OSPF Hijacking

Matthew Driver
Jack Sadle

Integrated Information Technology
ROTC
University of South Carolina

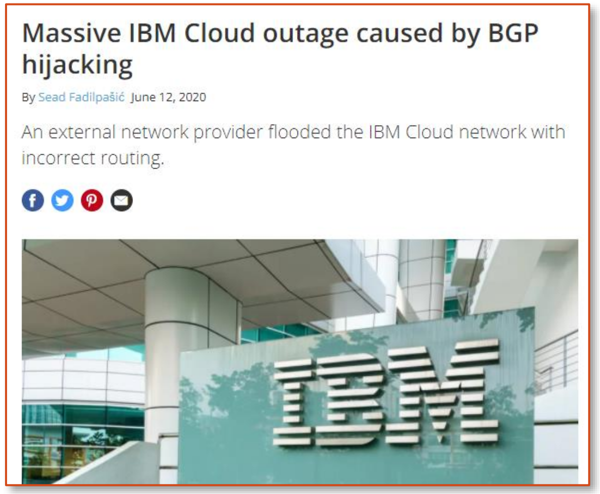
December 1st, 2020

Agenda

- Introduction
- Problem description
- Background information
- Open Shortest Path First
    - Hijacking
- Proposed solution and Implementation
- Conclusion

Problem Description

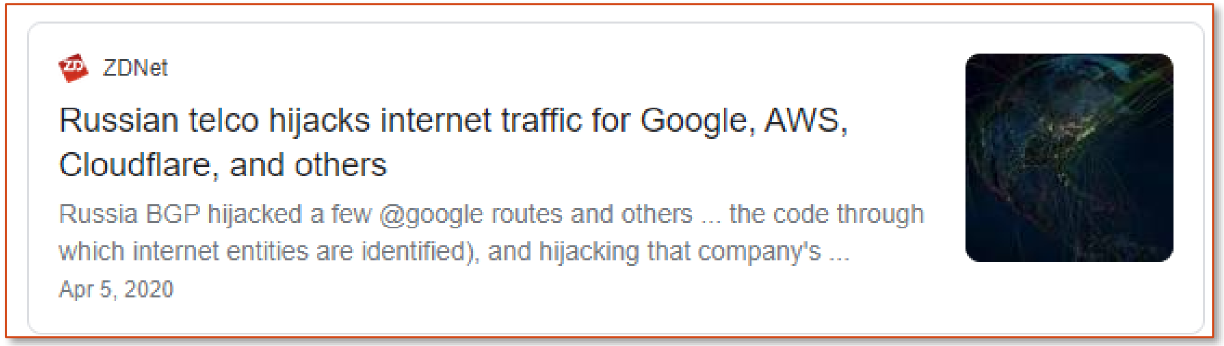
- Computer networks can be attacked by disrupting peer network routers.
- Using OSPF (Open Shortest Path First), routers send data to each other in a network via packets on routes that are established based on their distance to each other.
- In an OSPF network, the packet will take the shortest path along the routers in the network to get to their destination.
- Attackers can falsify the information carried within the routing protocols, thus hijacking IP addresses.
- This is done when an attacker manipulates the OSPF routing protocol so that traffic is misdirected to a rogue router projecting false routes.
- Attacks occur frequently across the world; e.g., see figure.



Massive IBM Cloud outage caused by BGP hijacking

By Sead Fadilpašić June 12, 2020

An external network provider flooded the IBM Cloud network with incorrect routing.



