Network Working Group
INTERNET DRAFT
draft-ietf-rpsec-ospf-vuln-00.txt

Emanuele Jones
Alcatel
Olivier Le Moigne
Alcatel

May 2004

OSPF Security Vulnerabilities Analysis

Status of this Memo

Specification of Requirements

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC2119.

Abstract

Internet infrastructure protocols were designed at the very early stages of computer networks when "cyberspace" was still perceived as a benign environment. As a consequence, malicious attacks were not considered to be a major risk when these protocols were designed, leaving today's Internet vulnerable. This paper provides an analysis of OSPF vulnerabilities that could be exploited to modify the normal routing process across a single domain together with an assessment of when internal OSPF mechanisms can or cannot be leveraged to better secure a domain.

Table of Contents

1. Introduction

Internet infrastructure protocols were designed at the very early stages of computer networks when "cyberspace" was still perceived as a benign environment. As a consequence, malicious attacks were not considered to be a major risk when these protocols were designed, leaving today's Internet infrastructure vulnerable.

Since routers work in a cooperatively manner based on forwarding network information received from their peers, they are all threatened by the possibility that the exchanged routing information may have been contaminated or forged by a malicious or faulty entity.

This paper provides an analysis of OSPF [1] vulnerabilities that could be exploited to modify the normal routing process across a single domain, together with an assessment of when internal OSPF mechanisms can or cannot be leveraged to secure a domain.

1.1. Attacker's Definition

Throughout this paper the term attacker will be used to define any entity capable of posing any threat to an OSPF routing domain. Hence, this definition includes: 1) any subverted OSPF router, 2) any malicious software capable of interacting with an OSPF routing domain, 3) any faulty or misconfigured legitimate OSPF peer.

From a security standpoint, this paper is consolidating all possible OSPF deployment situations into two opposite scenarios.

The first scenario requires OSPF Cryptographic Authentication or Simple Password Authentication to be present on all links within a routing domain. The second scenario takes place when Null Authentication is adopted.

If one link is not protected then the whole routing domain becomes potentially vulnerable; if the attacker is in the position to obtain even a single copy of any OSPF message then the authentication provided by Simple Password is compromised and the security for the entire routing domain falls immediately in the second scenario.

In the first scenario, Cryptographic Authentication being deployed, there are two kinds of entities capable of attacking or posing threats: insiders and outsiders. An attacking entity is considered an insider if it is in possession of the secret key for any OSPF Cryptographic Authentication session either through: cryptanalysis, social engineering, coercion or access to a compromised/subverted routing resource. This also includes threats arising from malfunctioning or faulty-configured OSPF routers. An outsider is an attacker that is not in possession of the secret key.

In the second scenario, when the routing domain is not protected by OSPF Cryptographic or Simple Password authentication there is no distinction between insider and outsider entities. Any attacker can successfully forge OSPF messages on behalf of any OSPF peer, legitimate or not.

1.2. Attacker's Location

Since OSPF routers on broadcast, on Point-to-Multipoint, NBMA and on virtual links will accept unicast packets that are destined directly to them, no assumption is made on the location of the attacking entity. This leads to a scenario where an attacker, in possession of a secret key, if at all needed, can attack a router located in a remote routing domain. The proper implementation of ingress filtering and other mechanisms described by RFC2827 [2] and recently by the Internet Draft [3] should mitigate this situation, forcing insider and outsider attackers to at least have access to one of the links in the routing domain target of their attack.

1.3. Vulnerabilities Damages and Consequences

Generally speaking attackers will be able to disrupt and manipulate the routing domain, posing serious threats to the actual delivery of data and control plane packets.

For instance, if the routing information creates loops in the forwarding path some packets will never be delivered, denying service to many destinations. Loops also create congestion by leaving packets in the network longer than necessary and by consuming resources without providing any useful service in the end. The incorrect forwarding of large amounts of traffic over one link may overwhelm the link and result in the delaying, or even prevention, of traffic delivery. Moreover, incorrect routing information could result in data traffic transiting networks that otherwise would have never seen that data.

Finally, routing information that incorrectly reports OSPF Areas, or any other portion of the domain, as unreachable will deny services to all hosts connected to or exchanging traffic with said areas.

