IPSec: SEBAGAI SALAH SATU APLIKASI TEKNIK KRIPTOGRAFI/ KEAMAANAN DATA PADA JARINGAN KOMPUTER

Ignatius Suraya
Jurusan Matematika, Fakultas Sains Terapan
Institut Sains & Teknologi AKPRIND Yogyakarta
Jalan Kalisahak 28, Yogyakarta 55222
Telepon (0274)-563029 Fax (0274)-563847

ABSTRACT

Data security on a computer network is essential, especially data that is confidential. Currently there are several alternative methods for data security on the network such as by encrypting data before it is sent, using digital signatures, installing a firewall so that no intruder from the outside that can get into the internal computer networks and others. Some of the solutions above can be used to improve security, but there are also weaknesses, such as the use of firewalls to prevent intruders from outside, but the intrusion cannot be prevented if data is intercepted by a person residing in the network itself. Cryptographic techniques are implemented on the communication protocol IPSec to get the security aspect. IPSec is a set of communications protocols that implement several cryptographic techniques to ensure security in communication through computer networks. One of solutions to improve data security in computer networks with TCP / IP is using IPSec. IPSec works by encrypting the data before it is sent automatically without the intervention of the sender. By using IPSec, so if data has been intercepted by a third party, the data is already encrypted so it is difficult to know the original data. IPSec is not a perfect communication protocols, but until now, the IPsec security protocol is still regarded as the best compared to other IP security protocols. And more important is the ease of implementation on a system, so that it can make computer users to think again of the importance of data security in a system.

Keywords: computer network security, TCP/IP, IPSec, cryptography technique

INTISARI

Keamanan data pada sebuah jaringan komputer sangatlah penting, terutama data yang bersifat rahasia. Saat ini terdapat beberapa alternatif metode untuk keamanan data pada jaringan, misal nya dengan mengenkripsi data sebelum dikirimkan, menggunakan tandatangan digital (*digital signature*), memasang firewall sehingga tidak ada penyusup dari luar yang dapat masuk ke jaringan komputer internal dan lain-lain. Beberapa solusi diatas dapat digunakan untuk meningkatkan keamanan, namun juga terdapat kelemahan, seperti penggunaan firewall dapat mencegah penyusup dari luar, tetapi tidak dapat mencegah jika data disadap oleh orang yang berada dalam jaringan itu sendiri. Teknik kriptografi diimplementasikan pada protokol komunikasi IPSec untuk mendapatkan aspek keamanan tersebut. IPSec merupakan serangkaian protokol komunikasi yang menerapkan beberapa teknik kriptografi untuk menjamin keamanan dalam komunikasi melalui jaringan komputer. Salah satu solusi untuk meningkatkan keamanan data pada jaringan komputer dengan protokol TCP/IP adalah dengan menggunakan IPSec. IPSec ini bekerja dengan melakukan enkripsi pada data sebelum dikirimkan secara otomatis tanpa campur tangan pihak pengirim. Dengan menggunakan IPSec, maka seandainya data berhasil disadap oleh pihak ketiga, data tersebut telah terenkripsi sehingga sangat sulit untuk dapat mengetahui data aslinya. IPSec memang bukanlah protokol komunikasi yang sempurna, tetapi hingga kini, IPsec masih dianggap sebagai protokol keamanan yang paling baik dibanding protokol keamanan IP yang lain. Dan yang lebih penting lagi adalah kemudahan dalam implementasi pada suatu sistem, sehingga dapat menjadikan para pengguna komputer untuk berpikir kembali akan pentingnya keamanan data pada suatu sistem.

Kata kunci: keamanan jaringan komputer TCP/IP, IPSec, teknik kriptografi

PENDAHULUAN

Pada sebuah jaringan komputer, keamanan pengiriman serta penerimaan data sangat penting untuk menjamin bahwa data yang dikirim tidak jatuh ke pihak lain, terutama jika data tersebut bersifat rahasia. Untuk itu perlu dilakukan implementasi metode-metode pengamanan data pada jaringan.

Banyak metode yang dapat diimplemen tasikan, seperti penggunaan tanda tangan

digital, enkripsi ataupun pemasangan *firewall.* Pada jaringan yang berhubungan dengan internet, maka pemasangan *firewall* menjadi wajib karena dengan adanya *firewall*, maka pihak dari luar tidak dapat memasuki jaringan internal kecuali diijinkan. *Firewall* efektif untuk mencegah pencurian data ataupun masuknya penyusup yang hendak mengacaukan sistem jaringan. Tetapi dengan adanya *firewall*, tetap tidak bisa mencegah penyadapan data yang dilakukan oleh pihak di dalam jaringan itu sendiri. Cara lain untuk meningkat kan keamanan data adalah dengan menggunakan enkripsi pada data yang akan dikirimkan. Jika data yang dikirimkan berupa file, maka dilakukan enkripsi pada file tersebut sehingga data file tersebut tidak bisa dibaca lagi dengan menggunakan cara biasa, tetapi harus dilakukan pengembalian enkripsi (dekripsi) sehingga data file tersebut kembali normal. Untuk melakukan hal ini, maka pihak pengirim harus proaktif dengan melakukan prosedur enkripsi sebelum dia mengirim-kan file tersebut. Begitu pula dengan pihak penerima harus melakukan decode sehingga file yang diterima dapat diakses secara normal.

