Conf-9504139--3

SAND95-0486C

ATM Forum Technical Committee
ATM Forum/95-0137

****

TITLE: Requirements for Security Signalling

****

SOURCE:

Lyndon G. Pierson
Sandia National Laboratories*
P.O. Box 5800
Albuquerque, NM 87185-0807
Phone: (505) 845-8212
Fax: (505) 844-2067
Email: lgpiers@sandia.gov

Thomas D. Tarman
Sandia National Laboratories*
P.O. Box 5800
Albuquerque, NM 87185-0777
Phone: (505)844-4975
Fax: (505)844-9641
E-mail: tdtarma@sandia.gov

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

****

DATE: February 5, 1995

****

DISTRIBUTION: SA&A and Signalling SWGs

****

ABSTRACT:

There has been some interest lately in the need for "authenticated signalling", and the development of signalling specifications by the ATM Forum that support this need. The purpose of this contribution is to show that if authenticated signalling is required, then supporting signalling facilities for directory services (i.e. key management) are also required. Furthermore, this contribution identifies other security related mechanisms that may also benefit from ATM-level signalling accommodations. For each of these mechanisms outlined here, an overview of the signalling issues and a rough cut at the required fields for supporting Information Elements are provided. Finally, since each of these security mechanisms are specified by a number of different standards, issues pertaining to the selection of a particular security mechanism at connection setup time (i.e. specification of a required "Security Quality of Service") are also discussed.

****

Notice:

This contribution has been prepared to assist the ATM Forum, and is made by Sandia National Laboratories as a basis of discussion. This contribution should not be construed as a binding proposal on Sandia National Laboratories. Specifically, Sandia reserves the right to amend or modify the statements made herein.

****

I. Introduction

In [1], the need is expressed for an additional information element that will convey authentication information in the signalling channel to switches and end systems. It is asserted that this capability is needed to minimize toll fraud and to support scalable firewalls, mobile users, and complicated billing scenarios. However, authenticated signalling is only a part of the security picture. Security services such as access control and encryption are also widely used, and certain directory services will be required for implementation of these security services. For example, a network architect may elect to provide access control to his ATM network through a firewall, which relies on access control lists, which rely on strong authentication based on public-key cryptography (e.g. DSS). Finally, the authentication mechanism in turn relies on a directory service (such as

X.509) to provide public keys in a secure manner so that the recipient can be certain that "this public key belongs to this node or human user". Although ATM support for strong authentication is a good start, signalling standards that support the additional security mechanisms listed above will also be needed if a complete security package for ATM switched virtual circuits is desired.

The purpose of this contribution is motivate the consideration of additional information elements which support these security features at the ATM level, and to roughly identify what is required of the signalling subsystem to support these features. To this end, this contribution is organized as follows: Section II motivates the need for security-specific ATM signalling by defining what is intended to be protected, the expected security threats, and the required mechanisms to secure these assets. Section III describes these required mechanisms in greater detail, and their information requirements in the context of ATM signalling. In Section IV, additional signalling observations pertaining to the negotiation of security capabilities are presented. Finally, this contribution is concluded in Section V.

II. The Need for Standardized ATM Security

This section motivates the need for signalling support of ATM-level security functions by describing the ATM-connected information assets that need protection and the expected threats to these assets, and identifies protection methods that can mitigate these threats.

A. Assets to be Protected

The first step in a security analysis of any distributed system is the identification of the assets that require protection via network security mechanisms. Common information assets associated with BISDN traffic that must be protected include:

1. the sensitivity of communicated information to disclosure to unintended persons or machines
2. the integrity of communicated information against modification or falsification by unintended persons
3. the availability of communication resources against any kind of denial of service by unauthorized persons

B. Threats to these Assets

Once the information assets are identified, "threat-asset" pairs can be assigned. By performing this analysis, the security problem can be properly bounded, thus reducing unnecessary mechanisms that complicate the overall security system design, while at the same time, ensuring completeness. The "threat-asset" pairs for this scenario include:

