Network Working Group
Internet Draft
Expire in six months

Luis A. Sanchez
Gregory D. Troxel
BBN Technologies
November 21, 1997

Rapid Authentication for Mobile IP

<draft-ietf-mobileip-ra-00.txt>

Status of This Memo

Abstract

This document describes a mechanism that provides Mobile IP nodes and agents with the necessary keys and information needed to establish mobility security associations within a foreign network. This mechanism aims at reducing the latency and computational burden introduced by public-key based key management protocols in network topologies where visiting mobile nodes register with their respective home agents several times through different foreign agents requiring Mobile-Foreign Authentication. This mechanism employs a key distribution center capable of generating the security contexts needed to authenticate Mobile IP control messages. This mechanism, designed as an extension to the Mobile IP protocol, preservs backward compatibility and interoperability with RFC2002 compliant implementations of Mobile IP.

Table of Contents

1.0 Introduction
    1.1 Requirements Terminology
    1.2 Technical Definitions
2.0 Rapid Authentication Overview
3.0 Conventional Mobility Security Association (CMSA)
4.0 Rapid Authentication Extensions for Mobile IP
    4.1 Authentication Extensions
    4.2 Agent Advertisement Extension
5.0 Rapid Authentication Control Messages for Mobile IP
    5.1 Request Message (RA-Req)
    5.2 Reply Message (RA-Rep)
    5.3 Distribution Message (RA-Dist)
    5.4 Distribution Acknowledgment Message (RA-Dist-Ack)
    5.5 Rapid Authentication Message Generation
6.0 Rapid Authentication Payload Processing
    6.1 RA-Req Processing
    6.2 RA-Rep Processing
    6.3 RA-Dist Processing
    6.4 RA-Dist-Ack Processing
7.0 Agent Advertisement Processing
8.0 Performance Considerations
Acknowledgments
References
Disclaimer
Author Information

1.0 Introduction

The Mobile IP protocol as described in RFC2002 relies on control messages transmitted from mobile hosts to establish IP tunnels. These tunnels provide the mechanism needed to redirect traffic addressed to the mobile host using an IP address associated with its current topological location. This new feature would be a security vulnerability if request messages sent by hosts masquerading as authorized hosts were honored without cryptographically verifying the authenticity of such messages. This vulnerability has been identified as a security problem in the Internet today[Bel89]. In order to avoid such security problems, Mobile IP requires that all request messages transmitted by a Mobile Node (MN) to a Home Agent (HA) be authenticated using a message authentication code. The default mechanism uses the keyed-MD5 algorithm [Riv92] in preffix+suffix mode with a key size of 128 bits.

Mobile Node to Home Agent authentication is not the only case where authentication is useful. For instance, an MN might want to verify

that a Foreign Agent (FA) is trustworthy before authenticating a request to the HA to bind the MN's address to the Care-of Address

(COA) given by that particular FA. Another possibility is for the FA to be able to choose to provide or decline service to the MN based upon some policy; the MN must be able to authenticate requests to the FA for this to be possible with authentication-based access control. Another scenario where authentication might be useful is when the FA wishes the HA to authenticate itself to the FA in order to avoid denial-of-service (DoS) attacks by an attacker injecting false binding rejections claiming to be from the HA. In all these cases the use of keyed-MD5 or other MAC algorithms to authenticate registration and reply messages is sufficient to establish the authenticity of the messages exchanged between FAs and MNs.

Mobile IP does not mandate a protocol to establish the security contexts (shared key, authentication algorithm, type of replay protection, etc.) between a pair of nodes. It is the collection of these security contexts that encompases a Mobilility Security Association [Perk96]. Mobile Agents and nodes establish pairwise Mobility Security Associations (MSA) manually using shared secrets previously agreed upon. Manual configurations don't scale, making this authentication scheme a management nightmare even for small size networks. Using a key management protocol such as ISAKMP provides the scalability and flexibility needed when establishing security associations with a performance cost. For example, consider an MN which has been unregistered for a long time contacting a foreign agent in some domain where there are multiple FAs. This will likely require some certificate fetches and public-key operations to validate and perform a key exchange. If the MN has not recently registered with any foreign agents, this is acceptable. However, we would like to avoid this burden when the MN moves to another FA in the same domain. Regardless of the reason for an MSA to be present between an MN and an FA or an FA and an HA, it is desirable for these MSAs to be created quickly for subsequent authentications.

Rapid Authentication (RA) is a mechanism that allows the establishment of Mobility Security Associations between mobile nodes and agents in a particular foreign domain without using any public key operations, generating multiple round trips, or key lookups that leave the foreign domain. Rapid Authentication uses a key exchange approach with symmetric cryptography, to distribute the keying material needed to authenticate Mobile IP control messages among mobility agents and nodes while in a foreign domain. Rapid Authentication is designed to be a compatible extension to the standards-track Mobile IP protocols, so that if a host does not implement RA, interoperability will not be impaired. This document assumes that there is some mechanism for MSA creation between mobility entities and the Key Distribution Center.

In order to understand this document, the reader should be thoroughly familiar with most of RFC2002.

1.1 Requirement Terminology

In this document, the words that are used to define the significance of each particular requirement are usually capitalized. These words are defined in [RFC 2119] and are inlcuded in this document for completeness. These key words are:

- MUST

  This word or the adjective "REQUIRED" means that implementation of the item is an absolute requirement of the specification.

- SHOULD

  This word or the adjective "RECOMMENDED" means that there might exist valid reasons in particular circumstances to not implement this item, but the full implications should be understood and the case carefully weighed before not implementing this or not implementing it in a conforming manner.

- MAY

  This word or the adjective "OPTIONAL" means that implementation of this item is truly optional. One vendor might choose to include the item because particular buyers require it or it enhances the product, while another vendor may omit the same item.

