity yang ditujukan untuk operasi channel dua arah dan penanganan konflik lainnya. Penentuan master ini juga dilakukan dengan metode yang secure. Walaupun security mode untuk media stream di set oleh source, akan tetapi yang membangkitkan kunci enkripsi adalah master.

Pembentukan kunci enkripsi ini dilakukan tanpa memperdulikan apakah master ternyata adalah receiver atau source dari media yang dienkripsi. Agar operasi multicast channel bisa dilakukan dengan menggunakan kunci bersama, maka MC (yang juga adalah master) harus membangkitkan kunci. Ketika endpoint membuka media logical channel yang secure, maka mode tersebut harus didefinisikan pada field *OpenLogicalChannel dataType*. Kunci enkripsi semula harus dikirimkan melalui *OpenLogicalChannel* atau *OpenLogicalChannelAck* tergantung pada hubungan master/slave originator dari *OpenLogicalChannel*. *OpenLogicalChannelAck* harus bertindak sebagai konfirmasi dari mode enkripsi yang ditentukan. Jika *OpenLogicalChannel* tidak diterima oleh called terminal, maka akan dikirimkan pesan *dataTypeNotSupported* atau *dataTypeNotAvailable* (kondisi transien) pada field pesan kesalahan yang ada pada message *OpenLogicalChannelReject*.

4.2.3 Keamanan dalam Multipoint conference call

Pada dasarnya isu autentikasi dan privasi pada multipoint call sama dengan yang dilakukan pada point-to-point call, perbedaannya terletak pada MC(U) yaitu sebagai control point utama. MCU menset policy mengenai level autentikasi dan endpoint yang ikut dalam conference bisa dibatasi berdasarkan level autentikasi yang diterapkan oleh MC(U). Endpoint bisa menggunakan perintah *ConferenceRequest/ConferenceResponse* untuk mendapatkan certificate dari partisipan lainnya dari MC(U). MC(U) juga selalu bertindak sebagai master dan yang mensuplai kunci enkripsi bagi partisipan dalam multipoint conference.

Privacy bagi masing-masing source dalam satu session bersama (diasumsikan menggunakan multicast) dapat diperoleh dengan kunci individual atau kunci bersama. Dua mode ini bisa dipilih secara acak oleh MC(U) dan tidak bisa dikendalikan dari endpoint manapun kecuali diperbolehkan oleh MC(U) itu sendiri. Dengan kata lain, kunci

bersama bisa digunakan oleh beberapa logical channel yang dibuka oleh source yang berbeda.

4.2.4 Keamanan media stream

Media stream harus diencode dengan menggunakan algoritma dan kunci yang dinyatakan oleh H.245 channel untuk menjamin privacy dan integrity.

Media session key dimasukkan kedalam *encryptionUpdate* sebagai h235key. Kunci tersebut bisa dilindungi dengan menggunakan salah satu mekanisme dari tiga mekanisme yang mungkin pada saat kunci tersebut dilewatkan diantara dua endpoint.

≪≪ Jika channel H.245 sudah aman, maka tidak diperlukan proteksi lainnya untuk kunci. Key dilewatkan melalui channel yang sudah aman. Digunakan ASN.1 pada *secureChannel*.

≪≪ Jika kunci rahasia dan algoritma dilewatkan melalui channel diluar H.245 channel, maka digunakan shared secret untuk mengenkripsi kunci. Untuk kasus ini digunakan ASN.1 pada *sharedSecret*.

≪≪ Certificate bisa digunakan ketika H.245 channel tidak aman, tapi bisa juga diterapkan pada channel H,245 yang sudah aman. Jika digunakan certificate maka kunci dienkripsi dengan menggunakan public key dan ASN.1 membentuk *certProtectedKey*.

Kapanpun pada saat conference, receiver (atau transmitter) bisa meminta kunci yang baru (*encryptionUpdateRequest*). Hal tersebut diperlukan apabila dicurigai bahwa salah satu logical channel sudah tidak sinkron. Master yang menerima permintaan untuk membarui kunci kemudian akan membangkitkan kunci baru sebagai jawaban permintaan tersebut. Master juga bisa secara asinkron mendistribusikan kunci baru dengan menggunakan message *encryptionUpdate*.

Setelah menerima *encryptionUpdateRequest* maka master harus mengirimkan *encryptionUpdate*. Jika conference adalah multipoint, maka MC (yang adalah master) harus mendistribusikan kunci baru kepada semua receiver sebelum kunci tersebut diberikan pada transmitter. Transmitter data pada logical channel harus menggunakan kunci baru sesegera mungkin setelah menerima message pembaharuan kunci. Transmitter (dianggap bukan master) bisa juga meminta kunci yang baru, sehingga enkripsi bisa terjadi secara independen, per paket.

