BGP-4 MD5 Authentication
<draft-przygienda-bgp-md5-00.txt>

Status of This Memo

   This document is an Internet Draft, and can be found as
   draft-przygienda-bgp-md5-00.txt in any standard internet drafts
   repository. Internet Drafts are working documents of the Internet
   Engineering Task Force (IETF), its Areas, and its Working Groups.
   Note that other groups may also distribute working documents as
   Internet Drafts.

   Internet Drafts are draft documents valid for a maximum of six
   months. Internet Drafts may be updated, replaced, or obsoleted by
   other documents at any time. It is not appropriate to use Internet
   Drafts as reference material, or to cite them other than as a
   ``working draft'' or ``work in progress.''

   Please check the I-D abstract listing contained in each Internet
   Draft directory to learn the current status of this or any other
   Internet Draft.

Abstract

   This memo describes MD5 authentication scheme for BGP-4 routing
   protocol analogous to the one proposed for SNMP Version 2 and RIP-2.
   The mechanism provides greatly enhanced probability for a system
   attacked to detect and ignore messages received. A sequence number
   improves additionally the resistance against replay attacks.

1. Use of Imperatives

   Throughout this document, the words that are used to define the
   significance of particular requirements are capitalized. These words
   are:

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

   MUST NOT This phrase means that the item is an absolute prohibition of
             this specification.

     SHOULD This word or the adjective "RECOMMENDED" means that there may
             exist valid reasons in particular circumstances to ignore
this
             item, but the full implications should be understood and the
case
             carefully weighed before choosing a different course.

SHOULD NOT This phrase means that there may exist valid reasons in
             particular circumstances when the listed behavior is
acceptable
             or even useful, but the full implications should be
understood
             and the case carefully weighed before implementing any
behavior
             described with this label.

        MAY This word or the adjective "OPTIONAL" means that this item is
             truly optional. One vendor may choose to include the item
             because a particular marketplace requires it or because it
             enhances the product, for example; another vendor may omit
the
             same item.

    2. Introduction

        Recent developments in the Internet has introduced a stronger
        need for improved authentication of routing information. RIP-2
        and OSPF provide originally for unauthenticated service and
        clear-text password authentication. Both are not sufficient to
        withstand attacks currently widespread in the Internet. In case
        of disabled authentication only misconfiguration can be detected
        and clear password protections can be intercepted easily by an
        hostile attacker. Recently, both OSPF [Moy97] and RIP-2 [BA97]
(1)
        added additional mechanisms using well-known MD-5 signature
        algorithms [Riv92] that is considered to be secure and fast
enough
        for protection of routing protocol data units [Tou95]. BGP-4
        [RL95, RL97] contains already authentication information marker

in the message header that can be used for a MD5 signature. Its
fixed length however prevents a more generic approach using keyed

_____

1. on which large parts of this document are based

   algorithms generating more than 128 bits long signatures without
   redefining its meaning.

   This memo proposes an authentication algorithm, as was originally
   proposed for SNMP Version 2, augmented by a sequence number. Keyed
   MD5 is chosen here as the authentication algorithm for BGP-4.
   This mechanism will provide a greatly enhanced probability that a
   system being attacked will detect and ignore hostile information.
   This property derives from the fact that only the output of an
   authentication algorithm (e.g., Keyed MD5) rather than the secret
   Authentication Key is transmited. This output is a one-way
   function of a message and a secret Authentication Key. Again, the
   Authentication Key is never sent over the network unencrypted,
   therefore providing protection against passive attacks.

   Protection against forgery or message modification is inherent to
   this scheme. A sequence number is provided that makes a replay
   attack much harder. It is possible to replay a message until
   the sequence number changes. The mechanism does not provide
   confidentiality. The messages are not encrypted. Such a protection
   is provided in other protocols such as PNNIv2 [AF97] or IETF's recent
   work [Atk95] and could be considered in the future.

   Keyed MD5 is being used for OSPF cryptographic authentication
   [Moy97], and is therefore present in routers already, as is some form
   of password management.

3. Method Description

   The method requires three issues to be addressed:

    1. Changed packet formats,

    2. Authentication procedures, and

    3. Management controls.

3.1. OPEN Message Extensions

   The OPEN message in BGP-4 specifies an optional parameter that
   is specifically reserved for authentication purposes. For MD-5
   purposes the authentication code with value 1 MAY be used by an

implementation. In case this authentication code is used, the OPEN
message contains the parameter and it MUST be formatted the following
way:

```
     0                   1                   2                   3
     0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
    +-+-+-+-+-+-+-+-+
    |  Auth. Code   |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    | reserved 0                                                    |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

The meaning of fields specified reads as:

 1. The "Authentication Code" is Keyed Message Digest Algorithm,
    indicated by the value 1.

All other octets are reserved and MUST be set to 0.

[3.2]. Message Header Format

