Trends in Information Security

Patrick Heim

Ernst & Young LLP

Threat of External Attacks Increasing

- Computer Security Institute's annual "Computer Crime and Security" survey:
  - "The old rule that we would see 80% of the penetration coming from the inside, 20% from the outside, is outmoded," says Richard Power, editorial director for the institute. "This isn't to say the threat from the inside has diminished -- it hasn't. It is just showing that the threat from outside is now co-equal to it."

Threat of External Attacks Increasing

- Proliferation of "Hacker Tools"
- Opportunistic Attacks based on Broad Sweeps - “BO” and NetBus Scans
- Skill required by hackers to perform an attack is decreasing - “script kiddies”

Increase in Trojan-Horse Applications

- Current Threats - Back Orifice and "buttplugs", NetBus, RAT
- Effective against large installed base of MS Operating systems.
- Seeking faux status as "administration tools" - e.g. NetBus Pro

Increase in Trojan-Horse Applications

- Defenses:
  - Content Filters & Intrusion Detection Systems
  - Policies against executing "foreign" code (e.g. electronic greeting cards)
  - Blocking of outbound connections on non-standard ports.
  - Trojan-horse security scanners.
  - Updated anti-virus software.

Unix / Linux and the Hacker Community

- The emergence of Linux as the hacker platform of choice.
- Platform of choice for the development of sophisticated hacker tools:
  - Nmap - Sophisticated stealth portscanning
  - Nessus - Freeware security scanner that is being perpetually enhanced.
  - Hunt - Session monitoring and hijacking.
  - Cheops - Automated / graphical network mapping program.
  - Strobe - High speed portscanner

Unix / Linux and the Hacker Community

- Less constrained by OS limitations than MS operating systems. - “Kernel Hackers”
- "Trinux - A Linux Security Toolkit" pre-packages sophisticated hacker and security tools in a format usable by novices.
- Defenses: None. Stay current with the underground (in)security community.

Growing Dislike of Microsoft

- "Windows Refund Day" - antagonism against the MS profit model and rebellion against "Wintel Monopoly".
- "Closed Source" vs. "Open Source" philosophies.
  - Hackers are driven by social acceptance and status in the hacker community. They target Microsoft products because of their proliferation and ease of attack.

New Feature Overload

- New features are continuously bundled in with operating systems – many are network and Internet related.
- Features are added at a rapid expanding rate making security analysis and manufacturer QA difficult.
- Each new feature expands the number of items that must be controlled and can introduce new security holes.

New Feature Overload

- Defenses:
  - Limit the ability of users to download and install programs.
  - Enable a policy of "no non-firm standard software" without prior approval of IS.
  - Do not grant superuser / administrative access to users even for their own workstations.
  - Discourage "updates" unless they address specific problems.

Buffer Overflow Based Attacks

- Buffer Overflow Definition:
  - The ability to execute code by overflowing assigned application buffer spaces and injecting arbitrary code which executes in the security context of the exploited application. (smashing the stack)
- Result of poor programming practices.
  - Lack of bounds checking
  - Executable stack
- Primarily on Unix platforms – ease of generating a remote shell.

Buffer Overflow Based Attacks

- Increasing at a rapid rate as people discover their efficacy and learn to program buffer overflows.
  - 49 Buffer Overflow Posting on Rootshell
- Example:
  - NFS Statd Solaris Remote Root Buffer Overflow
- Defenses:
  - Code reviews (slint)
  - Non-executable stacks - may break some applications.

Buffer Overflow Based Attacks

- Defenses:
  - Disable all unused services
  - Monitor security postings for new vulnerabilities and apply patches to all systems where a significant threat may exist.
  - Filter at the firewall.

Highly Skilled International Hackers

- Lack of state-of-the-art equipment is compensated with cleverness and a great deal of time.
- More malicious / profit driven than domestic hackers.
  - SHANGHAI, Feb 23 (Reuters) - China cracked some 100 cases of computer hacking last year ranging from mischief to serious crime, the International Finance News said on Tuesday.

Highly Skilled International Hackers

- When there are no technological defenses, brute force is used.
  - China sentenced to death two brothers who broke into a bank's computer network and stole 260,000 yuan ($31,400). They were prosecuted for theft.
- Internet connectivity
  - Provides access channel to domestic companies. Prior to the Internet, International hacking was dependent on point-to-point international telecommunications which were expensive and unattainable by most.

Trends in Security Software & Hardware

- Modular and Cheaper Workgroup Firewalls (e.g. SonicWall)
- Intrusion Detection continues to grow in sophistication and acceptance.
- Active Security - Automated responses to attacks.
- Centralized Management / Distributed Agents.

Trends in Security Software & Hardware

- More Content Filtering
- Convergence of Host based and Network Based IDS
- Growth in industry acceptance of PKI
- Continued growth in token / Smartcard based access solutions.