ATM Forum Technical Committee
ATM Forum/99-0181

****

TITLE: Issues in Security Service Discovery and Routing

****

SOURCES:

Thomas Tarman*
Sandia National Laboratories
P.O. Box 5800
Albuquerque, NM 87185-0806
USA
Phone: +1-505-844-4975
Fax: +1-505-844-2067
Email: tdtarma@sandia.gov

Peter Sholander
Scientific Research Corporation
2300 Windy Ridge Parkway, Suite 400 South
Atlanta, GA 30339
USA
Phone: +1-770-859-9161
Fax: +1-770-859-9315
Email: psholander@scires.com

****

DATE: April, 1999 (Rome)

****

DISTRIBUTION: Security

****

ABSTRACT:

The Security Specification, Version 1.0 allows security services to be provided by many devices in a network. It correctly presumes that if a virtual circuit needs these security services, then network topology and device policy will act to ensure that the appropriate security services are applied to the virtual circuit.

This contribution moves that the Security Service Discovery and Routing function be included in the Security Version 2.0 work scope.

****

****

1. Introduction

The ATM Forum Security Specification, Version 1.0 allows security services to be provided by many devices in a network. The security agent identifiers, addressing mechanism, and security message exchange protocol allow these devices to be arranged so that security associations may be nested to up to 16 levels. Therefore, ATM security for a virtual circuit need not be applied "all at once", in a single security device. Rather, the security functions can be distributed across a network (as long as the appropriate physical and/or personnel security protections are in place in the domains where ATM security protections have not been applied).

* This work was supported by the United States Department of Energy under Contract DE-AC04-94AL85000. Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy.

The Version 1.0 specification assumes that if a virtual circuit needs security services that are distributed across multiple devices, then the network topology will be constrained to ensure that the appropriate security services are applied to the virtual circuit. However, this constraint is overly restrictive. The specification's Security Message Exchange (SME) protocol has a rich identification and addressing scheme that can also support call routing based on both the security services that are requested by an upstream node, and the security services available in the ATM network. This contribution describes this Security-Based Routing concept in more detail, and describes options for mechanisms that implement security service resource discovery and routing.

2.0 Conceptual Overview

Figure 1~~Figure 1~~ shows an example of distributed security services in a private ATM network.

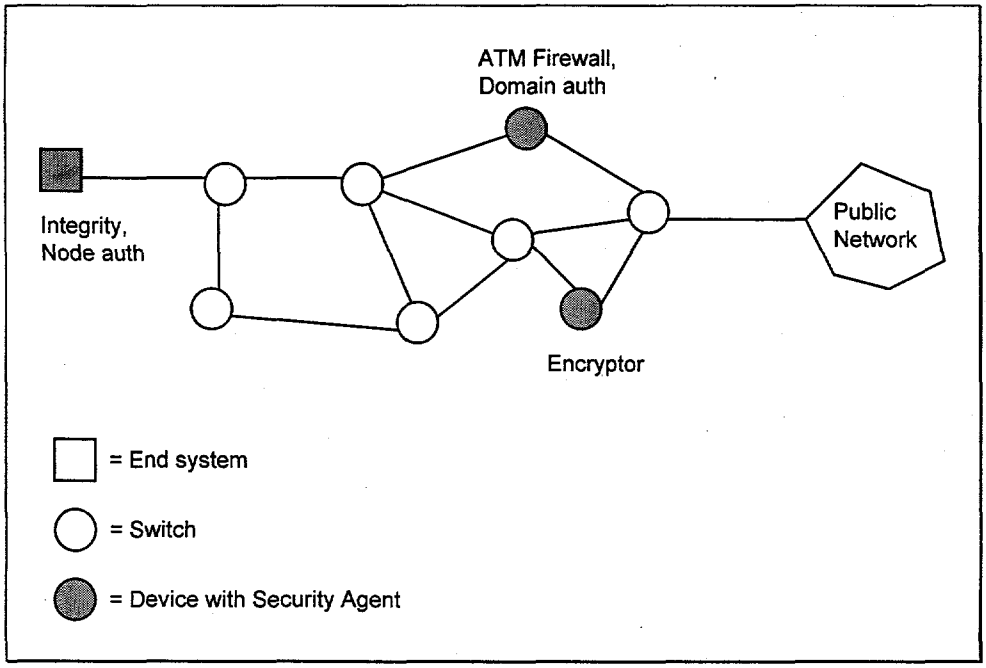

Figure 1: Distributed Security Services

In this example, let the end system implement security agent functions that provide node authentication and AAL5 integrity services as defined in [1]. In addition, assume that the private network, to which the end system is attached, implements ATM firewall functions and domain authentication (authentication on behalf of the domain's end systems) in one device, and encryption services in another device. In this case, a number of security services that may apply to one virtual circuit are distributed across a private network, and require proper call routing in order to apply the security services that are 1) required by the call, and 2) allowed/required under site security policy.

