Where the Wild Things Are

Steven M. Bellovin

smb@research.att.com

908-582-5886

AT&T Labs Research

Murray Hill, NJ 07974

Current Trends

- More sophisticated attacks.
- Hacking for profit.
- Denial of service attacks.
- “Better” Web scripts.
- Targeted marketing — i.e., data gathering — on the Web.
- Firewalls loosing potency.

Sophisticated Attacks

- Password sniffing — required good knowledge of TCP to implement.
- Sequence number guessing.
- Connection hijacking.
- Better operational security by the hackers — encrypted files, multi-hop attacks, log file modifications.

Hacking For Profit

- A vendor reports prices changed on Web pages.
- One ISP was hacked by a competitor.
- There are reports that one break-in was a fake — it was a publicity stunt.
- At least two reported instances of packet storms aimed at customers using ISPs that imposed usage-sensitive pricing.

Denial of Service Attacks

- These attacks don't break in, but they deny you access to your own resources. These are the moral equivalent of teenagers who slash car tires for “fun”.
- Several recent incidents reported; more are expected.
- Sometimes can be used as an adjunct to a break-in. For example, an attacker can disrupt communications between a primary and a secondary authentication server, and replay cryptographic credentials.
- Defense against such attacks is *very* difficult.

The Panix Incident

- Attack code published in at least two different hacker publications.
- The attack exploited a fundamental feature of TCP's connection establishment sequence.
- The attackers were quite sophisticated, and did not just use canned programs.
- No one knows why Panix was targeted.

Sophisticated Web Scripts

- Scripts do more and more.
- Complexity implies insecurity.
- Increasing numbers of Web pages require helper applications, plug-ins, applets, etc.

Targeted Marketing Data

- Web browsers leak information.
- Increasing use of “cookies” can be used to track individual behavior.
- Third-party cookies provide broader overview of who reads what pages.
- What does that imply for the military community?

Are Firewalls Still Useful?

- More and more people need (or want) connectivity.
- Small ISPs and dial-up PPP make connectivity easy.
- Organizations are more and more decentralized.
- People want holes punched through the firewalls.

☞ The easiest way past a firewall is to go around it.

- New model: use multiple small firewalls, near the resources that need protecting.

New Defenses

- Smaller firewalls can be placed where needed.
- IP-layer encryption becoming readily available.
- Attacks are generally preceeded by scouting; good log files are becoming more important (but they're also growin larger and larger).
- We need an “Internet flight recorder” for post-mortems.