A Survey of BGP Security: Issues and Solutions

Butler, Farley, McDaniel, Rexford

Kyle Super
CIS 800/003
October 3, 2011

Outline

- Introduction/Motivation
- Sources of BGP Insecurity
- BGP Security Today
- BGP Security Solutions: Architectures
- BGP Security Solutions: Experimental
- Future Directions/Conclusion

Motivation

- BGP: Dominant Interdomain Routing Protocol
  - Deployed Since Internet First Commercialized
  - Current Version 4 In Use for Over Ten Years
  - Popular Despite Providing No Performance/Security Guarantees
- Usually Routing Outages and Failures Limited
  - But Sometimes Not: Potential for Major Damage
  - Eg: Florida ISP 1997, Turkey TTNet 2004, Con-Edision 2006, Pakistan Telecom 2008

Motivation

- What's the Big Deal?
  - Many Critical Applications Rely on the Internet
  - Eg: Online Banking, Stock Trading, Telemedicine
- Department of Homeland Security:
  - BGP Security Critical to National Strategy
- Internet Engineering Task Force:
  - Working Groups: Routing Protocol Security Requirements, Secure Interdomain Routing

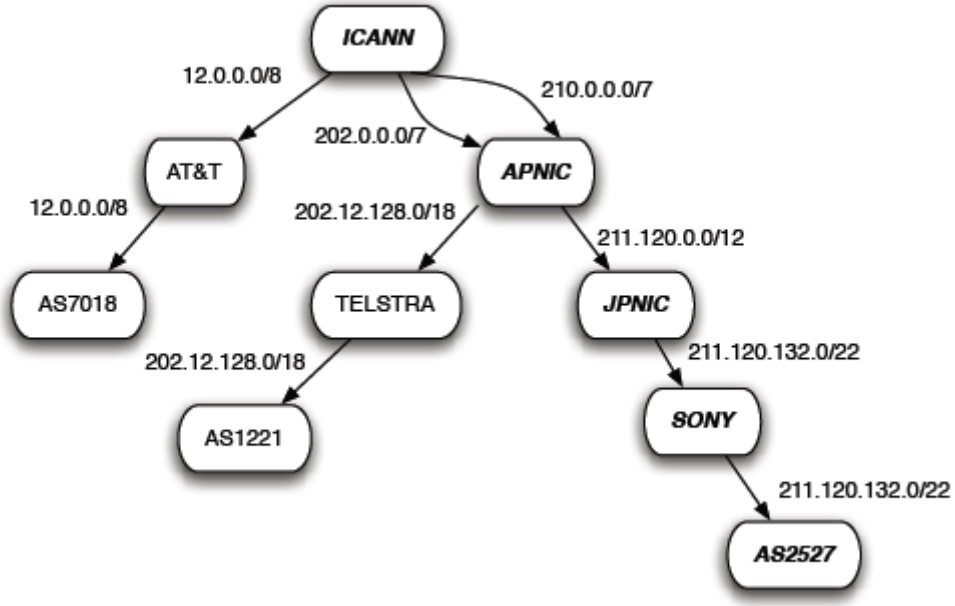
Sources of BGP Insecurity

- IP Prefixes and Autonomous System Numbers
- Using TCP as the Underlying Transport Protocol
- Routing Policy and BGP Route Attributes

