SESSION 7 – SYSTEM SECURITY

Course Writer: Dr. Ed. Danso Ansong, Dept of Computer Sc.
Contact Information: edansong@ug.edu.gh

UNIVERSITY OF GHANA
College of Education
School of Continuing and Distance Education

- UNIX was not designed with security in mind. UNIX was developed as a research tool, and openness is still one of the major advantages (and weaknesses) of UNIX.

The key topics to be covered in the session are as follows:

- Protection and Safety of Systems
- System Security
- File and account security
- Monitoring and Auditing tools
- Malicious Detection

- Refer to the following reading material which is available on Sakai

RECOMMENDED TEXT

- Unix And Linux System Administration Handbook, 5th [Chapter 5]
- Essentials of Systems Administration 3rd Edition [Chapter 7]

Chapter Objectives

At the end of the session, the student will be able to:

- Deploy basic security measures in a system
- Provide File and Account Security
- Configure and install security Monitoring and Auditing tools
- Detect malicious programs etc.

Chapter Objectives

- Recognize the seven common sense rules of system security
- Understand file, and account security.
- Understand the use of monitoring/auditing tools for system security.
- Recognize the symptoms of viri, trojans, and worms.

System Security

- Computer Security is an oxymoron!
  - UNIX was not designed with security in mind. UNIX was developed as a research tool, and openness is still one of the major advantages (and weaknesses) of UNIX..
  - Personal computers and their Operating Systems, were not designed with security in mind. They were developed as personal systems which would only be used by one user.

$$\text{Security} = \frac{1}{\text{Convenience}}$$

System Security

- Seven common sense rules of security:

1. Don’t put files on your system that are likely to be interesting to hackers or nosy employees. Trade secrets, personnel files, payroll data, election results, etc., must be handled carefully if they’re on-line. Reasonable security can be attained using **compress** and **crypt** on sensitive files.
2. Plug holes that hackers can use to gain access to your system. Read bulletins from your vendor, the security mailing lists and Usenet News groups that provide patches for security holes.

System Security

- Seven common sense rules of security:

3. Don’t provide places for hackers to build nests on your system. Hackers often break into one system and then use it as a base of operations to get into other systems. World-writeable anonymous ftp directories, group accounts, and accounts with poorly chosen passwords all encourage nesting activity.

System Security

- Seven common sense rules of security:

4. Set basic traps on systems that are connected to the Internet. Tools such as **tripwire, crack, SATAN, tcpd, and COPS** will help to keep you abreast of infestations.
5. Monitor the reports generated by the security tools. A minor problem that is ignored in one report may grow into a catastrophe by the time the next report is sent.

System Security

- Seven common sense rules of security:

6. Teach yourself about UNIX system security. A number of high-priced security consultants will happily come to your site and instill terror in you and your management about the insecurity of your systems. They'll explain that for only $50K they can make your site secure.
7. Prowl around looking for suspicious activity. Investigate anything that seems unusual, such as odd log messages or changes in the activity of an account (more activity, strange hours, activity while the owner is on vacation).

System Security

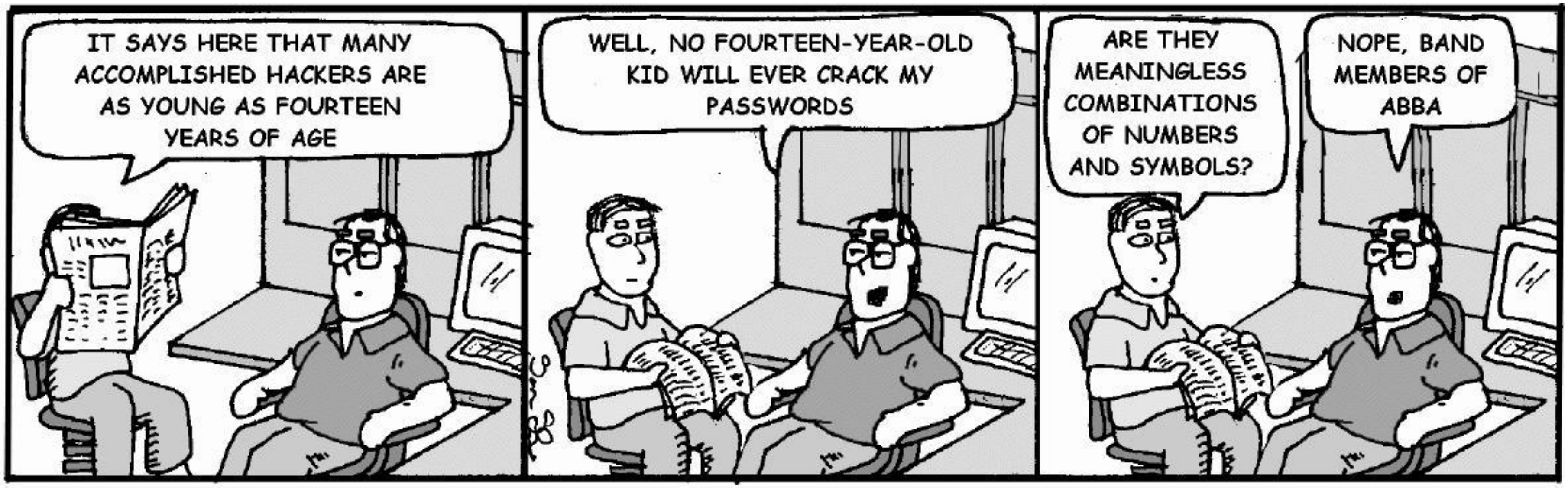
- Account Security
  - Password security is one of the most important areas the system manager has to monitor.
    - Many users chose poor passwords.
    - Many other users have no password on their account.
    - Most users resist changing their passwords.
  - Most versions of UNIX have implemented some form(s) of password protection:
    - Shadow password files.
    - Password programs which require the user to change passwords periodically.
    - password programs which prevent simple passwords.

