

**Introduction to Information Security**  
**Prof. Dilip. Ayyar**  
**Department of Computer Science and Engineering**  
**Indian Institute of Technology, Madras**

**Lecture – 57**

(Refer Slide Time: 00:11)

## Applying Updates

- Operating systems are intended to be dynamic
- As users' needs change, new hardware is introduced, and more sophisticated attacks are unleashed, operating systems must be updated on a regular basis
- However, vendors release a new version of an operating system every two to four years
- Vendors use certain terms to refer to the different types of updates.




So we will see applying updates. Operating systems are intended to be dynamic. As users needs changes new hardware is introduced and more sophisticated attacks are unleashed, operating systems must be updated on a regular basis. I have seen places or organization where they use windows 2003, and the last update was performed somewhere in 2004, so it is totally vulnerable system. But vendors release a new version of an operating system every two or four years. Vendors use certain terms to refer to the different types of updates also.

(Refer Slide Time: 00:56)

## Applying Updates (continued)

- A **service pack** (a cumulative set of updates including fixes for problems that have not been made available through updates) provides the broadest and most complete update
- A **hotfix** does not typically address security issues; instead, it corrects a specific software problem




Now service pack, it is a cumulative set of updates including fixes for problems that have not been made available through updates, and it provides broadest and more complete update. So service pack is what that is it is cumulative or collective set of updates including fixes for the problem that were identified and which were not made available through updates. A hot fix does not typically address security issue; instead, it corrects a specific software problem. The way a particular function within an OS performs it may have a bug, so hot fix actually fixes that it is not actually security problem, but it can be any issue within the OS.

(Refer Slide Time: 01:52)

## Applying Updates (continued)

- A **patch** or a software update fixes a security flaw or other problem
  - May be released on a regular or irregular basis, depending on the vendor or support team
  - A good patch management system:
    - Design patches to update groups of computers
    - Include reporting system
    - Download patches from the Internet
    - Distribute patches to other computers

<http://www.microsoft.com/windows/serversystem/updateservices/default.aspx>  
<http://www.microsoft.com/technet/security/topics/patchmanagement/secmod193.ms>



A patch or a software update fixes security flaw or other problems. It may be released on

a regular or irregular basis depending upon the vendor or the support team. A good patch management system, what criteria should it have, it should design patches to update a group of computers, it should include a reporting system, it should download all the patches from the net, and it should distribute patches to the other computer. There are two good links of Microsoft given here, you can take the look. Now with respect to patches, I have seen application software for a particular industry, where lot of bugs, lot of security issues, lot of coding errors, so there were lots of issues in that software and the vendor kept on applying patches to them.

Now, one fine day when the audit was happening, we found that there are something close to 1300 patches put on their particular system. And the new version was not released after encompassing or after collecting all the patches no service pack was released. Now suddenly the system crashed, we do know that there were 1300 patches to be fixed somewhere for insignificant issues, somewhere for very significant issues. Now after the system crashed and it was restored; some of the patches were not applied. Now the entire system started behaving erratic. So, now you understand what is or why a patch management system is required, you should also document all the patches that have been applied specifying the patch was made for this particular vulnerability or for this particular error or for this particular bug, it should be noted, it should be applied properly, tested properly. Ultimately, when the vendor releases a new version, all these patches should be included in that version, so that the organization that is going to use that software will not face problems of inconsistent software errors.

(Refer Slide Time: 04:33)

## Securing the File System

- Another means of hardening an operating system is to restrict user access
- Generally, users can be assigned permissions to access folders (also called directories) and the files contained within them




In another way of hardening an OS is to restrict user access. Generally users can be assigned permission to access folders also called directories, and the files contained within them.

(Refer Slide Time: 04:50)

## Securing the File System

- Microsoft Windows provides a centralized method of defining security on the Microsoft Management Console (MMC)
  - A Windows utility that accepts additional components (snap-ins)
  - After you apply a security template to organize security settings, you can import the settings to a group of computers (Group Policy object)




Windows provides a centralized method of defining security on the MMC, which is Microsoft management console. A window utility that accepts additional components called snap-ins. After you apply a security template to the organize security setting, you can import the settings to a group of computers group policy object. Now if you open your computer and type in the search gpedit.mmc, it will open up the group policy editor. If you type mmc, it will open the Microsoft management console.