Header RTP yang berisi payload header tidak perlu dienkripsi. Akan tetapi harus disadari bahwa jika ukuran paket RTP lebih besar dari ukuran MTU (*Maximum*

Transmission Unit) maka apabila ada fragment yang hilang akan menyebabkan paket RTP tidak bisa didekripsi untuk mendapatkan data aslinya.

4.2.5 *Trusted elements*

Dasar authentication (trust) dan privacy ditentukan oleh terminal-terminal pada channel komunikasi. Pada connection establishment channel hal ini bisa terjadi antara caller dan hosting network component. Karena itu, setiap entiti yang merupakan ujung dari H.245 control channel terenkripsi atau setiap tipe logical channel *encryptedData* harus dianggap sebagai elemen yang bisa dipercaya dalam koneksi, bisa termasuk MC(U) dan gateway. Hasil mempercayai elemen bisa memberikan mekanisme privacy (algoritma dan kunci) kepada elemen tersebut. Kita juga bisa memastikan privacy antara dua endpoint hanya jika koneksi antara trusted element bisa dibuktikan terlindungi dari man-in-the-middle attack.

4.3 Analisis

4.3.1 *Perbandingan option pada H.235*

Option-option untuk autentikasi

Dua jenis autentikasi yang digunakan adalah berbasis enkripsi simetris dan berbasis subscription. Enkripsi simetris tidak bisa memberikan autentikasi pada level user tapi metode tersebut tidak memerlukan hubungan apapun terlebih dahulu.

Option-option untuk enkripsi

Enkripsi bisa dilakukan dengan menggunakan protocol yang telah ada dengan algoritma public key dan bisa juga dilakukan dengan menggunakan protokol lainnya seperti IPSEC dan TLS. Jika menggunakan IPSEC atau TLS maka protokol di atasnya tidak perlu khawatir mengenai masalah enkripsi dan bisa menggunakan transparent service.

Managemen kunci

Perbedaan metode yang digunakan dalam managemen kunci terletak pada keragaman kompleksitas dan level keamanannya. Metode Out-of-band memiliki kompleksitas yang paling sedikit tapi memiliki ancaman keamanan yang besar. Metode Diffie-Hellman yang digunakan tanpa autentikasi sangat rentan terhadap man-in-the-middle attack. Oakley key Determination Protocol menghasilkan level keamanan yang paling tinggi tapi dengan kompleksitas yang lebih tinggi pula.

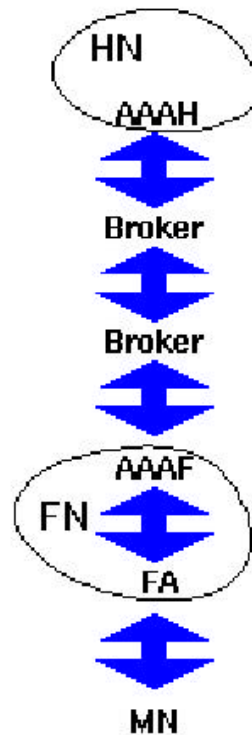
Dalam setiap implementasi, pilihan metode manajemen kunci yang digunakan merupakan trade-off antara level keamanan dan kompleksitas.

4.3.2 Kebutuhan keamanan pada sistem H.323 yang diberikan oleh implementasi H.235

Authentication, integrity dan privacy sudah bisa ditangani oleh H.235 tetapi masalah non-repudiation masih membutuhkan study yang lebih jauh. Jadi ada tiga cara dalam penggunaan H.245 dan H.225: seperti yang digunakan pada standar H.323 v1 yaitu menggunakan koneksi yang terpisah, H.245 tunneling melalui H.225, dan FastStart dalam H.323 v2. Tunneling membutuhkan tambahan keamanan dan bagaimana cara enkripsi channel H.245 bekerja ketika di tunnel melalui H.225 tidak dicakup oleh H.235.

4.4 Non-repudiation

Seperti telah disinggung sebelumnya bahwa H.235 tidak mencakup banyak masalah seputar non-repudiation. Akan tetapi seperti yang sudah disebutkan di awal bahwa paper ini akan membahas beberapa protokol AAA yang bisa digunakan untuk menjawab persoalan tersebut. Aspek penarikan biaya pada AAA dipelajari lebih jauh (Project Ipay) dan juga telah dikembangkan prototipe protokol untuk mengumpulkan informasi biaya dalam Mobile IP. Dalam model tersebut ada lima buah komponen, yaitu buyer, FA, AAAF, Broker, dan AAAH.



