Pembahasan Pengamanan untuk Jaringan Komputer berbasis IPv6

Albert Raditya Sukiyanto - NIM : 13506077[1)]
1) Jurusan Teknik Informatika ITB, Bandung 40132, email: if16077@students.if.itb.ac.id

Abstract
Makalah ini akan mengkaji aplikasi matematika diskrit (terutama pada bidang pengamanan jaringan) dalam jaringan komputer berbasis TCP/ IP, khususnya IPv6. Maraknya penggunaan peralatan yang berbasiskan Jaringan Komputer dan protokol TCP / IP, baik komputer maupun peralatan lain, misalnya handpone, camera, handycam, dll, sehingga penggunaan IP sendiri sudah makin penting. Apalagi Internet Protokol juga marak dibicarakan terlebih dikarenakan sekarang ini sedang terjadi proses pergantian dari IPv4 menjadi IPv6.

Pengamanan IPv6 menggunakan sebuah protokol IPSec yang diaplikasikan pada layer IP. Pada IPSec digunakkan sebuah algoritma untuk bertukar kunci rahasia yang akan digunakkan untuk mengamankan IPv6, yaitu Algoritma Diffie Hellman. Algoritma tersebut yang akan dibahas secara lebih lanjut pada makalah ini.

Kata Kunci: *Pengamanan, IPv6, Algoritma Diffie-Hellman*

1. PENDAHULUAN

Penulis Memutuskan untuk mengambil makalah ini karena penulis merasa keamanan data merupakan hal yang penting pada saat komunikasi melalui jaringan komputer. Jaringan Komputer adalah himpunan interkoneksi (*interconnected*) sejumlah komputer autonomous. Dan, Sistem terdistribusi adalah sebuah sistem dengan satu unit kendali dan sejumlah unit yang dikendalikan untuk para pengguna. Jaringan komputer sering kali salah diartikan dengan sistem terdistribusi. Pada sistem terdistribusi keberadaan sejumlah komputer autonomous bersifat transparan bagi pemakainya. Sedangkan pada suatu jaringan pengguna harus secara eksplisit menangani seluruh manajemen jaringannya sendiri. Sehingga sistem terdistribusi adalah sistem yang dibuat diatas sebuah jaringan, yaitu pada perangkat lunaknya.

Jaringan komputer memiliki banyak kegunaan, kegunaan jaringan computer, antara lain:
1. Berbagi pakai (*resource sharing*).
2. Untuk mendapatkan keandalan tinggi (*high reliability*)
3. menghemat uang (*saving money*)

Daya tarik pada jaringan komputer: :
1. Akses informasi yang berbeda ditempat yang jauh
2. Komunikasi orang ke orang
3. Hiburan interaktif

Suatu jaringan biasanya dibedakan melalui dua buah klasifikasi, yaitu menurut teknologi transmisi (jaringan broadcast dan jaringan point-to-point) dan berdasarkan jarak (Data Flow Machine, Multicomputer, LAN, MAN, WAN, Wireless Network, Internetwork).

TCP/IP termasuk dalam deretan protokol komunikasi yang digunakan untuk menghubungkan host-host pada jaringan Internet. TCP/ IP menggunakan banyak protokol didalamnya, adapun protokol utamanya adalah TCP/ IP.

Gambar 1: Ilustrasi Jaringan Komputer

Sejarah TCP dan Internet
TCP/IP pertama kali dikembangkan oleh DOD (Department of Defense) di Amerika, yaitu pada tahun 1969 lembaga riset Departemen Pertahanan Amerika yaitu DARPA (Defence Advance Research Project Agency) dan menghasilkan ARPANET.

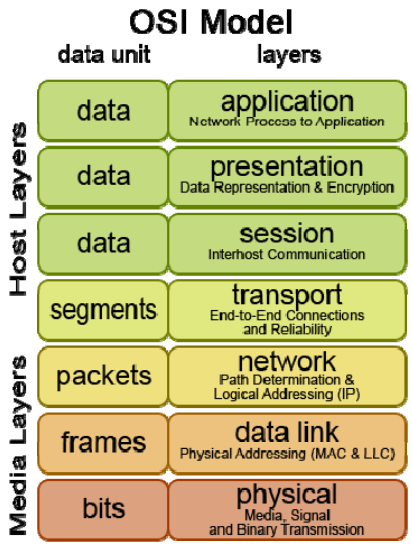
Aplikasi Internet yang pertama kali ditemukan adalah FTP (File Transfer Protocol) sebuah aplikasi untuk kebutuhan transfer file antar *host*. Aplikasi E-mail (Electronic Mail) kemudian ditemukan selanjutnya. Untuk keperluan *remote login* khususnya bagi para administrator jaringan ditemukan aplikasi Telnet. Tiga aplikasi tadi menjadi populer dimasa ARPANET.