1.2 Technical Definitions

This section provides definition of terms applicable to Rapid Authentication.

Mobility Security Association

> A Mobility Security Association (MSA) denotes the association between a pair of nodes (nodes A and B) by a collection of security contexts comprised of the identities of the nodes, SPI values by which each locates the MSA, authentication algorithm and mode, authentication key, and style of replay protection.

Conventional Mobility Security Association

> A Conventional Mobility Security Association (CMSA) denotes the association between a pair of nodes (nodes A and B) by a collection of security contexts comprised of the identities of the nodes, SPI values by which each locates the CMSA, an authentication algorithm and mode, an encryption algorithm

and mode, an authentication key, an key-encrypting key, a style of replay protection and expiration time.

Rapid Mobility Security Association

A Rapid Mobility Security Association (RMSA) denotes the association between a pair of nodes (nodes A and B) by a collection of security contexts comprised of the identities of the nodes, SPI values by which each locates the RMSA, the identity of the party that functioned as the RKDC, the authentication algorithm and mode, the authentication key, the style of replay protection and the expiration time.

Rapid Key Distribution Center

A host functioning as Key Distribution Center for Rapid Authentication in Mobile IP. RKDCs generate keys, SPIs and other related information required to establish a Mobility Security Association between Mobile Agents and Mobile Nodes. Foreign Agents serve as RKDCs.

2.0 Rapid Authentication Overview

Rapid Authentication (RA) is a mechanism that allows establishment of MSAs between the mobile nodes and agents in a particular foreign domain without using any public key operations, generating multiple round trips, or key lookups that leave the foreign domain. The central idea of Rapid Authentication is to allow Foreign Agents to function as a Kerberos-style [Kohl93] Key Distribution Centers (KDC). These Foreign Agents are capable of creating the security contexts that Mobile Nodes and Agents require in order to generate Mobility Security Associations among themselves. Foreign Agents supporting Rapid Authentication and functioning as key distribution centers are known as Rapid Key Distribution Centers or RKDCs. In order for this mechanism to work, security associations must exist between the RKDC and the Mobile Node requesting Rapid authentication, the RKDC and the Home Agent of the Mobile Node and between the RKDC and the nearby Foreign Agent. These security associations, also known as Conventional Mobile Security Associations (CMSA), include among other security contexts, a key encrypting key and an authentication key. RKDCs use the key encrypting keys to encrypt the authentication keys required by both mobile nodes and agents to authenticate Mobile IP control messages. These security associations could be in place a priori (before a Mobile Node requests Rapid Authentication) or be established as a result of a request message sent from a Mobile Node to an RKDC. CMSAs could be created manually, via ISAKMP/Oakley, ZmKeyGen [MOIPS97] or some other key management mechanism.

Rapid Authentication introduces four new Mobile IP control messages:

1) RA-Req
2) RA-Rep
3) RA-Dist
4) RA-Dist-Ack

All RA control messages follow the same format: a Rapid Authentication header, Rapid Authentication data and an authentication extension. The RA header is common to all messages and it includes among other fields: the home IP address of the Mobile Node requesting RA, the IP address of the target Foreign Agent, the IP address of RKDC and an Identification Field to be used for anti-replay protection. The authentication extensions provide authentication and integrity for the RA control messages exchanged among nodes and agents.

The Rapid Authentication process begins with the RA-Req message. The RA data in this message indicates the authentication algorithm and the length of the key required by the Mobile Node. The RA-Rep messages do not contain RA data. RKDCs use this message to indicate to Mobile Nodes the status of their requests. RKDCs employ RA-Dist messages to distribute the security contexts needed to create MSAs among nodes and agents. These contexts include SPI values, Key Lifetime, Authentication Key, etc. RA-Dist messages are acknowledge by their recipient using the RA-Dist-Ack message. Like the RA-Rep message, the RA-Dist-Ack message does not contain RA data and is used by nodes and agents to indicate RKDCs the status of a particular RA-Dist message received. Rapid Authentication also introduces a new Agent Advertisement extension to provide advertisement of RA support by Foreign Agents. This extension allows Foreign Agents to advertise whether or not they are functioning as RKDCs since it is possible that FAs supporting RA MAY not function as RKDCs for administrative reasons. This extension also allows Foreign Agents to announce the list of RKDCs for which they have valid CMSA enabling Mobile Nodes to request RA with a target Foreign Agent via their common RKDC.

Rapid Authentication operates in two modes: direct and target mode. In direct mode operation, Mobile Nodes have IP connectivity with the RKDC. In target mode operation, Mobile Nodes do not have IP connectivity with RKDCs, only link connectivity. In this mode, Mobile Nodes send RA-Req messages via Foreign Agents for which they have link layer connectivity. Foreign Agents supporting RA forward these request messages to the appropriate RKDC. The basic Rapid Authentication operation is straight forward. Mobile Nodes send RA-Req messages to RKDCs. The request messages come directly from the Mobile Node (direct mode operation) or get forwarded by a Foreign Agent (target mode operation). RKDCs send RA-Rep messages indicating whether or not they can generate the security contexts required for the mobile nodes and

agents to establish MSAs among themselves. In target mode operation, RKDCs send reply messages to the Mobile Nodes via Foreign Agents. RKDCs verify if they have CMSAs established with both the

Mobile Node and the target Foreign Agent. If so established, the RKDC creates SPIs, authentication keys and all other required information. The RKDC encrypts the authentication keys using the default encryption algorithm, DES with 56-bit keys. RKDCs generate RA-Dist messages containing the SPIs, algorithm information, authentication keys, etc. and transmit them to the mobile nodes and agents. All nodes and agents receive one message containing the SPI values that they will use to identify the MSAs. Since the MSAs are simplex, each nodes receives two SPIs, one for outgoing and one for incoming traffic for that communication. Foreign Agents however, receive two sets of SPI values (a total of four); two for identifying the MSA between the Foreign Agent and the Home Agent and two for identifying the MSA between the Foreign Agent and the Mobile Node. Once both the mobile nodes and agents receive the RA-Dist messages and the mobility security associations are established, they reply to the RKDCs by transmitting RA-Dist-Ack messages indicating the status of the transaction. Upon reception of a RA-Dist-Ack message reporting good status, RKDCs destroy all keying information and clear all states.

