Secure Origin BGP (soBGP)

Alvaro Retana (aretana@cisco.com)
IP Routing Deployment and Architecture
Core IP Engineering
Agenda

• Where is soBGP coming from?
• What problems does soBGP solve?
• How does soBGP solve these problems?
  Deployment Examples
  What is needed to deploy soBGP?
• Current Status
BGP Security Background

- BGP ties the Internet together
  Critical Communications and Business Infrastructure!
- The system is vulnerable to different threats
  Configuration/Human Errors
  “Patches” have been applied as threats are exploded – most implemented on point-to-point connections
- End-to-end solutions require collaboration from all the users of the system: SPs, enterprise users, vendors, etc.
BGP Security – No Single Answer

• Solutions exist and have been deployed to solve or counteract individual threats
  Inbound filters, route limits, martian checks, implementation enhancements, etc.
  Independent of each other and include solutions external to the system (to secure compromised routers and/or guarantee availability)

• The BGP Transport Connection
  Existing mechanisms have already been designed and deployed to protect it: TCP MD5, IPSec.

• soBGP (Secure Origin BGP) targets the need to verify the validity of an advertised prefix
  Is the originator authorized to advertise the route?
Agenda

• Where is soBGP coming from?
• What problems does soBGP solve?
• How does soBGP solve these problems?

Deployment Examples

What is needed to deploy soBGP?

• Current Status
soBGP Goal

- Validate an AS is authorized to originate a prefix.
  
  Verify a peer which is advertising a prefix has at least one valid path to the destination.
soBGP Design Requirements

• System should take advantage of operational experience and existing Internet Architecture.
  Implicit trust built into the Internet
  IP address assignment and delegation system

• Minimize impact to current implementations of the BGP protocol
  Minimum changes to existing protocol formats.
  Optimize memory and processing requirements.
soBGP Design Requirements (cont.)

• Must *not* rely on a central authority of any type.
  Distributed processing and trust

• Should not rely on routing to secure routing (No external database connection on system initialization).
soBGP Design Requirements (cont.)

- Must be incrementally deployable (it must provide some level of security without the participation of every AS).
- Must allow deployment flexibility (on box or off box cryptography, etc.).
- Flexibility should be provided to allow operators to configure the level of security vs. overhead and convergence speed.
Agenda

• Where is soBGP coming from?
• What problems does soBGP solve?
• How does soBGP solve these problems?

Deployment Examples
What is needed to deploy soBGP?

• Current Status
soBGP At-a-Glance

• Verifies that the originator of a route is authorized to do so.
  Verifies that the advertised AS_PATH represents a valid path to the originator.

• BGP Security Message (extension to BGP)
  New BGP Message used to carry security information
  No changes to existing messages for backwards compatibility and incremental deployment.
  Leverages existing and future protocol and security mechanisms

• Fixed additional scalability requirements
  Per-AS information and route policies advertised once.
  No additional information in UPDATES, resulting in low processing impact.
soBGP At-a-Glance (cont.)

- Takes advantage of the existing Internet Architecture
  Trust relationships, loose AS associations, etc.
- Use of Certificates to advertise and correlate AS identity, prefix ownership and route policy.
  - Entity Certificate = Used to establish identity
  - Authorization Certificate = Used to assign and delegate IP address space
  - Policy Certificate = Used to define per-AS or pre-prefix policies and propagate AS interconnectivity topology map
- Uses Web-of-Trust model to validate certificates.
  - No specific root (single point of failure), but distributed responsibility.
soBGP At-a-Glance (cont.)

• Built in Flexibility

UPDATE and Certificate propagation may be decoupled.

On or off-box cryptography operations (inside the local AS).

Incrementally deployable – provides some security in any multi-AS scenario.

Configurable level of validation and weights.
Certificate Transport

• Certificates are transported in a new BGP message type, the SECURITY message.
  • Certificates are carried within TLVs
  • Expandable to other security related information

• Negotiated at session startup (capability exchange)
  • Certificates may be exchanged before routing
  • Routing may be exchanged before certificates
  • Certificates only session may exist
BGP Security Message

- Security information carried inside the protocol
  The system doesn’t rely on routing to secure it.
  Propagation characteristics similar to those of UPDATES: Internet-wide reach!

- No changes in UPDATES or other BGP messages.
  Additional memory requirement doesn’t increase with the number of routes in the system...but with the number of entities and blocks authorized.
  No additional memory/processing requirements for routers that do not need/want to receive security information.

