An Operational Perspective on BGP Security

Geoff Huston

February 2005

Asia Pacific Network Information Centre
APNIC

Disclaimer

This is not a description of the approach taken by any particular service provider in securing their network. It is intended to illustrate the set of trade-offs that are typical in the ISP environment and the current status of securing inter-domain routing in the Internet.

Its about Management of Risk

- Operational security is not about being able to create and maintain absolute security. Its about a pragmatic approach to risk mitigation, using a trade-off between cost, complexity, flexibility and outcomes

- Making a reasoned judgement to spend a certain amount of resources in order to achieve an acceptable risk outcome

Risk Management

Understand the threat model:

- What might happen?
- What are the likely consequences?
- How can the consequences be mitigated?
- What is the cost tradeoff?
- Does the threat and its consequences justify the cost of implementing a specific security response?

Asia Pacific Network Information Centre
APNIC

Lets talk routing security…

Protecting routing protocols and their operation

- What you are attempting to protect against are efforts intended to:
  - Compromise the topology discovery / reachability operation of the routing protocol
  - Disrupt the operation of the routing protocol

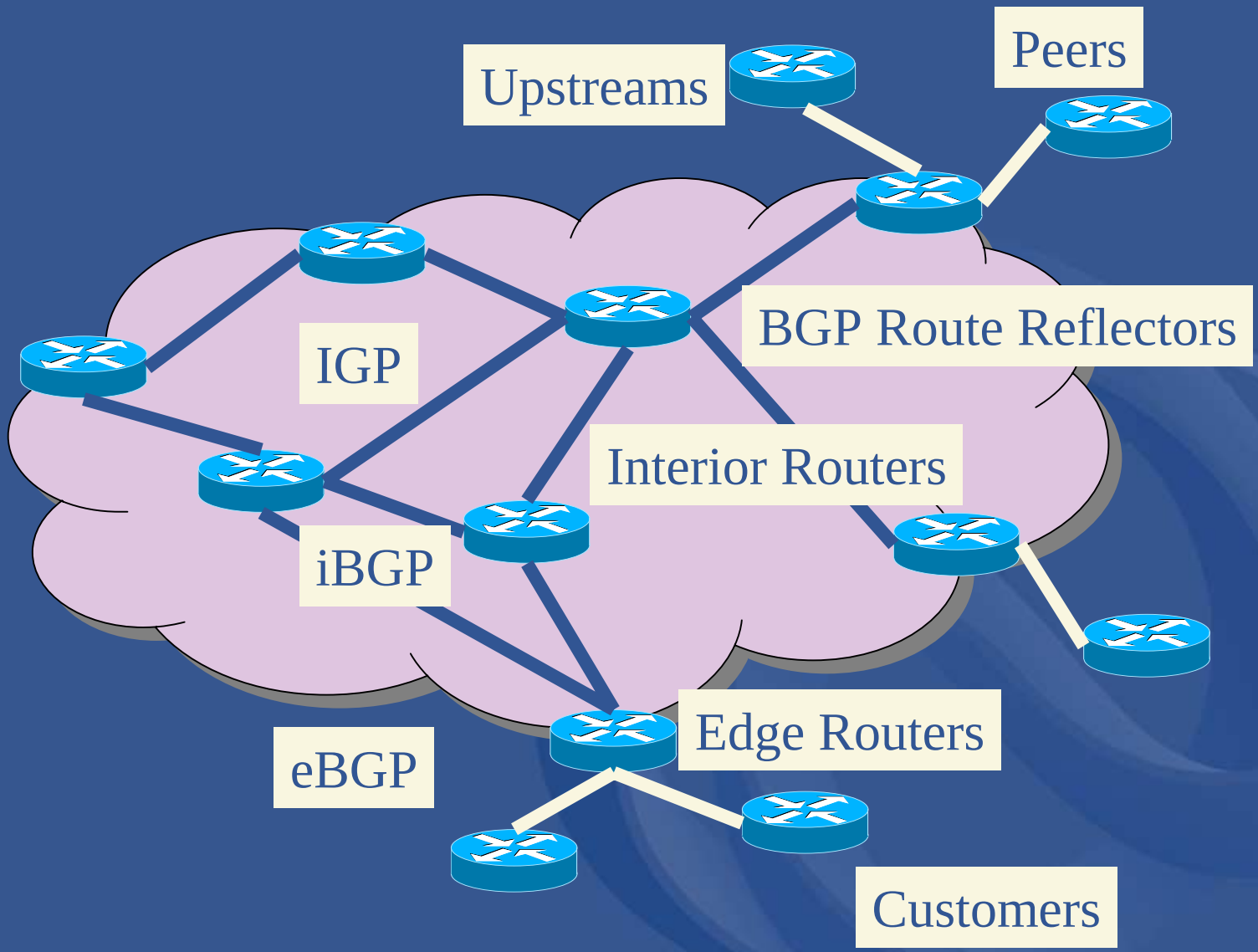
Protecting the protocol payload

- What you are attempting to protect against are efforts intended to:
  - Insert corrupted address information into your network's routing tables
  - Insert corrupt reachability information into your network's forwarding tables

The threat

- Corrupting the routers' forwarding tables can result in:
  - Misdirecting traffic (subversion, denial of service, third party inspection, passing off)
  - Dropping traffic (denial of service, compound attacks)
  - Adding false addresses into the routing system (support compound attacks)
  - Isolating or removing the router from the network

