

SAC121: SSAC Briefing on Routing Security

ICANN DNS Symposium, November 2022

Geoff Huston

SAC121: SSAC Briefing on Routing Security

- **Background Technical Information**
- **Routing Security and the Domain Name System (DNS)**
- **Efforts to Enhance Routing Security**
- **Operating Secured Infrastructure**
- **Key Takeaways**

Internet Routing for DNS Query

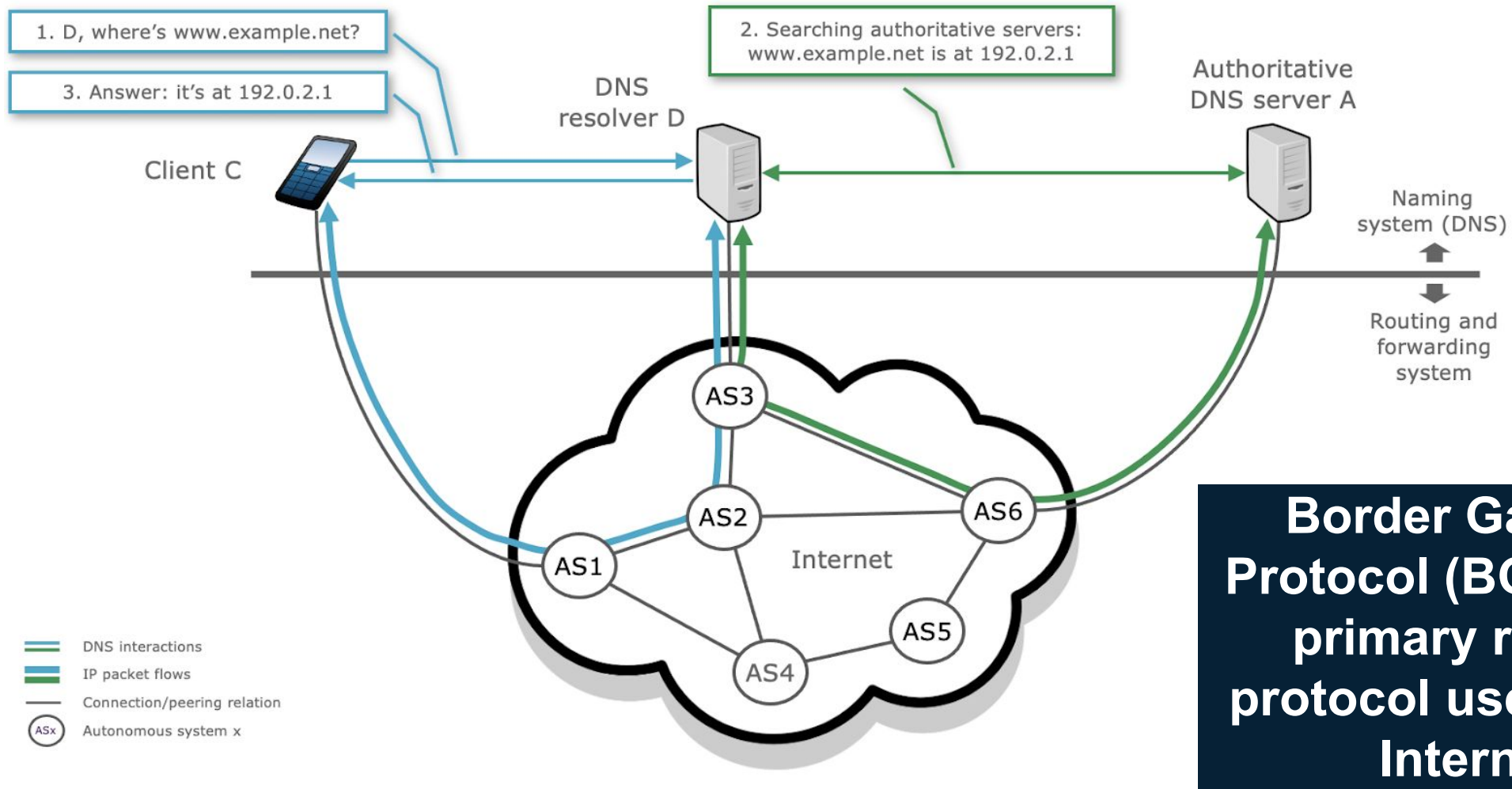


Figure 1: DNS traffic passing through multiple autonomous systems

Route Hijack for DNS Query

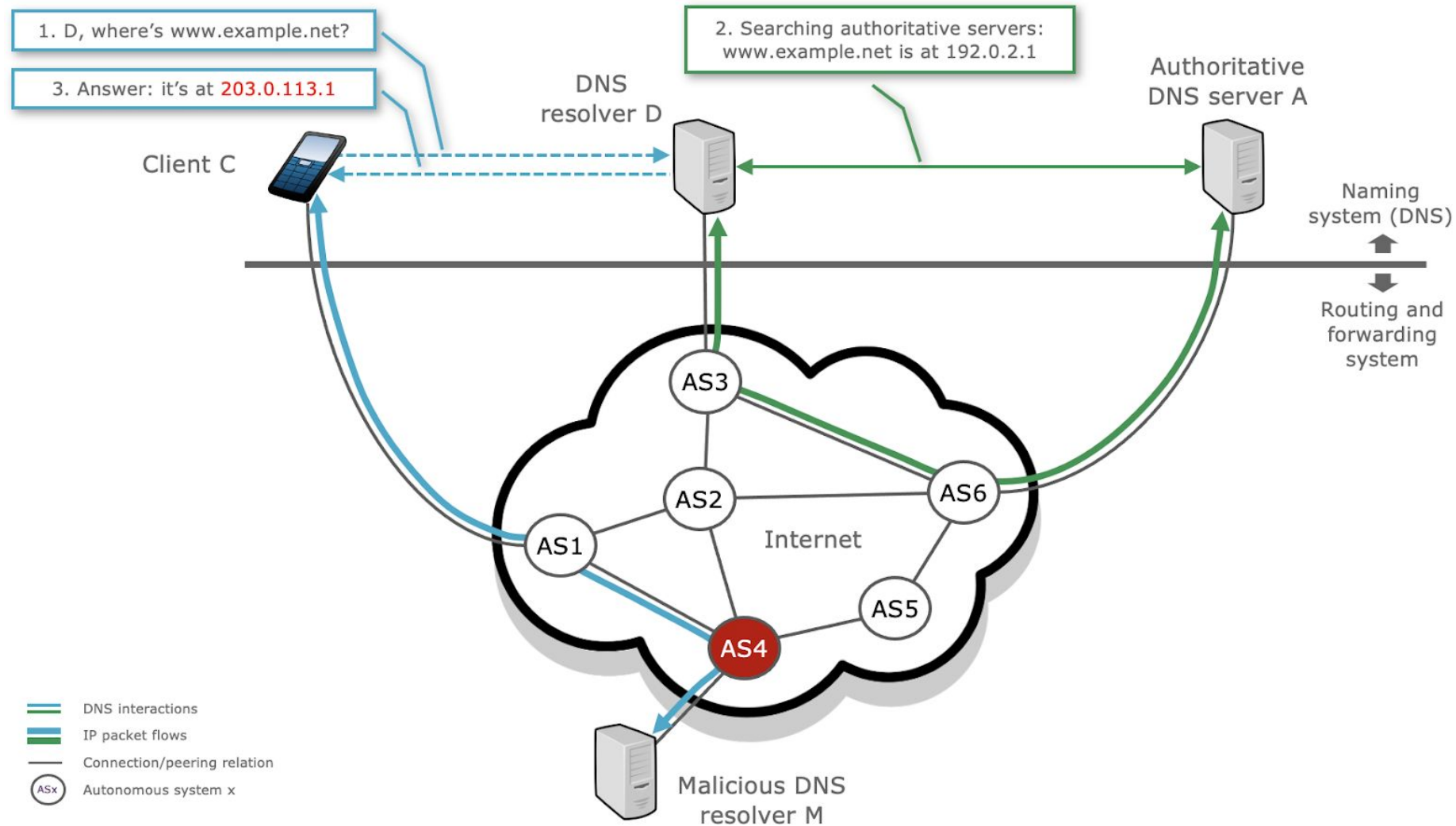
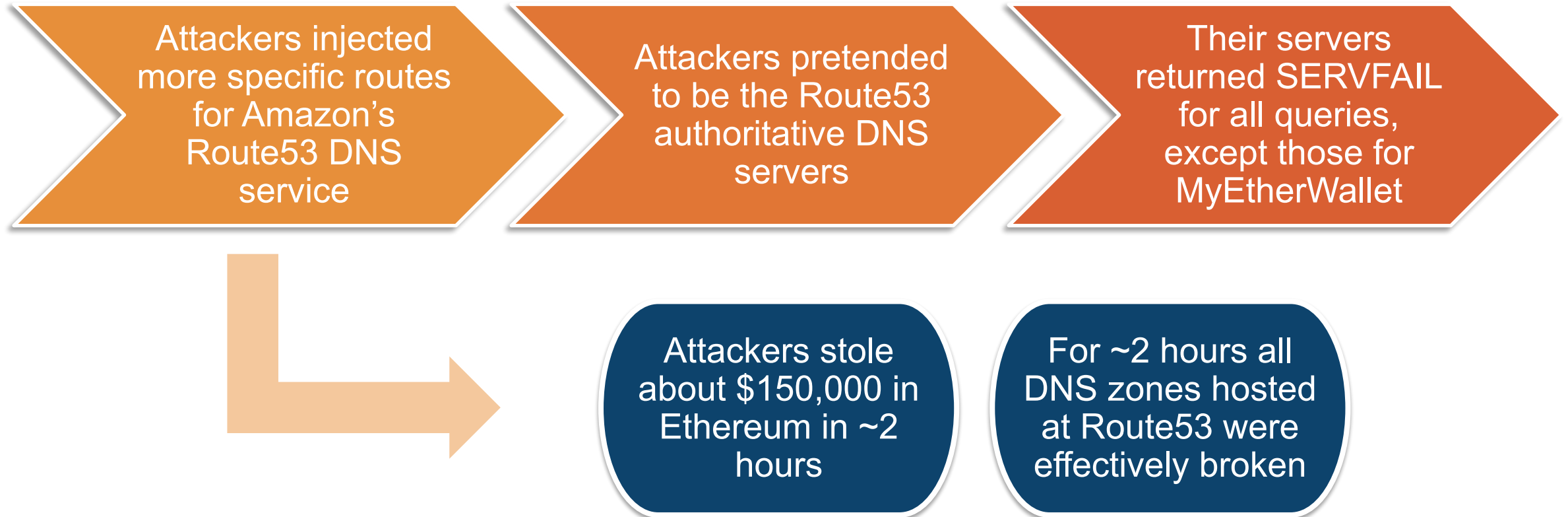


