An Operational Perspective on BGP Security

Geoff Huston

GROW WG

IETF 63

August 2005

Risk Management

- 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

- Its about making an informed and reasoned judgment to spend a certain amount of resources in order to achieve an acceptable risk outcome

Threat Model

Understanding the threat model for routing

- 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?

Routing Security…

Protecting routing protocols and their operation

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

Threats

- 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

Operational Security Measures

- Security considerations in:
  - Network Design
  - Device Management
  - Configuration Management
  - Routing Protocol deployment
- Issues:
  - Mitigate potential for service disruption
  - Deny external attempts to corrupt routing behaviour or payload

Protecting the BGP 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

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 **credible**?
- 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 (personally) really want to see…

- The use of authenticatable attestations 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 attestations used to provide a cost effective method of validating routing requests
  - as compared to the today's state of the art based on techniques of vague trust and random whois data mining

And what would be even better…

- Such attestations to be carried in BGP as payload attributes
- Attestation validation to be a part of the BGP route acceptance / readvertisement process

And what (I think) should be retained…

- 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

- It would be good to adopt some basic security functions into the Internet's routing domain
  - Certification of Number Resources
    - Is the current controller of the resource verifiable?
  - Explicit verifiable trust mechanisms for data distribution
    - Signed routing requests
    - Adoption of some form of certificate repository structure to support validation of signed routing requests
    - Have they authorized the advertisement of this resource?
    - Is the origination of this resource advertisement verifiable?
  - Injection of reliable trustable data into the protocol
    - Address and AS certificate / authorization injection into BGP

Next Steps?

- PKI infrastructure support for IP addresses and AS numbers
- Certificate Repository infrastructure
- Operational tools for nearline validation of signed routing requests / signed routing filter requests / signed entries in route registries
- Carrying signature information as part of BGP Update attribute

Question for GROW

- Is there interest in working on specification / description of tools that use a resource PKI for near line validation of routing requests?