BGP Security
A Range of Solutions

Sandra Murphy

Sparta, Inc.

sandy@sparta.com, sandy@tislabs.com

The Sequence of Solutions

- Increasing protection – increasing cost
- Peer-peer connection transport protection (outsider protection)
- Origination Protection (protect against prefix hijacking)
- Origination and AS_PATH Adjacency Protection
- Origination and AS_PATH Route Protection

Peer-peer Connection Transport Protection

- Several methods
  - TCP MD5
  - IPSEC
- Management the biggest problem
  - Installing keys in many, many routers
  - Rekeying at decent intervals – synchronize with peer
  - Removing key if necessary
- Need tools to make this scale!

Origination Protection

- Authorization only (AS is authorized address) or Authorization and Authentication (AS is also currently announcing address)
- Need to decide what “authorized” means wrt announcing aggregates (your own and proxy)
- Need authority (not necessarily central) that:
  - Stores info completely, accurately and securely
  - Accepts changes securely – with model for authorization
  - Can be queried securely
- Need way to communicate with authority at appropriate latency – periodic download, inline, etc.
  - Chicken and egg problem for contact with external authority – how do you route to database that is securing the routing?

Origination and AS_PATH Adjacency Protection

- Like Smith/Garcia-Luna-Aceves and soBGP work
- Protection indicates that adjacent AS's in AS_PATH do peer
- Need way to securely transmit adjacency
  - Transmission inline? (Security is provided by digital signatures)
  - Query a database? (the same as the address database or some other database – and same chicken and egg problem)
- Processing demands
  - Crypto sign and verify
  - Storage of secured info and related security stuff (like keys)
  - Check of AS_PATH against secure info
- Residual vulnerabilities?

Origination and Route Protection

- Like S-BGP (Steve Kent at BBN)
- Protection (digital signatures) indicates that each AS in path passed that route on to its neighbor
- Protection passed inline; related security stuff may be downloaded (with same chicken and egg problem)
- Processing demands
  - Sign and verify inline or as often as needed
  - Storage of secured info and related security stuff (like keys)
  - Redundancy in announcements makes it possible to reduce impact
- Residual vulnerabilities?