

Routing Security



Outline

■ Routing Security

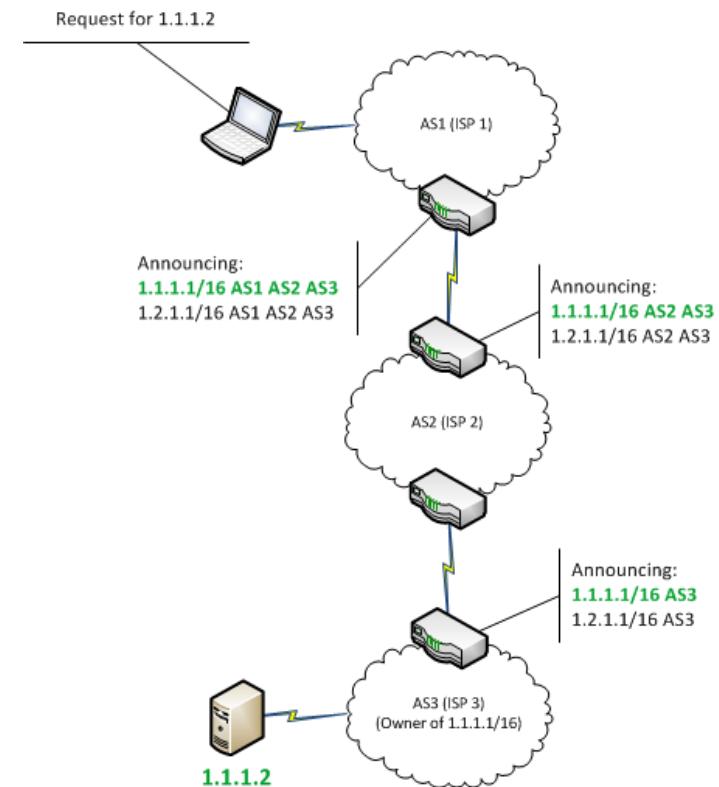
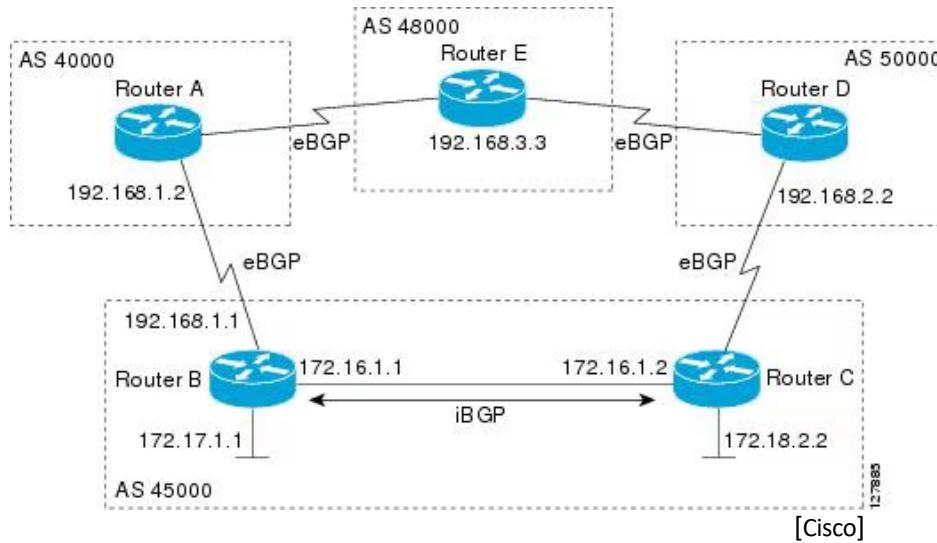
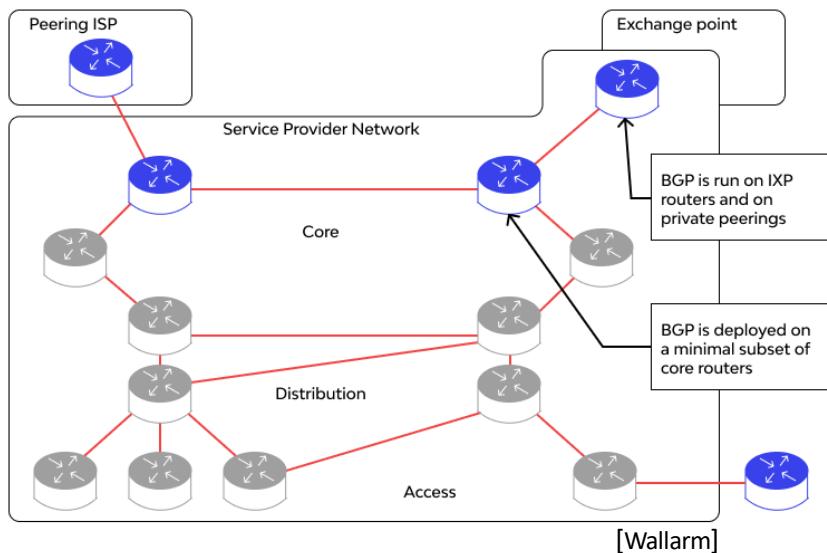
- Interdomain Routing
 - BGP Concepts (review)
 - BGP Security Vulnerabilities
 - BGP Security Support Technologies
- Intradomain Routing
 - IGP Concepts (review)
 - IGP Vulnerabilities and Attacks
 - Example of OSPF LSA Injection Attack
 - Summary



