SAND96-1422C
CONF-960622--3

Security Technologies and Protocols for Asynchronous Transfer Mode Networks

Thomas D. Tarman
Sandia National Laboratories*
P.O. Box 5800
Albuquerque, NM 87185-0451 USA
(505) 844-4975
tdtarma@sandia.gov

Abstract

Asynchronous Transfer Mode (ATM) is a new data communications technology that promises to integrate voice, video, and data traffic into a common network infrastructure. In order to fully utilize ATM's ability to transfer real-time data at high rates, applications will start to access the ATM layer directly. As a result of this trend, security mechanisms at the ATM layer will be required. A number of research programs are currently in progress which seek to better understand the unique issues associated with ATM security. This paper describes some of these issues, and the approaches taken by various organizations in the design of ATM layer security mechanisms. Efforts within the ATM Forum to address the user community's need for ATM security are also described.

1. Introduction

Asynchronous Transfer Mode (ATM) is a new data communications technology that uses cell-switching to combine voice, video, and data into an integrated architecture. However, as a cell-switching technology, ATM presents unique challenges to security. For example, much of today's network security mechanisms are based on higher-layer protocols such as IP. However, to support high data rate, time sensitive traffic such as video distribution, applications that are "native" to ATM (i.e. applications that directly access ATM, bypassing the overhead of higher-layer protocols) will become more prevalent. This implies the need for security mechanisms such as ATM layer firewalls, authentication, and encryption to be implemented at the ATM layer.

Although ATM technical specifications have been developing over the past few years, very little consideration was given to security. For "early adopters" of ATM technology, including Sandia, this lack of recognition was troubling. For this reason, Sandia initiated research programs to develop mechanisms to satisfy its internal ATM security needs, and to accelerate the development of ATM security specifications. These programs developed mechanisms and ATM protocols for key agile end-to-end encryption, authentication, key exchange, and encryption control. These mechanisms and protocols have been designed, implemented, and evaluated in the laboratory to measure performance and interoperability.

To accelerate the development of security mechanisms in the ATM protocols, Sandia has taken these implementations to the ATM Forum's Technical Committee as proposals for inclusion in their specifications. As a result of these proposals, and proposals offered by several other organizations, the ATM Forum Technical Committee decided to form a Security Working Group in October, 1995 to formally develop these proposals into an ATM Security Specification. The group's goal is to have the

* This work was supported by the United States Department of Energy under contract DE-AC04-94AL85000.

specification available by early 1997, and has already made significant progress toward reaching that goal.

This paper provides a survey of developing technologies, protocols, and specifications for ATM security. Described here are current network security approaches, the characteristics of ATM that make ATM network security unique, and the ATM layer mechanisms that are required to satisfy these unique requirements. Current research and results by Sandia and others related to ATM security, and the state of ATM security specifications in the ATM Forum is also addressed.

2. Network Security

The goal of network security is to protect an organization's computing assets from threats, including threats of information disclosure, information modification, and disruption of service. This protection is accomplished through the use of security mechanisms such as those which perform mathematical (cryptographic) transformations on the data, or those that implement architectural security protections. Depending on the site's security, performance, and cost requirements, these security services can be implemented at one or more layers in the network protocol stack.

A number of mechanisms exist today to provide security protection for IP networks. IP encryption mechanisms enforce security through cryptographic transformations on the IP data payload which rely on a secret variable (a key) in order to successfully perform the inverse transformation. Without the key, an interloper cannot reconstruct the information contained in the IP payload. This is useful for organizations which wish to construct "virtual private networks" across a public IP network.

IP authentication mechanisms, on the other hand, do not strive to enforce secrecy on the IP data payload. Rather, their purpose is to ensure that the data payload (and parts of the header) do not change as the packet is switched through the network, and that the packet is mathematically bound to its originator. This binding, which is accomplished with a secret key held by the originator, allows the recipient or a third party to verify the source and contents of the packet.

Other mechanisms enforce a site's security policy through architectural means. Examples of such mechanisms include IP firewalls and filtering routers. These devices enforce security policy through "filtering" IP packets based on a number of variables, such as source address and service type. The effect that such mechanisms have on a site's security is that they perform selective isolation of the protected network. One advantage of this mechanism is that the security protection is concentrated on a single point, therefore, security management for a domain is reduced from management of all the assets in the domain to management of a single "gateway" device.

