Securing the Net: Where the Holes Are

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

The New Bad Guys

- The spammers now pay the hackers
  - Hacked PCs are being used to spread spam
  - Many recent worms (i.e.. SoBig.F) carry spam engines
  - A profit motive for hacking!
- Major corporations and universities have done it.
- Politicians are hacking
- Organized crime?
  - Online extortion is happening today

"It is a well-known fact that no other section of the population avail themselves more readily and speedily of the latest triumphs of science than the criminal class."

Inspector John Bonfield, Chicago police

1888

Spyware

- Growing problem
- Spread by various means:
  - Voluntarily downloaded, because of deceptive license agreements
  - Embedded in desired software
  - Exploit various security holes
  - Sometimes spread by worms (see above...)

Network Attacks

- Distributed denial of service (DDoS)
- Eavesdropping on WiFi traffic at hotspots
- Attacks to come:
  - Fake hotspots
  - Fraud against hotspot providers
  - Are these happening already?

Phishing

- Rapidly-growing form of identity and credential theft
- Simple technical solutions won't work; there's a human dimension to the problem:
  - paypal.com versus paypa1.com
  - login.paypal.com versus login-paypal.com
- Sites can supply cryptographic credentials; users have to verify them *properly*

Firewalls

- Firewalls are less useful – lots more connectivity today
- Who uses a company-supplied laptop?
- How many of those laptops will connect to the company network after the conference?
- The August 2001 IETF meeting was during the Code Red worm outbreak. We spotted a dozen infect machines on the conference LAN.

Why Do We Have Such Problems?

- It's (mostly) not the protocols
  - We can encrypt most protocols with little effort
  - Sometimes, crypto is pointless – cryptography can't stop spam
- Some of it is due to the Internet's fundamental architecture
  - But giving that up would mean giving up many of the benefits of the Internet, such as decentralization
- But what is the cause?

Buggy Code and Complex Software

- Most security problems are due to buggy code
  - This is the oldest unsolved problem in computer science
  - We can make things better; can we make them good?
- Many of the rest are due to user misconfigurations or user misunderstanding
  - Can we make computers simple to administer? That may be difficult – the basic concepts can be hard.

What Can We Do?

- Firewalls and intrusion detection systems are not network security devices; they're the network's response to bad software.
- Design our systems to isolate vulnerable components.
- Design our systems to be robust in case of partial penetration.
- Educate users.