Seringkali hal tersebut dianggap merepotkan sehingga pihak pengirim tidak melakukan enkripsi terhadap file yang akan dikirimnya sehingga jika file tersebut ditangkap oleh pihak ketiga maka dapat diakses dengan mudah oleh pihak yang tidak dikehendaki tersebut. Untuk pengiriman surat elektronik (email), dapat diamankan dengan menggunakan tanda tangan digital (*digital signature*). Tetapi hal ini juga memerlukan kesadaran dari pihak pengirim email untuk mengimplemen tasikan tanda tangan digital pada email yang dia kirim, dimana hal ini seringkali juga diabaikan.

Salah satu cara untuk mengatasi masalah yang timbul dari implementasi metode keamanan di atas yaitu dengan menggunakan IPSec. IPSec adalah suatu cara untuk meningkatkan keamanan pengiriman data khususnya pada jaringan komputer yang menggunakan protokol TCP/IP (Huggins, 2004). IPSec bekerja dengan melakukan enkripsi data yang dikirim secara otomatis tanpa campur tangan pihak pengirim (Jones, 2003). Seandainya data yang telah dienkripsi oleh IPSec ini dapat disadap oleh pihak ketiga, data tersebut tidak dapat terbaca jika tidak mengetahui kunci enkripsi yang digunakan. Keuntungan penggunaan IPSec adalah:

1. Keamanan data itu sendiri.
2. Otentikasi dimana IPSec akan menandai data yang dikirim dengan kunci enkripsi sehingga penerima dapat yakin bahwa data yang dikirim berasal dari pengirim yang benar, bukan berasal dari pihak lain yang menyamar sebagai pihak pengirim.
3. Integritas data karena IPSec melakukan perhitungan *checksum* yang akan dicocokkan saat data tiba di pihak penerima. Dengan *checksum* ini, pihak penerima dapat yakin bahwa data tersebut tidak dilakukan modifikasi di tengah perjalanannya oleh pihak lain.

PEMBAHASAN

Keamanan Jaringan Komputer

Masalah keamanan jaringan komputer secara umum dibagi menjadi empat kategori yang saling berkaitan:

1. *Secrecy*/*confidentiality*: informasi yang dikirim melalui jaringan komputer harus dijaga sedemikian rupa kerahasiaannya sehingga tidak dapat diketahui oleh pihak yang tidak berhak mengetahui informasi tersebut.
2. *Authentication*: identifikasi terhadap pihak-pihak yang sedang melakukan komunikasi melalui jaringan harus dapat dilakukan. Pihak yang berkomunikasi melalui jaringan harus dapat memastikan bahwa pihak lain yang diajak berkomunikasi adalah benar-benar pihak yang dikehendaki.
3. *Nonrepudiation*: pembuktian korespondensi antara pihak yang mengirimkan informasi dengan informasi yang dikirimkan juga perlu dilakukan dalam komunikasi melalui jaringan komputer. Dengan pembuktian tersebut, identitas pengirim informasi dapat dipastikan dan penyangkalan pihak tersebut atas informasi yang telah dikirimnya tidak dapat dilakukan.
4. *Integrity control*: informasi yang diterima oleh pihak penerima harus sama dengan informasi yang dikirim oleh pengirim. Informasi yang telah mengalami perubahan dalam proses pengiriman, misalnya diubah oleh pihak lain, harus dapat diketahui oleh pihak penerima.

Dalam protokol OSI (*Open Systems Interconnection*) *Reference Model* terdapat beberapa kemungkinan penempatan aspek keamanan jaringan. Terdapat pula kemungkinan bahwa aspek keamanan jaringan tidak hanya ditempatkan pada salah satu layer melainkan dikombinasikan pada beberapa layer sekaligus karena penempatan pada tiap *layer* memiliki keunggulan masing-masing.

Pada *physical layer*, kabel transmisi

dapat diamankan dengan penggunaan tabung pelapis yang berisi gas bertekanan tinggi. Pada *data link layer*, paket pada jalur point-to-point dapat dienkripsi ketika meninggalkan sebuah mesin dan didekripsi ketika masuk ke mesin yang lain. Pada *network layer*, penggunaan *firewall* dan protokol IPsec digunakan untuk menjamin keamanan. Pada *transport layer*, koneksi dapat dienkripsi untuk menjamin kemanan antar proses (*end-to-end*). Terakhir, pada *application layer*, aspek autentikasi dan *nonrepudiation* dapat dijamin dengan algoritma pada aplikasi yang digunakan.

IPSec (IP Security)

IPSec dapat menjaga keamanan data pada lalu lintas jaringan dengan menerapkan kebijakan-kebijakan keamanan. Kemungkinan terdapat beberapa kebijakan keamanan yang dibuat dengan menggunakan IPSec, namun pada suatu saat hanya bisa diterapkan satu kebijakan pada suatu komputer. Setiap aturan dalam suatu kebijakan keamanan terdiri *filter list*, *filter action*, dan metode autentikasi.

