Basic Security for HP-UX System Administrators

Bill Hassell

Director of IT

Systems and Methods, Inc.

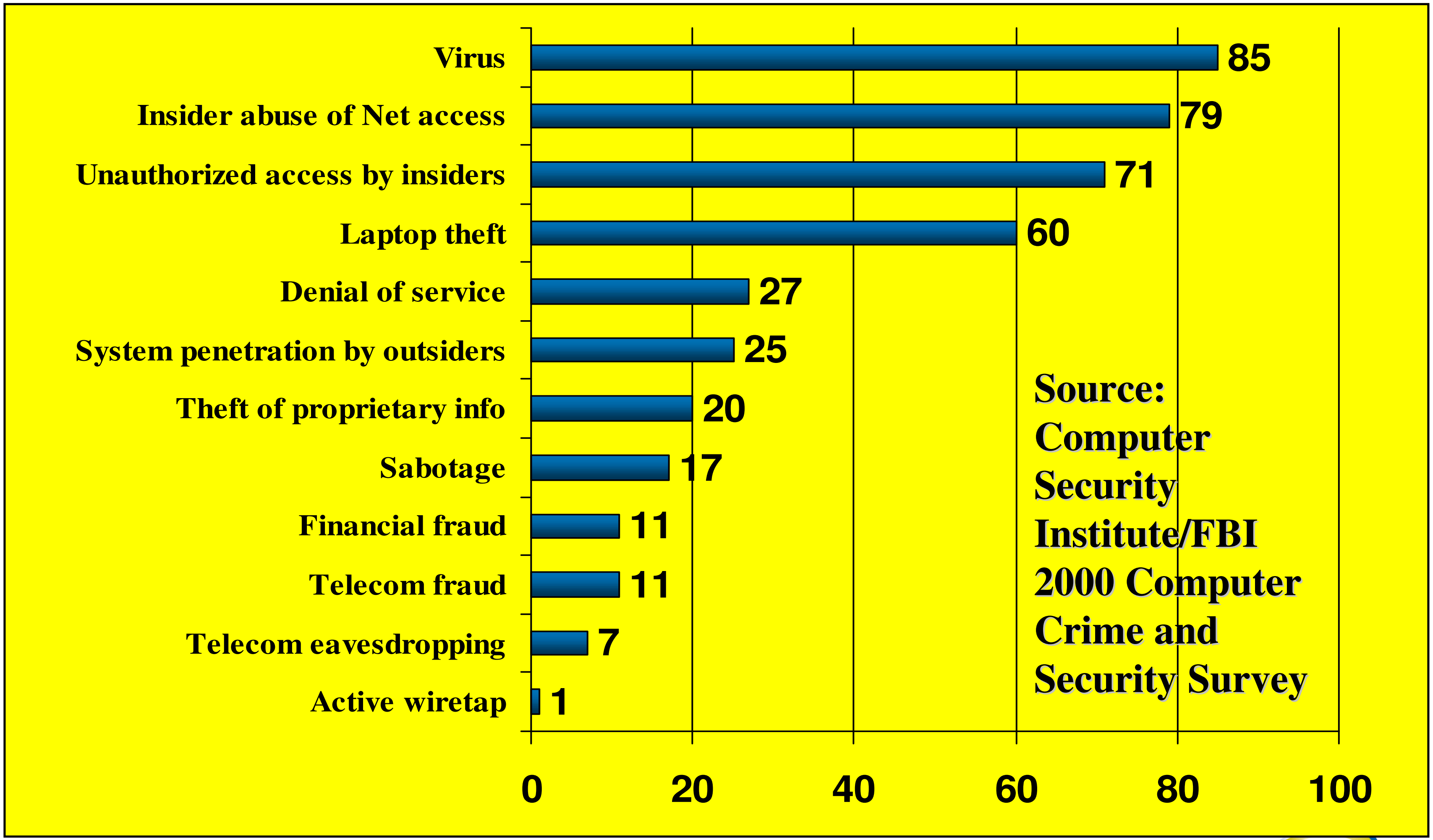
Major Security Areas

- Physical
- System Setup
- Logins
- Modems
- Patches
- IntraNetworks
- The Internet

Why is it important?

