NSF Network Trustworthiness Panel

Joe Touch
PCEN Director
Computer Networks Division
USC/ISI

3 Questions

- 1. Why isn't security working?

- 2. How are our models doing?

- 3. What is the impact of P2P?

E-Business works $$$

- Modular components
  - SSL works under HTTP, IMAP

- Automatic
  - Default 'on'
  - Fixed CA sets enable bootstrapping

- Visible
  - Follow the bouncing lock…

Firewalls work

- Location, location, location

- Single point of management

- Less heterogeneity

- Bang for the buck

- *But we need to secure other things...*

Complexity kills

- Monolithic
  - IPsec – encapsulation, keying, firewalling, tunneling, routing... **vs. SSL**

- Hard to install
  - Kerberos, VPNs **vs. SSL**

- Hard to manage
  - DNSSEC **vs. firewalls**

Metrics for good models

- Simple / general / modular
- Semantically valid
- Applicable

...

- *Active / adaptive?*
  - *Flexible, but from their generality*
- *Diverse?*
  - *Works if transparent & automatic*

Integral model parts

- Design costs
  - Default to capability *first*

- Install costs
  - Cost of install < cost to repair

- Ongoing management
  - Cost to maintain = 0 (or nearly)
  - Automate away!

Peer-to-eternity, or back?

- Internet = common services
- P2P = stovepipe recapitulation
  - Need application-layer functions
  - Results in non-modular systems

- Need:
  - Extended network layer services
  - Automation and defaults

Key Observations

- **Abstraction, not optimization**
  - Simplicity drives utility
  - Capability *is* performance
  - Completeness can kill
  - Optimize later… maybe

- **Automation, not customization**
  - Generic defaults
  - Self-determined overrides
  - No permanent decisions
  - *Design for deployment*