1. *Filter list* dapat mengidentifikasi tipe dari lalu lintas jaringan dan mengacu kepada kebijakan keamanan yang sudah dibuat manakala ada yang cocok dengan kondisi-kondisi yang ada pada *filter list*. Sebagai contoh, *filter list* mungkin saja hanya mengidentifikasi lalu lintas *Internet Control Message Protocol* (ICMP) dan *Hypertext Transfer Protocol* (HTTP).
2. *Filter action* menyatakan tindakan-tindakan yang harus dilakukan jika lalu lintas jaringan sesuai dengan kondisi yang ada pada *filter list*. *Filter action* didefinisikan oleh seorang administra tor dengan tujuan mengijinkan, menolak, atau untuk autentikasi terhadap lalu lintas data yang masuk maupun keluar pada saat suatu kondisi terpenuhi. Sebagai contoh, seorang administrator dapat menyaring semua lalu lintas ICMP dan melakukan enkripsi terhadap lalu lintas HTTP. *Filter action* dapat juga menentukan algoritma *hash* dan enkripsi yang digunakan pada kebijakan keamanan tersebut.
3. Kebijakan keamanan yang lainnya adalah mengijinkan lalu lintas IP tertentu untuk lewat pada jaringan dengan syarat pengirim dapat melakukan proses autentikasi terhadap identitasnya. Terdapat tiga metode untuk autentikasi yaitu *certificates*, *protocol Kerberos*, dan *preshared key*. Suatu aturan yang dibuat dapat menggunakan salah satu metode atau lebih tergantung dari kebutuhan keamanan data.

Beberapa aturan yang sudah didefinisikan secara *default* antara lain:

1. *Default response*: meyakinkan bahwa respon dari suatu komputer akan masuk ke jalur komunikasi yang aman. Jika pada kebijakan keamanan dengan menggunakan IPSec pada suatu komputer tidak mempunyai aturan yang sudah didefinisikan untuk komputer lain yang meminta jalur komunikasi yang aman, maka aturan pada *Default response* akan diaplikasikan untuk melakukan negosiasi dengan penggabungan keamanan.
2. *Permit ICMP*: mengijinkan lalu lintas ICMP untuk melewati suatu jaringan. ICMP adalah suatu protokol pada lingkungan TCP/IP yang berguna untuk menyatakan *error* dan mampu untuk menyederhanakan koneksi yang terjadi. Fitur seperti *file sharing*, perintah *ping* dan *tracert*, serta aplikasi yang lain membutuhkan lalu lintas ICMP supaya dapat melewati suatu jaringan.
3. ESP (*Encapsulating Security Payload*): dapat digunakan dalam suatu kebijakan keamanan ketika data akan dikirim melalui internet. ESP menyediakan *service* berupa pengiriman data secara aman dengan cara melakukan enkripsi pada lalu lintas jaringan. Selain itu ESP juga menyediakan jasa layanan autentikasi data serta pengecekan terhadap integritas dari suatu data.

Beberapa kebijakan keamanan *default* pada Windows, adalah (Huggins, 2004):

1. *Client* (*respond only*): digunakan saat komputer meminta komputer lain untuk menggunakan IPSec. Suatu komputer tidak menggunakan IPSec untuk merespon sampai komputer lain menyatakan permintaan secara khusus. *Client* (*respond only*) hanya menggunakan aturan *default response*.
2. *Server* (*request security*): digunakan pada *server* dan *client*. Pada saat *policy* ini diimplementasikan pada suatu komputer, maka komputer akan berkomunikasi dengan *server* menggunakan IPSec. Namun *server* akan berkomunikasi dengan menggunakan jalur biasa jika *client* tidak dikonfigurasi menggunakan IPSec. Pada jalur komunikasi yang tidak aman, IPSec tidak digunakan. *Server* (*request security*) *policy* menggunakan aturan *default response*, *permit* ICMP, dan ESP.
3. *Secure server* (*require security*): digunakan pada *server* dan *client* secara

bersama sama. *Policy* ini menggunakan IPSec untuk melakukan komunikasi dan tidak akan pernah berpaling pada jalur komunikasi yang tidak aman. *Secure Server policy* terdiri aras *default response*, *permit* ICMP, dan ESP. Jika *secure sever* (*require security*) digunakan, maka semua lalu lintas harus dienkripsi menggunakan ESP pada *server* supaya dapat berkomunikasi dalam jaringan.

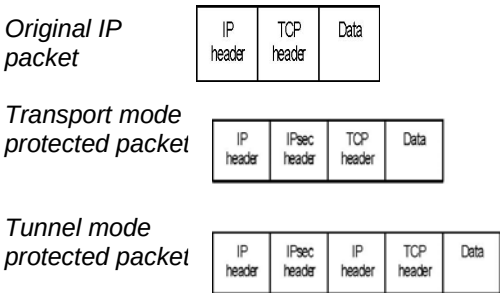
Salah satu solusi yang menjamin tingkat keamanan paling tinggi adalah dengan mengimplementasikan aspek keamanan pada *application layer*. Dengan implementasi aspek keamanan pada *layer* ini maka keamanan data dapat dijamin secara *end-to-end* (proses ke proses) sehingga upaya apa pun untuk mengakses atau mengubah data dalam proses pengiriman data dapat dicegah. Namun pendekatan ini membawa pengaruh yang besar yaitu bahwa semua aplikasi yang dibangun harus ditambahkan dengan aspek keamanan untuk dapat menjamin keamanan pengiriman data.