```
     0                   1                   2                   3
     0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |  Auth. Type    |                0x000000                     |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    | Auth Data Len  |                0x000000                     |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    | Sequence Number                                              |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |    Key ID      |                0x000000                     |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |          Length           |     Type      |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

The message header format for the OPEN and subsequent UPDATE and
KEEPALIVE messages MUST have the marker formatted in the following
way:

   1. The "Authentication Type" is Keyed Message Digest Algorithm,
      indicated by the value 1.

   2. An unsigned 8-bit field that contains the length in octets of the
      trailing Authentication Data field. The presence of this field
      permits other algorithms (e.g., Keyed SHA) to be substituted for
      Keyed MD5 if desired.

   3. An unsigned 32 bit sequence number. The sequence number MUST be
      non-decreasing for all messages sent with the same Key ID.

   4. An unsigned 8-bit field that contains the Key Identifier or
      Key-ID. This identifies the key used to create the Authentication
      Data for this BGP-4 message. In implementations supporting more
      than one authentication algorithm, the Key-ID also indicates
      the authentication algorithm in use for this message. A key is
      associated with a session.

   The trailer consists of the Authentication Data, which is the output
   of the Keyed Message Digest Algorithm. When the Authentication
   Algorithm is Keyed MD5, the output data is 16 bytes; during digest
   calculation, this is effectively followed by a pad field and a length
   field as defined by [Riv92].

3.3. UPDATE and KEEPALIVE Message Trailer

   The OPEN and all subsequent UPDATE and KEEPALIVE messages MUST be
   trailed after length padded to 32-bit boundary with the indicated
   length of authentication data.

```
    0                   1                   2                   3
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |  BGP Header
   +  ..............
   |  BGP Data
   +  ..............
   |  Padding to 32-bit boundary with reserved 0 octets
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   +  0xFFFF                         |  0x0001                      |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   /  Authentication Data (var. length; 16 bytes with Keyed MD5)   /
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

In memory, the following trailer is appended by the MD5 algorithm and
treated as though it were part of the message.

```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|               sixteen octets of MD5 "secret"                 |
/                                                              /
|                                                              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| zero or more pad bytes (defined by RFC 1321 when MD5 is used) |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                        64 bit message length MSW             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                        64 bit message length LSW             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

3.4. Message Generation

The BGP-4 packet is created as usual, except that the marker is set
to contain the authentication type (1), the authentication data
length, the sequence number and the Key Identifier.

The value used in the sequence number is arbitrary, but two
suggestions are the time of the message's creation or a simple
message counter.

The BGP-4 Authentication Key is selected by the sender based on the
session. Each key has a lifetime associated with it. No key is ever
used outside its lifetime.

  1. The BGP-4 header's packet length field indicates the standard
     BGP-4 portion of the packet.

  2. The Authentication Data Offset, Key Identifier, and
     Authentication Data size fields are filled in appropriately.

  3. The BGP-4 Authentication Key, which is 16 bytes long when the
     Keyed MD5 algorithm is used, is now appended to the data. For
     all algorithms, the BGP-4 Authentication Key is never longer than
     the output of the algorithm in use.

   4. Trailing pad and length fields are added and the digest
      calculated using the indicated algorithm. When Keyed MD5 is the
      algorithm in use, these are calculated per [Riv92].

   5. The digest is written over the BGP-4 Authentication Key. When
      MD5 is used, this digest will be 16 bytes long.

   The trailing pad is not actually transmitted, as it is entirely
   predictable from the message length and algorithm in use.

3.5. Message Reception

   When the message is received, the process is reversed:

   1. The digest is set aside,

   2. The appropriate algorithm and key are determined from the value
      of the Key Identifier field,

   3. The BGP-4 Authentication Key is written into the appropriate
      number (16 when Keyed MD5 is used) of bytes starting at the
      offset indicated,

   4. Appropriate padding is added as needed, and

   5. A new digest calculated using the indicated algorithm.

   If the calculated digest does not match the received digest,
   the message is discarded and appropriate Authentication failed
   NOTIFICATION sent. The connection is closed subsequently.

   If the sequence number is not zero and smaller than the last received
   one, the message is discarded and appropriate Authentication failed
   NOTIFICATION sent. The connection is closed subsequently.

   A router that has forgotten its current sequence number but remembers
   its key and Key-ID MUST send its next packet with a sequence number
   of zero. This leaves a small opening for a replay attack although
   appropriate procedures can be provided by an implementation to report
   excessive zero key usage. Router vendors are encouraged to provide
   stable storage for keys, key lifetimes, Key-IDs, and the related
   sequence numbers.

