Network Working Group
Internet-Draft
Category: Standards Track
draft-ietf-isis-hmac-01.txt

T. Li
Procket Networks
R. Atkinson

10 April 2000

IS-IS Cryptographic Authentication

Status of this Memo

ABSTRACT

This document specifies an algorithm-independent cryptographic authentication mechanism for use with the IS-IS routing protocol.

1. Use of Imperatives

Throughout this document, the words that are used to define the significance of particular requirements are capitalized. These words have the meaning defined in RFC-2119, which is hereby incorporated by reference. [7]

2. Introduction

Growth in the Internet has made us aware of the need for improved authentication of routing information. Other routing protocols are known to have been the subject of both active and passive attacks. At present, IS-IS provides for unauthenticated service or password authentication. Both are vulnerable to passive attacks currently widespread in the Internet. Well-understood security issues exist in routing protocols [3]. Clear text passwords, currently specified for use with IS-IS, are no longer considered sufficient [4] in the Internet.

If authentication is disabled, then only simple misconfigurations are detected. Simple passwords transmitted in the clear will further protect against the honest neighbor, but are useless in the general case. By simply capturing information on the wire - straightforward even in a remote environment - a hostile process can learn the password and overcome the network. While IS-IS packets aren't themselves routed, anyone with access to a system on the physical link can inject forged packets (unless a cryptographic authentication method is in use).

We propose that IS-IS use an authentication algorithm, as was originally proposed for SNMP Version 2. Keyed MD5 is proposed as the standard authentication algorithm for IS-IS, but the authentication mechanism is believed to be algorithm-independent.

While this mechanism is not unbreakable (no known mechanism is), it provides a greatly enhanced probability that a system being attacked will detect and ignore hostile messages. This is because we transmit the output of an authentication algorithm (e.g., Keyed MD5) rather than the secret IS-IS Authentication Key. This output is a one-way function of a message and a secret IS-IS Authentication Key. This IS-IS Authentication Key is never sent over the network in the clear, thus providing protection against the passive attacks now commonplace in the Internet.

In this way, protection is afforded against forgery or message modification. It is possible to replay a LSP until the LSP sequence number changes, but the normal dynamics of the protocol make LSP replay less of an issue in the long-term. The mechanism does not afford confidentiality, since messages stay in the clear; however,

the mechanism is also exportable from most countries, which test a privacy algorithm would fail.

Other relevant rationales for the approach are that Keyed MD5 is being used for RIPv2 and OSPF cryptographic authentication, and is

therefore present in routers already, as is some form of password management. In the interest of code reuse, this IS-IS extension specifies Keyed-MD5 as the mandatory-to-implement algorithm. There are no specific known vulnerabilities in Keyed-MD5 as used in this context. A similar approach has been standardized for use in IP-layer authentication. [6]

This document is a publication of the IS-IS Working Group within the IETF. It is also a contribution to ISO IEC JTC1/SC6, for eventual inclusion with ISO 10589.

3. Implementation Approach

Implementation requires three issues to be addressed:

(1) TLV format for use with cryptographic authentication,

(2) Authentication procedures, and

(3) Management controls.

3.1. IS-IS PDU Format

The IS-IS protocol, as specified in ISO 10589, provides for the authentication of Link-State PDUs (LSPs) through the inclusion of authentication information as part of the LSP. This authentication information is encoded as a Type-Length-Value triple.

The type of the Authentication TLV is 10. The length of the TLV is variable. The value of the TLV depends on the Authentication Type being used.

The first octet of the value field indicates the Authentication Type. Authentication Type 0 is reserved. Type 1

indicates a clear-text password, and Type 255 is used for routing domain private authentication methods.

This document specifies an extension for cryptographic authentication. When cryptographic authentication is in use, the Authentication Type in the first octet of the Value field is set to 54 and the second octet of the Value field contains a Key Identifier (Key-ID). The Key Identifier is used by the recipient to select the particular IS-IS Security Association in use for this PDU. The remainder of the Value field contains the Authentication Data itself. Thus, the Length of the TLV is (2 + sizeof(authentication data)), when the Authentication Type is cryptographic authentication.

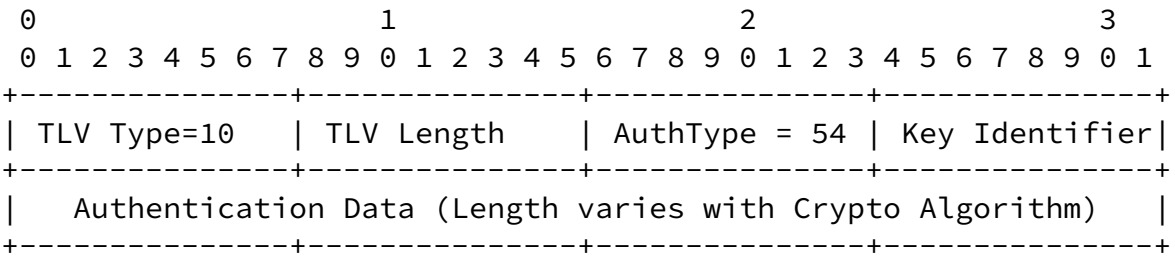

Figure 1: Authentication TLV Format,
when Cryptographic Authentication is in use

3.2 Authentication Procedures

Conforming or compliant implementations MUST implement the HMAC-MD5 cryptographic algorithm with this extension. The algorithm-dependent details of HMAC-MD5 are specified in Appendix A.