Pendekatan lain didasarkan bahwa tidak semua pengguna menyadari pentingnya aspek keamanan sehingga mungkin menyebabkan mereka tidak dapat menggunakan fitur keamanan pada aplikasi dengan benar. Selain itu tidak semua pengembang aplikasi memiliki kemauan untuk menambahkan aspek keamanan pada aplikasi mereka. Oleh karena itu, aspek keamanan ditambah kan pada network layer sehingga fitur kemanan dapat dipenuhi tanpa campur tangan pengguna atau pengembang aplikasi. Pada akhirnya pendekatan kedua, mendapat dukungan lebih banyak daripada pendekatan pertama sehingga dibuat sebuah standar keamanan *network layer* yang salah satu desainnya yaitu IPSec. IPSec merupakan kumpulan protokol yang dikembangkan oleh IETF (*Internet Engineering Task Force*) untuk mendukung pertukaran paket yang aman melalui IP *layer*. IPSec didesain untuk menyediakan keamanan berbasis kriptografi yang memiliki karakteristik *interoperable* dan berkualitas. Layanan keamanan yang disediakan mencakup *access control*, *connectionless integrity*, *data origin authentication*, proteksi *replay attack* (*sequence integrity*), *data confidentiality* dan *traffic flow confidentiality*. Layanan tersebut disediakan pada IP *layer* sehingga mendukung proteksi untuk IP layer dan *layer* di atasnya.

Secara teknis IPSec terdiri atas dua bagian utama. Bagian pertama mendeskripsikan dua protokol untuk penambahan *header* pada paket yang membawa *security identifier*, data mengenai *integrity control*, dan informasi keamanan lain. Bagian kedua berkaitan dengan protokol pembangkitan dan distribusi kunci. Bagian pertama IPsec adalah implementasi dua protokol keamanan yaitu:

a. *Authentication Header* (AH) menyediakan *data integrity*, *data origin authentication* dan proteksi terhadap *replay attack*.
b. *Encapsulating Security Payload* (ESP) menyediakan layanan yang disediakan oleh AH ditambah layanan *data confidentiality* dan *traffic flow confidentiality*.

Setiap protokol mendukung dua mode penggunaan *transport mode* dan *tunnel mode*. Pada transport mode, protokol menyediakan proteksi terhadap *layer* di atas IP *layer*. Layanan keamanan pada mode ini dilakukan dengan penambahan sebuah IPsec *header* antara IP *header* dengan *header* protokol *layer* di atas IP yang diproteksi. Sedangkan pada *tunnel mode*, protokol diaplikasikan untuk menyediakan proteksi pada paket IP sehingga sekaligus melindungi *layer* di atas IP *layer*. Hal ini dilakukan dengan mengenkapsulasi paket IP yang akan diproteksi pada sebuah IP *datagram* yang lain (Gambar 1).



Gambar 1 *Transport Mode* dan *Tunnel Mode* Protokol IPsec

Bagian kedua IPsec adalah implementasi protokol IKE (*Internet Key Exchange*) yang berfungsi dalam pembangkitan dan pertukaran *criptographic key* secara otomatis. *Criptographic key* digunakan dalam autentikasi *node* yang berkomunikasi dan proses enkripsi dan dekripsi paket yang dikirimkan.

Data Integrity dan Authentication IPSec

Integritas data yang dikirimkan melalui jaringan dijamin oleh IPSec melalui metode autentikasi *digital signature* atas informasi yang dikirimkan secara paket-per-paket. Layanan jaminan integritas data ini disediakan dengan menggunakan algoritma HMAC (*Hash Message Authentication*

Code) baik oleh protokol AH maupun oleh protokol ESP.

1. *Hash Message Authentication Code* (HMAC)
   HMAC adalah algoritma autentikasi menggunakan kunci rahasia. Integritas data dan autentikasi asal data yang disediakan oleh HMAC bergantung pada penyebaran kunci rahasia yang digunakan. Jika hanya sumber (pengirim) dan tujuan (penerima) yang mengetahui kunci HMAC, maka autentikasi asal data dan integritas data untuk paket-paket yang dikirim antara kedua pihak tersebut dijamin.
   MAC menggunakan fungsi *hash* satu arah, H, dan kunci rahasia K. Beberapa fungsi hash yang digunakan di antaranya adalah: MD5 dan SHA-1. Salah satu praktek kriptografi menyangkut HMAC adalah hanya menggunakan sebagian *bit* (sepanjang t *bit*) paling kiri dari keluaran algoritma HMAC. Notasi yang digunakan untuk menyatakan penerapan praktek ini yaitu HMACH-t. Contohnya, HMAC-MD5-96 menyatakan HMAC yang menggunakan fungsi *hash* MD5 dan hanya menggunakan 96 *bit* paling kiri dari hasil keluaran algoritma HMAC, sehingga memberikan keuntungan yaitu lebih sedikit informasi *hash* paket yang bisa didapat oleh penyerang.
2. *Authentication Header* (AH)
   AH didefinisikan sebagai protokol IP yang diberi nomor 51. Dengan demikian, *field* protokol pada *header* paket IP yang diproteksi akan memiliki nilai 51 yang menunjukkan bahwa *header* yang mengikutinya adalah sebuah *header* AH (Gambar 2).

Next header	*Payload length*	*Reserved*
Security Parameter Index (SPI)		
Sequence Number		
Authentication Data		

Gambar 2 *Header* AH

Pesan berisi informasi yang akan dikirim melalui jaringan akan dipecah-pecah menjadi paket-paket IP. Hal yang pertama dilakukan oleh IPsec dalam pemrosesan paket tersebut adalah memeriksa apakah paket tersebut akan diberikan layanan keamanan dengan protokol AH. Hal ini dilakukan dengan mencocokan paket yang bersangkutan dengan entri pada *Security Policy Database* (SPD). Apabila terdapat entri pada SPD, IPSec akan menentukan sebuah *Security Association* (SA) berisi informasi mengenai algoritma MAC (*Message Authentication Code*) yang digunakan untuk paket tersebut sesuai dengan *source* dan *destination* paket yang bersangkutan. Setiap pasangan *source* dan *destination* memiliki SA berbeda yang ditentukan secara manual sebelumnya atau secara otomatis melalui protokol IKE.

