

Network Working Group
Request for Comments: 3586
Category: Standards Track

M. Blaze
AT&T Labs - Research
A. Keromytis
Columbia University
M. Richardson
Sandelman Software Works
L. Sanchez
Xapiens Corporation
August 2003

IP Security Policy (IPSP) Requirements

Status of this Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

Copyright Notice

Copyright (C) The Internet Society (2003). All Rights Reserved.

Abstract

This document describes the problem space and solution requirements for developing an IP Security Policy (IPSP) configuration and management framework. The IPSP architecture provides a scalable, decentralized framework for managing, discovering and negotiating the host and network security policies that govern access, authorization, authentication, confidentiality, data integrity, and other IP Security properties. This document highlights such architectural components and presents their functional requirements.

Table of Contents

1. Introduction.....	2
1.1. Terminology.....	2
1.2. Security Policy and IPsec.....	2
2. The IP Security Policy Problem Space.....	3
3. Requirements for an IP Security Policy Configuration and Management Framework.....	5
3.1. General Requirements.....	5
3.2. Description and Justification.....	5
3.2.1. Policy Model.....	5
3.2.2. Security Gateway Discovery.....	6

3.2.3.	Policy Specification Language.....	6
3.2.4.	Distributed policy.....	6
3.2.5.	Policy Discovery.....	6
3.2.6.	Security Association Resolution.....	6
3.2.7.	Compliance Checking.....	7
4.	Security Considerations.....	7
5.	IANA Considerations.....	7
6.	Intellectual Property Statement.....	7
7.	References.....	8
7.1.	Normative References.....	8
7.2.	Informative References.....	8
8.	Disclaimer.....	8
9.	Acknowledgements.....	8
10.	Authors' Addresses.....	9
11.	Full Copyright Statement.....	10

1. Introduction

1.1. Terminology

The keywords "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].

1.2. Security Policy and IPsec

Network-layer security now enjoys broad popularity as a tool for protecting Internet traffic and resources. Security at the network layer can be used as a tool for at least two kinds of security architecture:

- a) Security gateways. Security gateways (including "firewalls") at the edges of networks use IPsec [RFC-2401] to enforce access control, protect the confidentiality and authenticity of network traffic entering and leaving a network, and to provide gateway services for virtual private networks (VPNs).
- b) Secure end-to-end communication. Hosts use IPsec to implement host-level access control, to protect the confidentiality and authenticity of network traffic exchanged with the peer hosts with which they communicate, and to join virtual private networks.

On one hand, IPsec provides an excellent basis for a very wide range of protection schemes; on the other hand, this wide range of applications for IPsec creates complex management tasks that become especially difficult as networks scale up and require different security policies, and are controlled by different entities, for different kinds of traffic in different parts of the network.

As organizations deploy security gateways, the Internet divides into heterogeneous regions that enforce different access and security policies. Yet it is often still necessary for hosts to communicate across the network boundaries controlled by several different policies. The wide range of choices of cryptographic parameters (at multiple protocol layers) complicates matters and introduces the need for hosts and security gateways to identify and negotiate a set of security parameters that meets each party's requirements. Even more complexity arises as IPsec becomes the means through which firewalls enforce access control and VPN membership; two IPsec endpoints that want to establish a security association must identify, not only the mutually acceptable cryptographic parameters, but also exactly what kind of access the combined security policy provides.

While the negotiation of cryptographic and other security parameters for IPsec security associations (SAs) is supported by key management protocols (e.g., ISAKMP [RFC-2408]), the IPsec key management layer does not provide a scheme for managing, negotiating, or enforcing the security policies under which SAs operate.

IPSP provides the framework for managing IPsec security policy, negotiating security association (SA) parameters between IPsec endpoints, and distributing authorization and policy information among hosts that require the ability to communicate via IPsec.

2. The IP Security Policy Problem Space

IPSP aims to provide a scalable, decentralized framework for managing, discovering and negotiating the host and network IPsec policies that govern access, authorization, cryptographic mechanisms, confidentiality, data integrity, and other IPsec properties.