The damages [4] that might result from these attacks are:

starvation: data traffic destined for a node is forwarded to a part of the network that cannot deliver it,

network congestion: more data traffic is forwarded through some portion of the network than would otherwise need to carry the traffic,

blackhole: large amounts of traffic are directed as to be forwarded through one router that cannot handle the increased level of traffic and drops many/most/all packets,

delay: data traffic destined for a node is forwarded along a path that is in some way inferior to the path it would otherwise take,

looping: data traffic is forwarded along a path that loops, so that the data is never delivered,

eavesdrop: data traffic is forwarded through some router or network that would otherwise not see the traffic, affording an opportunity to see the data,

partition: some portion of the network believes that it is partitioned from the rest of the network when it is not,

cut: some portion of the network believes that it has no route to some network that is in fact connected,

churn: the forwarding in the network changes at a rapid pace, resulting in large variations in the data delivery patterns (and adversely affecting congestion control techniques),

instability: OSPF becomes unstable so that convergence on a global forwarding state is not achieved,

overload: the OSPF messages themselves become a significant portion of the traffic the network carries.

resource exhaustion: the OSPF messages themselves cause exhaustion of critical router resources, such as table space and queues.

These consequences can fall exclusively on a single OSPF Area or may effect the operation of the OSPF network domain as a whole.

2. Generic Attack Techniques

The OSPF protocol is subject to the following attacks (list taken from the IAB Internet-Draft providing guideline for the security considerations section of Internet-Drafts [5]).

Eavesdropping: The routing data carried in OSPF is carried in clear-text, so eavesdropping is a possible attack against routing data confidentiality.

Message Replay: In general, OSPF with Cryptographic Authentication provides a sufficient mechanism for replay protection of its messages. Nonetheless, there are still some scenarios in which an outsider attacker can successfully replay OSPF messages; these are illustrated over the next sections.

Message Insertion: OSPF with Cryptographic Authentication enabled is not vulnerable to message insertion from outsiders. In the case of

an insider or in the absence of Cryptographic Authentication, message insertion becomes a trivial operation even for a remote attacker.

Message Deletion: OSPF provides a certain degree of protection against message deletion. The receiver itself cannot detect if a message has been deleted or not, but the sender will detect a deleted Link State Update (LSU) message since it will not receive any OSPF Link State Acknowledgment message for it. There is no acknowledging mechanism for Hello messages, but the deletion of some, generally four or more, consecutive Hello messages belonging to the same router will cause "adjacency breaking" and thus be easily detected by all the parties involved.

Message Modification: OSPF with Cryptographic Authentication provides protection against modification of messages. In the case of an insider or in the absence of Cryptographic Authentication message modification becomes possible.

Man-In-The-Middle: OSPF with Cryptographic Authentication provides protection against man-in-the-middle attacks. In the case of an insider or in the absence of Cryptographic Authentication, the protocol becomes exposed to man-in-the-middle attacks through the lower network layers - such as ARP spoofing - on all OSPF peers that are one hop apart; while OSPF peers connected over virtual links are exposed to Layer 3 man-in-the-middle attacks too.

Denial-of-Service: While bogus routing information data can represent a Denial of Service attack on the end systems that are trying to transmit data through the network and on the network infrastructure itself, certain bogus information can represent a more specific Denial of Service on the OSPF routing protocol itself. For example, it is possible to reach the limits of the Link State Database of a victim with External LSAs or with bogus LSA headers during the Link State Database Exchange phase.

3. Vulnerabilities and Risks

3.1. OSPF General Vulnerabilities

The risks in OSPF arise from the following fundamental vulnerabilities:

3.1.1. Local Intrusion Global Impact

Compromising a single network equipment (router) or a link's security has an obvious and immediate local impact (ability to disable local links, to change properties, to stop routers etc...). Unfortunately, due to the lack of end-to-end authentication

mechanisms - such as a Public Key Infrastructure (PKI) - a breach in a single link has also a global impact since the attacker is now in the position to tamper with information regarding any other remote network equipment belonging to the same routing domain.

3.1.2. Remote Attacker

Even though OSPF is designed and deployed to be used as an intra-domain routing protocol, in most scenarios and situations an OSPF router will still accept unicast IP packets directly addressed to itself as described in paragraph 8.1 of RFC2328 [1]. "On physical point-to-point networks, the IP destination is always set to the address AllOSPFRouters. On all other network types (including virtual links), the majority of OSPF packets are sent as unicasts, i.e., sent directly to the other end of the adjacency." This opens the door to attacks that may be originating from outside the OSPF domain. Timing the stream of different packets needed for a given attack poses a certain degree of difficulty if executed from a remote AS, but it may not be enough to stop a skilled and motivated attacker. This means that, for example, customers on the access edges of a network can start attacking the routing domain in the core, if said domain were not to be protected by Cryptographic Authentication or if the malicious subscribers were to obtain the secret key.