Informasi mengenai algoritma MAC yang digunakan dalam SA ditambahkan pada *header* AH yaitu pada field SPI (*Security Parameter Index*) setelah sebelumnya memberi nilai pada *field next header*, *payload length* dan *Reserved*. *Field next header* diberi nilai numerik dari tipe protokol dari data yang diproteksi (misalnya TCP atau UDP pada *transport mode*, atau IP pada *tunnel mode*). Selain itu, *field payload length* diberi nilai sesuai panjang *header* AH, kemudian *field reserved* diberi nilai kosong (*null value*).

Field sequence number pada awalnya diberi nilai kosong, untuk kemudian ditambahkan satu-per-satu untuk setiap paket terproteksi yang dikirimkan. *Sequence number* tidak dapat berulang sehingga apabila sudah mencapai nilai maksimum 2^{32} maka SA untuk pengiriman pesan yang berjalan harus dimatikan terlebih dahulu dan dibentuk SA baru untuk pengiriman pesan lanjutan. Hal ini dimaksudkan untuk mencegah terjadinya *replay attack* atas paket pesan. *Field authentication data* adalah *field* yang panjangnya variabel berisi hasil dari fungsi pengecekan integritas yang disebut ICV (*Integrity Check Value*). Protokol AH pada IPsec tidak mendefinisikan (algoritma) *authenticator* tertentu tetapi mengharuskan implementasi *authenticator* untuk menjamin interoperabilitas antara implementasi IPsec yang berbeda. Dua *authenticator* yang harus diimplementasikan adalah HMAC-SHA-1-96 dan HMAC-MD596. Kedua fungsi merupakan fungsi MAC dengan kunci rahasia yang keluarannya di-*truncate* menjadi 96 *bit*.

ICV dihitung dengan menjalankan fungsi yang didefinisikan oleh *authenticator* pada SA dengan parameter kunci rahasia dan seluruh paket IP yang terproteksi termasuk header AH. Namun demikian, *field-field* pada *header* IP yang sifatnya berubah-ubah seperti TTL (*Time To Live*) dan *header checksum* serta *field authentication data* itu sendiri diberi nilai kosong terlebih dahulu sebelum dimasukkan ke dalam fungsi. Setelah nilai ICV tersebut didapat maka nilainya dimasukkan dalam *field authentication*

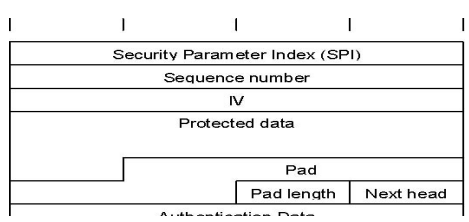
data. Nilai-nilai *field* dari *header* IP yang berubah juga dimasukkan kembali ke dalam *field* masingmasing.

Pemrosesan AH selesai sampai titik ini dan paket IP yang terproteksi siap untuk dikirimkan. Bergantung pada ukuran paket yang dihasilkan, paket tersebut mungkin terfragmentasi dalam perjalanannya. Hal ini tidak menjadi masalah dan akan ditangani oleh pihak penerima. Pihak penerima pesan harus melakukan reassembly atas paket yang terfragmentasi. Setelah paket utuh diterima, hal pertama yang dilakukan adalah menentukan SA yang digunakan untuk memproteksi paket tersebut. SA yang digunakan ditentukan melalui *field destination* dan *field protocol* pada *header* IP serta field SPI pada *header* AH. Bila tidak ditemukan SA yang sesuai, maka paket tersebut di-*discard*. Kemudian, pengecekan *sequence number* dilakukan. Sama halnya dengan sebelumnya, apabila paket yang diperiksa gagal memenu hinya maka paket tersebut di-*discard*. Paket yang gagal memenuhi pengecekan *sequence number* menunjukkan bahwa paket terproteksi tersebut telah di-*replay* oleh pihak lain.

Proses yang teakhir dilakukan adalah pengecekan ICV yang terdapat pada *field authentication data* pada *header* AH disimpan dan *field* tersebut diberi nilai kosong. *Field* pada *header* IP yang berubah-ubah juga diberi nilai kosong. Setelah itu, algoritma *authenticator* yang didefinisikan SA dijalankan pada paket tersebut dan hasilnya dibandingkan dengan ICV yang disimpan sebelumnya. Jika hasilnya sama maka paket tersebut terautentikasi dan paket IP yang diproteksi dapat di-*restore* dan diperlakukan sebagaimana paket IP biasanya

3.*Encapsulating Security Payload* (ESP)

ESP didefinisikan sebagai protokol IP yang diberi nomor 50. Dengan demikian, *field* protokol pada *header* paket IP yang diproteksi akan memiliki nilai 50 yang menunjukkan bahwa *header* yang mengikutinya adalah sebuah *header* ESP (Gambar 3).