The central problem solved by IPSP is that of controlling security policy in a manner that is useful for the wide range of IPsec applications and modes of operation. In particular:

- IPSP hosts may serve as IPsec endpoints, security gateways, network management hubs, or a combination of these functions. IPSP will manage end-users computers (which may be fixed workstations controlled by a single organization or mobile laptops that require remote access to a corporate VPN), firewalls (which provide different services and allow different levels of access to different classes of traffic and users), VPN routers (which support links to other VPNs that might be controlled by a different organization's network policy), web and other servers (which might provide different services depending on where a client request came from), and so on.

- IPSP administration will be inherently heterogeneous and decentralized. A basic feature of IPsec is that two hosts can establish a Security Association even though they might not share a common security policy, or, indeed, trust one another at all. This property of IPsec becomes even more pronounced at the higher level abstraction managed by IPSP.
- The SA parameters acceptable to any pair of hosts (operating under different policies) will often not be specified in advance. IPSP will often have to negotiate and discover the mutually-acceptable SA parameters on-the-fly when two hosts attempt to create a new SA.
- Some hosts will be governed by policies that are not directly specified in the IPSP language. For example, a host's IPsec policy might be derived from a more comprehensive higher-layer security policy managed by some other system. Similarly, some vendors might develop specialized (and proprietary) tools for managing policy in their products. In such cases, it is necessary to derive an IPSP policy specification for only those aspects of a host's policy that involve interoperability with other hosts running IPSP.
- IPSP must scale to support complex policy administration schemes. In even modest-size networks, one administrator must often control policy remotely, and must have the ability to change the policy on many different hosts at the same time. In larger networks (or those belonging to large organizations), a host's policy might be governed by several different authorities (e.g., several different departments might have the authority to add users to a firewall or open access to new services). Different parts of a policy might be "owned" by different entities in a complex hierarchy. IPSP must provide a mechanism for delegating specific kinds of authority to specific entities.
- The semantics of IPSP must be well defined, particularly with respect to any security-critical aspects of the system.
- IPSP must be secure, sound, and comprehensible. It should be possible to understand what an IPSP policy does; the difficulty of understanding an IPSP policy should be somewhat proportional to the complexity of the problem it solves. It should also be possible to have confidence that an IPSP policy does what it claims, and that IPSP implementation is correct; architecturally, the security-critical parts of IPSP should be small and well-specified enough to allow verification of their correct operation. Ideally, IPSP should be compatible with

formal methods, such as implementing security policies with provable properties.

3. Requirements for an IP Security Policy Configuration and Management Framework

3.1. General Requirements

An IPSP solution MUST include:

- A policy model with well-defined semantics that captures the relationship between IPsec SAs and higher-level security policies,
- A gateway discovery mechanism that allows hosts to discover where to direct IPsec traffic intended for a specific endpoint,
- A well-specified language for describing host policies,
- A means for distributing responsibility for different aspects of policy to different entities,
- A mechanism for discovering the policy of a host,
- A mechanism for resolving the specific IPsec parameters to be used between two hosts governed by different policies (and for determining whether any such parameters exist); and,
- A well-specified mechanism for checking for compliance with a host's policy when SAs are created.

The mechanisms used in IPSP must not require any protocol modifications in any of the IPsec standards (ESP [RFC-2406], AH, [RFC-2402], IKE [RFC-2409]). The mechanisms must be independent of the SA-negotiation protocol, but may assume certain functionality from such a protocol (this is to ensure that future SA-negotiation protocols are not incompatible with IPSP).

3.2. Description and Justification

3.2.1. Policy Model

A Policy Model defines the semantics of IPsec policy. Policy specification, checking, and resolution should implement the semantics defined in the model. However, the model should be independent of the specific policy distribution mechanism and policy discovery scheme, to the extent possible.

3.2.2. Security Gateway Discovery

The gateway discovery mechanism may be invoked by any host or gateway. Its goal is to determine what IPsec gateways exist between the initiator and the intended communication peer. The actual mechanism employed may be used to piggy-back information necessary by other components of the IPSP architecture (e.g., policy discovery, as is done in [SPP]). The discovery mechanism may have to be invoked at any time, independently of existing security associations or other communication, to detect topology changes.