	ASSET	THREAT
a.	Info Sensitivity	Disclosure by improper connection to an unintended destination
b.	Info Sensitivity	Disclosure by usurping of a connection initially made properly
c.	Info Sensitivity	Disclosure by interception of data on a trunk or within a switch
d.	Info Integrity	Modification/Falsification by masquerade of

		intended Source or Destination as the connection is initiated.
e.	Info Integrity	Modification/Falsification by masquerade of intended Source or Destination after the connection is properly initiated.
f.	Info Integrity	Modification/Falsification by insertion and/or deletion of data on a trunk or within a switch
g.	Service Availability	Denial of service by repeatedly serving false certificates of authentication variables or Access Control Lists (ACLs).
h.	Service Availability	Denial of service by presenting false information to the switching fabric (false destination addresses, etc.)
i.	Service Availability	Denial of service by failure to properly screen (filter) connection set ups on the basis of Access Control Lists (allowing a flood of connections intended to be disallowed)

C. Specific Protection Methods required by BISDN Traffic

The specific protection methods required to allow network customers to reduce loss expectancy to an acceptable level include:

1. Initial authentication services (protection re: pairs a, d, h)
2. Periodic re-authentication services (protection re: pairs b, e)
3. Assurances regarding communication route (protection re: pairs c, f)
4. Encryption services (protection against pairs c, f)
5. Authenticated directory services (in support of the implementation of authentication, ACL, and encryption services and route assurance) (protection re: g, h, i)

It should be noted that each of these protection methods either rely directly or indirectly on strong authentication. As stated in [1], authentication is a valuable tool for secure transactions over an untrusted network infrastructure. Without strong authentication, confidence in the identity of call participants is greatly diminished, and the probability for the commission of fraud increases at least proportionally. Clearly, this is unacceptable, and the omission of authentication from services that expect to bill customers is out of the question.

Given the need for confidence in the identity of other users (where "users" can be people or nodes with addresses that identify them uniquely and/or geographically), the question becomes "where should authentication and its dependent security mechanisms exist?". By designing support for security services within the Forum's signalling specifications, these services can be "integrated into", rather than "added onto", the ATM service. Integrated, low-level security services, with signalling standards to support the services' needs, have the following advantages:

1. Intermediate systems (such as switches) can participate in ATM security signalling without the need to "look into" user data (see [1]).

2. Protocol processing is reduced, resulting in increased speed.
3. Standard set of security mechanisms are accessible by all higher layer protocols, including applications .
4. A "first line of defense" against security attacks is provided. That is, ATM-level security can be used to thwart all but the most complicated attacks (reducing the risk to an acceptable probability), and applications are allowed to implement additional layered security mechanisms, if necessary.

III. ATM Signalling Implications

The integration of these low-level security services into ATM layer processing requires support from the signalling subsystems that reside in the end-systems and the switches. The following section describes how ATM signalling can help meet the needs of these low-level security services.

A. Authentication and Supporting Services

Authentication Services

Most of today's strong authentication mechanisms use cryptographic principles to "sign" a message so that the signature cannot be forged by someone who does not possess the private "key". This implies that although authentication is an important tool, it cannot be implemented over large networks conveniently without some means to distribute public decryption keys to those users who wish to verify the claimed identity of another user. Many methods are currently used today to accomplish this, one of which being X.509. X.509 is a hierarchical directory service that can provide public keys to requesting users, whereby the key servers "certify" the authenticity of the key, and the key servers' public key is itself "certified" by some higher authority, and so on. By arranging this public key certification system hierarchically, it is presumed that the mapping between a user's identity and her public key can be verified with arbitrary strength.

