Available online at www.elixirpublishers.com (Elixir International Journal)

Computer Science and Engineering

Elixir Comp. Sci. & Engg. 40 (2011) 5206-5208

ISSN: 2229-712X

Open technological challenges, issues and vulnerabilities in ATM security

Sunil Kumar

Department of MCA, IIMT Engineering College, Meerut (U.P.), India.

ARTICLE INFO

Article history:

Received: 31 August 2011;

Received in revised form:

17 October 2011;

Accepted: 27 October 2011;

Keywords

Quality of Service (QoS),
Broadband-Integrated Services Digital Network (B-ISDN),
Multi-Protocol Label Switching (MPLS),
Third Generation (3G),
Second Generation (2G),
AAL,
GSM,
GPRS,
VoUMTS.

ABSTRACT

Asynchronous Transfer Mode (ATM) is a connection-oriented packet switching technique that is universally accepted as the transfer mode of choice for Broadband Integrated Services Digital Network. The Quality of Service (QoS) capabilities of ATM is one of its major strength. In this paper we have explore some of the technological challenges and issues which plays important role in the security of ATM networks.

Introduction

Asynchronous transfer mode (ATM) is a technology that has its history in the development of broadband ISDN in the 1970s and 1980s. Technically, it can be viewed as an evolution of packet switching. Like packet switching for data (e.g., X.25, frame relay, transmission control protocol [TCP]/Internet protocol [IP]), ATM integrates the multiplexing and switching functions, is well suited for bursty traffic (in contrast to circuit switching), and allows communications between devices that operate at different speeds. Unlike packet switching, ATM is designed for high performance multimedia networking [2][4][5].

Asynchronous Transfer Mode (ATM) is a switching technique for telecommunication networks. It uses asynchronous time-division multiplexing and it encodes data into small, fixed-sized *cells*. This differs from networks such as the Internet or Ethernet LANs that use variable sized *packets* or *frames*. ATM provides data link layer services that run over OSI Layer 1 physical links. ATM has functional similarity with both circuit switched networking and small packet switched networking. This makes it a good choice for a network that must handle both traditional high-speed data traffic (e.g., file transfers), and real-time, low-latency content such as voice and video. ATM uses a connection-oriented model in which a virtual circuit must be established between two endpoints before the actual data exchange begins. ATM is a core protocol used over the SONET/SDH backbone of the Integrated Services Digital Network (ISDN).

Why ATM?

Most of today's network are characterized by transporting just a service for which it was specially designed for, and is often not at all applicable to transporting another service. However, the developing trends in the networking field has brought about a large number of communication services or applications with different service requirements, which may sometimes have unknown requirements. Most customers are always looking forward to getting a network that will take, possible in a single system, the ever increasing number of new services. This large span of new requirements need widely accepted network that is flexible enough to cater for all of these services in the same way. Moreover, if packets are large, which minimizes the amount of segmentations and reassembly that had to be carried out. However, this might not be very suitable for real time traffic(e.g. voice and video) because they will introduce long delays. By forcing the packets length to 53 bytes and giving priority to real time traffic, this traffic need not wait long before being given access to the communication channel. Flexibility and the advancement in technology concepts has therefore led to the development of the Asynchronous Transfer Mode(ATM) network.

ATM Advantages

1. Flexible Bandwidth Allocation
2. Support for all types of data traffic.
3. Simple routing due to connection-oriented mode.
4. Potential QoS guarantees.
5. Compatibility with existing networks.
6. Enable new application due to high speed and integration of traffic types.
7. Simplified Network Management.
8. Incremental Migration.
9. Long Architectural Lifetime.
10. Technological allows per circuit billing and monitoring.
11. High performance via hardware switching.

Tele:
E-mail addresses: mtechsunilarora@gmail.com

12. Scalability in speed and network size.

Applications of ATM

Many application areas will benefit from the use of an ATM network-Medical images such as X-ray may require upto 10 gigabits of digital representation. To enable real-time collaborative discussion between physicians separated by a distance, this large digitized x-ray image has to be transmitted at multigigabit speed. This could be achieved using B-ISDN as it incorporates ATM technology which allows transmission of information at high speeds.