BGP Concepts

- Review
 - BGP (Border Gateway Protocol) and its role on the Internet [RFC 4271]
 - primary **interdomain** routing protocol
 - enables different Autonomous Systems (ASes) to **exchange routing information** and **determine the best paths** for delivering packets globally
 - each AS is identified by a unique number (ASN) and represents a network managed by a single administrative entity (e.g., ISP, enterprise, university)
 - BGP operates as a **path-vector protocol**, exchanging information about reachable networks (IP prefixes) and the AS path required to reach them
 - Peering Relationships:
 - external BGP (eBGP) – connects ASes across administrative boundaries
 - internal BGP (iBGP) – distributes routing information within an AS
 - BGP **selects paths based on policies and metrics** such as AS path length

BGP Concepts



Examples of BGP Deployment

BGP Security Concerns

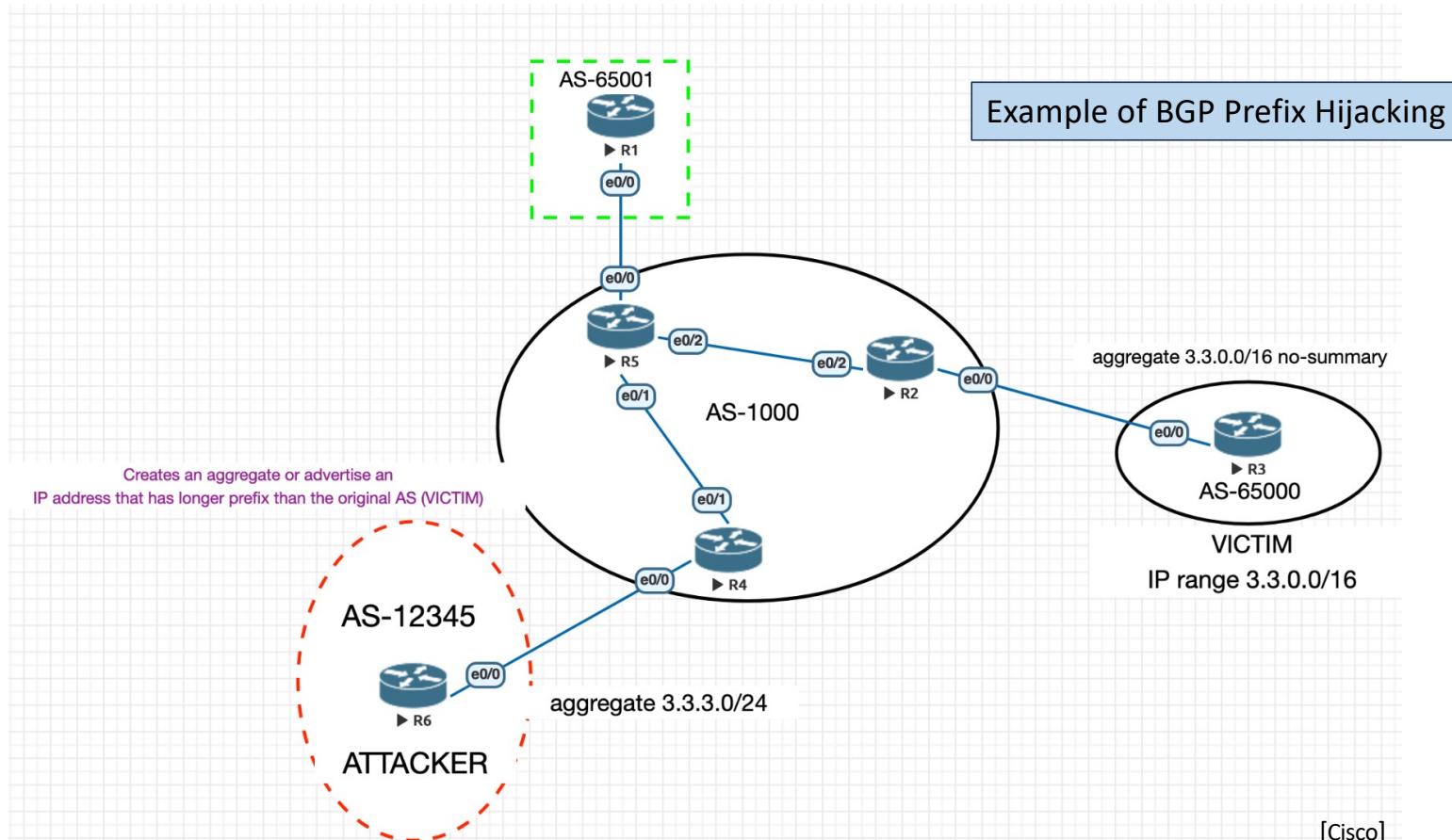
- Originally, BGP was designed with minimal security considerations
 - Trust-based model
 - assumes that all peers behave correctly and do not propagate incorrect routing info
 - Lack of Authentication
 - updates are not authenticated, allowing attackers to spoof legitimate BGP messages
 - Global Propagation of Faults
 - errors or malicious changes in one AS can propagate globally, affecting connectivity
 - No Built-In Validation of Route Announcements
 - does not verify the ownership of IP prefixes being advertised, enabling attackers to hijack prefixes or leak routes
 - Susceptibility to Session Attacks
 - BGP sessions between routers are vulnerable to interception and manipulation (e.g., TCP session hijacking or reset attacks)

