Security, Cryptography, and Magic

Steven M. Bellovin
smb@research.att.com
http://www.research.att.com/~smb

Weak Points of the Internet

- The DNS
- Routing
- Host security

Cryptography can help with the first two, but...

Security Flaws

- At least 85% of CERT advisories describe problems that cryptography can't fix.
- 9 out of 13 advisories last year are about buffer overflows.
  - Of the othes, 2 describe problems in cryptographic modules…

Going Around the Cryptography

- Cryptography relies on the secrecy of keys. Can we protect them, on today's systems?
- Smart cards, etc., encrypt, decrypt, and sign what the host system hands them. Can we trust the host?
- What about the certificate hierarchy?

Certificates

- Most users don't know what certificates are.
- Of those who do, most don't verify the signature chain.
- Most of those people don't know if they should trust an arbitrary root.
- Conclusion: for most practical purposes, we don't have a PKI -- and most people neither know nor care.

Cryptography and Identity

- Given the PKI problems, encrypted traffic is effectively unauthenticated.
- This does prevent broad-spectrum eavesdropping.
- But active attacks can go around the cryptography to penetrate systems -- and such attacks are taking place.

Conclusions

- Cryptography is necessary, but not sufficient.
- Using cryptography *properly* is very hard.
- We can wave our magic wands and solve that problem, and deploy strong cryptography everywhere.
- But we don't have a big enough wand to fix the buggy code.