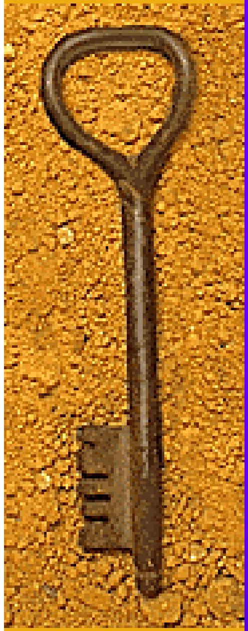
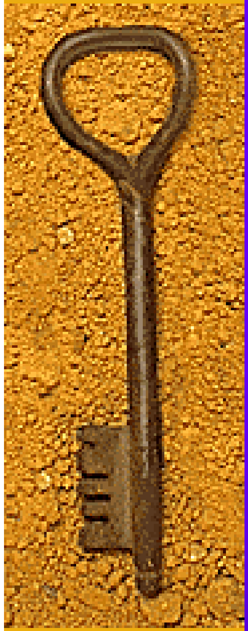
How to Make Your HP-UX System More Secure

Jeff Rupert, CISSP
Hewlett-Packard Company
331 East Evelyn Avenue
Mountain View, CA 94041
Phone: 650-694-2127
Fax: 650-694-2540
Email: jeff_rupert@hp.com



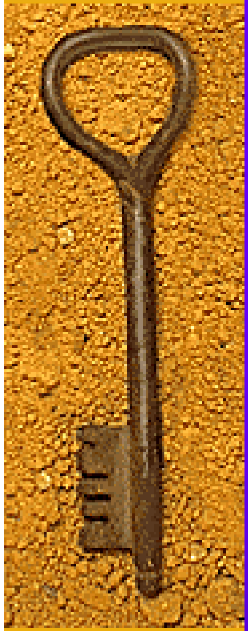
Today’s Agenda

- Physical Security
- Account Security
- File System Security
- Security Bulletins/Patches
- Modem Security
- Tightening Network Services
- Monitoring Logfiles
- Trusted Systems
- Security Tools
- Security Training



Why is Security Important?

- UNIX was designed for an open environment
- U.S. Computer Security Act of 1987 (Liability)
- Hacking (or Cracking) tools are easily and widely available
- Cost and frequency of security breaches is increasing

