SAN099-1795C

ATM Forum Technical Committee
ATM Forum/99-yyyy

****

TITLE: Security Services Discovery by ATM Endsystems

****

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, x551
Fax: +1-770-859-9315
Email: psholander@scires.com

****

DATE: July, 1999 (New Orleans)

****

DISTRIBUTION: Security

****

ABSTRACT:

This contribution proposes strawman techniques for Security Service Discovery by ATM endsystems in ATM networks. Candidate techniques include ILMI extensions, ANS extensions and new ATM anycast addresses. Another option is a new protocol based on an IETF service discovery protocol, such as Service Location Protocol (SLP). Finally, this contribution provides strawman requirements for Security-Based Routing in ATM networks.

****

****

1 Introduction

A previous contribution [1] proposed Security Service Discovery and Routing as a Phase II work item. Security Service Discovery (SSD) would allow ATM end-users to automatically discover the location and capabilities of Security Agents (SA) within their private ATM network. Security-Based Routing would then constrain the connection path, so that it flowed through the requested/required sequence of SAs.

This proposed Phase II work item addresses two current market needs -- namely policy-based networking and Virtual Private Networks (VPNs). Policy-based networking currently refers to efforts to bring Quality of Service (QoS) features to the IP world. In that context, "policy" typically refers to which hosts, applications and users allowed to access QoS features such as preferential forwarding and assured bandwidth. VPNs are typically used as a security feature wherein a closed user group is provided added security, often via cryptographic techniques, while tunneling their private network traffic across a public

---

[1]* 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.

DISCLAIMER

DISCLAIMER

Portions of this document may be illegible in electronic image products. Images are produced from the best available original document.

network. In both cases, the management of the policy databases, QoS features and security devices is currently a non-trivial management burden on network administrators. Hence this work item (Security Service Discovery) has two goals. The first is to minimize the management burden for configuring security parameters in both endsystems and Security Agents. The second is to maximize the commonality of policy management tools between traditional QoS policies (such as bandwidth reservations) and the newly emerging "Security QoS" policies.

2 Motivation

The need for security service discovery arises from the desire to deploy ATM security devices in a manner that does not impose network topology constraints. By deploying ATM security services in such a fashion, flexibility in the application of security services to ATM virtual circuits can be achieved. In general, such flexibility allows endsystems and/or network administrators to determine a proper mix of security services for a given virtual circuits, and allows the network to route the virtual circuit to the appropriate security agents.

For example, security service discovery and security-based routing allows network administrators to upgrade their networks with new security agents without a "forklift" upgrade. Existing security agents can remain in place while new security agents (e.g., ones that implement stronger encryption algorithms) are added to the network. These new security agents will be "discovered" by the network or other security agents, and calls can then be routed through the new devices. The "old" security agents can remain in the network to provide backward compatibility.

In another example, security-based routing can be used to provide high-performance authentication at the private network ingress. This scenario, called the "ATM network badge office", requires that a new external end system perform strong authentication upon its first request to connect into the private network. In this case, the connection request is forwarded to an ATM firewall that performs a Security Message Exchange. Once this step is successfully completed, the remote end system is provided with a key which it can use in subsequent connections (signaled without the Security Message Exchange (SME) protocol) to perform data origin authentication. In this phase, the call should be routed differently because SME authentication is no longer required.

Finally, a private ATM network may attach to multiple ATM service providers that provide different levels of security protections. In this case, stronger security measures may be needed for virtual circuits that traverse the "less trusted" public ATM network(s). Therefore, virtual circuits must be routed to security agents that provide stronger security services.

3 Existing Capabilities in ATMSECv1

The ATM Forum's Security Specification Version 1.0 [2] provides three methods for ATM endsystems to learn about the capabilities of Security Agents within their private ATM network. The first is via management. Each endsystem can be preconfigured with a list of SAs and their capabilities. The second method is a mandatory security policy which constrains the network topology so that an endsystem's VP and VCs have security services applied, without the endsystem's explicit knowledge, by security devices on the trusted side of the SA.

The third method assumes that the ATM endsystem lacks any knowledge of the SAs in its private ATM network, but that it can select the security policy for each VC. In that case, Section 5.1.4.5. of ATMSECv1 ("Endpoint Requests for Security Services") allows an endpoint or host that does not provide security services to request security services from a downstream security agent as follows:

1) Insert a Security Services Information Element into the SETUP message on the signaling channel.
2) Set the Security Message Exchange Protocol Type field (octet 5.9) to the "undefined" codepoint ("0 0").
3) Insert any combination of the following optional fields, indicating the desired service(s) and/or algorithm(s):
   a) Security service declaration,

b) Data confidentiality algorithm,
c) Data integrity algorithm,
d) Hash algorithm,
e) Signature algorithm,
f) Key exchange algorithm,
g) Session key update algorithm,
h) Access control algorithm.

Multiple algorithms may be inserted in preference order for each requested security service. Upon receipt of such a request, the security agent replaces the Security Services Information Element with one of its own choosing, based on its security policy. A security agent is under no obligation to use the options requested by the endpoint or host.

While this process is somewhat scalable, it is not secure, as it assumes a trusted link between the endpoint and security agent.

The remainder of this contribution discusses more scalable and secure ways for ATM endsystems to obtain information about addresses and capabilities of the SAs in their private ATM network. The first three techniques are extensions to existing ATM Forum protocols – namely ILMI, ANS and ATM anycast. The last technique would adapt an IETF service discovery protocol, such as SLP, for use in ATM networks.

