OSPF MD5 Authentication
draft-ietf-ospf-md5-02.txt

Fri Oct 14 09:40:36 PDT 1994

Fred Baker
Advanced Computer Communications
fbaker@acc.com

Randall Atkinson
Information Technology Division
Naval Research Laboratory
atkinson@itd.nrl.navy.mil

Status of this Memo

1. Introduction

Growth in the Internet has made us aware of the need for improved
authentication of routing information. OSPF provides two authentication
mechanisms for use in an area: "No Authentication" and "Simple
Password". Both are vulnerable to passive attacks currently widespread
in the Internet. Well-understood security issues exist in routing
protocols [4]. Clear text passwords, currently specified for use with
OSPF, are no longer considered sufficient [5].

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.

We propose that OSPF use an authentication algorithm, as in SNMP Version
2, augmented by a sequence number. MD5 is proposed as the standard
authentication algorithm for OSPF, but the mechanism is intended 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.,
MD5) rather than the secret OSPF Authentication Key. This output is a
one-way function of a message and a secret OSPF Authentication Key.
This OSPF 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 message until the sequence
number changes, but the sequence number makes replay in the long term
less of an issue. 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 MD5 is used in SNMP
Version 2, and is therefore present in routers already, as is some form
of password management. A similar approach has been proposed for
authentication in IP version 6 (IPv6).

_____

2. Implementation Approach

Implementation requires three issues to be addressed:

  (1)   A changed packet format,

  (2)   Authentication procedures, and

  (3)   Management controls.

2.1. OSPF PDU Format

The basic OSPF message format provides for a 24 byte header with an
arbitrary data content. When MD5 is used, the same header and content
are used, except that the eight byte "authentication key" field is
reused to describe a "Keyed Message Digest" trailer. This consists in
five fields:

  (1)   The "Authentication Type" is Keyed Message Digest Algorithm,
         indicated by the value 2.

  (2)   A 16 bit offset from the OSPF header to the MD5 digest (if no
         other trailer fields are ever defined, this value equals the OSPF
         Data Length).

  (3)   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 OSPF message. A key is associated with an
         interface.

  (4)   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., SHA) to be substituted for MD5 if
         desired.

(5)   An unsigned 32 bit non-decreasing sequence number.

The trailer consists of the Authentication Data, which is the output of
the Keyed Message Digest Algorithm. When the Authentication Algorithm
is 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 RFC
1321.