System Security

- Account Security
  - One method which can increase account security is to use an authentication system such as Kerberos
    - Kerberos uses DES encryption of “tickets” (much like an AFS token) to authenticate a user.
    - Kerberos replaces the password program and sends encrypted passwords (or challenge results) over the network.
    - Kerberos can be set up such that all data is encrypted on the network.
    - Kerberos is becoming more popular, and is being included in more Operating Systems.

System Security

- Account Security
  - The best security tool at any site is an alert administrator.
    - Watch for users logging in at odd hours, or logged in while they are on vacation.
    - Watch for off-site logins by local users.
    - Scan the password file to look for users with UID or GID of zero.


IT SAYS HERE THAT MANY ACCOMPLISHED HACKERS ARE AS YOUNG AS FOURTEEN YEARS OF AGE
WELL, NO FOURTEEN-YEAR-OLD KID WILL EVER CRACK MY PASSWORDS
ARE THEY MEANINGLESS COMBINATIONS OF NUMBERS AND SYMBOLS?
NOPE, BAND MEMBERS OF ABBA

System Security

- File Permissions
  - Once you have established reasonable access security for a system you need to look at the system binaries to ensure they are secure.
    - Are there any world writeable directories on the system?
    - Are there setuid or set gid programs on the system?
    - Have the modify dates on system binaries changed inexplicably?
    - Search path security must be a concern for root.
      - Never put "." in the root path.

System Security

- File Permissions
  - Once you make the system files secure, you have to look at what the users do with their accounts.
    - Are the user home directories “locked up”?
      - Many users leave their account mode 777 if you don’t force them to do otherwise.
      - Do the users have setuid programs in their path?
      - If the user is in multiple groups, are the group permissions set correctly?

System Security

- Data Encryption
  - One cheap method of providing security is to use some form of data encryption for sensitive files.
    - **crypt** is standard on UNIX systems, but is easy to break.
      - The standard UNIX passwords are encrypted with crypt. Linux/BSD use MD5 password encryption.
      - One of the major flaws of crypt is that many strings may encrypt to the same encrypted value, hence password crackers don’t have to have exact matches of a password, just something that encrypts to the same value!
      - If you use crypt, compress the data first. Compressed data is usually un-intelligible, so someone trying to de-crypt compressed data will have a harder time cracking the data.

System Security

- Data Encryption
  - DES encryption utilities are available in the United States. They provide a very good encryption method, but are very difficult to deal with (most Operating Systems do not provide nice methods of incorporating DES encryption).
  - pgp - Pretty Good Privacy - uses a much better encryption method than crypt (and some say better that DES), but is sometimes cumbersome to use. It is easier to tie pgp into the Operating System than DES utilities..

System Security

- Single User Security
  - One of the biggest security holes on workstations is the ability of the user to boot the system into single user mode.
    - Sun Workstations have implemented ROM monitor security that allows the administrator set up three levels of security:
      - None - no Monitor security enabled.
      - Command - requires password for certain monitor commands (examine memory, boot).
      - Full - requires password for all commands.
    - The password for the full and command modes is not the root password. This password is stored in the system EEPROM, and should be a different password from the root password.