- UNIX was designed for an open environment.
- U.S. Computer Security Act of 1987. (Liability: The Computer Security Act states that if financial loss occurs due to computer fraud or abuse, the company, and not the perpetrator, is liable for damages.)
- Hacking (or Cracking) tools are easily and widely available. (Tools include password guessing tools, sniffers, consecutive number dialers looking for modems, and address impersonation programs.)

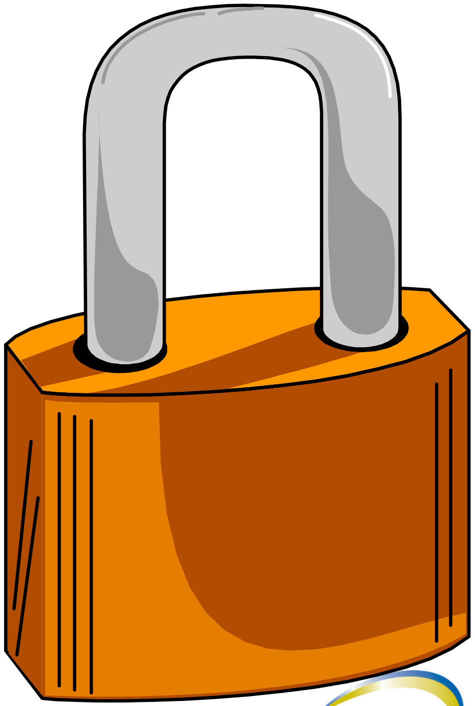
Types of Attacks



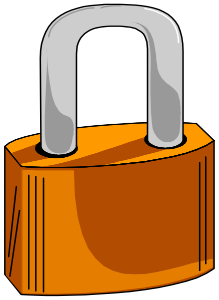
Source: Computer Security Institute/FBI 2000 Computer Crime and Security Survey

Physical

- Locked doors to consoles
- Full walls thru ceiling and raised floors
- Hardware password
- /etc/securetty
- Logout Rules
  - Screen Lockout Rules
  - AutoLogout
    - **`ksh/posix: TMOUT (secs)`**
    - **`csh: autologout (mins)`**



