Network Working Group
Request for Comments: 2520
Category: Experimental

J. Luciani
Nortel Networks
H. Suzuki
Cisco Systems
N. Doraswamy
Nortel Networks
D. Horton
CiTR Pty Ltd

February 1999

NHRP with Mobile NHCs

Status of this Memo

This memo defines an Experimental Protocol for the Internet community. It does not specify an Internet standard of any kind. Discussion and suggestions for improvement are requested. Distribution of this memo is unlimited.

Copyright Notice

Abstract

This document describes an extension to NHRP [1] which would allow Mobile NHCs to perform a registration with and attach to an NHS in their home LIS in an authenticated manner.

As described in this document, Mobile NHCs are NHCs which are not configured with enough information to find a specific serving NHS in their home LIS, but which have a mechanism to find an NHS (which may or may not be a serving NHS) to which they will attach. As described in [1], an NHC may attach to a 'surrogate' NHS by using a mechanism such as an anycast address. In this case, the NHC may use the surrogate NHS to send a NHRP Registration Request toward the NHC's home LIS where a serving NHS resides. However, as defined in [1], packet authentication is performed on a hop by hop basis. In the mobile NHC case, it is not practical for the mobile NHC be in a security relationship with every surrogate NHS, thus it is presumably desirable to have some form of end to end only authentication for the case of a mobile NHC's registration. This document describes an authentication extension for NHRP which has such end to end only semantics.

1. Introduction

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 [4].

This document describes an extension for Mobile NHCs to use when they wish to register with their home LIS but initially connect to a non-serving NHS to do so. The reader is encouraged to read [1] for more details on the NHRP registration process.

2.0 Definition of the NHRP Mobile NHC Authentication Extension

Compulsory = 1
Type = 10 (proposed)
Length = variable

The NHRP Mobile NHC Authentication Extension is carried in NHRP Registration packets to convey end to end authentication Information. This extension is defined in contrast to the NHRP Authentication Extension defined in [1] which has hop by hop semantics.

This new extension is used when a mobile NHC initially connects to an NHS which is not one of its serving NHSs and the mobile NHC and nonserving NHS are not in a security relationship. The mobile NHC does this in order to send an NHRP Registration Request, via normal routing and forwarding processes, to one of its serving NHSs with which it does have a security relationship. As defined in [1], a serving NHS is an NHS in the NHC's home LIS with which the NHC will register. Upon receiving such an NHRP Registration Request, the serving NHS will do the following: authenticate the sender NHC, set up a VC to the NHC, and then send an NHRP Resolution Reply in response on that new VC.

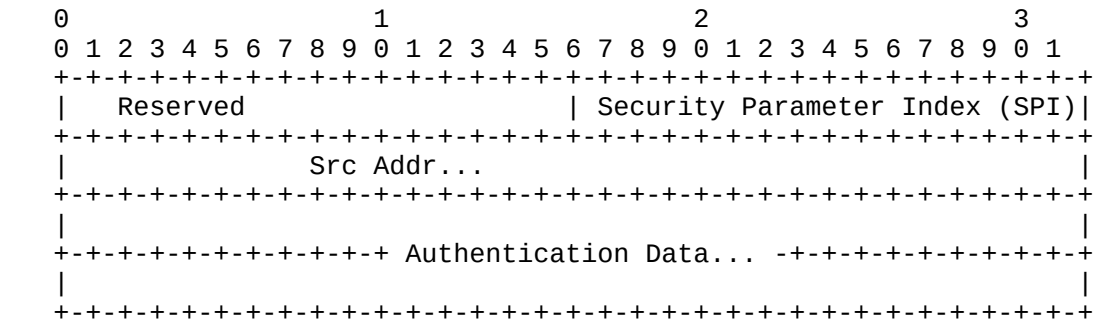
Note that, as defined in [1], a transit NHS (such as the one to which the mobile NHC initially connects) must ignore an extension which it does not understand and that an NHS must not change the order of extensions in an NHRP packet. Thus, the end to end semantics of this extension are preserved without causing changes to existing implementations.

If a serving NHS receives a packet which fails the hop by hop authentication test defined in [1] then the NHS MUST generate an Error Indication of type 'Authentication Failure' and discard the packet. However in the case where the NHRP Mobile NHC Authentication Extension is used as described above, sending an Error Indication is not possible since no route exists back toward the mobile NHC assuming a VC does not already exist between the mobile NHC and the

serving NHS which received the NHRP Registration Request. In this case, the NHRP Registration Request is merely dropped.

2.1 Header Format

The authentication header has the following format:



Security Parameter Index (SPI) can be thought of as an index into a table that maintains the keys and other information such as a hash algorithm. Src and Dst communicate either offline using manual keying or online using a key management protocol to populate this table. The sending NHRP entity always allocates the SPI and the parameters associated with it.

The Src Addr field is a variable length field which contains the address assigned to the outgoing interface. The length of the field is obtained from the source protocol length field in the mandatory part of the NHRP header. The tuple <spi, src addr> uniquely identifies the key and the other parameters that are used in authentication.

The length of the authentication data field is dependent on the hash algorithm used. The Authentication Data field contains the keyed hash calculated over the following fields: fixed part (with hop count, packet size and checksum being treated as if set to zero), mandatory part, and extensions up to and including the Mobile NHC Authentication extension.

Note that [1] defines an explicit ordering of extensions such that:

(a) If the Responder Address extension exists then it must appear before the Authentication Extension.

(b) Any extensions that may be modified in transit (e.g., Forward Transit Extension, Hop by Hop Authentication Extension) must appear after the Mobile NHC Authentication Extension.