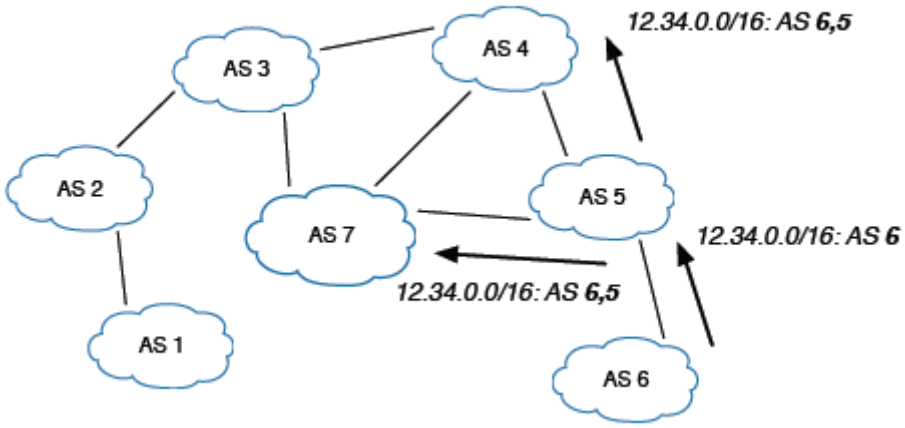
IP Prefixes and AS Numbers

- IP Addresses Assigned to Institutions in Blocks
  - Contiguous Address Blocks: 192.168.0.0/24
  - Leads to Smaller Routing Tables/Fewer Announcements
  - Prefixes Can Be Contained Within Each Other
    - Eg: 211.120.0.0/12 Vs. 211.120.132.0/22
    - Routers Select Most Specific Route Table Entry
- Autonomous System Numbers 1-64511
  - Numbers 64512-65535 Private: Stub Networks

IP Address Delegation

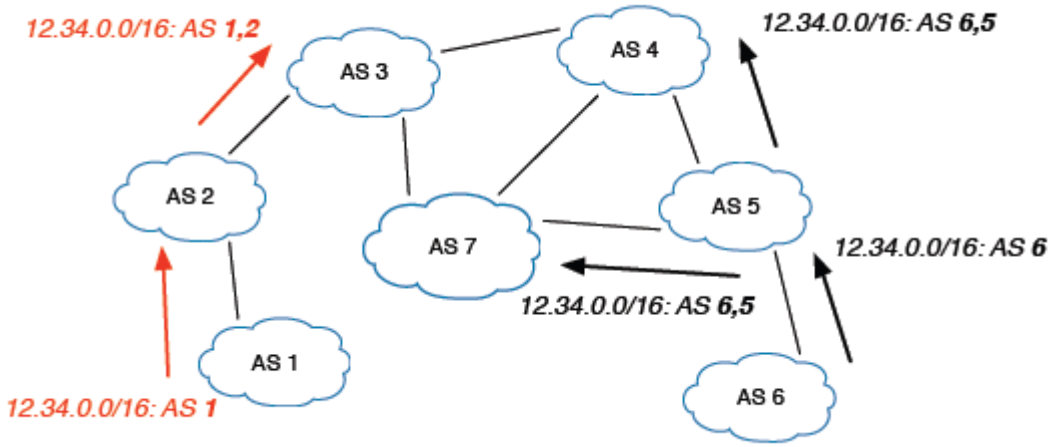


Normal Route Origination



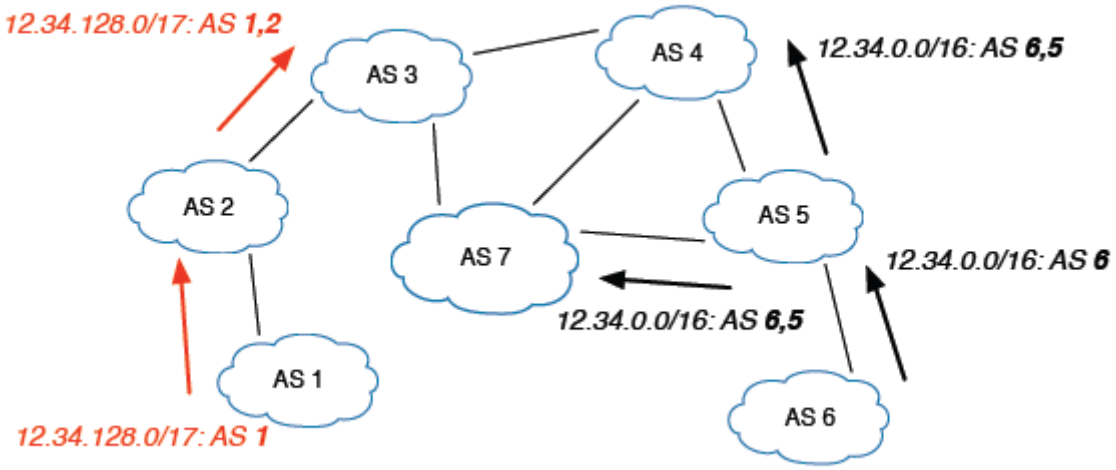
Malicious Route Origination

- BGP Does Not Verify AS Number/IP Addresses
  - Prefix Hijack: Black Holes, Interception Attacks



