Securing BGP

Geoff Huston

November 2007

Agenda

- An Introduction to BGP
- BGP Security Questions
- Current Work
- Research Questions

An Introduction to BGP

Background to Internet Routing

- The routing architecture of the Internet is based on a decoupled approach to:
  - Addresses
  - Forwarding
  - Routing
  - Routing Protocols

- The routing system is the result of the interaction of a collection of many components, hopefully operating in a mutually consistent fashion!

IP Addressing

- IP Addresses are not locationally significant
  - An address does not say “where” a device may be within the network
  - An address does not determine how a packet is passed across the network
  - It’s the role of the *routing system* to announce the “location” of the address to the network
  - It’s the role of the *forwarding system* to direct packets to this location

IP Forwarding

- Forwarding is a local autonomous action
  - Every IP routing element is equipped with a forwarding table
- End-to-end packet forwarding relies on mutually consistent populated forwarding tables held in every routing element
- The role of the *routing system* is to maintain these forwarding tables

IP Routing

- The routing system is a collection of switching devices that participate in a self-learning information exchange (through the operation of a routing protocol)
- All self-learning routing systems have a similar approach:

  You tell me what you know and I'll tell you what I know!
- The objective is to support a distributed computation that produces consistent "best path" outcomes in the forwarding tables at every switching point, at all times
- Routing involves significant levels of mutual trust

Routing Structure

- The Internet's routing architecture uses a 2-level hierarchy, based on the concept of a *routing domain* ("Autonomous System")
- A "domain" is an interconnected network with a single exposed topology, a coherent routing policy and a consistent metric framework

- *Interior Gateway Protocols* are used *within* a domain
  - OSPF, IS-IS
- *Exterior Gateway Protocols* are used to *interconnect* domains, or "Autonomous Systems" (ASes)
  - BGP

