Realistic Security

Realistic Security

`smb@research.att.com`

`http://www.research.att.com/~smb`

973-360-8656

AT&T Labs Research

Florham Park, NJ 07932

What is “Realistic Security”?

- Acknowledge that components will fail.
- Acknowledge that people won’t always co-operate.
- Design for overall acceptable security despite these problems.

Commercial Security

- Assumption: The Internet is a bad neighborhood.
- Solution: Use a firewall.
- Problem: People have to get their work done.

A Typical Firewall

The Internet is a Bad Neighborhood

- Most companies had Code Red on the inside of their firewalls.
- Viruses still spread.
- The (deployed) firewalls aren’t stopping this stuff.

Military Security

- Assumption: The Internet is a bad neighborhood.
- Assumption: Firewalls aren't secure enough.
- Solution: Ban connectivity.

A Secure Firewall

But People Have to Get Their Work Done

What's Really Going On?

- The security policy doesn't match the threat.
- The security policy doesn't match the job requirements.
- The security policy doesn't match the organizational culture.
- *The security policy doesn't match reality.*

What is the Threat?

- Bad software on the inside.
- Hackers—of all sorts—on the outside.
- Insider attacks

Responding to Threats

- Different threats demand different countermeasures.
- Simple firewalls may keep out script kiddies.
- Background checks and more are needed to keep out industrial spies.

Bad Code

- *Most security problems are due to buggy code.*
- The primary purpose of a firewall is to keep the bad guys away from the bugs.
- Can we live without it?
- This talk doesn't use Powerpoint, but...
- We have to have the programs, but we shouldn't.

Defense in Depth

- Get the best code that will do the job. (But make sure you understand what the job really is.)
- Be scrupulous in applying patches.
- Screen inputs to suspect code (i.e., mail server virus filters).
- Monitor outputs (IDS).
- This is a per-application firewall.

Organizational Culture

- A university is not a corporation; a corporation is not the CIA.
- People often select their jobs for the organizational culture.
- “You can’t solve social problems with software.” (Marcus Ranum)

Example: Telecommuting 1

- A Silicon Valley company tried to ban modems.

⇒ Employees attached modems to their office phones.

- The company installed a digital phone system.

⇒ Employees ordered “fax lines”.

- A disgruntled ex-employee started war-dialing the exchange.
- The right solution: a *properly-managed* modem pool.

Example: Telecommuting 1a

- Some companies charge for cost recovery on modem pools.
- It appears cheaper to run your own.
- Result: unauthorized modem pools, which aren't as secure.
- (The same applies to access via the Internet.)

Example: Telecommuting 2

- Employees use personally-owned machines to telecommute.
- Bean-counter level bars use of (firewall-protected) Internet connection for personal use.
- Result: employees switch between unprotected personal surfing and secure intranet access.
- Result: attacks enter the corporation via the employee's machine.

Example: Firewalls

- Firewalls can have flaws.
- Firewall policies can have flaws.
- Defense: multiple levels of firewalls; avoid common-mode failures.
- Protect each department with custom firewall.

Example: 802.11B Wireless

- WIreless LANs are very insecure.
- People want them anyway—and base stations are cheap and transparent.
- Have an official wireless LAN *outside* the firewall, and use a VPN to let users in.

Example: Production Server Complex

- Must be secure.
- Must be available.
- Requirements often bar remote maintenance access.
- What happens when something breaks at 1am Sunday on a holiday weekend?
- Plan for emergencies; supply *secure* remote access.

Example: Extranets

- Companies need extranets.
- Must make it easy for business units to create secure links.
- If not—unofficial, poorly-secured links will be created.

Example: Passwords

- People *will* pick bad passwords, or write them down, or share them, etc.
- Password quality checking doesn't work well—people evade it.
- Solution: use token-based authentication.

Example: Social Engineering

- Social engineers—con artists—are very good.
- The only defenses are constant education and constant drills.
- SAC's posture: "A peacetime air force on a wartime footing."

Conclusions

- The way people “should” act is at variance with the way they do.
- Ignoring this results in insecurity.
- Make it easy for people to do the right thing.