BGP Hijacking

Hannah Gardner & Jeremy Gill

Advisors: Jorge Crichigno & Jose Gomez

Department of Integrated Information Technology

University of South Carolina

December 2nd, 2021

Agenda

- Introduction
- Background Information
- Problem Description
- Proposed Solution
- Conclusion

Introduction

- The **Internet** is a network of networks, or autonomous systems (AS).
- **Border Gateway Protocol** (BGP) allows autonomous systems to connect to other autonomous systems.
- BGP offers **network stability** because it can find alternative routes in cases of route failures.

Background Information

- **BGP peers/neighbors** are two routers which have established a connection to exchange routing information.
- BGP peers **advertise networks** to update each peer's routing table.

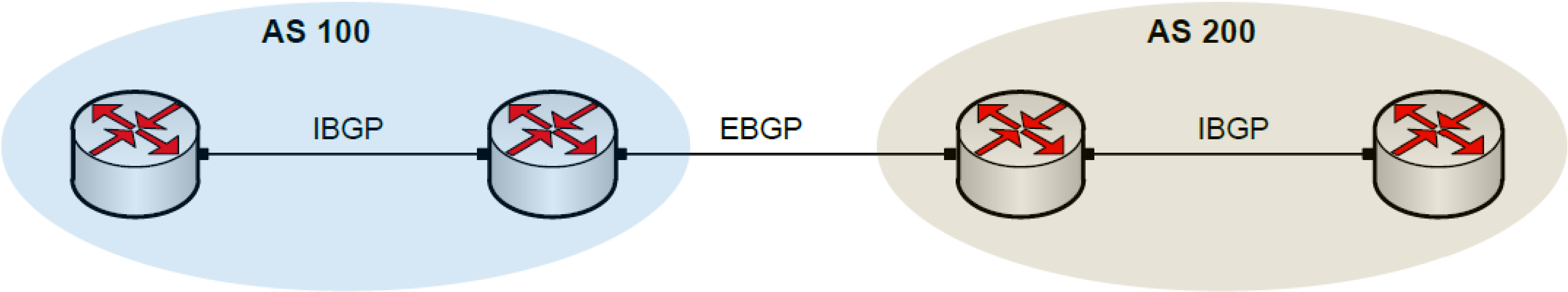


Fig 1: Two autonomous systems, AS 100 and AS 200 communicate through external BGP (EBGP)

Background Information

- **BGP hijacking** occurs when malicious routers advertise networks that do not belong to them (i.e., impersonating legitimate routers).

- Consequently, the attacker can **reroute** Internet traffic.

- This traffic can be **monitored or redirected**, resulting in performance degradation.

Problem Description

- BGP routes can be **hijacked** when a malicious actor spoofs route information.

- In this scenario, there are 2 networks, LAN 1 and LAN 2. A malicious router advertises that it is LAN 2, therefore **redirecting traffic** moving from LAN 1 to LAN 2 to itself.

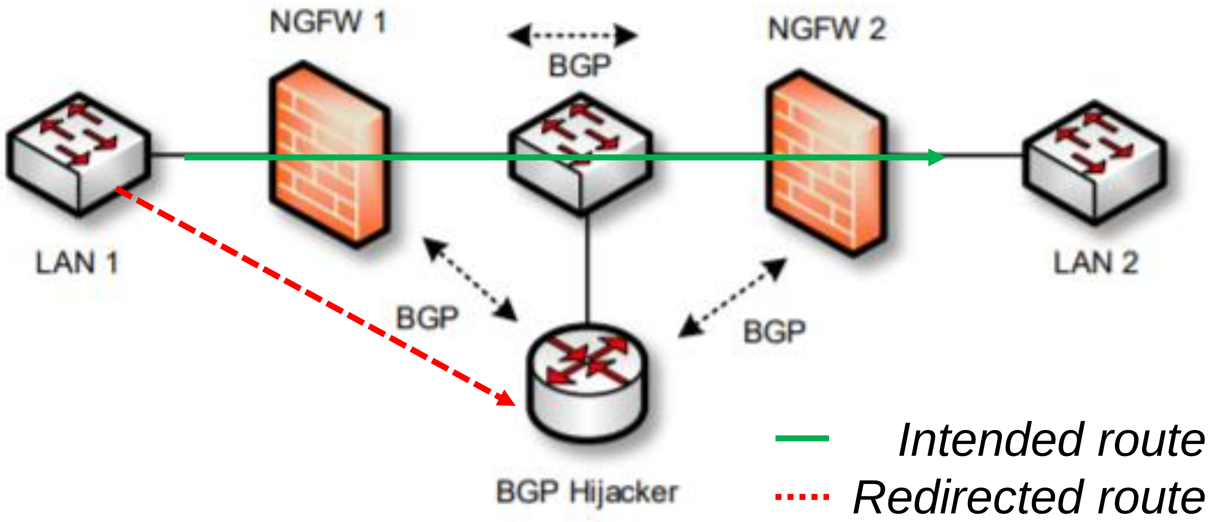


Fig. 2: Traffic is redirected from its intended recipient to a malicious actor via spoofing.

Proposed Solution

- **BGP authentication** adds a layer of security between trusted peers.

