Owning the Routing Table

New OSPF Attacks

Alex Kirshon[1], Dima Gonikman[1], Dr. Gabi Nakibly[1,2]

[1] Technion, CS department

[2] National EW Research and Simulation Center
Rafael – Advanced Defense Systems Ltd.

Introductions

- Network security researcher
  - National Electronic Warfare Research & Simulation Center (part of Rafael – Advanced Defense Systems Ltd.).
  - High-end research and consulting services to organizations aiming to defend their information assets.
- Adjunct researcher and lecturer
  - The Technion (Israel Institute of Technology)

Overview

- We present newly found vulnerabilities in the OSPF protocol.
  - The most popular intra-AS routing protocol
- Allowing to remotely own a router's routing table without having to own the router itself.
- Why is this so desirable?
  - Traffic diversion
  - Routing loops
  - Network cuts
  - and much, much more…

Why is this so desirable?

- Gaining control over the routing table enables an attacker to do tricks such as:
  - Routing loops
  - Traffic diversion
    - towards longer routes or black holes
    - or through an attacker-controlled router
  - Network cuts
  - And much much more
- All this can be used to:
  - DoS the entire network (or parts thereof).
  - Eavesdropping on arbitrary traffic flows
    - which otherwise the attacker had no access to

Who is vulnerable?

- Potentially all commercial routers are vulnerable!
- The vulnerabilities were found in the spec of the OSPF protocol [RFC 2328].
- The attacks have been verified against Cisco IOS 15.0(1)M.
  - IOS's latest stable release

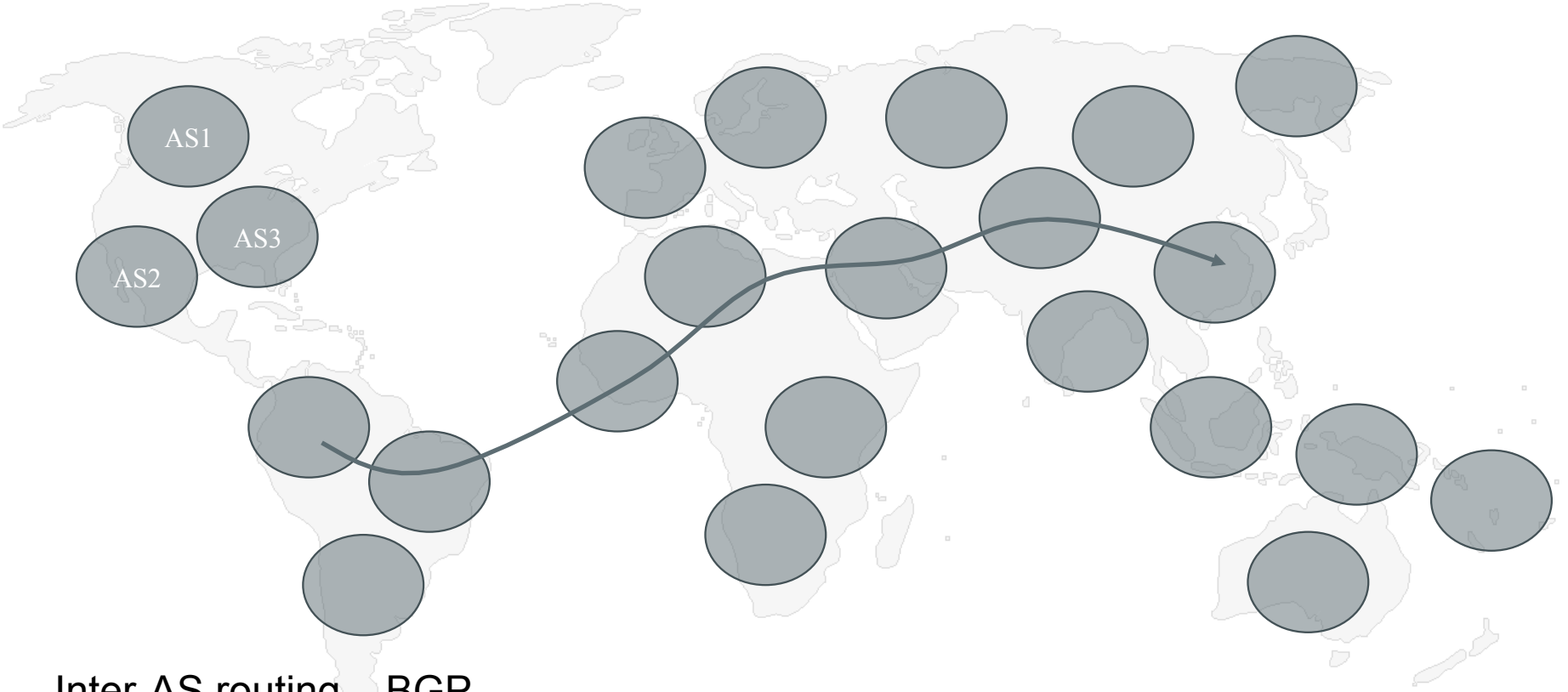
How the new attacks differ from known ones?