ZDNet

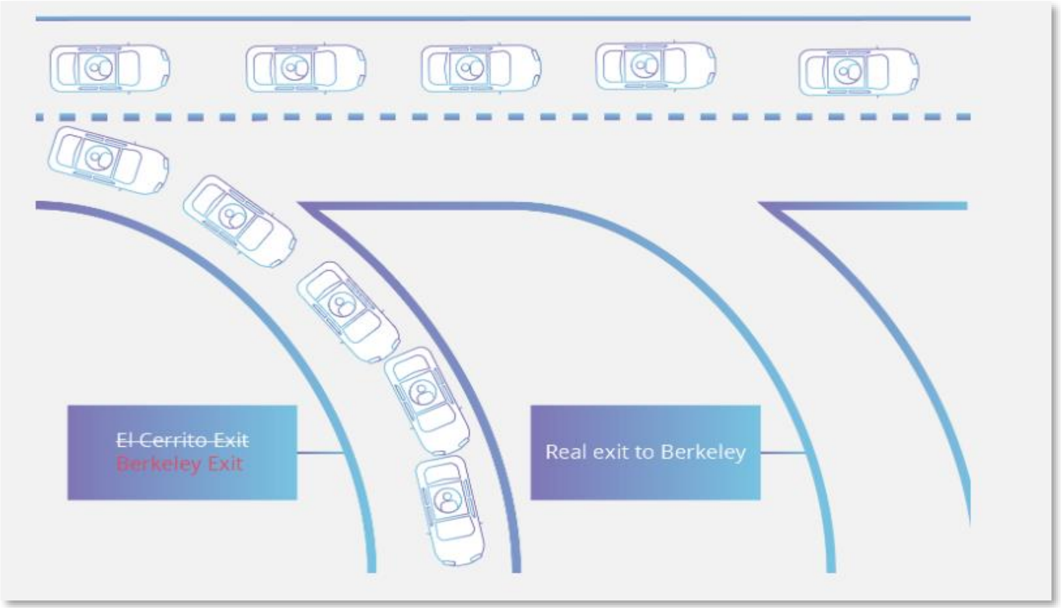
Russian telco hijacks internet traffic for Google, AWS, Cloudflare, and others

Russia BGP hijacked a few @google routes and others ... the code through which internet entities are identified), and hijacking that company's ...

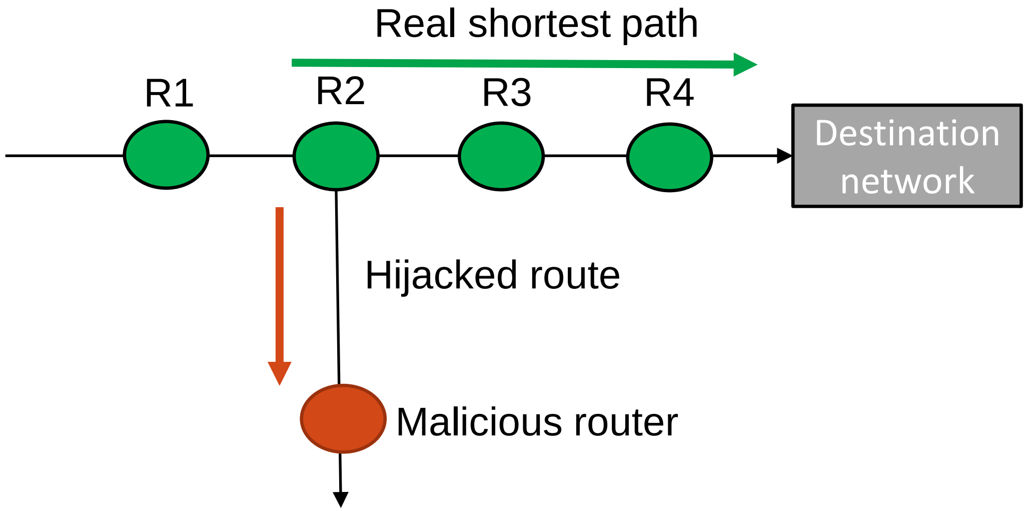
Apr 5, 2020

Problem Description

- Spoofing routing information can generally be used to cause systems to misinform (lie to) each other, cause a Denial of Service (DoS) attack, and redirect traffic to follow a path it would not normally follow.
- These kinds of threats to data security can cause the theft of information, shutdowns, and many other harmful results.