Although the author of [1] discusses DSS as a particular method for implementing authentication, a number of alternatives exist. Even though it can be argued that a particular standard should be selected for authenticated signalling, the fact remains that users will probably want to be able to choose for themselves which authentication approach will be used in their networks. For example, government users may be willing to tolerate increased connection setup times if they can be given increased confidence in the identity of the remote node. Also, as cryptographic algorithms change, new signature standards and cryptographic hash functions will become available which may have properties that users consider more valuable than those of current standards. As a result, an authentication information element must contain, in addition to the fields suggested in [1], a field that identifies the authentication standard that is used. Furthermore, the information element should be variable in length to ensure that it can contain sufficient information for the algorithm to function.

The following list summarizes the minimum contents of the Authentication IE as proposed above and in [1]:

1. Source Address
2. Destination Address
3. Signature/Hash Algorithm
4. IE Length
5. Timestamp
6. Sequence Number

7. Algorithm-specific Information (including Digital Signature)

where the timestamp and sequence number fields are required so that the ATM node or switch that receives this IE can determine if the signature is genuine, or if it is the result of a replay attack.

Directory Services

Support for directory services such as X.509 directly pertains to ATM signalling because to support low level authentication, a low-level mechanism must be in place to obtain the required public keys for authentication of claimed identities. As with digital signature-based user/node authentication, any one of a number of standard approaches can be used to provide directory services. The following list summarizes a minimum set of information required by Directory Services request and response information elements:

1. Source Address (of requesting node or server)
2. Destination Address (of requesting node or server)
3. Directory Service Type
4. IE Length
5. Timestamp
6. Sequence Number
7. Directory Information
8. Digital Signature of directory server

Where "Directory Information" (item 7) contains a certificate (which is signed by the certification authority) that contains the address, name, public key, etc. of the node and/or user. The server's digital signature (item 8) signs the content of this IE.

B. Other Security Services

Access Control Services - Firewalls

Another issue that is raised in [1] is the need for firewalls that implement ATM-level access control decisions at connection setup time, and "get out of the way" during the rest of the call. By implementing firewalls in this fashion, scalability and higher throughputs can be readily achieved. Again, as with other security services discussed in this contribution, authentication is necessary for secure access control. However, authentication is not sufficient; a new method of multiplexing higher-layer services over ATM virtual circuits is required.

Currently, standards such as [2] specify that all higher-layer services between two connected nodes (using a given network-layer protocol) must be multiplexed over the same ATM VC. Thus, if a new service is started between two nodes that already have a connection in place, the new service will "ride on top of" the existing connection, with no signalling required to establish a new virtual circuit (and hence, no opportunity to authenticate and deny this new service at the ATM level). To resolve this problem, two modifications are required:

* Specify a standard for "higher-layer protocols over ATM" such that a new SVC is requested when each new service is started. This gives ATM-layer access control devices the opportunity to deny connection requests for each higher-layer service request.

* Specify an IE that is used at connection setup time which provides, at a minimum, the following information:

    1. Source Address
    2. Destination Address
    3. Higher-layer protocol
    4. Service identification (e.g. port number)

    This provides the information required by an ATM-layer access control device to make an "informed" access control decision.

In addition, authentication IEs must be exchanged to strongly identify the calling and called parties and requested service type in the connection setup exchange.

Access Control Services - Distribution of Access Control Lists

Access Control Lists (ACLs) allow a network administrator to configure (and reconfigure) the firewall device with access control rules based on the site security policy (which is derived from a "threat-asset" analysis similar to the one above). In a network that uses a firewall, particularly those where the firewall may be in a remote (but physically secure) location, it may be desired to remotely load the firewall with its ACL. This obviously requires strong authentication in order to perform this operation securely. Therefore, an information element that carries ACL data should contain the following fields:

1. Source Address
2. Destination Address
3. ACL Format Specifier
4. IE Length
5. Timestamp
6. Sequence Number
7. ACL Information
8. Digital Signature

where the "Digital Signature" spans the entire IE, the "ACL Format Specifier" designates the ACL format standard that is used, and the "ACL Information" contains data that allows the firewall to make access control decisions based on the contents of the connection establishment IE, shown above.