3.0 CMSA Generation

We will assume that two FAs are capable of creating a security association with each other for use in the Rapid Mobility protocol. This association, known as a CMSA, includes an authentication key, a key-encrypting key, type of replay protection, encryption and authentication algorithm identifiers, SPI values and expiration times. CMSAs could be created manually, via ISAKMP/Oakley, ZmKeyGen [MOIPS97] or some other mechanism. The KEK is used to encrypt the keying material generated at the RKDCs before is sent to the final destination. The destination uses the corresponding KEK to decrypt the keying material. A possible scheme for generating CMSAs will be defined in a separate document.

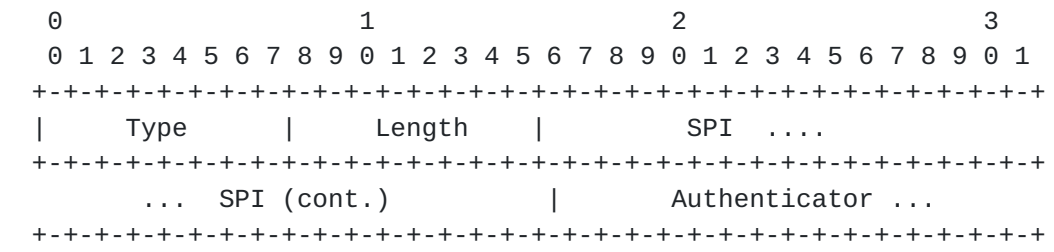
4.0 New Mobile IP Extensions

4.1 Authentication Extensions

RA introduces three new Mobile IP extensions to provide authentication to control messages exchanged between mobile nodes and agents with RKDCs as specified below.

Type Value	Authentication Extension
129	Mobile-RKDC Authentication
130	Foreign-RKDC Authentication Extension
131	Home-RKDC Authentication Extension

These extensions follow the same format used in other Mobile IP authentication extensions. The extension format is depicted below for reference.

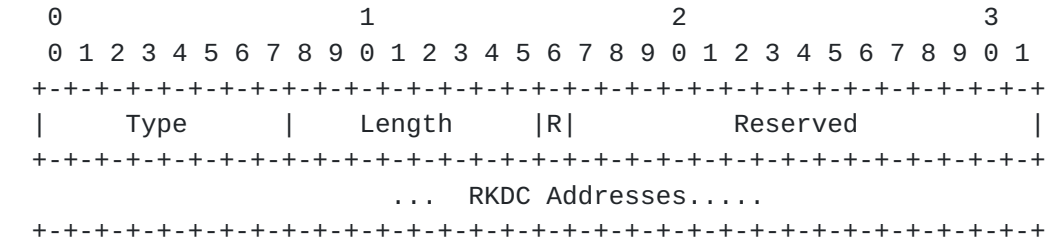


Type	129,130,or 131.
Length	4-octets plus the number of octets in the Authenticator.
SPI	Security Parameter Index is a 4-octet field with an arbitrary value that combined with a destination IP address identifies a security association.
Authenticator	This is a variable length field that depends upon the algorithm used. Default authentication algorithm is keyed-MD5 in prefix+suffix mode. This algorithm produces a 16-octet value.

The Mobile-RKDC Authentication Extension MUST be present in all RA control messages exchanged between Mobile Nodes and RKDCs. The Foreign-RKDC Authentication Extension MUST be present in all RA control messages exchanged between Foreign Agents and RKDCs. The Home-RKDC Authentication Extension MUST be present in all RA control messages exchanged between RKDCs and HAs.

4.2 Agent Advertisement Extensions

RA also introduces one new Mobile IP extension to provide advertisement of RA support by FAs. The RA Advertisement Extension follows the exact same format used in other Mobile IP extensions. The extension format is depicted below.