Gambar 3 *Header* ESP

Sebagaimana halnya pada protokol AH, paket yang akan diproses harus ditentukan terlebih dahulu apakah akan diberi layanan keamanan IPsec. Serupa dengan yang dilakukan pada AH, informasi paket yang diterima dicocokan pada entri di SPD. Apabila paket tersebut terdapat pada entri SPD maka paket tersebut akan diberikan layanan keamanan ESP. Sebuah SA kemudian akan ditentukan dari definisi yang ditentukan secara manual sebelumnya maupun secara otomatis dengan protokol IKE. Berbeda dengan protokol AH yang hanya menentukan *authenticator* (algoritma autentikasi yang digunakan), SA pada protokol ESP juga menentukan sebuah *encryptor* (algoritma enkripsi paket yang digunakan). Hal ini disebabkan ESP tidak hanya menyediakan fitur *data integrity* tetapi juga fitur *data confidentiality*.

Nilai numerik informasi mengenai SA yang telah ditentukan kemudian dimasukkan ke dalam *field Security Parameter Index* (SPI) sebagaimana dilakukan pada protokol AH. Demikian pula dengan *field sequence number* akan diinisiasi dengan nilai nol dan di-*increment* setiap pemrosesan paket pesan yang diproteksi. Seperti pada protokol AH, *field* ini diperlukan untuk untuk menjamin keamanan pengiriman paket dari *replay-attack*.

Field IV (*Initialization Vector*), *Protected data*, *Pad*, dan *Padlength* akan berisi nilai hasil pemrosesan *data confidentiality*. *Field-field* ini akan dijelaskan pada bagian berikutnya. Untuk sementara, *field-field* tersebut diasumsikan telah diisi nilai sebagaimana mestinya. Kemudian, *field next header* diberi nilai sesuai dengan nilai numerik protokol dari *payload* paket yang terproteksi. Dengan demikian, apabila ESP digunakan dalam *transport mode* dengan *payload* berupa paket TCP maka akan memiliki nilai 6 dan bila digunakan dalam *tunnel mode* (*payload* berupa paket IP) akan memiliki nilai 4.

Terakhir, sebagaimana dalam protokol AH, *field authentication data* akan berisi nilai yang digunakan dalam pengecekan integritas paket atau ICV. Seperti halnya pada protokol AH, *authenticator* yang harus diimplementasi dalam protokol ESP adalah HMAC-MD5-96 dan HMAC-SHA-96 untuk menjamin interoperabilitas antar implementasi IPSec yang berbeda-beda. Semua *field* dari field SPI hingga *field*

next header kemudian dimasukkan ke dalam fungsi hash yang telah ditentukan pada SA dan hasilnya dimasukkan ke dalam *field authentication data*.

Sampai di sini pemrosesan fitur *data integrity* dari paket protokol ESP selesai dijalankan. Paket kemudian siap untuk dikirimkan melalui saluran komunikasi. Fragmentasi paket juga mungkin terjadi sebagaimana pada paket AH dan akan ditangani pula oleh pihak penerima paket.

Pihak penerima pesan harus melakukan *reassembly* atas paket yang terfragmentasi. Setelah paket utuh diterima, hal pertama yang dilakukan adalah menentukan SA yang digunakan untuk memproteksi paket tersebut. SA yang digunakan ditentukan melalui *field Destination* dan *field Protocol* pada *header* IP serta *field* SPI pada *header* ESP. Bila tidak ditemukan SA yang sesuai, maka paket tersebut di-*discard*.

Data Confidentiality Pada IPSec

Protokol AH tidak menyediakan fitur data *confidentiality* pada IPSec, ini hanya disediakan oleh protokol ESP dengan menggunakan algotitma kriptografi simetri, sehingga menyebabkan pembagian tugas protokol IPSec ke dalam dua jenis (AH dan ESP). Pengguna dapat memilih untuk tingkat kepentingan keamanan atau tingkat kerahasiaan, misalnya: jika pesan harus dijaga kerahasiaannya dapat dipakai protocol ESP dan jika pesan tidak bersifat rahasia dapat dipakai protokol AH.

Analisa Terhadap IPSec

Para ahli telah melakukan analisa tentang kelebihan dan kelemahan IPSec dan hasilnya untuk rekomendasi perbaikan. Kelebihan IPSec adalah sebagai berikut:

1 Dapat melindungi protokol apapun yang berjalan di atas IP, sehingga IPSec merupakan suatu metode umum yang dapat menyediakan keamanan komunikasi melalui jaringan komputer
2 Menyediakan keamanan secara transparan, dari sisi aplikasi *user* tidak perlu menyadari keberadaannya.
3 Tidak mengharuskan penggunaan algoritma enkripsi atau *hash* tertentu sehingga jika algoritma yang sering digunakan sekarang telah dipecahkan, fungsinya dapat diganti dengan algoritma lain yang lebih sulit dipecahkan.

Sedangkan kelemahan IPSec adalah:

1 Terlalu kompleks, penyediaan fitur tambahan menambah kompleksitas yang tidak perlu.
2 Masih ada kesalahan dalam dokumentasi.
3 Algoritma *default* dalam IPSec telah dapat dipecahkan (DES dianggap tidak aman dan MD5 mulai diserang), walaupun algoritma penggantinya sudah tersedia, administrator harus memastikan bahwa mereka menggunakan algoritma lain untuk mendapatkan keamanan yang lebih tinggi.