For example, if the end system wished to place a call with AAL5 integrity and ATM cell encryption applied to the virtual circuit then the integrity service must be activated at the end system, and the call must be routed through the encryptor. To support such routing, the network or security agents must be aware of the request for encryption services, locate the whereabouts of the encryptor, and route the call to that encryptor. It should be noted that the encryptor location function must support not only the encryption

request (e.g., algorithm, key length, etc.), but also site policies (e.g., Mandatory Access Controls) that may restrict/dictate the use of encryption between given endpoints.

As another example, incoming calls may need additional network-based authentication, depending on the call's requested destination. For example, although calls to a public server (e.g., WWW, FTP, etc.) do not require strong authentication, calls to a valuable resource (e.g., supercomputing cluster, internal information server, etc.) may require that the network perform additional authentication steps. In Figure 1, this requirement can be supported by selectively routing calls through an ATM firewall that implements additional authentication steps.

3.0 Security-Based Routing

This section describes the concept of security-based routing in more detail. Two approaches to implementing this feature are described, along with issues regarding security-agent addressing and trust in the routing decision points.

Constrained Routing based on Requested Security Services and Site Policy

In order to route calls through "appropriate" ATM security agents, mechanisms are required to request security services and to decide whether a security request can be honored under the constraints of Administrative Domain (AD) security policy. Security V1.0 does support requests for network-provided security services. However, it does not provide a framework for supporting policy decisions. To support policy decisions, a policy definition language is needed to specify which security agents and/or end systems are allowed to request certain security features.

Assuming that a secure call request is supported by AD security policy, the problem of directing a secure ATM call through the appropriate security agents still exists. This function requires some sort of source-routing capability in ATM networks so that a SA or switch can direct the call through the appropriate security agent. Designated Transit Lists (DTLs) may provide the proper mechanism for constraining calls in such a fashion.

PNNI-Based

Security routing decisions can be implemented by switches provided they know the whereabouts of security agents (described later). This routing infrastructure could be implemented via extensions to the PNNI protocol which provide the requisite topology discovery, link state (security state) tracking, and constrained routing.

This approach is advantageous in that many of the mechanisms already exist in PNNI to support security-based routing. However, modifications to the protocol are required to implement policy features, security capability discovery and specification, tracking of the network's "security state", and perhaps constrained routing. In addition, if security agent state needs to be summarized across PNNI hierarchies then the encoding rules for specifying security state must be carefully designed.

Finally, security-based routing is necessarily a trusted operation. If it is implemented in the switches, then the switches' routing codes must be trusted. This trust level can be unrealistic, especially for large, multi-vendor and multi-country neworks.

Security Agent-Based

A second approach to security-based routing is to implement such functions within the Security Agents (SA). An SA-based approach would effectively implement a Security Overlay Network, wherein security agents learn about each other's locations, maintain security link state among themselves, and perform more

loosely constrained routing (i.e., so that any VC path can be selected, as long as it passes through the right security agents).

The advantage to this approach is that it minimizes the impact on PNNI. In addition, SAs are normally trusted entities anyway, so the concern about trust is reduced (but not necessarily eliminated).

The main disadvantage to this approach is the duplication of functions with PNNI. It also requires an overlay of authenticated, and possibly encrypted, VCs between the SAs.

Security Agent Addressing Issues

Security-based routing requires that the security agents to have addresses with "network-significance". In [1], security agent identifiers can be used to perform explicit addressing of SAs during the security message exchange protocol. However, there is no restriction on the selection of security agent identifiers (other than the fact that they must be unique). For security-based routing to work, PNNI nodes must be able to route to SAs (which can be considered "special switches"). In order to route to SAs, the SA address (SA identifier) must have network significance.

4.0 Security Resource Discovery

Security-based routing requires that the security agents and/or switches be aware of where various security services are located in the AD. This function can be performed with a directory service (e.g., ATM Name Service, or ANS), or with a flooding protocol that allows security agents and/or switches to become aware of the security topology. In both cases, an encoding method (language) for specifying SA capabilities is required. In addition, if hierarchical organization of SAs is required (e.g., for scalability of routing tables and/or ANS), then this security specification language may need to support summarization.

An ANS-based approach would probably be the easiest to implement. In this approach, when a security service comes on-line, it would register with ANS. Included in this registration would be the SA address, and a specification of the SA's security capabilities (e.g., service, algorithm, etc.). When a secure call is requested, the SA or switch would query ANS for the address(es) of downstream SA(s) that implement the required services. These addresses could then be used in the routing specification for the call (as described earlier). The advantage of this approach is that security service information does not need to be replicated throughout the network. The disadvantage is the need for a secure channel between the SA/switch and the ANS, and the increase in call setup time due to ANS queries.

Another approach floods the security agent topology information to the SAs and/or switches in the AD (depending on the method for security-based routing). In this case, the SAs/switches know where security services reside, and can route the call without the added delay of an ANS query. However, this approach may require extensions to the PNNI protocol, or development of a new, inter-SA protocol.

5.0 Motion

We move to include Security Service Discovery and Routing in the Phase II work scope.

References

[1] ATM Forum Technical Committee, ATM Security Specification Version 1.0, af-sec-0100.01, March, 1999.