Dalam perjalanan masa ARPANET semakin besar, sehingga protokol yang digunakan pada waktu itu NCP (Network Communication Protocol) sudah tidak mampu menampung *node* komputer yang semakin besar. Maka, lahirlah protokol TCP/IP yang selanjutnya pada tahun 1983 oleh ARPANET dinyatakan menjadi standar untuk jaringan. Lalu sebuah perusahaan bernama BBN membuat TCP/IP berjalan diatas komputer dengan sistem operasi UNIX, sejak saat itulah UNIX dan TCP/IP digabung.

2. PEMBAHASAN

2.1 Konsep Dasar Protokol
Protokol dapat dimisalkan sebagai penerjemah dua

orang yang berbeda bangsa ingin berkomunikasi. Protokol internet yang pertama kali dirancang pada awal tahun 1980-an. Akan tetapi pada saat itu, protokol tersebut hanya digunakan untuk menghubungkan beberapa node saja. Baru pada awal tahun 1990-an mulai disadari bahwa internet mulai tumbuh ke seluruh dunia dengan pesat. Sehingga banyak bermunculan protokol internet. Sehingga disadari bahwa dibutuhkan sebuah protokol internet yang standar, yaitu OSI (Open System Interconnection). Tetapi pada perkembangannya, TCP/IP menjadi standar de facto yaitu standar yang diterima karena pemakaiannya secara sendirinya semakin berkembang.



Gambar 2: 7 Lapisan / Layer Model OSI (Open System Interconnection)

2.2 TCP / Transmission Control Protocol

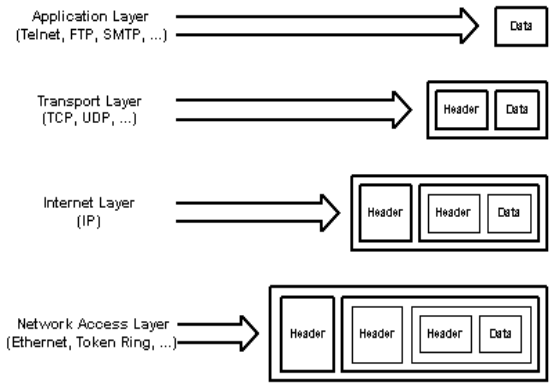
Transmission Control Protocol atau yang sering kali disingkat menjadi TCP berfungsi untuk melakukan transmisi transmisi data per-segmen (packet data dipecah dalam jumlah yang sesuai dengan besaran packet kemudian dikirim satu persatu hingga selesai). Agar pengiriman data sampai dengan baik, maka pada setiap packet pengiriman, TCP akan menyertakan nomor seri (sequence number). Adapun komputer tujuan yang menerima packet tersebut harus mengirim balik sebuah sinyal acknowledge dalam satu periode yang ditentukan. Bila pada waktunya komputer tujuan belum juga memberikan acknowledge, maka terjadi time out yang menandakan pengiriman packet gagal dan harus diulang kembali. Model protokol TCP disebut sebagai connection oriented protocol.

2.3 IP / Internet Protocol

IP (Internet Protocol) address atau alamat IP yang bahasa awamnya bisa disebut dengan kode pengenal komputer pada jaringan merupakan komponen vital pada internet, karena tanpa alamat IP seseorang tidak akan dapat terhubung ke internet.

2.3.1 Konsep Dasar IPv4

Alamat IP (IPv4) pada awalnya adalah sederetan bilangan biner sepanjang 32 bit yang dipakai untuk mengidentifikasi *host* pada jaringan. Prinsip kerjanya adalah packet yang membawa data dimuati alamat IP dari komputer pengirim data kepada alamat IP pada komputer yang akan dituju, kemudian data tersebut dikirim ke jaringan. Packet ini kemudian dikirim dari router ke router dengan berpedoman pada alamat IP tersebut menuju ke komputer yang dituju. Oleh karena itulah alamat IP suatu komputer itu unik.



Gambar 3: Model TCP/IP

2.3.2 Pembagian kelas IPv4

Pada IPv4 dapat dibagi menjadi 3 kelas yang tergantung dari besarnya bagian host:

1. Kelas A (bagian host sepanjang 24 bit, terdiri dari 16,7 juta host)
2. Kelas B (bagian host sepanjang 16 bit, terdiri dari 65.534 host)
3. Kelas C (bagian host sepanjang 8 bit, terdiri dari 254 host)

Konsep kelas ini memiliki keuntungan yaitu pengelolaan rute informasi tidakmemerlukan seluruh 32 bit tersebut melainkan cukup hanya bagian jaringannya saja, sehingga besar informasi rute yang disimpan di router, menjadi kecil.