3.1.3. Attacker Disabling Fight Back

It is often the case while reading papers, or other literature material, about OSPF to come across the concept of an OSPF "natural" fight back mechanism, for example [6]. OSPF fight back can be defined as follows: any router receiving an LSA that lists itself as the advertising router and noticing that the content of this LSA is not coherent with its status of resources will try to correct the situation either by flushing or updating the erroneous LSA. The following three scenarios show how the OSPF fight back mechanism can be disabled clearing the way to stealthy attacks.

3.1.3.1 Periodic Injection

This is a brief explanation on how a malicious LSA will succeed in attacking a routing domain, overriding any fight back:

According to RFC2328 [1], a router will never emit (or update) its LSAs faster than once every MinLSInterval (5 seconds). This allows for almost permanent changes in the routing domain, if an attacker is flooding the OSPF domain with malicious LSAs at a rate higher

than one every MinLSInterval.

On top of this, if an OSPF implementation behaves as described by RFC2328 [1, paragraph 13], the router owner of the LSA may never fight back and it will collaborate in the flooding of malicious routing information on its behalf. The flooding happens because the malicious LSA is considered newer than the copy already present in the legitimate owner's Link State Database - the malicious LSA will

have a higher sequence number - (check performed on Step 5) and because the legitimate copy of the LSA already present in the Link State Database was not received via flooding but installed by the router itself (check performed in step 5.a). When step 5.f is finally executed - after the malicious LSA has been already flooded - a simple test reveals that the LSA was owned by the router and that it contained erroneous information. Only at this stage action is taken to correct it; but since any router must wait MinLSInterval before updating any of its LSAs, the owner will fight back every MinLSInterval while the flooding is in progress. We have also observed a complete lack of fight back in implementations that erroneously reset MinLSInterval when flooding LSAs.

3.1.3.2 Partitioned Networks

If the flooding mechanism does not have a path to rely malicious LSAs to the legitimate owner, said owner will never initiate a fight back. An example of this could be a subverted router conveniently located on a partitioning link. If said router is removed, the entire network domain would be partitioned into two disconnected portions. This subverted router could choose to inject a given malicious LSA only into one part of the routing domain, claiming that this LSA is coming from a legitimate router located on the opposite portion of the network. The legitimate router will never be made aware of the forged information on its behalf and thus will never initiate a fight back. This will create fatal inconsistencies between the Link State Databases of the various OSPF routers.

3.1.3.3 Phantom Routers

All information injected in the routing domain on behalf of non-existing (phantom) OSPF routers will never trigger a fight back reaction. Thus, this information will remain in the Link State Databases of the legitimate routers for MaxAge (1 hour, by default). It is important to underline that even if Link State Advertisements (LSAs) crafted on behalf of phantom routers are kept in the Link

State Database, these are not taken into account by the Shortest Path First (SPF) algorithm.

3.1.4. Attacker Leveraging Fight Back

The fight back mechanism can contribute to amplify certain Denial of Service attacks. One single false LSA may unleash a significant number of LSA updates that are trying to correct it. Even though such a reaction is both efficient and desirable, it may be leveraged to amplify the effects of certain Denial of Service attacks, if continuously triggered.

3.1.5. Dealing with External Routes

Every piece of routing information that is dealing with outside routes, forged or real, that is introduced in the domain - by means of route redistribution via BGP, RIP or any other routing protocol including statically configured - cannot be verified and it is propagated to all OSPF Areas of the domain that are not configured

as stub-areas or NSSA. Even though verification of routes that are outside the routing domain is clearly beyond the scope of OSPF, the current flooding mechanism of such information may be used as an efficient intrinsic vector for conveying malicious/bogus messages. Moreover, if an attacker manages to subvert an ASBR node, or successfully masquerades as one, there will be no fight back from any of the other ASBRs regarding ownership, validity and metric advertisement for the External routes claimed by the subverted ASBR; thus, the attacker could easily attract to itself big portions of the traffic destined outside the AS.

3.2. Protocol-specific Vulnerabilities

There are two types of authentication mechanisms in OSPF: Simple Password and Cryptographic. Simple Password authentication consists of a plain text password carried in the header of each OSPF message; the vulnerability of this Authentication method is obvious and will not be discussed further. There are five different OSPF message types: Hello, Database Description, Link State Request, Link State Update, Link State Acknowledgement. The next sections discuss general vulnerabilities for every field in the five OSPF messages as well as the ones arising from Cryptographic Authentication. Each section also defines the ability for outsiders, insiders or faulty OSPF peers to exploit these weaknesses.

