SBGP — Secure BGP

smb@research.att.com

http://www.research.att.com/~smb

973-360-8656

AT&T Labs Research

Florham Park, NJ 07932

Threat Model

- Configuration error
- Fraudulent origination
- Fraudulent modification
- Compromised routers
- Routers run by evil companies
- Wiretapping and packet injection?

Basic Model

- Routing origination is digitally signed
- BGP updates are digitally signed
- address-based PKI used to validate signatures; no new trusted parties or trust paths

More Details

- Signing party certifies who the next hop is; this information is propagated throughout the net
- Signatures carried in optional, transitive BGP option
- Predistribute (most) certificates to near each BGP speaker
- Offload certificate verification
- Lazy validation of routes
- Cache signed routes and originations

Costs

- Bandwidth – steady state overhead is 1.4 Kbps (start-up transient is much worse)
- Consumes a lot of CPU — hardware assist probably needed
- Need a lot more memory to store data
- *Setting up the PKI*

Limitations

- PKI is complex, but it's based on existing relationships
  Mistakes take sites off the net
- Doesn't do a good job authenticating withdrawals
- Router upgrades needed

Other Approaches

- TCP MD5 (RFC 2385) protects single hop
- BTP TTL Security Hack also protects a single hop
- SO-BGP guards against origination fraud, but not against mid-path disruptions
- None of theses protects against evil routers on-path

Status

- Running code exists
- See `http://www.ir.bbn.com/projects/s-bgp/` for papers and code