- Control over the routing tables is achieved by
  - falsifying or modifying routing advertisements of other routers in the AS
    - routers which the attacker may not control
- Known attacks:
  - Trigger “fight-back” by the router whose advertisement was modified
  - non-persistent effect
- The new attacks:
  - Evade “fight-back”
  - Persistent and stealthy

Agenda

- OSPF primer
- OSPF security strengths
- Known OSPF attacks
- The new found vulnerabilities and attacks

Internet Routing – The Big Picture

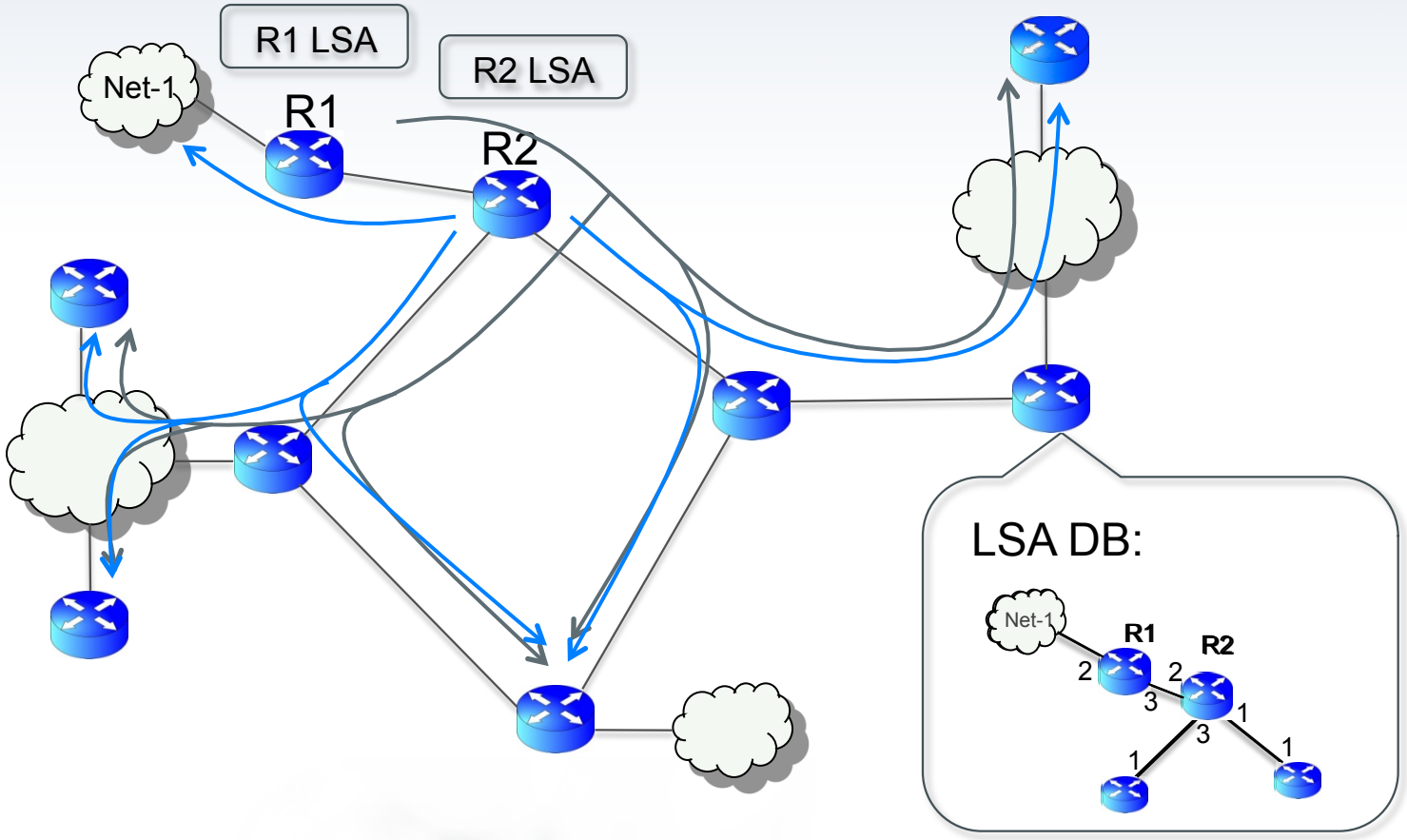


Inter-AS routing – BGP
Intra-AS routing – OSPF, RIP, IS-IS

OSPF Primer

- Every router periodically advertises its 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
  - Allowing it to build the topology map of the AS.
- A router processes every LSA addressed to it
  - via multicast or unicast.

How OSPF works?