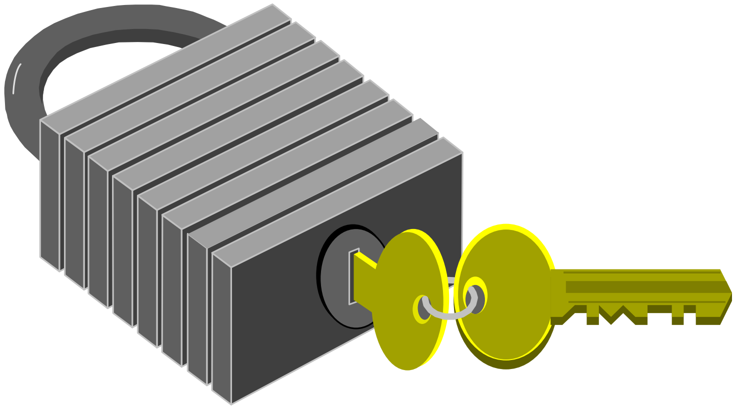
Physical



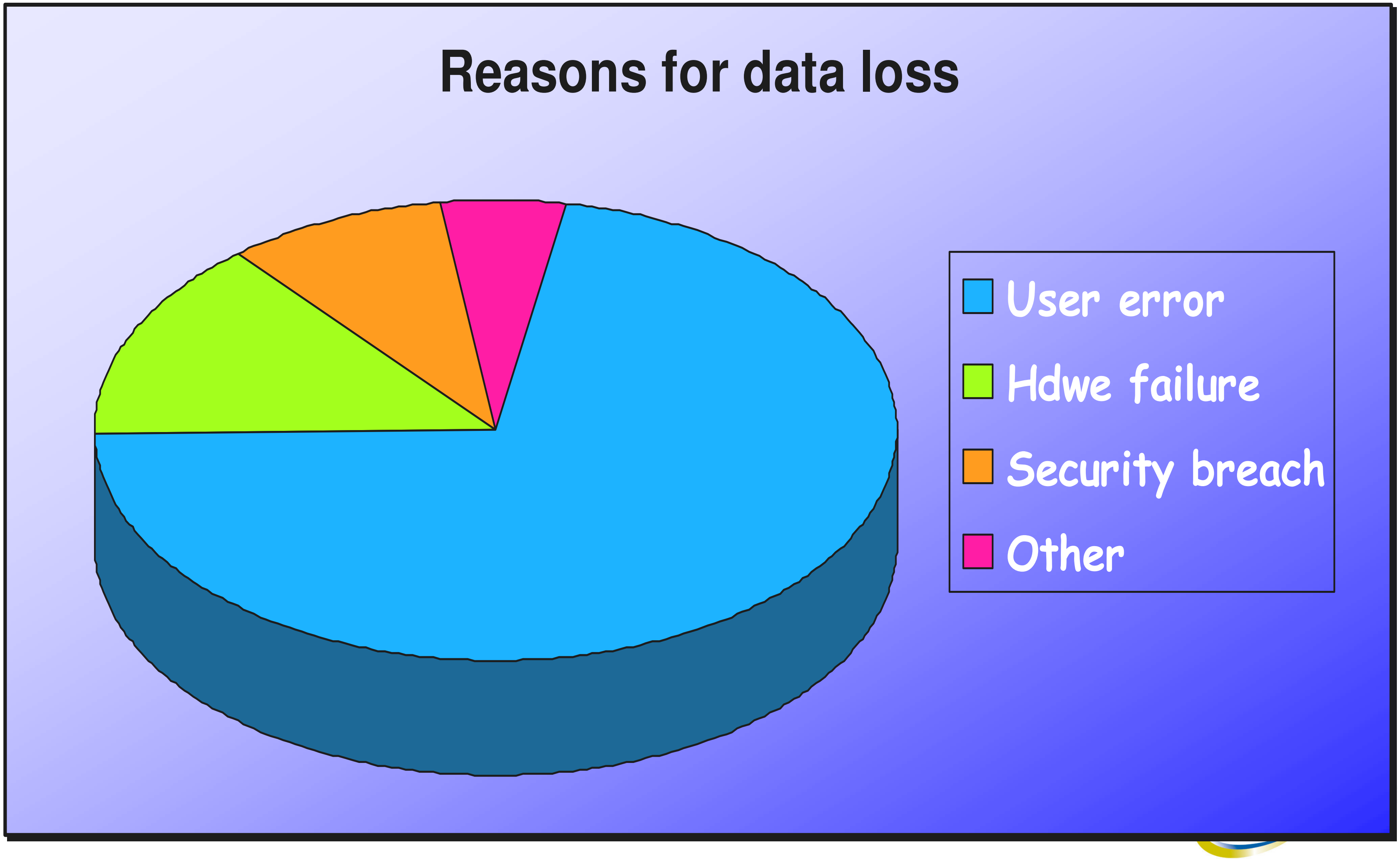
- Destroy printer output containing sensitive information. (Use a confidential bin, then shredder)
- Secure network cables and hubs/routers from exposure. Disable unused ports on switches.
- Disallow personal computer connections, especially by contractors.
- Don’t keep computer keys in the computer.

Backup Media

- Backup Media Lockup
  - tapes = data compromise
  - offsite storage
- Removable Media
  - External boot drives
  - Optical discs
  - USB drives
- Network Backups
  - Automated scripts (validate receiver!)
- Test!
  - Verify contents at least quarterly
  - Rehearse your disaster recovery plan

