Network Working Group J. Etienne
Internet-Draft May 3, 2001
Expires: November 1, 2001

OSPF with digital signature against an insider
draft-etienne-rfc2154-flaws-00.txt

Status of this Memo

Copyright Notice

Abstract

This text comments the security offered by RFC2154[1] "OSPF with Digital Signatures" and shows it is insecure against insiders attacks. It is describes an experimental extension of OSPF to digitaly sign the LSAs.

Table of Contents

1. Reader requirement

The reader is supposed to know OSPF(RFC2328[2]), the digital signature extension(RFC2154[1]), and have notions in protocol security. We have inserted precises references to help the reader.

2. Attacker model

The attacker model isn't clearly specified in the rfc, so we assume an attacker who takes deliberate actions (unexpected by the protocol) in order to influence the routing for personal gains (e.g. make a network unreachable, route packets toward a attacker to perform traffic analysis or man-in-the-middle attacks).

3. Packet Authentication

In OSPF cryptographic authentication (RFC2328.D.3[2]), the neighbors of a link share a secret key and sign all the packets with it. It provides some protections against external nodes injecting packets in OSPF local exchanges without being detected. But this sheme has 2 weaknesses: (i) the authentication is done per link and (ii) the anti-replay has a flaw.

3.1 Packet anti-replay

Packets can still be replayed because several packets can legally have the same sequence numbers. The main reason is OSPF doesn't provide a rollover procedure for the sequence number and to avoid this case, the standard advices to use the number of seconds as sequence number. So an external node can sucessfully replay a packet multiple times until the destination router(s) accept(s) a packet with a higher sequence number. This delay can be up to 10 seconds (default hello interval) and more in case of packet loss.

RFC2154[1] doesn't mention this problem.

3.2 Packet authentication per source

The OSPF's authentication protects the routers from unauthorized access by external nodes but a router can still send fake packets without being detected.

RFC2154.2[1] shortly mentions this problem : "The basic idea of this proposal is to ... use a neighbor-to-neighbor authentication algorithm (like keyed MD5) to protect local protocol exchanges". But this algorithm isn't described, so we consider the hole still open.

4. LSA anti-replay

In OSPF, the sequence numbers(RFC2328.12.1.6[2]) of LSAs aren't stored in a non-volatile memory and are reused after a reboot. An attacker may exploit this feature to feed victims with obsolete LSAs. The replayed LSAs have a valid signature so the victims won't detect the forgery.

RFC2154[1] doesn't mention this problem.

5. Globally synchronized timestamps

RFC2154.7.2.createtime[1] requires to have globally synchronized clock between Trusted Entities but doesn't explain how to synchronized them. The solution isn't trivial because the synchronization must be secure against insider attacks as well. As RFC2154[1] doesnt specify how to achieve a globally synchronized clock with possibly subverted time servers, we consider this as a weakness.

6. LSA's age

The age field (RFC2328.12.1.1[2]) of a LSA is modified in transit, so it can't be cover by the digital signature and an attacker may forge it.

RFC2154.3.1[1] proposes to cover the age field only when it is set to MaxAge (RFC2328.B.MaxAge[2]). It is possible because OSPF never increase a LSA's age beyond MaxAge so the field won't modified in transit. It prevents a router from forging a LSA with an age of MaxAge but an attacker can still set the age to any value between 0 to MaxAge-1. For example, an attacker can set the age close to MaxAge and flood it. The LSA will be installed in each router and prematurely expire, causing an easy denial of service, so we consider the hole still open.

7. Local roles

On broadcast and NBMA networks, OSPF elects a designated router (RFC2328.7.3[2]). A designated router has an influential role in OSPF, it originates the net-LSA for transit broadcast/NBMA networks and is the center on the database exchanges. The designated router is elected (RFC2328.9.4[2]) based on a priority (RFC2328.9[2]). An attacker may claim an higher priority to be elected and take advantages of its designated role.

RFC2154[1] doesn't mention this problem.

8. Global roles

Area Border Routers (ABR RFC2328.3.3[2]) and Autonomous System Boundary Routers (ASBR RFC2328.3.3[2]) advertize informations (summary-LSA RFC2328.12.4.3[2] and AS-external-LSA RFC2328.12.4.4[2]) about non directly connected links. If signing LSAs prevent forgery, a router can still send incorrect informations in its own LSAs. For example, an ABR can inject summary LSAs with falsly small metrics and thus attrack the outgoing traffic of the whole area (e.g. blackhole, traffic analisys, packet modification).

8.1 Area Border Router

ABRs of an area are connected together by the area and by the backbone. Because they have access to the same informations (i.e. the original data from a hierachical level and how the others ABRs export it into the other), they can check each other.

This assumes there is at least one uncorrupted ABRs per area. Moreover if the topology changes, the ABRs temporarily may have a different database and obtain different results even if no router is corrupted. So the result's exploitation may be difficult.

Using this, RFC2154.9.1[1] presents two interesting proposals: (i) The first one is each ABR checks the calculation of the other ABRs and issue a warning if an attack is diagnozed. With N ABRs connected to a area, the cpu load is multiplied by N-1 on each ABR. (ii) The second one goes further and originates the LSAs resulting from the calculations, thus each router can choose which LSA to use. this multiply the number of LSA originated by an ABR by N-1. These LSAs will be flooded and stored in each router of the area, so the memory and network cost are increased significantly.

Both solutions increases the protocol cost and RFC2154[1] finds them too expensive to be used. Moreover if all the ABRs are corrupted, the attack will be undetected.

8.2 Autonomous System Boundary Router

By definition, the informations external to the autonomous area aren't controled by OSPF. so an ASBR can produce incorrect route without being detected.

RFC2154.9.3[1] explain it.

9. Security considerations

This text shows that OSPF with digital signature is insecure against insiders attacks.

If the attacker model is reduced to a faulty router which accidentally send bogus packets due to software or hardware bugs, the vulnerabilities described in this text are still valid but much less likely.

References

[1] Murphy, S., Badger, M. and B. Wellington, "OSPF with Digital Signatures", RFC 2154, June 1997.

[2] Moy, J., "OSPF Version 2", STD 54, RFC 2328, April 1998.

Author's Address

Jerome Etienne

EMail: jme@off.net
URI: http://w3.arobas.net/~jetienne

Full Copyright Statement

Acknowledgement

Funding for the RFC editor function is currently provided by the Internet Society.