Owning the Routing Table

Part II

Gabi Nakibly[1], Eitan Menahem[2],
Ariel Waizel[2], Yuval Elovici[2]

[1]National EW Research & Simulation Center,
Rafael – Advanced Defense Systems Ltd.
[2]Telekom Innovation Laboratories, Ben Gurion University

Background

- This work is a second installment of our research on **OSPF security**.
  - The first part was presented at **Black Hat USA 2011**.
- In this part we push the envelope further and present a **more powerful** attack that allows to take control of a **Cisco's router routing table**.

Overview

- The holy grail of routing attacks is owning the routing table of a router
  - without having to own the router itself.
- We present a newly found vulnerability of the OSPF protocol.
- It allows to own the routing tables of all routers in a routing domain from just a single compromised router.

Why is this so desirable?

- Owning the routing tables allows doing tricks such as:
  - Black holes
  - Network cuts
  - Traffic diversion
    - towards longer routes
    - or through an attacker-controlled router
  - And much much more

Who is vulnerable?

- The vulnerability is due to an ambiguity in the OSPF spec [RFC 2328].
- Therefore, potentially many commercial routers may be vulnerable!
- The attack has been successfully verified against Cisco IOS 15.0(1)M.

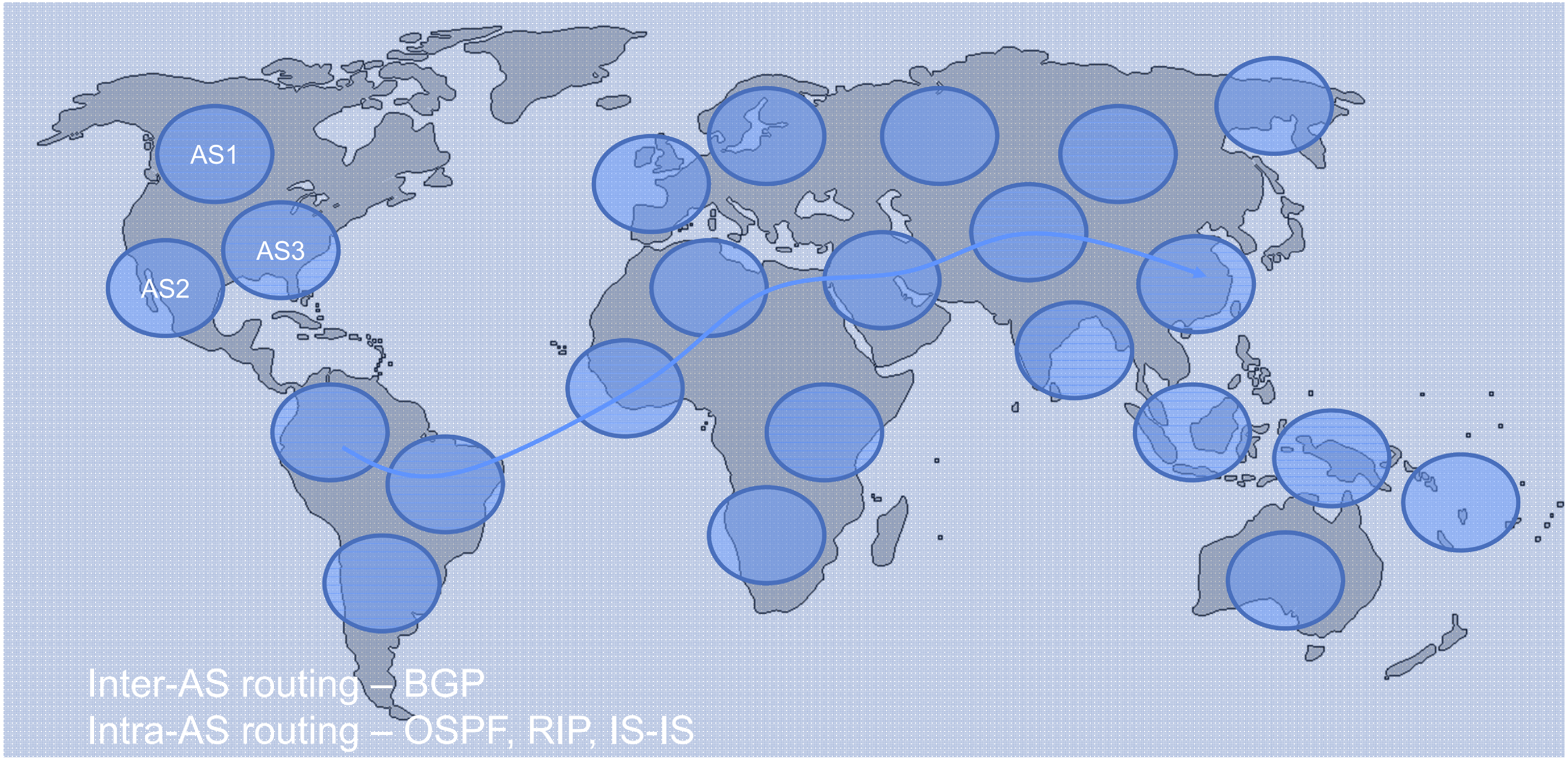
How the new attack differs from known ones?