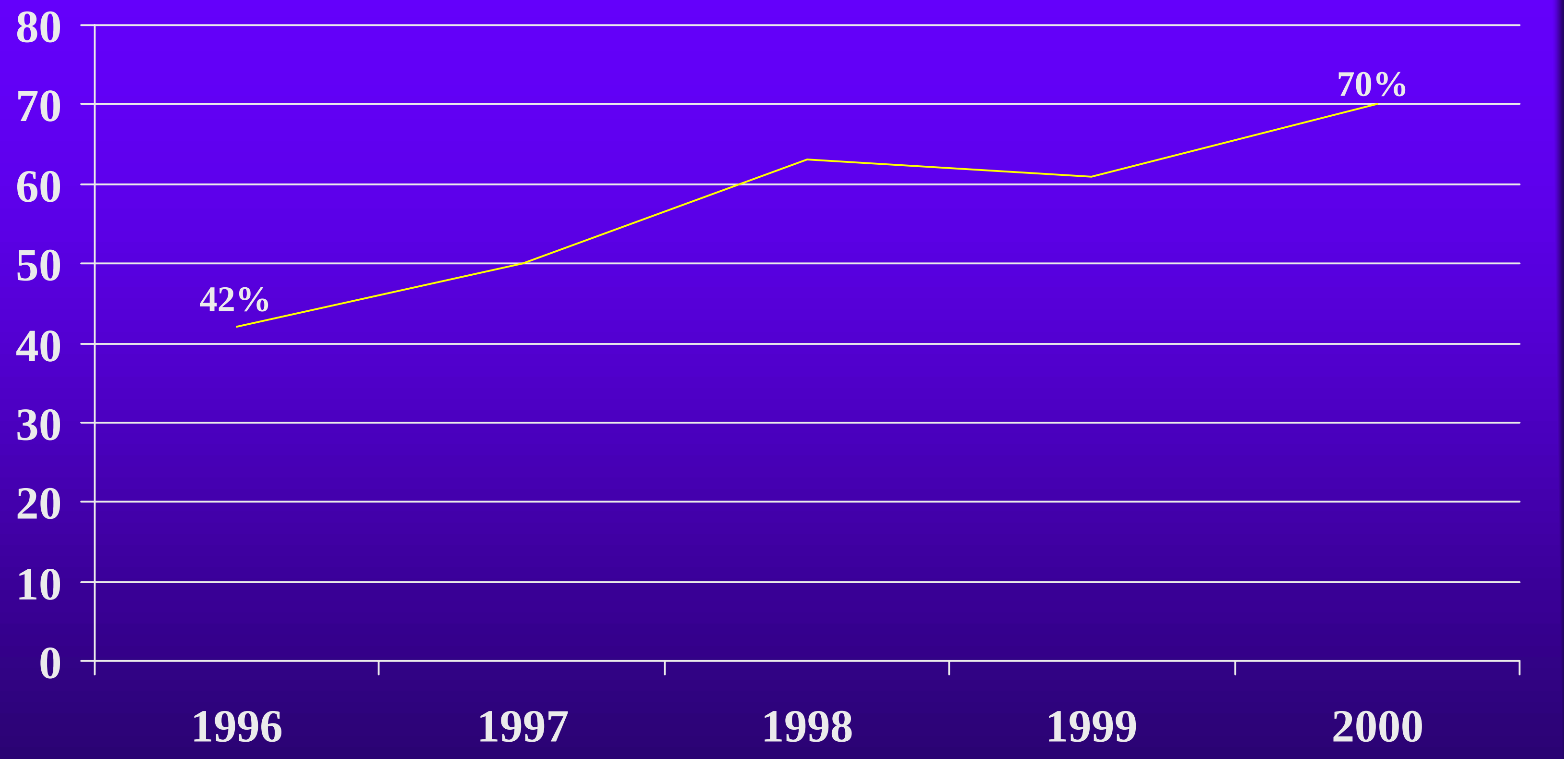


CSI/FBI 2000 Computer Crime and Security Survey

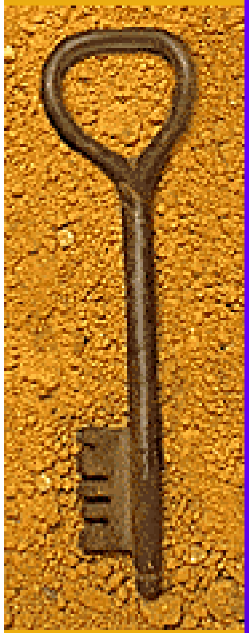
- Computer Security Institute and FBI Survey
- 4,284 anonymous surveys distributed
- 643 responses received
- Not all questions were answered
- Full report can be ordered at:

http://www.gocsi.com

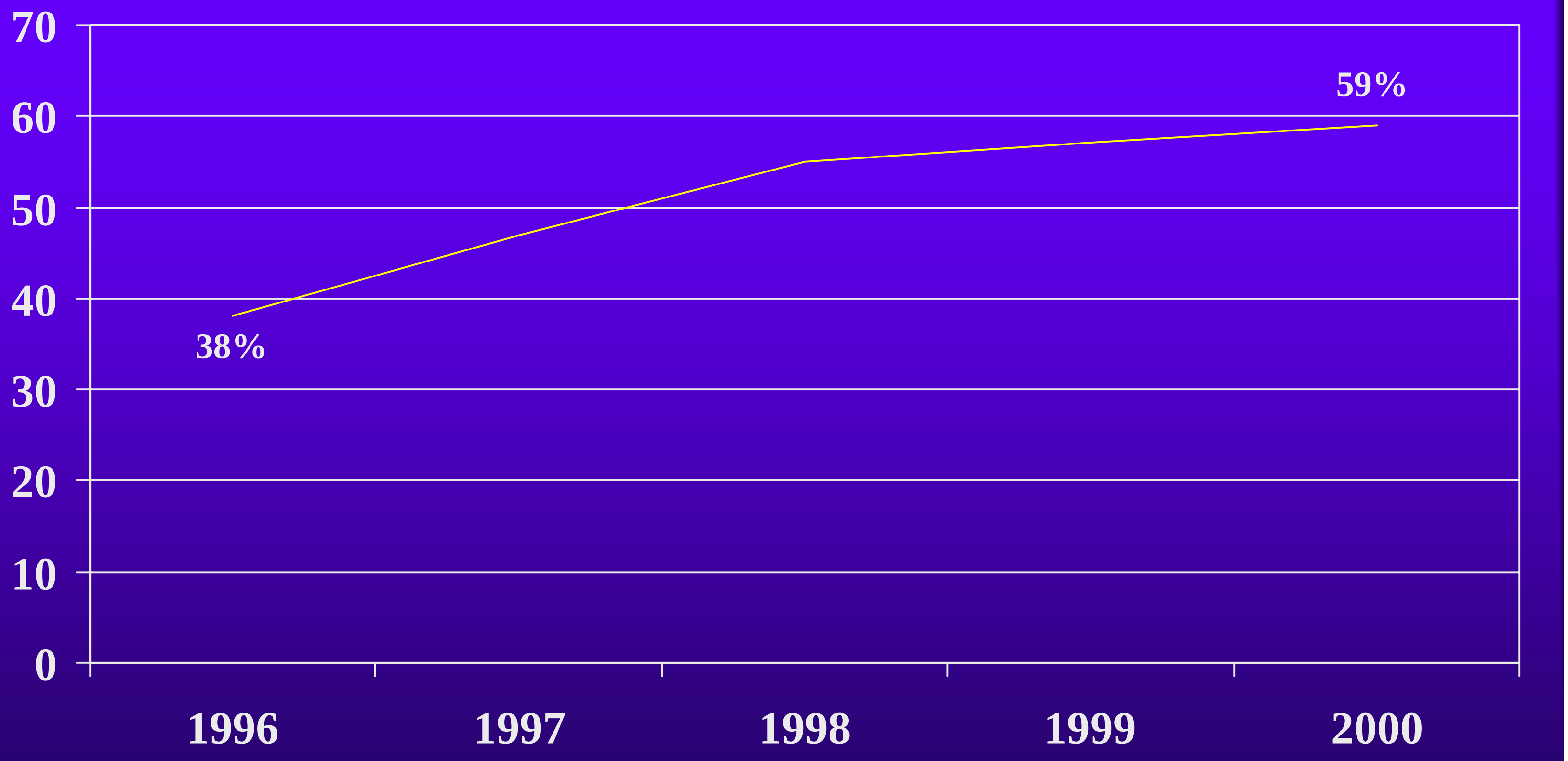
Percentage who reported an unauthorized use of their computer systems within the past 12 months



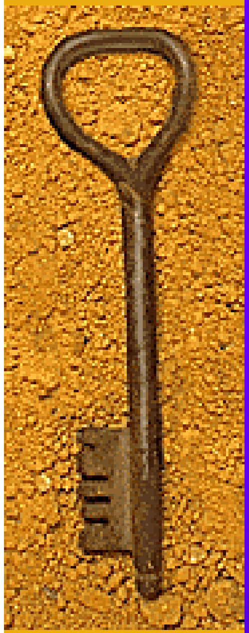
Source: Computer Security Institute/FBI 2000 Computer Crime and Security Survey



