ANALISIS KEAMANAN PADA JARINGAN *ASYNCHRONOUS TRANSFER MODE* (ATM)

Gina Nuryanti
Jurusan Teknik Informatika Fakultas Teknik Universitas Komputer Indonesia
Jl. Dipati Ukur No. 112-114 Bandung 40132

ABSTRAK

Pada beberapa tahun terakhir keamanan menjadi semakin penting pada lingkungan jaringan dengan munculnya teknologi *internetworking*. Teknologi *Internetworking* menyediakan saluran komunikasi ke jaringan lain sedemikian sehingga jaringan berbeda dapat berkomunikasi satu sama lain. Bagaimanapun juga, komunikasi *Internetworking* sangat rentan terhadap bermacam-macam serangan dalam suatu lingkungan publik. Kebanyakan teknologi jaringan pada mulanya tidak diintegrasikan dengan mekanisme keamanan, harus dilakukan perancangan ulang agar menyediakan beberapa layanan keamanan. ATM adalah salah satu dari teknologi itu.

Pada mulanya, ATM merupakan mode transfer untuk mengimplementasikan teknologi BISDN (Broadband Integrated Services Digital Network) sedemikian sehingga semua format data trafik (voice, video, data) dapat ditransfer di atas jaringan telekomunikasi. ATM selalu mengirimkan data dalam suatu unit yang berukuran tetap yang disebut sel. Suatu sel mempunyai 5 Byte header dan 48 Byte *payload* (informasi). Sel disambungkan berdasarkan 5 Byte header. Dengan cara itu, suatu sel dapat melewati *switch* dengan cepat. Untuk mempertemukan kebutuhan yang berbeda dari trafik yang spesifik, ATM juga memperkenalkan konsep *Quality of Service* (QoS). Sesungguhnya isu keamanan ATM belum memperoleh perhatian yang cukup sampai 1995, akhirnya suatu kelompok di dalam ATM Forum telah dibentuk untuk menunjukkan isu keamanan tersebut. Oleh karena itu, dibandingkan dengan area keamanan lain, keamanan ATM masih dalam tahap permulaan.

Kata kunci : Internetworking, BISDN, ATM, QoS.

ABSTRACT

In recent years, security has been more and more significant in network environment with the emergence of the internetworking technology. The internetworking technology can provide the communication channels across networks so that machines in different networks can talk to each other. However, the internetworking communication will be exposed to all kinds of attacks in such an open environment. Most of the network technologies, without integrating with security mechanism originally, have to be redesigned to provide some security services. ATM is one of those technologies.

Originally ATM is a transfer mode to implement the BISDN(Broadband Integrated Services Digital Network) technology so that all forms of data traffic(voice, video, data) can be transferred over telecommunication networks. ATM always delivers data in a fixed size unit, which is called a cell. A cell has 5 octet header and 48 octet payload. Cell switching will base on the 5 octet header. In the way, a cell can go through a switch very quickly. To meet different requirements of specific traffic, ATM also introduces the concept of Quality of Service(QoS). In fact, issues in ATM security have not gained enough attention until 1995, when a group within ATM Forum was established to address the security issues. Therefore, compared with other security area, ATM security is still in its beginning.

Keyword : Internetworking, BISDN, ATM, QoS.

I. PENDAHULUAN

ATM merupakan konsep teknologi komunikasi yang telah distandarisasi oleh International Telegraph and Telephony / CCITT (kini Internatinal Telecomunication Union / ITU) sebagai implementasi BISDN.

ATM dirancang untuk mentransfer informasi dengan kecepatan tinggi dan dialirkan melaui satu jaringan telekomunikasi.

Karakteristik ATM, yaitu :

a. Pada basis link demi link tidak menggunakan perlindungan *error* dan *flow control*.
b. ATM beroperasi pada mode *connection oriented*
c. Pengurangan fungsi *header*
d. Panjang *field* informasi dalam satu sel relatif kecil

Pada prinsipnya informasi yang masuk ke jaringan ATM akan dibagi menjadi paket-paket berukuran sama disebut sel. Tiap sel ditambah header agar paket dapat dirutekan ke tujuan. Sel-sel dimasukan kedalam pipa transmisi berukuran besar yang mencampur semua sel dari sumber yang berbeda.

