Network Working Group
INTERNET DRAFT
draft-murphy-ospf-signature-02.txt

Sandra Murphy
Madelyn Badger
Trusted Information Systems
June 1996

OSPF with Digital Signatures

Status of this Memo

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 [3]. Routers supporting digital signatures will be able to use the authenticated routing information as an IP TOS or by source routing.

1. Acknowledgements

The idea of signing routing information is not new. Foremost, of course, there is the design that Radia Perlman reported in her thesis [4] and in her book [5] for signing link state information and for distribution of the public keys used in the signing. IDPR [7] also recommends the use of public key based signatures of link state information. Kumar and Crowcroft [2] discuss the use of secret and public key authentication of inter-domain routing protocols. Finn [1] discusses the use of secret and public key authentication of several

different routing protocols. The design reported here is closest to that reported in [4] and [7]. It should be noted that [4] also presents techniques for protecting the forwarding of data packets, a topic that is not considered here, as we consider it not within the scope of the OSPF working group.

The authors would also like to acknowledge many fruitful discussions with many members of the OSPF working group, particularly Fred Baker of Cisco Systems, Dennis Ferguson of MCI Telecommunications Corp., John Moy of Cascade Communications Corp., and Curtis Villamizar of ANS, Inc.

2. Introduction

It is well recognized that 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 between neighbors. The simple password authentication is vulnerable because any listener can discover and use the password. Keyed MD5 authentication is very useful for protection of protocol packets passed between neighbors, but does not address authentication of routing data from its source to its eventual destination, through routers which may themselves be faulty.

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 all 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 functions:

(1) Support for a digital signature algorithm in authenticated routers.

(2) Support for a signed version of all routing information LSAs

(3) Support for a new LSA: Router Public Key LSA

(4) Addition of an IP TOS for Authenticated Routing.

(5) Support TOS routing and forwarding in Authenticated Routers.

(6) A mechanism for Key Certification and Distribution.

(7) A router will need to be configured with, or supplied with:

Trusted Entity Information Set: (can be one set, or one per supported Signature Algorithm)

Trusted Entity Public Key
Signature Algorithm and Parameters

Router Information Set: (can be one set, or one per attached area and/or per supported Signature Algorithm)

Router Private Key
Router Certified Public Key and Data:

Key Id
Router Id
Router Role
Signature Algorithm and Parameters
Router Public Key

Router Information per attached Area:

Environment flag (authenticated, non-authenticated, mixed)

3. 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.

4. LSA Processing

4.1. Signed LSA

When the router builds a routing information LSA for an area, the environment for that area must be checked. In a mixed environment the router must build a signed and an unsigned version of the LSA. In an authenticated environment only the signed version of the LSA must be sent. In a non-authenticated environment only the unsigned version of the LSA must be sent. The unsigned version of the LSA will be the standard OSPF V2 [3] LSA. 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 a Key Id, Signature and Signature Length 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, with two exceptions. First, an

LSA created with age=MaxAge has a signature that begins with the age field (see section on MaxAge). Second, the LSA Header Checksum is set to zero for the generation of the signature.

When the router receives a routing information LSA, the type field is examined. Unsigned LSAs are handled in the standard OSPF V2 [3] way. When a signed LSA is received, the signature should be verified using the public key of the advertising router having the indicated Key Id. If there is no such key stored for the advertising router, then the signed LSA must be discarded. If the missing key has a Key Id greater than that of the currently stored key, then an LS Request packet should be sent requesting both the missing key and a retransmission of the LSA signed with that key. 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 an SPF tree for this TOS, and these routes will be put into the OSPF routing table.

4.2. Public Key LSA

An authenticated router sends a Router Public Key LSA (PKLSA)in the same manner as all other LSAs. This LSA contains the router's public key and 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 PKLSAs should be sent/requested before other LSAs. The Router PKLSA is sent at intervals like all other LSAs, and it is sent immediately if a router obtains a new key to distribute. A PKLSA is sent via OSPF flooding within an OSPF area. PKLSAs are not summarized outside an area with the exception of the Autonomous System Border Router's PKLSAs which must be flooded wherever AS external LSAs are flooded.

