

Network Working Group
Request for Comments: 2401
Obsoletes: 1825
Category: Standards Track

S. Kent
BBN Corp
R. Atkinson
@Home Network
November 1998

Security Architecture for the Internet Protocol

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 (1998). All Rights Reserved.

Table of Contents

1. Introduction	3
1.1 Summary of Contents of Document	3
1.2 Audience	3
1.3 Related Documents	4
2. Design Objectives	4
2.1 Goals/Objectives/Requirements/Problem Description	4
2.2 Caveats and Assumptions	5
3. System Overview	5
3.1 What IPsec Does	6
3.2 How IPsec Works	6
3.3 Where IPsec May Be Implemented	7
4. Security Associations	8
4.1 Definition and Scope	8
4.2 Security Association Functionality	10
4.3 Combining Security Associations	11
4.4 Security Association Databases	13
4.4.1 The Security Policy Database (SPD)	14
4.4.2 Selectors	17
4.4.3 Security Association Database (SAD)	21
4.5 Basic Combinations of Security Associations	24
4.6 SA and Key Management	26
4.6.1 Manual Techniques	27
4.6.2 Automated SA and Key Management	27
4.6.3 Locating a Security Gateway	28
4.7 Security Associations and Multicast	29

5. IP Traffic Processing	30
5.1 Outbound IP Traffic Processing	30
5.1.1 Selecting and Using an SA or SA Bundle	30
5.1.2 Header Construction for Tunnel Mode	31
5.1.2.1 IPv4 -- Header Construction for Tunnel Mode	31
5.1.2.2 IPv6 -- Header Construction for Tunnel Mode	32
5.2 Processing Inbound IP Traffic	33
5.2.1 Selecting and Using an SA or SA Bundle	33
5.2.2 Handling of AH and ESP tunnels	34
6. ICMP Processing (relevant to IPsec)	35
6.1 PMTU/DF Processing	36
6.1.1 DF Bit	36
6.1.2 Path MTU Discovery (PMTU)	36
6.1.2.1 Propagation of PMTU	36
6.1.2.2 Calculation of PMTU	37
6.1.2.3 Granularity of PMTU Processing	37
6.1.2.4 PMTU Aging	38
7. Auditing	39
8. Use in Systems Supporting Information Flow Security	39
8.1 Relationship Between Security Associations and Data Sensitivity	40
8.2 Sensitivity Consistency Checking	40
8.3 Additional MLS Attributes for Security Association Databases	41
8.4 Additional Inbound Processing Steps for MLS Networking	41
8.5 Additional Outbound Processing Steps for MLS Networking	41
8.6 Additional MLS Processing for Security Gateways	42
9. Performance Issues	42
10. Conformance Requirements	43
11. Security Considerations	43
12. Differences from RFC 1825	43
Acknowledgements	44
Appendix A -- Glossary	45
Appendix B -- Analysis/Discussion of PMTU/DF/Fragmentation Issues	48
B.1 DF bit	48
B.2 Fragmentation	48
B.3 Path MTU Discovery	52
B.3.1 Identifying the Originating Host(s)	53
B.3.2 Calculation of PMTU	55
B.3.3 Granularity of Maintaining PMTU Data	56
B.3.4 Per Socket Maintenance of PMTU Data	57
B.3.5 Delivery of PMTU Data to the Transport Layer	57
B.3.6 Aging of PMTU Data	57
Appendix C -- Sequence Space Window Code Example	58
Appendix D -- Categorization of ICMP messages	60
References	63
Disclaimer	64
Author Information	65
Full Copyright Statement	66

~~RFC 2401~~

~~Security Architecture for IP~~

~~November 1998~~

Kent & Atkinson

Standards Track

[Page 2]

El

RFC 2401

Security Architecture for IP

November 1998

1. Introduction

1.1 Summary of Contents of Document

This memo specifies the base architecture for IPsec compliant systems. The goal of the architecture is to provide various security services for traffic at the IP layer, in both the IPv4 and IPv6 environments. This document describes the goals of such systems, their components and how they fit together with each other and into the IP environment. It also describes the security services offered by the IPsec protocols, and how these services can be employed in the IP environment. This document does not address all aspects of IPsec architecture. Subsequent documents will address additional architectural details of a more advanced nature, e.g., use of IPsec in NAT environments and more complete support for IP multicast. The following fundamental components of the IPsec security architecture are discussed in terms of their underlying, required functionality. Additional RFCs (see Section 1.3 for pointers to other documents) define the protocols in (a), (c), and (d).

- a. Security Protocols -- Authentication Header (AH) and Encapsulating Security Payload (ESP)
- b. Security Associations -- what they are and how they work, how they are managed, associated processing
- c. Key Management -- manual and automatic (The Internet Key Exchange (IKE))
- d. Algorithms for authentication and encryption

This document is not an overall Security Architecture for the Internet; it addresses security only at the IP layer, provided through the use of a combination of cryptographic and protocol security mechanisms.

The keywords MUST, MUST NOT, REQUIRED, SHALL, SHALL NOT, SHOULD, SHOULD NOT, RECOMMENDED, MAY, and OPTIONAL, when they appear in this document, are to be interpreted as described in RFC 2119 [Bra97].

1.2 Audience

The target audience for this document includes implementers of this IP security technology and others interested in gaining a general background understanding of this system. In particular, prospective users of this technology (end users or system administrators) are part of the target audience. A glossary is provided as an appendix

~~RFC 2401~~

~~Security Architecture for IP~~

~~November 1998~~

El

RFC 2401

Security Architecture for IP

November 1998

to help fill in gaps in background/vocabulary. This document assumes that the reader is familiar with the Internet Protocol, related networking technology, and general security terms and concepts.

1.3 Related Documents

As mentioned above, other documents provide detailed definitions of some of the components of IPsec and of their inter-relationship.

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts



Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research



With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips



Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.