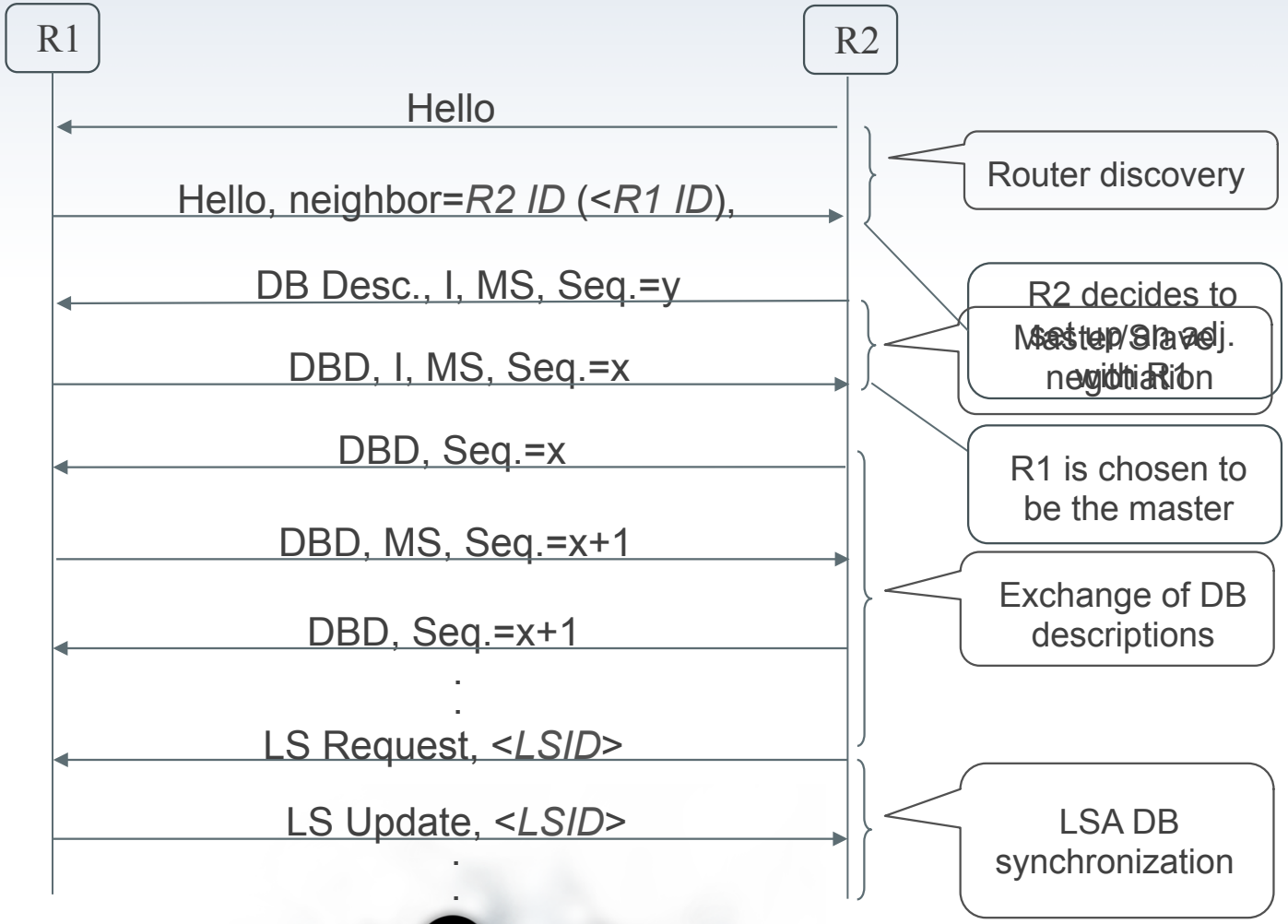
LSA Flooding

- An LSA is re-advertised every 30 minutes.
- Each LSA has a higher sequence number then its predecessor
  - An LSA with a higher seq. number always runs over one with a lower seq. number.

Discovering Neighbors

- To discover their neighbors the routers use the Hello protocol.
- After mutual discovery an adjacency may be set up between them.
  - By synchronizing their LSA databases.
- Once the adjacency is set up each router may include its peer in its LSA.

Setting Up Adjacencies



OSPF Security Strengths

- Per-link HMAC (MD5) authentication
  - Every link has its own shared secret
- Every LSA is flooded throughout the AS
- The “fight back” mechanism
- One LSA holds only a small part of topology information
- Links must be advertised by both ends
  - Bidirectional requirement

The Attacker

- Location: inside the AS
  - Controls a single legitimate router in an arbitrary location
  - Knows the MD5 shared secrets on the attached links
    - The first attack assumes that this secret is the same for all links;
    - The second attack does not assume this.
- Goal: Control the routing tables of other routers in the AS.

Known Attacks

- Falsifying self LSAs
  - Falsify cost to an existing neighbor
    - very limited
  - Advertise links to networks outside the AS
    - Can not influence routing to networks within the AS.
  - Advertise links to stub networks
    - One-track tool. Can only be used to attract traffic.
  - Advertise links to transit networks or existing routers
    - Does not influence the routing tables due to the bidirectional requirement

Known Attacks (cont.)

- Falsifying other routers' LSAs
  - Known examples: Seq++, MaxSeq,…
  - Triggers immediate fight back
    - A non-persistent attack
    - Not very stealthy
- Impersonating a phantom router
  - Overwhelming the DB LSA with garbage LSAs
  - Does not have an affect on the routing table
    - due to the bidirectional requirement;
      - No real router advertises a link to the phantom.

Known Attacks (cont.)