When an authenticated router receives a Router PKLSA it must check both the Trusted Entity certification and the Router's signature. The Signature Algorithm must be the same for both signatures. If either verification fails, for any reason, the PKLSA is discarded. If the PKLSA verifies successfully, it must be stored for use in verifying signed LSAs 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. These PKLSAs are differentiated by Key Id. Each router may have one PKLSA for each Algorithm supported in a given area. The current key is defined as the key with the largest Key Id having the desired Signature Algorithm. 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). A key can also be flushed (superseded) by a correctly certified Router PKLSA giving a larger Key Id and the same Signature Algorithm as a prior PKLSA.

5. LSA formats

5.1. 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.

5.2. LSA Type Field

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

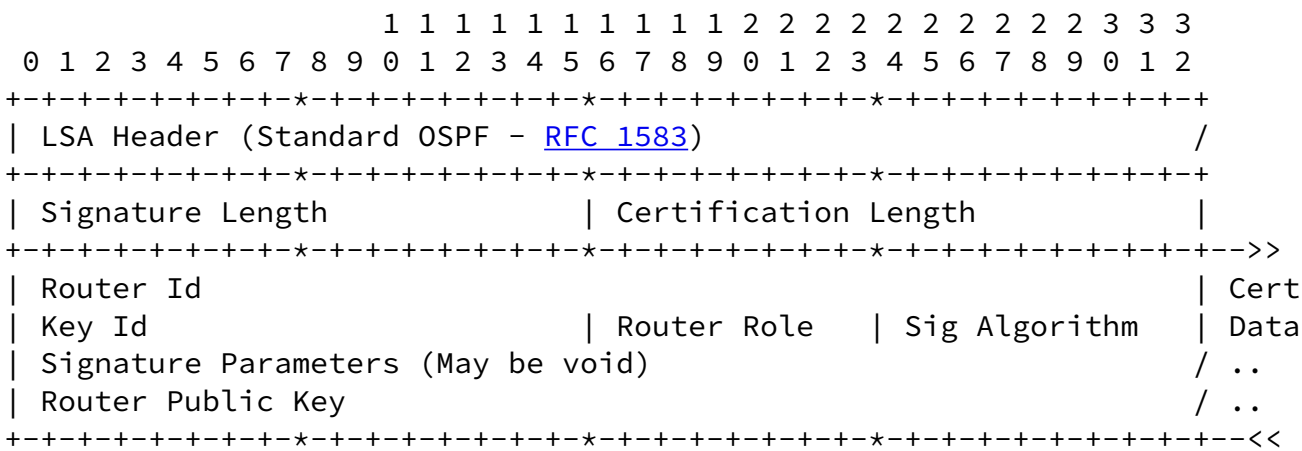
The top bit of the LSA Type field will be set to indicate that an LSA is signed. This creates a new signed LSA type for each existing type.

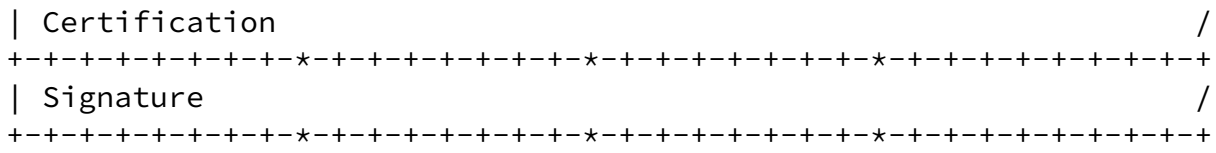
5.3. Router Public Key LSA (PKLSA)

This LSA is the vehicle for an authenticated router to provide a public key to other authenticated routers. This public key is what other routers use to verify the signatures created by this router. A Router PKLSA will be communicated in the usual database exchange and via flooding mechanisms. The regular period for sending this LSA should be LSRefreshTime. The Router PKLSA will also be sent when there is a new key, or a key to be flushed from the system.

This LSA contains the advertising router's public key, identifying information, and a certification of that key and information by a Trusted Entity. The certification is a signature of the key and information created by the Trusted Entity. This certification signature can be verified using the Trusted Entity's public key which must be known to all authenticated routers. If there are multiple signature algorithms and therefore more than one Trusted Entity public key, the signature algorithm for the router public key and the Trusted Entity public key must be the same.

