OSPF with Digital Signatures

Status of this Memo

This document is an Internet Draft. 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 valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet Drafts as reference material or to cite them other than as “work in progress”.

To learn the current status of any Internet Draft, please check the 1id-abstracts.txt listing contained in one of the Internet Drafts Shadow Directories on ds.internic.net (US East Coast), venera.isi.edu (US West Coast), munnari.oz.au (Pacific Rim), or nic.nordu.net (Europe).

Abstract

This memo describes the extensions to OSPF required to add digital signature authentication to Link State data. The augmented design is backward compatible with standard OSPF V2 [1]. Routers supporting digital signatures will be able to provide authenticated routing as an IP TOS or by source routing.

1. Introduction

There is a need for greater security in routing protocols. OSPF currently provides "simple password" authentication where the password travels "in the clear", and there is work in progress to provide keyed MD5 authentication for OSPF protocol packets. The simple password authentication is vulnerable because any listener can discover and use the password. MD5 authentication is very useful for protocol packets between neighbors, but does not address authentication of routing data from its source through multiple hops to its eventual destination.
The basic idea of this proposal is to add digital signatures to OSPF LSA data, and to recommend the use of a neighbor-to-neighbor authentication algorithm (like keyed MD5) to protect other protocol exchanges. Link State information will be signed by the originator of that information and the signature will stay with the data in its travels via OSPF flooding. This will provide end-to-end integrity and authentication for LSA data. Routers providing digital signatures will be "authenticated routers", and can be mixed with non-authenticated routers. An application will be able to specify authenticated routing as an IP TOS, and have packets forwarded accordingly.

A digital signature attached to an LSA by the source router provides assurance that the data really does come from the advertising router. It will insure that the data has not been modified in transit. In the case where incorrect routing data is distributed by a faulty router, the signature provides a way to trace the problem to its source.

Digital signatures for OSPF LSAs can be implemented with the following major elements:

1. Add support for a digital signature algorithm in authenticated routers.
2. Support a signed version of all routing information LSAs.
3. Support a new LSA: Router Public Key LSA.
4. Add an IP TOS for Authenticated Routing.
5. Support TOS routing and forwarding in Authenticated Routers.
6. Implement a mechanism for Key Certification and Distribution.
7. A router will need to be configured with, or supplied with:
   - Public Key of Trusted Entity
   - The following can be for the router or per area if needed:
     - Router Private Key
     - Router Public Key, Id and Role certified by a Trusted Entity
     - Signature Algorithm Information (type, parameters)
     - Hash Algorithm Information (type, parameters)
     - Environment flag (authenticated, non-authenticated, mixed)
2. Overview

Authenticated OSPF routers perform all the normal functions of a standard OSPF router. In addition to the standard functionality, an authenticated OSPF router generates signed routing information LSAs, sends a new key information LSA, manages key and signature algorithm information, and verifies signatures received. An authenticated OSPF router must support TOS routing, specifically for TOS=authenticated routing.

Authenticated OSPF routers can send out a signed and an unsigned version of each LSA. The unsigned version is for backward compatibility with non-authenticated routers. The signed LSAs contain the same routing information, and are flooded, aged, and used in routing calculation like unsigned LSAs. There is an environment flag per area that tells the router whether to send signed LSAs, unsigned LSAs, or both. If all routers in an AS are authenticated then only signed LSAs must be sent. If authentication is turned off, then only unsigned LSAs are sent. If authenticated and non-authenticated routers are mixed in an area, then signed and unsigned versions of the same LSAs must be sent out. This design works best if all the routers in an AS are authenticated, but it can still be useful in a mixed environment.

Standard OSPF routers will discard the unfamiliar LSAs containing key and signature data, so, in a mixed environment there will be "islands" of authenticated routers. Authenticated routing will function on each "island", which might be an OSPF area, as follows. Each authenticated router builds an SPF tree for TOS=Authenticated Routing, using metrics from the signed LSAs, and stores the paths that result in the routing table. To take advantage of the routes supplied, an application must set the TOS=Authenticated Routing bit in the IP header, and the IP forwarding code must use the TOS routes from the routing table. Alternatively, source routes could be generated using the TOS routing information. TOS 0 routing will function normally throughout the AS.