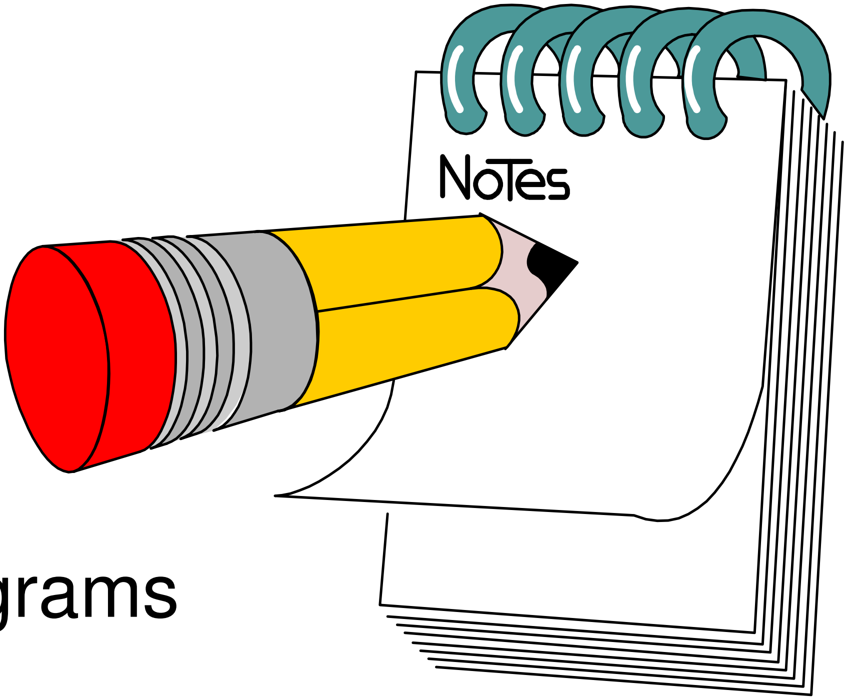


Restoring Data



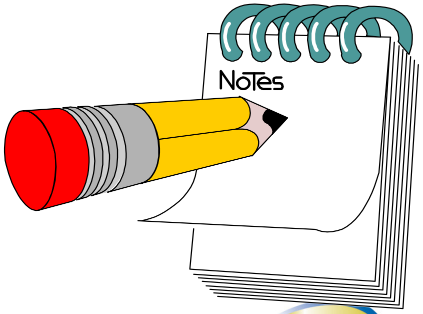
Logins

- Passwords and crack
  - (legal/political issues!)
- Aging
- Stale Accounts
- Shared Accounts
- Restricted Shells/Programs
- Monitoring Access
  - wtmp, btmp, sulog, shutdownlog
- userinfo script



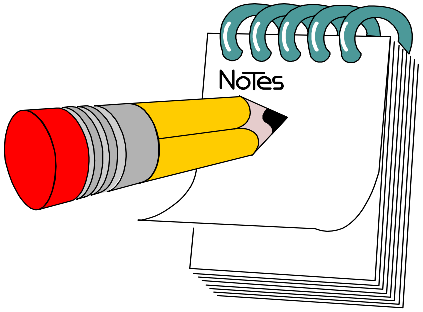
HP-UX Fixups

- No umask in /etc/profile or /etc/csh.login
- Bad permissions in /usr/local
  - find /usr/local –type d –exec chmod 755 {} \;
- Find all world-writable in HP-UX:
  - find /stand /sbin /dev /usr /opt –perm –002
  - Filters:
    - */man/cat.*
    - hfs and vxfs only (not cdfs, nfs …)



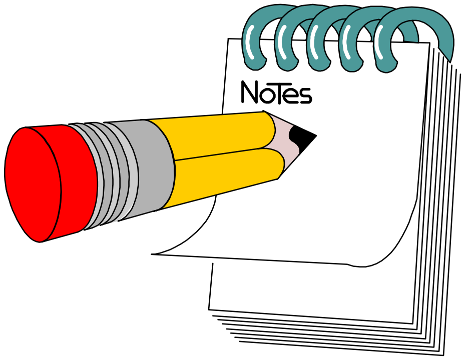
HP-UX Fixups

- Check /etc/PATH and root's $PATH
  - Duplicate paths
  - Non-existant paths
  - Paths that are not directories
  - Paths that are symlinks
  - :: or :.: or : at end of $PATH
  - Group or world-writable directories

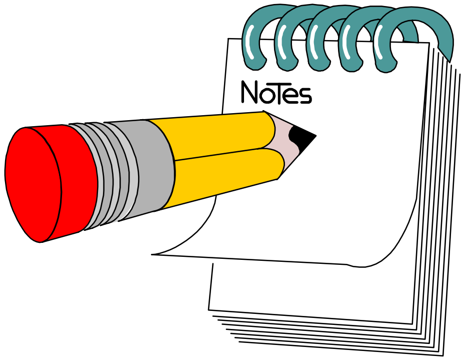


HP-UX Fixups

- Check /etc/passwd and /etc/group
  - pwck
  - grpck
- Check for $HOME/.rhosts
  - Root’s $HOME
  - User accounts
  - Permissions not = 600
- Create /etc/security
  - man security (11.11 or docs.hp.com)