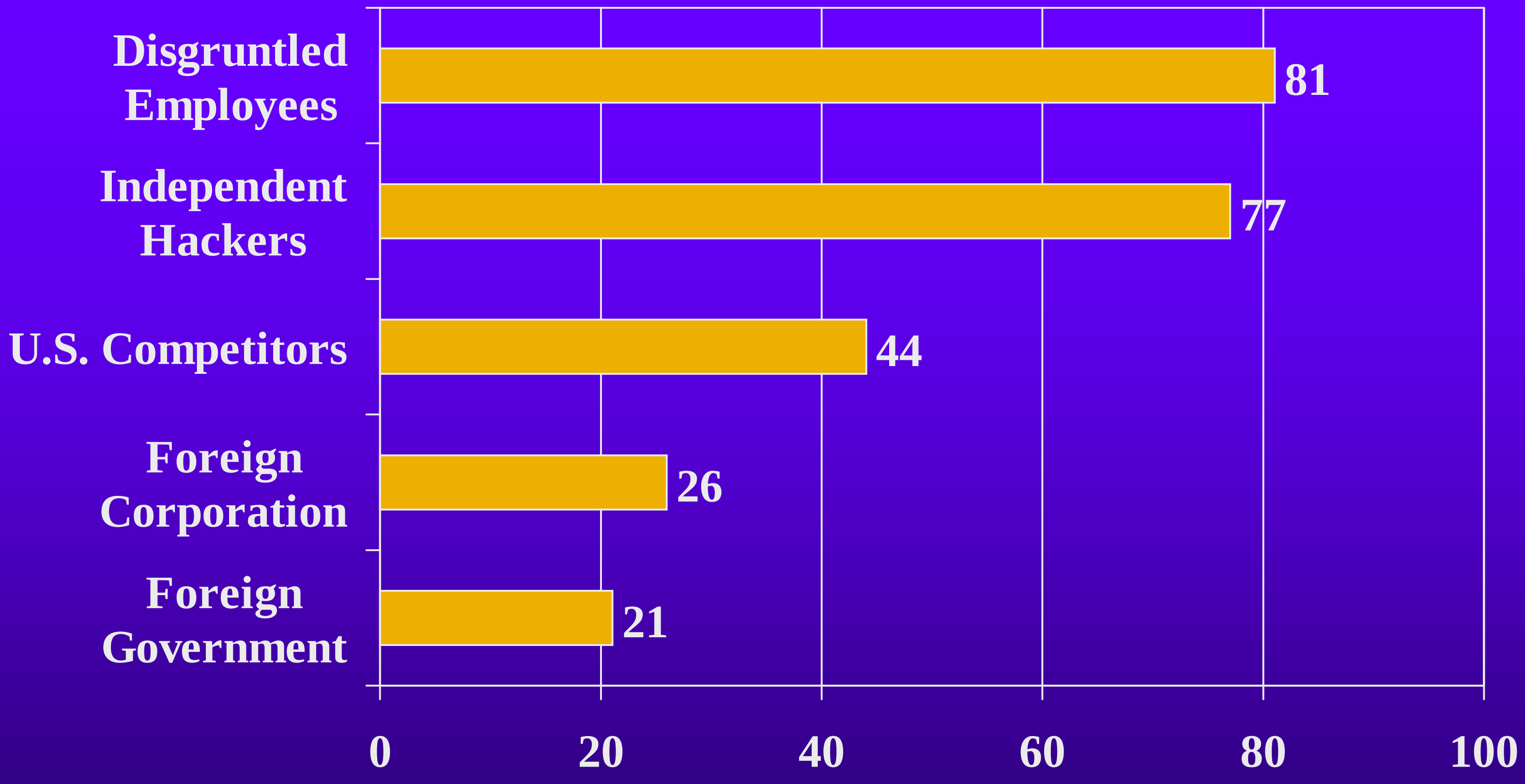
Percentage citing an Internet connection as a frequent point of attack