Encryption Services

Finally, to provide an "extra level" of security protection, some users and network architects may look to encryption. Although the primary purpose of encryption is to maintain data confidentiality, it also implicitly implements authentication in the sense that if one can successfully decrypt a message from someone who has a unique, secret key, then one knows that the message could have originated only from that source. In order for encryption to function, signalling must occur between the encryption and decryption devices. These messages could allow two encryption devices to exchange session keys (which, incidentally, requires strong authentication), and/or to indicate commands to "go secure" and "re-synchronize". Although encryption may not be necessary (or cost effective) for most applications, ATM signalling which SUPPORTS the exchange of such messages is necessary for two reasons:

1. to provide a standard framework for signalling secure channels when needed

2. to allow selection of a "common" encryption algorithm, including the selection of "no encryption" if neither device has a common algorithm (more on this in Section IV).

It is important to note that "supporting signalling" is required at this point. Since each encryption device manufacturer typically has a unique set of commands and capabilities for their devices, it may not be possible to standardize on a fixed set of information elements that implement specific encryption commands. This will require further study.

IV. Some Signalling Observations

As mentioned in the previous section, it is expected that users will have a diverse set of security requirements, and will want the flexibility to be able to choose from a set of available security protection mechanisms. Given this situation, and assuming that the ATM Forum wishes to support ATM-level security, the Forum is faced with three choices:

1. Pick one standard for each security service and specify that standard in the Forum's implementation agreements
2. Specify several standards for each security service in the implementation agreements
3. Specify the signalling protocols such that they support a variety of security services, but do not "care" what standards (if any!) specify those services.

Option 1 is inadequate for the reasons specified earlier, that is, users will want to choose from a variety of security mechanisms, according to their security and performance requirements. Furthermore, as security standards and algorithms change in the future, many users will want to take advantage of the new and enhanced features that these standards offer.

Option 2 is clearly inadequate because of the sheer numbers of standards that exist today, as well as the number of non-standard security services that may be used in ATM networks.

Option 3 is probably the best choice due to its flexibility. By designing security-specific signalling standards such that they support ARBITRARY protocols for strong authentication, key management, etc., the user is given the opportunity to choose an approach that is suitable for her requirements. In addition, devices that support diverse sets of security mechanisms (or even devices that do not support security at all!) can find a "common ground" on which to communicate.

Within this option, there are a number of sub-options that can be pursued. The following are two possibilities:

1. An additional information element is sent along with the connection request from the calling party that notifies the called party of the required security mechanisms, and the called party responds with either "call accepted" or "call rejected".

2. A more elaborate protocol in the connection setup protocol that establishes a "Security Quality of Service" for that call based on "back and forth" negotiation of security capabilities between the calling and called parties.

Although the first option provides the required agreement of security capabilities, the second approach is more robust. By negotiating a "security quality of service" during the

connection establishment phase, all involved parties (end systems, switches, key servers, etc.) can establish a common language without the need to specify and re-specify (to exhaustion) security capabilities. In either case, the specification (or negotiation) of security capabilities achieves the desired objective of signalling support for multiple variations of security mechanisms and standards.

V. Conclusions

This contribution has shown that strong authentication is a valuable component for not only billing and accounting (as stated in [1]) but also a number of other security services, specifically key management, encryption, and access control. For example, encryption requires key management (for distribution of session keys), which relies on strong authentication, which in turn, relies on directory services (to obtain the public keys of other parties for strong authentication). However, there exists today a number of different standards for each of these security services, each of which could be appropriately utilized by users to meet their security needs. This situation complicates the work of the ATM Forum in developing implementation agreements that address the users' security needs, and may require some sort of security "negotiation" phase at connection setup time to determine what mechanism, if any, should be used for security-related functions.

V. References

[1] Ted Smith and John Stidd, Xerox Corporation, "Requirements and Methodology for Authenticated Signalling", ATM Forum/94-1213.

[2] Juha Heinanen, "Multiprotocol Encapsulation over ATM Adaptation Layer 5", RFC 1483.