(Refer Slide Time: 05:32)

## Securing the File System

- Group Policy settings: components of a user's desktop environment that a network system administrator needs to manage
- Group Policy settings cannot override a global setting for all computers (domain-based setting)
- Windows stores settings for the computer's hardware and software in a database (the registry)



Group policy settings components of the user's desktop environment that a network administrator needs to manage. And group policy settings cannot override a global setting for all computers; it is a domain based setting. Windows stores setting for the computer's hardware and software in a database which is the registry.

(Refer Slide Time: 05:56)

## Hardening Applications

- Just as you must harden operating systems, you must also harden the applications that run on those systems
- Hotfixes, service packs, and patches are generally available for most applications; although, not usually with the same frequency as for an operating system
  - Think of Microsoft Office



Just as you must harden the operating systems, you must also harden the applications that run on these systems. So hot fixes, service packs and patches are generally available for most applications; although, not usually with the same frequency as an operating system. You think of Microsoft office, Microsoft windows periodically releases patches, whereas Microsoft office does not release patches so periodically.

(Refer Slide Time: 06:28)

## Hardening Servers (continued)

- Mail server is used to send and receive electronic messages
- In a normal setting, a mail server serves an organization or set of users
- All e-mail is sent through the mail server from a trusted user or received from an outsider and intended for a trusted user





A mail server is used to send and receive electronic messages. In normal setting, a mail server serves an organization or set of users. All e-mail is sent through the mail server from a trusted user or received from an outsider and intended for a trusted user.

(Refer Slide Time: 06:49)

## Hardening Servers (continued)

- In an open mail relay, a mail server processes e-mail messages not sent by or intended for a local user
- File Transfer Protocol (FTP) server is used to store and access files through the Internet
  - Typically used to accommodate users who want to download or upload files



In a open mail relay, a mail server processes the e-mail messages not sent by or intended for a local user. We spoke about this a few slides ago, on how actually telnet into the mail server gives certain commands like `h e l o` or `v h l o` then receipt from then subject, mail from receipt to subject data and although. Then ftp server is used to store an access file through the internet. Typically it is used to accommodate users who want to download or upload files. Now, FTP in Today's environment is considered very in secure by most of the security practitioners. Alternate methods are used to transfer file that is upload and download files, so FTP generally is not used nowadays unless it is a small organization and it is for a specific purpose of transferring files within a small group of people.

(Refer Slide Time: 07:53)

## Hardening Servers (continued)

- FTP servers can be set to accept anonymous logons
- A Domain Name Service (DNS) server makes the Internet available to ordinary users
  - DNS servers frequently update each other by transmitting all domains and IP addresses of which they are aware (zone transfer)



FTP servers can be set to accept anonymous logons. A DNS server makes the internet available to ordinary users; these are all simple explanations of or definitions of different aspects. DNS servers frequently update each other by transmitting all domains and IP address of which they are aware which is called the zone transfer.

(Refer Slide Time: 08:19)

## Hardening Networks

- Two-fold process for keeping a network secure:
  - Secure the network with necessary updates (firmware)
  - Properly configure the network devices




Again in the case of networks is a twofold process for keeping a network secure. Secure their network with necessary updates firmware updates. Properly configure the network devices; if it is a router do not keep everything open update the firmware as and when the vendor releases it; if it is a fire wall, do the same thing.

(Refer Slide Time: 08:44)

## Firmware Updates

- RAM is volatile—interrupting the power source causes RAM to lose its entire contents
- Read-only memory (ROM) is different from RAM in two ways:
  - Contents of ROM are fixed
  - ROM is nonvolatile—disabling the power source does not erase its contents




Firmware is update; RAM is volatile, so interrupting the power source causes the RAM to lose its entire contents. ROM is different from RAM in two ways contents of the ROM are fixed; a ROM is non-volatile, so disabling the power source does not erase its contents.

(Refer Slide Time: 09:07)

## Firmware Updates (continued)

- ROM, Erasable Programmable Read-Only Memory (EPROM), and Electrically Erasable Programmable Read-Only Memory (EEPROM) are firmware (flash)
- The contents of EEPROM chips can also be erased using electrical signals applied to specific pins.
  - Most ROM chips these days can be updated "flashed"