3.2.1. Packet Header with Cryptographic Authentication Enabled

IP Header

No field of the IP header is protected by the Message Authentication Code (MAC) available when Cryptographic Authentication is enabled. This poses a threat to OSPF any time the protocol relies on any IP field. For example RFC2328 [1] states on paragraph 10.5: "When receiving an Hello on a point-to-point network (but not on a virtual link) set the neighbor structure's Neighbor IP address to the packet's IP source address".

OSPF Header

Neighbor OSPF routers may reset their Cryptographic Sequence Number states when a peer reboots (if the "resetting" peer is not capable of storing Cryptographic Sequence Numbers across reboots) or when the peer's Cryptographic Sequence Number rolls over. At this point, any previously logged packet can be maliciously replayed and will look legitimate if the secret key has not changed in the mean time. Moreover, if the replayed packet is chosen with a high enough sequence number, it will block the communication between the recently rebooted router and its peer(s) for RouterDeadInterval plus the time needed to establish a new adjacency [7]. This vulnerability is exploitable by any outsider that is able to log OSPF packets. It is important to underline that this vulnerability could be used to break adjacencies between OSPF peers.

Breaking an adjacency will cause an OSPF router to update its own

Router LSA which in turn will force a new SPF calculation, this may lead to changes in the routing table due to the loss of one peer. If the router is also the Designated Router (DR) for the link, breaking an adjacency also entails modifying the corresponding link's Network LSA, potentially resulting in transit links being declared as stub connections and/or partitioning of the domain.

Finally, even for an insider attacker (with or without the ability to log packets) forging a single Hello message, with a high enough sequence number, is an excellent and quick option to break any established adjacency. In conclusion this vulnerability may be appealing to both outsider and insider attackers.

3.2.2. Hello Message

In general errors in Hello message parameters such as incorrect AreaID, RouterDeadInterval, HelloInterval and so on will cause the

Hello to be silently discarded with no further impact.

Other Hello parameters are analyzed next, and in order to modify the following parameters, the attacker must be an insider, i.e. in possession of the secret for the link to be attacked or the link must be configured with the Null Authentication security option.

3.2.2.1. Neighbor

Omission of one or more adjacent neighbors in the neighbor list will immediately break the adjacency and force a synchronization process between the legitimate owner of the Hello message and all the omitted neighbors.

Breaking an adjacency will cause an OSPF router to update its own Router LSA which in turn will force a new SPF calculation, this may lead to changes in the routing table due to the loss of one peer. If the router is also the Designated Router (DR) for the link, breaking an adjacency also entails modifying the corresponding link's Network LSA, potentially resulting in transit links being declared as stub connections and/or partitioning of the domain.

3.2.2.2. DR and BDR

Tampering with these two fields can lead to several problematic scenarios,(concerning broadcast and NBMA networks) each leading to different consequences for the routing domain.

In order to be taken into account by the DR election process on a victim router, the attacker must list the victim router ID into the active neighbor list of its malicious Hello. Next some examples of attacks are described.

In the Hello message, setting to null the DR and BDR fields, on behalf of a legitimate router on the network, and listing all neighbors in the malicious Hello, will force a full re-election of the DR and BDR.

Bogus Hello messages from a non-existing router, with a Router Priority and an IP address higher than any legitimate router on a network, listing itself as DR will allow the attacker to successfully convince all the routers present in the neighbor list (of the malicious Hello) that the DR has changed. Any router believing in the non-existing DR will update its Router LSA by

listing a link to a stub network instead of the transit network (because it is not fully adjacent to the non-existing DR). Thus, this router will not use this network anymore as a transit network; this will lead to connectivity loss.

If the attacker is listing the current DR and BDR in the active neighbors, then the current DR and BDR will also be deceived into thinking that the non-existing router is the new DR. This will have an impact on all the routers connected to the network at once.

3.2.2.3. Deletion of Hello Messages

If no Hello message is received from a given neighbor for a period of time longer than RouterDeadInterval, then the adjacency with this router is considered to be broken.

Breaking an adjacency will cause an OSPF router to update its own Router LSA which in turn will force a new SPF calculation, this may lead to changes in the routing table due to the loss of one peer. If the router is also the Designated Router (DR) for the link, breaking an adjacency also entails modifying the corresponding link's Network LSA, potentially resulting in transit links being declared as stub connections and/or partitioning of the domain.