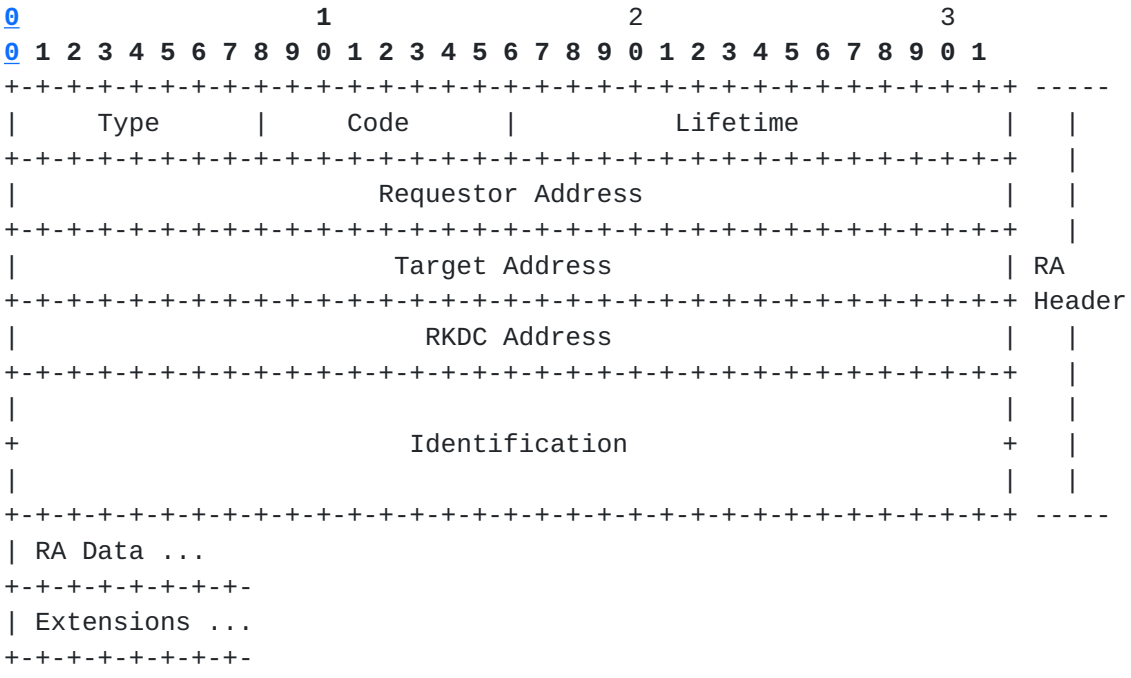
Type 132

Length	2-octets plus 4*N where N is the number of RKDC addresses.
R	Indicates whether or not this FA functions as an RKDC.
Reserved	Available for future use and expansion. This field is sent as zero and ignored at the receiving end.
RKDC Address	A variable length field containing the IP address(es) of other RKDCs for which this FA has a CMSA.

FAs supporting RA SHOULD append this extension to their agent advertisement. The R bit is set to 1 to indicate that the FAs sending this advertisement are also functioning as RKDCs. This extension enables MNs to request RA with the Target via their common RKDC. This extension can only be used with ICMP router discovery messages. Note that an MN MAY request RA with a Target even if they don't share a common RKDC.

5.0 Rapid Authentication Control Message Format

RA defines a set of new control messages with the following format:



Type

A 1-octet field indicating the RA control message type. See below for a list of currently defined code values.

Type Value	Message Type
04	RA-Req
05	RA-Rep
06	RA-Dist
07	RA-Dist-Ack

Code

A value indicating specific control information for each RA message.

Lifetime

A 2-octet field indicating the number of seconds remaining before the association is considered expired. A value of 0xffff indicates infinity.

Requestor Address

The home address of the MN requesting RA. Only MNs MAY request RA.

Target Address

A 4-octet field containing the IP address of the Foreign Agent that the MN wishes to establish a RMSA with.

RKDC Address

A 4-octet field containing the IP address of the host acting as RKDC for a particular RMSA.

Identification

This 8-octet field contains a random value (nonce) or a timestamp used for protecting against replay attacks. This field is similar to the identification field found in Mobile IP Registration messages. See section 9.0 for a detailed a description.

RA Data

The RA data is of variable length and depends on the RA message type.

Extensions

Any of the following Mobile IP control message extensions may appear in RA control messages:

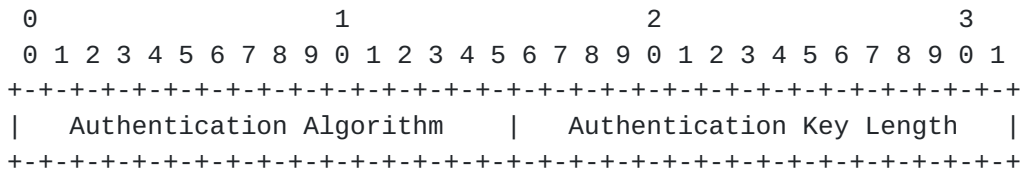
Extension Number	Extension Type
129	Mobile-RKDC Authentication
130	Foreign-RKDC Authentication
131	Home-RKDC Authentication

5.1 Request Message (RA-Req)

The RA-Req message is comprised of the RA header, RA data and appropriate extension. The RA-Req type value is 04. The following values are defined for use within the code field:

Code Field	Request Type
01	Direct Mode Request
02	Target Mode Request

The RA data for the RA-Req message includes a 4-octet field containing the requestor's key information required by the RKDC to generate the appropriate keying material. This information includes the authentication algorithms requested and the size of authentication key as specified below.



Authentication Algorithm

This 2-octet field indicates a specific algorithm. The value 1 indicates MD5 as per RFC2002. All hosts implementing RA MUST implement this algorithm. Values from 64000-64999 are reserved for private use, and values 65000-65535 are experimental.

Authentication Key Length

This 2-octet field specifies the size in bits of the authentication key the requestor is asking the RKDC to

generate. A value of 0 means "do not generate key."

5.2 Reply Message (RA-Rep)

The RA-Rep message is comprised of the RA header and appropriate authentication extension. Reply messages DO NOT contain RA Data. The RA-Rep type value is 05. The following values are defined for use within the code field:

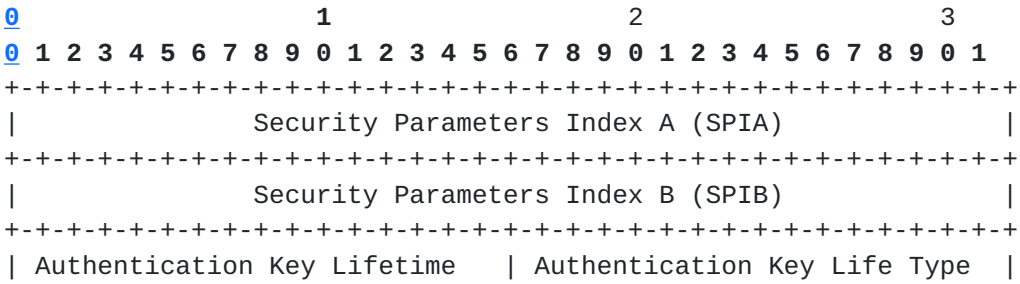
Code Field	Action Type
01	request accepted
02	denied, no CMSA with target
03	denied, administratively prohibited
04	denied, insufficient resources
05	denied, failed authentication
06	denied, requested Lifetime too long
07	denied, reason unspecified
08	denied, request mode mismatch
09	denied, identification field mismatch