In supercomputer centre, during the visualization of 3-D images, a user may wish to interact with it in real time that is, the effects of changing the image's parameters should be simultaneous. This would require a network capable of high data rate and low latency which could be provided by B-ISDN.

A recent industry development for the internetworking between IP and ATM is Multi-Protocol Label Switching (MPLS) standardized by the IETF. MPLS is being standardized as a technology that can best be described as a synergistic approach between IP and ATM. MPLS merges the flexibility of the IP routing protocols with the speed that ATM switches provide to introduce fast packet switching in frame-based IP networks.

ATM provides convergence in the sense that both voice and data can be carried together.

For voice, the ATM Forum has defined a number of techniques for voice and Telephony over ATM(VTOA). The initial standards by ATM Forum were based on AAL1 while the newer ones are based on AAL2. AAL1 provides Circuit Emulation Service(CES) including its low speed variant Low Speed Circuit Emulation Service(LSCES) and more efficient Dynamic Bandwidth Circuit Emulation Service(DBCES). Apart from circuit emulation, ATM also provides trunking solutions based on AAL1 and AAL2.

ATM technology plays an important role in providing broadband access to DSL subscribers. Recently, a variant of conventional DSL technology, called Voice over DSL(VoDSL) has evolved, which provides multiple voice communication channels along-with data access over the same DSL link. However, with the introduction of AAL2 protocol, the capability of the ATM network to efficiently support even voice-based services increased manifolds. This led to an overall enhancement in the DSL technology and new variant was born.

The wireless networks too have evolved from 2G networks like Global System for Mobile communications(GSM) and General Packet Radio Service(GPRS) to newer 3G networks like Universal Mobile Telecommunications System(UMTS). The ability of ATM to provide speed transfer with service guarantees emerges as a suitable choice for transfer of voice and data in wireless networks.

Security issues

Requirement of ATM security system

1. **Authentication:** It is concerned with assuring that a communication is authentic.
2. **Confidentiality:** It is the protection of transmitted data from passive attacks.
3. **Integrity:** It deals with a stream of messages, assuring that messages are received as sent, with no duplication, insertion, modification, reordering or replays.
4. **Non-repudiation**: Prevents either sender or receiver from denying a transmitted message.

Objectives of ATM Security: An ATM security should provide-

1. Verification of Identities: Security system should be able to establish and verify the clammed identity of any actor in an ATM network.
2. **Controlled Access and Authorization**: The actors should not be able to gain access to information or resources if they are not authorized to.
3. **Protection of Confidentiality**: Stored and communicated data should be confidential.
4. **Protection of data Integrity:** The security system should guarantee the integrity of the stored and communicated data.
5. **Strong Accountability**: An entity cannot deny the responsibility of its performed actions as well as their effects.
6. **Activates Logging**: The security system should support the capability information about security activities in the Networks elements with the possibility of tracing this information to individuals or entities.
7. **Alarm reporting:** It should be able to generate alarm notification about certain adjustable and selective related events.
8. **Audit:** When violations of security happen, the system should be able to analyze the logged data relevant to security.
9. **Security Management**: The security system should be able to recover from successful or attempted breaches of security.

Challenges in ATM security

1. The first challenge in securing ATM network is how to find a cryptography mechanism used to provide confidentiality, authentication and even integrity service for the security system to match the high communication speed of a switch.
2. Another issue is that ATM cell payload is 48 bytes. Therefore any block cipher with block size more than 384 bits can't be applied to encrypt a cell.

The solution to this problem is stream ciphers but they also suffer from the problem of resynchronization.

3. High speed ATM introduces difficulties in key management. The system has to change the session key frequently to prevent access by a hacker.
4. Finally, charging the service and maintaining a secure billing system is also a problem because of ATMs capacity to support multi-service traffic.

ATM Vulnerabilities

Fiber Tapping

With the use of a chemical solvent to dissolve the insulation surrounding a fibre and attaching a device to detect the leaked light, an attacker has access to all the data being transmitted through that fibre which is undetectable at the receiver end.