- The only known attack that evades “fight-back”:
  - Periodic Injection
    - Vulnerability: a router can not flood an LSA more than once per MinLSInterval (5 sec. by default)
      - According to the spec a false LSA is flooded by the victim and only then a fight-back in sent.
    - The false LSA is repeatedly advertised at a high rate
    - The victim can not advertise its “fight-back” LSA
  - This is a very high-maintenance attack
    - No hit-and-run
    - Not stealthy

Known Attacks – Summary

- It is the common conception that even if the attacker is an insider having the MD5 secret it can not persistently falsify the LSA of a router it does not control.
  - Hence, OSPF attacks can not significantly poison the routing tables of other routers.
- The new attacks we shall now present shatter this misconception.

The New Attacks

- Attack #1 – Remote False Adjacency
  - Make another router include a non-existing link in its LSA
  - Assume MD5 shared secrets are the same for all links
- Attack #2 – Disguised LSA
  - Falsify the entire LSA of another router
  - Does NOT assume anything about MD5 shared secrets

Attack #1 – Remote False Adjacency

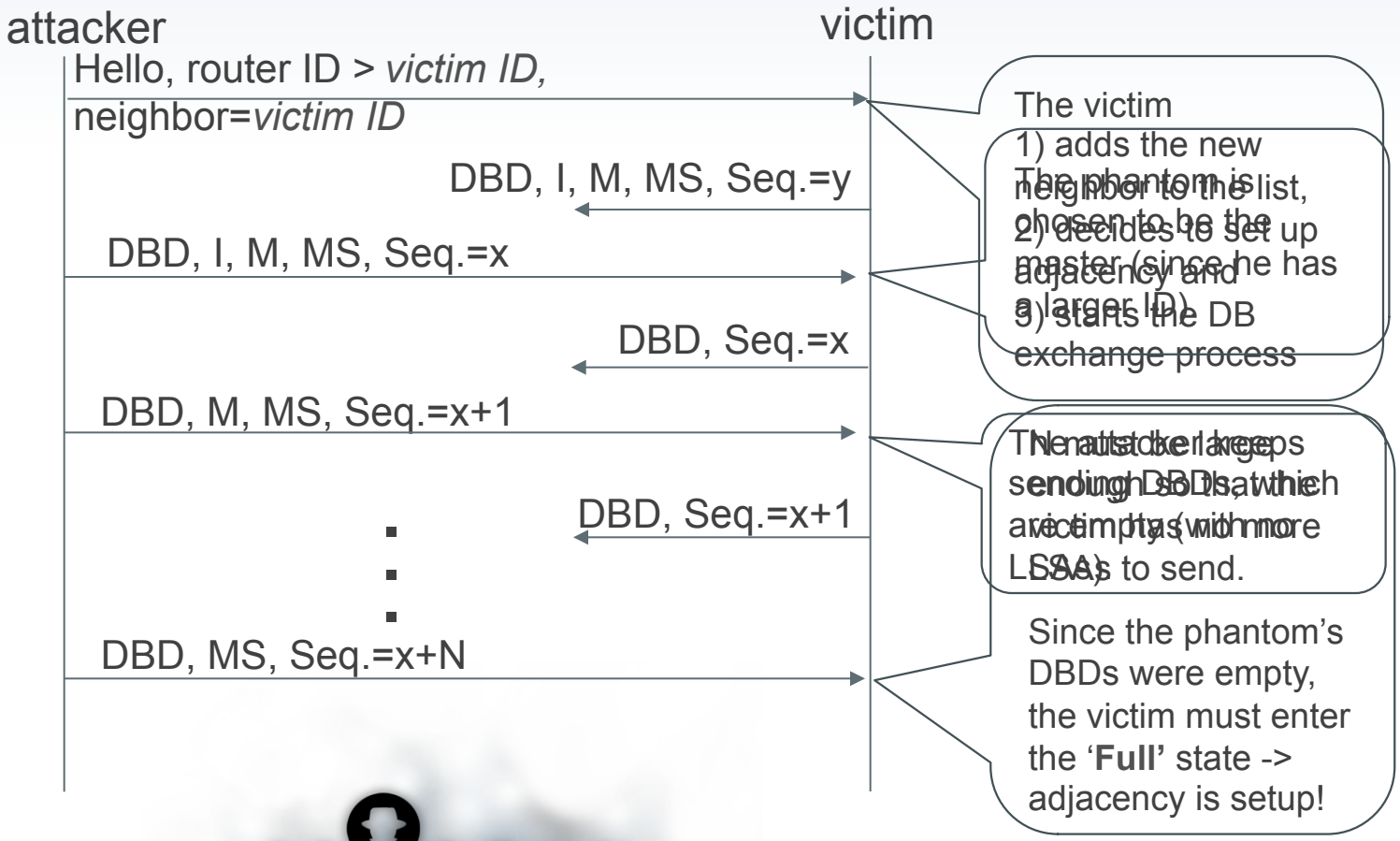
- The vulnerability
  - A master router can successfully complete the adjacency setup without actually seeing the messages sent by the slave router [RFC 2328 Sec. 10.8].
- The attack
  - A victim router is made to believe there is a new (actually, phantom) router on its LAN.
  - An adjacency is set up remotely between it and the phantom router.
  - This affects the LSA of the victim router without actually controlling it.