2.3.3 Format alamat IPv4

Pemberian alamat dalam internet mengikuti format alamat IP (RFC 1166). Alamat ini dinyatakan dengan 32 bit (bilangan 0 dan 1) yang dibagi atas 4 bagian (setiap bagian terdiri dari 8 bit atau oktet) dan tiap kelompok dipisahkan oleh sebuah tanda titik. Untuk memudahkan pembacaan, penulisan alamat dilakukan dengan angka desimal, misalnya:

192.168.1.2

Jika dinyatakan dalam biner menjadi :

11000000.10101000.00000001. 00000010

Dari 32 bit ini berarti banyaknya jumlah maksimum alamat yang dapat dituliskan adalah 2^{32} atau 4.294.967.296 alamat.

Adapun format alamat IPv4 terdiri dari 2 bagian, netid

dan hostid. Netid sendiri menyatakan alamat jaringan sedangkan hostid menyatakan alamat lokal (host/ router). Akan tetapi dari 32 bitini tidak boleh semuanya angka 0 atau 1 (0.0.0.0 digunakan untuk jaringan yang tidak dikenal dan 255.255.255.255 digunakan untuk broadcast)

Dengan perkembangan internet dan jaringan akhir-akhir ini telah membuat internet protocol (IP) yang merupakan tulang punggung jaringan berbasis TCP/ IP dengan cepat menjadi ketinggalan zaman, dan alamat IPv4 pun juga akan habis terpakai.

2.3.4 Penggantian IPv4 menjadi IPv6

Setelah IPv4 sukses penggunaannya oleh para pengguna internet, kemudian timbul suatu permasalahan baru dimana IPv4 hanya dapat menampung para pengguna internet sebanyak 4,3 milyar saja, sedangkan angka ini diperkirakan akan melonjak kembali beberapa tahun kedepan. Berdasarkan hal itulah kemudian dirancang suatu internet protocol baru yang dinamakan IP next generation (IPng) pada tahun 1996 yang penggunaannya secara bertahap akan menggeser penggunaan dari IPv4 yang telah sukses sebelumnya.

IPng atau disebut juga IPv6 sendiri adalah suatu protokol layer ketiga terbaru yang diciptakan untuk menggantikan IPv4 atau yang sering dikenal sebagai IP. Alasan utama dari penciptaan Internet Protocol Version 6 ini adalah untuk mengoreksi masalah pengalamatan pada versi 4 (IPv4). Karena kebutuhan akan alamat internet semakin banyak, maka IPv6 diciptakan dengan tujuan untuk memberikan pengalamatan yang lebih banyak dibandingkan dengan IPv4, sehingga perubahan pada IPv6 masih berhubungan dengan pengalamatan IP sebelumnya. Perubahan terbesar pada IPv6 adalah terdapat pada header, yaitu peningkatan jumlah alamat dari 32 bit (IPv4) menjadi 128 bit (IPv6).

2.4 IPv6 (Internet Protocol Version 6)

Seperti yang telah diketahui sebelumnya IPv4 akan diganti oleh IPv6 dikarenakan keterbatasan pengelamatan.

Tabel 1. Contoh address IPv6

Octect or Bytes	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Bits	0-8	9-16	17-24	25-32	33-40	41-48	49-56	57-64	65-72	73-80	81-88	89-96	97-104	105-112	113-120	121-128
Hex	20	1	DB	08	F5	F5	00	00	F5	F5	00	00	C0	00	02	01
Binary	00100000	00000001	11011011	00001000	11110101	11110101	00000000	00000000	11110101	11110101	00000000	00000000	11000000	00000000	00000010	00000001
Decimal	32	1	219	8	245	245	0	0	245	245	0	0	192	0	2	1

Shortcuts:

Leading Zero Compression	20	01	DB	8	F5	F5	0	0	F5	F5	0	0	C0	0	2	1
Zero-Compressed	20	01	DB	8	F5	F5	::		F5	F5	0	0	C0	0	2	1
Mixed Notation IPv4-mapped	20	01	DB	8	F5	F5	::		F5	F5	FF	FF	192	0	2	1

2.4.1 Kelebihan IPv6

Keunggulan Internet Protocol version 6 dibandingkan Internet Protocol version 4 adalah Otomatisasi Setting. Alamat pada IPv4 pada dasarnya statis terhadap *host*. Biasanya diberikan berurut pada *host*. Walaupun sekarang ini sudah terdapat DHCP (Dynamic Host Configuration Protocol), tetapi DHCP merupakan fungsi tambahan pada IPv4 sedangkan pada IPv6 fungsi untuk men-setting secara otomatis disediakan secara standar dan merupakan default-nya. Pada setting otomatis terdapat dua cara tergantung penggunaan address, yaitu:

1. Setting Otomatis Stateless
   Cara ini tidak perlu menyediakan server untuk pengelolaan dan pembagian IP address, hanya setting router saja dimana host yang telah tersambung di jaringan tersebut. Kemudian *host* menambah pattern bit yang diperoleh dari informasi yang unik terhadap *host*, lalu membuat IP address sepanjang 128 bit dan menjadikannya sebagai alamat IP dari host tersebut.