Figure 2: Hypothetical Route Hijack affecting the DNS

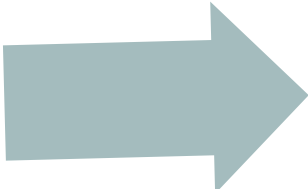
Routing Incident: MyEtherWallet / Route53

MyEtherWallet (myetherwallet.com) was attacked by unidentified criminals using a BGP hijacking attack

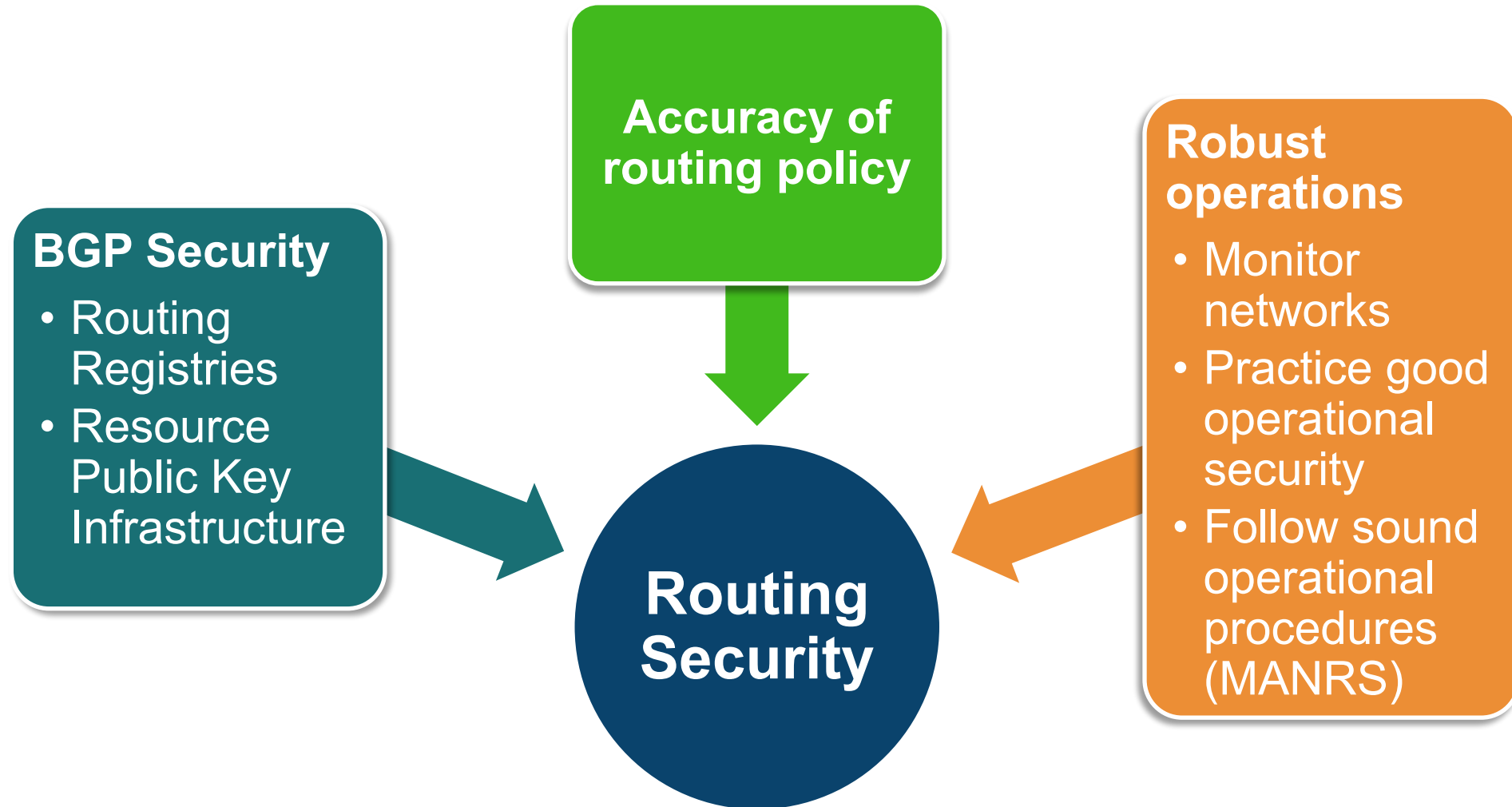


The Relevance of Routing Security for the DNS

The DNS protocol and DNS resolution are susceptible to routing incidents

- Many authoritative DNS servers answer any query they receive
 - Many DNS clients do not authenticate the identity of the server that provides the answer, and do not perform DNSSEC validation
 - Stub resolvers have no visibility into which authoritative servers provide answers to queries
 - Vast majority of DNS queries are in the clear and use UDP as the transport protocol
- 
- A routing attack can substitute one DNS server for another without the awareness of the client
 - Routing attacks can alter the network path of a query, allowing third parties to inspect DNS queries or otherwise eavesdrop on transactions.

Efforts to Enhance Routing Security



BGP Security: Routing Registries

Network operators can register their autonomous systems and the prefixes they originate in a routing registry.



Highlights

- Allows other operators to see what prefixes and routes a given AS should be announcing
- Most useful when carefully and continuously managed for consistency, coverage, and accuracy

Limitations

- When routing registries take on too broad of a scope or are not actively managed their consistency and utility falls.
- The contents of different routing registries may not be mutually consistent and there is no clear way to resolve conflicts between them.

BGP Security: Resource Public Key Infrastructure (RPKI)

Resource Public Key Infrastructure (RPKI) is a way for entities with functional control of IP Address prefixes to assert which autonomous systems are permitted to originate those prefixes.



Highlights