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

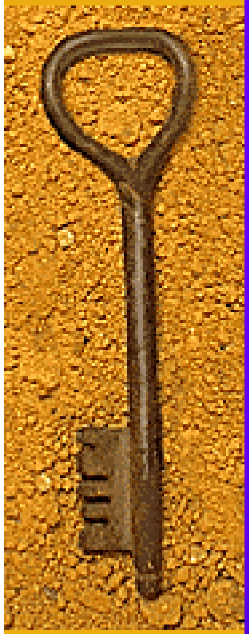


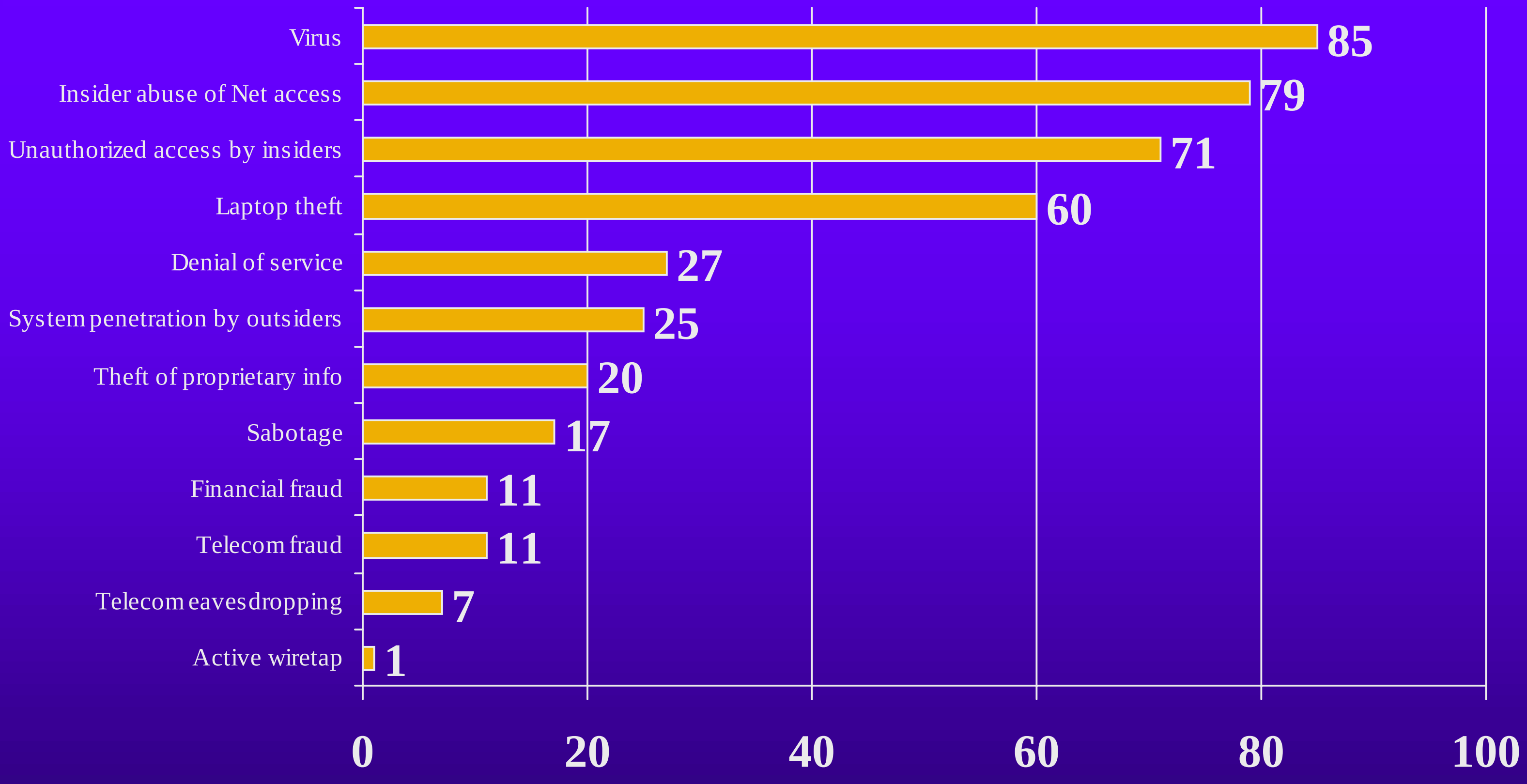
Percentage Citing These as Likely Sources of Attack



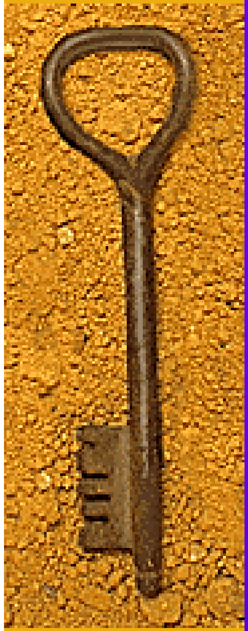
Source: Computer Security Institute/FBI
2000 Computer Crime and Security Survey

Types of Attack or Misuse Detected in Past 12 Months





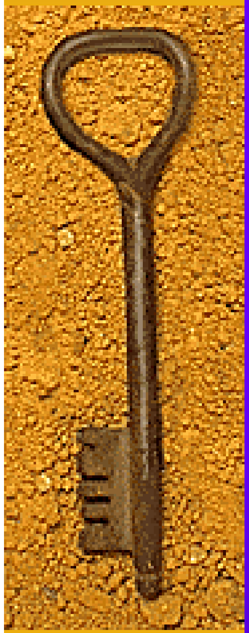
Source: Computer Security Institute/FBI
2000 Computer Crime and Security Survey



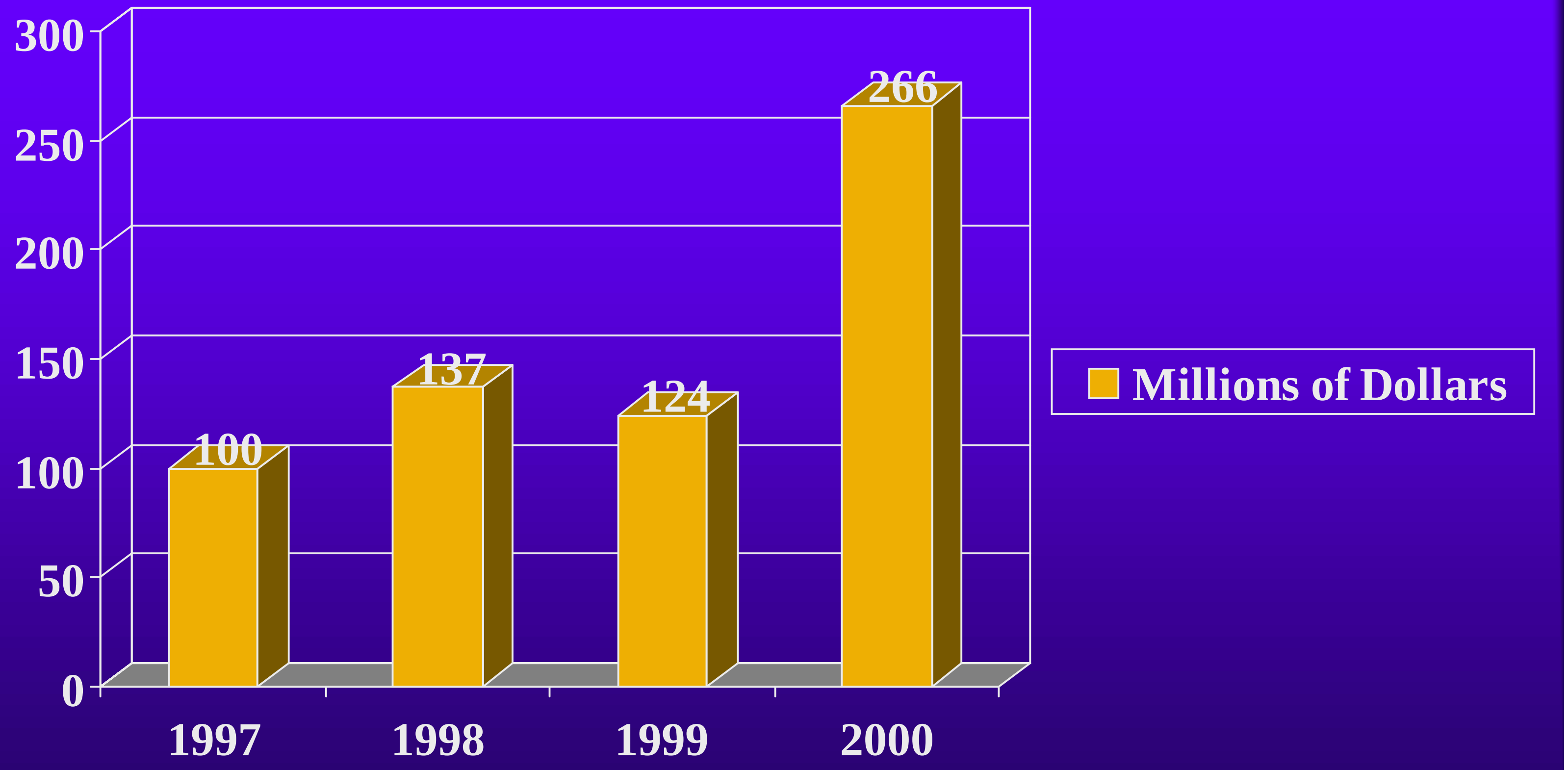
Dollar Amount (in millions) of losses by type in past 12 months reported by respondents willing to quantify losses