Assumptions

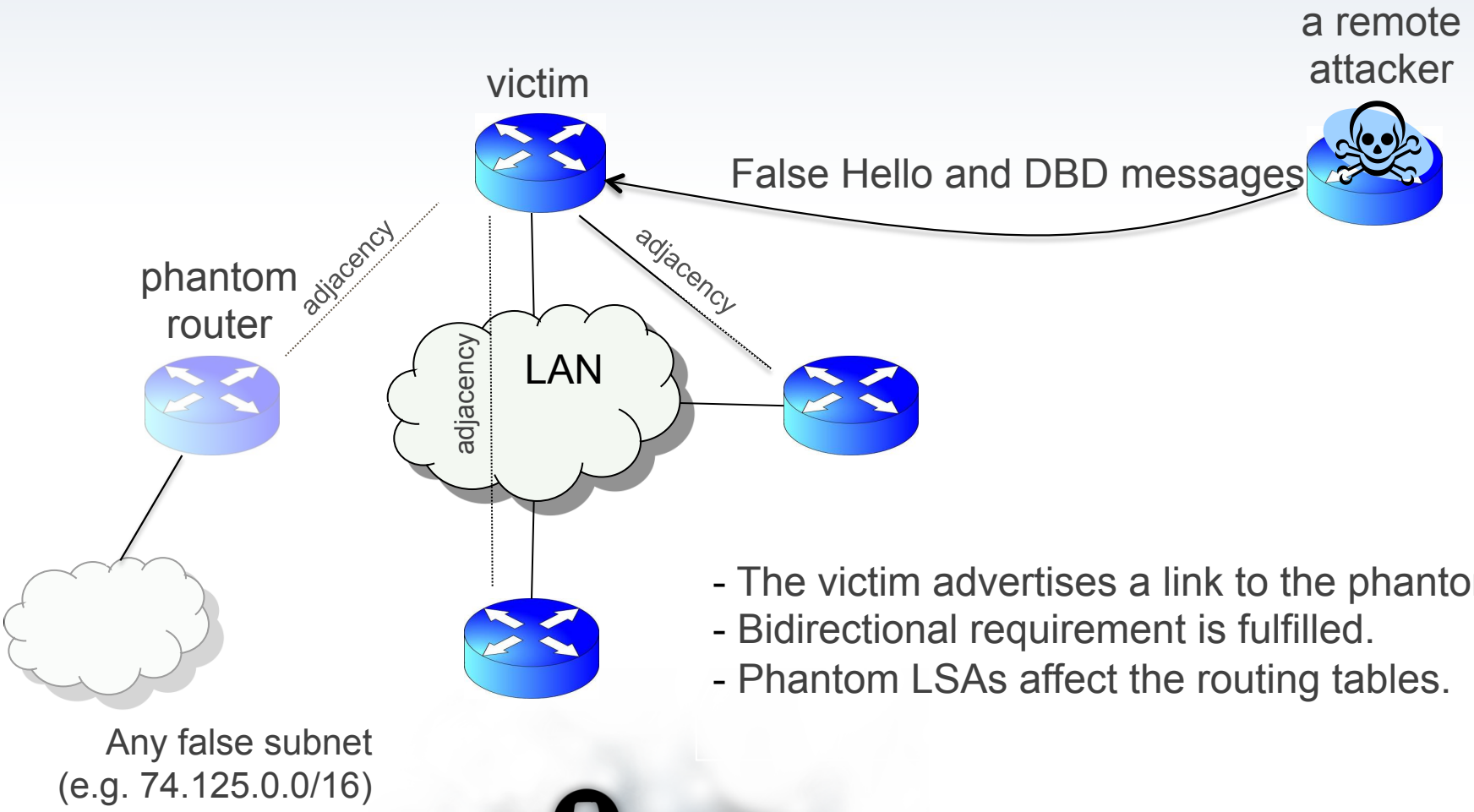
- The attacker knows the shared secret of the remote LAN.
  - In most cases this is the same shared secret for all LANs in the AS.
- The attacker knows the configuration parameters of the remote LAN
  - e.g., HelloInterval, RouterDeadInterval,…
  - In most cases these are the same parameters for all LANs in the AS.

The Attack Sequence

- In all attacker-originated packets:
  - IP source = <*spoofed phantom IP address*>