- The new attack gains full and persistent over the routing table of another router.
  - Known attacks cannot do that
- It achieves this because it can persistently falsify routing advertisements of other routers.
  - Without triggering "fight-back" from the victim router.
    - More on this later on.

Agenda

- OSPF primer
- OSPF security strengths
- Known OSPF attacks
- The newly found vulnerability and attack

Internet Routing – The Big Picture



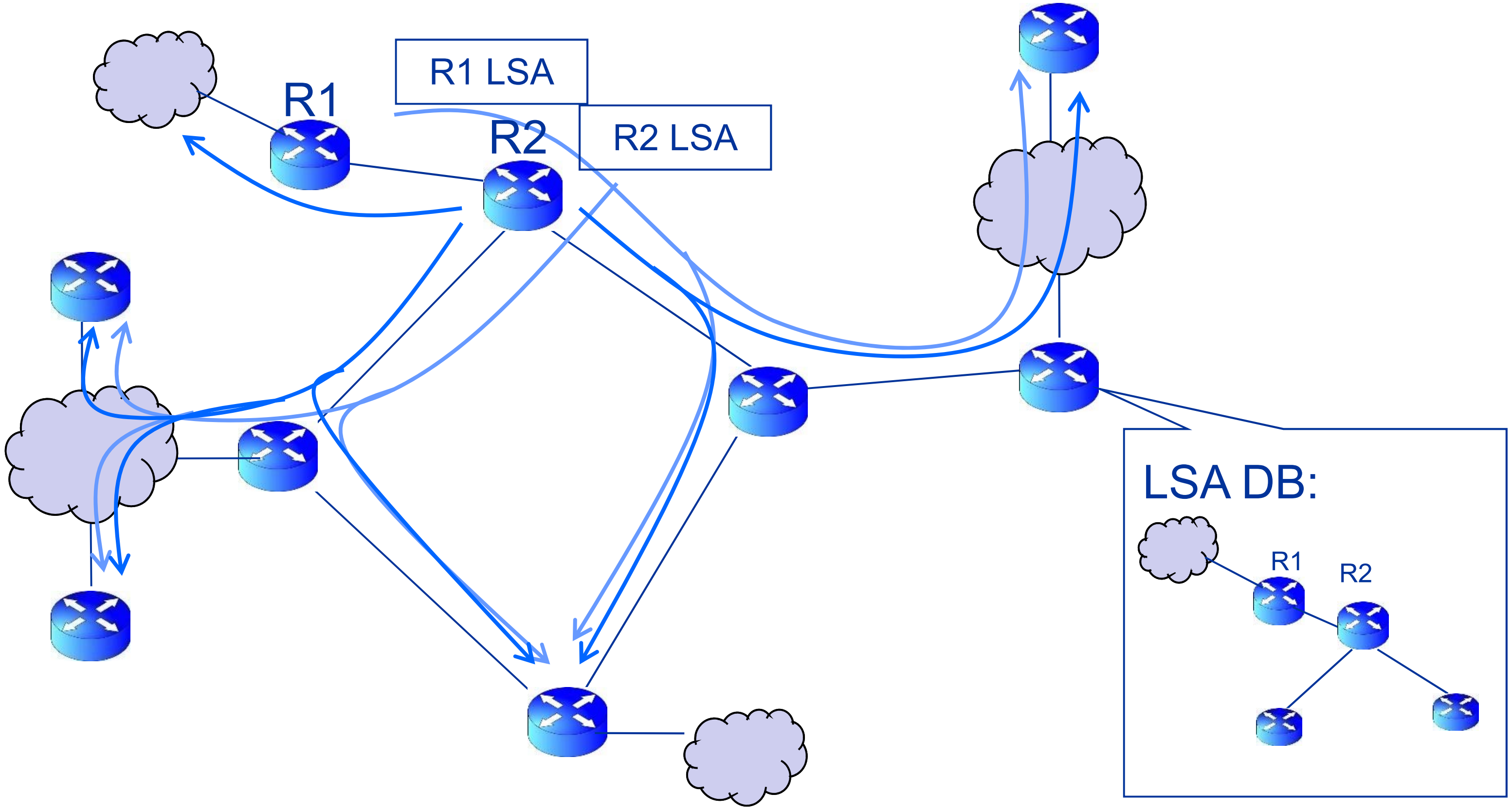
Inter-AS routing – BGP

Intra-AS routing – OSPF, RIP, IS-IS

OSPF Primer

- Every router periodically advertises it’s link state (i.e. “who are my neighbors?”).
  - This is called Link State Advertisement (LSA).
- The LSAs are flooded throughout the network hop-by-hop.
- Every router receives the LSAs of all other routers
  - and installs it in its LSA DB
  - this allows to build the topology map of the AS.

LSA flooding



OSPF Primer (cont.)

- There are several types of LSAs. The most important one is:
  - Router LSA – contains the links of a given router.
- Throughout the presentation we shall refer only to Router LSAs unless we specifically indicate otherwise.

The Attacker

- Location: inside the AS
  - Controls a single legitimate router in an arbitrary location
  - This means it can flood LSAs to its neighbors
- Goal: Full control of the routing tables of all other routers in the AS.

OSPF Security Strengths

- Every LSA is flooded throughout the AS
- The “fight back” mechanism
- One LSA holds only a little piece of topology information

Known Attacks

- Falsifying self LSAs
  - Falsify only a small portion of the AS topology, hence full control over the routing table can not be achieved.
- Falsifying other routers’ LSAs
  - Triggers immediate fight back
    - non-persistent
- Falsifying phantom router LSAs
  - Does not have an affect on the routing table
    - since no real router advertises a link back to the phantom.