HP-UX Fixups



- Install Secure Shell
  - software.hp.com
  - Select: security and manageability
  - search for Shell
  - Provides encrypted communication for terminal, ftp and tunnels (X/windows)
    - no cleartext logins or passwords (ie, telnet, rcp, rlogin)
    - authentication by Public/Private key
    - rapidly becoming the standard
    - ssh scp sftp
    - disable telnet, ‘r’ commands and ftp
  - New features (A.03.71.000)
    - UsePAM
    - chroot for ssh and sftp

Automated fixups

- Bastille (11.0 and 11.11)
  - Requires X/windows and Perl 5
  - Analyze and recommend
  - Option to make all selected changes
  - Based on Bastille for Linux
  - software.hp.com
    - select: **security and manageability**
    - search for **Bastille**
- Building a Bastion host
  - Kevin Steves (ex-HP)
  - secinf.net/unix_security/ Building_a_Bastion_Host_Using_HPUX_11.html

Automated fixups

- scan-security-def script
  - Trusted/shadow/un-Trusted
  - global security settings
  - decodes the security file
  - excerpts:

```
yoda: trusted system settings, HP-UX 11.11

     YES = User picks own password
     YES = New password requires rule checking
      NO = Null password allowed
     YES = System generates pronounceable password
      NO = System generates passwords having characters only
      NO = System generates passwords having alpha chars only
      NO = Boot authorization for some users is allowed
       7 = Minimum days between password changes
     150 = Maximum days for a password to stay valid
     120 = Expiration in days for a new (unused) password
      10 = Warning in days before password expires
       4 = Maximum login retries (network user)
      10 = Maximum login retries (serial port user)
     200 = Days since last login before account disabled
       2 = Serial line delay (secs) before retry
      20 = Serial line time (secs) to type userID or password
      15 = Maximum password length
```

