3GPP TSG SA WG3 Security - S3#16 S3-000685
28-30 November, 2000
Sophia Antipolis, France

IPSP Working Group
Internet Draft
draft-ietf-ipsp-arch-00.txt

M. Blaze
AT&T Labs - Research
A. Keromytis
U. of Pennsylvania
M. Richardson
Sandelman Software Works
L. Sanchez
BBN/GTEI
July 2000

IPsec Policy Architecture

Status of this Memo

Abstract

This document describes an IP Security Policy architecture that conforms to the requirements set forth in [IPSP-REQ]. The architecture defines the mechanisms and protocols needed for discovering, accessing, and processing security policy information of varying granularity. The architecture accommodates topology and policy changes without need of manual reconfiguration of clients and security gateways.

1. Introduction

Consider the simple scenario represented by the figure above: Host A wishes to communicate with Host B; A only knows B’s network identifier (address) and what security requirements for such a communication itself requires (e.g., A wants to use strong encryption when talking to B). Both hosts are connected to a wide area network through their security gateways (SG1 and SG2

respectively). Hosts A and B may know about their local security gateways, because of local configuration; they do not know about the other's security gateway however (or any possible intervening security gateways). In some cases, they may not even know about their local security gateways (e.g., in the case of a large private network with outside links through a number of firewalls). The security gateways may impose certain restrictions on the traffic they see (e.g., only encrypted traffic is allowed to go between A and B).

In such a scenario, Host A needs to determine:

- What its local policy with regards to end-to-end communication with Host B is. This decision may be deferred to the network administrator, as a matter of corporate policy.

- What B's policy with regards to the same end-to-end communication is; if there is an intersection of the two policies, it has to be determined, and the appropriate IPsec SAs have to be negotiated and established.

- What security gateways (if any) are in the path between A and B, and what their policies with respect to that communication is. For example, SG1 may allow any kind of traffic between A and B, whereas SG2 may require that any such traffic also be encrypted to itself. Or, SG1 may require that traffic to Host B only be authenticated but not encrypted end-to-end (e.g., certain financial institutions impose such requirements on traffic as a result of legislative controls), but that such traffic may be encrypted from Host A to SG1 and then from SG1 to Host B again. Naturally, Host A needs to ensure that SG1 actually has the authority to make such statements. Depending on the individual policies involved, any combination of these SAs may have to be established by Host A:

  - SA between Host A and Host B
  - SA between Host A and SG1
  - SA between Host A and SG2
  - SA between SG1 and SG2
  - SA between SG1 and Host B
  - SA between SG2 and Host B

- The same requirement with regards to communication security policy holds in the opposite direction as well (from Host B to Host A), since most traffic is in fact bidirectional. Note however that different requirements may exist for the two directions.

- If either of the Security Gateways decides to establish an SA between itself and the end-host (or some other SG), it may have to recursively invoke the discovery protocol.

The scenario may be further complicated by the fact that Host A, Host B, SG1, and SG2 may all lie in different administrative domains with correspondingly different security policies.

Manual configuration of policies and gateways is difficult even in the simple scenario described in this section. An architecture for automated gateway and policy discovery and resolution is necessary. Automatic keying may then be used to establish the necessary SAs, e.g., IKE [RFC-2409] or Photuris [Photuris].

Note that even in the trivial case of two hosts without an intervening security gateway, the IPSP architecture allows the two peers to determine what is necessary to establish a secure communication channel (e.g., what authorities or CAs they both trust).

Furthermore, note that there are multiple aspects of the overall security policy that applies to a particular communications that has to be made available in different parts of an IPsec implementation; packet selectors have to be specified in the SPD of a security gateway (or end-host), whereas SA parameters have to be provided to the key management system (and ultimately in the SADB).

Two more caveats:

The Security Policy System (SPS) defines a distributed database of security policy information. It provides the mechanisms needed for discovering, accessing, and processing security policy information of hosts, subnets, or networks.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC 2119].

2. Architecture Overview

The basic premises of the IPSP architecture are:

- Use of the SPP protocol [SPP] for gateway discovery and security policy distribution.

- Use of a trust management system and language [RFC-2704] to resolve and exchange policies respectively. Section 4 gives more details.