Owning the Routing Table – Part I

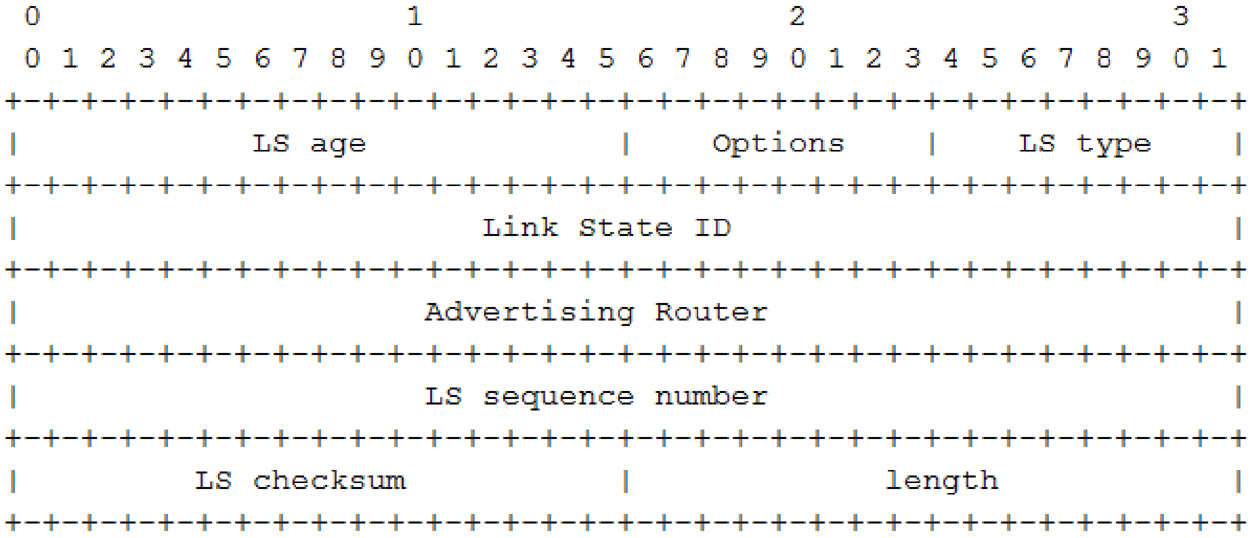
- Until 2011 the common knowledge was that an inside attacker cannot gain full and persistent control over the routing table of a router it does NOT control.
- At Black Hat USA 2011 we presented the first general technique to evade fight-back.
  - Thereby, persistently falsifying LSAs of other routers.
  - This was called the “Disguised LSA” attack.
    - See http://www.blackhat.com/html/bh-us-11/bh-us-11-briefings.html#Nakibly

The New Attack

- We now present an even more powerful attack.
  - It too allows to persistently falsify LSAs while evading fight-back
- On top of that, it offers some added bonuses:
  - The routing table of the victim router is erased
    - Can be used as a means to easily DoS a router
  - Only a single well-crafted attack packet is required