3.2.2.4. Hello Message Replay

The Hello Replay attack cannot be perpetrated by an outsider as described by [7]. "The HELLO packet lists the recently seen routers, so if an attacker replays a HELLO packet back to its source, the source won't see itself in the list and will deduce the connection isn't bidirectional. [...] On broadcast, NBMA or Point to Multipoint networks, the neighbor is identified by its IP address, so both attacks can be used." [7, paragraphs 3.2.2 and 3.2.3] This clashes with what is stated by RFC2328 [1, paragraph 10.5]: "When receiving a Hello Packet from a neighbor on a broadcast, Point-to-MultiPoint or NBMA network, set the neighbor structure's Neighbor ID equal to the Router ID found in the packet's OSPF header." Zebra seems to be in agreement with the RFC's interpretation provided above and is not vulnerable to the Hello Replay attack.

In conclusion, the RouterID field is covered by Cryptographic Authentication and therefore it cannot be modified by an outsider without infringing on the MAC (Message Authentication Code), and if the Hello message is replayed to its owner without modifying anything the RouterID will match the one of the owner and the message will be ignored.

3.2.3. DB Description, Link State Request and Acknowledgment

There is no clear threat except for an insider attacker, or a faulty router, that behaves as described in the resource consumption section.

3.2.4. Link State Update

In order to modify the parameters described in the following subsections, the attacker must be able to successfully inject malicious LSUs. Hence, the attacker must either subvert, impersonate or fake a router which is at least in the exchange state or higher. In the two latter cases, the attacker must be an insider, i.e. in possession of the secret key for a link or a link must be configured with the Null Authentication security option.

3.2.4.1 Link State Update Header

The Link State Update (LSU) Header does not appear to present any vulnerability in and for itself. In the case of attacks involving bogus LSAs, some fields of the LSU header may need to be maliciously modified to be consistent with the bogus information carried by the LSAs.

In general, errors in some LSU Header parameters such as incorrect RouterID, AreaID and AuType will cause the LSU to be silently discarded with no further impact.

3.2.4.2. Link State Advertisement Header

LS age (MaxAge Attack)

Setting the age field of an LSA to MaxAge will cause the LSA to be flushed from all the routers reached by the flooding mechanism. The owner of the LSA will fight back by issuing a new LSA with age set to 0 and a higher sequence number. Any attack exploiting this vulnerability could cause unnecessary flooding and refreshing of the Link State Database, hence making the routing information inconsistent. Routers that do not have a copy of the LSA in their Link State Databases will not contribute to the flushing of it, this can help the owner of the LSA in its fight back [8].

LS sequence number (Max Sequence Number Attack)

This is an implementation bug that has been published long ago [9] and not a protocol vulnerability. Nonetheless it is listed in this memo for historical reasons and because at least one recent implementation of OSPF was still affected by it.

The bug concerns sequence numbers roll-over. When an LSA reaches its maximum (0x7FFFFFFF) value it is not flushed by flooding it with its age set to MaxAge; instead, the erroneous implementation will simply re-issue the LSA with a rolled-over sequence number. Any newer instance will always be considered outdated when compared to the old

one having the LS sequence number set to the maximum value. Thus, an insider attacker could install a bogus LSA on all routers for a

MaxAge-long interval without any effective fight back from the owner of the LSA [9].

3.2.4.3. Router Link State Advertisement

Remove, add routers to the domain

It is possible to tamper with the topology of a domain by introducing phantom OSPF routers through bogus Router LSAs. Depending on how said phantom OSPF nodes are claiming to be interconnected with each other and with real OSPF peers, they may or may not be utilized by the SPF algorithms present in other OSPF peers. A similar situation applies when a Router LSA is maliciously flushed impacting routes across the domain. Adding or deleting OSPF routers through bogus existing router LSAs will trigger a fight back reaction by the owner of the LSA, except under the circumstances stated in paragraph 3.1.3.

E Bit

A Router LSA carrying the E bit set to 1 automatically allows a router to introduce External LSAs in the routing domain. This could be exploited to escalate a normal router into an ASBR.

Setting the E bit to 1 on Router LSAs will trigger a fight back reaction by the owner of the LSA, except under the circumstances stated in paragraph 3.1.3.