ROUTER PUBLIC KEY LSA





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

Signature Length: the length of the Signature field.
Certification Length: the length of the Certification field.
Router Id: Advertising Router.
Key Id: This is the Identifier of the Router Public Key. This Id will differentiate between multiple keys supplied by the same router.
Rtr Role: Router (R=1), Area Border Router (ABR=2), Autonomous System Border Router (ASBR=3), ABR and ASBR (4).
Sig Algorithm: Signature Algorithm to be used. Identifies the type of the Router Public Key, the Certification, and the Signature. The Signature Algorithm encompasses the hash algorithm used as well. Currently defined value = RSA-MD5(1).
Signature Parameters: These parameters are unique to the given Signature Algorithm. The Signature Parameters for RSA-MD5 are void.
Router Public Key: A key that can be used by other routers to verify the signatures produced by this router. The internal format for the Router Public key is Signature Algorithm dependent. RSA-MD5 given below.

Certification: The Trusted Entity's signature of the certified data.
Signature: The advertising router's signature of this message using the private key identified by the Key Id. This signature can be verified using the enclosed certified public key. The signature covers the LSA header and message starting with the LSA header options field and ending with the Trusted

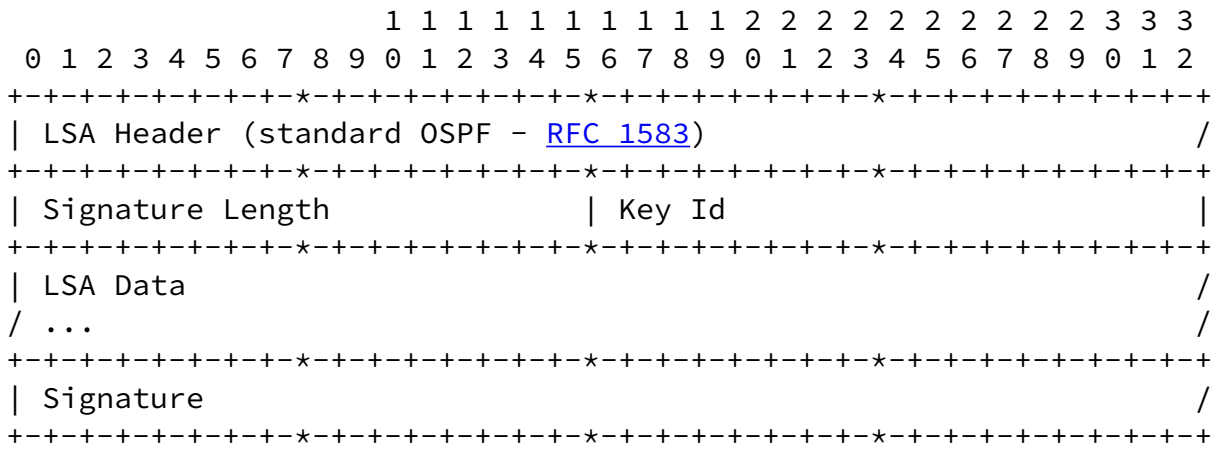
Entity certification field. There are two exceptions to this coverage:

1) If the LSA was generated with an age=MaxAge, then the signature begins with the age field. (See the section on MaxAge).
2) The checksum in the LSA Header is set to zero for the computation of the signature.

5.4. Signed LSA

A signed LSA can be any OSPF LSA with signature data and a digital signature attached. The top bit of the LSA Type field is set to indicate the presence of a signature. A Signature length and Key Id 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



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 Length: The length in bytes of the Signature field.
Key Id: This is the Identifier of the router public/private key

pair used in signing this LSA.

Signature: Digital signature of the signed LSA.
The signature covers the LSA header and data starting with the LSA header options field. There are two exceptions to this coverage:
1) If the LSA was generated with an age=MaxAge, then the signature begins with the age field. (See the section on MaxAge).
2) The checksum in the LSA Header is set to zero for the computation of the signature.

5.5. RSA-MD5 Signature Algorithm

RSA-MD5 is the signature algorithm that all authenticated routers must support. Other algorithms may be supported; their formats will have to be recorded here in future versions of this document.