BGP Security Vulnerabilities

1. Prefix Hijacking

- attackers advertise IP prefixes they do not own, **redirecting** traffic meant for legitimate networks to their own AS
- may lead to (i) interception or modification of traffic; (ii) traffic blackholing (making the destination unreachable)
- **Mitigation**
 - **Resource Public Key Infrastructure (RPKI)** – validates the origin AS of a route by associating IP prefixes with ASes; **uses cryptographic signatures** to verify route announcements
 - **Route Filtering** – ISPs can configure **prefix filters** to ensure only valid routes are propagated
 - **BGP Monitoring Tools** – use tools to detect anomalies in prefix advertisements (e.g., BGPmon or ARTEMIS)

BGP Security Vulnerabilities

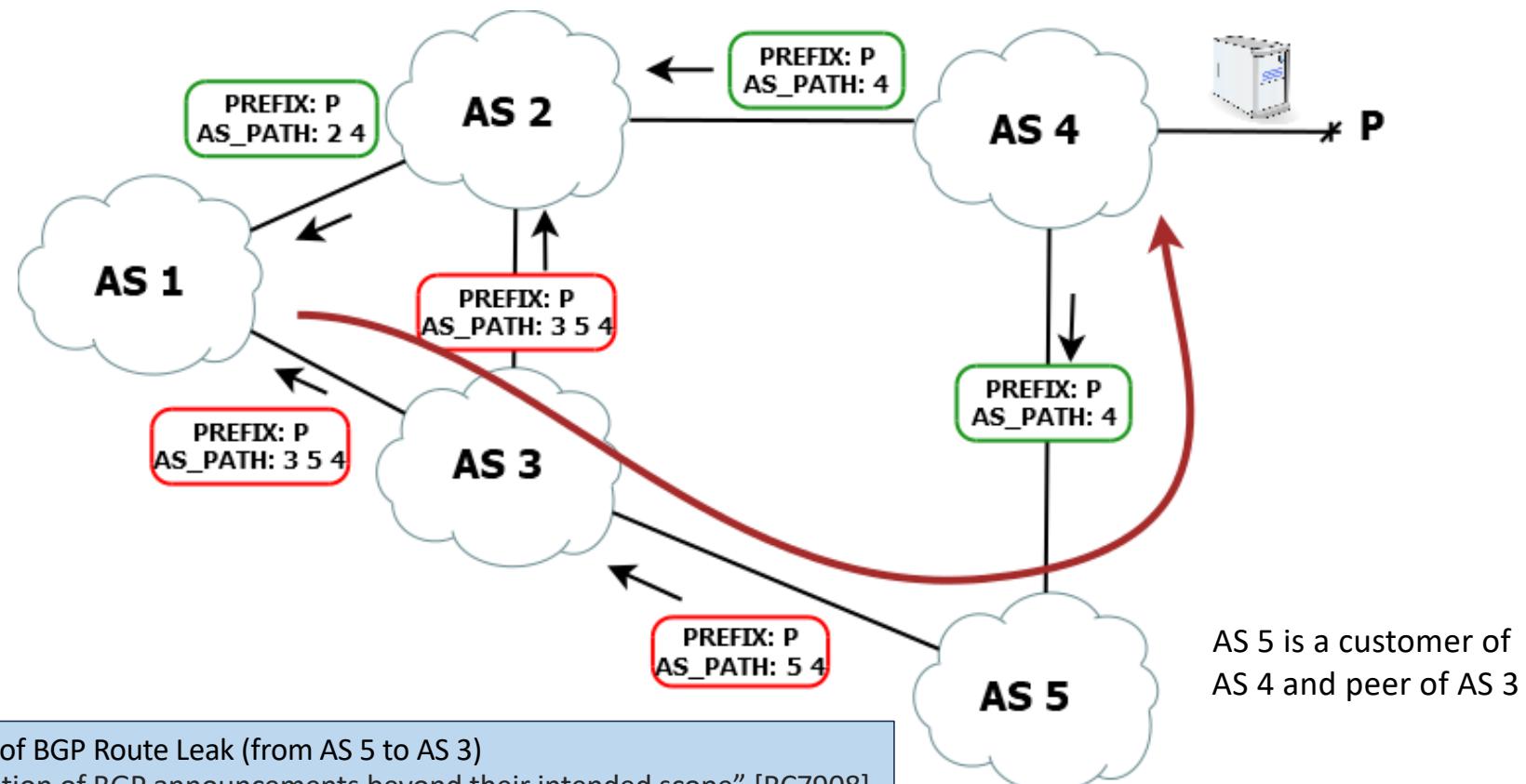


BGP Security Vulnerabilities

2. Route Leaks

- misconfigured or malicious ASes improperly propagate routes intended for a limited scope (e.g., private peering) to the global BGP tables
- leads to suboptimal routing, i.e., traffic taking inefficient paths
- overloading of intermediate ASes, causing performance degradation
- Mitigation
 - Route Policy Enforcement – configure strict export policies to control which routes are shared with peers (use the NO_EXPORT community attribute to prevent propagation)
 - MANRS (Mutually Agreed Norms for Routing Security)
 - set of guidelines and tools for prevention of route leaks (<https://manrs.org>)