In support of these mechanisms, ancillary mechanisms exist for key exchange, negotiation of the security association between two parties, and the distribution of public keys. Public keys allow end systems to validate the claimed source of a packet that is signed with the source's private key, and must be distributed efficiently if public key authentication is to be used in a large network.

3. ATM Protocols

ATM is a new data, voice, and video communications technology that has applicability in the Local, Metropolitan ,and Wide Area Network (LAN, MAN, and WAN) environments. As a LAN technology, ATM is very different from earlier "legacy" technologies (such as Ethernet and FDDI) in that it is virtual circuit switched rather than packet switched. That is, ATM cells are switched along a virtual circuit rather than broadcast on a shared medium.

ATM virtual circuits connections (VCCs) can be established through one of two methods: administratively or on-demand. Administratively configured virtual circuits, or Permanent Virtual Circuits (PVCs) are established by a network administrator for each point-to-point association that requires one. On-demand virtual circuits, or Switched Virtual Circuits (SVCs) are established by the requesting end system through the use of signaling protocols. For example, a point-to-point SVC can be established using the User to Network Interface (UNI) protocol as follows:

1. The calling party builds a "SETUP" message, which contains "Information Elements" (IEs) that specify the address of the called party, requested quality of service, etc.

2. This message is sent to the network, which uses the Network to Network Interface (NNI) protocol to determine a route for the virtual circuit.

3. Once a route is determined which meets the required quality of service, the network forwards the "SETUP" message to the called party.

4. The called party completes the call by sending a "CONNECT" message back to the calling party.

Once a point to point virtual circuit is established, all data that is sent on the connection is switched by the network to the receiver. This is different from packet-switched, shared media LAN technologies, which broadcast packets (with complete addressing information) on a LAN segment.

Another difference between ATM and the shared-media technologies is that ATM addresses (which are analogous to MAC addresses for Ethernet and FDDI) are dynamically determined, rather than statically configured. This address determination is performed using the Interim Local Management Interface (ILMI) when the end system physically connects to the network (switch). If the end system moves, or connects to a different port on a switch, then its ATM address will change.

4. Security and ATM

One of the important goals of network security is access control. As stated above, access control can be implemented cryptographically and/or architecturally at the application layer and at the IP layer. However, there is strong support for so-called "native ATM applications". These applications, for throughput or real-time performance reasons, bypass intermediate protocol layers and interface directly with the ATM layer. Examples of such applications include ATM telephony, video distribution, and process control. Given the current set of ATM standards, in order to provide access control for these applications, one must either disallow them altogether, establish PVCs for each connection, or implement application-specific access control features. The first option is clearly unacceptable, the second cannot be easily managed for large networks, and the third option leads to proprietary, heterogeneous, and possibly insecure implementations.

To control access to ATM-connected nodes and applications, end-system identification is imperative. The ILMI address registration procedure described above, however, allows an end-system's address to change when it is moved. Furthermore, the End System Identifier (ESI) portion of the address need not be globally unique. In fact, depending on the implementation of the network interface, it may be possible to change the ESI to any value, which can allow a surreptitious user to spoof access control devices that function on ATM addresses. For these reasons, ATM addresses cannot be reliably used as globally unique identifiers for the purpose of access control.

In addition, access control based on the claimed identity of an end system is not strong enough for some (if not most) sites. For the reasons stated above, addresses can be spoofed, allowing a user to assume access privileges which are intended for someone else. To counter this threat, strong authentication is required. This capability, which does not currently exist within ATM SVC setup protocols, should be based on a cryptographically strong algorithm which is a function of a (unique) secret key that is held by each party.

Also, as stated in the previous section, ATM is a virtual circuit switched protocol. This in itself is a security improvement over most "legacy" LAN technologies in that point-to-point communications are (nominally) kept separate from other end systems, whereas with shared media technologies all packets on a network can be captured by a workstation in "promiscuous mode". However, since the basic unit of information for ATM is a small, fixed-size cell, very little security information can be conveyed on a cell-by-cell basis. This limitation implies that security mechanisms for ATM must be accomplished through the use of signaling channels such as the UNI SVC signaling channel, or through an "auxiliary" signaling channel.