The impact



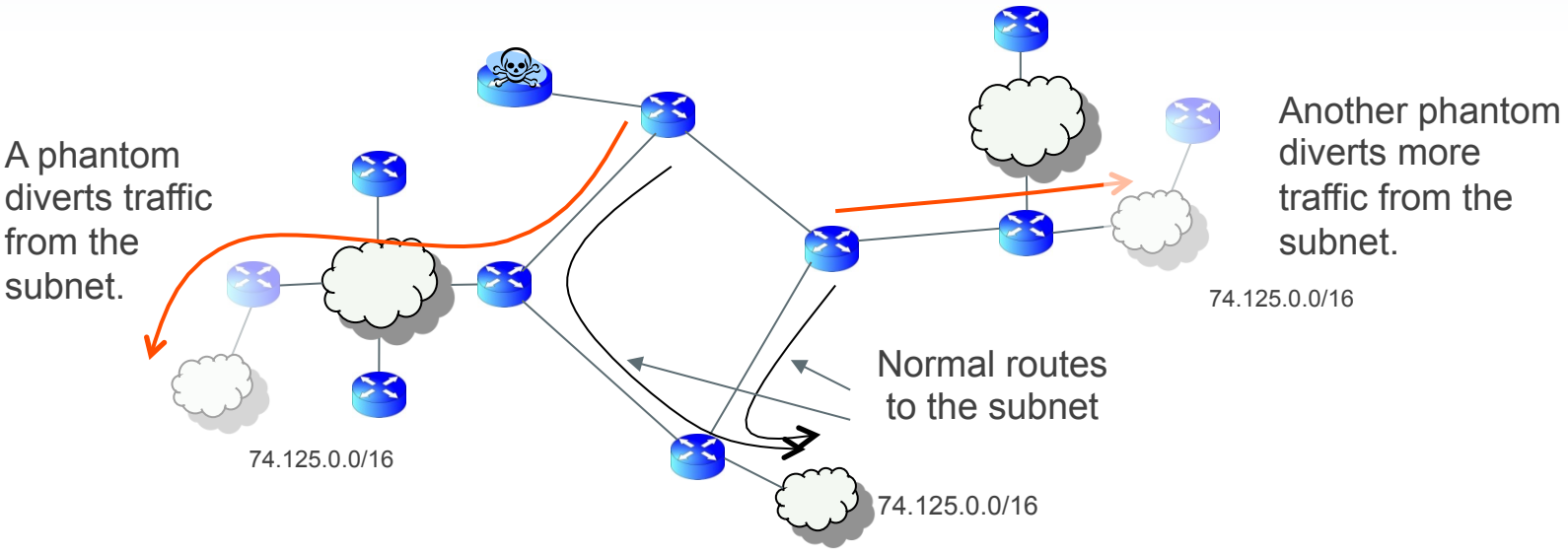
- The victim advertises a link to the phantom!
- Bidirectional requirement is fulfilled.
- Phantom LSAs affect the routing tables.

The Impact

- The DR advertises a link to the phantom router.
  - The attacker has managed to affect the LSA of the victim.
  - The link between the phantom and the LAN is now bidirectional.
    - This is the crux of the attack!
- The attacker advertises arbitrary LSA on behalf of the phantom router.
- All routers will consider the LSA of the phantom while calculating their routing tables.
  - This is why the attack is powerful.

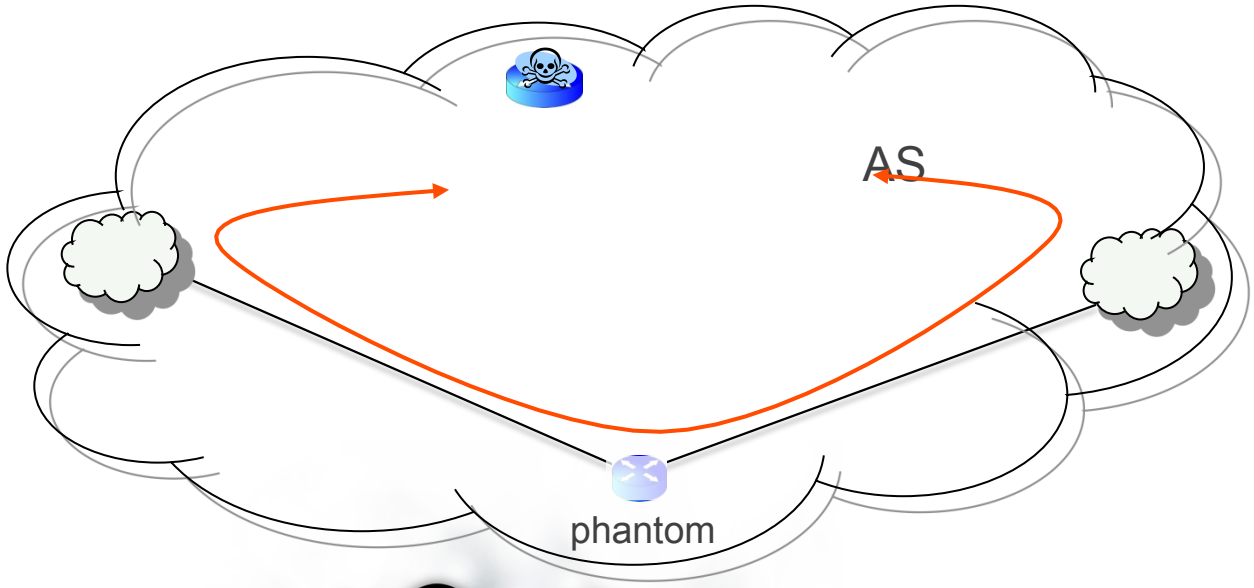
Potential use case

» The attacker can black hole traffic from all over the AS to a specific subnet.



Another Potential Use Case

- A strategic “location” of the phantom can black hole most of the traffic in the AS.
- For example, connect the phantom to two remote LANs.
  - The phantom appears to be a very desirable shortcut…



Caveats

- The adjacency must be maintained by sending an Hello message every RouterDeadInterval.
  - 40 seconds, by default
- The victim floods LSAs to the phantom and expects Acks.
  - According to the OSPF spec the victim will endlessly retransmit the LSAs over and over.
    - Nonetheless, a Cisco router gives up after 125 seconds and then tears down the adjacency.