RSA-MD5 Signature Algorithm

```
    Sig Alg value = 1
    Sig Parms = void
```

For the MD5/RSA algorithm, the signature is as follows

```
   hash = MD5 ( data )

   signature = ( 01 | FF* | 00 | prefix | hash ) ** e (mod n)
```

where MD5 is the message digest algorithm documented in RFC 1321, "|" is concatenation, "e" is the private key exponent of the signer, and "n" is the public modulus of the signer's public key. 01, FF, and 00 are fixed octets of the corresponding hexadecimal value. "prefix" is the ASN.1 BER MD5 algorithm designator prefix specified in PKCS1, that is,
hex 3020300c06082a864886f70d020505000410 [NETSEC].
This prefix is included to make it easier to use RSAREF or similar packages. The FF octet is repeated the maximum number of times such that the value of the quantity being exponentiated is one octet shorter than the value of n.

(The above specifications are Public Key Cryptographic Standard #1 [9].)

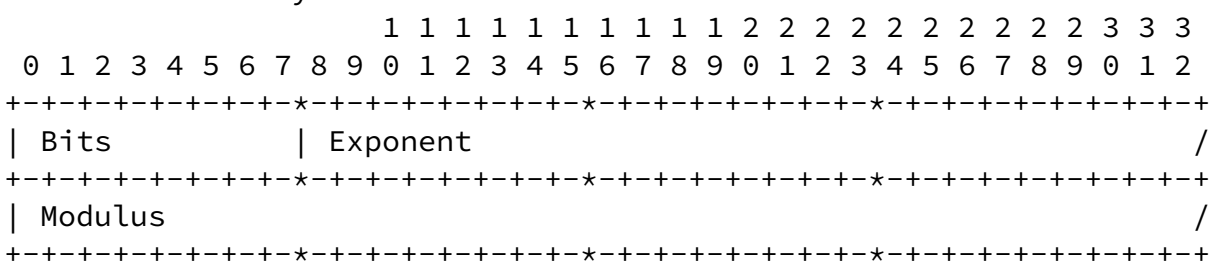
The size of n, including most and least significant bits (which will be 1) SHALL be not less than 512 bits and not more than 2552 bits. n and e

SHOULD be chosen such that the public exponent is small.

Leading zeros bytes are not permitted in the MD5/RSA algorithm signature.

A public exponent of 3 minimizes the effort needed to decode a signature. Use of 3 as the public exponent may be weak for confidentiality uses since, if the same data can be collected encrypted under three different keys with an exponent of 3 then, using the Chinese Remainder Theorem, the original plain text can be easily recovered. This weakness is not significant for OSPF because we seek only authentication, not confidentiality.

Router Public Key for RSA-MD5



Bits: The number of bits in the Exponent
Exponent: RSA public key exponent
Modulus: RSA public key modulus

6. 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.

7. Of Cryptography and Keys

This design relies on Public Key cryptography. The common examples are RSA and DSA. All authenticated routers must support RSA with an MD5 hash as a signature algorithm. There are some good books on the subject of cryptography [6], 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 it's 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 identifying data 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 identifying data (including 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) 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. Original distribution of certified keys 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.

8. Remaining Vulnerabilities

Note that with this mechanism, one router can still distribute incorrect data in the information for which it itself is responsible. Consequently, an autonomous system employing digital signatures with this mechanism will not be completely invulnerable to routing disruptions from a single router. For example, the area border routers and autonomous system border routers will still be able to inject incorrect routing information. Also, any single internal router can be incorrect in the routing information it itself originates about its own links.

8.1. Area Border Routers

Even with the design proposed here, the area border routers can inject incorrect routing information into their attached areas about the backbone and the other areas in Type 3 and 4 LSA's. They can also inject incorrect routing information into the backbone about their attached area.

Because all the area border routers in one area work from the same database of LSA's received in their common area, it would be possible for the area border routers to corroborate each other. Any area border router for an area could double check the Type 3 and 4 LSA's received over the backbone from other ABR's from the area, and could double check the Type 3 and 4 LSA's flooded through the area from the other area border routers. The other routers in the area or backbone should be warned of any check failure. The warning could be a signed message from the area border router detecting the failure flooded in the usual mechanism.