Gambar 9. Arsitektur sistem penarikan biaya

Hubungan trust yang ada hanyalah ada sebelum sesi servis adalah antara Broker dan MN, yaitu dengan cara Broker menyimpan public key milik semua MN yang terdaftar pada Broker tersebut dan MN menyimpan public key milik Broker yang dipercayainya. Pada setiap session dibangun hubungan trust antara komponen lainnya melalui jembatan Broker-MN. Dalam model ini bisa dijamin non-repudiation karena Broker telah memiliki public key milik digital certificate tertentu sebagai bagian dari data biaya. Selain itu, MN bisa mempercayai bahwa ia tidak akan dimintai biaya secara ilegal oleh service provider yaitu dengan memverifikasi bahwa servis tersebut telah benar-benar disetujui dan dijamin oleh Broker tersebut dan ia mempunyai public key milik service provider sebagai dasar kepercayaannya.

Jadi bila kita memperkenalkan konsep Broker dari pihak ketiga yang dipercayai maka kita bisa menggunakan model dan protokol yang sama untuk membangun hubungan trust antara setiap komponen yang terlibat dalam H.323 call, yaitu seperti terminal dan gatekeeper menjamin non-repudiation. Sementara itu selain kemungkinan menggunakan model AAA, jika semua autentikasi dilakukan berdasarkan sertifikat maka non-repudiation bisa dijamin sampai level tertentu.

5. Legal Interception dan keamanan VoIP

Untuk kepentingan penegakan hukum maka haruslah ada cara tertentu untuk melakukan pengintaian elektronik terhadap pelaku kriminal yang dicurigai tanpa sepengetahuan mereka. Teknik key recovery bisa digunakan untuk tujuan tersebut, namun implementasi kebutuhan pemerintah tersebut hampir mustahil bisa dilakukan dalam semua kasus dan lebih dari itu mekanisme tersebut akan menghasilkan kelemahan bagi sistem.

Sistem enkripsi dengan key recovery memberikan suatu bentuk akses kepada plain text diluar channel enkripsi-dekripsi biasa. Bagian penting dalam key recovery adalah:

- ⚡ Mekanisme bagi pihak ketiga untuk melakukan akses secara tersembunyi terhadap plain text dari data yang telah dienkripsi.
- ⚡ Harus ada kunci rahasia khusus (atau sekumpulan kunci rahasia) yang harus diamankan untuk satu periode waktu tertentu.

Bagian ini akan membahas secara singkat persyaratan legal interception dan risikonya pada komunikasi IP. Juga dibahas bagaimana aspek keamanan yang bisa dilanggar ketika melakukan legal interception, khususnya dalam H.323.

5.1 Requirement pada sistem key recovery

Dari sudut pandang pengguna, key recovery system sebenarnya tidak dibutuhkan karena bila kunci enkripsinya hilang dalam suatu komunikasi maka cara yang mudah adalah dengan menegosiasikan sekumpulan kunci yang baru dengan pihak kedua daripada mencari kunci pertama yang hilang. Kebutuhan utama dalam mekanisme communication interception adalah:

- ⚡ Akses cepat: kemampuan untuk mendapat kunci dekripsi dengan cepat
- ⚡ Akses terhadap komunikasi H.323 yang terenkripsi tanpa disadari oleh usernya
- ⚡ Akses berdasarkan identitas, lokasi dan content: misalnya mencari lokasi user dalam kasus kecelakaan
- ⚡ Key recovery system yang terstandarisasi secara internasional

5.2 Resiko keamanan dan biaya pada key recovery system

Key recovery system lebih tidak aman, lebih mahal biayanya, dan lebih sulit menggunakannya dibandingkan dengan sistem yang mirip tanpa fasilitas key recovery. Key recovery mengurangi keamanan traffic H.323 karena banyak mengurangi mekanisme proteksi yang ada pada enkripsi, seperti kontrol penuh oleh user pada cara mendekripsi

data. Kunci kriptografik digunakan untuk memberikan confidentiality, sementara authentication dicapai dengan cara menggunakan kode autentikasi dan digital signature.

Non-repudiation sangatlah penting dalam e-commerce, yaitu digunakan signature untuk membuktikan ada persetujuan yang disepakati dan disetujui oleh individu tertentu.