- Builds upon routing registries by designating the autonomous systems that are permitted to originate a routing announcement for a prefix
- Provides some protection from common sources of routing incidents
- Discussions on the efficacy of the RPKI are ongoing, but it may soon be required by some regulators

Limitations

- Not a complete solution to routing security
- All participants always need access to all the data
- No notification to relying parties when they need to update their data
- RPKI cannot secure the full path, only couples the origination of prefixes to ASes

Operating Secured Infrastructure

Organizations should practice good operational security and monitor their routes in order to detect anomalies and failures.

Endogenous Monitoring

- Monitoring from within the network being monitored
- Monitor ability to reach other networks
- Most important is connection to upstream provider

Exogenous Monitoring

- Monitoring from outside the network being monitored
- Monitor connectivity from external networks
- Important, but more expensive than endogenous
- Anycast adds additional complexity

Operator Coordination

- Every org needs access to routing expertise to help remediate issues
- Network operator groups (NOGs) help facilitate relationship building & information sharing

MANRS for Network Operators

- Filtering
- Anti-spoofing
- Coordination
- Global Validation

Key Takeaways



The routing system today is subject to a continuous stream of routing anomalies that affect its integrity and that sometimes cause large DNS outages.

Internet routing security is a combination of BGP protocol security, accuracy of routing policy, and robust operations

Organizations should monitor their routes in order to detect anomalies and failures.

Routing security is not a substitute for other technologies also key to securing the DNS. It is only one part of a complete approach to securing a network.

Thank you