Link ID, Link data

Adding links (stub or transit) to any Router LSA will result in adversely impacting the normal flow of data-traffic through the domain. The same applies in the case of a Router LSA omitting any link previously present. More specifically: advertised stub networks are not verifiable by the Shortest Path First algorithms running on other routers present in the same Area. So, if a bogus Router LSA lists a stub network matching the network address of any existing remote network, other OSPF routers will actually consider the router owner of this LSA as a possible path to said remote network. This implies that a malicious or faulty entity advertising bogus stub networks could attract traffic towards itself and/or deviate normal routing across the domain.

Adding any kind of link to a Router LSA will trigger fight back by

the owner of the LSA, except under the circumstances stated in paragraph 3.1.3.

Metric
The metric fields of an LSA can be modified in the attempt to affect the SPF algorithm. Such operation could serve the purpose of attracting traffic to a node for eavesdropping or overloading; on the other hand, it could also be used for starving a given node.

Modifying the fields of a Router LSA regarding a link's metric will trigger a fight back reaction by the owner of the LSA, except under

the circumstances stated in paragraph 3.1.3.

3.2.4.4. Network Link State Advertisement

Remove or add links to a domain
It is possible to tamper with the topology of a domain by introducing phantom transit links through bogus Network LSAs. Depending on how said phantom transit links are connected to real or phantom OSPF routers, the bogus nodes may or may not be utilized by the SPF algorithms present in other OSPF peers. A similar situation applies where an existing transit link is maliciously flushed impacting routes across the domain.

Adding or subtracting transit links through bogus Network LSAs will trigger a fight back reaction by the owner of the LSA, except under the circumstances stated in paragraph 3.1.3.

Attached Router
It is possible to add or eliminate nodes from a transit link by tampering with the list of attached routers. If a legitimate node is removed from this list, that router will be considered disconnected by all the remaining OSPF peers in the domain, even though its Router LSA will state the opposite. There must be consistency between Network and Router LSAs for a router to be considered part of a link.

Subtracting a router from the list of attached routers through a bogus Network LSA will trigger a fight back reaction by the owner of the LSA, the DR for the network link, except under the circumstances stated in paragraph 3.1.3.

3.2.4.5. Summary Link State Advertisement

It is possible to add or eliminate information contained in both types of Summary Link State LSA affecting routes across different Areas.

Forging bogus Summary Link State LSAs will trigger a fight back reaction by the owner of the LSA, except under the circumstances stated in paragraph 3.1.3.

3.2.4.6. AS External Link State Advertisement

Every external route introduced by an ASBR is advertised by a single External LSA. There is no way for OSPF routers to verify the information carried by External LSA messages. Introduction of bogus External LSAs will affect the domain's knowledge of the outside world. Bogus External LSAs can be used to attract a portion of the data traffic destined outside the domain to a specific node for eavesdropping or overloading purposes. The same considerations apply to any attempt to starve one or more nodes.

Introducing false External LSAs will trigger a fight back reaction by the owner of the LSA and/or will not be recognized as legitimate

information by other routers if the LSA is forged on behalf of anon-ASBR router, except under the circumstances stated in paragraph 3.1.3.

Forward

The Forward field of an External LSA specifies the host (OSPF router or not) meant to be used as gateway for that external route; said host can be located everywhere in the domain including Stub Areas. If this field is forged and the forward host is not an OSPF router then there will be no OSPF fight back from the host itself, but there may be a fight back reaction from the ASBR owner of the LSA. By exploiting this feature, an attacker could redirect traffic destined outside the routing domain to any given host in the domain which may, or may not, be under its control. For example, this can be used to generate loops between an ABR and any of its neighbors located in its Stub Area, simply by mentioning one of these neighbors in the forward field of an External LSA advertisement for traffic destined outside the domain.

Forging bogus AS External LSAs with modified Forward field information will trigger a fight back reaction by the owner of the LSA, except under the circumstances stated in paragraph 3.1.3.

3.3. Resource Consumption Vulnerabilities

Every resource may be exploited in the attempt to interfere with traffic flows from legitimate users. In some cases the resource may be so overwhelmed by malicious/illegitimate packets that legitimate users will not only experience a drop in the performance of the service, but they may be even prevented from accessing the service itself. If one, or more, critical resource of a router is busy serving bogus traffic, or dropping malicious routing messages, then the whole router will be impacted and enter a delicate and more vulnerable state. Next is a list of possible weaknesses that can be exploited to produce a resource consumption attack.

3.3.1. OSPF Cryptographic Authentication

With Cryptographic Authentication disabled both outsider and insider entities - including attackers and faulty routers - can successfully forge malicious/erroneous OSPF messages that will be in the position to attack a router or exhaust its control plane resources, such as queues and CPU cycles.

