# Crashing the Net

Steven M. Bellovin
AT&T Labs Research
smb@research.att.com
http://www.research.att.com/~smb

# Physical Layer

- Backhoes
  - Natural enemy of cables.
  - Most fibers haven't evolved strong defenses, but some are symbiotic with gas pipelines.
- Squirrels
  - Many squirrels find insulation tasty.
  - Some seem to home in on electrical fields.

*Do these attacks scale?*

# Massive Fiber Cut Pauses East West Traffic (*Inter@ctive Week*, 29 September 1999)

"At least four Internet service providers are experiencing severe traffic backlogs because of a massive fiber-optic cable cut that put out four OC-192 lines connecting data networks on the East and West Coasts.

"Industry sources told *Inter@ctive Week* that the cut was accidentally made by an unidentified gas company in Ohio around 12:30 EST today.

"The news is sending shockwaves through the networking community, with many carrier operators struggling to understand why, all of a sudden, their traffic is routed through London and Denmark. At least four Internet service providers are being affected by the outage…"

# Other Risks -- Routing

- Routing tables tell the traffic how to flow.
- Routing tables are generated by routing protocols.
- Each router believes its neighbors.
- If one of them lies, it confuses all of the others...

# *RISKS Digest* 19.12 (1 May 97)

"Internet service providers lost contact with nearly all of the U.S. Internet backbone operators… some for up to 3 hours. The problem was attributed to MAI Network Services ... which provided Sprint and other backbone providers with incorrect routing tables…

"Furthermore, the routing tables Sprint received were designated as optimal, which gave them higher credibility than otherwise. Something like 50,000 routing addresses all pointed to MAI."

# Other Risks -- DNS

- Under the hood, the Internet relies on IP addresses to identify hosts.
- The Domain Name System (DNS) maps host names into IP addresses.
- If the mapping is wrong, bad things happen...

# *RISKS Digest* 19.25 (18 July 97)

"[On] 17 Jul 1997, a remarkable event occurred. The 4AM update of the root nameserver database was botched - horribly. The ... effect of this is that the Internet does not work right. In this episode, the top-level domains .com and .net have ceased to exist...

"The problem apparently began ... during the autogeneration of the NSI top-level domain zone files... Quality-assurance alarms were evidently ignored and the corrupted files were released at 2:30am EDT."

*If it can happen by mistake,*
*it can happen by malice.*

# Hack Puts AOL Off Limits (*CNET News.com* 16 Oct 1998)

"Internet users trying to send email to America Online users or get to the online giant's site have been plagued by problems due to a major glitch with the Internet's domain naming system.

"The problem was caused when someone forged an email message to the InterNIC, run by Network Solutions, requesting that Network Solutions change AOL's designated name server."