4 ILMI Extensions

The Integrated Local Management Protocol (ILMI) [3] uses the IETF's Simple Network Management Protocol (independently of UDP over IP) and an ATM Interface Management Information Base (MIB). It provides any ATM device (e.g. endsystems, switches, etc.) with status and configuration information concerning the VPCs, VCCs, registered ATM Network Prefixes, registered ATM addresses, registered services, and capabilities available at its ATM Interfaces. ILMI runs during endsystem initialization, and periodically thereafter. The SNMP Trap messages allow ILMI to push information from the switch to an endsystem.

ILMI's optional Service Registry MIB already provides a general-purpose service registry for locating ATM network services such as the LAN Emulation Configuration Server (LECS). Hence, one SSD technique might add security-related information, such as the addresses and capabilities of the SAs, to the ILMI protocol.

ILMIv4 restricts the SNMP message size to 484 bytes. The traffic requirements are that ILMI traffic must have an (SCR, PCR) $\leq$ (1%, 5%) of the interface bandwidth. As such, it is for further study whether security-related extensions to ILMI could contain both the SA addresses as well as their capabilities.

This approach might required a secured version of ILMI (which might be useful for all ILMI information in security-conscious networks) depending on factor such as the user's authentication procedure with its SA. This topic is for further study. One big issue is providing a generic framework for secure ILMI that meets government sector requirements without unduly burdening less demanding commercial sector applications. Another issue is whether Secure ILMI would use ATM layer security for the underlying ILMI VC, application layer security for the SNMP protocol, or both

5 ATM Name Service (ANS)

The ATM Name System (ANS) [4] is modeled on the IETF's Domain Name System. It is a system for storing and retrieving mappings between names and a small set of defined objects. As such, it could be used to map between "well-known names" for ATM security services and their local address. Eventually, ANS may use an LDAP service that allows more complex queries to locate addresses or other information about objects, such as SAs. In either case, dynamic update of ANS is probably required. However, that update process can be independent of the underlying routing protocol, such as PNNI.

6 ATM Anycast

PNNIv1.0 supports routing based on anycast addresses with scope. This capability allows an application to request a point-to-point connection to a single ATM end system, or server, that is part of an ATM group. Scope allows the SETUP message to be limited to certain levels within a PNNI hierarchy.

The ATM Forum already has well-known anycast (or "group") addresses for the LAN Emulation Configuration Server (LECS) and the ATM Name Server. An additional well-known address could be added for the Security Agent. Section 1.6 of ATMSECv1 lists numerous security profiles. Hence, the straightforward approach would use a separate anycast address for each profile and/or combinations of profiles. This may cause scalability problems, and slow the introduction of new security profiles. A second approach would have the anycast address point to the nearest SA. If that SA does not support the requested security service then it could forward the SETUP message to the appropriate SA that does provide the requested security service. (A third approach wherein the nearest SA returns the address of another SA, that does support the requested security service, to the endsystem is basically the ANS approach discussed in Section 5.)

While this approach would benefit from a secure version of PNNI, it might work over vanilla PNNI depending on the user's authentication procedure with its SA and other factors such as the alignment of PNNI peer groups with security/trust domains. As such, the required trust model is for further study.

7 Service Discovery via an Overlay Approach

Automated service discovery is a current issue within the IETF. One example is the Service Location Protocol [5]. SLP defines a generalized directory agent and a client/server protocol that runs the endsystem and that directory agent. This approach would allow native ATM security applications to obtain information about the Security Agents' addresses and capabilities via an overlay approach. Just as in ILMI, SLP could run over native ATM rather than using UDP (or TCP) over IP. Of course this overlay model still suffers from the same bootstrapping problem as the native approaches discussed above – namely how does the endsystem finds its directory agent?

If the working group chooses an overlay approach then other protocols, besides SLP, should be considered. However, a standard (or proposed standard) IETF protocol should probably be chosen.

8 Requirements for Security-Based Routing

This section gives strawman requirements for security-based routing in ATM networks. In brief, any UNI and PNNI changes should be confined to the SSIE.

R-1: Security-based routing shall be backward-compatible with existing PNNIv1.0 signalling and routing, and both UNI 3.1 and UNI 4.0 signalling. (Security-based routing shall not required upgrades to existing PNNIv1.0 switches. It may require that endsystems support the security-related addenda to UNI 4.0 signalling.)

R-2: Security-based routing should require no new IEs in either PNNI or UNI signalling.

R-3: Security-based routing should minimize the number of new TLVs within existing PNNI and UNI IEs. Those TLVs should be confined to the existing Security Services IE (SSIE).

R-4: Security-based routing shall work within one lowest-level PNNI peer group.

R-5: Security-based routing should work across multiple, hierarchical PNNI peer groups.

R-6: Security-based routing for ATM networks should interwork with security-based routing for IP networks, via extensions to PNNI Augmented Routing (PAR).

R-7: Security agents shall have addresses with "network-significance".

9 Motion

We move to include this contribution, on security services discovery and security-based routing, into the Phase II living list.

10 References

[1] T. Tarman and P. Sholander, "Issues in Security Service Discovery and Routing", ATM Forum Contribution 99-0181, April 1999.

[2] T. Tarman and P. Sholander, SBR Contribution, ATM Forum Contribution 99-yyyy, July 1999.

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

[4] ATM Forum Technical Committee, Integrated Local Management Interface (ILMI) Specification Version 4.0, af-ilmi-0065.000, September, 1996.

[5] Joann Ordille, "Baseline Text for the ATM Name System V2.0", ATM Forum/BTD-SAA-ANS-02.00, January, 1999.

[6] E. Guttman, C. Perkins, J. Veizades and M. Day, "Service Location Protocol, Version 2", RFC 2608, June 1999.