2.2 SPI and Security Parameters Negotiation

SPI's can be negotiated either manually or using an Internet Key Management protocol. Manual keying MUST be supported. The following parameters are associated with the tuple <SPI, src>- lifetime, Algorithm, Key. Lifetime indicates the duration in seconds for which the key is valid. In case of manual keying, this duration can be infinite. Also, in order to better support manual keying, there may be multiple tuples active at the same time (Dst being the same).

Algorithm specifies the hash algorithm agreed upon by the two entities. HMAC-MD5-128 [2] is the default algorithm and MUST be implemented. Other algorithms MAY be supported by defining new values. IANA will assign the numbers to identify the algorithm being used as described in [1].

Any Internet standard key management protocol MAY so be used to negotiate the SPI and parameters.

2.3 Message Processing

Unauthenticated 'Mobile' Registration Request processing proceeds as follows [1]:

- the NHC inserts the internetwork address of a serving NHS in the 'Destination Protocol Address' field; If the NHS address is unknown, then the NHC inserts its own internetwork address. A ' responder address' extension is optionally added.
- the non-serving NHS forwards the packet along the routed path based on the contents of the 'Destination Protocol Address' field.
- the serving NHS which receives the NHRP Registration Request will set up a direct VCC to NHC after authenticating the request
- the serving NHS will then send the NHRP Registration Reply back to the NHC on that new VCC. Note that the NHS MUST wait some configured interval before doing this reply in order to prevent a race condition from occurring between the VC setup and sending the NHRP reply packet.
- the NHC will subsequently send all NHRP traffic to the serving NHS on the direct VCC.

When the NHC adds the authentication extension header, it performs a table look up in order to fetch the SPI and the security parameters based on the outgoing interface address. If there are no entries in the table and if there is support for key management, the NHC initiates the key management protocol to fetch the necessary parameters. The NHC constructs the Authentication Extension payload and calculates the hash by zeroing out the authentication data field. The result is placed in the authentication data field. The src address field in the payload is the internetwork address assigned to the outgoing interface.

If key management is not supported and authentication is mandatory, the packet is dropped and this information is logged.

On the receiving end, the serving NHS fetches the parameters based on the SPI and the internetwork address in the authentication extension payload. The authentication data field is extracted before being zeroed out in order to calculate the hash. It computes the hash on the entire payload and if the hash does not match, then an "abnormal event" has occurred.

The keys used by the mobile NHC for communicating with the serving NHS in NHRP Registration Requests can be used in subsequent resolution and purge requests made directly to the serving NHS after receiving the NHRP Registration Reply. However, the authentication extension defined in [1] MUST be used when these keys are applied to resolution and purge packets.

Hop by Hop Authentication[1] and End to End authentication MAY be used in combination to provide protection against both spoofing and denial of service attacks. If only an end-to-end Mobile NHC Authentication Extension is present, it MAY be the policy of each transit NHS to reject the NHRP Registration Request based on the requirement for having a Hop by Hop authentication present. Such a requirement is a local matter.

2.4 Security Considerations

It is important that the keys chosen are strong since the security of the entire system depends on the keys being chosen properly.

End-to-end authentication counters spoofing attacks on the home subnet through not relying on the potentially compromised chain of trust. The use of end-end authentication is further described in [3].

Hop-by-hop authentication prevents denial of service attacks by introducing access control at the first point of contact to the NHRP infrastructure.

The security of this extension is performed on an end to end basis. The data received can be trusted only so much as one trusts the end point entities in the path traversed. A chain of trust is established amongst NHRP entities in the path of the NHRP Message. If the security in an NHRP entity is compromised, then security in the entire NHRP domain is compromised.

Data integrity covers the entire NHRP payload up to and including the Mobile NHC Authentication Extension. This guarantees that the data and extensions covered by this authentication hash were not modified and that the source is authenticated as well. If the authentication extension is not used or if the security is compromised, then NHRP entities are liable to both spoofing attacks, active attacks, and passive attacks.

There is no mechanism to encrypt the messages. It is assumed that a standard layer 3 confidentiality mechanism will be used to encrypt and decrypt messages. It is recommended to use an Internet standard key management protocol to negotiate the keys between the neighbors. Transmitting the keys in clear text, if other methods of negotiation is used, compromises the security completely.

References

[1] Luciani, J., Katz, D., Piscitello, D., Cole, B. and N. Doraswamy, "NBMA Next Hop Resolution Protocol (NHRP)", RFC 2332, April 1998.

[2] Krawczyk, H., Bellare, M. and R. Canetti, "HMAC: Keyed Hashing for Message Authentication", RFC 2104, February 1997.

[3] Perkins, C., "IP Mobility Support", RFC 2002, October 1996.

[4] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

Authors' Addresses

James V. Luciani
Nortel Networks
3 Federal Street
Mail Stop: BL3-03
Billerica, MA 01821

Phone: +1 978 916 4734
EMail: luciani@baynetworks.com

Hiroshi Suzuki
Cisco Systems
170 West Tasman Dr.
San Jose, CA 96134

Phone: +1 408 525 6006
EMail: hsuzuki@cisco.com

Naganand Doraswamy
Nortel Networks
3 Federal Street
Mail Stop: BL3-03
Billerica, MA 01821

Phone: +1 978 916 4734
EMail: naganand@baynetworks.com

David Horton
CiTR PTY Ltd
Level 2 North Tower
339 Coronation Drive
Milton, Australia 4064

Phone: +61 7 32592222
EMail: d.horton@citr.com.au

Full Copyright Statement