IPSP Working Group M. Richardson, Sandelman Software Works
Internet Draft A. Keromytis, U. of Pennsylvania
draft-richardson-ipsp-requirements-00.txt L. Sanchez, BBN/GTEI
Expires April, 2000

IPsec Policy Discovery Protocol requirements

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC2026.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet- Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

To view the entire list of current Internet-Drafts, please check the "1id-abstracts.txt" listing contained in the Internet-Drafts Shadow Directories on ftp.is.co.za (Africa), ftp.nordu.net (Northern Europe), ftp.nis.garr.it (Southern Europe), munnari.oz.au (Pacific Rim), ftp.ietf.org (US East Coast), or ftp.isi.edu (US West Coast).

Abstract

This document describes the problem and solution requirements for an IPsec Policy Discovery protocol.

1.0 Introduction

1.1 Definition of terminology

Network security technologies are quickly being deployed over the Internet these days; in particular, two categories enjoy widespread usage:

a) security enforcement agents
Security gateways (commonly known as firewalls) are being installed along the perimeter of private internets to enforce access control and protect confidentiality of network traffic; these upper-layer gateways along with traditional link encryptors make up a scattered and uncoordinated set of security enforcement agents attempting to protect the Internet traffic.

b) secure communication protocols
   Cryptographic algorithms are being incorporated into secure communication protocols such as IPSec, SSL and SOCKS in order to support strong data integrity, authentication, and confidentiality services.

On one hand, these technologies provide the much needed security protection over the open Internet; on the other hand, they create a complex management task that beg for scalable solutions.

The deployment of security gateways divides the Internet into heterogeneous regions upholding different security policies, and the use of different cryptographic mechanisms at multiple protocol layers creates the need for negotiating the security mechanism and the key parameters. As a result, in order to support a secure communication-between two or more end-points, all the end-points and the security enforcement agents on the communication's route must work together to determine the suite of security services that can satisfy the security policies, and negotiate a common set of security mechanisms to implement these security services. While the negotiation of security mechanisms and key parameters may be supported by key management protocols such as ISAKMP [RFC-2408], a general and efficient process for managing the security policies and deducing the security services for this multi-party multi-layer security enforcement strategy is still unavailable.

A IPsec Policy Discovery Protocol (IPDP) must provide the essential infrastructure and the protocols necessary for conducting this process. An IPDP must provide
IPSec with the scalability and management needed to become fully deployable in operational environments.

1.2 Problem Description

The security management problem can be restated in the form of the following four questions:

a) How does one manage the process of creating and modifying security policies so as to maintain their mutual consistency?

b) How does one deduce the security requirements of an inter-domain communication based on the security policies of network domains?

c) How to select the choices of security services and enforcement agents in order to satisfy the security requirements?

d) How to orchestrate the negotiation of security mechanisms and cryptographic parameters in order to provide seamless support of security services?

The security management and scalability problems found in IPSec are captured in the following example:

In order to pass IP datagrams through several layers of IPSec-based firewalls, both the source and the destination of the datagrams must establish security associations with all or some of these firewalls encountered en-route.

However, neither the source nor the destination may know of the existence of all intermediate firewalls a priori, due to either their lack of knowledge about the network topology or the dynamics of the routing algorithms.

Consequently, negotiations must be conducted in sequence, on a trial-and-error basis. For instance, the source may become aware of the presence of a firewall if it receives ICMP messages from the firewall as it discards the packets for which it doesn't have a security association.

The source must then negotiate a security association with the firewall, use session keys to authenticate and/or encrypt the packets and retransmit them to the firewall.

This process could be repeated until no more ICMP messages are received from any firewall and the source is certain that the packets have successfully arrived at their destination.

This clumsy process can be further complicated by the fact that many firewalls may drop the packets without sending back any ICMP messages. Also, long-term security associations may have been arranged between some of the firewalls if technologies such as virtual private networks (VPNs) are used in part of the Internet. As a result, the tasks of finding existing security associations while negotiating for necessary new ones can be difficult, time consuming, and probably impossible to complete.

