Internet Security: Then and Now

Steven M. Bellovin
smb@research.att.com
http://www.research.att.com/~smb
Early Communications Technology
Network Connectivity

• With no networks, security was simpler:
  – Corrupt insiders
  – Physical attack
  – Some connectivity goes way back, but there was too little to present an attractive target

• Networks carry good things and bad: hosts are exposed

• Must protect the network, too
  – Do highway robbers steal the asphalt?
What is Security?

- The classics: confidentiality, integrity, availability

Today
- Control *any* access to hosts
  - Hosts themselves inadequately secured
- Privacy
- Web servers
- Prevent abuse of network bandwidth
- Out-of-band attacks
Threats

- Password sniffing
  - Started in 1993, on major backbones
  - Wireless makes it worse – but ARP-spoofing is bad, too
- Protocol weaknesses
  - Example: TCP sequence number guessing
  - More complex protocols today (NetBIOS, SIP, H.323)
- DDoS
- Worms and viruses
- Buggy code
Privacy

• Sites know a *lot* about people
• How do they protect this information?
• Or don't they?
• Note: correlations yield a *lot* of information
• Example: orkut.com's privacy policy explicitly gives them the right to share personally identifying data with Google.
Web Servers

- Very hard to protect
- The most dangerous service – port 80 – can't be blocked off
- The hardest problem is buggy code – and web servers have lots of it
Buggy Code

- Oldest unsolved problem in computer science
- Will probably remain unsolved
- National Research Council study: 85% of CERT advisories through 1998 described problems not fixable by crypto
- Most were due to buggy code or configuration errors
Defenses
Defenses

- Protocol analysis
- Crypto
  - Point-to-point and VPNs
- Black holes
- Firewalls
Protocol Analysis

- Hard to do
- Point-to-point is easier – bolt-on crypto
- Multiparty is hard
  - BGP – must trust remote data
  - Think VoIP and SIP – must trust many parties
- *Authorization* is the hardest part
  - Again, much harder for multiparty
Crypto

- Naivete 10 years ago – some people thought crypto was the solution
  - Crypto is a solution to some problems
- Crypto is hard – not the protocols (though those are hard enough), but managing them
  - Who is authorized to talk to you
- Three successful uses: SSL, IPsec VPNs, ssh
- A failure: secure email
SSL

• To some extent, a fig leaf: “it's safe to shop here, because your traffic is encrypted”

• 99.999% of consumers don't check certificates
  – 99.999% don't know what a certificate is
  – 99.999% don't know their root CAs, or why they're trustable

• Vulnerable to active attack by sophisticated adversary

• But – it does stop credit card sniffing. (Bad guys hack servers instead.)
IPsec VPNs

- Moderate-scale deployment
- Multi-vendor harder than it should be – much harder
- Simple authorization model: central site hands out credentials
- Mixed bag – not nearly as common or as effective as we'd hoped 10 years ago
Secure Email?

- By most standards, secure email is a failure
- Virtually unused, except by ubergeeks
- Why:
  - Hard to use – needlessly hard?
  - Where do keys come from?
  - Many models require central deployment – the Internet is bad at centralization
  - People don't perceive a threat
ssh

- Decentralized deployment
- No authority needed
  - No key server needed
- Tunnels other protocols
  - Easier to deploy than IPsec; no kernel mods needed
- Deals with a perceived threat model
Black Holes and DDoS

- Few good defenses out there
- Most common “defense”: null-route the victim, to avoid collateral damage
- Most attacks have been self-limiting – this far
- We don't have good defenses in the network
  - This is the attack where the network itself is at risk
Firewalls

● Our best defense against buggy code
● Not a network security device
  - Firewalls are the network response to the host security problem
  - Damning indictment of the state of the art of software engineering
● But firewalls are failing
Big Firewalls are Obsolescent

- Too much connectivity, around and through the firewall
  - We run too useful a network...
- Mobile hosts
  - Remember the worm problem at the last NANOG?
- Split-use hosts
  - Home machines used for telecommuting
- How did Code Red and Slammer, get inside corporate nets?
Now What?

- The threat isn't going away
- We don't have major new defenses on the horizon
- We have to leverage the Internet's strengths
Future Directions

• We can usually secure special-purpose hosts, in ones and twos

• Manageability is the key: must find a way to \textit{scale} good system management

• Saying “no” is easy – how do we say “yes”? 
  – Crypto where it helps – preferably, decentralized crypto 
  – Limit range of peers, enforced by crypto 
  – Sandboxes on hosts 
  – Special-purpose appliances – use an Internet Phone, rather than a PC
Things that Won't Work

- ISP-enforced security
  - Hurts innovation
  - Doesn't scale well – large ACLs; customer complaints
- Mandatory, automatic patches
  - Breaks too much software
- Central management of decentralized concepts
  - But central management is needed to solve centralized authorization issues
- Wishing the problem will go away
If We Fail...