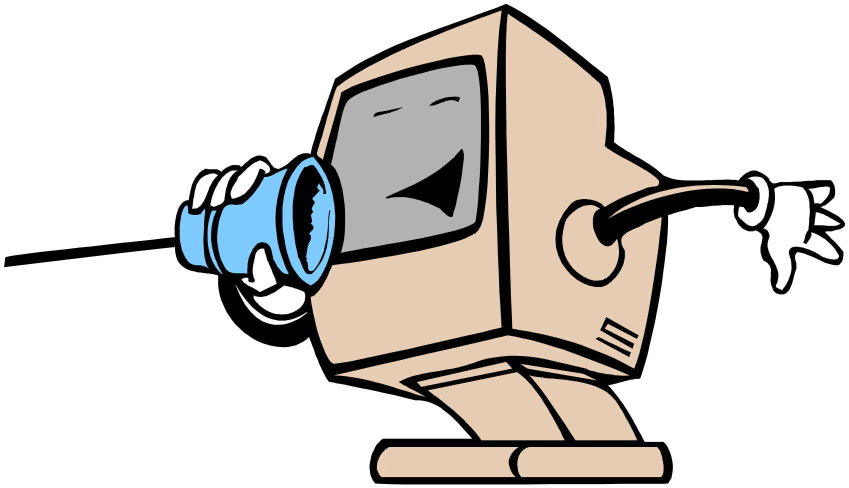
Automated fixups

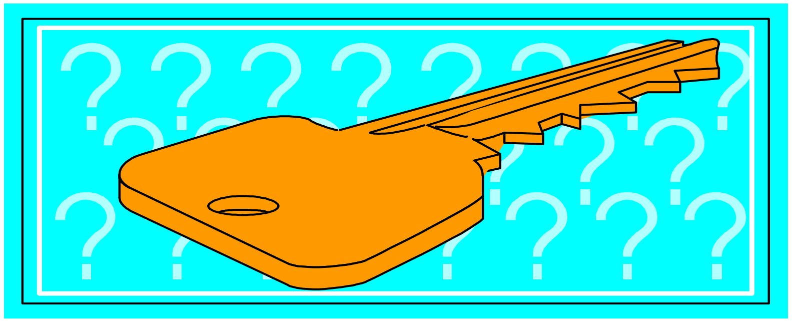
- scan-security-def script
  - continued excerpts:

```
 /etc/default/security:
       *** Access controls ***

       0 = Abort login if no $HOME directory found
       1 = /etc/nologin prevents user logins
       0 = Max logins per user
   def=0 = login required for single user mode *
    root = users that can boot singleuser mode at console *
           * does not apply to Trusted Systems

       *** Password controls ***
       6 = Minimum password length
       1 = Old password history depth
  def=-1 = default password expiration in days *
   def=0 = default minimum days before change allowed *
   def=0 = default days to warn about password change *
       1 = Minimum lowercase chars required
       0 = Minimum uppercase chars required
       1 = Minimum numeric chars required
       0 = Minimum special chars required
           * does not apply to Trusted Systems

       *** su session controls ***
  suroot = group that allows su to root
     022 = default umask for all logins
/usr/bin:/usr/contrib/bin: = PATH used when "-" not used in su
none = ENV variables saved with su
```

Modems

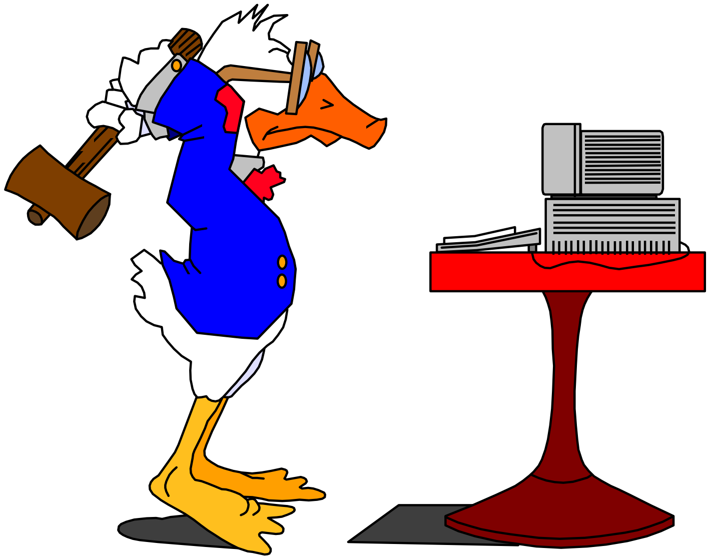
- Dial-in
- Dial-Back
- Modem Servers
- Remote Support Link





B1 and C2 Security

- C2 Trusted systems
  - passwd file hiding
  - login rules/privileges
  - shadow password (11i)
- B1 security
  - no real root user
  - security for *every* device
  - major sysadmin effort



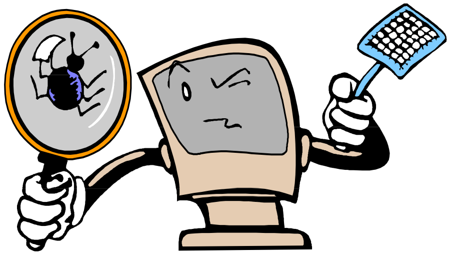
Monitoring

- Systems
  - Logfiles
    - `syslog.log`
      - `syslog-summary` script
    - `wtmp`
    - `btmp`
    - `sulog`
    - `shutdownlog`
  - COPS
  - cron, email alerts

- Networks
  - SATAN
  - Router rules
  - Denial of service
    - Ping of Death, NTP
- Surveillance
  - Legal/political issues

Patches

- Patch notification by email subscription!
  - www.hp.com/united-states/subscribe/gateway
  - itrc.hp.com
    Follow first link: "maintenance and support" then "notifications" (at bottom of page) and select "support information digests"