3. LSA Processing

The router sends a Router Public Key LSA in the same manner as all other LSAs. This LSA contains the router’s public key and some identifying information that has been certified by a trusted entity. The router public key is used to verify signatures produced by this router. When forming an adjacency or synchronizing databases, the Router Public Key LSAs should be sent/requested before other LSAs. The Router Public Key LSA is sent at intervals like all other LSAs, and it is sent immediately if a router obtains a new key to distribute.
When the router receives a Router Public Key LSA (with a valid signature), it must store the key information for use in verifying signatures from the advertising router. For every authenticated router that this router is in contact with, there may be one or more Router Public Key LSAs stored at any given time. The LSAs are differentiated by the Key Id stored in the Link State Id field of the LSA Header. The current key is defined as the key with the longest time remaining to expiration. A key can be flushed from routing tables by a properly signed MaxAge version of the Router Public Key LSA sent by the originating router (see section on MaxAge). If the Router Public Key LSA ages to MaxAge before the key reaches its expiration time, the key should be retained in the database until it expires or is flushed by the originating router.

When the router builds a routing information LSA, in a mixed environment it must build a signed and an unsigned version of the LSA. The unsigned version of the LSA will be the standard OSPF V2 [1] LSA. All LSAs will have the TOS capable bit set in the OSPF options field. The signed LSAs will have the top bit of the LSA type field set to indicate the presence of a signature, the metrics (if present) will include TOS = Authenticated Routing, and the LSA will have signature information and a signature in it. The signature is computed on the LSA header and data, starting with the Options field and continuing to the end of the message (except in the case of MaxAge LSAs - see section on MaxAge).

When the router receives a routing information LSA, the type field is examined. Unsigned LSAs are handled in the standard OSPF V2 [1] way. When a signed LSA is received, the signature should be verified using the current public key of the advertising router. If there is no key stored for the advertising router, then the signed LSA must be discarded. If the signature verification fails the LSA must be discarded. If the signature verifies, then the signed LSA is stored for use in the routing calculations. The TOS = Authenticated Routing metrics in the signed LSA will be used in the construction of a SPF tree for this TOS, and these routes will be put into the OSPF routing table.

4. LSA formats

4.1. Options field

There is an Options Field in LSAs, Hellos, and Database Description Packets. This field describes the optional capabilities supported by the advertising OSPF router. The TOS bit must be set in the Options field of all LSAs/packets sent by an Authenticated Router.
4.2. LSA Type Field

This proposal requires a new LSA type for the Router Public Key LSA.

The top bit of the LSA Type field will be set to indicate that an LSA is signed. This creates a new signed LSA type for each existing type.

4.3. Router Public Key LSA

This LSA is the vehicle for an authenticated router to provide its public key to other authenticated routers. This public key is what other routers use to verify the signatures created by this router. A Router Public Key LSA will be communicated in the usual database exchange and flooding mechanisms. This LSA contains the Public Key of the advertising router and a certification of that key by a Trusted Entity. Certification is: the (Router Id, Role and Public Key) signed with the Trusted Entity’s private key. This signature can be verified using the Trusted Entity’s public key which must be known to all authenticated routers. The regular period for sending this LSA should be LSRefreshTime. The Router Public Key LSA will also be sent when key management provides a new key for distribution.

```
ROUTER PUBLIC KEY LSA
+------------------------------------+
<p>| LSA Header(standard)               |
| LS AGE      Options    LS Type=X   |
|     Link State Id = Key Id         |
| Advertising Router = Router Id    |
|   LS Sequence Number              |</p>
<table>
<thead>
<tr>
<th>LS Checksum             Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>SigType HashAlgID  Key Size</td>
</tr>
<tr>
<td>Cert Length        Sig Length</td>
</tr>
<tr>
<td>Router Id</td>
</tr>
<tr>
<td>Router Role (R, ABR, ASBR)</td>
</tr>
<tr>
<td>Router Public Key</td>
</tr>
<tr>
<td>Key Expiration Time</td>
</tr>
<tr>
<td>Certification</td>
</tr>
<tr>
<td>Signature</td>
</tr>
</tbody>
</table>
+------------------------------------+
```

The LSA Header is standard as defined in RFC 1583.

