Why Do We Need More Research?

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

What are the Real Problems?

- Lack of appropriate cryptography.
- Buggy software.
- Routing attacks.
- Environmental issues.

We don’t have good solutions for any of these.

Cryptography

- Need more speed, especially for public key algorithms.
- Scaling
  - Can we use cryptography ubiquitously?
  - If we do, how do we manage our networks?
- PKI
  - Scale
  - Revocation
  - Confusion

PKI Confusion

- Almost no one checks certificates.
  - Most people don't know what they are, or when to trust them.
- Lots of expired certificates out there.
  - Some heavily-used software doesn't check things properly.
- Will people notice the difference between whitehouse.gov and whitehouse.com?
  - Don't try the latter from your office, folks...

Can We Afford Cryptography?

- Cryptography breaks compression.
- Cryptography breaks assorted network management tools.
- Cryptography breaks cross-layer techniques that may be needed for quality of service.
- Cryptography breaks NAT boxes.

What are the alternatives for all of these?

Buggy Software

- 85% of all CERT advisories describe problems that cannot be solved with cryptography.
- 9 of 13 advisories last year were for buffer overflows.
  - 2 of the remainder described problems in crypto modules.
- If your software is buggy, how can it be secure? We don't know how to write correct code!

Routing Attacks

- Routers believe their neighbors.
- If its neighbors lie, a router can be deceived about the proper route, thus allowing eavesdropping, hijacking, denial of service, etc.
- Such “attacks” have already happened accidentally. Doing it deliberately isn’t very hard.
- Proposed solutions don’t seem to scale.

Environmental Problems

- Running a large network is hard.
  - "The amount of clue is constant, but the Internet is growing."
- Operational errors often translate into security problems.
- We build our systems out of unreliable, untrustworthy COTS components -- but we want systems to be reliable and trustworthy.

Challenges

- Learn how to use cryptography.
- Learn how to write correct code.
- Secure the routing infrastructure.
- Make systems that are powerful yet simple to use.

"If we knew the answer, it wouldn't be research."