	1998	1999	2000
Theft of Proprietary Info	$33.6	$42.5	$66.7
Financial Fraud	$11.2	$39.7	$56.0
Virus	$7.9	$5.3	$29.2
Insider Net Abuse	$3.7	$7.6	$28.0
Sabotage	$2.1	$4.4	$27.1
Unauthorized access by insiders	$50.6	$3.6	$22.6
Laptop theft	$5.3	$13.0	$10.4
Denial of service	$2.8	$3.3	$8.2
System penetration by outsiders	$1.6	$2.9	$7.1
Telecom fraud	$17.3	$0.8	$4.0
Active wiretapping	$0.2	$0.0	$5.0
Telecom eavesdropping	$0.6	$0.8	$1.0

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

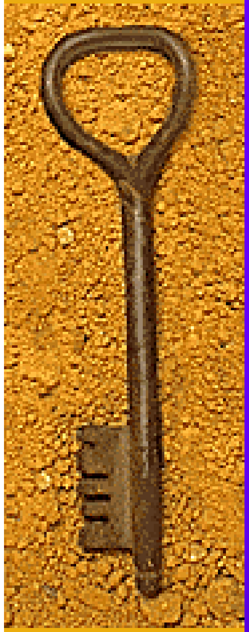


Total Amount Reported by Respondents Willing to Quantify Losses



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

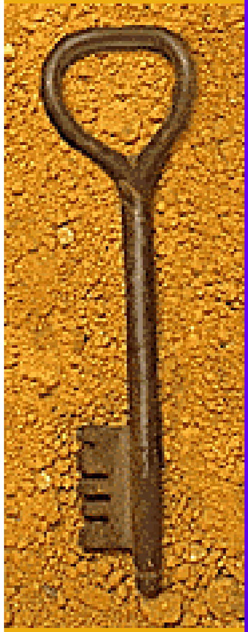
Physical Security



Physical Security

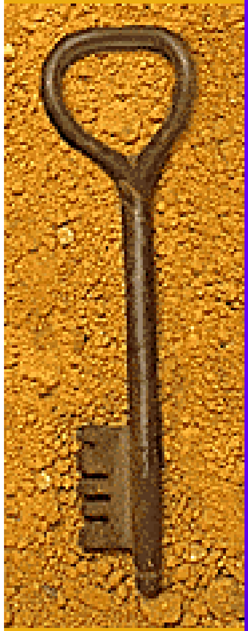
- Restrict access to the computer room
- Computer room walls should go from under raised floor to above ceiling
- Store backup media in a secure area
- Keep system in a secure area
- Keep copies of full backups, etc. offsite

Physical Security *(continued)*



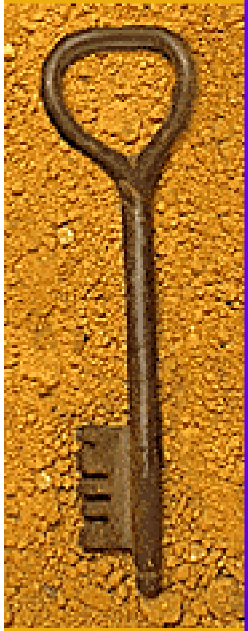
- Lock cabinets containing important information
- Destroy unwanted printer output containing sensitive information
- Secure network cables from exposure
- Log off when leaving terminal unattended
- Clear terminal screens after logging off

Account Security



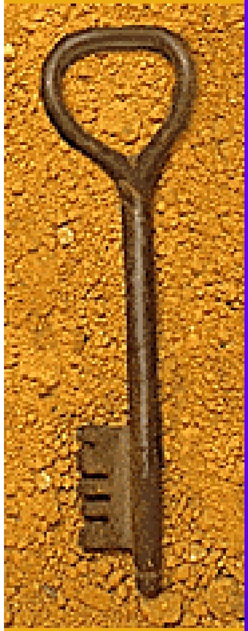
Account Security: Passwords

- Password Guidelines
  - New users should change their password first time they log on
  - All users should have a password
  - Users should not write passwords down
  - Users should not share passwords with anyone
  - Users should not store passwords in function keys
  - Check for weak passwords periodically (Crack)