Another possibility would be that the area border routers in an area could originate multiple sets of Type 3 and Type 4 LSA's -- one for itself containing its own information and one for each of the area border routers in the area containing the information each of them should originate. Each router in the area or backbone could then determine for itself whether the area border routers agreed. This distribution of information but coordination of processing is in keeping with the paradigm of link state protocols, where information and processing is duplicated in each router.

The two alternatives mean much additional processing and additional message transmission, over and above the additional processing required for signature generation and verification. Because the vulnerability is isolated to a few points in each area, because the source of incorrect information is detectable (in those situations where the incorrect information is spotted) and because the protection is costly, we have not added this protection to this design.

8.2. Internal Routers

The internal routers can be incorrect about information they themselves originate.

A router could announce an incorrect metric for a valid link. There is no way to guard against this, but the damage would be small and localized even if the router is announcing that the link is up when it is down or vice versa.

A router could announce a connection that does not in fact exist. If a router announces a non-existent connection to a transit network, the OSPF Dijkstra computation will not consider the connection without a similar announcement from another router at the other "end". Therefore, no damage would result (above network impact to transmit and store the incorrect information) without the cooperation of another router. A

router could also announce a connection to a stub network or a host route that does not exist. The Dijkstra computation can not perform the same check for a similar announcement from the other "end", because no other end exists. This is a vulnerability.

A faulty router announcing a nonexistent connection to a stub network or host could result in the faulty router receiving IP packets bound for that network or host. Unless the faulty router then forwarded the packets to the correct destination by source routing, the failure of packet delivery could expose the incorrect routing. To exploit the vulnerability deliberately, the faulty router would have to be able to handle and pass on the received traffic for the incorrectly announced destination. Furthermore, if the incorrect routing were discovered, the signatures on the routing information would identify the faulty router as the source of the incorrect information.

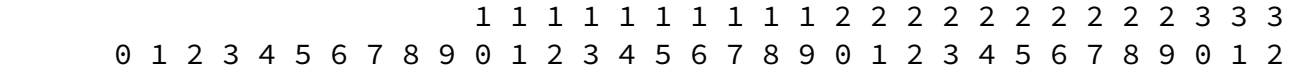
Even so, there may be reason to protect against one faulty router disrupting routing by announcing these unsubstantiated connections. In the worst case, a faulty router could announce nonexistent host routes to a large number of addresses in the area or autonomous system. (Note that announcing a large number of incorrect routes would raise the probability that the incorrect routing would be detected, leading to detection of the faulty router as the source of the error.) To guard

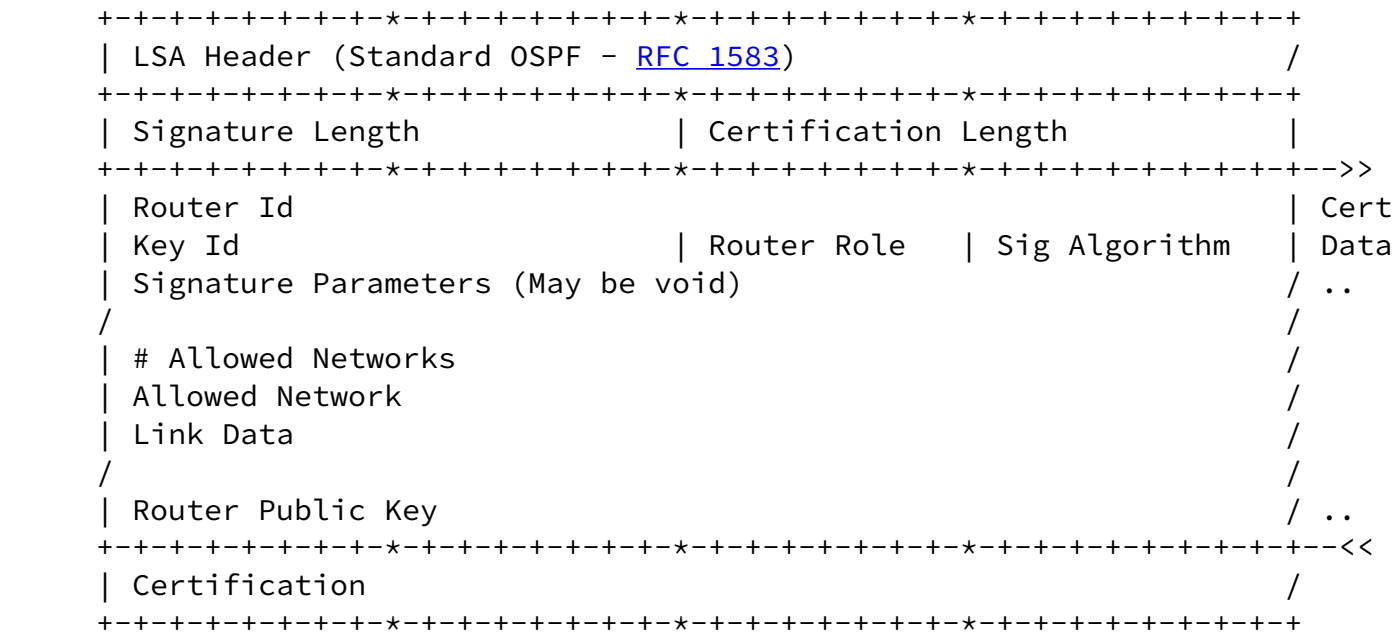
against this vulnerability would require that there be some substantiation of the connections a router could announce.

