Where the Wild Things Are: BGP Threats

smb@research.att.com

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

973-360-8656

AT&T Labs Research

Florham Park, NJ 07932

BGP Attacks — Are They Real??

- Misconfigurations
- Subverted routers
- Evil originators

Misconfigurations

- Most famous incident: AS 7007
- Others have happened, too — in December 1999, AT&T Worldnet was off the air for long enough that the Wall Street Journal noticed, because someone else was advertising a critical network of ours.
- Many less-noticed attacks

Prefix Hijacking

- Discussed recently on the NANOG mailing list
- People are advertising blocks they have no rights to; others are believing it
- Why? Spamming!
- (Is a law being broken?)

Spammers

- The spammers are employing hackers
- If you're committing one felony, the second is free. . . ?
- They're hacking routers and/or config systems.
- They're hacking routers belonging to major ISPs and exchange points; it's not just *Joe's Bar, Grill, and Packets*.
- Do you filter your peers' advertisements for correctness, as opposed your downstreams'?
- This is happening today.

Connection Rerouting

- Hack two routers, one near each end of a connection
- Use one to advertise a better route to the destination
- Set up a GRE tunnel to a monitoring point
- Set up a GRE tunnel to the other router
- Re-inject the packets
- Do your customers monitor path changes?
- This is happening today.

Conclusions

- More serious enemies can do more damage
- Major hijackings are easier to notice and correct; smaller-scale ones can be more deadly, and are harder to spot
- Today's defenses can't even cope with today's attacks
- To a first approximation, everyone is vulnerable
- What should we do?