Components of the network model



The routing model

IGP

- used to manage interior topology
- IGP payload is interior interface and loopback addresses

BGP

- Used to manage external routes
- Implements local routing policies

Asia Pacific Network Information Centre
APNIC

Basic Network design

Isolate your network at the edge:

- Route all traffic at the edge
- NO sharing LANs
- NO shared IGPs
- NO infrastructure tunnels

Isolate your customers from each other:

- NO shared access LANs

Isolate routing roles within the network:

- Exterior-facing interface routers
- Internal core routers

Configuration Tasks - Access

- Protecting routing configuration access
  - ssh access to the routers
  - filter lists
  - user account management
  - access log maintenance
  - snmp read / write access control lists
  - protect configurations
  - monitor configuration changes
- Protecting configuration control of routers is an essential part of network security

Configuration Tasks – IGP

- Protecting the IGP
  - No shared IGP configurations
    - Don't permit third party managed equipment to participate in IGP routing
  - No IGP across shared LANs!
    - shared LANs represent a point of vulnerability

Asia Pacific Network Information Centre
APNIC

Configuration Tasks - BGP

- Protecting BGP
  - Protect the TCP session from intrusion
  - Minimize the impact of session disruption on BGP.
  - Reduce third party dependencies to a minimum (use local nexthop targets, for example)
  - Monitor and check

Configuration Tasks - BGP

- Basic BGP configuration tasks:
  - No redistribution from iBGP into the IGP
  - Use session passwords and MD5 checksums to protect all BGP sessions
  - For iBGP use the local loopback address as the nexthop (next-hop-self)
  - Use filter lists to protect TCP port 179
  - Use maximum prefix limiting (hold mode rather than session kill mode preferred)
  - Use eBGP multi-hop with care (and consider using TTL hack)
  - Align route reflectors with topology to avoid iBGP traffic floods
- Operating BGP:
  - Use soft clear to prevent complete route withdrawals
  - Use BGP session state and BGP update monitors and generate alarms on session instability and update floods

Configuration Tasks – BGP

- Check your config with a current configuration template
  - Rob Thomas' template at http://www.cymru.com/Documents/secure-bgp-template.html is a good starting point
  - Remember to regularly check the source for updates if you really want to using a static bogon list

BGP Configuration template

- Global settings
  - Record neighbor state changes
    - bgp log-neighbor-changes
  - Set route dampening
    - Don't damp DNS rootserver routes
    - Damp flapping customer-advertised routes using prefix-length sensitive settings
    - Don't damp upstream-advertised routes
  - No route redistribution from iBGP into IGP

BGP Configuration template

- Per-Neighbor settings
  - Reduce impact of session reset
    - Always perform soft reset of BGP sessions
  - MD5 protection of the TCP session
    - Per-neighbor password
  - Use per-neighbor prefix filter templates
    - Inbound and outbound filters on prefixes
  - Use local address for nexthop
    - Next-hop-self
  - Use maximum prefix threshold with hold option
    - Maximum-prefix <n> discard-over-limit
  - Don't negotiate the BGP version
    - Version 4
  - IP filters for TCP port 179
  - If using multihop, then use TTL threshold

Protecting the payload

- How to increase your confidence in determining that what routes you learn from your eBGP peers is authentic and accurate
- How to ensure that what you advertise to your eBGP peers is authentic and accurate

Customer Routes

- Authenticate customer routing requests:
  - Check validity of the address
    - Own space – validate request against local route object registry
    - Other space – validate request against RIR route object database registered POC
      - This is often harder than it originally looks!
  - Adjust explicit neighbor eBGP route filters to accept route advertisements for the prefix
  - Apply damping filters

SKA Peer Routes

- Higher level of mutual trust
- Accept peer routes - apply local policy preferences
- Filter outbound route advertisements according to local policy settings
- Use max prefix with “discard-over-limit” action (if available)

Upstream Routes

- One-way trust relationship
- Apply basic route filters to incoming route advertisements
  - RFC 1918 routes
  - own routes (?)

Even so

- Its not all that good is it?

Routing Security

- The basic routing payload security questions that need to be answered are:
  - Who injected this address prefix into the network?
  - Did they have the necessary credentials to inject this address prefix? Is this a valid address prefix?
  - Is the forwarding path to reach this address prefix trustable?
- What we have today is a relatively insecure system that is vulnerable to various forms of disruption and subversion
  - While the protocols can be reasonably well protected, the management of the routing payload cannot reliably answer these questions

What I really want to see…

- The use of authentication certificate chains to allow automated validation of:
  - the authenticity of the route object being advertised
  - authenticity of the origin AS
  - the binding of the origin AS to the route object
- Such certificates to be carried in BGP as payload attributes
- Certificate validation to be a part of the BGP route acceptance / readvertisement process

What would also be good…

- A mechanism to check the validity of a received AS path

And what should be retained…

- Is BGP as a “block box” policy routing protocol
  - Many operators don’t want to be forced to publish their route acceptance and redistribution policies.
- BGP as a “near real time” protocol
  - Any additional overheads of certificate validation should not impose significant delays in route acceptance and readvertisement

Status of Routing Security

- We are nowhere near where we need to be
- We need more than “good routing housekeeping”
- We are in need of the adoption of basic security functions into the Internet’s routing domain
  - Injection of reliable trustable data
    - Address and AS certificate injection into BGP
  - Explicit verifiable trust mechanisms for data distribution
    - Adoption of some form of certification mechanism to validate routing protocol information distribution

Thank You!