1.3 Basic Terminology

Security Gateway
: A security gateway refers to an intermediate system that implements IPSec protocols. For example, a router or a firewall implementing IPSec is a security gateway.

Security Domain
: A set of communicating entities and resources that share a common security policy enforced at a security gateway or host. The definition of security domain applies to networks protected by security gateways as well as to single hosts since a host could be the enforcer of its own policies. Security domains could exist inside other security domains.

Security Association
: A simplex "connection" that affords security services to the

traffic carried by it. Two types of securiy associations (SAs) are defined: transport mode and mode. A transport mode SA is a security association between two hosts. A tunnel mode SA is essentially an SA applied to an IP tunnel. Whenever either end of a security association is a security gateway, the SA MUST be tunnel mode.

Security Association Bundle
: A group of security associations that are used for communications that share a common endpoint. For example, all the SAs that a particular host needs to use to communicate with another host, including any SAs that host itself needs with intermediate gateways.

2.0 IPDP feature requirements

A IPsec Policy Discovery Protocol must be a distributed system which provides hosts and security gateways with the policy information required to establish a secure communication end-to-end. The goal of a policy discovery protocol is to provide the following services to hosts and security gateways:

1. **Discovery of security gateways**
2. **Management of dynamic security associations.**
3. **Resolution of security requirements for inter-domain communication**
4. **Consistency checking of local security policies.**

As part of this, a Policy Discovery Protocol should provide a language that allows one to specify security policies in terms of primitives such as user identity or role, source and destination machine address and port number, encryption and authentication algorithms.

A host should be able to discover any remote security gateways relevant in an end-to-end communication. The host must be able to validate the identities of (local and remote) security policy agents and security gateways. It must be able to verify that the gateways in question are entitled to represent a destination host.

A related service required by the IPsec Policy Discovery Protocol is a mechanism to express security policies and to populate a security server with the policies for a given security domain. The mechanism should follow an object-oriented approach, where one can declare various configuration objects within a security domain as part of an overall hierarchy supporting inheritance.

Attributes of the objects should be mandatory or optional. A mandatory attribute has to be defined for all objects of the class; optional attributes can be skipped. Attributes can also be single or multiple valued.

2.1 IPDP architecture requirements

The architectural requirements of the IPsec Policy Discovery Protocol are as follows:

2.1.1 Discover Gateways

IPDP must be able to determine a set of necessary security gateways through which a message must travel to complete a communication on a single path between two hosts.

2.1.2 Verify Identities

IPDP must allow hosts to verify the identities of gateways and other hosts with which they are communicating. It must also be able to verify that a gateway that claims to represent a particular host actually does have the authority to represent that host.

2.1.3 Manage Bundles of Security Associations

IPDP must be able to effectively manage bundles of security associations. It must be able to create bundles from policy information, determine if existing security associations or bundles may be used when creating new bundles, create new security associations as needed for new bundles, and keep security associations in existing bundles up-to-date.

2.1.4 Require no changes to security protocols

IPDP must not require changes, additions or modifications to the algorithms or protocols of the security protocols that use it.

2.1.5 Key Management Protocol Independence

IPDP must be independent of any particular key management protocol.

2.1.6 No Exterior Infrastructure Dependency

IPDP must not depend upon an exterior infrastructure, although implementations may use an exterior infrastructure. For example, public keys may be distributed using the existing DNS infrastructure. IPDP must not prohibit other means for distributing keys. Particular implementations may, however, rely on the DNS for key distribution, though they may not be as robust as implementations that provide several key distribution mechanisms.

It is necessary, however, that the routing infrastructure be in place so IPDP servers may be contacted. This is not a difficult requirement, since that infrastructure must be in place to send the communications that require the use of IPDP.

References:

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

[RFC-2408] D. Maughan, M. Shertler, M. Schneider, J. Turner, RFC2408: "Internet Security Association and Key Management Protocol (ISAKMP)", November 1998.

Author's Address

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

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

EMail: angelos@dsl.cis.upenn.edu

Expiration and File Name

This draft expires April 1, 2000

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