2. Setting Otomatis Statefull
   Merupakan pengelolaan secara ketat dalam hal range IP address yang diberikan pada *host* dengan menyediakan *server* untuk pengelolaan keadaan alamat IP, dimana cara ini hampir mirip dengan cara DHCP pada IPv4. Pada saat melakukan settring secara otomatis, informasi yang dibutuhkan antara router, server, dan *host* adalah ICMP (Internet Control Message Protocol) yang telah diperluas. Pada ICMP dalam IPv6 ini, termasuk pula IGMP (Internet Group management Protocol) yang dipakai pada *multicast* dalam IPv4.

Selain Otomatis Setting, Keamanan pada IPv6 juga lebih terjaga. Saat ini metode pengamanan dengan menggunakan S-HTTP (Secure HTTP) untuk pengiriman nomor kartu kredit, dll dengan mengenkripsinya atau mengenkripsi email dengan PGP (Pretty Good Privacy) telah dipakai secara umum Tetapi cara diatas adalah keamanan yang ditawarkan oleh aplikasi (kita harus memakai aplikasi tertentu untuk mendapatkan keamanan diatas). Jika kita membutuhkan sekuriti pada komunikasi tanpa tergantung pada aplikasi tertentu maka diperlukan fungsi sekuriti pada layer TCP/IP, karena IPv4 tidak mendukung fungsi keamanan ini kecuali dipasang suatu aplikasi khusus agar bisa mendukung sekuriti.

Berbeda dengan IPv6. Pada IPv6 telah mendukung komunikasi terenkripsi maupun *authentication* pada layer IP. Dengan memiliki fungsi sekurity pada IP itu sendiri, maka dapat dilakukan hal seperti packet yang dikirim dari host tertentu seluruhnya dienkripsi. Pada IPv6 untuk authentication dan komunikasi terenkripsi memakai header yang diperluas atau yang disebut AH (Authentication Header) dan payload yang dienkripsi yang disebut ESP (Encapsulating Security Payload). Pada komunikasi yang memerlukan enkripsi kedua atau salah satu header tersebut ditambahkan . Fungsi sekurity yang dipakai pada layer aplikasi, misalnya pada S-HTTP dipakai SSL sebagai metode enkripsi, sedangkan pada PGP memakai IDEA menjadi metode enkripsinya. Sedangkan manajemen kunci memakai cara tertentu pula. Sebaliknya, pada IPv6 tidak ditetapkan cara tertentu dalam metode enkripsi dan manajemen kunci, sehingga menjadi fleksibel dapat memakai metode manapun. Hal ini dikenal sebagai SA (Security Association). Fungsi Sekuriti pada IPv6 selain pemakaian pada komunikasi terenkripsi antar jaringan dengan cara mengenkripsi packet oleh gateway dari 2 jaringan yang melakukan komunikasi tersebut.

Selain itu kelebihan lain dari IPv6 seperti yang telah diketahui sebelumnya bahwa IPv6 mempunyai address 128 bit. Sehingga dapat menampung kira-kira 3.4 x 10^{38} address. Selain itu masih terdapat keunggulan-keunggulan yang lain.

3. HASIL DAN PEMBAHASAN

3.1 Dasar Pengamanan IPv6

Pengamanan Internet Protocol version 6 menggunakan sebuah protokol yang dinamakan IPSec. IPsec (IP Security) adalah sebuah protokol yang digunakan untuk mengamankan transmisi datagram dalam sebuah internetwork berbasis TCP/IP. terdapat beberapa standar untuk melakukan enkripsi data dan juga integritas data pada lapisan kedua dalam DARPA Reference Model (internetwork layer). IPSec melakukan enkripsi terhadap data pada lapisan yang sama dengan protokol IP dan menggunakan teknik *tunneling* untuk mengirimkan informasi melalui jaringan Internet atau dalam jaringan Intranet secara aman.