3.2.3. Policy Specification Language

In order to allow for policy discovery, compliance checking, and resolution across a range of hosts, a common language is necessary in which to express the policies of hosts that need to communicate with one another. Statements in this language are the output of policy discovery, and provide the input to the policy resolution and compliance checking systems. Note that a host's or network's security policy may be expressed in a vendor-specific way, but would be translated to the common language when it is to be managed by the IPSP services.

3.2.4. Distributed policy

As discussed above, it must be possible for all or part of a host's policy to be managed remotely, possibly by more than one entity. This is a basic requirement for large-scale networks and systems.

3.2.5. Policy Discovery

A policy discovery mechanism must provide the essential information that two IPsec endpoints can use to determine what kinds of SAs are possible between one another. This is especially important for hosts that are not controlled by the same entity, and that might not initially share any common information about one another. Note that a host need not reveal its entire security policy, only enough information to support the SA resolution system for hosts that might want to communicate with it.

3.2.6. Security Association Resolution

Once two hosts have learned enough about each other's policies, it must be possible (and computationally feasible) to find an acceptable set of SA parameters that meets both host's requirements and will lead to the successful creation of a new SA.

3.2.7. Compliance Checking

When a host proposes the output of the SA resolution scheme, it must be checked for compliance with the local security policy of each host. The security and soundness of the SAs created by IPSP-managed communication should depend only on the correctness of the compliance checking stage. In particular, even if the SA resolution scheme (which is likely to be computationally and conceptually complex) produces an incorrect result, it should still not be possible to violate the specified policy of either host.

4. Security Considerations

This document discusses the high-level requirements for a policy framework and architecture for IPsec. A justification for the various components is given.

5. IANA Considerations

No action is required by IANA.

6. Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on the IETF's procedures with respect to rights in standards-track and standards-related documentation can be found in BCP-11.

Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF Secretariat.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to practice this standard. Please address the information to the IETF Executive Director.

7. References

7.1. Normative References

- [RFC-2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Level", BCP 14, RFC 2119, March 1997.
- [RFC-2401] Kent, S. and R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, November 1998.

7.2. Informative References

- [RFC-2402] Kent, S. and R. Atkinson, "IP Authentication Header", RFC 2402, November 1998.
- [RFC-2406] Kent, S. and R. Atkinson, "IP Encapsulating Security Payload (ESP)", RFC 2406, November 1998.
- [RFC-2408] Maughan, D., Shertler, M., Schneider, M. and J. Turner, "Internet Security Association and Key Management Protocol (ISAKMP)", RFC 2408, November 1998.
- [RFC-2409] Harkins, D and D. Carrel, "The Internet Key Exchange (IKE)", RFC 2409, November 1998.
- [SPP] Sanchez, L. and M. Condell, "The Security Policy Protocol", Work in Progress.

8. Disclaimer

The views and specification here are those of the authors and are not necessarily those of their employers. The authors and their employers specifically disclaim responsibility for any problems arising from correct or incorrect implementation or use of this specification.

9. Acknowledgements

The authors thank the members of the IPsec Policy working group that contributed to this document.

10. Authors' Addresses

Matt Blaze
AT&T Labs - Research
180 Park Avenue
Florham Park, NJ 07932 USA

EMail: mab@crypto.com

Angelos D. Keromytis
Computer Science Department
Columbia University
1214 Amsterdam Avenue, M.C. 0401
New York, NY 10027, USA

EMail: angelos@cs.columbia.edu

Michael C. Richardson
Sandelman Software Works Corp.
470 Dawson Avenue
Ottawa, ON K1Z 5V7 Canada

Phone: +1 613 276-6809

EMail: mcr@sandelman.ottawa.on.ca

Luis A. Sanchez
Xapiens Corporation
PO Box 9023694
San Juan, PR 00902 USA

Phone: +1 (787) 832-4717

EMail: lsanchez@xapiens.com

11. Full Copyright Statement

Copyright (C) The Internet Society (2003). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assignees.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.

