

SBGP / SoBGP:

What do we Really Need and how do we
Architect a Compromise to get it?

Randy Bush <randy@ijj.com>

David Meyer <dmm@sprint.net>

Andrew Partan <asp@partan.com>

Steve Bellovin <smb@research.att.com>

Alvaro Retana <aretana@cisco.com>

NANOG / Salt Lake City 2003.06.03

<<http://psg.com/~randy/030603.nanog-sxbgp.pdf>>

What is the Threat Model?

- Configuration error (7007, 128/8)
- Traffic Diversion
- Distant data-based attack w/ source spoofing
- DDoS to kill a path (smb)
- Monkey in the Middle and Wiretap Attackers
- “Most of these are Unlikely and we can do with an Interim Solution”

EXTREME BEYOND THIS POINT!

Collapse of lava bench occurs without warning, causing violent steam explosions and ocean surge.





Remember NANOG Feb 2000

smb Described DDoS Attacks

As he Was Speaking, the First
Attacks on big sites Occurred

My Idea of a Compromise

- The Big Costs are ISPs' Ops Deployment
- Full Deployment will Take Years
 - PKI : address allocation, peers
 - Hardware Support
- Start now: don't get Caught Out Later
 - Origin Sign Now, Full Path Eventually
 - Registry-based PKI Now for Addresses
 - Peer-based PKI Now for ISPs
 - Hardware Support Start Now
 - One Protocol, no Second Deployment Later