LS Type: X for Router Public Key LSA. Top bit set to indicate a signed LSA.

LS ID: Key Id. This is the Identifier of the Router Public Key.
This Id will differentiate between multiple keys supplied by the same router.

Advertising Router: Router’s OSPF Router Id.
Length: total length of the LSA.
Sig Type: Signature algorithm to be used. Identifies the type of the Router Public Key, the Certification, and the Signature. Currently defined values = RSA(1), DSA(2).
HashAlg Id: Identifies the hash algorithm used to hash data prior to signing. Identifies the hash to use with the given key, the hash used to process Router information for the Certification, and that used on this message before signing. Currently defined values = MD5(1), SHA(2)
Key Size: the size in bits of the Router Public Key. (Note: the length in bytes of the Router Public Key field can be computed from the key size.)
Certification Length: the length of the Certification field.
Signature Length: the length of the Signature field.
Router Id: Same OSPF router Id given in the header
Router Role: Router (R=1), Area Border Router (ABR=2), Autonomous System Border Router (ASBR=3).
Router Public Key: A key that can be used by other routers to verify the signatures produced by this router.
Key Expiration Time: The time by which the Router Public Key should be replaced by a newer key value.
Certification: The trusted Server’s signature of the Router Id, Role, Expiration Time and Public Key given above.
Signature: The advertising router signs this message using it’s private key. This signature can be verified using the enclosed certified public key. The signature covers the message starting with the options field when LS Age is not MaxAge. When LS AGE = MaxAge, the signature starts with the Age field. (See the section on MaxAge).

### 4.4. Signed LSA

A signed LSA can be any OSPF LSA with a digital signature attached. The top bit of the LSA Type field is set to indicate the presence of a signature. A signature type and offset follow the LSA header. The metrics in the LSA must include metrics for TOS = Authenticated Routing. The actual signature follows the LSA Data. Signed LSAs are sent via OSPF reliable flooding, like other LSAs.
SIGNED LSA
+------------------------------------+
| LSA Header(standard)               |
| LS AGE      Options     LS Type    |
|             Link State Id           |
| Advertising Router = Router Id     |
|       LS Sequence Number           |
| LS Checksum    Length               |
+------------------------------------+
| SigType HashAlgId  Key Size        |
| Key Id             Sig Offset       |
| ...                  :               |
| / LSA Data          /                |
| ...                  :               |
| | Signature          |                  |
+------------------------------------+

The LSA Header format is standard as defined in RFC 1583.
LS Type: Standard LSA type + the top bit set to indicate the presence of a signature.
Sig Type: Signature algorithm to be used. Currently defined values = RSA(1), DSA(2).
Hash Alg Id: Identifies the hash algorithm used. Currently defined values = MD5(1), SHA(2).
Key Size: the size in bits of the Router Public Key.
Key ID = This is the Identifier of the router public/private key pair. This Id will differentiate between multiple keys supplied by the same router.
Sig Offset: The offset from the front of the header to the start of the signature.
Signature: Digital signature of the signed LSA from the start of the LSA Header Options field (except for MaxAge LSAs - see section on MaxAge) to the end of the LSA data.

5. Processing Max Age

The age field in the OSPF LSA header is used to keep track of how long a given LSA has been in the system. This, along with the sequence number, allows a router to decide which LSAs are current, and allows old or inaccurate LSAs to be flushed from the system. When the age field reaches MaxAge, routers stop using the LSA for routing, and they flood the MaxAge LSA to make sure that all routers stop using this LSA. When a router fails, eventually its LSAs age out of the system in this way. If a router wants to flush its own LSA from the system it can set the age to MaxAge and flood the LSA.
This element of the protocol is difficult to protect using digital signatures. The age field cannot generally be included in the signature, because it must be updated by routers other than the originating router. For the same reason, the age field is not included in the checksum computation. The age field should be protected, because if a faulty router started to age out other router’s LSAs, it would effectively deny service to those other routers.