IP Address Deaggregation

- Routers Select Most Specific Table Entry



TCP as the Transport Protocol

- Routers Exchange Announcements/Withdrawals
  - BGP Session over TCP Connection
  - Communication Susceptible to Attack
- Attacks Against Confidentiality
  - Third Party Can Eavesdrop BGP Session
  - Learns Policy and Routing Information
  - Business Relationships Can Be Inferred

TCP as the Transport Protocol

- Attacks Against Message Integrity
  - Man-In-The-Middle Attacks
  - Message Insertion:
    - Could Inject Incorrect Information
    - Could Overwhelm Routers with Too Many Messages
  - Message Deletion:
    - Could Delete Keep-Alive Messages
  - Message Modification
  - Message Replay:
    - Re-assert Withdrawn Route, Withdraw Valid Route

Denial of Service Attacks

- Exploit the TCP Connection Establishment
  - Three Way Handshake (SYN, SYN-ACK, ACK)
  - Connection Closure (FIN, RST)
- Send RST Packet to Force Connection Closed
- SYN Packet Flooding
  - Consumes Resources, Overwhelms Routers
  - Neighbors Assume Connection Dead
    - Upon Reconnection: Route Flapping
- Physical Attacks: Backhoe Attack
  - Or Swamp Link with Traffic

Routing Policy and BGP Attributes

- Local Preference, AS Path Length, Origin Type, Multi-exit Discriminator
- Adversary Could Manipulate These Values
  - Shorten AS Path Length
  - Lengthen AS Path: Make Route Look Legit
    - Or Use Too Many Resources to Store Path
  - Remove AS from Path: Thwart Filtering
  - Add AS to Path: Causes AS Path Loop
  - Modify Origin Type, MED to Influence Decision

BGP Security Today

- Routers Need Byzantine Robustness:
  - Termination, Agreement, Validity
- Typical Approaches: Implemented Locally
  - Protecting Underlying TCP Connection
  - Defensively Filter Routes

Cryptographic Techniques

- Pairwise Keying: Shared Secret Between Routers
  - O(n^2) Keys Needed: Too Complex
  - Keys Must Be Changed: Cryptanalysis Attacks
- Cryptographic Hash Functions (MD5, SHA-1)
  - Message Authentication Codes
    - Ensures Message Integrity and Authentication
    - Requires Shared Secret
- Diffie-Hellman Key Exchange
  - Uses Modular Arithmetic Complexity
  - Allows Hosts to Exchange Keys without Prior Secret

Cryptographic Techniques

- Public Key Infrastructure
  - One Public Key/Private Key Pair per AS
  - Allows Communication without Prior Secret
  - Requires Hierarchical Infrastructure
    - Public Keys Need to Be Distributed
- Public Key Cryptography
  - Encryption: E with Public, D with Private
  - Digital Signature: Hash with Private, Verify with Public

Cryptographic Techniques

- Attestations and Certificates
  - Attestation: Proof AS Can Advertise Resource
  - Digital Signature Chain to Root of Authority
  - Requires Public Key Infrastructure
  - Certificate: Verifies Public Keys in PKI
    - Also Digitally Signed in Chain

Pairwise BGP Session Protection

- MD5 Signature: Ensures Message Integrity
  - Sign BGP or Underlying TCP Message
  - Requires Shared Secret Key
- Smith/Garcia-Luna-Aceves Countermeasures
  - Pairwise Encryption with Sequence Numbers
  - UPDATE Timestamp, PREDECESSOR Attribute, UPDATE Digital Signatures
  - Requires Shared Secret, Modification to BGP
- Gouda Hop Integrity Protocol
  - Sequence Numbers and Message MACs with PKI

Pairwise BGP Session Protection

- Generalized TTL Security Mechanism
  - Provides Protection from Remote Attack
  - Assumes Routers are One-Hop Neighbors
  - Set TTL IP Packet Attribute to 255
    - Decremented at Each IP Layer Hop
    - Discard Packets with TTL < 254
  - Cannot Protect Against Insider Threats
  - Less Useful In Multi-hop Settings
  - Cheap Protection Against Unsophisticated Attacks

Pairwise BGP Session Protection

- Ipsec: Network Layer Security Protocols
  - Provides Encryption/Authentication of IP Packets
  - Also Provides Needed Key Infrastructure
  - Ubiquitous, Well-Understood, Easy to Use
  - Two Protocols with Differing Security: AH/ESP
  - Only Provides Pairwise Protection
    - Does Not Protect Against Widespread Attacks