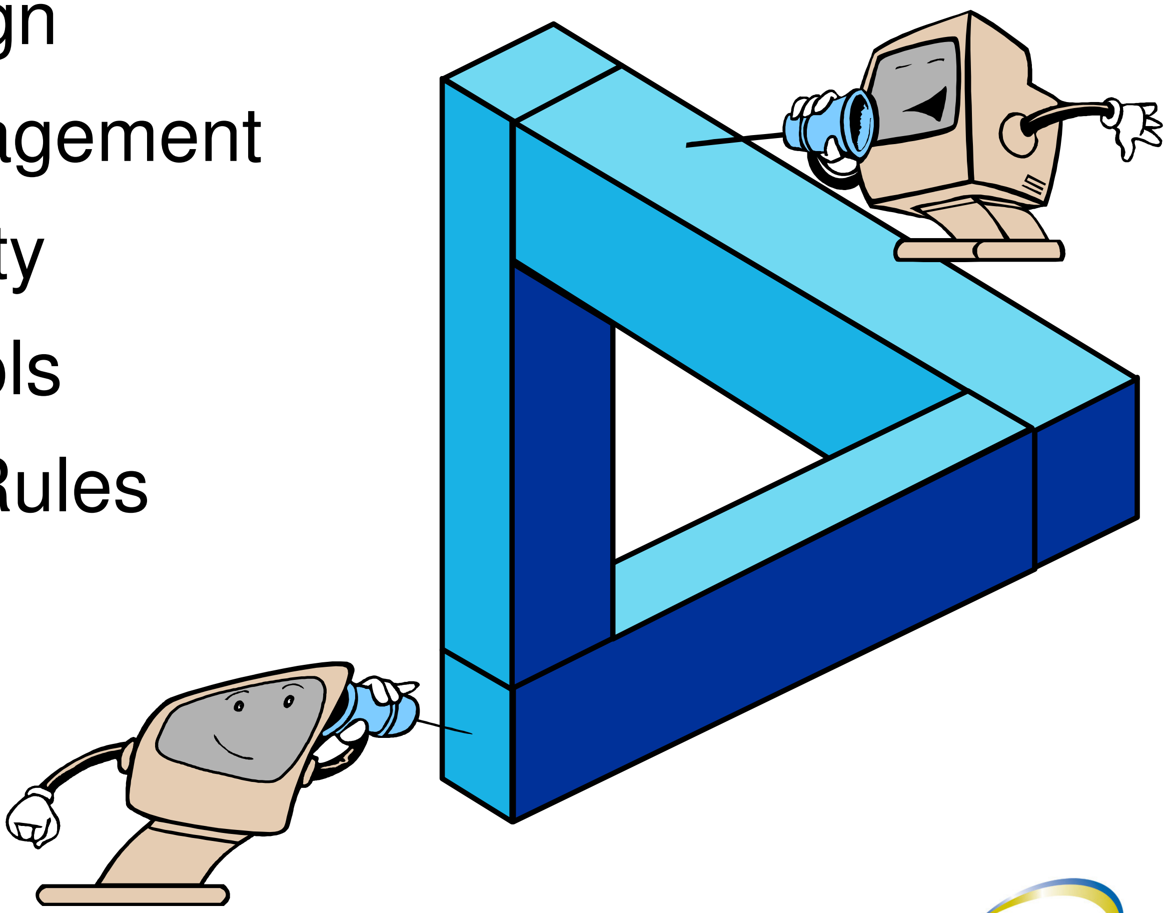


- Security Patch management:
  - us-ffs.external.hp.com/export/patches/
    - see the hp-ux_patch_matrix file
  - security_patch_checker
    - Perl 5 needed
    - must download the data file prior to run
    - software.hp.com -> security and manageability
      - search for the Security Patch Checker

HP WORLD 2004
Solutions and Technology Conference & Expo

IntraNetworks

- Network Design
- Network Management
- Router Security
- Mixed Protocols
- Connectivity Rules



Security Policies

- Have one in place
- Formal training required for everyone
- Part of new hire process
- Different policy for contractors
- Standardized tools and settings (macros)

The Internet

- Firewalls
  - email (viruses, esp. macros)
  - telnet/ftp
  - SSH2 (ssh scp sftp)
  - X/windows (ssh tunnels)

- Open Subnet
  - shutdown everything
  - add absolute minimum services, ideally secure
- Suspect Node
  - ftp://contrib:9unsupp8@hprc.external.hp.com

Conclusions

- Always dynamic
- Watch legal issues
- Secure access = no access
- Read/summarize the logs (automated)
- Security through obscurity - NOT
- You don’t know what you don’t know

HP WORLD 2004

Solutions and Technology Conference & Expo

Co-produced by:

interex

shared knowledge • shared power

encompass

AN HP USER GROUP