Koneksi Logik ATM ada dua macam, yaitu :

1. *Virtual Channel Connections* (VCC) merupakan koneksi logik antar dua *endpoint* untuk mentransfer informasi pada jaringan ATM
2. *Virtual Path Connection* (VPC) merupakan koneksi logik dari kesatuan VCC yang memiliki ujung-ujung yang sama.

Menurut model referensi protokol BISDN jaringan ATM melibatkan tiga lapisan, yaitu :

1. Lapisan Fisik (Physical Layer) digunakan untuk mengirimkan informasi (bit/cell).
2. Lapisan ATM (ATM Layer) adalah lapisan diatas lapisan fisik yang memiliki karakteristik

independent terhadap media fisik yang digunakan. Lapisan ATM menambah 5 Byte *header* pada 48 Byte data yang diterima dan AAL mengirimkannya ke lapisan fisik. Demikian pula proses sebaliknya Lapisan ATM menerima sel (53 Byte) dari lapisan fisik, memproses header dan mengirim 48 Byte data ke AAL.

3. Lapisan Adaptasi ATM (ATM Adaptation Layer/AAL) berfungsi memperkaya layanan yang disediakan lapisan ATM sehingga dapat memenuhi level yang diminta oleh *higher layer*.

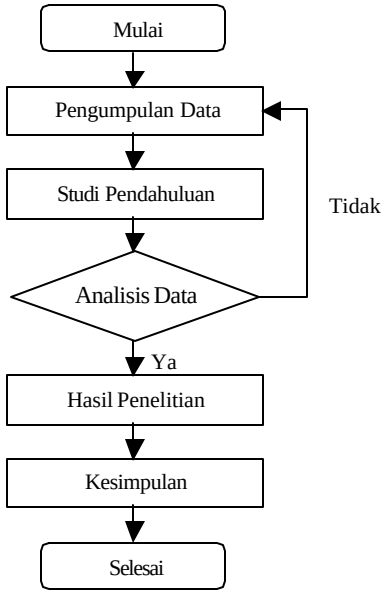
Model referensi protokol BISDN jaringan ATM juga melibatkan tiga taraf yaitu :

1. Taraf pemakai (User Plane) meliputi seluruh mekanisme yang berhubungan dengan transfer informasi dari *user*
2. Taraf kendali (Control Plane) bertanggung jawab terhadap fungsi-fungsi kendali panggilan dan kendali koneksi meliputi menetapkan / memutuskan suatu koneksi dan monitoring karakteristik suatu koneksi yang mana fungsi-fungsi ini merupakan fungsi-fungsi pensinyalan
3. Taraf manajemen (Management Plane) meliputi fungi manajemen lapisan yaitu berhubungan dengan sumber daya dan parameter-parameter yang ada dalam entitas protokolnya dan fungsi taraf manajemen menyediakan koordinasi diantara seluruh taraf yang ada.

II. METODOLOGI PENELITIAN

Metodologi penelitian yang digunakan adalah deskriptif analisis yaitu dengan cara mendeskripsikan permasalahan yang ada pada masa sekarang.

Teknik yang digunakan dalam pengumpulan data tugas akhir ini adalah studi kepustakaan yaitu penulis menggunakan sumber-sumber otentik dari buku, jurnal, artikel dan *browsing* internet untuk mendapatkan data dan informasi selengkap-lengkapnya.



Gambar 1. Diagram Alir Metodologi Penelitian

III. HASIL PENELITIAN

1. Serangan pada Jaringan ATM dan Akibatnya

1. *Eavesdropping* adalah suatu serangan terhadap jaringan komunikasi dengan cara melakukan pencantolan (*tap*) pada media transmisi sehingga penyerang bisa mengakses informasi yang tersedia.
2. *Spoofing* adalah serangan yang dilakukan oleh seseorang dengan cara berpura-pura menjadi salah satu *user* kepada pihak ketiga.
3. *Denial of Service* adalah mekanisme serangan apabila seorang penyerang melakukan pemutusan *Virtual Circuit* (VC) yaitu pengiriman *sinyal release* atau *drop party* secara berulang-ulang melalui salah satu *switching* kepada suatu VC.
4. Pencurian *Virtual Channel* yaitu bila salah satu satu *user* pada suatu *switching* menggunakan satu atau lebih VC untuk mengirimkan sel-sel data ke *user* lainnya. VC-VC tersebut sudah tersambung sebelumnya antar *switching* dimana *user-user* tersebut berada.
5. *Traffic Analysis* mengacu pada ancaman yang dilakukan *Cracker* dengan cara mengumpulkan dan menganalisa informasi seperti *volume* data, waktu pengiriman dan pihak yang berkomunikasi pada suatu VC.