Pairwise BGP Session Protection

	Integrity	Confidentiality	Replay Prevention	DOS Prevention
MD5 Integrity [29]	yes	no	yes	no
Countermeasures [33]	yes	yes	yes	no
HOP Protocol [34]	yes	no	yes	no
GTSM [35]	no	no	no	no
IPsec (AH) [40]	yes	no	yes	yes
IPsec (ESP) [41]	yes	yes	yes	yes

Defensive Filtering of BGP Announcements

- ASes Filter Ingress/Egress Routes by Policy
- Documented Special Use Addresses (Loopback)
- Bogons/Martians: Addresses with no Allocation
- Private AS Numbers
- Limit AS Path Length, Prefix Size, Number of Announcements
- Filter Routes from Customers, Stub-ASes
- Overwrite BGP Attributes (MED, Origin)
- Heuristic: Does Not Provide Strong Security
  - Large ASes Have Complex/Changing Rules

Routing Registries

- ASes Provide Policy/Topology Information
- Constructs Global View of Routing Info
  - ASes Query Information, Filter Invalid Routes
- Registry Information Needs to Be Correct
  - Authentication to Avoid Malicious Modification
- Corporations Consider Info Proprietary
- ASes Lack Incentive to Update Information

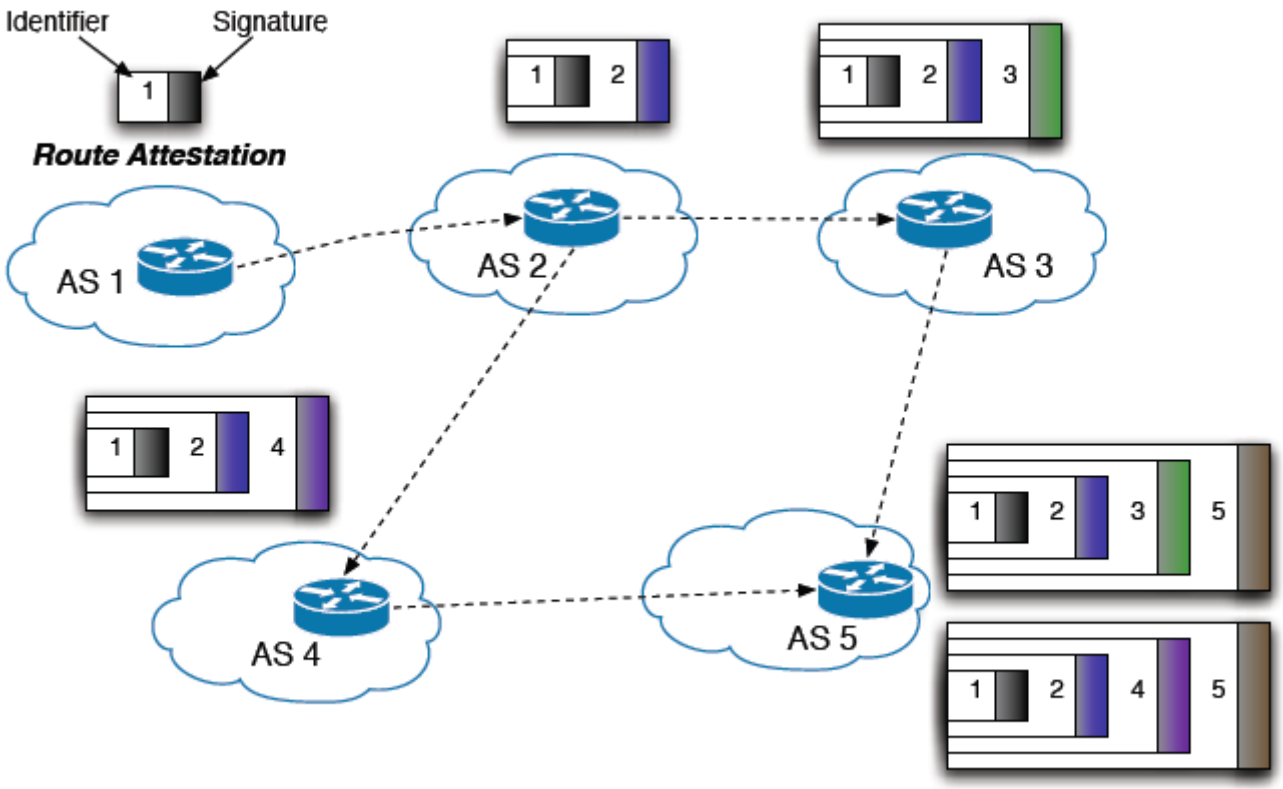
Protect Routing Infrastructure

- Protect Access to Physical Link
  - And Provide Redundant Links
- Protect the Management Interface (SNMP)
  - Use SSH/VPNs to Connect to Router
- Give BGP Messages High Priority
  - Messages Get Through During a Flooding DoS

