Host versus Network Security

Steven M. Bellovin
smb@research.att.com
http://www.research.att.com/~smb
What’s a Network Problem?

• “Hackers Break Into Microsoft’s Network” (Wall Street Journal, 10/27/00)
• “In the Wake of Web-Site Hacking, No Easy Answers, or Solutions” (New York Times, 2/9/00)
Microsoft Break-in

- A *host* problem, not a network problem.
- The network was the vehicle for the attack.
- “Highway robbery” doesn’t mean that someone stole the pavement...
Denial of Service Attacks

• These attacked the network, not Web sites.
• A real network problem.
• Can’t be solved by end-systems, firewalls, etc.
Model of the Internet

- Smart hosts, dumb network.
- Network’s concern is packet transport.
- Host’s concern is packet processing.
Network Security Issues

• Availability
  – Protocol infrastructure (i.e., DNS)
  – Routing
  – Link-flooding

• Theft of Service
  – Primarily for switched services and shared media
Availability

• “How many backhoes are needed?”
• “How many **backbones** are needed?”
Host Security Issues

• Break-ins
• Data confidentiality
• Transmission confidentiality
• Remote user authentication
• Buggy software
Who Does What?

• ISPs
  – Provide sufficient redundancy to protect links
  – Harden infrastructure protocols
  – Protect their own resources

• End users
  – Encryption
  – Suitable authentication
  – Firewalls
Why ISPs Can’t Protect Users

• They don’t know what users want to do
• Your “odd behavior” is my new, cutting-edge application
• Your “allowed service” is my vulnerability

• But what of ordinary consumers?