Rekomendasi dari Ferguson dan Schneier untuk perbaikan IPSec adalah:

1 Hilangkan *transport mode*. *Tunnel mode* merupakan *superset* dari fungsionalitas *transport mode*.
2 Hilangkan protokol AH, dengan tidak perlunya *transport mode*.
3 Modifikasi protokol ESP sehingga selalu menyediakan fitur autentikasi, hanya enkripsi yang opsional. Autentikasi dan enkripsi pada ESP bersifat opsional, dengan adanya algoritma *NULL*.
4 Modifikasi protokol ESP sehingga semua data (termasuk kunci dekripsi) terautentikasi.

Implementasi IPSec

Untuk dapat mengimplementasikan IPSec, hal yang penting adalah dengan memastikan bahwa ada hubungan yang cocok di antara komputer yang akan berkomunikasi. Level keamanan yang ada pada data dalam jaringan akan sangat bergantung pada level keamanan yang sudah dispesifikasikan pada IPSec dari semua komputer yang melakukan negosiasi. Jika pada kedua komputer mempunyai kebijakan keamanan yang saling melengkapi, maka dapat melakukan komunikasi dengan menggunakan IPSec. Namun sebaliknya jika terjadi konflik pada kebijakan keamanan dari masing-masing komputer, maka komunikasi akan dilakukan dengan melalui jalur yang tidak aman, atau bahkan tidak akan melakukan komunikasi sama sekali. Hubungan komunikasi yang terjadi dengan menggunakan kebijakan secara *default*, dapat dilihat pada Tabel 1.

Tabel 1 Komunikasi yang terjadi antar komputer pada *Default Policy*

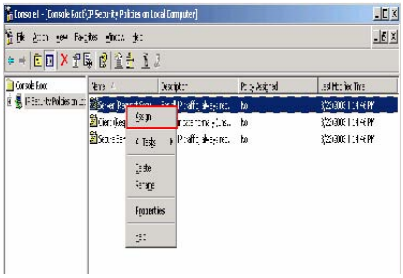
	No *policy* assigned	*Client* (Respond Only)	*Server* (Requests Security)	Secure *Server* (Require Security)
No *policy* assigned	No IPSec	No IPSec	No IPSec	No commu nication
Client (Respond Only)	No IPSec	No IPSec	IPSec	IPSec
Server (Requests Security)	No IPSec	IPSec	IPSec	IPSec

Hal yang penting untuk diketahui adalah adanya suatu keseimbangan antara mengamankan data dari *user* yang tidak berhak dan membuat *user* yang punya akses untuk dapat masuk ke dalam jaringan. Untuk itulah hal yang perlu dilakukan adalah dengan melakukan analisis resiko pada jaringan, menentukan level keamanan yang diperlukan pada suatu organisasi, serta melakukan identifikasi terhadap informasi-informasi yang perlu untuk dilindungi dari serangan pada jaringan. Terdapat tiga level keamanan untuk implementasi kebijakan keamanan dengan menggunakan IPSec, yaitu (Jones, 2003):

1. Level keamanan minimal, dapat digunakan pada komputer yang tidak melakukan komunikasi data penting. IPSec *default* tidak aktif pada level keamanan ini.
2. Level keamanan tingkat *standard*, dapat digunakan ketika hendak menyimpan data penting pada komputer. Level ini akan menjaga keseimbangan antara kerja efisien dengan keamanan. *Client* (respond only) dan *server* (*request security*) memberikan level keamanan *standard*.
3. Level keamanan tingkat tinggi, digunakan ketika komputer menyimpan data sangat penting dan sangat beresiko terhadap akses ilegal. Pada level ini, jalur komunikasi antar komputer yang tidak aman yang tidak mempunyai IPSec tidak akan diijinkan. Kebijakan *secure server* (*require security*) memberikan level keamanan tingkat tinggi.

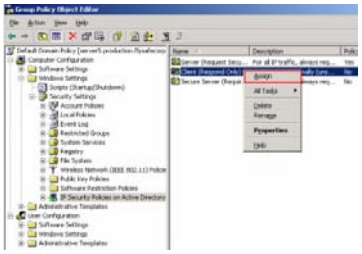
Langkah implementasi IPSec pada Microsoft Windows adalah sebagai berikut:

1. Untuk *server* dilakukan dengan cara masuk ke dalam IP *Security Policies* setelah itu *assign* kebijakan *Server* ataupun *Secure Server* (Gambar 4).



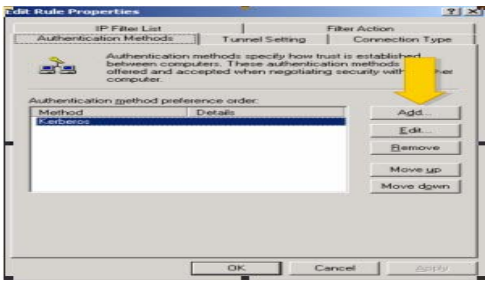
Gambar 4 Pemilihan Kebijakan IPSec

2. Untuk *client* dilakukan dengan cara *assign* pada kebijakan *Client*.
3. Untuk *Active Directory* dilakukan dengan mengedit *Group Policy Editor* (Gambar 5).