BGP Security Architectures

- Secure BGP (S-BGP)
  - Implementation Exist, IETF Considering Standard
  - Uses Two PKIs
    - Authenticate Address Allocation Hierarchically
    - Certificate Proving AS Originated a Statement
  - Address Attestation: Prove AS Originates Address
  - Route Attestation: Routes Signed from AS to AS
    - Routes Cannot Be Modified
  - Resource Intensive: CPU, Memory, Storage
    - Could Double Convergence Times

Secure BGP


Identifier
Signature
1
Route Attestation
AS 1
1 2
AS 2
1 2 3
AS 3
1 2 4
AS 4
AS 5
1 2 3 5
1 2 4 5

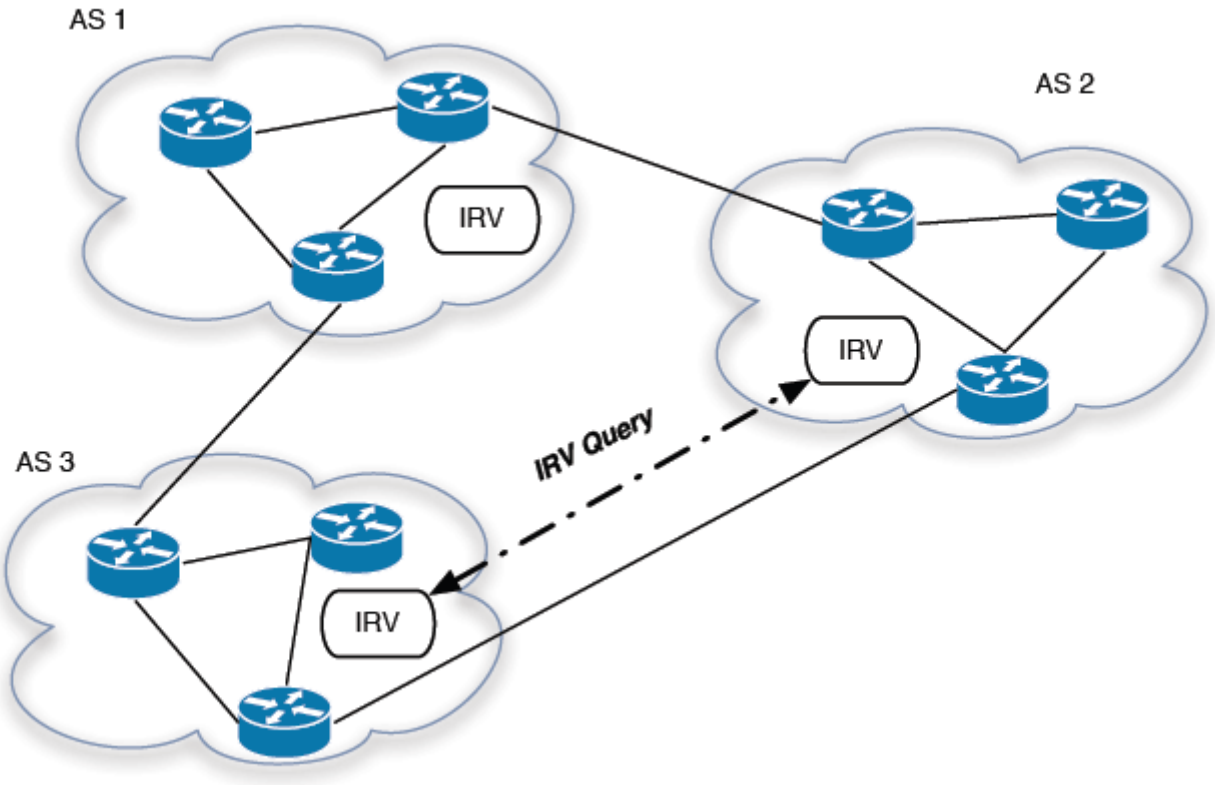
BGP Security Architectures

- Secure Origin BGP (soBGP)
  - PKI: Three Certificate Types
    - Bind Public Key to Router
    - Policy Details: Protocol Parameters and Topology
      - Routers Construct Global View of Network
    - Address Attestation
  - Info Transmitted via BGP SECURITY Messages
    - Requires Modification of BGP Implementations
    - Long-Term Info Verified Before Beginning BGP Sessions
  - Offers Tradeoffs (Computation vs. Security)
    - Verify Routes Before/After Accepting Them
    - Verify Entire Route/First Hop/Not At All

BGP Security Architectures

- Interdomain Route Validation (IRV)
  - Each AS Contains an IRV Server
  - Upon Receiving Update, Local IRV Server Queries IRV Server for Each AS Hop to Confirm Path
  - Flexible: Can Decide which ASes to Query
    - Partial Queries, Trusted ASes, Cached Routes
  - ASes Retain Control of their Information
  - Use Underlying Network/Transport Security
    - Ipsec for IP and TLS for TCP
  - Limitation: Requires Working Network

Interdomain Route Validation



Experimental BGP Security Systems

- Reducing Computational Overhead
  - Origin Authentication: Validate Address Ownership with Merkle Hash Trees
  - Secure Path Vector: One-Time Signatures generated from Root Value
  - Signature Amortization: One Signature for UPDATE Message Group
  - Reference Locality: Exploit Path Stability to Reduce Number of Signatures

Experimental BGP Security Systems

- Alternatives to PKI
  - Pretty Secure BGP: Each AS Maintains Address Info for Neighbors

Experimental BGP Security Systems

- Detecting and Mitigating Anomalies