A fundamental concept of IS-IS Cryptographic Authentication is the "IS-IS Security Association". An IS-IS Security Association contains a Key Identifier, the Cryptographic Authentication Algorithm (e.g. HMAC-MD5) to use, a Lifetime, and the Cryptographic Authentication Key to use. The Cryptographic Authentication Key is also the password for the PDU Type, as specified in ISO 10589.

An implementation MAY include cryptographic authentication information in PDUs even if it does not fully implement cryptographic authentication. This allows an implementation to generate authentication information without verifying the authentication information as a transition aid for networks in the process of deploying authentication.

An implementation that does not implement cryptographic

authentication MAY accept a PDU that contains the cryptographic authentication type.

The remainder of this section describes the algorithm-independent processing for IS-IS Cryptographic Authentication.

The Type, Length, Authentication Type, and Key Identifier fields are filled with their final values prior to calculation of the cryptographic Authentication Data. The Authentication Data field, the Checksum field, and the Remaining Lifetime fields are all filled with all zeros for the calculation of the cryptographic Authentication Data for a given LSP. Sending systems calculate the Checksum value after the Authentication Data field has been filled in. After the Checksum value has been calculated, it is placed in the IS-IS packet.

[New paragraph discussing how contents are dealt with for non-LSPs (e.g. CSNPs, IIHs) coming here soon.]

When multiple valid IS-IS Security Associations exist for a given IS-IS system, sending systems SHOULD pick an IS-IS Security Association that is not about to expire in order to facilitate smooth key rollover.

Receiving systems first check the Key-ID field and use its value to locate the appropriate IS-IS Security Association. If no

IS-IS Security Association exists, the packet is discarded as not authentic, without any further processing. If the matching IS-IS Security Association is located, then the receiving system independently computes the cryptographic Authentication Data using the key contained in that IS-IS Security Association and the values in the received IS-IS packet. For receive-side authentication computations, the Authentication Data field itself, the Checksum field, and the Remaining Lifetime fields are each assumed to be zero. If the computed cryptographic Authentication Data is identical to the received Authentication Data, the packet is accepted as authentic and undergoes normal IS-IS receive-side processing. If there is any difference, the packet is discarded as not authentic, without any further processing.

An implementation SHOULD log authentication failures of

received IS-IS PDUs if this can be done without creating a denial of service attack on the Intermediate System. Details of this are unspecified here.

Intermediate Systems (i.e. routers) that implement cryptographic authentication and initiating LSP purges MUST remove the body of the LSP and add the authentication TLV. Intermediate Systems MUST NOT accept unauthenticated purges. Intermediate Systems MUST NOT accept purges that contain TLVs other than the Authentication TLV. These restrictions are necessary to prevent a hostile system from receiving an LSP, setting the Remaining Lifetime field to zero, and flooding it, thereby initiating a purge without knowing any authentication information.

3.3. Key Management Requirements

It is strongly desirable that a hypothetical security breach in one Internet protocol not automatically compromise other Internet protocols. The Cryptographic Authentication Key of this specification SHOULD NOT be stored or transmitted using protocols or algorithms that have known flaws.

Implementations MUST support the storage and use of at least two IS-IS Security Associations at the same time. During normal operation, only one IS-IS Security Association (i.e. one key) will usually be active in a given IS-IS system. However, during the key change period, both the old IS-IS Security Association and the new IS-IS Security Association (i.e. two keys) will be active in the same system at the same time.

An IS-IS Security Association MUST contain at least the lifetime of the IS-IS Security Association (e.g. date/time first valid and date/time no longer valid), the Key Identifier, the Cryptographic Authentication Algorithm, and the Cryptographic Key itself. The IS-IS Security Association lifetime MAY be infinite or MAY have a specific date/time for start and end.

Implementations MUST support manual key distribution (e.g., the privileged user manually typing in the parameters for the IS-IS Security Association (i.e. key, key lifetime, and key identifier) on the router console. If more than one algorithm is supported, then the implementation MUST require that the algorithm be specified for each IS-IS Security Association at the time the other IS-IS Security Association information is entered. IS-IS Security Associations that are out of date MAY be deleted at will by the implementation without requiring human intervention. Manual deletion of active IS-IS Security Associations by the privileged operator SHOULD also be supported.

It is desirable to use a key management protocol to distribute IS-IS Authentication Keys among communicating IS-IS implementations. Such a protocol would provide scalability and significantly reduce the human administrative burden. The Key ID can be used as a hook between IS-IS and such a future protocol. Key management protocols have a long history of subtle flaws that are often discovered long after the protocol was first described in public. To avoid having to change all IS-IS implementations should such a flaw be discovered, integrated key management protocol techniques were deliberately omitted from this specification.