2. Spesifikasi Kebutuhan Layanan Keamanan ATM

1 Authentikasi yaitu menentukan orang atau user yang benar-benar berhak atas akses atau layanan.

2 *Confidentiality* yaitu memberikan jaminan bahwa hanya orang atau *user* yang telah mendapatkan otorisasi yang dapat mengakses data atau informasi dan untuk menjamin keakuratan suatu proses distribusi kunci

3 Integritas yaitu menjamin bahwa data yang ditransmisikan terbebas dari perubahan yang dilakukan pihak ketiga

4 *Non-repudiation* untuk menjamin bahwa jaringan komunikasi tersebut bisa memberikan laporan atau fakta-fakta mengenai penggunaan layanan oleh setiap user, sehingga seseorang tidak bisa menyangkal fakta bahwa dia telah benar-benar menggunakan atau melakukan akses terhadap jaringan

3. Kerangka Sistem Keamanan ATM

1. Verifikasi identitas yaitu sistem keamanan harus mampu menentukan dan memeriksa identitas dari setiap *user* dalam jaringan ATM.
2. Pengendalian akses dan otorisasi adalah suatu mekanisme yang tidak memungkinkan *user* mendapatkan akses terhadap sumber informasi yang tidak berhak diakses oleh *user* tersebut.
3. Perlindungan terhadap *Confidentiality* yaitu data yang tersimpan dan ditransmisikan pada jaringan terjamin kerahasiaannya.
4. Perlindungan terhadap integritas data adalah sistem keamanan harus bisa menjamin integritas dari data yang tersimpan dan ditransmisikan pada jaringan.
5. *Accountability* yang ketat adalah semua pihak tidak bisa menyangkal terhadap tanggung jawab dari tindakan yang dilakukannya serta dampak dari tindakan tersebut.

Tabel 1 Kerangka Sistem Keamanan ATM

Functional Security Requirement		Security Service
Verification of Identities		*User Authentication*
Controlled Access and Authorization		*Access Control*
Protection of Confidentiality	*of stored data*	*Access Control*
	of data in transit	*Confidentiality*
Protection of Integrity	*of stored data*	*Access Control*
	of data in transit	*Integrity*
Strong Accountability		*Non-repudiation*

4. Bahan pertimbangan implementasi kemanan jaringan ATM

4.1. Kriptografi

Enkripsi adalah sebuah proses merubah suatu data menjadi kode yang tidak bisa dimengerti atau dibaca oleh orang yang tidak berhak. Enkripsi merupakan implementasi dari teknik Kriptografi *(Cryptography)*. Adapun jenis kriptografi adalah sebagai berikut :

1. *Symmetric Key Cryptosystem*

   Tipe kriptografi *symmetric* membagi sebuah pesan dalam beberapa blok sebesar n bits, kemudian mengenkripsi setiap blok tersebut dengan sebuah kunci rahasia dengan menggunakan algoritma khusus.

2. *Asymmetric Key Cryptosystem*

   Berbeda dengan tipe *symmetric cryptosystem*, tipe *asymmetric* ini memungkinkan kunci enkripsi dan dekripsi yang berbeda.

4.2. Mode Operasi

a. ***CBC (Chiper Block Chaining)*** merupakan mode operasi yang langsung memasukan *ciphertext* yang dihasilkan dari operasi sebelumnya kedalam suatu operasi XOR dengan *plaintext* sebelum *plaintext* tersebut menghasilkan blok *cipher* dengan urutan tertentu.

b. ***Counter***, merupakan mode operasi yang memasukan *plaintext* kedalam operasi XOR dengan menggunakan *counter* sebelumnya yang telah dienkripsi.

4.3. Perangkat Keras Enkripsi

1. *Application Spesific Integrated Circuits* (ASIC)

   Perangkat ASIC memiliki keunggulan, yaitu berukuran relatif kecil dan mengkonsumsi daya relatif lebih sedikit dan bekerja relatif lebih cepat, karena perangkat ini didesain khusus untuk kasus ini. Kelemahannya adalah tidak mampu memberikan fleksibilitas terhadap suatu perangkat yang bisa dikonfigurasi ulang.