On the other hand, when Cryptographic Authentication is enabled, only insiders may successfully force malicious OSPF messages to be accepted by the victim's control plane. Unfortunately though, outsider entities are still in the position to generate a powerful resource consumption attack by intentionally exploiting the Cryptographic Authentication mechanism itself as described in [3]. These entities may inject OSPF packets with bogus cryptographic information that will consume critical resources only to be

discarded afterward. This will impact OSPF by delaying or even preventing legitimate messages to be authenticated and used.

3.3.2. Hello Message

DR and BDR Election

Hello messages are used by OSPF also to carry out the DR and BDR election process. The DR election process itself presents a possible resource consumption vulnerability since it may be fooled into electing a new DR at every run. When a new DR is elected all routers on the network will have to use resources to establish adjacency with this new DR; the same applies in the case of the BDR.

Number of Neighbors

OSPF routers create a neighbor data structure for each neighbor discovered through the Hello protocol. The resources to store this information could be exhausted on a broadcast or NBMA network with a large host address range.

Message Size
Since a router must list all its current active neighbors in each of its Hello messages, it may have to issue a Hello message bigger than the Layer 2 media's MTU, e.g. bigger than the Ethernet frame's size. Since this is usually a delicate area in implementation and design all the necessary care should be exerted.

3.3.3. Link State Request Message

Any Link State Request message forces the destination router to reply with a Link State Update message containing the requested LSA. An insider attacker, or a faulty router, could mount a resource consumption attack by continuously requesting Link State information from its neighbors at any desired rate.

3.3.4. Link State Acknowledgment Message

Not acknowledging Link State Update messages forces the originating peer to keep a copy of the LSU on the retransmission list; this leads to re-transmission loops wasting resources on both sides.

3.3.5. Link State DB Overflow

Router/Network LSA
Router/Network LSAs received from non-existing OSPF peers will not be used by the SPF algorithm and will not directly adverse the routes nor the topology. Nonetheless, these LSAs will consume resources in the Link State Database and will not be removed from this database until they "naturally" expire after MaxAge (1 hour). If the purpose of an attacker is to simply consume database resources, then crafting LSAs on behalf of non-existing OSPF routers is a good option since it makes the effects of the attack last longer and triggers no fight back reaction at all. Finally, it is important to highlight that Link State Database overflows produced by Router and Network LSAs will not be limited by the mitigation mechanism detailed in RFC1765 [10].

External LSA
External LSAs may also be successfully exploited in the attempt to fill Link State Database resources. If these LSAs are crafted on

behalf of non-existing ASBRs, their information will not be used by any SPF algorithm; however they will be successfully installed in the Link State Databases. Moreover, External LSAs are forwarded to all routers in the domain (except routers located in Stub Areas), expire only after MaxAge if no fight back is place, and are never consolidated by OSPF.

Link State Database Description Messages
The Database Exchange process poses a resource consumption threat on the slave router participating to the process. An insider attacker - or a faulty router - capable of leading a victim into the Database Exchange process could advertise a huge list of non-existing links through Database Description messages. The victim will keep updating this list and start asking for details via Link State Request messages. The number of bogus links that the victim router will have to store poses an immediate resource consumption threat, while the prolonged request for details about the bogus LSAs will keep the victim's retransmission list full and busy.

Retransmission List Exhaustion
Any LSU that is not acknowledged is put on a re-transmission list. OSPF messages present in this list are sent over regular intervals until they are acknowledged by the receivers. Failing to acknowledge LSUs, accidentally or voluntarily, will trigger resource consumption on the remote peer's retransmission mechanisms.

3.3.6 Others

Routing table size/performance issue
Increasing the size of the routing table could potentially move a router into a very delicate state and eventually reach the limits assigned to some resources. This could be achieved by using Router, Network or External LSAs from existing peers and somehow disabling the fight back from the legitimate owners.

Fragmentation
Fragmentation of OSPF messages due to Layer 2 MTU is a crucial factor for any given implementation; any situation involving such process should be carefully tested. For example in the case of a router running the open source routing suite Zebra over Ethernet links, receiving a forged Router LSA that claims to have more than 118 links will adversely impact the routing daemon. Even though the LSA does not violate RFC2328, which states that a Router LSA must be entirely contained into one single IP packet, a Router LSA listing more than 118 links does exceed the Ethernet MTU and will be fragmented over multiple Ethernet frames: this seems to have a serious impact on the behavior of Zebra.