- Most of the burden of discovering and processing policy is placed on the initiator of a communications. Thus, expensive operations such as policy resolution is (optionally) performed by the initiator of a communications; security gateways need only perform compliance checking, which is computationally cheaper. Policy Servers MAY optionally perform policy resolution, to improve caching and accelerate communication establishment.

- IPsec policy is defined in terms of local policy (describing what requirements the host has for a particular communications) and signed policy statements from trusted entities. What entities (and to what extent) are trusted is a matter of local policy; signed policy statements are acquired through the SPP protocol. These statements may be used by an IPSP-compliant system in two ways:

  - To determine what traffic is allowed through a security gateway or accepted by the remote host.

  - To convince a security gateway or remote host to allow traffic through.

  Local policy is expressed in a vendor-specific way. It MUST

however be converted to a KeyNote local policy for processing by IPSP. The Policy Model [TDB] describes the semantics of the conversion.

(A "KeyNote local policy" is a policy statement that is unconditionally trusted by the host. Such statements MUST be securely stored and protected from tampering. In their simplest form, local policies reduce to a list of trusted keys or CAs.)

3. Use of SPP in IPSP

SPP is a security gateway and policy discovery protocol. It allows a host to determine what security gateways lie in the path to a specific destination, and what their security policies are. SPP may also be used to distribute certificates (or, more generally, credentials). Note that since trust management credentials are signed, it may not be necessary to sign the entire SPP payload when exchanging policies (to be resolved before next version).

For more details on SPP, see [SPP].

4. Compliance Checking and IPSP

Policies exchanged in SPP are encoded in KeyNote [RFC-2704] credentials. These are signed statements that describe the acceptable combinations of IPsec selectors (source/destination address and masks, transport protocol and ports, etc.) and SA parameters (encryption/authentication algorithms, key lengths, etc.)

A host's local policy specifies what public keys are trusted to make such statements; if KeyNote is used to specify local policy, further restrictions on what these keys are allowed to mandate can be expressed. Other languages (or methods) may be used to express local security policy as well; however, these policies MUST be translated to KeyNote local policies for processing by the trust management system. A separate document will describe the names and semantics of the various action attributes used in the KeyNote credentials used in IPsec, based on the IPsec policy model described in [TBD].

Policy servers in SPP store credentials (signed policy statements) created by the local network security administrator, as well as cached credentials acquired by querying other SPP servers. These credentials are then provided to the security gateway that forwarded the SPP query, and to the host that initiated the SPP protocol. The credentials may then be used in the key management protocol to authorize the host to establish SAs, if necessary, as described in [IPSP-TRUST]. In particular, the end-host may:

- Analyze the provided credentials to determine what, if any, SAs must be negotiated with a particular security gateway or end host (policy resolution). The algorithm for doing so is described in a separate document [TBD].

- Simply use the trust management engine to determine which of its local policies with regards to a particular communications is acceptable by the security gateway or remote host. For this, the end-host emulates the compliance checking process that the

security gateway or remote host will perform when negotiating SAs.

- The end-host may simply use the acquired credentials in the key management protocol. If the necessary SAs are established, the end-host may commence communications (or proceed with the policy discovery); otherwise, an error is reported, or one of the previous two approaches used.

The use of KeyNote credentials inside a key management protocol is described in [IPSP-TRUST].

Security gateways download policies from their configured Policy Servers, to initialize their SPD tables.

Note that while KeyNote credentials may also provide authentication information to be used by a key management protocol, other authentication mechanisms (e.g., PKIX certificates) can be used for this purpose as well.

Policy decorrelation is necessary to ensure that no conflicting policies exist. This process is desribed in [SPP] and is directly applicable to policies expressed in terms of KeyNote credentials.

Trust relations between different domains may also be described in terms of KeyNote credentials. A separate document will describe the operational implications of this. In particular, the implications of delegation across domains and policy decorrelation needs to be carefully examined and documented.

5. Legacy End-hosts

This section describes IPSP operation when either or both of the end-hosts (origin and/or destination end-hosts) are not IPSP-aware.

5.1 Legacy Origin End-host

When an origin end-host operating inside a Security Domain does not implement the Security Gateway Discovery Protocol, coordination between Security Gateways and the end-host is not possible.

A Security Gateway that intercepts a packet from such a host MAY initiate a Security Gateway discovery process, specifying that it will be proxying traffic for the end-host. This will allow the Security Gateway to establish IPsec tunnels with other Security Gateways (and potentially the destination end-host itself) that protects the origin end-host’s traffic.