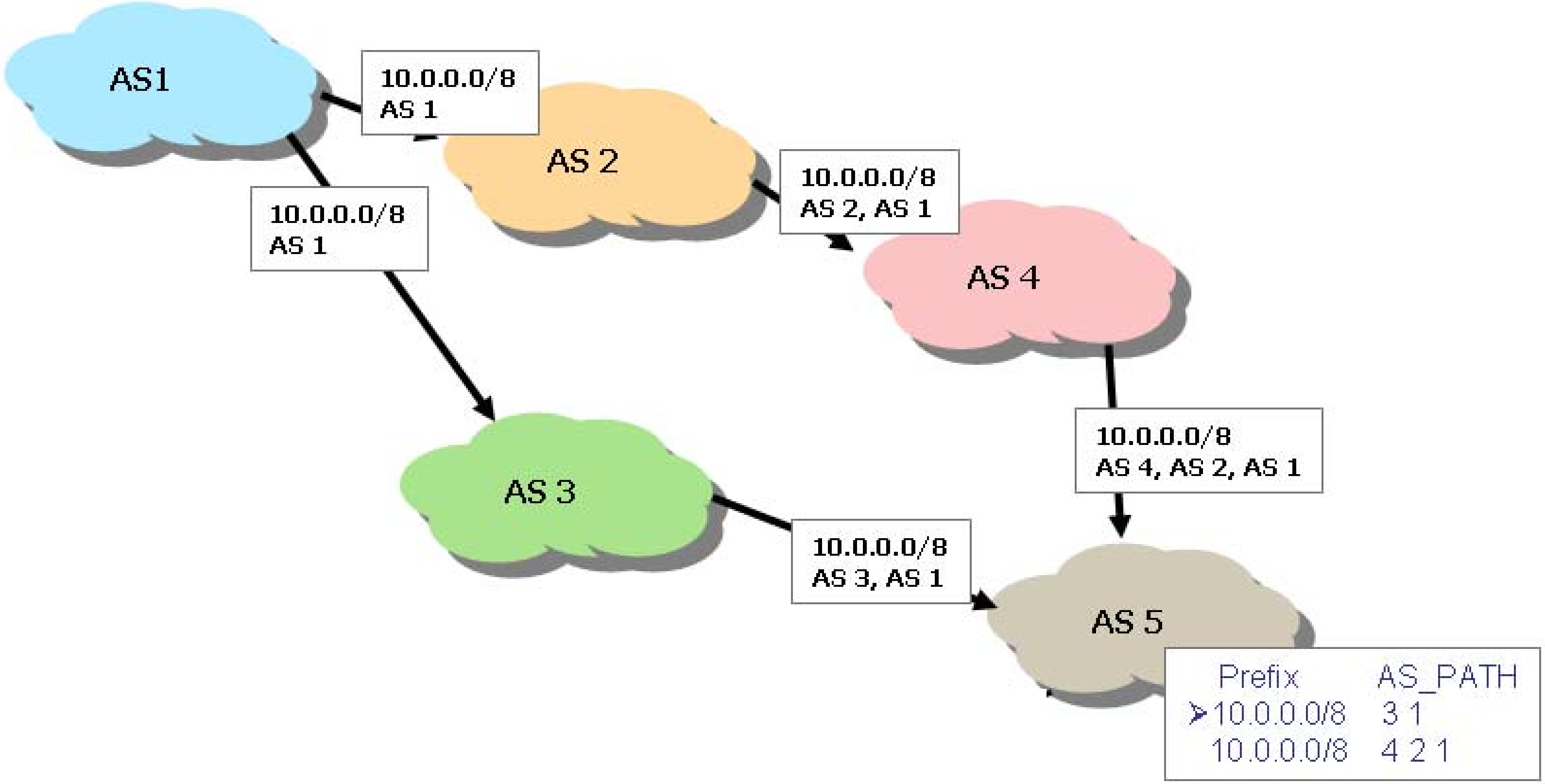
BGPv4

- BGP is a Path Vector Distance Vector exterior routing protocol
- Each routing object is an address and an attribute collection
  - Attributes: AS Path vector, Origination, Next Hop, Multi-Exit-Discriminator, Local Pref, …
- The AS Path attribute is a vector of AS identifiers that form a viable path of AS transits from this AS to the originating AS
  - The AS Path Vector is used to perform rapid loop detection and a path metric to support route comparison for best path selection

BGP is an inter-AS protocol

- Not hop-by-hop
- Addresses are bound to an “origin AS”
- BGP is an “edge to edge” protocol
  - BGP speakers are positioned at the inter-AS boundaries of the AS
  - The “internal” transit path is directed to the BGP-selected edge drop-off point
  - The precise path used to transit an AS is up to the IGP, not BGP
- BGP maintains a local forwarding state that associates an address with a next hop based on the “best” AS path
  - Destination Address -> [*BGP Loc-RIB*] -> Next Hop address
  - Next_Hop address -> [*IP Forwarding Table*] -> Output Interface

BGP Example



Prefix	AS_PATH
➢10.0.0.0/8	3 1
10.0.0.0/8	4 2 1

BGP Transport

- TCP is the BGP transport
  - Reliable transmission of BGP Messages
    - Messages are never repeated!
  - Capability to perform throttling of the transmission data rate through TCP window setting control
- May operate across point-to-point physical connections or across entire IP networks

BGP is an *incremental* protocol

- Maintains a collection of local “best paths” for all advertised prefixes
- Passes incremental changes to all neighbours rather than periodic full dumps
- A BGP update message reflects changes in the local database:
  - A new reachability path to a prefix that has been installed locally as the local best path (update)
  - All local reachability information has been lost for this prefix (withdrawal)

Messaging protocol

- The TCP stream is divided into messages using BGP-defined “markers”
- Each message is a standalone protocol element
- Each message has a maximum size of 4096 octets