Attack #2 – Disguised LSA

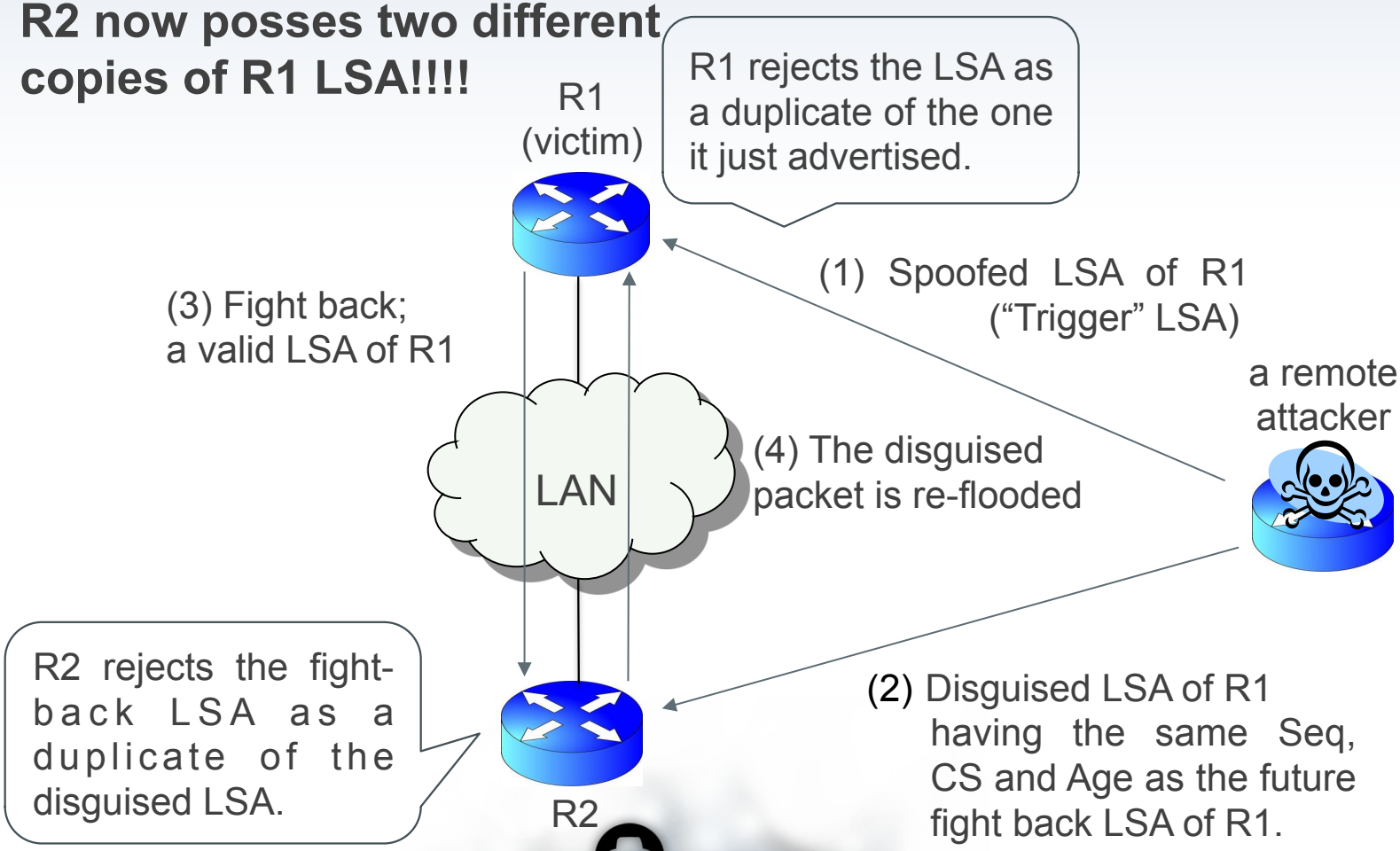
- The vulnerability
  - Two different instances of an LSA are considered identical if they have the same [RFC 2328 Sec. 13.1]:
    - Sequence number
    - Checksum
    - Age (+/- 15 minutes)
  - The actual payload of the LSA is not considered!
- The attack
  - Advertise a false LSA having the same values for these three fields as a valid LSA.
    - The benefit: no fight back is triggered since the victim views the false LSA as a duplicate of the LSA it just advertised.

Attack #2 – Disguised LSA (cont.)

- The attack (cont.)
  - But, there is a problem: all other routers in the AS will also consider the false LSA as a duplicate
    - therefore, they will not install it in their LSA DB.
  - Solution: Disguise the LSA to the next valid instance of the LSA
    - While at the same time trigger the victim to originate this next valid instance
      - The trigger is done using the fight-back mechanism

Illustration

The final outcome: R1 and R2 now posses two different copies of R1 LSA!!!!