 - BGPsec – provides cryptographic validation of the AS path to ensure routes follow authorized paths

BGP Security Vulnerabilities



BGP Security Vulnerabilities

3. BGP Session Hijacking

- attacker hijacks a BGP session by compromising underlying TCP session
- attacker must know TCP ports, seq #s, and IP addresses of BGP peers*
- attacker may insert, modify, or delete routing updates
- by injecting forged TCP packets or exploiting weak session auth
 - e.g., inject malicious routing updates, set RST flag (**BGP Session Reset Attack**)
- **Mitigation**
 - **TCP-AO** (Authentication Option) – for integrity/authenticity of TCP connections
 - restrict access to TCP port 179 using **ACLs**
 - use **random** TCP ports and seq #s to make hijacking harder (but doesn't solve)
 - use **IPsec** to encrypt and authenticate BGP sessions

* BGP routers establish p2p connections using TCP port 179

BGP Security Vulnerabilities

BGP Configuration Errors

- human errors or misconfigurations cause routing issues
- may mimic unintended attack
- **Mitigation**
 - **Automation and Templates** – use standardized configurations and automated deployment tools to minimize human error
 - **Route Testing** – validate routing configurations in a controlled environment before deployment
 - **Monitoring and Auditing** – regularly audit configurations and monitor routes for anomalies