2. *Reconfigurable Hadware* (*Erasable Programmable Logic Devices / Field Gate Arrays* (EPLD/EPGA))

   Keunggulannya perangkat dapat direkonfigurasi, memerlukan waktu perancangan dan verifikasi lebih singkat, perubahan bisa dengan mudah diakomodasi sehingga memungkinkan *upgrade* perangkat dilakukan tanpa harus betul-betul mengganti perangkat tersebut tetapi cukup dengan melakukan pemograman ulang. Kelemahan dari perangkat ini yaitu RC memiliki *overhead* logika yaitu kemampuan perangkat dalam mengakomodasi aplikasi kriptografi dan banyaknya rangkaian RC yang diperlukan untuk mempertahankan *throughput* ATM.

4.4. Authentikasi bisa menggunakan algoritma simetrik dan asimetrik

Tabel 2. Algoritma yang digunakan untuk Authentikasi

Profil	Signature	Hash	Catatan
AUTH-1	DES/CBC	n/a	1,2
AUTH-2	DSA	AHA-1	1
AUTH-3	ECDSA	SHA-1	1
AUTH-4	ESIGN	MD5	1
AUTH-5	FEAL/CBC	n/a	1,2
AUTH-6	RSA	MD5	1

Keterangan

1 : mendukung terhadap keamanan pertukaran pesan atau *Security Message Exchange* (SME)

2 : tidak menggunakan fungsi hash

n/a : tidak bisa diterapkan

4.5. Confidentiality menggunakan algoritma simetrik dan menggunakan mode operasi tertentu.

Tabel 4.3 Algoritma yang digunakan untuk *Confidensiality*

Profil	Enkripsi	Mode	Signature	Key Exchange	Hash	Key Update	Catatan
CONF-1	DES	CBC	RSA	RSA	MD5	MD5	1
CONF-2	DES	CBC	DSA	DH	SHA-1	SHA-1	1
CONF-3	DES	CBC	ECDSA	ECKASH	SHA-1	SHA-1	1
CONF-4	DES	CBC	DES/CBC	DES/CBC	n/a	MD5	1
CONF-5	DES	Counter	RSA	RSA	MD5	MD5	1
CONF-6	DES	Counter	DSA	DH	SHA-1	SHA-1	1
CONF-7	DES	Counter	ECDSA	ECKAS-DH	SHA-1	SHA-1	1
CONF-8	DES	Counter	DES/CBC	DES/CBC	n/a	MD5	1
CONF-9	Triple-DES	CBC	RSA	RSA	MD5	MD5	1
CONF-10	Triple-DES	CBC	DSA	DH	SHA-1	SHA-1	1
CONF-11	Triple-DES	CBC	ECDSA	ECKAS-DH	SHA-1	SHA-1	1
CONF-12	Triple-DES	CBC	Triple DES/CBC	Triple DES/CBC	n/a	MD5	1
CONF-13	Triple-DES	Counter	RSA	RSA	MD5	MD5	1
CONF-14	Triple-DES	Counter	DSA	DH	SHA-1	SHA-1	1
CONF-15	Triple-DES	Counter	ESIGN	EC/DH	SHA-1	SHA-1	1
CONF-16	Triple-DES	Counter	Triple DES/CBC	Triple DES/CBC	n/a	MD5	1
CONF-17	FEAL	CBC	ESIGN	DH	MD5	MD5	1
CONF-18	FEAL	CBC	FEAL/CBC	FEAL/CBC	n/a	MD5	1
CONF-19	FEAL	Counter	ESIGN	DH	MD5	MD5	1
CONF-20	FEAL	Counter	FEAL/CBC	FEAL/CBC	n/a	MD5	1

Keterangan
1 : mendukung terhadap keamanan pertukaran pesan atau *Security Message Exchange* (SME)
n/a : tidak bisa diterapkan