Tabel 2. DARPA Reference Model

ke-	Nama lapisan	Keterangan
4	Application Layer	Lapisan ini bertanggung jawab dalam rangka menyediakan akses kepada aplikasi terhadap jaringan TCP/IP. Protokol-protokol yang berjalan pada lapisan ini adalah protokol Dynamic Host Configuration Protocol (DHCP), Domain Name System (DNS), Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), Telnet, Simple Mail Transfer Protocol (SMTP), Simple Network Management Protocol (SNMP), dan lain-lain.
3	Host-to-Host Layer	Lapisan ini bertanggung jawab dalam rangka membuat komunikasi antar dua host, dengan menggunakan cara membuat sebuah sesi *connection-oriented* atau menyebarkan sebuah *connectionless broadcast*. Protokol-protokol yang berjalan pada lapisan ini adalah protokol Transmission Control Protocol (TCP) dan User Datagram Protocol (UDP).
2	Internetworking Layer	Lapisan ini bertanggung jawab dalam melakukan routing dan pembuatan paket IP (dengan menggunakan teknik *encapsulation*). Protokol-protokol yang berjalan pada lapisan ini adalah Internet Protocol (IP), Address Resolution Protocol (ARP), Internet Control Message Protocol (ICMP), serta Internet Group Management Protocol (IGMP).

IPSec diimplementasikan pada lapisan transport dalam OSI Reference Model untuk melindungi protokol IP dan protokol-protokol yang lebih tinggi dengan menggunakan beberapa kebijakan keamanan yang dapat dikonfigurasikan untuk memenuhi kebutuhan keamanan pengguna, atau jaringan. IPSec umumnya diletakkan sebagai sebuah lapisan tambahan di dalam stack protokol TCP/IP dan diatur oleh setiap kebijakan keamanan yang diinstalasikan dalam setiap mesin komputer dan dengan sebuah skema enkripsi yang dapat dinegosiasikan antara pengirim dan penerima. Kebijakan-kebijakan keamanan tersebut berisi kumpulan filter yang diasosiasikan dengan kelakuan tertentu. Ketika sebuah alamat IP, nomor port TCP dan UDP atau protokol dari sebuah paket datagram IP cocok dengan filter tertentu, maka kelakukan yang dikaitkan dengannya akan diaplikasikan terhadap paket IP tersebut.

Untuk membuat sebuah sesi komunikasi yang aman antara dua komputer dengan menggunakan IPSec, maka dibutuhkan sebuah framework protokol yang disebut dengan ISAKMP/Oakley. Protokol ISAKMP / Oakley menggunakan algoritma Diffie-Hellman. Selama proses negosiasi dilakukan, persetujuan akan

tercapai dengan metode autentikasi dan kemanan yang akan digunakan, dan protokol pun akan membuat sebuah kunci yang dapat digunakan bersama (shared key) yang nantinya digunakan sebagi kunci enkripsi data. IPSec mendukung dua buah sesi komunikasi keamanan, yakni sebagai berikut:

protokol Authentication Header (AH): menawarkan autentikasi pengguna dan perlindungan dari beberapa serangan (umumnya serangan man in the middle), dan juga menyediakan fungsi autentikasi terhadap data serta integritas terhadap data. Protokol ini mengizinkan penerima untuk merasa yakin bahwa identitas si pengirim adalah benar adanya, dan data pun tidak dimodifikasi selama transmisi. Namun demikian, protokol AH tidak menawarkan fungsi enkripsi terhadap data yang ditransmisikannya. Informasi AH dimasukkan ke dalam header paket IP yang dikirimkan dan dapat digunakan secara sendirian atau bersamaan dengan protokol Encapsulating Security Payload.

Tabel 3. Diagram paket AH

0 - 7 bit	8 - 15 bit	16 - 23 bit	24 - 31 bit
Next header	Payload length	RESERVED	
Security parameters index (SPI)			
Sequence number			
Authentication data (variable)			

protokol Encapsulating Security Payload (ESP): Protokol ini melakukan enkapsulasi serta enkripsi terhadap data pengguna untuk meningkatkan kerahasiaan data. ESP juga dapat memiliki skema autentikasi dan perlindungan dari beberapa serangan dan dapat digunakan secara sendirian atau bersamaan dengan Authentication Header. Sama seperti halnya AH, informasi mengenai ESP juga dimasukkan ke dalam header paket IP yang dikirimkan.

Beberapa perangkat keras serta perangkat lunak dapat dikonfigurasikan untuk mendukung IPSec, yang dapat dilakukan dengan menggunakan enkripsi kunci publik yang disediakan oleh Certificate Authority (dalam sebuah public key infrastructure) atau kunci yang digunakan bersama yang telah ditentukan sebelumnya (skema Pre-Shared Key/PSK) untuk melakukan enkripsi secara privat.