BGP Security Support Technologies

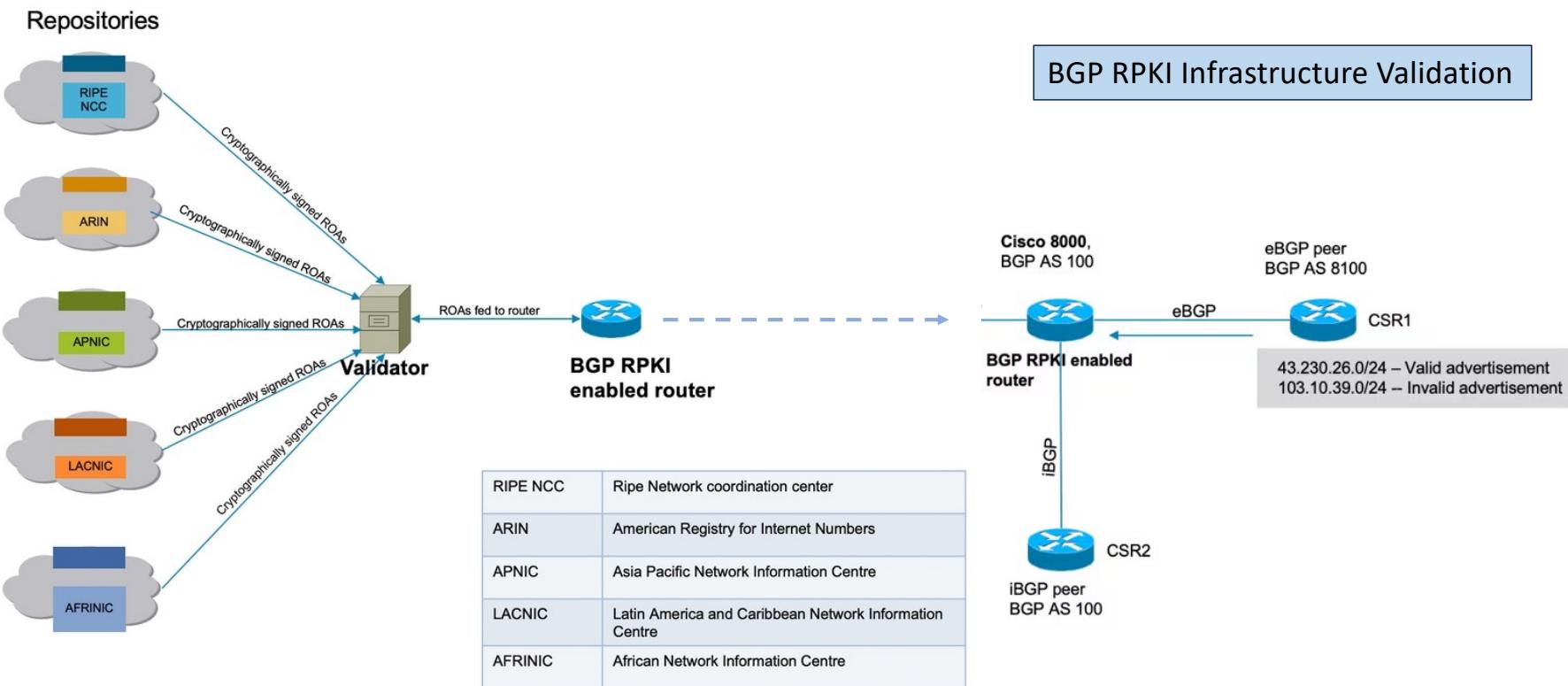
Resource Public Key Infrastructure (RPKI)

[RFC 6811]

- specialized PKI framework to support improved security for BGP
- addresses the critical issue of **route origin validation**, mitigating the risk of prefix hijacking
- provides cryptographic proof of route origin validity using **Route Origin Authorizations (ROAs)***
- BGP announcements are **validated against a RPKI database** through the interaction between routers and **RPKI validators**
- easy integration with the existing BGP-4 framework [RFC 4271]
- widely supported (e.g., Cisco, Huawei, Nokia) and adopted by ISPs
- requires robust management of the RPKI certificate hierarchy

* ROA object: (Origin AS, Network Prefix, Max Prefix Length, Signature)

BGP Security Support Technologies



[Cisco, adapted]

Security: 5- 13

BGP Security Support Technologies

BGPsec (Extension to BGP-4)

[RFC 8205]

- addresses specific BGP vulnerability: lack of AS path validation
 - enhances the authenticity and integrity of routing announcements by cryptographically signing BGP route updates
 - validates if the AS path advertised in a BGP update reflects the actual path through which the prefix announcement traveled (chain of trust)
 - prevents malicious actors from altering AS path attributes during transit
 - complements RPKI for end-to-end security
-
- *while RPKI verifies the legitimacy of the origin AS for an IP prefix, BGPsec ensures the integrity of the AS path*