https://www.cloudflare.com/learning/security/glossary/bgp-hijacking/

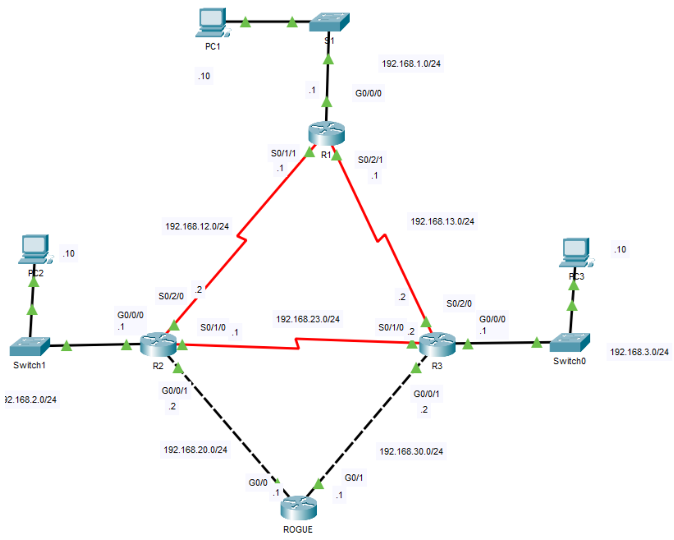


Background Information

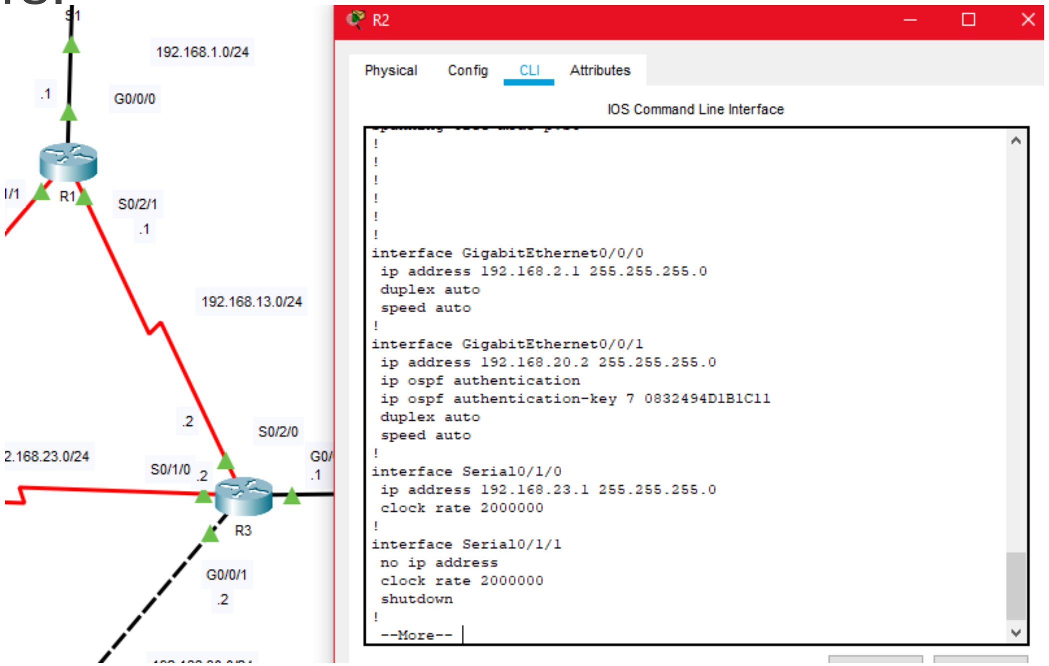
- OSPF is perhaps the most widely used routing protocol in the world.
- It was developed so that the shortest path through a network is calculated based on the cost of the route, taking in account the bandwidth, delay and load.
- OSPF routers are configured by adding the adjacent Local Area Networks (LANs) and Wide Area Networks (WANs) to its routing table.
- A router would add the networks connecting all other routers in order to establish OSPF communication with these devices.
- These entries in the routing table have established distances so that the OSPF protocol can identify the shortest path to a destination network.
- In order to hijack an OSPF route, a rogue router advertises a shorter route to a legitimate network, therefore adding itself as the more viable route in the routing table.

Proposed Solution and Implementation

- The proposed solution to minimize an attack on an OSPF network is to implement OSPF Authentication on each router. Each router should have a password to authenticate, each of different characters.



