Stanford Linear Accelerator Center

SLUO
SLAC USERS ORGANIZATION

Computer Security

Review and Plans

SLAC Users Organization

Wednesday, 15 July 1998

Bob Cowles, SLAC Computer Security

Stanford Linear Accelerator Center

Security Activity

- Minor incidents occurring 4-5 times/month
  - Anonymous FTP servers used for "warez"
  - User accounts used to run IRC "bots"
- Often password "sniffed" at another site
- Cleanup requires 4-16 hours per incident
- Stolen account concerns

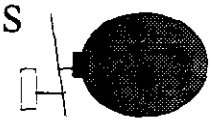
Stanford Linear Accelerator Center

Incident on 2 June 1998

- Entry from another site via rlogin (.rhosts)
- More than 25 machines compromised
  - Accounts (uid 0) created in /etc/passwd
- More than 50 user accounts used
- .rhosts to access computers
  - Potential sites - 30 edu, 6 gov, 11 others
- Internet disconnect and user revalidation

Stanford Linear Accelerator Center

Security Exposures

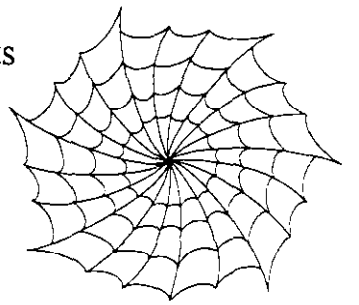


- Network based attacks
  - Applies to both OS and servers (daemons)
    - Security patches not applied or old releases
    - Poorly configured
  - Default accounts and passwords
  - Inappropriate file system permissions
    - SUID/SGID
    - AFS vs. Unix

Stanford Linear Accelerator Center

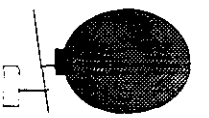
Security Exposures (cont)

- User account compromise
  - Sniffed password
  - Cracked password
  - r* commands using .rhosts
- Web of trusted hosts
  - NIS
  - .rhosts



Stanford Linear Accelerator Center

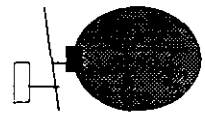
Previous Restrictions



- Web servers on port 80 and SMTP mail delivery restricted to selected hosts
- X sessions from outside the DMZ cannot open windows on SLAC networked machines without using mxcons or ssh
- Finger, NFS, TFTP, Bootp, xdmcp, DNS zone transfer and NIS blocked at the DMZ

Stanford Linear Accelerator Center

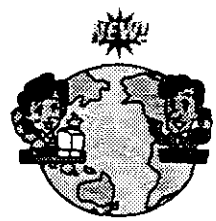
Restrictions
(additional)



- TCP/UDP ports <1024 blocked by default
  - affects rsh outgoing
- NT Networking blocked at DMZ
- NTP, FTP, POP & IMAP incoming restricted to select machines
- juno & unixhub blocked for user access
  - affects NFS file restore and archive

Stanford Linear Accelerator Center

Password Handling



- Passwords can be handled through telephone call to phone number of record (need to keep info current)
- PI's at remote sites are considered as computing czars for handling accounts at their location
- More aggressive "encouragement" for selection of good passwords

Stanford Linear Accelerator Center

Other Changes

- Retire old machines/systems
- More checks on centrally maintained systems
  - Look for compromises and "signatures"
- Strongly discourage unencrypted passwords
  - Greatly reduce ftp servers
  - encourage use of AFS and ssh
  - Implementing SSL on webservers very soon

Stanford Linear Accelerator Center

Future

- Decrease exposure to cracked passwords
  - Enforce selection of stronger passwords with periodic change required
  - Simplify password changing process
  - Hide encrypted form of password
  - Centralize password database using Kerberos

Stanford Linear Accelerator Center

Future (cont)

- Decrease exposure to sniffed passwords
  - Strongly encourage ssh
    - telnet, rsh, rcp, rlogin replacement
    - can tunnel other protocols: X, ftp, email
    - pursue site-license for Windows
    - promise to reconnect ssh services sooner
  - Explore Virtual Private Networking

Stanford Linear Accelerator Center

Future (cont 2)

- Stronger push for central WinNT admin
  - NT requires professional administration
- Secure business systems & accel. controls
  - requires some infrastructure duplication
  - build security zones w/ different policies
- Aggressive application of security patches
  - may result in more reboots

Stanford Linear Accelerator Center

Future (cont 3)

- Increased logging of incoming and outgoing network connections and traffic
- Increased monitoring of files for signatures associated with "suspicious software"
- Restrictions placed on non-SCS managed machines connected to SLAC network

Stanford Linear Accelerator Center

Under Investigation

- International issues
  - US - export regulations
  - France, Russia - usage regulations
- Windows Terminal Server [Hydra]
  - Provides Windows shell environment
  - Runs multiple users at one time
  - Requires careful configuration

Stanford Linear Accelerator Center

Under Investigation (cont)

- Direct-dial access using ppp — Millsom@SLAC
  - 2-4 months to full deployment
  - need testers now to "bleed" for the rest of you
- Virtual private networks (VPN) — Cottrell@SLAC
  - 6 months to full deployment, pilot earlier
- Support for Linux
- Email and hard disk encryption tools

Stanford Linear Accelerator Center

Linux

- Do not select full install
  - Do **NOT** install **BIND** (named), **Samba**, email daemons (imapd, popd, sendmail), or other daemons (ftpd, statd, httpd, etc.) unless needed
  - To mount NFS space, the system must be scanned and problems fixed
- Limit local password file
- Keep system current (i. e. Red Hat 5.1) plus patches for mailx, etc.

Stanford Linear Accelerator Center

Win9x

- Follow the Windows 95 guidelines on the web page
  - Notify departmental support person
    - Disable Master Browser capability
    - Remove NetBEUI and Netware (IPX)
    - In most cases, remove File & Print Sharing
  - Non-compliance will upset many people!
- Win98 not yet fully tested

Stanford Linear Accelerator Center

Challenges

- Balance costs
  - Keeping intruders out
  - Detecting intruders who have entered
  - Cleaning up after intruders

- Maintain
  - Secure, reliable infrastructure
  - Open, collaborative research environment
- Be sure the Physics gets done!

Stanford Linear Accelerator Center

Stanford Linear Accelerator Center