4.6. Integritas data menggunakan algoritma simetrik

Tabel 4.4 Algoritma yang digunakan untuk Integritas data

Profil	MAC	Signature	Key Exchange	Hash	Key Update	Catatan
INTEG-1	DES/CBC	RSA	RSA	MD5	MD5	1,2
INTEG-2	DES/CBC	DSA	DH	SHA-1	SHA-1	1,2
INTEG-3	DES/CBC	EC/DS	EC/DH	SHA-1	SHA-1	1,2
INTEG-4	DES/CBC	DES/CBC	DES/CBC	n/a	MD5	1,2
INTEG-5	H-MD5	RSA	RSA	MD5	MD5	1,2
INTEG-6	H-MD5	DES/CBC	DES/CBC	n/a	MD5	1,2
INTEG-7	H-SHA-1	DSA	DH	H-SHA-1	SHA-1	1,2
INTEG-8	H-SHA-1	EC/DSA	AC/DH	H-SHA-1	SHA-1	1,2
INTEG-9	H-SHA-1	DES/CBC	DES/CBC	n/a	SHA-1	1,2
INTEG-10	FEAL/CBC	ESIGN	DH	MD5	MD5	1,2
INTEG-11	FEAL/CBC	FEAL/CBC	FEAL/CBC	n/a	MD5	1,2

Keterangan
1 : mendukung keamanan pertukaran pesan
2 : mendukung integritas dengan atau tanpa diperlukannya perlindungan pengulangan (replay protection). Pemilihan dirundingkan saat *call setup time*
n/a : tidak bisa diterapkan

4.7. Akses Kendali

Akses kendali dilaksanakan pada basis tiap VC. Secara umum akses kontrol dapat didasarkan pada label keamanan baku, identitas sumber atau tujuan, waktu, jenis layanan, protokol lapisan atas (seperti Internet Protokol), atau parameter lain yang ditentukan saat penetapan koneksi.

IV. KESIMPULAN

Aspek keamanan jaringan ATM pada taraf pemakai masih terus dikembangkan dan baru pada tahap permulaan. Sistem keamanan jaringan ATM pada tahap pemakai harus fleksibel dan kompatibel dengan teknologi lainnya.

Strategi keamanan jaringan ATM pada taraf pemakai dilaksanakan dengan memilih algoritma dan mode operasi yang sesuai dengan kebutuhan untuk memberikan perlindungan terhadap informasi.

ATM Forum Security Working Group telah mengeluarkan *draft* mengenai spesifikasi dan kerangka keamanan ATM untuk membantu para pemakai jaringan ATM mengidentifikasi masalah yang mungkin terjadi pada layanan keamanan jaringan ATM. Masalah-masalah lainnya sudah dan terus dibahas dalam ATM Forum. Semakin banyak masalah yang teridentifikasi, akan menjadikan keamanan ATM semakin jelas dan semakin baik.

Dari aspek dukungan *vendor*, saat ini sudah tersedia beberapa perangkat untuk keamanan ATM. Sebagian besar memang masih merupakan perangkat enkripsi. Realisasi ini relatif kecil dibandingkan dengan luasnya cakupan keamanan ATM, namun demikian hal ini akan memberikan banyak pengalaman dalam rangka implementasi layanan keamanan pada jaringan ATM.

V. DAFTAR PUSTAKA

1. W. Stalling *"Data and Computer Communications"*, Prentice Hall International, 1996
2. D.C. Green, "Komunikasi Data" , Edisi Bahasa Indonesia, ANDI Yogyakarta, 1996
3. A. S. Tanenbaum, "Jaringan Komputer", PT. Prehalindo, 2000
4. B. Kumar, *"Broadband Communication"*, McGraw-Hill International, halaman 141-363 (1995)
5. M. D. Pycker, *"Asynchronous Transfer Mode : Solution for Broadband ISDN"*, Prentice Hall International, page 105-109 (1995)
6. ATM Forum, *"Asynchronous Transfer Mode (ATM) Tutorial"* , page 1-6 (1995)
7. Anonim, "Kelebihan dan Kekurangan ATM", http://www.geocities.com /downy_f/kedanke.htm (2002)
8. ATM Forum Technical Committee, *"ATM Security Framework 1.0* (afsec-0096.000-Final Ballot in January 1998)" , page 1-25 (1997)
9. ATM Forum Technical Committee, *"ATM Security Specification Version 1.0 (str-sec-01.03 - Straw Ballot in April 98)"* , page 1-215 (1998)
10. Donglin Liang, *"A Survey on ATM Security"*, page 1-11 (1995)

Digitally signed by Gina
cn=Gina, ou=Gina, o=Gina, c=ID
Date: 2003.08.26 16:58:28 +07'00'
Reason: Document is certified