Finally, encryption of ATM cell streams also presents some unique challenges. Unlike most other LAN protocols, ATM allows for a number of different link rates in its physical layer interface specifications. This implies that ATM encryptors must be able to operate at a number of different cell rates. In order to accomplish scaling of encryption, parallel implementations of encryption algorithms may be required to "keep up" with fast cell streams (such as those at OC-12c, or 622 Mbps), whereas serial algorithms may be chosen for slower cell streams (such as those at DS-3, or 45 Mbps) to reduce cost. In cases where a host with a "fast" interface needs to talk through the network to a host with a "slower" interface, interoperability of parallel and serial implementations is required. Depending on the mode of operation that is used with this algorithm (e.g.

Cipher Block Chaining (CBC)) and the granularity of parallelism (e.g. one encryptor per block of data), this may not be possible.

5. ATM Security Research

5.1 Sandia's ATM Research

Sandia National Laboratories has been researching various areas of ATM security since October, 1992. This research has largely been predicated on Sandia's use of ATM for LAN, MAN, and WAN connectivity, and its need for security in its ATM networks. Two projects, which have recently been completed, are described here: End-to-End Encryption for ATM Networks, and Protocol Extensions for ATM Security. Current research efforts will also be described.

5.1.1 End-to-End Encryption for ATM Networks

This project examined unique issues in the design and use of end-to-end ATM encryption devices. These issues include interoperability of parallel/non-parallel algorithm implementations, resynchronization, and key agility.

Early in the project, the observation was made that fast encryption devices (which likely implement parallel versions of the encryption algorithm) may need to talk to slower encryption devices (which, for economic reasons, may implement a serial version of the algorithm). This presented a problem in that certain modes of operation (such as CBC) which employ feedback around the non-linear encryption algorithm cannot be parallelized, and at the same time, be expected to interoperate with non-parallel implementations. For such devices to successfully interoperate, other modes of encryption such as Electronic Codebook (ECB) mode or counter mode are required. As a result of this observation, and the fact that ECB has a number of security weaknesses, counter mode (which is described in [4]) was used in the design of the prototype encryptor.

Since cell loss can be a relatively "common" occurrence in ATM networks, an ATM encryptor must be able to maintain synchronization in spite of cell loss to avoid severe degradation in application performance. However, unlike CBC mode, counter mode cannot self-synchronize in the event of one or more lost cells. Therefore, a method of resynchronization is required. The method adopted by the research team used a special Operations And Management (OAM) cell which allowed an encryptor to periodically send synchronization information to its corresponding decryptor. Since OAM cells are delivered in the data-bearing virtual circuit, temporal ordering between the resynchronization information and its associated data stream is guaranteed. Without this guarantee (e.g. if a separate virtual circuit is used for carriage of resynchronization information), the resynchronization information could be delivered to the decryptor at the wrong point in the decryption process, thereby rendering the resync operation ineffective.

Since an ATM device may need more than one secure virtual circuit, the ATM encryptor to which the device is attached must be able to switch keys and cryptographic contexts each time a cell arrives on a different virtual circuit. To accommodate this requirement, the prototype encryptor was outfitted with a content addressable memory (CAM) to store encryption contexts according to the virtual path identifier (VPI) and virtual circuit identifier (VCI) of each encrypted VCC. This approach allowed the encryptor to achieve the maximum required context switching rate of ~350,000 contexts per second.

Once built, a pair of prototype encryptors were installed on the California Research and Education Network (CalREN) ATM testbed and evaluated against the objectives described above. Test configurations were established which involved two hardware prototypes and a software implementation resident in an ATM interface's device driver. The tests showed that the objectives of interoperability, resynchronization, key agility, and operation at SONET OC-3c rates (155 Mbit/s) were met. In particular, the hardware encryptors were shown to induce very little degradation in memory to memory TCP throughput (when compared to non-encrypted virtual circuits), even under severe cell loss. This implies that the resynchronization strategy was very effective in minimizing error extension due to cell loss.

Further details of the encryption prototype and test results can be found in [2].