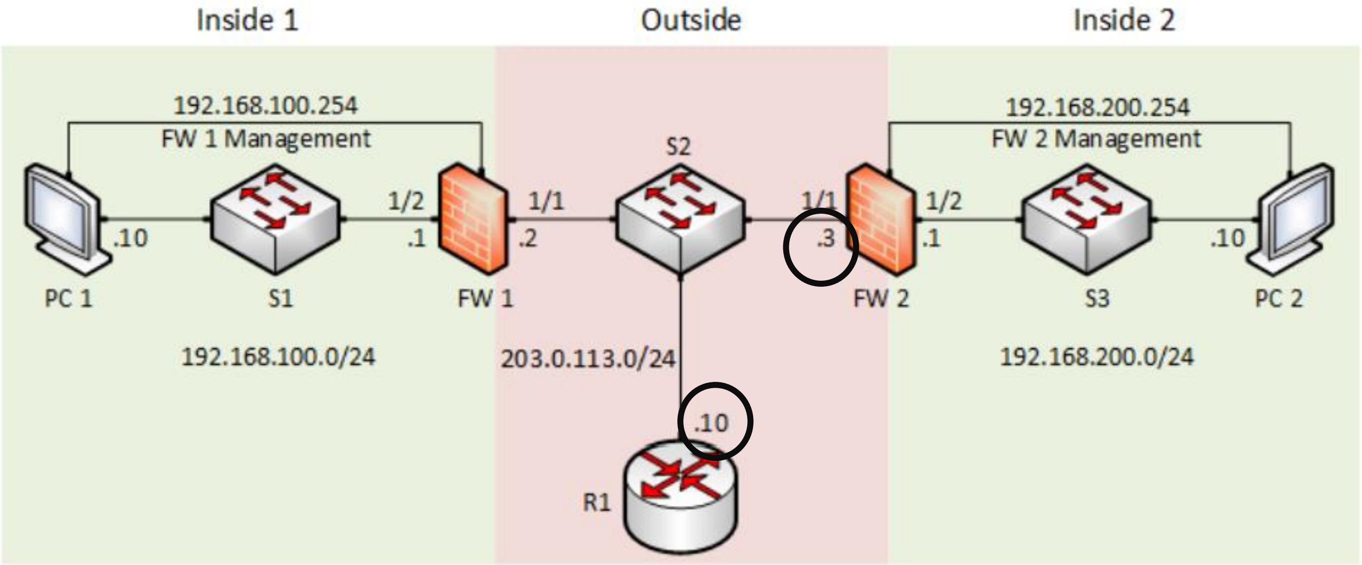
- BGP authentication uses the **Message Digest 5 (MD5)** cryptographic hash function to produce a signature that can only be reproduced by legitimate peers.

Proposed Solution

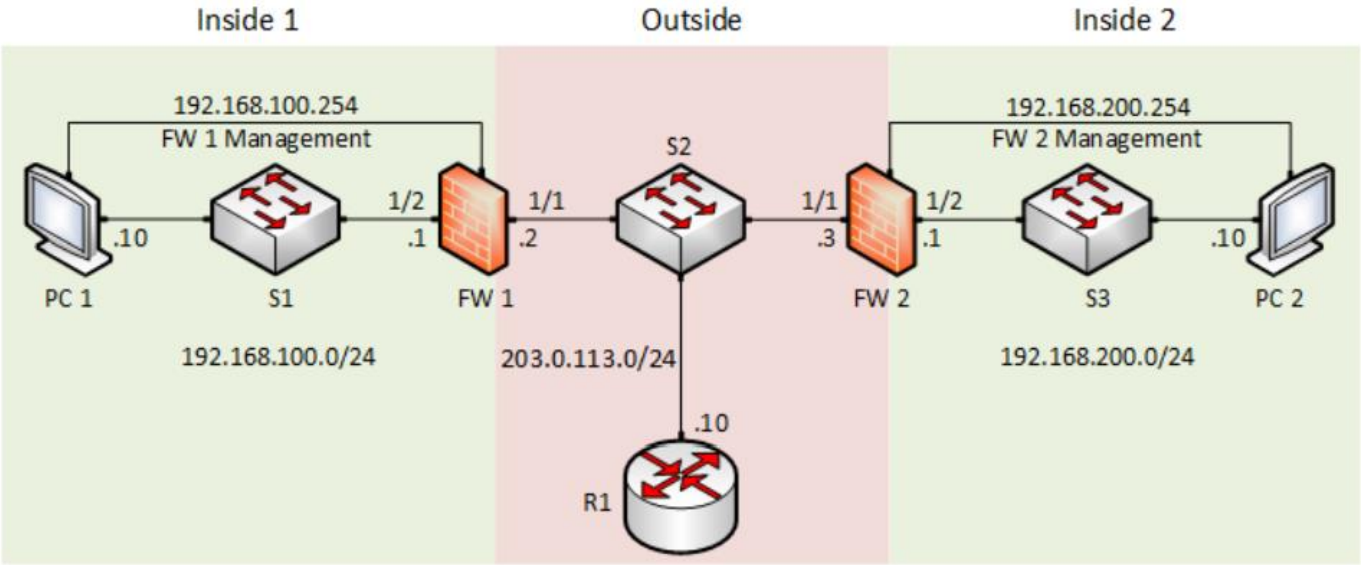
The malicious router hijacks the route between the 100 network and the 200 network.

By observing the routing table, we see that the 200 network's next-hop changes from 203.0.113.**3** to 203.0.113.**10**

This means the router has hijacked the route!



Proposed Solution



With BGP authentication,
this is no longer possible.

Conclusion

- BGP is necessary for networks to connect and communicate with other networks.

- BGP authentication greatly reduces the vulnerability of threat actors posing as legitimate networks and stealing data.