3.4. Vulnerabilities through Other Protocols

3.4.1. IP

OSPF runs directly over IP. Therefore, OSPF is subject to attack through attacks on IP. Direct attacks against the IP stack of a router, such as integrity and fragmentation attacks, will impact OSPF but are clearly beyond the scope of this document.

3.4.2. Other Supporting Protocols (Management)

The security of OSPF is inherently dependent on the security of the managing procedures. Critical examples are the configuration of the state of any interface, the Manual Stop procedure and the Timer Values.

Manual stop

A manual stop event causes the OSPF router to bring down all its adjacencies, release all associated OSPF resources, and delete all associated routes. If the mechanisms by which an OSPF router was informed of a manual stop is not carefully protected, OSPF connections could be destroyed by an attacker. Consequently, OSPF security is secondarily dependent on the security of whatever protocols are used to operate the platform.

Timer events

The RxmtInterval, InfTransDelay, RouterDeadInterval, HelloInterval timers together with the RouterPriority parameter are critical to OSPF operation. For example, if the HelloInterval timer value is changed, all remote peers will refuse Hello messages from that router and after RouterDeadInterval bring the adjacency down. Consequently, OSPF security is secondarily dependent on the security of the protocols by which the platform is managed and configured.

3.5. Residual Risk

OSPF Cryptographic Authentication assumes that the cryptographic algorithms are secure, that the secrets used are protected from exposure and are chosen well so as not to be guessable, that the platforms are securely managed and operated to prevent break-ins, etc.

Information theory states that the English language has about 1.3 bits of entropy for each 8-bit character. If an administrator were to choose the secret key for the Cryptographic Authentication to be any English word, the entropy associated to the secret key protecting the session would be drastically reduced from 128 bits to the point where it could be guessed in a matter of minutes or days.

On top of that, Common Line Interfaces (CLI) will generally limit the key input to a specific subset of ASCII characters - letters and number plus a few symbols - and will not accept a 128-bits number value (for example in hexadecimal format).

This becomes crucial in all those cases where the secret defending an OSPF adjacency is poorly chosen and changed once every three months, or every year, or never. In all these scenarios an attacker that somehow managed to obtain a copy of a single OSPF Hello message may eventually be able to crack the secret key and attack the entire routing domain for a prolonged period of time.

4. References

[1] J. Moy. "OSPF Version 2", STD 54, RFC2328, April 1998.

[2] P. Ferguson, D. Senie. "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing", BCP 38, RFC2827, May 2000.

[3] A. Zinin. "Protecting Internet Routing Infrastructure from Outsider CPU Attacks", work in progress, February 2003. Available as <draft-zinin-rtg-dos-00.txt> at Internet-Draft shadow sites.

[4] A. Babir, S. Murphy, Y. Yang. "Generic Threats to Routing Protocols", work in progress, April 2004. Available as <draft-ietf-rpsec-routing-threats-06.txt> at Internet-Draft shadow sites.

[5] E. Rescorla, B. Korver. "Guidelines for Writing RFC Text on Security Considerations", work in progress, January 2003. Available as <draft-iab-sec-cons-03.txt> at Internet-Draft shadow sites.

[6] F. Wang, S. Felix Wu. "On the Vulnerabilities and Protection of OSPF Routing Protocols" In Proceedings 7th International Conference on Computer Communications and Networks: 148-152. Los Alamitos, CA: IEEE Comp. Soc., 1998.

[7] J. Etienne. "Flaws in Packet's Authentication of OSPFv2", work in progress, November 2001. Available as <draft-etienne-ospv2-auth-flaws-00.txt> at Internet-Draft shadow sites.

[8] S. Murphy, et al. "Retrofitting Security into Internet Infrastructure Protocols." Proceedings of DARPA Information Survivability Conference and Exposition (DISCEX'00), 2000.

[9] B. Vetter, F. Wang and S. F. Wu. "An Experimental Study of Insider Attacks for the OSPF Routing Protocol", in 5th IEEE International Conference on Network Protocols, Atlanta, GA, Oct 28-31, 1997.

[10] J. Moy. "OSPF Database Overflow", Experimental, RFC1765, March 1995.

Authors' Addresses

Emanuele Jones
Alcatel
600 March Road - Kanata, ON, Canada K2K 2E6
EMail: emanuele.jones@alcatel.com

Olivier Le Moigne
Alcatel
600 March Road - Kanata, ON, Canada K2K 2E6
EMail: olivier.le_moigne@alcatel.com

Full Copyright Statement