5.1.2 Protocol Extensions for ATM Security

Another research project at Sandia investigated how the ATM SVC setup protocols can be enhanced to support ATM layer security mechanisms such as access control, end to end encryption, and ATM layer firewalls. The goal of this project was to design these protocols such that they have minimal impact on the current specification, and yet provide useful security enhancements. Throughout this project, the

approaches that were developed were presented to the ATM Forum for adoption in their specifications

As stated earlier, strong authentication is required for ATM firewalls and end systems that implement access control protections for ATM hosts and applications. The approach that was adopted by Sandia involved the definition of an Authentication Information Element (AIE) which can be included in any UNI signaling message (e.g. SETUP and CONNECT). By appending an AIE to a signaling message, the source and contents of the signaling message can be verified by the destination, or even a third party (for billing or non-repudiation purposes). To address export and flexibility considerations, this information element was designed such that any one of a number of authentication algorithms can be used in any specified degree of strength.

Another mechanism that was developed under this project was a means for exchanging keys between two end to end ATM encryptors. This mechanism, a variant of the Diffie-Hellman key exchange protocol, was implemented as a Key Exchange IE in the ATM signaling channel. This IE, when used with the Authentication IE in the SETUP and CONNECT messages, allows the encryptors to derive a session key for the ATM VCC at connection setup time.

In addition to the IEs that were defined for security signaling, OAM cells were defined for messaging between two encryptors once a secure VCC is established. These cells include a "resync" OAM cell (described earlier), and a "request for resync" OAM cell, which can be used by a decryption engine to request resynchronization if sync loss is detected. These OAM cells used the "Security Setup" and "Security Maintenance" OAM cell formats that were proposed to ANSI by the U.S. Department of Defense.

To test these implementations, the Vendor Independent Network Control Entity (VINCE) package was used. This package, which was developed by the Naval Research Laboratory, provided source code for the host and switch-resident UNI signaling processes, as well as device drivers for the network interface adapters. This source code was written for the Fore Systems ASX-100 switch, the SBA-100 and SBA-200 ATM adapters, and Sun SPARCstation/SunOS 4.1.3 hosts, and provided much flexibility for integration of our extensions into the existing UNI signaling protocol.

Once integrated with VINCE, the protocol extensions were evaluated to determine their effectiveness and impact on virtual circuit setup. Although these extensions were generally effective, it was discovered that our implementation of the Digital Signature Algorithm (DSA), which was used for authentication, spent a significant amount of time initializing, whereas the Rivest-Shamir-Adleman (RSA) algorithm did not. As a result, it was observed that connection setup using DSA caused timeouts to occur in the signaling protocol, which required the user to attempt to re-establish the SVC once the algorithm completed initialization. To fix this problem, the DSA validation engines were pre-initialized when the UNI signaling process were started (which naturally resulted in longer startup times). RSA, on the other hand, did not require as much time to initialize, therefore, the timeout problem was not observed in this case.

More detailed information regarding this project and results can be found in [7].

5.1.3 Other Sandia Projects

Currently, Sandia is engaged in the research and development of an ATM end-to-end encryption device that is not only key-agile, but also "robustness-agile". By "robustness-agile", it is meant that the encryptor can encrypt VCCs at various levels of cryptographic robustness (or strength), which is a function of algorithm and key length. Clearly, strong access control to the encryption capabilities is required, as higher levels of robustness typically protect more sensitive data. Therefore, the authentication techniques developed by previous work will be used here as input for the encryptor's access control functions. In addition, architectural enhancements which provide more flexible management of access control policy and public key authentication certificates will also be explored. Finally, adaptation of additional algorithms (such as DES) will be pursued.

5.2 Other Organizations

A number of organizations other than Sandia are also investigating approaches to provide security for ATM networks. These efforts, while largely focused on the development of products, have nevertheless helped to uncover other (more operational) aspects of ATM security.

Due to the importance of encryption with respect to ATM security, and the unique challenges of ATM encryption, ATM encryption has received much

attention in ATM network security research. In response to the U.S. Department of Defense's need for high grade ATM encryption, the National Security Agency (NSA), under the Milkbush program, developed a prototype encryption device. This program uncovered several technical details, and developed a number of solutions which are being used in the Fastlane encryptor (a production, government-grade ATM encryption device). With respect to commercial-grade encryption, the Microelectronics Center of North Carolina (MCNC) developed an ATM encryptor which operates up to OC-12c rates [6]. Secant Networks is expecting to market production versions of the MCNC encryptor this year.