Gambar 5. *Group Policy Editor*

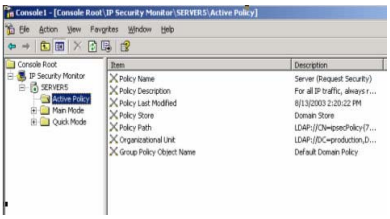
4. Untuk mengaktifkan proses autentikasi di antara 2 komputer yang menggunakan IPSec, dapat dilakukan dengan menambah jenis autentikasi yang secara *default* adalah dengan menggunakan *Kerberos*. Dengan *Kerberos*, maka tidak diperlukan lagi konfigurasi lainnya, sehingga membantu administrator dalam pekerjaannya (Gambar 6).



Gambar 6 *Edit Rule Properties*

Apabila koneksi jaringan dengan menggunakan perintah *ping* tidak berhasil, maka dapat dilakukan dengan cara menghenti kan IPSec untuk kemudian dijalankan kembali. Hal ini harus dilakukan pada semua komputer yang akan melakukan komunikasi. Namun terkadang, ada juga permasalahan bahwa dua komputer yang sebetulnya tidak berhak

melakukan komunikasi namun tetap saja bisa melakukan komunikasi. Hal ini biasanya dapat dilihat dan diamati dengan menggunakan IPSec Monitor (Gambar 7).



Gambar 7 IPSec *Monitor*

KESIMPULAN

1. Penggunaan IPSec akan meningkatkan keamanan pada jaringan komputer karena IPSec melakukan enkripsi terhadap data yang dikirim pada jaringan tersebut. Seandainya terjadi penyadapan data oleh pihak ketiga, maka data asli tidak dapat dilihat dengan mudah tanpa mengetahui kunci enkripsi yang digunakan.
2. IPSec akan melindungi data secara otomatis tanpa sepengetahuan pengguna jaringan komputer sehingga pengguna dapat melaku kan pengiriman data seperti biasa tanpa ada prosedur khusus yang harus dilakukan.
3. Implementasi IPSec dapat dilakukan dengan mudah sehingga tidak memerlukan keahlian khusus oleh administrator.
4. IPSec merupakan salah satu solusi keamanan jaringan berupa protokol keamanan yang berada di *network layer* untuk pengiriman pakat IP.

DAFTAR PUSTAKA

Alshamsi, Abdel Nasir dan Takamichi Saito, A Technical Comparison of IPsec and SSL, Tokyo University of Technology, 2004.

Dahlgren, Anders dan Oskar Jönsson, IPsec, the Future of Network Security?, Göteborg University, 2000, http://www.handels.gu.se/epc/archive/00002483/01/dahlgrenjonsson.pdf

Ferguson, Neil dan Bruce Schneier, A Cryptographic Evaluation of IPsec. Counterpane Internet Security, Inc., 1999, http://www.schneier.com/paper-ipsec.pdf

Glenn, Rob dan Stephen Kent, RFC 2410: The NULL Encryption Algorithm and Its Use with IPsec, The Internet Society: Network Working Group, 1998, http://www.ietf.org/rfc/rfc2410.txt

Harkins, Dan dan Dave Carrel, RFC 2409: The Internet Key Exchange (IKE), The Internet Society: Network Working Group, 1998, http://www.ietf.org/rfc/rfc2409.txt

Huggins, D., 2004, *Windows Server 2003 Network Infrastructure*, QUE, Indianapolis.

Jones, D., 2003, *Microsoft Windows Server 2003*, QUE, Indianapolis.

Kent, Stephen dan Randall Atkinson, RFC 2401: Security Architecture for the Internet Protocol, The Internet Society: Network Working Group, 1998, http://www.ietf.org/rfc/rfc2401.txt,

Kent, Stephen dan Randall Atkinson, RFC 2402: IP Authentication Header, The Internet Society: Network Working Group, 1998, http://www.ietf.org/rfc/rfc2402.txt

Kent, Stephen dan Randall Atkinson, RFC 2406: IP Encapsulating Security Payload (ESP), The Internet Society: Network Working Group, 1998, http://www.ietf.org/rfc/rfc2406.txt

Krawczyk, Hugo, et al, RFC 2104: HMAC: Keyed-Hashing for Message Authentication, The Internet Society: Network Working Group, 1997, http://www.ietf.org/rfc/rfc2104.txt

Madson, Cheryl dan Naganand Doraswamy, RFC 2405: The ESP DES-CBC Cipher Algorithm with Explicit IV, The Internet Society: Network Working Group, 1998, http://www.ietf.org/rfc/rfc2405.txt

Madson, Cheryl dan Rob Glen, RFC 2403: The Use of HMAC-MD5-96 within ESP and AH, The Internet Society: Network Working Group, 1998, http://www.ietf.org/rfc/rfc2403.txt

Madson, Cheryl dan Rob Glen, RFC 2404: The Use of HMAC-SHA-1-96 within ESP and AH, The Internet Society: Network Working Group, 1998, http://www.ietf.org/rfc/rfc2404.txt

Nedeltchev, Plamen dan Radoslav Ratchkov, IPsec-based VPNs and Related Algorithms, 2002, http://www.cisco.com/warp/public/784/packet/apr02/pdfs/plamen.pdf

Pereira, Roy dan Rob Adams, RFC 2451: The ESP CBC-Mode Cipher Algorithms, The Internet Society: Network Working Group, 1998, http://www.ietf.org/rfc/rfc2451.txt

Tanenbaum, Andrew S., Computer Networks, Fourth Edition, Prentice-Hall, 2003

Thayer, Rodney, et al, RFC 2411: IP Security Document Roadmap, The Internet Society: Network Working Group, 1998, http://www.ietf.org/rfc/rfc2411.txt