To protect the age field, the signature should include the age field when, and only when, the age field value is MaxAge. Verification of the signature on a signed LSA should include the age field when, and only when, the age field value is MaxAge.

The processing of MaxAge will also change slightly for authenticated routers. An LSA will be removed from any router’s Link State Database in one of two ways: 1) the router receives a version of the LSA with the age field set to MaxAge, or 2) the LSA incrementally reaches MaxAge while it is stored by the router. A received LSA with the age field set to MaxAge could have been sent by the originating router or by any other router which had aged the LSA to MaxAge in its database. But for authenticated routers, only the MaxAge LSA sent by the originating router would be recognized as valid, as only the originating router can generate a signature covering the age field. A signed LSA with age MaxAge flooded by a router that is not the LSA’s originating router will be ignored by all authenticated routers. In this way, the originating authenticated router can prematurely age an LSA, but other routers cannot. It is also true that a non-originating router’s flooding of signed LSAs that have reached MaxAge in its database will be ignored. If an authenticated router goes down, its signed LSAs will be aged out by each remaining router individually. This will slow database convergence when an authenticated router goes down, but the databases will still converge, and a fairly obvious security hole will be closed.

6. Of Cryptography and Keys

This design relies on Public Key cryptography. The common examples are RSA and DSA, but a specific algorithm is not mandated by this design. There are some good books on the subject [2], but the high level view of how this design uses Public-Key cryptography is as follows:

Each router has a private key that must be secret, and a public key that everyone may know. A signature can be generated with the private key, and verified using the public key. This verification ensures that the data signed has not been altered in transit, and that it was signed by the router having the correct private key. There is a Trusted Entity
somewhere that has a secret private key, and a public key that all routers must know. A router must be configured with its own pair of keys (public and private), and with the public key of the Trusted Entity. It must obtain a copy of its own public key plus some identifying data (id and role), signed by the Trusted entity. The signature by the Trusted Entity is its certification that it has verified, according to autonomous system policy, the binding between the Router ID and the public key.

An authenticated router sends its certified public key in a Router Public Key LSA via OSPF flooding. All authenticated routers receiving this key store it to use in verifying the advertising router’s signatures. The certification can be checked using the Trusted Entity’s public key, which, again, all routers must know.

Each router signs its LSAs by first running a one-way hash algorithm (like MD5 or SHA, not mandated) on the data, and then using its private key to sign the digested data. The signature for an LSA is appended to the LSA.

Periodically, keys will have to be changed, and the new router public keys will have to be certified by the Trusted Entity. A router could generate its new key pair, or could receive them via a key distribution scheme. Certification could be done out-of-band, or via an encrypted exchange of information with the Trusted Entity. Key distribution is beyond the scope of this memo.

Each router must be able to store several keys for each authenticated router in the area and each ASBR. When a new key is distributed by a router, both the new and the old key must be valid for a key-rollover period.

7. Security Considerations

This entire memo is about security considerations.

8. References


9. Author’s Address

Sandra Murphy
Trusted Information Systems
3060 Washington Road
Glenwood, MD 21738
EMail: murphy@tis.com

Madelyn Badger
Trusted Information Systems
3060 Washington Road
Glenwood, MD 21738
EMail: mrb@tis.com
Table of Contents

Status of this Memo .............................................. 1
Abstract .......................................................... 1
1 Introduction ................................................... 1
2 Overview ....................................................... 3
3 LSA Processing .................................................. 3
4 LSA formats .................................................... 4
4.1 Options field .................................................. 4
4.2 LSA Type Field ................................................ 5
4.3 Router Public Key LSA ....................................... 5
4.4 Signed LSA ................................................... 6
5 Processing Max Age .......................................... 7
6 Of Cryptography and Keys ................................... 8
7 Security Considerations ..................................... 9
8 References ................................................... 9
9 Author’s Address .............................................. 10