In addition to encryption, other organizations have been developing advanced products to provide other mechanisms for ATM network security. Most notably, Network Systems Corporation has been developing an ATM layer firewall which can filter ATM cells based on the VPI/VCI values in their headers and the information contained in the IP header (which, after the IP packet is segmented into cells, is contained in the first cell of the packet). This device achieves the scalability required of an ATM firewall through mechanisms such as CAMs and a Policy Cache™ [1].

6. ATM Forum Security Activities

As technical specifications and standards for ATM started to solidify, a small number of ATM Forum members became interested in the security aspects of ATM, and more specifically, what is needed in the ATM specifications to provide stronger security assurances for ATM users. Initially, security issues were addressed in the ATM Forum's User Group, also known as the Enterprise Network Roundtable (ENR), which formed a Security Focus Group in 1994. This focus group provided feedback to the ATM Forum's Technical Committee with respect to the user community's security requirements.

In November, 1994, Xerox submitted a contribution to the ATM Forum Technical Committee requesting that it consider additional technical measures to address the needs of business for strong authentication [5]. This contribution was tabled until the February, 1995, at which time Sandia presented its contribution regarding requirements for ATM security [3]. Discussion regarding the Xerox and Sandia contributions clearly indicated that the ATM Forum should consider security mechanisms in their specifications, and the decision was made to hold additional sessions at future Technical Committee meetings for the purpose of adding security features to the Signaling specification document.

In June, 1995, IBM proposed that the security work be assigned to a separate group, which will be tasked with the development of a separate security specification. This motion was passed by the membership, and the newly-formed "Security Ad-Hoc Working Group" immediately started work on the definition of its charter and scope of work. Once this work was completed, the Security Ad-Hoc Working Group was elevated to full working group status in October, 1995.

Currently (June, 1996), the Security Working Group is considering technical mechanisms that are relevant to the workscope that was defined for the Phase I Security Specification. This workscope includes authentication, confidentiality, and integrity mechanisms for the ATM user plane (data channels), authentication and integrity for the control plane (signaling channel), and support services such as access control, key exchange, and public key certification hierarchy. Current plans call for a completed Phase I Security Specification in February, 1997.

7. Conclusion

In order to fully utilize ATM's ability to transfer real-time, high data rate traffic, applications will start to access the ATM layer directly. With this migration, the need for ATM layer security will become more pronounced. Currently, a number of research efforts are in progress that are exploring issues related to ATM encryption, firewalls, signaling channel security, and security messaging. As a result of these research efforts, products are now being introduced which provide government and commercial grade encryption, and provide architectural security assurances (such as ATM layer firewalls). To help ensure interoperability as the ATM security market grows, the ATM Forum has formed a Security Working Group. This working group is currently writing a specification for ATM layer security mechanisms, and is expected to complete this work by February, 1997.

8. References

[1] J. Hughes, "A High Speed Firewall Architecture for ATM/OC-3c," *Proceedings, Interop Engineering Conference*, Spring, 1996.

[2] L. G. Pierson, "Integrating End-to-End Encryption and Authentication Technology into Broadband Networks," *Proceedings, Photonics East '95: SPIE International Symposium on Information, Communications, and Computer Technologies*, October, 1995.

[3] L. G. Pierson and T. D. Tarman, "Requirements for Security Signaling", ATM Forum Contribution 95-0137, February, 1995.

[4] Bruce Schneier, *Applied Cryptography, Second Edition*, John Wiley & Sons, New York, 1996.

[5] T. Smith and J. Stidd, "Requirements and Methodology for Authenticated Signaling,", ATM Forum Contribution 94-1213, November, 1994.

[6] D. Stevenson, N. Hillery, and G. Byrd, "Secure Communications in ATM Networks," *Communications of the ACM*, Vol. 38, No. 2, pp. 45-52, February, 1995.

[7] T. D. Tarman, et al., "Final Report for the Protocol Extensions for ATM Security Laboratory Research and Development Project," Sandia Report 96-0657, March, 1996.

DISCLAIMER