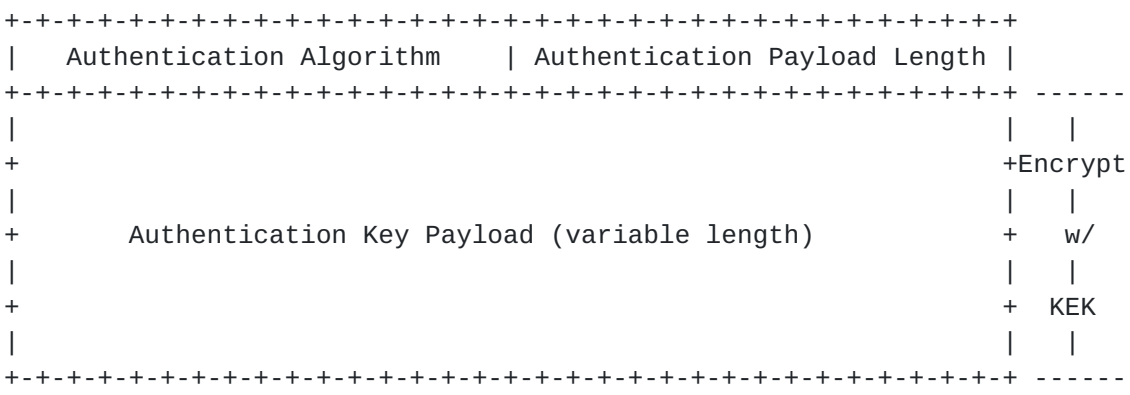
5.3 Distribution Message (RA-Dist)

The RA-Dist message is comprised of the RA header, RA data and appropriate authentication extension. The RA-Dist type value is 06. **The following values are defined for use within the code field:**

Code Field	Action Type
01	Direct Mode Distribution
02	Target Mode Distribution

The RA data has the following format:





SPIA

The Security Parameter Index A is a 4-octet field with an arbitrary value that identifies either the security association between the target and the requestor, the target and the requestor's home agent or the home agent and the requestor, as specified by the code field.

SPIB

The Security Parameter Index B is a 4-octet field with an arbitrary value that identifies either the security association between the requestor and the target, the requestor's home agent and the target or the requestor and the home agent, as specified by the code field.

Authentication Key Lifetime

A 2-octet field that specifies the time to live of this key. The value could be in units of seconds or kilobytes.

Authentication Key Life Type

A 2-octet field that indicates if the Authentication Key Lifetime field is in units of seconds (value= 0x0001) or kilobytes(value= 0x0002)

Authentication Algorithm

This 2-octet field that indicates the authentication algorithm in used. Default algorithm is keyed-MD5 in "prefix+suffix" mode. The code value is 0x0001.

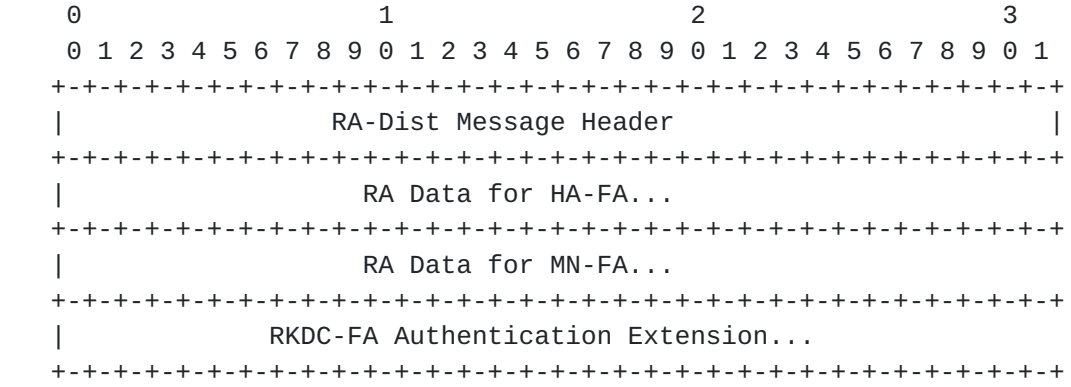
Authentication Payload Length

A 2-octet field that specifies in octets the length of the Authentication Key Payload field.

Authentication Key Payload

A variable length field containing the key to be used to authenticate Mobile IP messages exchanged between mobile nodes and mobile agents. This field includes Initialization Vectors(IVs), required padding and is encrypted with the appropriate Key Encryption Key (KEK) using the encryption algorithm negotiated during the establishment of the CMSA. The default encryption algorithm is DES with 56 bit keys. The value in the Authentication Payload Length field indicates the length of this field.

RA-Dist messages for FAs contain the RA header, two RA data sets and the appropriate authentication extension. They differ from RA-Dist messages destined to MNs or HAs in that instead of containing one RA Data set, these messages carry two sets of RA data. One RA data set is for configuring the mobility security association between the home agent and the foreign agent and the other is for configuring the mobile security association between the mobile node and the foreign agent. The RA-Dist message for FAs has the following format:



In RA-Dist messages destined for FAs, the RA Data format for both

HA-FA and MN-FA mobility security associations follows the general RA Data format specified earlier in this section. The authentication key payload in both RA data sets is encrypted with the same KEK. The CMSA between the RKDC and the FA specifies the appropriate KEK to be used to encrypt the payload. The RA-Dist message format for FA is the same regardless of whether the RA-Req message is in direct or target mode.