System Security

- Single User Security
  - PC systems have started to add in hardware security features.
    - On these systems the administrator can limit access to the CDROM, floppy, memory commands, etc.
    - The administrator can also limit which devices can be booted, and require a password for commands much like the Sun monitor.
  - MacIntosh systems rely upon software to provide security.
    - Applications like At Ease implement a login manager which requires passwords, and allows the administrator to limit access to devices/directories.
    - MacIntosh systems provide no hardware level security.

System Security

- Dialup Modems
  - Another large security problem on any computer is external access. This external access can be via dialup modems, or network connections.
    - For systems with dialup modems, set passwords on the modems such that a user has to know the password before they get connected to the system.
    - If passwords are not possible, implement call-back facilities. The user dials up, enters a code, they hang up, then the system calls them back.
    - Monitor dialup usage!

System Security

- One of the easiest ways to monitor system security is to read the log files!
  - Most versions of UNIX place logs in /var
    - /var/log – maillog, syslog, messages, sshd, authlog, secure, and other log files contain important information.
    - /var/adm – messages
  - Windows uses the Event Viewer to view the system logs. Set the system to record everything, and use event viewer to peruse the logs.
    - Better yet, get syslog for Windows!

System Security

- Security Tools
  - The System administrator can take security one step further by using several public domain tools to periodically scan passwords, system and user files looking for vulnerabilities:
    - COPS - (Computer Oracle and Password System) checks file/directory/device permissions, monitors the password and groups files, monitors the system startup scripts and crontab files, and mails the administrator a report.
    - crack - password cracking program.
    - SATAN/SAINT - checks well-known security holes in system binaries, and tries many means of gaining access to systems.
    - Nessus - New Satan-like scanner (more thorough).
    - Nmap – port scanner.

System Security

- Security Tools
    - tcpd - a TCP wrapper that provides logging for many TCP/IP programs.
    - TRIPWIRE - computes checksums for files, stores them in a database, then on subsequent runs checks to ensure the checksums have not changed. If checksum has changed the administrator get a report and can look at the files in question.
    - tiger - another SATAN clone from Texas A&M
    - courtney - yet another SATAN clone
    - the hackers tools - from rootshell, bugtraq, 2600, l0pht, underground web sites.

System Security

- There are many audit tools available for free download.
  - The Center for Internet Security offers tools to check Solaris, Windows, and Linux hosts, as well as routers for common security problems.
  - The System Administration, Networking, and Security Institute (SANS) has several tools for system auditing, and step-by-step guides to follow to secure your systems.
  - The CERT organization publishes guidelines for system security.

System Security

- Viruses (vira? viri? viru?)
  - Viruses have (until recently) been a pox upon personal computers and MacIntosh computers.
  - Unix virus code is more difficult to produce. Why?
    - UNIX has “permissions” required to write files.
    - UNIX is a much more complicated OS than MacOS or DOS/Windows. Until Linux not many hackers had access to home UNIX systems.
    - UNIX runs on several architectures, while MacOS and DOS only run on limited platforms. This makes machine code impractical for the virus programmer.

System Security

- Viruses (General)
  - A virus is a piece of code that attaches itself to other programs or files.
  - A virus becomes completely dependent on that program or file.
    - Each time you run the program or open the file, the virus code is executed.
    - With each execution the virus code has a chance to propagate.
    - Viruses spread from system to system when the code/files are shared between the systems.

System Security

- Viruses
  - There are two general types of virus programs; malicious, and non-malicious.
    - A non-malicious virus does not intend to cause any lasting damage to the computer system.
      - It propagates.
      - It may print messages on the screen.
      - It may utter noises from the speaker.
      - It does not include any code to **intentionally** do damage to the computer system.

System Security

- Viruses
  - A malicious virus makes a concentrated attempt to do damage to the computer system.
    - It may format your disk drive.
    - It may scramble the FAT table.
    - It may remove random files.
    - It may encrypt the data on the disk.

System Security

- Viruses
  - A virus is not a worm, nor is it a Trojan horse.
    - A Virus is a parasitic piece of code. It attaches itself to other code/files on the system. It relies on that piece of code in order to propagate/operate. When that code is executed so is the virus code. This gives the virus code the opportunity to propagate, and to perform other actions.
    - A worm is a piece of code that propagates itself to other systems, but the code does not attach itself to programs or files on the infected systems. Worms are stand-alone programs that do not rely on a "host" piece of code to propagate/operate.

System Security

- Viruses
    - A Trojan horse is a program that appears to do one thing, but in reality does something else. It does not attach itself to other code/files, and does not rely upon other code/files to propagate/operate. For instance a game program that removes all of your files (on purpose) would be a Trojan horse.