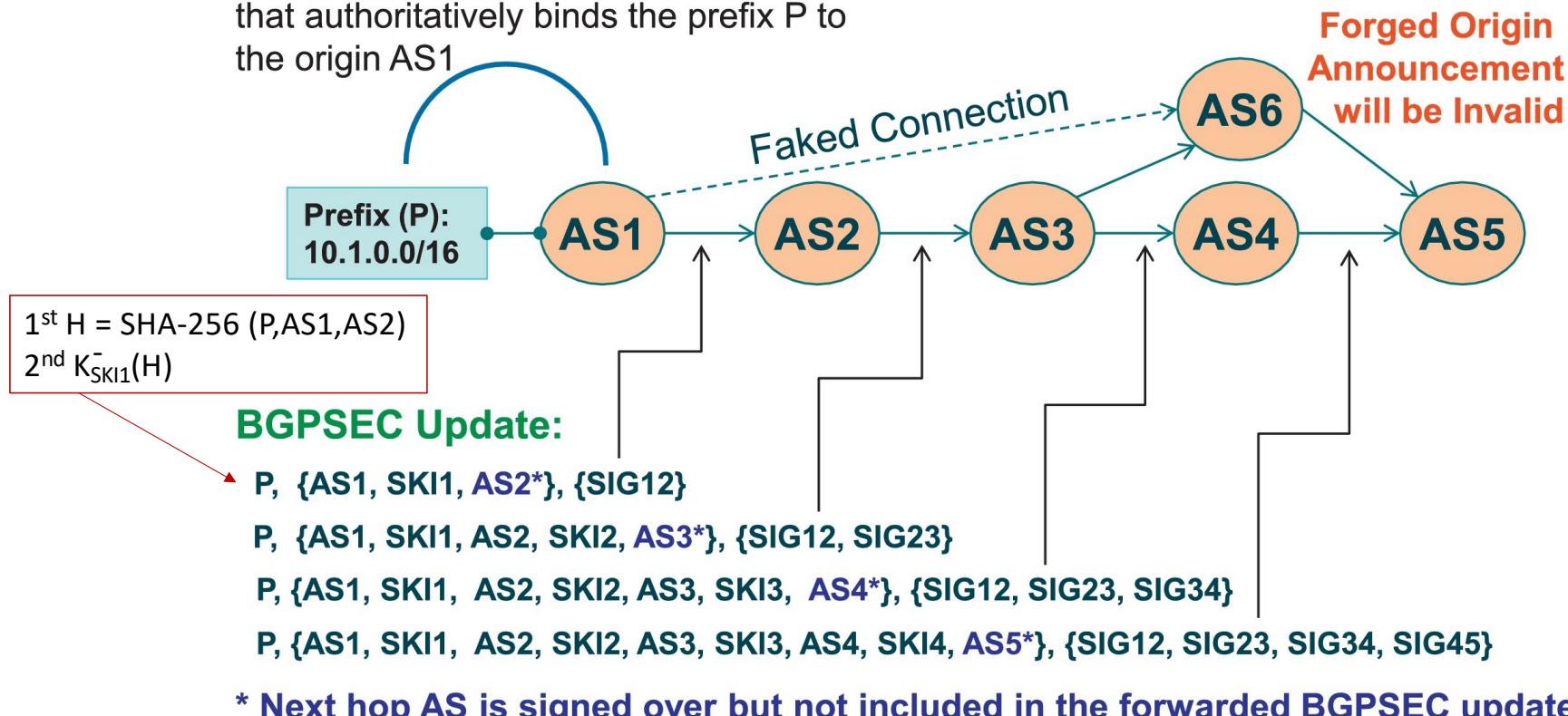
BGP Security Support Technologies

BGPsec

- Cryptographic AS Path Validation
 - each AS in the path signs the routing update using its private key (which is linked to its RPKI certificate through a Subject Key Index) before forwarding it
 - signature over: AS #, advertised prefix, next AS in the path and signature from prev AS
- Public Key Infrastructure (PKI)
 - uses PKI framework for signing and verifying updates
 - certificates are issued to ASes to prove their identities, tying AS #s to their public keys
- Backward Compatibility
 - routers not supporting BGPsec will simply propagate BGP updates w/o validation
- Incremental Deployment
 - allows for partial adoption, meaning only a subset of ASes need to implement it initially, and its benefits will gradually scale as adoption increases
- Increased Overhead
 - use of cryptographic signatures adds computational and bandwidth overhead

BGP Security Support Technologies

Route Origin Authorization (ROA) exists that authoritatively binds the prefix P to the origin AS1



[Sriram and Montgomery, 2017]

BGP Security Support Technologies

Autonomous System Provider Authorization (ASPA) (Internet draft, Oct 25)

- addresses BGP route leaks, a vulnerability not fully mitigated by RPKI or BGPsec AS Path Validation
- introduces an additional validation layer for BGP updates without the complexity of AS path cryptographic signatures of BGPsec
- similarly to RPKI, ASPA verifies the legitimacy of the AS path based on a globally available database of authorized provider relationships
- BGP routers can validate if an AS path conforms to the expected routing model (P2C, C2P, P2P):
 - providers and peers do not transit traffic between other providers or peers, without explicit business agreement

Outline

■ Routing Security

- Interdomain Routing
 - BGP Concepts (review)
 - BGP Security Vulnerabilities
 - BGP Security Support Technologies
- Intradomain Routing
 - IGP Concepts (review)
 - IGPs Vulnerabilities and Attacks
 - Example of OSPF LSA Injection Attack
 - Summary



Interior Gateway Protocols (IGPs)