BGP Messages

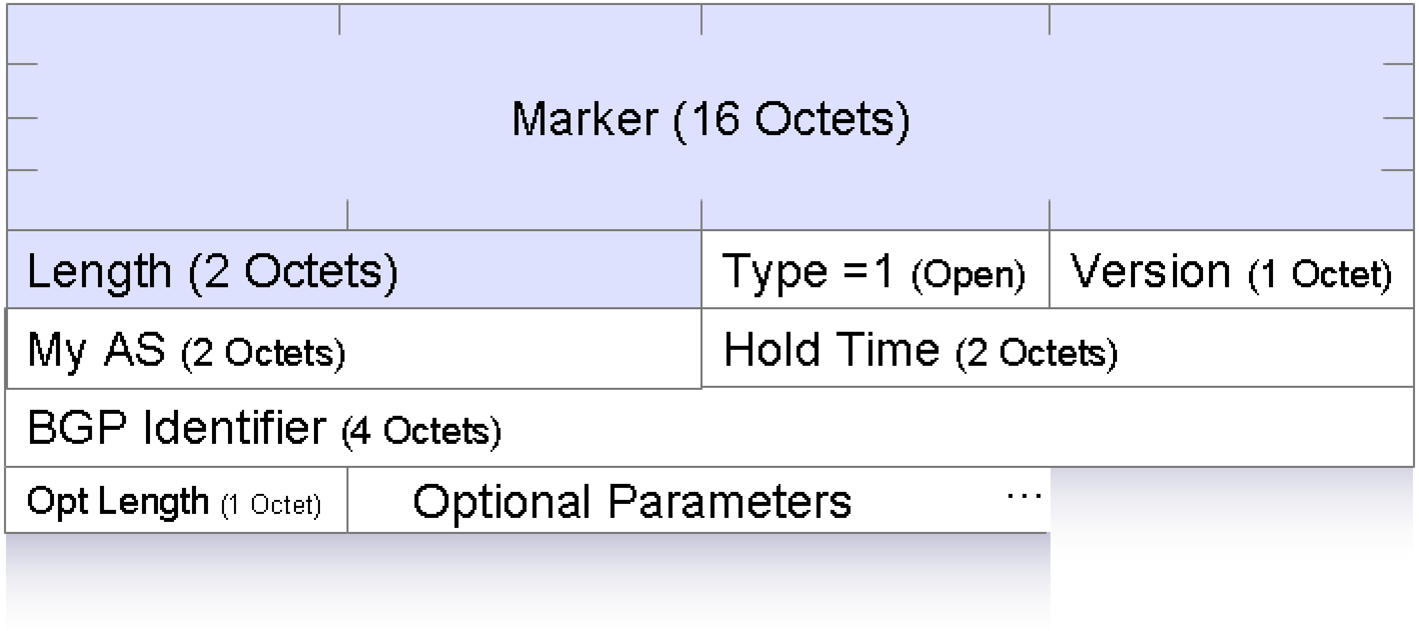
```
2007/07/15 01:46
    ATTRS: nexthop 202.12.29.79,
           origin i,
           path 4608 1221 4637 3491 3561 2914 3130
    PFX:   198.180.153.0/24
```

```
2007/07/15 01:46
    WDL:   64.31.0.0/19,
           64.79.64.0/19
           64.79.86.0/24
```

```
2007/07/15 01:46
    ATTRS: nexthop 202.12.29.79,
           origin i,
           path 4608 1221 4637 16150 3549 1239 12779 12654
    PFX:   84.205.74.0/24
```

```
2007/07/15 01:47
    ATTRS: nexthop 202.12.29.79,
           origin i,
           path 4608 1221 4637 4635 34763 16034 12654
    PFX:   84.205.65.0/24
```

BGP OPEN Message



Marker (16 Octets)

Length (2 Octets)

Type =1 (Open)

Version (1 Octet)

My AS (2 Octets)

Hold Time (2 Octets)

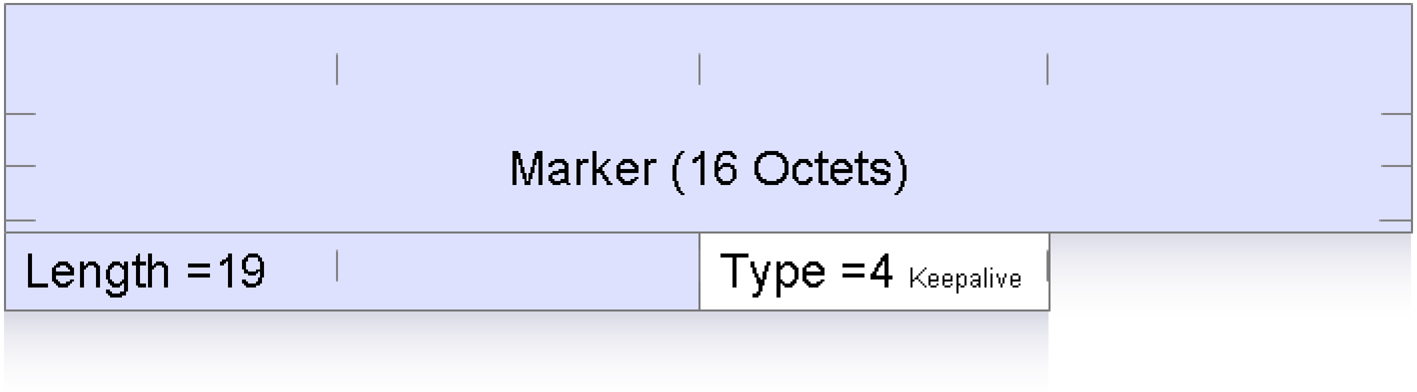
BGP Identifier (4 Octets)