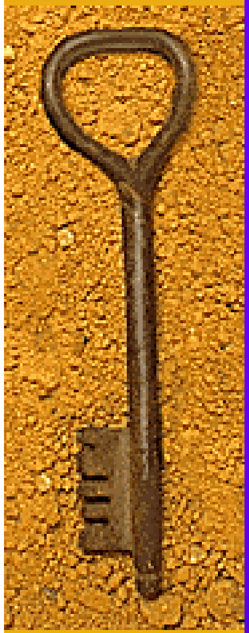
Account Security: Passwords *(continued)*

- Bad Password Composition
  - Your login name
  - Anyone else’s name
  - Women’s names
  - License plates
  - Dictionary words
  - Randomly generated passwords
  - Profane words



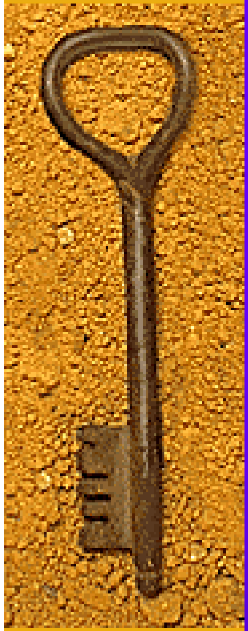
Account Security: Passwords *(continued)*

- Good Password Composition
  - Minimum of six characters
  - At least two alphabetic and one numeric or special character
  - Passwords that mix upper and lower case
  - Acrostic passwords (apsiape: a penny saved is a penny earned)



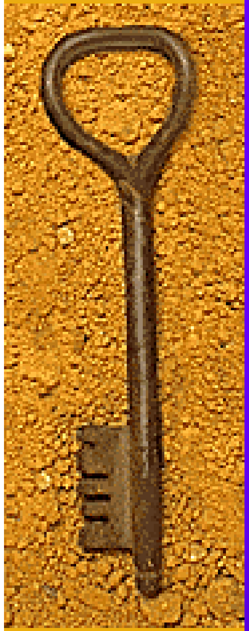
Account Security: Controlling Root Access

- Control number of users with root access
- Restrict root logins to console only (/etc/securetty file)
- Never leave a super-user shell open on an unattended terminal or workstation
- Log in with username and ‘su’ to root
- Change the root password periodically and whenever a root user leaves the company



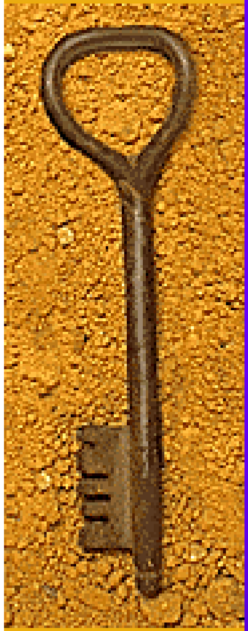
Account Security: Guest Accounts

- Create on an as-needed basis
- Remove when need no longer exists
- Make sure it has a strong password



Account Security: Trust Relationships

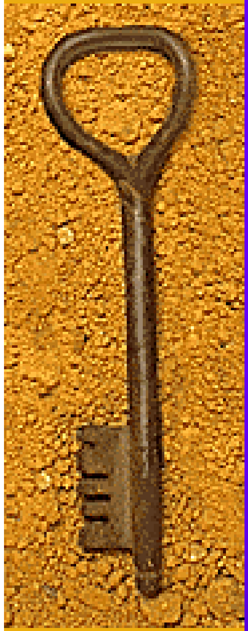
- Be careful with hosts.equiv files
- Restrict use of ‘.rhosts’ files
  - *if allowed permissions should be 600*
- Restrict use of ‘.netrc’ files
  - *if allowed permissions should be 600*



Account Security: Other Best Practices

- Remove accounts upon employee termination
- Disable login for well known accounts such as `sys`, `bin`, `uucp` and others
- Do not allow users to share accounts i.e. every account has a specific owner

File System Security

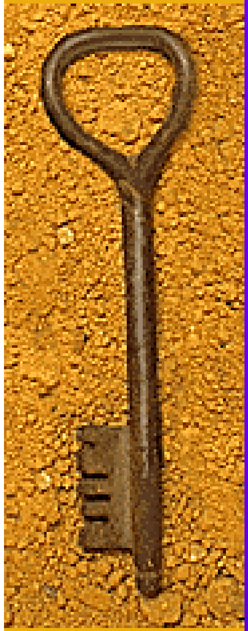


File System Security: Permissions

- Write protect startup files to `rw-------`
- Set `umask` value in .profile, .cshrc or .kshrc

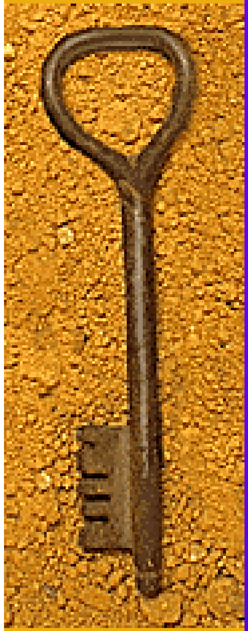
```
022 for root        = chmod 755 rwxr-xr-x
022 for users       = chmod 755 rwxr-xr-x
027 for users       = chmod 750 rwxr-x---
077 for users       = chmod 700 rwx------
```

- Device Files `/dev/null`, `/dev/tty` & `/dev/console` should be world writeable, but never executable, most others should be unreadable & un-writeable by regular users