2.2. Processing Algorithm

When the authentication type is "Keyed Message Digest", message
processing is changed in message creation and reception.

```
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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Version #   |    type       |       OSPF Data Length        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         Router ID                             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          Area ID                              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Reserved - Must be Zero     | AuType=Keyed Message Digest Fn|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Reserved - Must be Zero     |   Key ID    | Auth Data Len   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                Sequence Number (non-decreasing)               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
/            (OSPF Data Length-24) bytes Data                   /
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
/ Authentication Data  (var. length; 16 bytes when MD5 is used) /
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

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

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

2.2.1. Message Generation

The OSPF Packet is created as usual, with these exceptions:

  (1)   The OSPF checksum is not calculated, but is set to zero.

  (2)   The authentication type field indicates the Keyed Message Digest
         Algorithm (2).

  (3)   The authentication "password" field is reused to store a packet
         offset to the Authentication Data, a Key Identifier, the
         Authentication Data Length, and a non-decreasing sequence number.

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 OSPF Authentication Key is selected by the sender based on the
outgoing interface. Each key has a lifetime associated with it. No key
is ever used outside its lifetime. If more than one key is currently
alive, then the youngest key (the key whose lifetime most recently
started) SHOULD be used. Since the key's algorithm is an attribute of
the key, stored in the sender and receiver along with it, the Key ID
effectively indicates which authentication algorithm is in use if the

implementation supports more than one authentication algorithm.

   (1)   The OSPF header's packet length field indicates the standard OSPF
          portion of the packet.

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

   (3)   The OSPF Authentication Key, which is 16 bytes long when the MD5
          algorithm is used, is now appended to the data. For all
          algorithms, the OSPF 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 MD5 is the
          algorithm in use, these are calculated per RFC 1321.

   (5)   The digest is written over the OSPF 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.

2.2.2. Message Reception

When the message is received, the process is reversed:

   (1)   The OSPF Checksum is not calculated,

   (2)   The digest is set aside,

   (3)   The appropriate algorithm and key are determined from the value
          of the Key Identifier field,

   (4)   The OSPF Authentication Key is written into the appropriate
          number (16 when MD5 is used) of bytes starting at the offset
          indicated,

   (5)   Appropriate padding is added as needed, and

(6)   A new digest calculated using the indicated algorithm.

If the calculated digest does not match the received digest, the message
is discarded unprocessed. If the neighbor is in a state other than DOWN
or ATTEMPT and the received sequence number is less than the last one
received, the message likewise is discarded unprocessed. The received
sequence number must, of course, be stored by neighbor and zeroed upon a
"neighbor down" event. Acceptable messages are now truncated to "OSPF
Data Length" and treated normally.

3.   Management Procedures

3.1. 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 or fail to afford perfect
forward secrecy.

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 an interface. They MUST associate a specific lifetime (i.e.,

data/time first valid and data/time no longer valid) with each key, the
key identifier, 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 OSPF Authentication Keys among communicating OSPF
implementations. Such a protocol would provide scalability and
significantly reduce the human administrative burden. The Key ID can be
used as a hook between OSPF 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 OSPF implementations should such a flaw be discovered,
integrated key management protocol techniques were deliberately omitted
from this specification.

3.2. Key Management Procedures

As with all security methods using keys, it is necessary to change the
OSPF Authentication Key on a regular basis. To maintain routing
stability during such changes, implementations are required to store and
support the use of more than one OSPF Authentication Key on a given
interface at the same time.

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

As noted above in Section 2.2.1, the party creating the OSPF message
will select a valid key from the set of valid keys for that interface.
The receiver will use the Key Identifier and interface to determine
which key to use for authentication of the received message. More than
one key may be associated with an interface at the same time.

Hence it is possible to have fairly smooth OSPF Authentication Key
rollovers without losing legitimate OSPF 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 OSPF system must

be updated with the new key several minutes before they 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 OSPF
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.

3.3. 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 MAY
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
HELLO interval.

In the event that the last key associated with an interface 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 lfietime is
extended, the key is deleted by network management, or a new key is
configured.

4. Conformance Requirements

To conform to this specification, an implementation MUST support all of
its aspects. The MD5 authentication algorithm defined in RFC-1321 MUST
be implemented by all conforming implementations. A conforming
implementation MAY also support other authentication algorithms such as
NIST's 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 OSPF Authentication Keys once such a key
management protocol is standardized by the IETF.

5. Acknowledgments

This work was done by the OSPF Working Group, of which John Moy is the
Chair. This suggestion was originally made by Christian Huitema on
behalf of the IAB. Jeff Honig (Cornell) and Dennis Ferguson (ANS) built
the first operational prototype, proving out the algorithms. The
authors gladly acknowledge significant inputs from each of these
sources.

6. References

[1]   Moy, John, "OSPF Version 2", RFC 1583, March 1994.

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

[3]   F. Baker, R. Coltun, "OSPF Version 2 Management Information
      Base", RFC 1253, August 1991

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

[5]   N. Haller, R. Atkinson, "Internet Authentication Guidelines",
      RFC-XXXX (already submitted to RFC Editor), September 1994.

7. Security Considerations

This entire memo describes and specifies an authentication mechanism for
the OSPF routing protocol that is believed to be secure against active
and passive attacks. Passive attacks are clearly widespread in the
Internet at present. Protection against active attacks is also needed
even though such attacks are not currently widespread.

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
OSPF implementations. This mechanism also depends on the OSPF

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 OSPF configuration
parameters (e.g. routing table, OSPF Authentication Key) managable 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. Work is underway
within the IETF to specify a standard mechanism for IP-layer encryption.
That mechanism might be used to provide confidentiality for OSPF in the
future. Protection against traffic analysis is also not provided.
Mechanisms such as bulk link encryption might be used when protection
against traffic analysis is required.

The memo is written to address a security consideration in OSPF Version
2 that was raised during the IAB's recent security review [cite RFC
here].

8. Author's Address

     Fred Baker
     Cisco Systems
     519 Lado Drive
     Santa Barbara, California 93111
Phone: (805) 964 8007
Email: fred@cisco.com

     Randall Atkinson
     Information Technology Division
     Naval Research Laboratory
     Washington, DC 20375-5320
Voice: (DSN) 354-8590
Fax: (DSN) 354-7942
Email: atkinson@itd.nrl.navy.mil

DRAFT   OSPF MD5 Authentication   October 1994

Table of Contents