Acceptable messages are now truncated to a BGP-4 message itself and
treated normally.

[4](). New UPDATE Message Error Subcode

A new UPDATE Message Error subcode with the value 12 - Authentication
Failure MUST be understood by all implementations supporting keyed
authentication.

[5](). Management Procedures

[5.1](). Key Management Requirements

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

Implementations MUST support the storage of more than one key at
the same time, although it is recognized that only one key will
normally be active on a session. They MUST associate a specific
lifetime (i.e., date/time first valid and date/time no longer valid)
and a key identifier with each key, and MUST support manual key
distribution (e.g., the privileged user manually typing in the
key, key lifetime, and key identifier on the router console). The
lifetime may be infinite. If more than one algorithm is supported,
then the implementation MUST require that the algorithm be specified
for each key at the time the other key information is entered. Keys
that are out of date MAY be deleted at will by the implementation
without requiring human intervention. Manual deletion of active keys
SHOULD also be supported.

It is likely that the IETF will define a standard key management
protocol. It is strongly desirable to use that key management
protocol to distribute BGP-4 Authentication Keys among communicating
BGP-4 implementations. Such a protocol would provide scalability
and significantly reduce the human administrative burden. The Key
ID can be used as a hook between BGP-4 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 BGP-4 implementations

should such a flaw be discovered, integrated key management protocol
techniques were deliberately omitted from this specification.

5.2. Key Management Procedures

As with all security methods using keys, it is necessary to change
the BGP-4 Authentication Key on a regular basis. To maintain routing
stability during such changes, implementations MUST be able to store
and use more than one BGP-4 Authentication Key for a given session at
the same time.

Each key will have its own Key Identifier, which is stored locally.
The combination of the Key Identifier and the session associated with
the message uniquely identifies the Authentication Algorithm and
BGP-4 Authentication Key in use.

The party creating the BGP-4 message will select a valid key from
the set of valid keys for that session. The receiver will use
the Key Identifier and session to determine which key to use for
authentication of the received message. More than one key may be
associated with a session at the same time.

Hence it is possible to have fairly smooth BGP-4 Authentication
Key rollovers without losing legitimate BGP-4 messages because the
stored key is incorrect and without requiring people to change all
the keys at once. To ensure a smooth rollover, each communicating
BGP-4 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 BGP-4 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. The Key-ID in the received message is used to select the
appropriate key for authentication.

5.3. **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 switchover, 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 an session expires,
   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.

6. **Conformance Requirements**

   To conform to this specification, an implementation MUST support
   all of its aspects. The Keyed MD5 authentication algorithm MUST
   be implemented by all conforming implementations. MD5 is defined
   in [Riv92]. 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 implementations MUST support the
   smooth key rollover described under "Key Change Procedures."

   The user documentation provided with the implementation MUST contain
   clear instructions on how to ensure that smooth key rollover occurs.

   Implementations SHOULD support a standard key management protocol
   for secure distribution of BGP-4 Authentication Keys once such a key
   management protocol is standardized by the IETF.

7. Security Consideration

This memo describes and specifies an authentication mechanism for the
BGP-4 routing protocol that is believed to be secure against active
and passive attacks.

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 communicating
BGP-4 implementations. This mechanism also depends on the BGP-4
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 BGP-4
configuration parameters (e.g. routing table, BGP-4 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.

8. Acknowledgements

Large parts of this memo are based or has been taken over from the
RIP-2 MD-5 authentication [BA97].

References

    [AF97] ATM-Forum. Private Network-Network Interface Specification
            Version 2.0. ATM Forum, work in progress, 1997.

    [Atk95] R. Atkinson. IP Encapsulating Security Payload. Internet
            Engineering Task Force, August 1995.

    [BA97] F. Baker and R. Atkinson. RIP-2 MD5 Authentication.
            Internet Engineering Task Force, January 1997.

   [Moy97] J. Moy. OSPFv2, RFC 2178. Internet Engineering Task Force,
           July 1997.

   [Riv92] R. Rivest. The MD5 Message-Digest Algorithm, RFC 1321.
           Internet Engineering Task Force, April 1992.

   [RL95] Y. Rekhter and T. Li. A Border Gateway Protocol 4 (BGP-4),
           RFC 1771. Internet Engineering Task Force, March 1995.

   [RL97] Y. Rekhter and T. Li. A Border Gateway Protocol 4 (BGP-4).
           Internet Draft, 1997.

   [Tou95] J. Touch. Report on MD5 Performance, RFC 1810. Internet
           Engineering Task Force, June 1995.

Authors' Addresses

Tony Przygienda
Bell Labs, Lucent Technologies
101 Crawfords Corner Road
Holmdel, NJ 07733-3030
prz@dnrc.bell-labs.com