This is an OSPF Topology with an active spoofed router trying to infiltrate the network



```
!
!
!
!
!
!
interface GigabitEthernet0/0/0
 ip address 192.168.2.1 255.255.255.0
 duplex auto
 speed auto
!
interface GigabitEthernet0/0/1
 ip address 192.168.20.2 255.255.255.0
 ip ospf authentication
 ip ospf authentication-key 7 0832494D1B1C11
 duplex auto
 speed auto
!
interface Serial0/1/0
 ip address 192.168.23.1 255.255.255.0
 clock rate 2000000
!
interface Serial0/1/1
 no ip address
 clock rate 2000000
 shutdown
!
 --More--
```

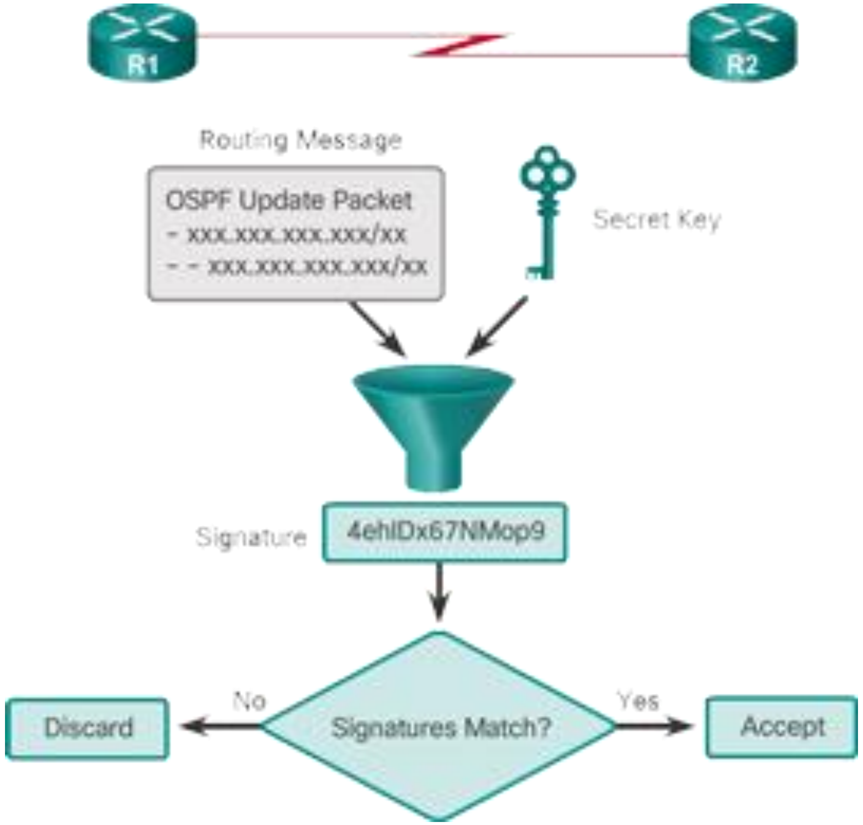
To combat security issues, we implement authentication measures on all routers through each interface

What is Router Authentication?

- Authentication is for security
- The risks of having no authentication means a rogue router may enter the network and gather data from the net
- OSPF supports 3 types of authentications:
  - Null (none)
  - Simple Password Authentication
  - MD5 Authentication
- MD5 is the safest method of authentication because it is calculated using the MD5 Algorithm and is never exchanged by peers.

Router Authentication Process

- R1 will combine the shared secret key with the routing message creating what is called a hash
- Using the MD5 Algorithm, a digital signature is calculated and sent to R2
- R2 will receive the message
- R2 will then combine the shared secret key with the routing message
- R2 will use the MD5 Algorithm to calculate the digital signature
- If the Digital signatures match, R2 will accept the OSPF update packets
- If the digital signatures do not match, R2 will not accept the OSPF update packets



Conclusion

- OSPF Hijacking can do massive damage with relative ease
- Attackers manipulate the OSPF routing protocol to steal network traffic
- Implementing authentication measures can help protect networks from these attacks