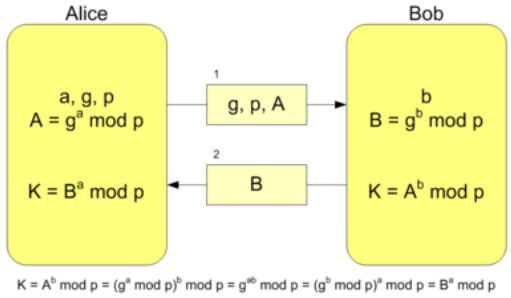
Tabel 4. Diagram paket ESP

0 - 7 bit	8 - 15 bit	16 - 23 bit	24 - 31 bit
Security parameters index (SPI)			
Sequence number			
Payload data (variable)			
	Padding (0-255 bytes)		
		Pad Length	Next Header
Authentication Data (variable)			

3.2.Protokol Diffie-Hellman

Protokol Diffie Hellman adalah sebuah protokol dalam kriptografi yang memperbolehkan 2 buah pihak yang belum memiliki pengetahuan mengenai satu sama lain untuk bertukar kode melalui jaringan komunikasi yang tidak diamankan. Dan kode ini dapat digunakan untuk mengenkripsi komunikasi yang berurutan menggunakan *symetri key cipher* (sebuah algoritma kriptografi untuk mendekripsi dan mengenkripsi data).

Kode ini pertama kali dikembangkan pada tahun 1976 oleh Whitfield Diffie dan Martin Hellman. Walaupun Diffie-hellman kode adalah anonymous key-agreement protokol, kode ini memberikan asas untuk berbagai protokol yang perlu di-autentikasi dan digunakan untuk memberikan *perfect forward secrecy* di mode singkat pada lapisan keamanan transport yang sempurna.



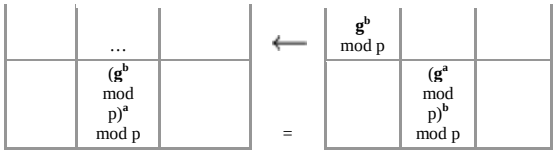
Gambar 4: Diagram Cara Pemakaian Diffie-Hellman Pertukaran Kode

Keterangan:
s = shared secret key (kode rahasia)
a = kode rahasia pihak I
b = kode rahasia pihak II
g = dasar publik (bilangan prima)
p = bilangan prima publik

Implemetasi yang paling sederhana dan asli dari protokol menggunakan himpunan bilangan modulo p yang *multiplicative*, dimana p adalah prima dan g adalah *primitif root modulo*. Berikut adalah contoh dari protokol tersebut:

Tabel 5. Contoh Penggunaan Protokol Diffie-Hellman

Alice				**Bob**	
Sec		Calc		Calc	Sec
	p, g			**p, g**	
a					**b**
		$g^a \bmod p$	→	…	



Keterangan:

1. Alice and Bob setuju untuk menggunakan sebuah bilangan prima p=23 dan basis g=5.
2. Alice memilih kode rahasia *a*=6, dan mengirim Bob ($g^a \bmod p$), $5^6 \bmod 23 = 8$.
3. Bob memilih kode rahasia *b*=15, dan mengirim Alice ($g^b \bmod p$), $5^{15} \bmod 23 = 19$.
4. Alice mengkomputasi $(g^b \bmod p)^a \bmod p$, $196 \bmod 23 = 2$.
5. Bob mengkomputasi $(g^a \bmod p)^b \bmod p$, $815 \bmod 23 = 2$.

Baik Alice dan Bob sudah mencapai nilai yang sama, dikarenakan g^{ab} dan g^{ba} adalah sama. Perhatikan bahwa a,b, dan $g^{ab} = g^{ba}$ dirahasiakan. Nilai-nilai yang lain tidak dirahasiakan. Setelah Alice dan Bob mengkomputasi rahasia yang telah mereka bagi, mereka dapat menggunakannya sebagai kunci enkripsi, yang hanya diketahui oleh mereka, untuk mengirimkan pesan melalui jaringan komunikasi yang sama. Tentu saja, makin besar nilai a, b, dan p dibutuhkan untuk membuat contoh ini aman, karena mudah untuk mencoba semua kemungkinan nilai dari $g^{ab} \bmod 23$. Jika p adalah sebuah bilangan prima yang nilainya minimal 300 digits, dan a maupun b setidaknya 100 digit, maka algoritma yang termangkus saat ini-pun belum dapat menemukan nilai g, p, dan $g^a \bmod p$, bahkan menggunakan semua komputasi buatan manusia. Masalah ini dikenal sebagai masalah logaritma diskrit. Perhatikan bahwa g tidak perlu bernilai besar.