  - Multi-Origin AS Conflicts: Community Attribute with ASes that can Originate Addresses
  - Intrusion Detection: Observe Address Ownership over Time, Flag Unexpected Changes
  - Prefix Hijacking Alert System: Server Alerts Valid Originator Upon Hijack
  - Pretty Good BGP: Monitor Historic Routing Data to Flag Unexpected Routes as Suspicious

Experimental BGP Security Systems

- Detecting and Mitigating Anomalies
  - Real-Time Monitoring: Maintain Info about Hosts on a Network, Check Info on Origin Conflict
  - Whisper Protocol: Originator Assigns Random Value, Value Hashed at Each AS Hop

Security Properties of Proposed Solutions

Solution Definition			Security Services		
System	In Use	Style	Topo. Auth.	Path Auth.	Origin Auth.
Route Filtering [18], [47],	yes	anomaly	*weak*	*weak*	*weak*
Routing Registries [49]	yes	anomaly	*weak*	*weak*	*weak*
S-BGP [60]	no	crypto	**strong**	**strong**	**strong**
soBGP [64]	no	crypto/anomaly	**strong**	none	**strong**
IRV [67]	no	crypto/anomaly	**strong**	**strong**	**strong**
Origin Authentication [70]	no	crypto	none	none	**strong**
SPV [74]	no	crypto	**strong**	**strong**	none
Signature Amortization [79]	no	crypto	**strong**	**strong**	none
Reference Locality [81]	no	crypto	**strong**	**strong**	none
psBGP [84]	no	crypto	*weak*	**strong**	*weak*
MOAS Detection [86]	no	anomaly	none	none	*weak*
Intrusion Detection [89]	no	anomaly	none	none	*weak*
PHAS [90]	no	anomaly	none	none	*weak*
Pretty Good BGP	no	anomaly	*weak*	none	*weak*
Real-Time Monitoring (Hu and Mao)	no	anomaly	none	none	*weak*
Whisper [95]	no	anomaly	none	*weak*	none
Pretty Good BGP [91]	no	anomaly	none	**strong**	**strong**

Conclusions

- Difficulties in Adopting Solutions
  - Number of ASes Increases Linearly with Time
  - Routing Registries Must Contain Up-to-Date Info
  - Computation Requirements Can Overload Routers
  - Simulation Impossible Due to Size of Internet
- Future Research Directions
  - Routing Frameworks and Policies (BCP)
    - Protect the Most Important Nodes
  - Attack Detection: Stop Attacks Before They Start
  - Data Plane Protection: Enforce Decisions
  - Partial Deployment: Gains from Limited Participation

Questions?