Opt Length (1 Octet)

Optional Parameters …

- Session setup requires mutual exchange of OPEN messages
- My AS field is the local AS number
- Hold time is inactivity timer
- BGP identifier code is a local identification value (loopback IPv4 address)
- Options allow extended capability negotiation
  - E.g. Route Refresh, 4-Byte AS, Multi-Protocol

BGP KEEPALIVE Message



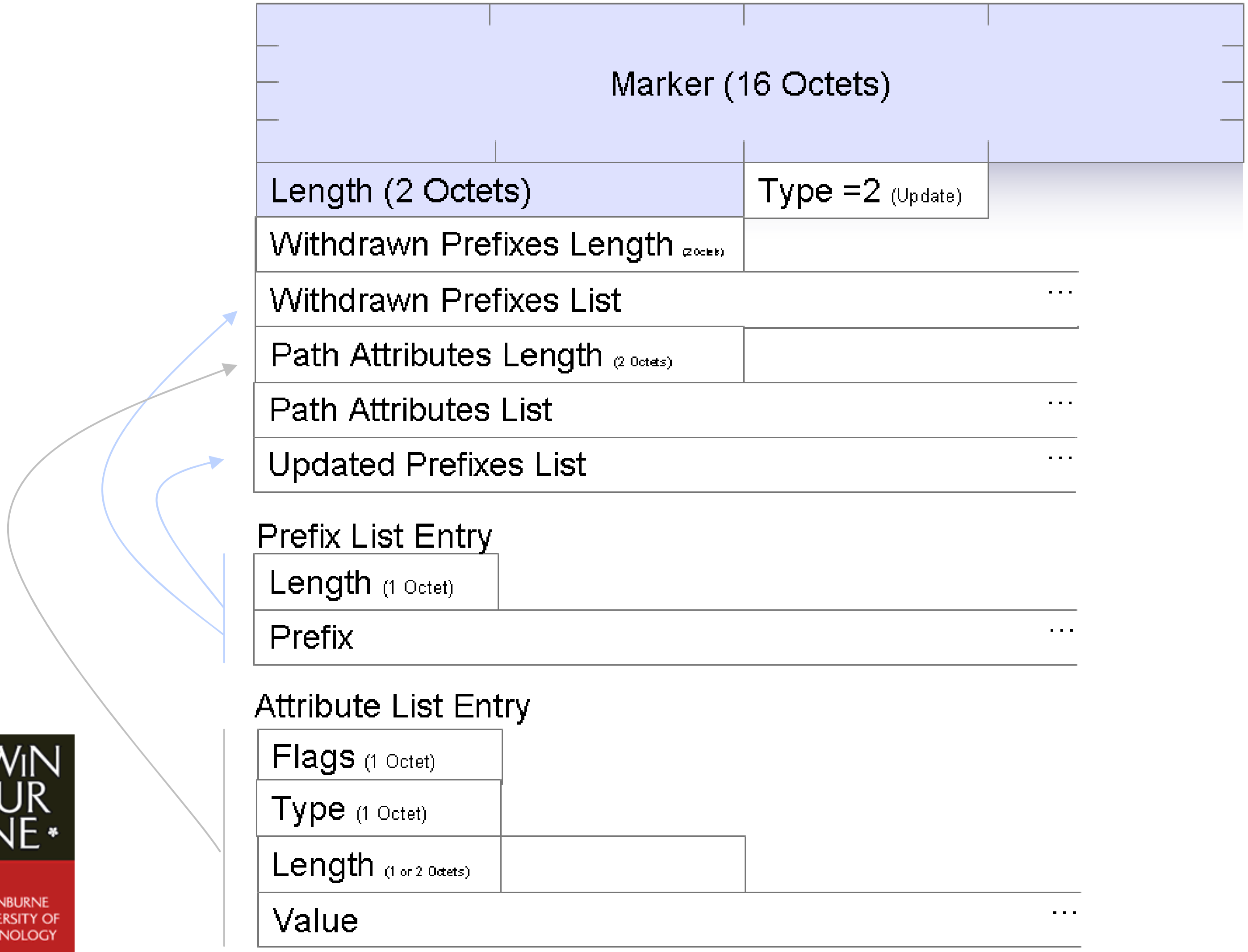
Marker (16 Octets)