5.4 Distribution Acknowledgment Message (RA-Dist-Ack)

The RA-Dist-Ack message is comprised of the RA header and appropriate authentication extension. Distribution messages DO NOT contain RA Data. The RA-Dist-Ack type value is 07. The following values are defined for use within the code field:

Code Field	Action Type
01	Received Direct Mode Distribution Message
02	Received Target Mode Distribution Message
03	denied, identification field mismatch
04	Encryption Failure
05	Invalid SPI
06	Authentication Failure

5.5 Rapid Authentication Message Generation

Mobile Nodes holding a valid CMSA with at least one RKDC MAY send RA-Req messages. A Mobile Node supporting RA SHOULD request RA with a particular FA upon receipt of an agent advertisement from that FA or

loss of binding with the original FA combined with agent advertisement from a new FA. In both cases, the foreign agent advertisement received at the MN MUST have the RA Advertisement extension in order for a Mobile Node to request RA. The extension indicates support for RA. See section 4.2 for details about RA advertisements.

FAs MAY forward RA-Rep messages to MNs. However, only RKDCs MAY send RA-Rep messages. RKDCs MUST respond to all RA-Req messages by sending a RA-Rep with the appropriate code field. Only RKDCs MAY send RA-Dist messages. In response to each valid RA-Req message the RKDC sends a RA-Rep message to the requestor (MN), creates RMSAs for those entities for which it has CMSAs with and, transmits RA-Dist messages to the agents and nodes.

RKDCs transmit three RA-Dist messages; one to the MN, one to the HA

and one to the FA. The RA-Dist messages for the MNs and HAs contain only one RA data set per message. However, the RA-Dist messages for FA contain two RA data sets per message. One RA data set for the HA-FA mobility security association and one for the MN-FA mobility security association. Section 5.3 specifies the format for the RA-Dist messages destined to foreign agents.

Mobile Nodes and Agents MAY send RA-Dist-Ack messages. FAs SHOULD forward RA-Dist-Ack messages to MNs. MNs, FAs and HAs MUST respond to all RA-Dist messages addressed to them by sending a RA-Dist-Ack with the appropriate code field.

6.0 Rapid Authentication Payload Processing

For RA-Req or RA-Dist control messages, the transmitting entity MUST do the following:

1. **Set a timer and initialize a retry counter.**
2. **If an RA-Rep or RA-Dist-Ack message corresponding to the appropriate RA-Req or RA-Dist message is received within the time** interval or before the RETRY LIMIT is reached, the transmitting entity continues normal operation.
3. **If an RA-Rep or RA-Dist-Ack message corresponding to the appropriate RA-Req or RA-Dist message is not received within a** time interval, the control message is resent and the retry counter is decremented.
4. **If the retry counter reaches zero (0) (i.e.** RETRY LIMIT is set) the event should be logged in the appropriate system audit file.
5. **At this point, Mobile Nodes transmitting RA-Req messages will clear RA state for this peer and fall back to conventional** authentication setup using ISAKMP/Oakley or the MOIPS ZmKeyGen. RKDCs transmitting RA-Dist messages will clear RA state for the pending RMSA (and therefore take no further action unless another message is received).

6.1 RA-Req Processing

When creating a RA-Req message, the MN MUST do the following:

1. **Set the value of the type field to 04**
2. **Determine the appropriate code field**
   a) **Set the value of the code field to 01 if the RKDC is the current** FA (direct mode)

b) Set the value of the code field to 02 otherwise. The MN sends the RMSA request to the target FA which in turn forwards the request to the RKDC (target mode)

3. **Set the association lifetime**
4. **Set the Requestor Address to IP home address of the MN**
5. **Set the Target Address to the FA's IP address found in the care of address field of the agent advertisement message**
6. **Set the RKDC Address.** The MN SHOULD have a valid CMSA with this RKDC.
7. **Place the identification value used for anti-replay attack protection**
8. **Construct the RA data payload**
9. **Calculate an integrity check value over the RA header, RA data, and the type, length and SPI fields of the authentication** extension using the authentication key created during the establishment of the CMSA with that RKDC

When an FA receives a RA-Req message it MUST do the following:

1) Check the code field.

If the value is 01 (Direct Mode Request) then:
a) Check the RKDC field
b) If the FA is the intended RKDC, it verifies the MN-RKDC authenticator.
If validation succeeds:
- check identification field for anti-replay protection. If a replayed message is detected:
- discard message
- send RA-Rep message with with appropriate code field (09)
- the event MAY be logged
If the message is original(not a replayed message):
- the FA sends a reply message with code field 01
- construct and transmit RA Distribution messages as specified in section 6.3
If validation fails:
- the FA sends a reply message with code field 05
- the event MAY be logged
c) If the FA is NOT the intended RKDC the FA sends a reply message with code field 08

If the value is 02 (Target Mode Request) then:
a) Check the RKDC field

b) If the FA is NOT the intended RKDC the FA forwards the RA-Req

to the the address found in the RKDC field

c) If the RKDC field contains the address of the FA, it verifies the MN-RKDC authenticator
   If validation succeeds:
   - check identification field for anti-replay protection. If a replayed message is detected:
     - discard message
     - send RA-Rep message with with appropriate code field(09)
     - the event MAY be logged
   If the message is original(not a replayed message):
   - the FA sends a reply message with code field 01
   - construct and transmit RA Distribution messages as specified in section 6.3
   If validation fails:
   - the FA sends a reply message with code field 05
   - the event MAY be logged