Intradomain Routing

- routes the flow of packets within a single AS
- Interior Gateway Protocols (IGPs) ensure efficient, stable, and reliable routing within AS maintaining correct and up-to-date routing tables
- **OSPF** (Open Shortest Path First) [RFC 2328; RFC 5340]
 - **link-state** routing protocol widely used in enterprise and ISP networks
- **IS-IS** (Intermediate System to Intermediate System) (OSI) [RFC 9479]
 - **link-state** protocol, often deployed in ISP backbones
- **EIGRP** (Enhanced Interior Gateway Routing Protocol) [RFC 7868]
 - Cisco-proprietary **hybrid** routing protocol
- **RIP** (Routing Information Protocol) [RFC 2453]

IGPs Security

Importance of Security in Intradomain Routing

- intradomain routing is **trusted by design**, assuming all routers belong to and are controlled by the AS operator
- insider threats, misconfigurations, or compromised routers can exploit this trust
- compromised IGP **can disrupt internal traffic flow**, affect the entire network or enable external attacks
- Examples:
 - malicious updates could blackhole traffic or redirect it for eavesdropping
 - instability caused by route flapping or false route advertisements (RAs)
- security challenges focus on the **integrity of topology and routing updates**

IGPs Vulnerabilities and Attacks

Lack of Confidentiality

- protocols like OSPF and IS-IS **do not encrypt their updates by default**, exposing sensitive topology information
- allows **passive sniffing** of routing packets on the network
- may result in:
 - leakage of internal network topology
 - helping attackers in planning further exploits
- **Mitigation**
 - encrypt routing traffic between routers using, e.g., IPsec

IGPs Vulnerabilities and Attacks

Replay Attacks

- attacker may resend **valid but old** RAs, tricking routers into using outdated or incorrect path
- attack involves capturing routing protocol packets (e.g., OSPF LSAs, IS-IS LSPs), delaying or replaying those packets to disrupt the network topology
- may result in traffic instability, looping, or blackholing, degrading perf
- **Mitigation**
 - ensure each update includes a sequence number and a TTL value (e.g., LSA Header and LSA Age / Max Age in OSPF) so routers ignore packets with old sequence numbers or expired timers
 - use cryptographic authentication: HMAC-SHA256 or other mechanisms to ensure packets are from trusted sources

IGPs Vulnerabilities and Attacks

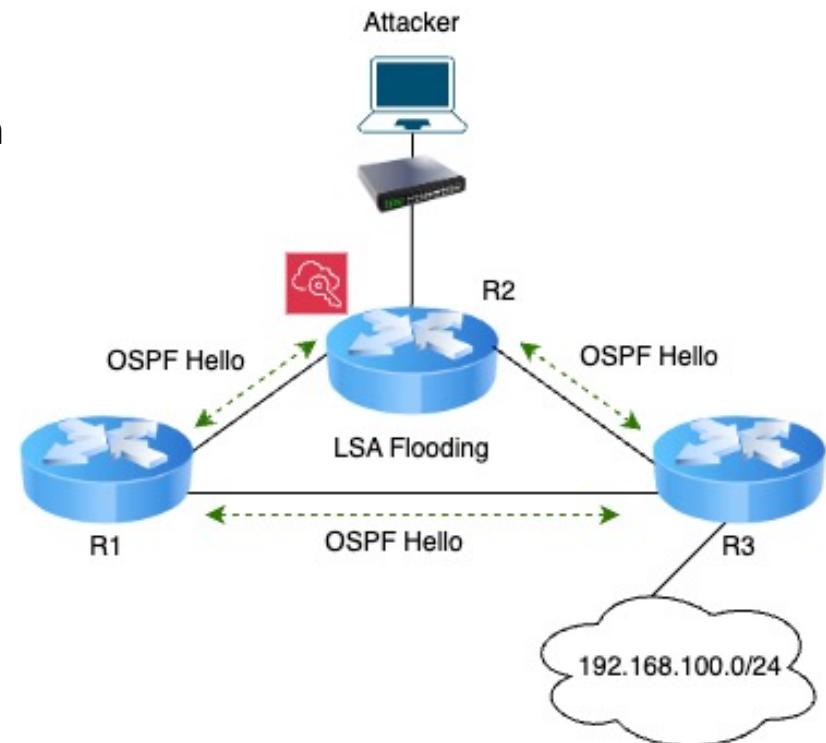
Spoofing and Injection Attacks

- attackers inject unauthorized, fake RAs to modify the network topology
- attack involves either gain access to a router or impersonate a legitimate router to inject false LSAs (OSPF) or LSPs (IS-IS) to advertise non-existent or malicious paths
- may result in traffic misdirection (e.g., redirecting traffic to attacker-controlled networks), creation of routing loops or blackholes
- Mitigation
 - authentication mechanisms – HMAC-SHA256 to authenticate LSAs (OSPF) or LSPs (IS-IS)
 - secure management practices – restrict physical and logical access to routers
 - encrypt and authenticate all routing comms using IPsec (adds complexity)