Background

- The LSA header:



```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|            LS age             |    Options    |    LS type    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                        Link State ID                          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                     Advertising Router                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                     LS sequence number                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         LS checksum           |             length            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

- An LSA is uniquely identified by:
  - LS type (for Router LSA it is always ‘1’)
  - Advertising Router
  - Link State ID

Background (cont.)

- Advertising Router
  - identifies the router that originated the LSA.
    - i.e., the router ID
- Link State ID
  - identifies the part of the AS that is being described by the LSA.
    - i.e., the router ID

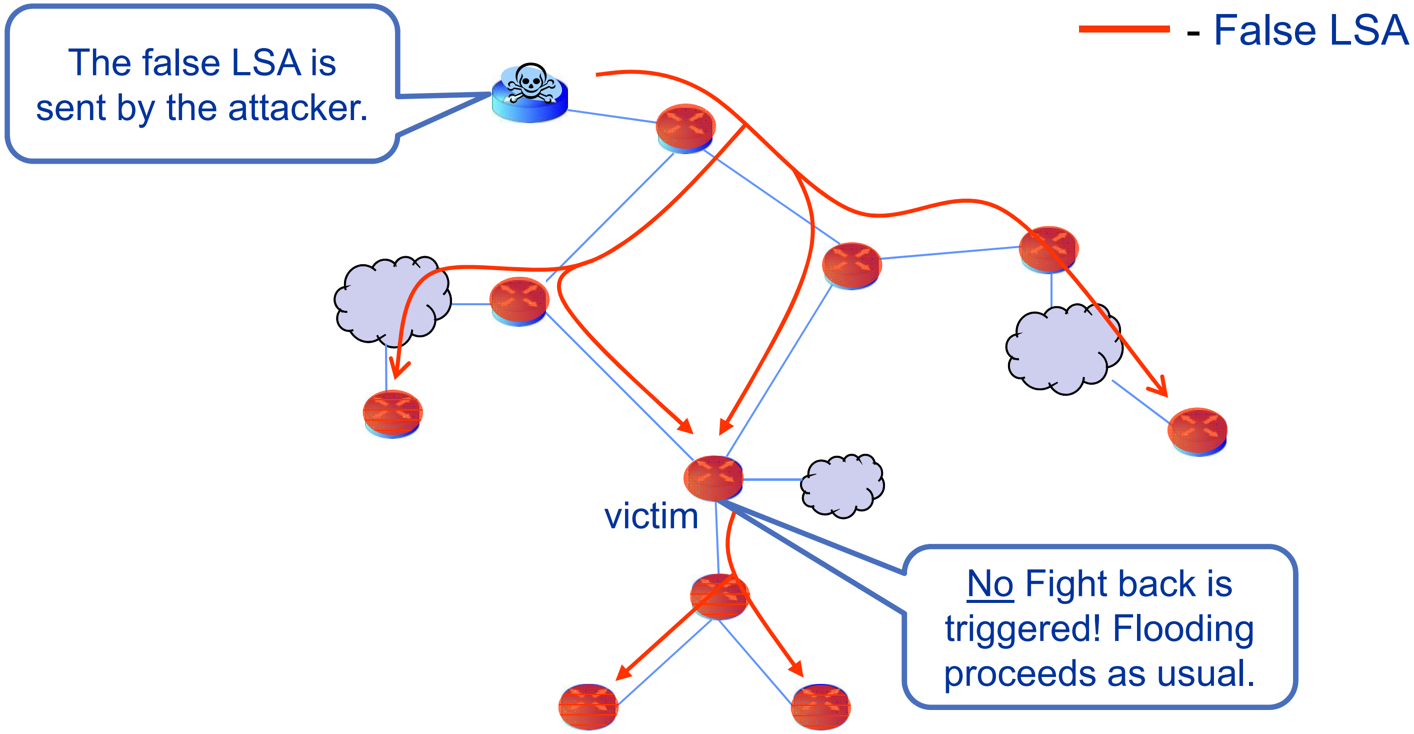
⇨ The two fields must have the same value.

- But, the OSPF spec does not specify a check to verify this on LSA reception!

The Vulnerability

- According to the OSPF spec (Sec. 13.4)
  - A router fights back only if it receives a false LSA in which
    - “the Advertising Router is equal to the router's own Router ID”