- Ability to have non-congruent UPDATE and Security Information propagation topologies
  Only BGP speakers that need the information have to receive it.
  No need to upgrade non-soBGP routers.
  Configurable security information and UPDATE propagation priorities.
Certificate Operation

**EntityCert**
- Signer AS
- AS
- PubKey

**PolicyCert**
- AS
- Policy

**AuthCert**
- Auth AS
- AS
- Address

Known valid keys:
- AS
- PubKey

Topology graph:
- Topology database:
  - Origin
  - AS Path
  - Prefix

Update

Routing DNA

soBGP – NANOG28

© 2003, Cisco Systems, Inc. All rights reserved.
Route Validation

- No cryptographic overhead in UPDATE validation and propagation
  - Databases may be pre-built for faster lookup.
  - Origin authorization and validity of AS_PATH verified.
- Web Of Trust used to authenticate and validate the information carried in the certificates.
  - Known keys are seeded by local administrator.
- Certificate Memory and processing requirements are a function of the number of Autonomous Systems and the number of authorized blocks
  - Reduced incremental memory and processing (vs carrying information in UPDATES).
  - No impact if router doesn’t need to verify authorization.
- Policy Information carried independent of authorization information
  - Flexible policies.
  - Allows originator to change policy (or connectivity information) without having to re-advertise UPDATES or other certificates.
Deployment

- The most straightforward deployment option is:
  - Exchange certificates at all eBGP peering points (AS edges).
  - Process the certificates, and build the required soBGP tables at each eBGP speaker.
  - Each eBGP speaker must then be capable of running the cryptographic processes needed to process certificates.
Deployment

• Certificates can also be exchanged at the AS edge, and “shuttled,” using iBGP connections, to a server within the AS.

• These servers then perform all certificate processing, and build the necessary databases.

• The edge routers then consult these servers, using RADIUS, to validate received updates.
• Certificates can also be exchanged, using multihop eBGP directly between the soBGP servers in each AS.
Deployment

- Certificates may also be exchanged with third party providers of some type.
- Certificates may be generated by one AS, and advertised by another AS.
- It doesn’t matter how the certificates injected into the internetwork, or received, as long as the same validation process is used.
Incremental Deployment

- Incremental deployment is a large hurdle for any security system.
- There’s no way to have a “flag day,” after which all AS’ must be running the security system, in a large internetwork.
- soBGP allows incremental deployment—*but the amount of security provided is proportional to the completeness of the deployment!*
Incremental Deployment

The two autonomous systems which would like to run soBGP can exchange their certificates directly through eBGP multihop sessions, or through some other mechanism.
Incremental Deployment

- They are able to validate the second hop in the AS Path, using the connectivity advertised in the PolicyCerts.
- As more of the AS’ participate, more of the path can be validated.
Deployment Example

The AS7007 Case

- In short, AS7007 de-aggregated the full BGP table and injected it back into the Internet. The result was that all the Internet traffic black holed into it.

http://flix.flirble.org/

De-aggregated Internet Table!

AS7007 — ISP S — ISP O — ISP M

Origin

10.1.0.0/16

10.1.1.0/24
Deployment Example I

The AS7007 Case

• AS7007 re-advertises the prefixes as originated by itself.

\[
\text{AS\_PATH} = 7007
\]

soBGP: no AuthCert allows 7007 to advertise 10.1.1.0/24!!
Deployment Example II

The AS7007 Case

- AS7007 re-advertises the prefixes as originated by the “origin”.

  \[\text{AS\_PATH} = 7007 \text{ Origin}\]

soBGP: Topology Graph doesn’t include link between “origin” and 7007!!
Deployment Example III

The AS7007 Case

- AS7007 re-advertises the prefixes as originated by the “origin” and adds itself to the AS_PATH; multi-homed case.

\[
\text{AS\_PATH} = 7007 \text{ ISP-S ISP-O Origin}
\]

soBGP: PolicyCert includes information about longest advertised prefix.

soBGP: PolicyCert can include information about non-transit SP customers OR no connectivity information (results in only being able to originate routes).
What is needed to deploy soBGP?

- soBGP capable software in routers and supporting devices.
- Infrastructure to generate certificates (local PolicyCerts, etc.)
- Certificates from other ISPs, RIRs or other trusted entities authenticating identity (ASN) and address allocation.
- Propagate certificates in-band using BGP Security Message.

  New information propagated on-demand (no periodic download needed).
Agenda

- Where is soBGP coming from?
- What problems does soBGP solve?
- How does soBGP solve these problems?
  Deployment Examples
  What is needed to deploy soBGP?
- Current Status
Current Status

• Drafts Submitted to IETF

  Extensions to BGP to Support Secure Origin BGP (soBGP)
  (draft-ng-sobgp-bgp-extensions –xx)

  Deployment Considerations for Secure Origin BGP (soBGP)
  (draft-white-sobgp-bgp-deployment- xx)

  RADIUS Attributes for soBGP Support (draft-lonvick-sobgp-
  radius- xx)

• Definition of Extensions complete

  Complete PKI definition, X.509 Certificate formats, etc. in
  progress.

• Code in Development (in IOS)

  Stretch goal is to be able to deploy soBGP in existing
  routers. **
Summary

- soBGP addresses the problem of verifying the ability of an AS to originate a route
- Incremental deployment without impact to ASes not implementing soBGP
  - Partial deployment also possible
- soBGP follows the existing Internet Architecture taking advantage of the implicit trust between ASes.
For More Information

soBGP:

ftp://ftp-eng.cisco.com/sobgp

The mailing list is open, archives are available, draft participation is encouraged!

Routing Protocols Security:

http://www.rpsec.org