Protokol Diffie-Hellman secara umum

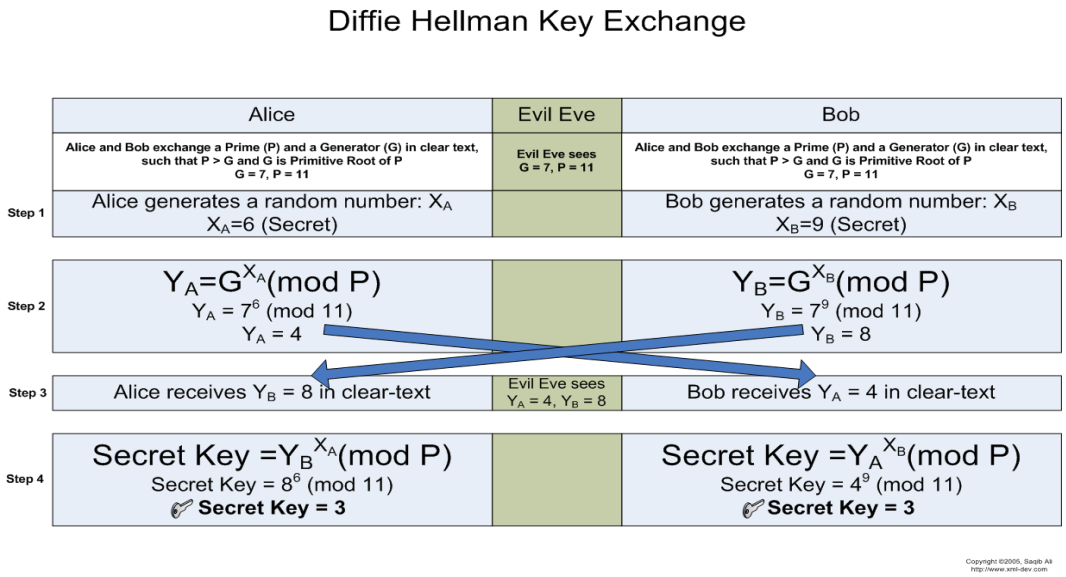
1. Alice dan Bob menyetujui sebuah siklus G terbatas dan element g yang akan dihasilkan ada didalam G (Hal ini biasanya dilakukan sebelum sisa protokol; g diasumsikan diketahui oleh semua penyerang.) G akan ditulis berulang.
2. Alice mengirim sebuah angka natural yang acak dan mengirimkan g^a kepada Bob
3. Bob mengirim sebuah angka natural yang acak dan mengirimkan g^b kepada Alice
4. Alice mengkomputasi $(g^b)^a$
5. Bob mengkomputasi $(g^a)^b$
6. Baik Alice dan Bob sekarang memiliki himpunan gab, yang mana berfungsi sebagai kode rahasia yang dibagi. Nilai $(g^b)^a$ dan $(g^a)^b$ sama dikarenakan keduanya adalah *power associative*.

Tabel 6. Contoh Jika Terjadi Curi Dengar (Eavesdropper) ketika Penggunaan Protokol Diffie-Hellman

Alice		**Bob**		**Eve**	
tahu	Tidak tahu	tahu	Tidak tahu	tahu	Tidak tahu
p = 23	b = 15	p = 23	a = 6	p = 23	a = 6
base g = 5		base g = 5		base g = 5	b = 15
a = 6		b = 15			s = 2
$5^6 \bmod 23 = 8$		$5^{15} \bmod 23 = 19$		$5^a \bmod 23 = 8$	
$5^b \bmod 23 = 19$		$5^a \bmod 23 = 8$		$5^b \bmod 23 = 19$	
$19^6 \bmod 23 = 2$		$8^{15} \bmod 23 = 2$		$19^a \bmod 23 = s$	
$8^b \bmod 23 = 2$		$19^a \bmod 23 = 2$		$8^b \bmod 23 = s$	
$19^6 \bmod 23 = 8^b \bmod 23$		$8^{15} \bmod 23 = 19^a \bmod 23$		$19^a \bmod 23 = 8^b \bmod 23$	
s = 2		s = 2			

Keterangan:
s = shared secret key (kode rahasia). S = 2
a = kode rahasia Alice. a = 6
b = kode rahasia Bob. b = 15
g = dasar publik . g = 5
p = bilangan prima publik . p = 23

Perhatikan bahwa kode rahasia Bob tidak akan dengan mudah dipecahkan oleh Alice, begitu juga sebaliknya. Dengan demikian Eve tidak dapat menemukan kode rahasia dengan mudah.