Length =19

Type =4 Keepalive

- “null” message
- Sent at 1/3 hold timer interval
- Prevent the remote end triggering an inactivity session reset

BGP UPDATE Message



Marker (16 Octets)

Length (2 Octets)

Type =2 (Update)

Withdrawn Prefixes Length (2 Octets)

Withdrawn Prefixes List …

Path Attributes Length (2 Octets)

Path Attributes List …

Updated Prefixes List …

Prefix List Entry

Length (1 Octet)

Prefix …

Attribute List Entry

Flags (1 Octet)

Type (1 Octet)

Length (1 or 2 Octets)

Value …

BGP UPDATE Message

- List of withdrawn prefixes
- List of updated prefixes
  - Set of “Path Attributes” common to the updated prefix list

- Used for announcements, updates and withdrawals
- Can piggyback withdrawals onto announcements
  - But this happens rarely in practice today

AS Path Attribute

- **AS_PATH** : the vector of AS transits forming a path to the origin AS
  - □ In theory the BGP Update message has transited the reverse of this AS path
  - □ In practice it doesn’t matter
    - The AS Path is merely a loop detector and a path metric

BGP Security Questions

BGP Security

- How do we talk?
    - Securing the TCP session
- Whom am I talking to?
    - Securing the BGP session
- What are you saying?
    - Verifying the authenticity and completeness of the routing information
- Should I believe you?
    - Verifying the integrity of the forwarding system

How do we talk?

- Long held TCP session
- Threats:
  - eavesdropping
  - session reset
  - session capture
  - message alteration
  - host processing exposure
  - host memory exposure

Whom am I talking to?

- Authenticate the BGP peer
  - MD5 and password exchange
    - Symmetric crypto is faster than asymmetric public / private key crypto
    - But key rollover is a problem
  - IPSEC
    - More agile key management
    - Stronger session protection
    - Higher overhead
- Are you who you say you are?
  - AS number PKI to validate AS right-of-use assertions

What are you saying?

- Announcing a route object
  - Requires update credentials
- Altering a route object
  - Requires update credentials
- Withdrawing a route object
  - Does not require update credentials
    - If I believe your announcement then I’ll believe your withdrawal

Should I believe you?

Update Credentials

- Origination part
  - AS a announces Prefix p
- Accumulation part
  - Update has AS path vector (x, y, z, a)
- Hop-by-hop part
  - Update has community value a::b

Origination Validation

- Is this a “valid” prefix?
- Has the prefix’s owner given this AS the authority to originate an announcement for this prefix into the routing system?
- Can I validate the prefix and the authority using my trust anchors?

AS Path Validation

- Did each AS in the AS Path vector add itself into the path vector?
  - Did the update propagate along precisely the same AS transit sequence as the AS Path vector?
- Is this a feasible forwarding path?
  - Could this packets I send actually be forwarded in the reverse direction along this AS path vector?
- Is this the actual forwarding path?
  - Can I validate that this AS Path vector represents the actual forwarding path?

Current Work

Current Proposals

- Secure BGP
- Secure origin BGP
- Pretty Secure BGP
- Internet Route Validation
- DNSV

sBGP

- PKI for addresses and ASes using the address distribution hierarchy
- Digitally signed attestations:
  - ROA to allow a prefix holder to authorize an AS to undertake route origination
  - Router Attestation to attest that a router is authorized to act for a particular AS
- Distribute PKI, ROAs and Router Attestations
- Augment BGP Updates with
  - origination signature
  - AS Path signature
    - Nested digital sequence, incrementally signed across (previous sign, prefix, this AS, next AS)

