Security for the NGI

Steven M. Bellovin
smb@research.att.com
AT&T Labs – Research

The Challenge

- Most of the security problems in today's Internet come from its power, not from design flaws.
- Any replacement will have to face the same challenges.
- That said, there are changes that can help.

Security Issues

- Cryptography.
- Correct code.
- New security model.
- Firewalls.
- Mobile code.

Cryptography

- Must be universally available.
  - "Exportable" ciphers are not strong enough.
- Must be strong enough to resist determined, well-funded attackers.
  - DES will not suffice.
- Must be secure in the face of buggy host software.
- *In general, escrow schemes fail on all three counts.*

Key Escrow?

- Many different needs/desires: intelligence, law enforcement, corporate key recovery, personal file recovery, personal privacy.
- Can we reconcile these needs?
- Do we know how to build – *and run* – such systems?
- Do they scale? Are they secure?

Correct Code

- About half of the security problems we see are due to buggy code.
- Cryptographic code is affected by these bugs, too.
- *As a profession, we do not know how to solve the problem. 40+ years of research hasn't helped much, either.*
- But we cannot give up and stop trying.

New Security Model

- The “Orange Book” doesn’t work for the new environment.
- Systems run the gamut from multi-company Web servers to individual PCs.
- Need very fine-grained security for things like credit card numbers.
- How do users and/or administrators *manage* such a security model?

Firewalls

- Firewalls – as an element of an overall security architecture – won't go away.
  - But centralized corporate-size firewalls are dinosaurs.
- Protocols must be firewall-friendly.
- Bad examples: X11, UDP, RPC, FTP.
- Many of these problems are unnecessary.

Mobile Code

- What do we do about it (Java, Javascript, ActiveX, MSWord, PostScript, etc.)?
- Users *want* glitzy features (or so the perception goes).
- How do we wall off untrusted code, while permitting semi-trusted code to have enough power?
- The Net is *not* the same as the local disk (or is it?).

Currently Missing Pieces

- Routing security
  - I expect such attacks soon...
- Object security
  - Some individual objects secured; no overall architecture.
- Multicast
- Availability