Experiment 5

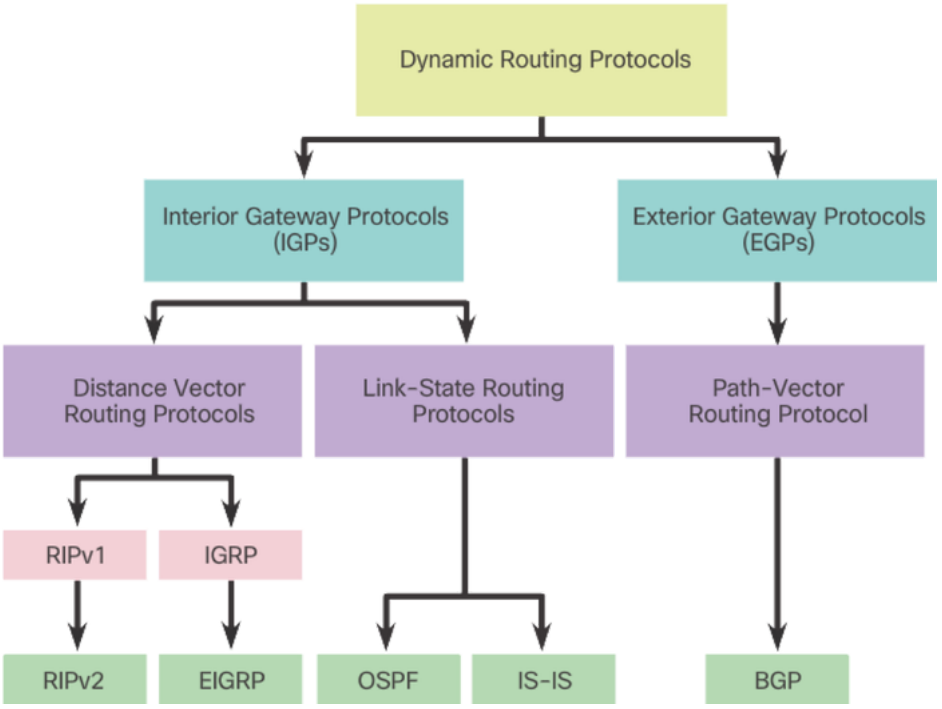
Name	Ameya S. Daddikar
College I.D.	161070015
Course	Btech. Computer Engineering

Aim

To study Routing Protocol attacks and defence mechanism.

Theory

Given below is a classification of various routing protocols. We will be looking for exploits and defenses for RIP, BGP and OSPF protocols.



RIP

Routing Information Protocol developed in 1980s used in small/medium networks, RIP is a distance vector routing protocol which use hop count as a routing metric, rip is able to route information across the network up to 15 hops. RIP support IPv6 in his newest version (RIPv2).

RIPv1 is extremely vulnerable to serious attack.

Attacks

The basic idea is to keep issuing fake RIP Response messages, containing basically whatever we need (in terms of routes). The other routers will eventually insert our malicious entries in they tables and start routing the packets accordingly.

Normally, RIP Response messages are sent to the dedicated multicast address 224.0.0.9, but the same messages seem to be accepted even when their destination IP address is a specific router. This is great, from an attacker point of view, because it allows he or she to be surgical in the injection process.

Other attacks

1. Forging RIP messages
   Spoofing source address and sending invalid routes, altering traffic flow.
   - Traffic Hijacking
   - Traffic Monitoring
   - Redirecting traffic from trusted to untrusted.
2. Obtaining Cleartext RIPv2 "password" when sent across network.
   Using retrieved password to send authenticated updates to RIPv2 routers, altering traffic flow with consequences listed above.

Defenses

- Disabling RIPv1 and using RIPv2 with MD5 authentication.
- Enabling MD5 based authentication for RIPv2
- Disabling RIP completely and using OSPF with MD5 authentication as interior gateway protocol. OSPF is the suggested IGP.

OSPF

Open shortest Path first developed in 1998 is a link state routing protocol that use metric as a routing metric, this protocol in enable to discover the network using identification messages (LSA).

There are three version of the protocol:

- OSPFv1: described in RFC 1131 (has never gone beyond the experimental phase, as far as I know);
- OSPFv2: described in RFC 2328, it superseeds v1 and it is the version deployed worldwide for dealing with IPv4 networks;
- OSPFv3: it supports IPv6 and is described in RFC 6340.

Attacks

There are various attacks known against OSPF (see on Google Scholar), but they are normally able to “only” generate a DoS condition.

In 2011, Alex Kirshon, Dima Gonikman, Dr. Gabi Nakibly demonstrated an attack, during the Black Hat USA, that was able to circumvent the fightback packets.

The idea behind the attack is quite simple.

Imagine two neighbours routers, A and B. The attacker generates two packets, one sent to the victim router A to trigger the fightback and another sent, at the very same time, to the router B inside which the malicious routes have to be injected. The fightback packet, sent by A is received by B after the malicious one and it is discarded because seen as identical, even though the content of the two packets is different.