File System Security: SUID & SGID Files

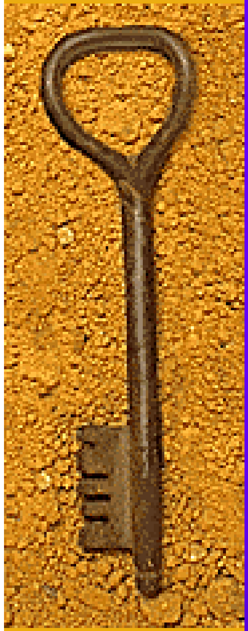
- Don’t write SUID & SGID shell scripts
- Most operating systems have SUID & SGID programs, but these are compiled programs
- Detect with the following commands:
  - `find / -type f -a -perm -4000 -print (suid)`
  - `find / -type f -a -perm -2000 -print (sgid)`



File System Security: Other Best Practices

- Make sure that system files and directories are only writable by root
- Make sure that files executable by root are not writable by anyone else.
- Make sure that users’ home directories are only writable by the owner.
- Eliminate all unnecessary world writable files and directories.
- Give users a restricted shell, or better yet, no shell at all.

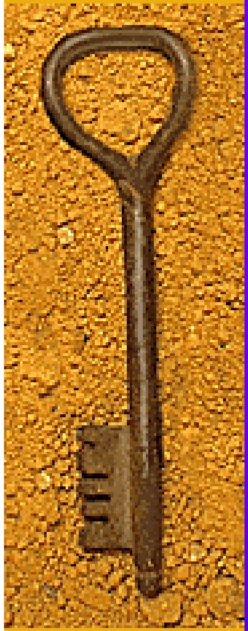
Security Bulletins & Patches



Security Bulletins & Patches

- Customers should subscribe to receive HP security bulletins
- These bulletins will outline specific patches to be installed to correct security vulnerabilities
- Can be found on HP’s I.T. Resource Center at: *http://itresourcecenter.hp.com*

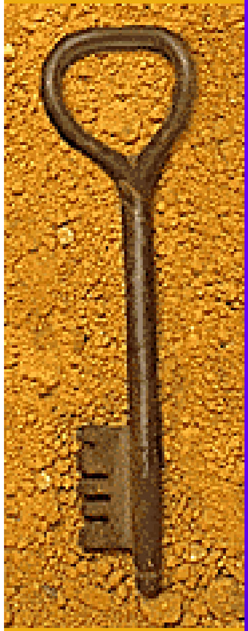
Modem Security



Modem Security

- All modems should have an additional dial-up password
- Details on creating dial-up passwords can be found in the `d_passwd` and `dialups` man pages
- All dial-up modems should log out users upon disconnect (check for hupcl in /etc/gettydefs)

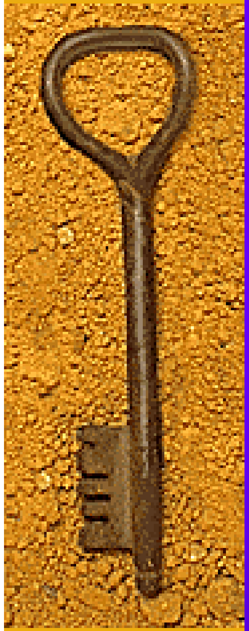
Tightening Up Network Services



Tightening Network Services

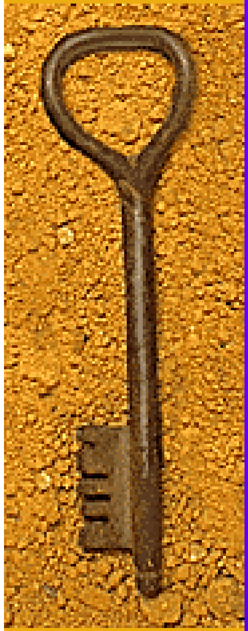
- Disable unnecessary network services in `/etc/inetd.conf`
- Configure access control lists with `/var/adm/inetd.sec`
- Correctly configure allowable services such as NFS, FTP & Anonymous FTP

Monitoring Logfiles



Monitoring Logfiles

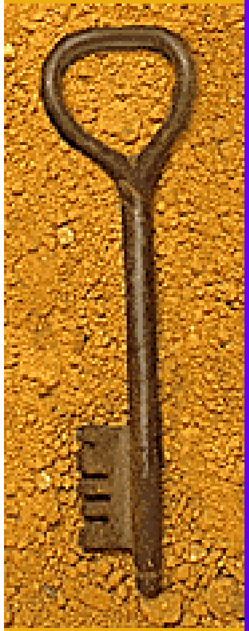
- `/etc/wtmp` (last command)
- `/etc/btmp` (lastb command)
- `/var/adm/sulog`
  (Tells you who has become root)
- `/var/adm/syslog/syslog.log`



Miscellaneous Best Practices

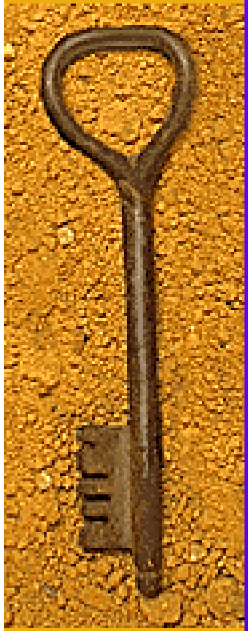
- Never put . (current directory) at the beginning of the path variable (especially root’s)
- Type in the full path name when not at the console.
- Do not allow write access to ANY directories in root’s path.
- Fix well-known security holes (sendmail, tftp, finger, etc.).