IGPs – Example of OSPF LSA Injection Attack

1. Pre-Attack: normal OSPF operation

- OSPF Hello Exchange
 - routers exchange Hello packets to establish and maintain neighbor relationships
(R1 ↔ R2 ↔ R3)
- LSA Flooding
 - each router advertises its topology information using LSAs
 - e.g., R3 advertises net 192.168.100.0/24; R1 and R2 receive and store this info in their Link-State Databases (LSDBs)
- Route Calculation
 - routers calculate the shortest path to subnet using Dijkstra's algorithm, preferring R3 as the legitimate next hop



IGPs – Example of OSPF LSA Injection Attack

2. Step1: attacker captures LSAs

- either to (i) sniffing traffic or (ii) direct access to R2's LSDB **if compromised**
- attacker learns the topology

3. Step2: crafts malicious LSA

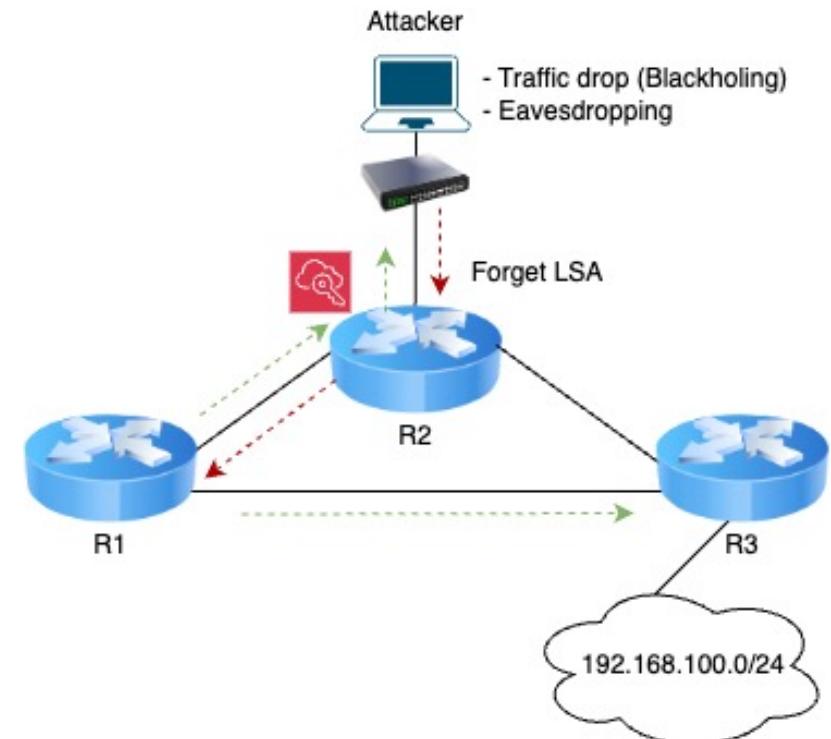
- sets lower metric for the subnet, making R2 appear to be the best route
- sets legitimate-looking sequence #'s and checksum values to avoid rejection

4. Step3: injects malicious LSA

- attacker uses R2 to flood the malicious LSA to its neighbors (R1 and R3)

4. Step4: routing update; redirection

- R1 routes traffic for 192.168.100.0/24 through R2 instead of R3



Interior Gateway Protocols (IGPs)

Summary

Protocol	Core RFC	Security RFCs	Principle	Notes
OSPFv2	RFC 2328	RFC 5709 (HMAC-SHA), RFC 7474 (IPsec)	Link-State	Widely used in IPv4 networks
OSPFv3	RFC 5340	RFC 7474 (IPsec for OSPFv3)	Link-State	Adds support for IPv6
IS-IS	RFC 9479	RFC 5304, RFC 5310	Link-State	Dual support for OSI and IP
EIGRP	RFC 7868	No specific RFC (MD5/HMAC [Cisco])	Hybrid (Link-State + Distance-Vector)	Cisco proprietary, less standardized
RIP	(RFC 1058), RFC 2453 (RIPv2)	No specific security RFC; supports MD5 in RIPv2	Distance-Vector	Simpler, less efficient; used for small networks

Summary

■ Routing Security

- Interdomain Routing
 - BGP Concepts (review)
 - BGP Security Vulnerabilities
 - BGP Security Support Technologies
- Intradomain Routing
 - IGP Concepts (review)
 - IGPs Vulnerabilities and Attacks
 - Example of OSPF LSA Injection Attack
 - Summary