Gambar 5: Contoh Bagan Pemakaian Diffie-Hellman Pertukaran Kode

Agar lebih aman ordo dari G haruslah prima atau memiliki banyak faktor prima untuk menghindari pemakaian algoritma Pohlig-Hellman untuk mendapatkan a-b. Karena alasan ini, bilangan prima Sophie Germain biasanya digunakan sebagai bilangan prima publik. Bilangan prima sophie Germain adalah p,

$$p = 2q + 1$$

Dimana, p adalah bilangan prima Siophie Germain, jika q adalah bilangan prima juga.

Pada deskripsi awal, protokol Diffie-hellman tidak menyediakan *authentication* untuk kedua belah pihak, dan karena itulah protokol ini lemah terhadap *man-in-the-middle-attack* (sebuah serangan, dimana penyerang dapat membaca, menyisipkan, dan memodifikasi sesuai kemauannya, pesan diantara kedua belah pihak tanpa diketahui oleh pihak manapun). Untuk itulah dibutuhkan sebuah protokol tambahan untuk mengautentikasi pesan yang diterima.

3.3 Simulasi Algoritma Diffie Hellman

1. Albert and Raditya setuju untuk menggunakan sebuah bilangan prima p=359 dan basis g=6.
2. Albert memilih kode rahasia *a*=100, dan mengirim Raditya (g^a mod p), 6^{100} mod 359 = 148.
3. Raditya memilih kode rahasia *b*=168, dan mengirim Albert (g^b mod p), 6^{168} mod 359 = 33.
4. Albert mengkomputasi (g^b mod p)^a mod p , 7.102217821 x10^{151} mod 359 = 123.
5. Raditya mengkomputasi (g^a mod p)^b mod p, 4.0176137929166 x10^{364} mod 359 = 123.

Dari Algoritma Diffie Hellman, kode rahasia yang dihasilkan adalah 123. Dan kode rahasia tersebut dapat digunakan untuk kode yang dipakai dalam mengenkripsi data. Dan bila

4. KESIMPULAN

Kesimpulan yang dapat diambil dari makalah ini adalah :

1. IPv6 menggunakan IPSec sebagai protokol keamanan. IPSec adalah sebuah protokol yang digunakan untuk mengamankan transmisi datagram dalam sebuah internetwork berbasis TCP/IP. Terdapat beberapa standar untuk melakukan enkripsi data dan juga integritas data pada lapisan kedua dalam DARPA Reference Model (internetwork layer).

2. Agar komunikasi aman, maka sesi komunikasi antara dua komputer dengan menggunakan IPSec, maka dibutuhkan sebuah framework protokol yang disebut dengan ISAKMP/Oakley. Protokol ISAKMP / Oakley menggunakan algoritma Diffie Hellman dalam mempertukarkan kunci rahasia yang akan digunakan dalam mengenkripsi data IPSec mendukung dua buah sesi komunikasi keamanan, yakni protokol Authentication Header (AH) dan protokol Encapsulating Security Payload (ESP).

3. Diffie Hellman adalah protokol dalam kriptografi yang memperbolehkan 2 buah pihak yang belum memiliki pengetahuan mengenai satu sama lain untuk bertukar kode melalui jaringan komunikasi yang tidak diamankan. Dan kode ini dapat digunakan untuk mengenkripsi komunikasi yang berurutan menggunakan *symetri key cipher*

(sebuah algoritma kriptografi untuk mendekripsi dan mengenkripsi data). Secara umum, Algoritma Diffie Huffman merupakan sebuah algoritma yang aman untuk saling mempertukarkan kunci rahasia.

DAFTAR REFERENSI

[1] Sobana, Aceh, 2006. *Jaringan Komputerdan Internet (Sebuah Pengantar).* http://www.geocities.com/malikiinfo/j2.PDF waktu akses : 25 Desember 2007 pukul 10.52

[2] Gilbert, H., 1995. *Introduction to TCP/IP* http://www.yale.edu/pclt/COMM/TCPIP.HTM waktu akses : 26 Desember 2007 pukul 15.25

[3] Stallfig, Paul, 2007. *IPv6-101: Introduction* http://www.f5.com/pdf/white-papers/ipv6-introduction.pdf waktu akses : 26 Desember 2007 pukul 15.25

[4] Terr, David, 2004. *Diffie-Hellman Protocol* http://mathworld.wolfram.com/Diffie-HellmanProtocol.html waktu akses : 26 Desember 2007 pukul 15.25

[5] http://en.wikipedia.org/wiki/Diffie_Hellman waktu akses : 26 Desember 2007 pukul 15.25

[6] Sugeng, Winarno, *Jaringan Komputer dengan TCP/IP*, Penerbit Informatika, 2006