Beberapa sistem key recovery menggabungkan authentication dan signature key dengan confidentiality key, sebagai hasilnya adalah kehilangan non-repudiation yang memungkinkan ikatan komitmen. Dalam kebanyakan kasus tidak mungkin untuk tidak mencakup authentication dan signature key dari infrastruktur key recovery, karena kadangkala kunci yang sama digunakan baik untuk signature dan enkripsi.

Authentication adalah isu penting dalam keamanan H.323 karena tidak hanya menjamin kerahasiaan tetapi juga memberikan integritas dan non-repudiation. Recovery system menawarkan mekanisme untuk mendapatkan kunci tersebut dan untuk menyimpannya sehingga memberi kelemahan pada isu keamanan tersebut.

Key Certification digunakan dalam electronic commerce untuk membuktikan identitas dari user yang dienkripsi (misalnya pemilik public key). CA (certification Authority) digunakan untuk mengeluarkan sertifikat yang berisi kunci public dari pemegang sertifikat. CA tidak pernah menyimpan kunci rahasia dari kunci public tertentu. Jadi key recovery tidak bisa digunakan dalam infrastruktur sertifikasi karena hanya akan menambah resiko membongkar kunci rahasia CA.

Resiko keamanan yang diakibatkan oleh key recovery system adalah memberikan kelemahan baru untuk dibongkar oleh para hacker untuk mengakses data dengan cepat. Mengelola dan mengimplementasikan key recovery system berarti membutuhkan individual yang bisa dipercaya, hal tersebut hanya menghasilkan resiko baru.

5.3 Arsitektur yang mungkin dari legal interception system dalam jaringan VoIP

Dalam skenario yang diperlihatkan pada Gambar 4, yaitu pada point-to-point call, maka interception bisa ditempatkan di gatekeeper diantara gatekeeper caller dan callee. Seperti yang disebutkan dalam H.235, maka kedua belah pihak harus melakukan mekanisme autentikasi dengan gatekeeper melalui RAS signaling. Disini call signaling messages (H.225 channel) dapat diintercept termasuk juga kunci autentikasinya (informasi mana yang diintercept tergantung mekanisme autentikasi yang digunakan, seperti yang dijelaskan pada 4.1.1).

H.235 juga menjelaskan bahwa dalam point-to-point call maka kedua entiti bisa menegosiasikan parameter keamanan call control channel (H.245 channel) yang akan

digunakan. Artinya negosiasi ini bisa transparan bagi gatekeeper yang dalam hal ini tidak mungkin mengakses komunikasi ataupun algoritma enkripsi dan kunci. Dalam kasus conference seperti pada Gambar 5, masalahnya menjadi lebih sederhana karena semua pihak harus melakukan autentikasi ke MCU dan MCU yang bertindak sebagai titik pusat adalah tempat yang baik untuk melakukan interception terhadap call signalling dan call control messages.

Isu lainnya adalah saat callee dan caller terletak jauh satu dengan lainnya dan dibutuhkan gateway. Disini gatekeeper bisa bertindak sebagai firewall dan komunikasi masuk dan keluar bisa saja difilter digatekeeper tersebut.

6. Kesimpulan

H.323 terdiri sekumpulan standar dari ITU-T yang menjadi protokol dasar IP Telephony. H.323 memberikan mekanisme keamanan yang baik yaitu dengan menggabungkan protokol H.235 kedalam komunikasi multimedia. H.235 Memberikan pilihan keamanan termasuk authentication, privacy, integrity, dan non-repudiation. Protokol H.235 berusaha mengatasi ancaman keamanan dalam berbagai skenario dan protokol. Akan tetapi masih ada beberapa isu yang merupakan bahan yang perlu dikaji lebih dalam seperti bagaimana menerapkan H.235 saat digunakan mekanisme H.245 tunneling, apa yang terjadi pada enkripsi channel H.245 saat ditunnel melalui H.225.

Sebagai kesimpulan kita bisa mengatakan bahwa H.323 adalah mekanisme yang sudah cukup baik yang bisa digunakan untuk call control dan call signalling dalam Internet Telephony, sisi keamanannya sudah cukup kokoh dan H.323 sudah ada di pasaran dan telah digunakan secara luas. Masalah yang muncul dengan legal interception bukanlah spesifik masalah komunikasi H.323, tetapi masalah tersebut terjadi pula pada sistem komunikasi manapun.

Daftar Pustaka

1. H.323 v4, Packet-based Multimedia Communication System, ITU-T, 2000.
 2. H.235, Security and Encryption for H-series (H.323 and other H.245-based) Multimedia Terminals, ITU-T, 2000.
-
-