sBGP Observations

- Generally regarded as the most complete specification of securing routing system
- Has the following drawbacks
  - Requires a PKI for addresses and ASes
  - Requires a novel mechanism to distribute attestations and validation material to every sBGP speaker
  - Requires certification for every router
  - High memory load
  - High processing load due to use of asymmetric crypto
  - High time penalty
  - Unclear as to the implications of off-loading sBGP processing
  - Incremental deployment is not supported in a robust manner

soBGP

- Assumes no PKI
- Relies on assertions by ASes
  - Address origination
  - AS Peering
- Distribution of assertions to all parties
- Augment BGP with
  - origination signature
  - Validate AS Path using AS Peering assertion graph for feasibility

soBGP Observations

- Hard to discern what is actually secured in soBGP
- Address assertions imply vulnerabilities from cooperating ASes
- AS peering assertions imply vulnerabilities from cooperating ASes
- No external independent validation mechanism for assertions implies weak security for address validity and AS peering adjancies
- AS peering attestations imply poor protection for the integrity of the AS path

psBGP

- Assumes a PKI for ASes, but no PKI for addresses (?)
- Uses AS assertions for
  - Address origination
  - AS Peering
  - Peer AS’s address origination
- Augment BGP with
  - Origination signature
    - Validate signature using reputation calculation
  - Validate AS Path using AS Peering assertion graph for feasibility

psBGP Observations

- Assumes PKI for ASes but no PKI for addresses – why?
- Relies on calculation of relative trust in neighbours’ attestations
- Attempt to post-fix web of trust models with explicit calculation of trust level
- Solution looking for a problem?

IRV

- No modifications to BGP
- Uses OCSP-like approach to perform a ‘back’ query to validate a BGP update
    - Query the origination AS’s IRV server for origination
    - Query the transit ASs’ IRV servers for AS Path

IRV Observations

- Origination information can be distributed in a signed form
  - No need to perform post-fact queries
- Chained queries to validate the path is heavier overhead than a compound signed path
- Implies delayed validation pass
  - Is short term vulnerability acceptable?
- Solution looking for a problem?

DNSV

- Early proposal
- Place the authority provided by a prefix holder to permit an AS to originate an advertisement into the DNS
- Needs an address PKI and DNSSEC in order to inject reliability into the address part of the DNS
- And if you have an address PKI and an AS PKI then why not use origination attestations and bypass the DNS step?

Refinements

- Numerous papers, generally concentrating on the AS path validation problem of sBGP
- Common starting assumption - its all too cumbersome!
- Improve speed of validation
  - Use update aggregation to replace asymmetric cryptography with symmetric cryptography by using one way hash chains and hash trees
  - Elliptical cryptography to aggregate across an AS Path signature sequence
- Reduce validation processing load
  - Delay validation of update until the update has reached a stable state (convergence)
  - Cache validation outcomes for reuse
  - Modify BGP to reduce update load profile
- Delayed validation
  - Avoid potential circular dependencies of requiring to accept the route in order to validate the credentials associated with the route
- Reduce information space
  - Use additional layers of indirection in routing to reduce the population of the routed object set

Research Questions

Research Questions

- What is essential and what is desireable in securing BGP?
  - BGP vs secure BGP performance profile
    - BGP performance profile is measured in terms of: Time to converge, size of RIBs, router processor load, router memory load, router autonomy, routing system robustness, routing system scaling capability
    - What are the acceptable trade-offs in terms of current understandings of acceptable BGP performance characteristics?
      - Is there a commonly accepted answer?

Research Questions

- Is securing the routing system alone actually helpful and valuable?
  - Can you validate forwarding paths being proposed by a routing system?
    - Is secure routing helpful in and of itself?
    - Or this this just pushing the vulnerability set to a different point in the network integrity space?
- If not, then is this a case of too high a cost or too low a benefit?
  - Is this a case of reducing the security credential generation and validation workload by reducing the security outcomes through reduced trust and/or reduced amount of validated information
  - Or is this a case of increasing the level of assurance and the amount of routing information secured by these mechanisms

Research Questions

- Are the semantics of routing security and incomplete credentials compatible concepts?
  - Can you deploy high integrity security using partial deployment scenarios?
  - Is BGP too incomplete in terms of its information distribution properties to allow robust validation of the intended forwarding state?
  - Does securing forwarding imply carrying additional information relating to the routing and forwarding state coupling in additon to routing

Questions?