System Security

- PC Viruses
  - PC viruses usually infect files with .exe, .com, and .ovr extensions. These files usually contain executable code.
  - The virus code sometimes infects the command.com file, the hard disk boot sector, the hard disk partition tables, or floppy disk boot sectors.
  - Some virus code is memory resident code. It goes memory resident then sits and waits for other programs to be pulled into memory. When these programs are in memory the virus infects them.
  - Some virus code goes to great lengths to hide itself...for instance the strings in the code are variably encrypted to keep virus scanners from finding the virus.

System Security

- PC Viruses
  - How is a file infected?
    - A user runs a program that is already infected.
    - The virus code is executed, and hunts other files to infect.
    - When an uninfected file is found, the running virus will append a code segment to the uninfected file (in many cases it inserts virus code at the end of the main code section).
    - Once the code is in place the virus (still running from another program at this point) will do one of the following to make the new code segment executable:

System Security

- PC Viruses
  - Some of the things that virus code has been known to do:
    - Change a FAT entry each time the system is booted.
    - Use a random number generator...if the random number generated is N, reformat the disk.
    - Cause odd screen behavior (all the characters fall to the bottom of the screen).
    - If the infected program is opened by a virus scanner, the virus moves itself to memory, disinfects the file, waits until the scanner is done, then re-infects the file.
    - Draw a Christmas Wreath, write Merry Christmas, and play "Oh Tannenbaum" (if the date is between Thanksgiving and Christmas).

System Security

- PC Viruses
  - On the 16th execution of an infected file, pick a random disk sector and write goo to it.
  - Change the order of bytes in database files as they are written to disk. Files look fine on infected systems, but are useless on virus-free systems.
  - Delete the host program if it is run on Friday the 13th.
  - Monitor keyboard input looking for certain strings. If a string is found a profanity is echoed to the screen (and sometimes placed in the file you are editing instead of the string you typed).
  - Watch the INT 09h (keyboard interrupt). If a keystroke is recognized while the virus is active, replicate the keystroke (make it look like a bouncy key).

System Security

- PC Viruses
  - Scan infected files for the string Microsoft. If found, change it to MACHOSOFT.
  - Draw a phallic symbol on the screen and cause it to “march” across the screen.
  - Create directories (with profanities for the directory names) on the system disk.
  - Flip the screen on a horizontal axis.
  - Demand a password before you can execute any programs.
  - Change disk writes into disk reads (or vice versa).

System Security

- PC Viruses
  - Format the system disks.
  - Trash the FAT table.
  - Halt the system.
  - Crash the system.
  - These days, most viri immediately begin attacking other hosts in an attempt to further propagate.
  - Many current viri also carry Denial of Service (DoS) attack code, which may be used by the attacker at a later date to cause infected hosts to attack another site on the Internet.

System Security

- Microsoft Word (Macro) Viruses
  - Recently hackers have found a new way to spread virus code.
    - Many Word Processors, Spreadsheets, and other productivity tools include a macro package. Many of these macro packages are actually based on the **BASIC** programming language.
    - Hackers have learned how to embed a virus code segment into Microsoft Word documents.
    - Every time the document is opened, the virus code is executed as part of the Macro facility startup code.
    - Each invocation of Word infects the document you are editing.

System Security

- Macro Viruses
  - Macro viruses **will** work on UNIX systems if the person who creates them knows UNIX commands and how to access UNIX calls from BASIC.
  - If you have Word Processors, Spreadsheets, or Productivity tools which have the Macro capabilities make sure to turn off the auto-macro execution.

Summary

- Securing the individual systems is the first step toward providing a secure environment.
  - Defense in depth – security should be implemented in layers – like an onion.
- Account and password security are basics that should not be ignored.
- SUID/SGID commands are evil.
- Single User security needs to be monitored.
- Become familiar with the tools available to monitor/implement security on your systems.
- Understand how viri, trojans, and worms work.

- Unix And Linux System Administration Handbook, 5th Edition By Evi Nemeth, Garth Snyder, Trent R. Hein, Ben Whaley, Dan Mackin. Released September 2017. Publisher(s): Addison-Wesley Professional. ISBN: 9780134278308
- Practice Of System And Network Administration, The: Devops And Other Best Practices For Enterprise IT, Volume 1, By Thomas A. Limoncelli, Strata R. Chalup, Christina J. Hogan. Released November 2016. Publisher(s): Addison-Wesley Professional. ISBN: 9780133415087
- Essential System Administration, Third Edition bv Æleen Frisch, Published by O'Reilly Media, Inc. (20(0-596-00343-9