Trusted Systems



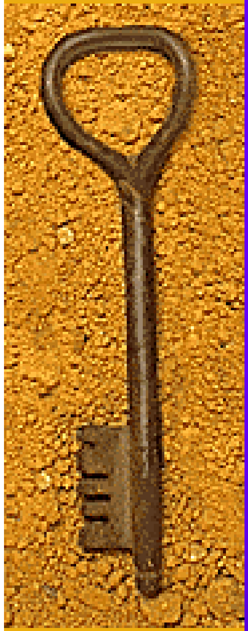
Trusted Systems Features:

- Is included as part of base operating system
- Provides Login Management Capabilities
- Provides Password Management Capabilities
- Provides Terminal Security Features



Trusted Systems - Login Management

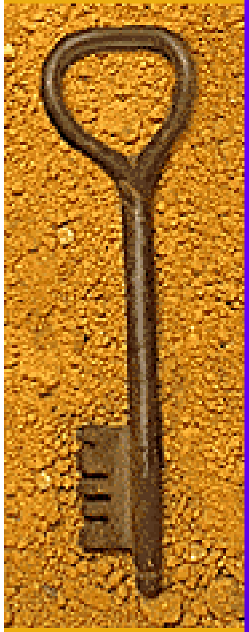
- Password required for single-user boot
- Creation of a defined password life-cycle
- Disables account after a certain number of successive login failures
- Provides time-of-day login access



Trusted Systems - Password Management

- System-wide password aging

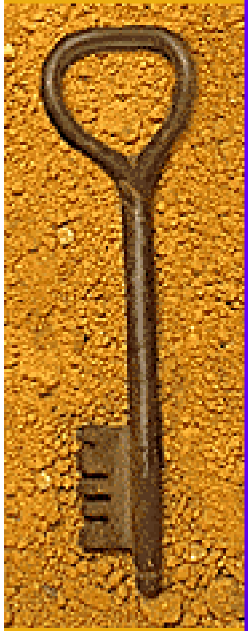
  (*includes min/max time between changes*)
- Warning period before password expires
- Password lifetime
- Random password generator
- Password history in HP-UX 11.00



Trusted Systems - Terminal Security

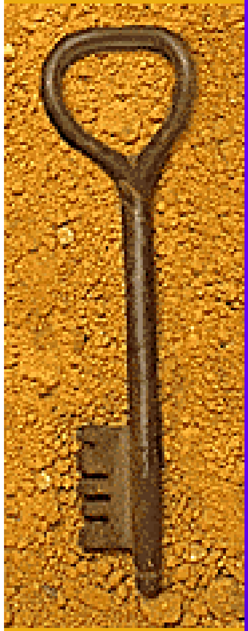
- Device-Based Access Control
- Terminal locked after successive login failures
- Time delay between unsuccessful logins
- Fixed amount of time to login
- List of authorized users per port

Security Tools



Security Tools

- COPS (Various system security checks)
- Crack (Password cracker)
- Tripwire (Detects changes to files)
- Tiger (Determines ways for root to be compromised)
- SATAN (Network security checker)



Security Tools

- To obtain security tools:

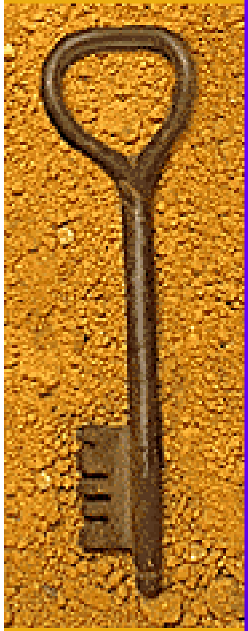
COAST Archive (Purdue University)

`http://www.cs.purdue.edu/coast`

or

`ftp://coast.cs.purdue.edu/pub/tools/unix`

Security Training

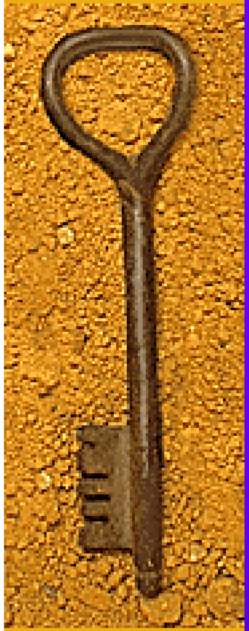


Security Training

Practical UNIX and Network Security (H3541S)

Course Overview:

This five-day course describes typical UNIX system and network vulnerabilities and introduces a variety of tools and techniques to defend against potential security breaches.



Security Training

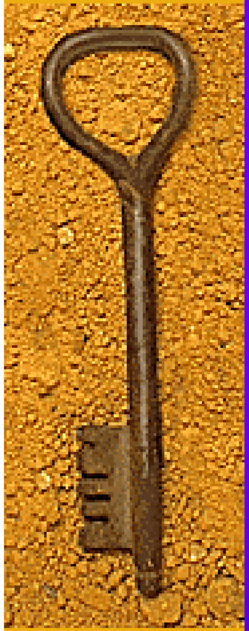
Security Conferences:

- CSI (Computer Security Institute)

  http://www.gocsi.com
- Usenix (Advanced Computing Systems Assoc)

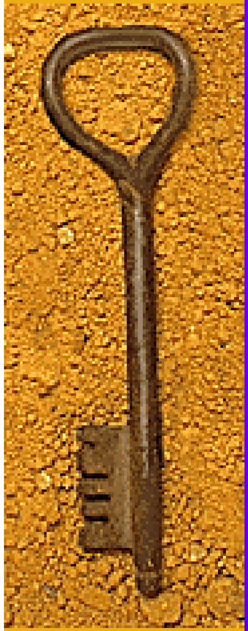
  http://www.usenix.org
- SANS (Systems and Network Security)

  http://www.sans.org



Today’s Agenda

- Physical Security
- Account Security
- File System Security
- Security Bulletins/Patches
- Modem Security
- Tightening Network Services
- Monitoring Logfiles
- Trusted Systems
- Security Tools
- Security Training



Questions?