This is possible because two OSPF LSA (Link State Advertisement) packets are considered identical if they have:

- the same sequence number;
- the same 16 bits checksum value;
- approximately the same age (within a 15 minutes time difference).

The sequence number and the age are quite easy to spot and fake, while the checksum has to be calculated. Luckily, it can be predicted, because it is calculated on LSA fields that have values that can be inferred in advance.

Other attack

Forging OSPF messages : Can be somewhat difficult but theoretically possible if no authentication required or cleartext password obtained.

Solution

Enable MD5 Authentication in OSPF implementation.

BGP and EGP

Border Gateway Protocol is the internet standard External Gateway
Protocol (EGP) was designed to exchange information and routing updates between different autonomous system, BGP is a Path vector Protocol and it makes routing decisions based on path, network policies, or rule-sets.

Attacks: BGP Hijacking

BGP hijacking is an illicit process of taking control of a group of IP prefixes assigned to a potential victim. Either intentionally or accidentally, it is achieved by changing paths used for forwarding network traffic, exploiting the weaknesses of BGP. The aim of this blog post is to explore these weaknesses and to discuss possible countermeasures.

- Partial BGP Hijacking
  A partial BGP hijacking occurs when two origin Autonomous Systems announce an identical IP prefix with the same prefix length. The BGP best path selection rules, such as preferring the shortest AS path, determine which path is the best.

- Complete BGP HIjacking
  The complete BGP hijacking occurs when an attacker announces de-aggregated thus a more specific IP prefix than the actual owner of the prefix.

Filtering IP prefixes on Tier 3 ISP and customer side, however, can reduce occurrence of BGP hijacks.

Defenses

Limit AS_PATH in Announced Prefixes
We can limit the AS_PATH in announced prefixes using BGP AS path filter. The regular expression ^$ in ACL statement matches empty AS_PATH thus it allows only locally announced prefixes being sent to ISP.

ip as-path access-list 1 permit ^$

router bgp 64502
neighbor 200.1.1.1 filter-list 1 out

The lines above are applied on the customer router (AS64502) towards ISP (AS64500) BGP peer address 200.1.1.1. The AS64502 is added to ASP_PATH after the filter is applied. The configuration prevents customer AS64502 to become transit AS in case of a multihomed connection. As a result, traffic sent from another ASs is not routed through customer but uses a high-speed link of upstream providers instead.

The ISP can also configure the AS_PATH filter towards customer BGP router 200.1.1.2.

ip as-path access-list 1 permit ^64502$

router bgp 64500
neighbor 200.1.1.2 filter-list 1 in

Announce Only Owned Prefixes
Now we create a prefix-list on a customer router that permits the announcement of only the assigned prefix 199.1.1.0/24. The list is applied toward ISP router. All other prefixes are not being sent.

ip prefix-list filter_out seq 10 permit 199.1.1.0/24

router bgp 64502
neighbor 200.1.1.1 prefix-list filter_out out

The ISP should only accept prefixes which have been assigned or allocated to its customer.

ip prefix-list as64502in seq 10 permit 199.1.1.0/24

router bgp 64500
neighbor 200.1.1.2 prefix-list as64502in in

Filter Own Prefixes and Accept only Prefixes with Length /24 and Less
Customers do not need to know about the path to their own prefixes so they should filter them. However, filtering the single prefix 199.1.1.0/24 is not sufficient. If someone announces customer prefix with the longer prefix length than /24 it would be installed into customer routing table. For this reason, we need to specify the prefix length to 32. The sequence 10 denies customer prefix 199.1.1.0 within the length from 24 to 32. The sequence 20 accept only prefixes that are not denied by a rule 10 and their prefix length is /24 and less.

ip prefix-list filter_in seq 10 deny 199.1.1.0/24 le 32
ip prefix-list filter_in seq 20 permit 0.0.0.0/0 le 24router bgp 64502
neighbor 200.1.1.1 prefix-list filter_in in

Filter Default Route
Unless customers do not need a default route they should block it. Sequence 10 denies a default prefix. All other routes are matched and permitted by sequence 20.

ip prefix-list filter_defaultin seq 10 deny 0.0.0.0/0
ip prefix-list filter_defaultin seq 20 permit 0.0.0.0/0 le 32router bgp 64502

Detecting BGP Hijacking
When the IP prefixes are hijacked, connection might be redirected and discarded as in the Pakistan Telecom incident. In this case detection of hijacking is an easy task since a service becomes unavailable. As for the BGP Man in the Middle attacks, when data might be intercepted or modified, detection is not so straightforward because the connection is working. BGP hijacking, however, can still be detected since the BGP AS_PATH attribute gets changed. Moreover, network traffic takes different (not optimal) path which leads to degraded performance and the increased round-trip time (RTT). Providers' Looking Glass (LG) servers or Route Views are great tools to discover a change in the routing paths.

Conclusion

Thus the routing protocol and the possible attacks on them are studied. Also their defence mechanisms are understood.