- If the victim router receives a false LSA having:
  - Link State ID = victim router’s ID
  - Advertising Router ≠ victim router’s ID
- Then, no fight back is triggered by the victim!
  - This is despite the fact that the LSA claims to describe links of the victim router itself.

Illustration


- False LSA
The false LSA is sent by the attacker.
victim
No Fight back is triggered! Flooding proceeds as usual.

All routers install the false LSA in their LSA DBs! The OSPF spec guarantees it.

But wait, it’s not that simple…

- There should be a problem:
  - Remember Sec. 12.1? An LSA is identified by both:
    - Advertising Router, and
    - Link State ID
  - Hence, the false LSA has a different identifier than that of the valid LSA (different Advertising Router fields).
    - This means that the two LSAs are different from the OSPF point of view.
  - This potentially makes the attack futile
    - The false LSA is installed in the LSA DB, but may simply be ignored by all routers while they keep using the valid LSA

Ambiguity

- On the other hand, according to the OSPF spec (Sec. 16.1)
  - During the routing table calculation LSAs are looked up in the LSA DB
    - “This is a lookup … based on the Vertex ID“ only!
      - Vertex ID = Link State ID
- This is an ambiguity in the spec
  - According to Sec. 12.1 an LSA is identified by the tuple (Link State ID, Adv. Router).
  - On the other hand, according to Sec. 16.1 an LSA is looked up by the Link State ID only.

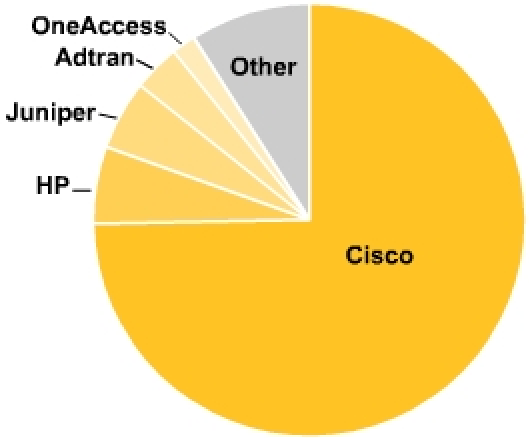
Ambiguity (cont.)

- All the routers in the AS (including the victim!) have in their LSA DBs two LSAs with the same Link State ID.
  - the false LSA, and
  - the valid LSA.
- Which LSA will be considered during the routing table calculation?
  - The OSPF spec does not provide an answer…
  - Hence, this is implementation dependent

Cisco

- Holds about 75% of the global enterprise router market.

Top Enterprise Router Revenue Market Leaders in 1Q12



© Infonetics Research, *Enterprise Routers Quarterly Market Share, Size, and Forecasts*, May 2012

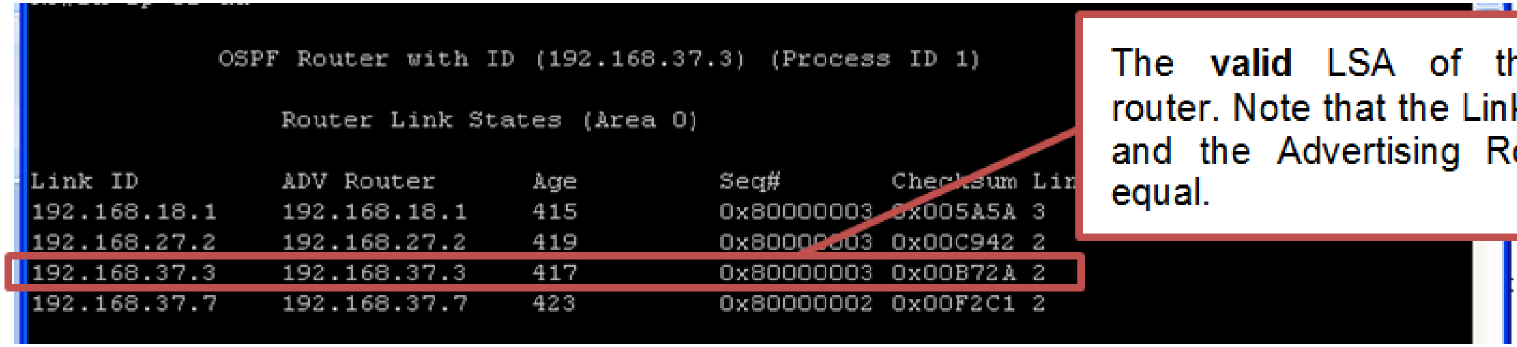
Validation on Cisco

- We use GNS3 emulation software with production IOS image.
- Cisco IOS 15.0(1)M
  - Almost latest IOS version.
    - This is the latest version we can get our hands on.
- 7200-series routers.
- The Scapy attack scripts are attached.

Validation on Cisco (cont.)

- Findings:
  - A false LSA with higher seq. num. than that of the valid LSA will replace the valid LSA in the LSA DB.
    - This happens in all routers including the victim!

before



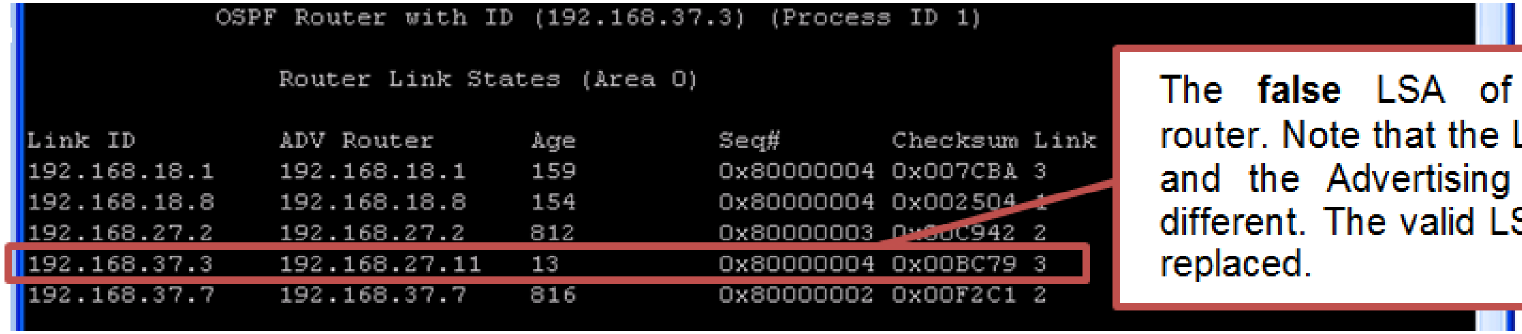
```
            OSPF Router with ID (192.168.37.3) (Process ID 1)

                Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Lin
192.168.18.1    192.168.18.1    415         0x80000003 0x005A5A 3
192.168.27.2    192.168.27.2    419         0x80000003 0x00C942 2
192.168.37.3    192.168.37.3    417         0x80000003 0x00B72A 2
192.168.37.7    192.168.37.7    423         0x80000002 0x00F2C1 2
```

The **valid** LSA of the victim router. Note that the Link State ID and the Advertising Router are equal.

after



```
           OSPF Router with ID (192.168.37.3) (Process ID 1)

               Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link
192.168.18.1    192.168.18.1    159         0x80000004 0x007CBA 3
192.168.18.8    192.168.18.8    154         0x80000004 0x002504 1
192.168.27.2    192.168.27.2    812         0x80000003 0x00C942 2
192.168.37.3    192.168.27.11   13          0x80000004 0x00BC79 3
192.168.37.7    192.168.37.7    816         0x80000002 0x00F2C1 2
```

The **false** LSA of the victim router. Note that the Link State ID and the Advertising Router are different. The valid LSA has been replaced.

Validation on Cisco (cont.)

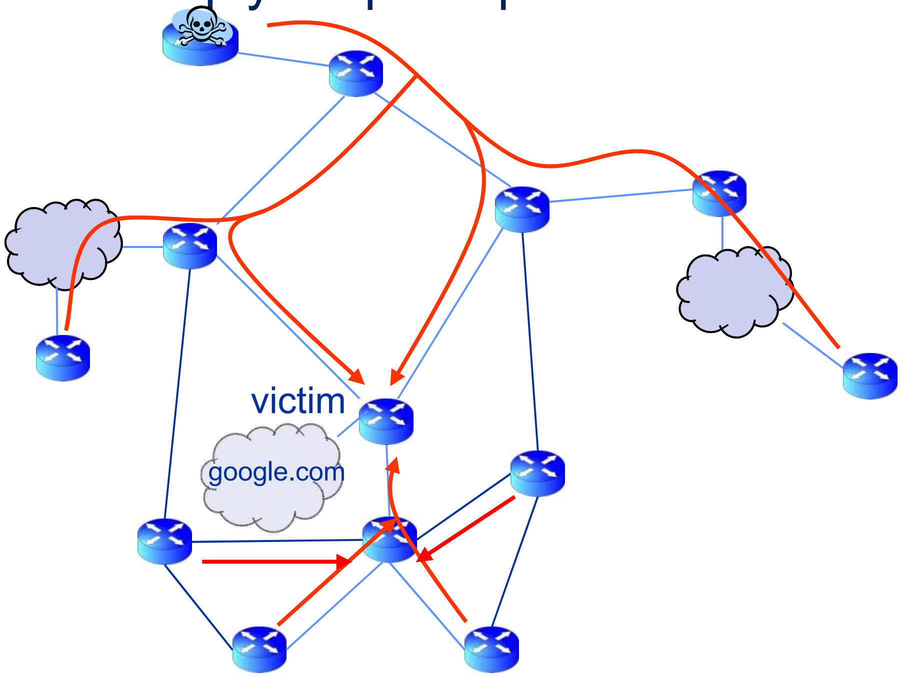
- Findings (cont.):
  - All the routers consider the false LSA during their routing table calculation!
    - All routers except the victim build their routing table accordingly.
  - The victim’s routing table is erased.
    - No OSPF path is calculated.