SONET Drop/Add Multiplexer Attacks

Aceess to SONET multiplexers found in the basement of buildings can be done by simple knowledge of the Management Information Base variables.

Spoofing

It means that an attacker tries to impersonate another user to the third part therefore can get access to resources belonging to the victim to take advantages or just destroy them.

Service Denial

If an attacker sends DROP or RELEASE PARITY which can disconnect the connection continuously the attacker can greatly disturb the communication between one user to another.

Stealing of Virtual circuits

If two switches in an ATM network compromise, the attacker can steal a VC from another user.

Traffic Analysis

A threat that the hacker can get information by collecting and analyzing the information like volume, timing and the communication parties of a VC.

Snooping

Many switches have special “sniffer” ports for troubleshooting purposes which allow easy access to data going through the switch.

Protocol Weaknesses

a.) **ILMI Attacks**: The Integrated Local Management Interface protocol used at private and public networks can be used by a private switch to configure ATM addresses thus allowing the attacker to register for additional ATM addresses because ILMI protocol does not authenticate.

b.) **PNNI Attacks**: Private Network to Private Interface is a hierarchical routing scheme to establish routing within the ATM public cloud. Network elements exchange connectivity information in the clear to choose a Peer Group Leader(PGL). Once the attacker has control over PGL he has complete control over how data gets routed in the cloud.

c.) **Soft PVCs**: A soft Permanent Virtual Channels are vulnerable to ILMI, PNNI attacks and information can be re-routed.

d.) **Internet based Attacks**: Network hackers go after the weakest link in the chain. The hacker will attack the network by accessing a poorly secured network on the Internet.

Conclusion

ATM is fast becoming the backbone of all networks for high speed data transmission but because of the cost factor it is not preferred for desktop connectivity. We have tried to explore the security issues, challenges and vulnerabilities in the ATM security.

References

[1] "Issues and Challenges in ATM Networks", Communications of the ACM, February 1995, VOL. 38, NO. 2, Pp 56-89.

[2] Asynchronous Transfer Mode", Martin De Prycker, Ellis Horwood, New York 1996, ISBN 0-13-178542-7, Pp 78-145.

[3] IEEE Communications Magazine, April 1992, VOL. 30, NO. 4 Pp 22-33.

[4] "Asynchronous Transfer Mode: Solution for Broadband ISDN", Martin de Prycker, Ellis Horwood, New York, 1991. ISBN 0-13-053513-3,Pp 85-105.

[5] "Data and Computer Communications", 5th ed., W. Stallings. Prentice Hall 1997. Cloth. ISBN: 0-02-415425-3, Pp 30-102.

[6] "Asynchronous Transfer Mode ", Ojesanmi O.A. and Ojesanmi S.O., ISBN --- , IJACE, Jan-June’10 Vol-3 Issue 1, Pp 41-49.

[7] "Asynchronous Transfer Mode- An Overview, It’s Architecture, Benefits, Vulnerabilities and Security ",Jagdev Singh Kaleka, ATM Forum, 2003; ISBN 0-13-525965-7, Pp 112-167.

[8] "Gigabit Networking", Craig Partridge, Addison-Wesley, Reading MA, 1993, ISBN 0-201-56333-9, Pp 165-189.

[9] "ISDN and Broadband ISDN with Frame Relay and ATM", William Stallings, third edition, Prentice-Hall, 1995, ISBN 0-02-415513-6, Pp98-113.

[10] "ISDN", Gary Kessler, McGraw-Hill, Second Edition, 1993, Pp 45-69.

[11] "ATM: Theory and Application", David E. McDysan and Darren L. Spohn, McGraw-Hill, 1995, ISBN 0-07-060362-6, Pp66-79.

[12] "ATM Networks - Concepts, Protocols, Applications", Haendel R., Huber M., Schroeder S., 2nd Edition, Addison-Wesley, 1994, ISBN 0-201-42274-3.

[13] "Broadband ISDN and Asynchronous Transfer Mode (ATM)", IEEE Communications, 9/89.

[14] "Asynchronous Transfer Mode: Solution for Broadband ISDN", Martin de Prycker, Ellis Horwood, New York, 1991. ISBN 0-13-053513-3.