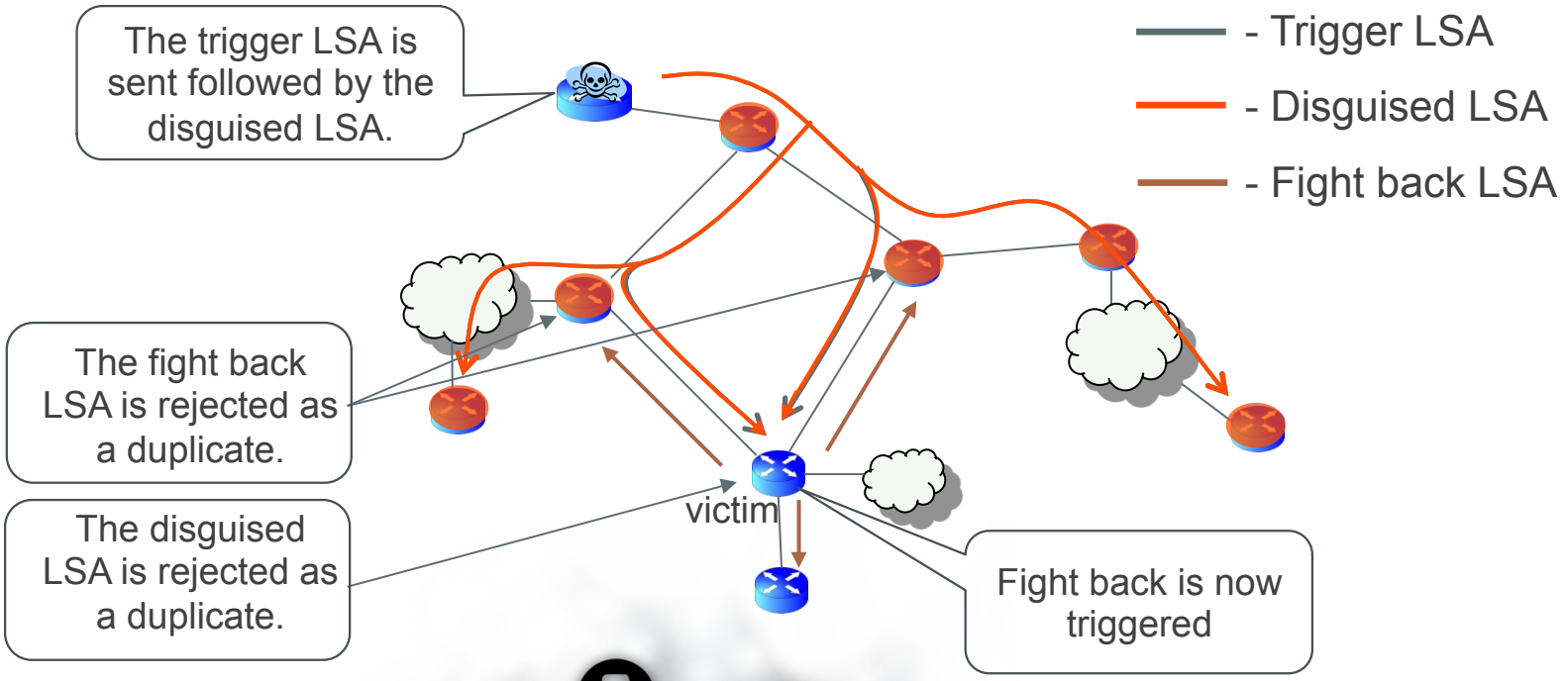
How the disguised LSA can be crafted?

- Age: this is the easiest one.
  - The disguised LSA will be advertised within 15 minutes of the valid (fight back) LSA.
- Sequence: the value is always incremented by one.
  - The disguised LSA will have the sequence of the trigger LSA plus 1.
- Checksum: this is the hardest feat, but not that hard.
  - The content of the next valid LSA is deterministic and predictable, hence the checksum is also predictable.
  - A dummy Link entry in added to the payload of the LSA.
  - The value of this entry is calculated such that the entire LSA will have the desired checksum.
    - This can be done since a checksum is a 16-bit result of a linear calculation on the LSA octets.

Potential Use case

» The attacker floods consecutively the trigger and then the disguised LSA.

- No need to know the MD5 key of the victim.



The Impact

- An effective tool to persistently falsify an LSA of a router not controlled by the attacker.
- All/most of the routers in the routing domain have a false LSA of the victim router.
- Can be repeated for different victim routers to fully control the topology viewed by the routers in the AS and consequently their routing tables.
  - This allows to create routing loops, network cuts, traffic diversion, etc.

Validation of the Attacks

- Both attacks are based on analysis of the OSPF specification [RFC 2328].
- The attacks are successful against Cisco IOS 15.0(1)M.
  - On a 7200-series router.
- The Scapy attack scripts are included in the disc.

Conclusions

» Up until now the common conception was that even if the attacker is an insider it can not persistently falsify the LSA of a router it does not control.

- The new attacks shatter this misconception.
- **Using these attacks one can control the entire routing domain from a single router.**

Questions?

gabin@rafael.co.il

Feedback

- Please complete the Speaker Feedback Surveys.
- This will help speakers to improve and for Black Hat to make better decisions regarding content and presenters for future events.