6.2 RA-Rep Processing

When creating a RA-Rep message the transmitting entity MUST do the following:

1. **Set the value of the type field to 05**
2. **Determine the appropriate code field as specified in section 5.2**
3. **Set the values for the Lifetime, Requestor Address, Target Address, and RKDC fields to the values found in the corresponding** RA-Req message
4. **Set the identification value used for anti-replay attack protection**
5. **Calculate an integrity check value over the RA header, RA data, and the type, length and SPI fields of the authentication** extension using the authentication key created during the establishment of the CMSA with that entity
6. **Append the appropriate authentication extension to the reply message**

When an MN receives a RA-Rep message it MUST do the following:

1. **Verify the authenticator**
   If validation fails:
   - the message is silently discarded and the event MAY be logged
2. **Check identification field for AR protection.** If a replayed message is detected it is silently discarded and the event MAY be logged
3. **Read the code field and proceed accordingly**

When an FA receives a RA-Rep message it MUST forward the message to the address found in the requestor field.

6.3 RA-Dist Processing

When creating a RA-Dist message the RKDC MUST do the following:

1. **Set the value of the type field to 06**
2. **Set the code field**
3. **Set the association lifetime**
4. **Set the values for the Requestor Address, Target Address, and RKDC fields to the values found in the corresponding RA-Rep** message
5. **Place the identification value used for anti-replay attack protection**
6. **Construct the RA data sets following the steps specified below:**
   a) Generate 2 random numbers of 4 octets each to be used as SPIA and SPIB for either MN-FA or FA-HA communication
   b) Generate Keys based on the information provided in the RA-Req message
   A key of size 00 indicates "do not generate key"
   c) Encrypt the keys using the appropriate KEK
   d) Set the authentication payload size
   e) Set keys lifetime and type accordingly
7. **Calculate an integrity check value over the RA header, RA data, and the type, length and SPI fields of the authentication** extension using the authentication key created during the establishment of the CMSA with that entity
8. **Append the appropriate authentication extension to the message**

When MNs or HAs receive a RA-Dist message they MUST do the following:

1. **Verify the authenticator**
   If validation fails:
   - the message is discarded and the event MAY be logged
   - send an RA-Dist-Ack message with error code 06
2. **Check identification field for anti-replay protection.** If a replayed message is detected:
   - discard message
   - send RA-Rep message with with appropriate code field (03)
   - the event MAY be logged
3. **Read the Authentication Payload Length field.** Note that if the the payload fields equals 0 then no keys were created for that RMSA
4. **Decrypt Authentication Keys using the appropriate KEK.**
   a) If decryption fails:
   - send an RA-Dist-Ack message with appropriate code field (04)
   - the event MAY be logged
   b) If decryption succeeds:

- Search the security association data base for a matching SPI value, for the same destination address and security protocol (i.e a matching mobility security association tuple)

If one exists then:
- do not create security association
- send an RA-Dist-Ack message with error code (05)
- the event MAY be logged

If no SPI collision is detected then:
- create a security association for the appropriate target using the SPIs and the MSA attributes in the RA Data.
- send an RA-Dist-Ack message

When an FA receives a RA-Dist message it MUST do the following:

1. **Repeat steps 1 and 2 above**
2. **Read the Authentication Payload Length field for the HA-FA RA data set. Note that if the the payload fields equals 0 then no keys** were created for that RMSA
3. **Decrypt Authentication Keys using the appropriate KEK.**
4. **Read the Authentication Payload Length field for the MN-FA RA data set. Note that if the the payload fields equals 0 then no keys** were created for that RMSA
5. **Decrypt Authentication Keys using the appropriate KEK.**

a) If either decryption failed:
- send an RA-Dist-Ack message with appropriate code field (04)
- the event MAY be logged

b) If both decryptions succeeded:
- For each RMSA, search the security association data base for a matching SPI value, for the same destination address and security protocol (i.e a matching mobility security association tuple).

If one exists then:
- do not create any security association
- send an RA-Dist-Ack message with error code (05)
- the event MAY be logged

If no SPI collision is detected then:
- create both security association for the appropriate targets using the SPIs and the MSA attributes in the RA Data.
- send an RA-Dist-Ack message with appropriate code field

6.4 RA-Dist-Ack Processing

When creating a RA-Dist-Ack message, the transmitting entity MUST do the following:

1. **Set the value of the type field to 07**
2. **Determine the appropriate code field.**
3. **Set the values for the Lifetime, Requestor Address, Target Address, and RKDC fields to the values found in the corresponding** RA-Dist message.

4. **Set the identification value used for anti-replay attack protection**
5. **Calculate an integrity check value over the RA header, RA data, and the type, length and SPI fields of the authentication** extension using the authentication key created during the establishment of the CMSA with that entity.
6. **Append the appropriate authentication extension to the message.**

When an RKDC receives a RA-Dist-Ack message it MUST do the following:

1. **Verify the authenticator**
   - If validation fails the message is silently discarded and the event
     MAY be logged
   - If validation succeeds:

   a) check identification field for AR protection. If a replayed message is detected it is silently discarded and the event MAY be logged

   b) check the code field
      - If the value is 01 or 02 the RKDC destroys all keys corresponding to this particular RA exchange
      - If the value is 05 the RKDC SHOULD generate a new RA-Dist message following the procedure described in section 6.3

When an FA receives a RA-Dist-Ack Rep message it MUST check the RKDC field in the RA header first. If the IP address is different than the FA's address the FA MUST forward the message to that address. If the address is the FA's address then it MUST process the message in the same way RKDCs do.