4.0. Key Management Procedures

As with all security methods using keys, it is necessary to change the IS-IS Authentication Key on a regular basis. To maintain routing stability during such changes, implementations MUST be able to store and use at least two IS-IS Security Associations (hence: authentication keys) in any given system at the same time.

Each IS-IS Security Association has its own Key Identifier, which is stored locally. The Key Identifier uniquely identifies the IS-IS Security Association in use.

The intermediate system creating the IS-IS message will select a valid key from the set of valid keys for that interface. The receiver will use the Key Identifier to determine which IS-IS Security Association to use for authentication of the received message. The receiver MUST NOT ignore the Key Identifier and try all known keys on an incoming packet as this creates an easily prevented denial-of-service attack on the IS-IS implementation. More than one IS-IS Security Association (hence: more than one key) MAY be associated with an interface at the same time.

Hence it is possible to have fairly smooth IS-IS Authentication Key rollovers without losing legitimate LSPs because the stored authentication key is incorrect and without requiring people to change all the keys at once. To ensure a smooth rollover, each communicating IS-IS system must be updated with the new key several minutes before the current key will expire and several minutes before the new key lifetime begins. The new key should have a lifetime that starts several minutes before the old key expires. This gives time for each system to learn of the new IS-IS Authentication Key before that key will be used. It also ensures that the new key will begin being used and the current key will go out of use before the current key's lifetime expires. For the duration of the overlap in key lifetimes, a system may receive messages using either key and authenticate the message as indicated by the Key ID.

4.3. Pathological Cases

Two pathological cases exist which must be handled, which are failures of the network manager. Both of these should be exceedingly rare.

During key rollover, devices may exist which have not yet been successfully configured with the new key. Therefore, routers SHOULD implement (and would be well advised to implement) an algorithm that detects the set of keys being used by its neighbors, and transmits

its messages using both the new and old keys until all of the neighbors are using the new key or the lifetime of the old key expires. Under normal circumstances, this elevated transmission rate will exist for a single update interval.

In the event that the last key associated with a system, it is unacceptable to revert to an unauthenticated condition, and not advisable to disrupt routing. Therefore, the router should send a "last authentication key expiration" notification to the network manager and treat the key as having an infinite lifetime until the lifetime is extended, the key is deleted by network management, or a new key is configured.

5. Conformance Requirements

To conform to this specification, an implementation MUST support all of its aspects. The HMAC-MD5 authentication algorithm MUST be implemented by all conforming implementations. MD5 is defined in RFC-1321. A conforming implementation MAY also support other authentication algorithms such as Keyed Secure Hash Algorithm (SHA).

Manual key distribution as described above MUST be supported by all conforming implementations. All conforming implementations MUST support the smooth key rollover described under "Key Change Procedures."

6. Acknowledgments

This work is derived directly from RFC-2082 and the similar work done for OSPFv2 Cryptographic Authentication.

7. References

[1] ISO-10589

[2] Rivest, R., "The MD5 Message-Digest Algorithm", RFC 1321, April 1992.

[3] S. Bellovin, "Security Problems in the TCP/IP Protocol Suite", ACM Computer Communications Review, Volume 19, Number 2, pp.32-48, April 1989.

[4] Haller, N., and R. Atkinson, "Internet Authentication

Guidelines", RFC 1704, October 1994.

[5] Braden, R., Clark, D., Crocker, S., and C. Huitema, "Report of IAB Workshop on Security in the Internet Architecture", RFC 1636, June 1994.

[6] Atkinson, R., "IP Authentication Header", RFC 1826, August 1995.

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

8. Security Considerations

This entire memo describes and specifies an authentication mechanism for the IS-IS routing protocol that is believed to be reasonably secure against active and passive attacks. Passive attacks are clearly widespread in the Internet at present. Protection against active attacks is also needed because active attacks are becoming more common.

Users need to understand that the quality of the security provided by this mechanism depends completely on the strength of the implemented authentication algorithms, the strength of the key being used, and the correct implementation of the security mechanism in all communicating IS-IS implementations. This mechanism also depends on the IS-IS Cryptographic Authentication Key being kept confidential by all parties. If any of these incorrect or insufficiently secure, then no real security will be provided to the users of this mechanism.

Specifically with respect to the use of SNMP, compromise of SNMP security has the necessary result that the various IS-IS configuration parameters (e.g. routing table, IS-IS Authentication Key) manageable via SNMP could be compromised as well. Changing Authentication Keys using non-encrypted SNMP is no more secure than sending passwords in the clear.

Confidentiality is not provided by this mechanism. Protection against traffic analysis is also not provided. Mechanisms such as bulk link encryption might be used when protection against traffic

analysis is required. Finally, this technique does not prevent replay attacks. Appropriate use of key management can reduce the residual risk associated with replay attacks if desired by the operator.

10. Authors' Addresses

Tony Li

Procket Networks
San Jose, CA

Email: tli@procket.com

Randall Atkinson
Engineer at large