5.2 Legacy Destination End-host

When a destination end-host does not implement the SGDP, it is the responsibility of the Policy Server of its Security Domain to specify the end-to-end security parameters (if any). This means that a Policy Server MUST be aware of which hosts it is responsible for.

6. Legacy Security Gateways

Legacy Security Gateways do not participate in the discovery

process, since they do not implement the SGDP. Such a system, upon receipt of a discovery packet may drop it (which will cause the discovery process to time-out), forward it with no further processing, or initiate an IPsec exchange with some remote host or Security Gateway, based on its local (non-IPSP-conforming) security policy. In the latter two cases, no further action is required by any IPSP-compliant system, as the legacy Security Gateway is transparent to the discovery process.

If the legacy Security Gateway drops the discovery packets and sends back an appropriate ICMP message, the recipient of such a message (another SG or the origin end-host) MAY establish the necessary IPsec SAs with the legacy SG to allow traffic to flow through the legacy SG. The legitimacy of the ICMP message MUST be verified through cryptographic (or other) means.

Alternatively, the Security Gateway or origin end-host MUST terminate the discovery process and notify the Policy Servers, SGs, and origin end-host involved in the discovery process.

No solution as yet exists if the legacy Security Gateway silently discards packets.

7. Security Considerations

This section has not been completed. It will be, in future versions of this draft.

8. IANA Considerations

No actions by IANA are required (yet).

9. ToDo List

- Describe semantics and operational requirements for inter-domain policies (delegation).
- Decorrelation in the context of delegation.
- Describe the resolution algorithm in detail (very similar to the one described in SPP).
- Determine whether all SPP messages must be protected, given that policies themselves are/may be signed.
- Describe SPD initialization by gateways (and end-hosts ?)
- Policy Server -- how does a host find out which one is the local one ? DHCP, manual configuration, LDAP, Service Discovery protocol, dedicated multicast address, other ?
- Mobile hosts and PS determination (same as above, more issues).
- Flesh out missing documents (find volunteers).
- Import policy model discussion.
- More verbose description of SPP ? Is reference sufficient ?

- Diagram with all possible SAs/tunnels in the example in Introduction.

References:

[RFC-2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", RFC-2119, March 1997.

[RFC-2401] S. Kent, R. Atkinson, RFC2401: "Security Architecture for the Internet Protocol", November 1998.

[IPSP-REQ] Blaze, M., Keromytis, A., Richardson, M., and L. Sanchez, draft-ietf-ipsp-requirements-00.txt: "IPsec Policy Discovery Protocol Requirements", October 1999.

[RFC-2409] Harkins, D., and D. Carrel, "The Internet Key Exchange (IKE)", RFC 2409, November 1998.

[Photuris] Karn, P., and B. Simpson, Photuris: Session Key Management Protocol, Work in Progress.

[IPSP-TRUST] Blaze, M., Ioannidis, J., and A. Keromytis, draft-blaze-ipsp-trustmgt-00.txt: "Compliance Checking and IPSEC Policy Management", March 2000.

[RFC-2704] Blaze, M., Feigenbaum, J., Ioannidis, J. and A. Keromytis, "The KeyNote Trust-Management System Version 2", RFC 2704, September 1999.

Authors' addresses:

Matt Blaze
AT&T Labs - Research
180 Park Avenue
Florham Park, New Jersey 07932-0971

Email: mab@research.att.com

Angelos D. Keromytis
Distributed Systems Lab
CIS Department, University of Pennsylvania
200 S. 33rd Street
Philadelphia, Pennsylvania 19104-6389

Telephone: +1 215 573 3639
Email: angelos@dsl.cis.upenn.edu

Michael C. Richardson
Sandelman Software Works Corp.
152 Rochester Street
Ottawa, ON K1R 7M4
Canada

Telephone: +1 613 276-6809
Email: mcr@sandelman.ottawa.on.ca

Luis A. Sanchez
BBN Technologies
GTE Internetworking

10 Moulton Street
Cambridge, MA 02140
USA

Telephone: +1 (617) 873-3351
Email: lsanchez@bbn.com

Expiration and File Name

This draft expires February 1, 2001

Its file name is draft-ietf-ipsp-arch-00.txt