7.0 Agent Advertisement Processing

When supporting RA, a foreign agent MUST process received Agent Advertisement from other FAs. Upon reception of an agent advertisement with the RA advertisement extension, a foreign agent supporting RA SHOULD establish a CMSA with the RKDCs listed in the extension. If the R bit is set, the foreign agent supporting RA SHOULD establish a CMSA with the foreign agent that sent the RA advertisement since it is serving as an RKDC. It is assumed that FAs are capable of establishing CMSAs manually, using ZmKeyGen, ISAKMP/Oakley or some other mechanism. If the FA does not support RA, Agent Advertisements from other FAs MUST be ignored and the FA MUST continue with regular FA operations as specified in RFC2002.

8.0 Performance Considerations

Requests from an MN to set up a RMSA MUST be authenticated to protect against flooding attacks. In particular, randomness for key generation is a scarce resource. It is important that message loss in the RA protocol not cause authentication failures that should properly be regarded as signs of an attack. It is acceptable for a packet to

arrive with an unknown SA identifier, but not for it to arrive with a known identifier and then fail the authenticity check.

It might be possible for a message to arrive using an RMSA that has not yet been created at the recipient. We discuss a number of strategies to avoid this problem and to deal with it. An RMSA, whether MN-FA or FA-HA, has an expected direction of use, since the first use will be a registration request from the MN. This suggests two strategies. One is that the message from FAi to FAj be sent before the message from FAi to MN, assuming that it will arrive before MN sends a message to FAj. This will almost certainly be true in the absence of loss. The other is to include the message to FAj in the message to MN, so that it may be included in the initial request. Also, it may be both sent and included, so that in most cases it will be processed before the message from MN arrives.

An entity creating an RMSA should cache response messages for a short period of time (perhaps 30 seconds) so they may be resent. This is important both to conserve entropy used in key generation and to ensure that the same response is generated to a subsequent retransmission of the request, raising the likelihood that the requesting pair for the RMSA will have a consistent RMSA.

An MN and an HA should be able to cache multiple associations with RKDCs in multiple trust domains. For example, assume foo.com has 30

FAs in "Corp", 30 FAs in "Research", and 5 each in "Dept-A" through "Dept-Q". As an MN roams, it creates MSAs with the first FA encountered in each domain, and RMSAs with others. Thus, as it switches among FAs, it can encounter FAs from the various trust domains, and still do only RA even though it may be switching from an FA in one domain to an FA in another. An MN (or HA) could use LRU caching with a number of associations or some other strategy.

9.0 Security Considerations

Rapid Authentication uses a Kerberos-style key distribution approach, to distribute the keying material and security contexts required by mobility agents and nodes to generate Mobility Security Associations for the purpose of authenticating Mobile IP control messages while in a foreign domain.

Mobility Security Associations are uniquely identified by an SPI, destination IP address and authentication protocol tuple. RKDCs have no previous knowledge of exiting MSAs at the nodes and agents, therefore making it possible for the RKDCs to generate SPI values that match existing ones for a particular destination IP address and authentication protocol pair. In the event of an SPI collision, either the node or the agent will send an RA-Dist-Ack message to the RKDCs with an invalid SPI error code. Upon reception of an RA-Dist-Ack message with this error code, RKDCs generate new SPI and other security contexts and transmit new RA-Dist messages.

Rapid Authentication protects against denial of service attacks using replayed messages by using either timestamps or nonces. The style of replay protection is negotiated during the establisment of the CMSA. Timestamping is the default anti-replay protection mechanism for Rapid Authentication. Timestamps require clock synchronization between the sender and the receiver. The use of Nonces for replay protection in Rapid Authentication is optional. RKDCs use the high-order bits of the Identification field to insert its nonce value. Mobile nodes and agents use the low-order bit of the identification field. RKDCs reply to mobile nodes using RA-Rep messages. RKDCs copy the low order 32 bits of the Identification field found in the RA-Req message in the Identification field of the reply. Mobile nodes and agents reply to RA-Dist messages sent by RKDCs using RA-Dist-Ack messages. Nodes and agents copy the high order 32 bits of the Identification field found in the RA-Dist message in the identification field of the reply. The value in the Identification field in RA control messages should not repeat for the lifetime of the particular CMSA under which

the RA control messages are being protected.

Acknowledgments

The authors thank Andrea Lobo and Matt Condell for their participation in requirements discussions for Rapid Authentication. Our gratitude to Isidro Castineyra, Matt Condell and Steve Kent for the significant contributions to this document. We thank Dennis Rockwell and Mary Hendrix (INS Corp.) for reviewing this document. We thank John Zao and Steve Kent for their contributions to the early parts of this work.

References

[Bel89] Steven M. Bellovin, "Security Problems in the TCP/IP Protocol Suite", ACM Computer Communications Review, Vol. 19, No. 2, March 1989.

[Riv92] Rivest, R., "The MD5 Message-Digest Algorithm", RFC 1321, April 1992.

[Perk96] Perkins, C., "IP Mobility Support", RFC 2002, October 1996.

[Kohl93] Kohl, J., et.al, "The Kerberos Network Authentication Service (V5), RFC 1510, September 1993.

[MOIPS97] J.Zao, et.al "A Public-Key Based Secure Mobile IP", Submitted to MobiCom 97.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", RFC 2119, March 1997.

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.

Author Information

Luis A. Sanchez
BBN Technologies
GTE Internetworking
10 Moulton Street
Cambridge, MA 02140
USA
Email: lsanchez@ir.bbn.com
Telephone: +1 (617) 873-3351

Gregory D. Troxel
BBN Technologies
GTE Internetworking
10 Moulton Street
Cambridge, MA 02140
USA
Email: gdt@ir.bbn.com
Telephone: +1 (617) 873-2494