BGP Security

- Compromise Misconfiguration
- Insider attack
- Prefix hijacking
- Invalid update forwarding
- Spoofing
- Traffic stealing
- Eavesdropping
- Denial of service

Border Gateway Protocol
- Connects autonomous systems (ASes)
- Critical infrastructure
- All interdomain traffic depends on it
- Outdated trust model
- Security problems known for 10+ years

Lots of attempts to secure it
- None widely adopted
- Needs new routers, software
- Provides little incremental benefit
- Forces ASes to reveal peering info

XMon-BGP: an External Security Monitor for BGP

Monitor BGP externally: External Security Monitor (XMon)
- New type of network component
- Checks the packets a router sends against packets it has received
- Runs on a trusted platform
- Nexus and a Trusted Platform Module (TPM)
- Everyone can be sure we’re checking BGP correctly
- Agnostic to implementation and configuration
- Any legal BGP implementation is OK

Why not run BGP on trusted hardware directly?
- Requires replacing the router
- Everyone has to agree which implementations are trusted (and bug-free!)

XMon-BGP nodes connect to form a security plane
- Notify each other of invalid messages
- Cooperate to monitor adjacent nodes
- All of B's messages are seen at A or C
- Virtual XMon
- Allows XMon-BGP to secure paths with some unmonitored ASes

Architecture

XMon-BGP is a sniffer or a proxy
- Sniffer: applicable at low link speeds; minimizes disruption
- Proxy: blocks bad traffic directly; applicable at all speeds
- Sniffers and proxies interoperate

How XMon-BGP reacts to invalid messages
- Block the message (proxy XMon only)
- Notify administrators
- Roll back invalid route: remedial IOS script

Safety and Policy Checking

Safety specification
- Based on the RFC: rules everyone agrees on
- Update is valid if it originates a local prefix or forwards a received route
- Forwarded routes must preserve received path, prepend local AS number
- Aggregation is allowed

Policy rules
- Negotiated pair-wise with other ASes, often peers
- Remote AS’s XMon enforces rules you specify
- Route preference, load balancing, privacy
- Written in standard Routing Policy Specification Language (RPSL)

XMon-BGP state
- XMon-BGP stores all routes received and not withdrawn
- Set of valid outputs is based on it
- Must remember all routes to each prefix, not just the best

Results

Is it correct?
- Never generates warnings for legal behavior
- Tests with Linux+Quagga, IOS
- Traces from PLUTO, RouteViews, and NLR

Is it fast enough?
- Checks 335,000 messages/sec
- 10^5 times faster than BGP traffic

How much incremental benefit?
- Securable path available for 80% of routes given 10% random deployment