Operational Requirements for Secured BGP

Steven M. Bellovin, Columbia University
John Ioannidis, Columbia University
Randy Bush, IIJ

Metagoal

- Must support today's uses of BGP
- Must support all legal policies
- *May* require minor changes to how such policies are carried out, but it's better if no changes are required, especially downstream

Objections

- New failure modes
- Cost
  - Capital and operational
- Dirty data
  - Applies to any possible solution
- Some ISPs won't publish policies
- Phased deployment

New Failure Modes

- Yes – there are new ways to lose connectivity
- Secured BGP is designed to reject some routes; mistakes or buggy software can trigger this
- Of course, routing misconfigurations and attacks can cause loss of connectivity, too – remember AS 7007?

Cost

- Capital costs
  - Some initial outlay; Moore's Law will help
- Operational expenses
  - ISPs and RIRs must run CAs
  - Big problem is likely to be customer care
- Who pays? What's the incentive?
- Database cleanup
  - RIRs have already been working on this
  - Good area for government funding

Policies

- Policies are hard to intuit
- Some proposed solutions require knowledge of policies; some ISPs won't publish them
- Only solutions are to find a security solution that doesn't require that, or to persuade the ISPs that they're wrong
  - The latter hasn't worked well in the past

Phased Deployment

- Can't deploy everywhere at once, even within an ISP
- Should give preference to solutions that work well in a phased deployment scenario
- Add tuning knobs for “security radius”?
- *Must* have mechanism for authoritative determination of whether or not an advertisement should have been signed

Security Warning

- We don't have to have perfect security
- **However...** it doesn't make sense to go to great effort to deploy a solution that the attackers can bypass
- Critical routers have been compromised in the past; there's no reason to think that can't happen again