One way to produce a substantiation of announced connections would be to have an authority in the autonomous system that would produce signed authorizations of the networks that a router would be allowed to announce. This means that before a router could be part of the OSPF exchanges it would need to communicate, either on-line or off-line, with the authority. When an existing connection disappears permanently or a new connection comes into being, a new authorization from the authority would be needed. As the existence of connections a router has with networks, hosts, and other routers is not as dynamic as the state of those connections, this would not be a hardship for network management for one router.

This authorization could be made part of the Router Public Key LSA and therefore distributed as part of the normal OSPF flooding mechanism, as follows:

ROUTER PUBLIC KEY LSA





```
| Signature                                                     /
+-+-+-+-+-+-+-+-*-+-+-+-+-+-+-*-+-+-+-+-+-+-*-+-+-+-+-+-+-+-+
```

The new Router Public Key fields are:
Allowed Network: The number of network ranges that follow in this advertisement
Allowed Network: An network address that this router is authorized to announce.
Link Data: The network's IP address mask.

(Note that the internal router vulnerability applies only to one-sided connections, but the protection could be applied to all connections a router may announce.)

As the connections that would require authorization should not change frequently, distributing the authorization with the speed of the OSPF flooding mechanism may be unnecessary. Some other authorization distribution mechanism could be employed.

8.3. Autonomous System Border Routers

The autonomous system boundary routers can produce incorrect routing information in the external routes information they originate. There is no way to double check or corroborate this information, as there is with area border routers. No authority within an autonomous system exists to authorize the networks an autonomous system boundary router could announce, as is the case for the internal networks an internal router could announce. Consequently, the autonomous system boundary routers

remain a unprotected vulnerability. With this in mind, special care should be taken to protect the autonomous system boundary routers with other means.

9. Security Considerations

This entire memo is about security considerations.

10. References

[1] Gregory G. Finn, "Reducing the Vulnerability of Dynamic Computer

Networks," ISI Research Report ISI/RR-88-201, University of Southern California Information Sciences Institute, Marina del Rey, California, June 1988.

[2] Kumar,B and Crowcroft,J., "Integrating Security in Inter-Domain Routing Protocols", Computer Communications Review, Vol 23, No. 5, October 1993.

[3] Moy, J., "OSPF Version 2," RFC 1583, Proteon, Inc., March 1994.

[4] Perlman, R., "Network Layer Protocols with Byzantine Robustness", Ph.D. Thesis, Department of Electrical Engineering and Computer Science, MIT, August 1988.

[5] Perlman, R., "Interconnections: Bridges and Routers", Addison-Wesley, Reading, Mass., 1992.

[6] Schneier, B., "Applied Cryptography: Protocols, Algorithms, and Source Code in C," John Wiley & Sons, Inc., New York, 1994.

[7] Steenstrup, M., "Inter-Domain Policy Routing Protocol Specification: Version 1", RFC 1479, BBN Systems and Technologies, July 1993.

[9] PKCS #1: RSA Encryption Standard, RSA Data Security, Inc., 3 June 1991, Version 1.4.

11. 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