      - This probably happens since Cisco’s OSPF implementation fails to find in the LSA DB during the routing table calculation an LSA with an Advertising Router field that equals to the current router ID.

Validation on Cisco (cont.)

- The victim’s routing table erasure is persistent!
  - The victim can not recover spontaneously.
  - The OSPF process must be re-initialized.
- If it wishes, the attacker can undo the erasure by sending another false LSA but with an Advertising Router = victim’s ID.
- The victim will fight back and the valid LSA is reinstalled.

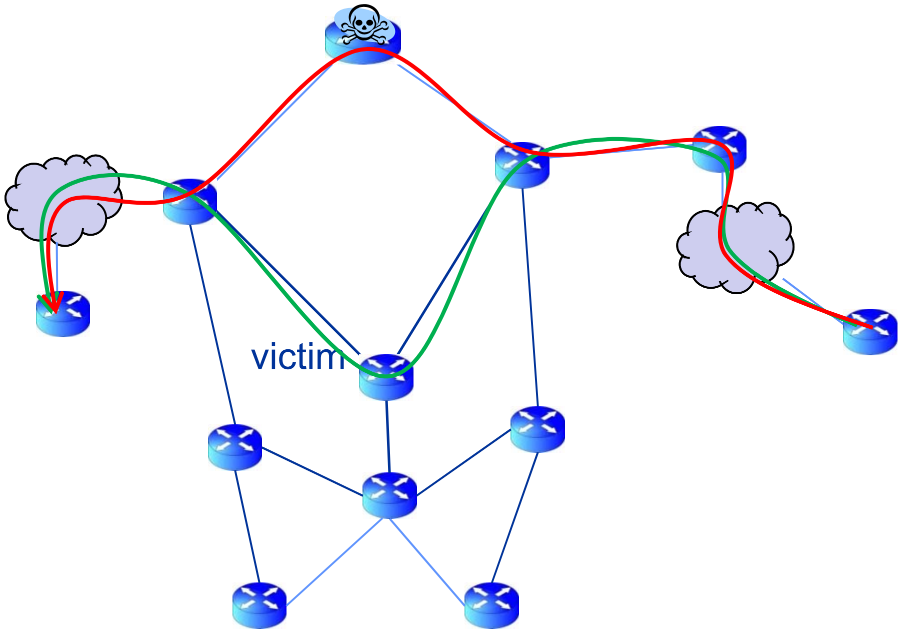
Attack Application Example #1

- Black hole
  - The false LSA announces that the victim router is directly connected to some external destination (e.g. the IP range of google.com)
  - All AS traffic to that destination will be directed to the victim router which will simply drop the packets.



Attack Applications Example #2

- Traffic diversion
  - The false LSA announce no links for the the victim router
  - All traffic will circumvent the victim.
    - Taking alternative routes, if such routes exist.
    - If not, the AS is partitioned.
    - Green and red paths are before and after the attack, respectively.



Conclusions

- We have presented a new attack the exploits the ambiguity in the OSPF spec.
- The attack is successful against a Cisco router
  - Potentially many other commercial routers may be vulnerable.
- **Using this attack one can control the routing domain from a single router.**