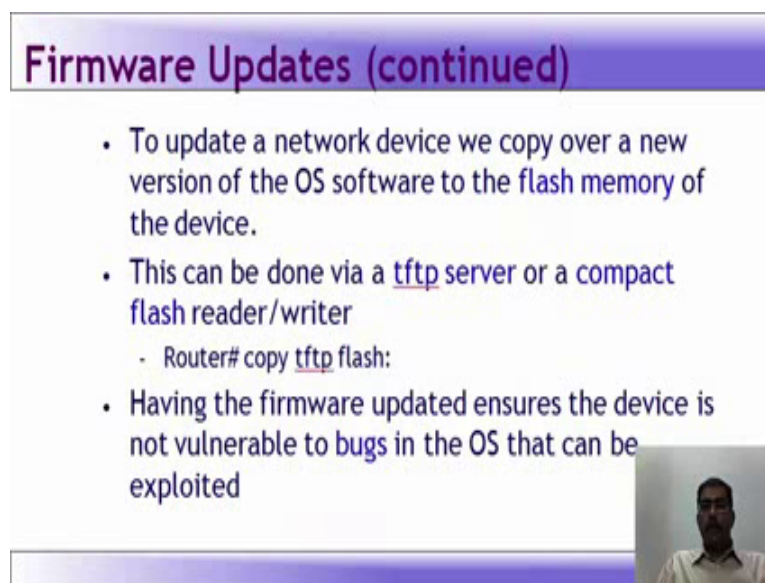
ROM, erasable programmable read only memory EPROM and electrically erasable programmable read only memory EEPROM are firmware or flash devices or flash. The contents of EPROM chips can also be erased using electrical signals applied to specific pins. Most ROM chips these days can be updated or you would have hear the terminology flashed. In say some fifteen years back, the desktops that were purchased do



not have the Ethernet pack built into them, so we had PCI card which we plug into the mother board and then connect the network cable. Now the EPROMS were available at that time, and if we needed to connect to novel network, so we create file to be flashed into that like autoexe.back conflict.sys and other things how it connects to the network certain configuration, we will put on to them and then take it to a place where they burnt the chip and put it on them network cards. This I am talking here almost fifteen to twenty years old.


So, now, those were the days where we had the flexibility of configuring the EPROMS. I think now the SONY play stations generally the PS2, PS3, PS4 devices, they do not generally play the pirated disks or the disks which are copied. I think there are methods to flash the ROM or make that BIOS recognized these disks also. I am not advocating anything, but I have seen people who have done that.

(Refer Slide Time: 11:03)



**Firmware Updates (continued)**

- To update a network device we copy over a new version of the OS software to the flash memory of the device.
- This can be done via a tftp server or a compact flash reader/writer
  - Router# copy tftp flash:
- Having the firmware updated ensures the device is not vulnerable to bugs in the OS that can be exploited



To update network device we copy over a new version of the OS software to flash memory of the device. This can be done via a tftp server or compact flash reader or writer. Now this is a small example in the router hash, you copy tftp flash. Having the firmware updated ensures that the device is not vulnerable to bugs in the OS that can be exploited. Now even in your home WIFI routers or your home access points, you have the facility to download the firmware and uploaded through your browser itself, so you do not have to know you do not have to connect through your telnet or any other port to perform the upgrade, so it is become much more simpler.

(Refer Slide Time: 11:55)

## Network Configuration

- You must properly configure network equipment to resist attacks
- The primary method of resisting attacks is to filter data packets as they arrive at the perimeter of the network
- In addition to making sure the perimeter is secure, make sure the device itself is secure by using strong passwords and encrypted connections
  - SSH instead of Telnet and console, vty passwords



You must properly configure the network equipment to resist attacks. The primary method of resisting attacks is to filter data packets as they arrive at the perimeter of the network. In addition to making sure that the perimeter is secure, make sure the device itself is secure by using strong password and encrypted connections; use ssh instead of telnet and console or vty password.

(Refer Slide Time: 12:29)

## Configuring Packet Filtering

- The User Datagram Protocol (UDP) provides for a connectionless TCP/IP transfer
- TCP and UDP are based on port numbers
- Socket: combination of an IP address and a port number
  - The IP address is separated from the port number by a colon, as in 198.146.118.20:80



Configuring packet filtering the UDP provides for connection less TCP IP transfer. TCP and UDP are based on port numbers. Socket is a combination of IP address and port number say if there is an IP address 198.146.118.20 and the port number is 80. The format is like this; it is separated by a colon.

(Refer Slide Time: 12:59)

## Network Configuration

- Rule base or access control list (ACL): rules a network device uses to permit or deny a packet (not to be confused with ACLs used in securing a file system)
- Rules are composed of several settings



Rule base or access control rules list. It rules a network devices uses to permit or deny a packet it is not to be confused with ACLs used in securing a file system. Rules are composed of several settings in network; rules can be for accept it can be denied or it can be so many other things based on the port number based on the services.

(Refer Slide Time: 13:26)

## Network Configuration

Table 4-6 Sample rule base

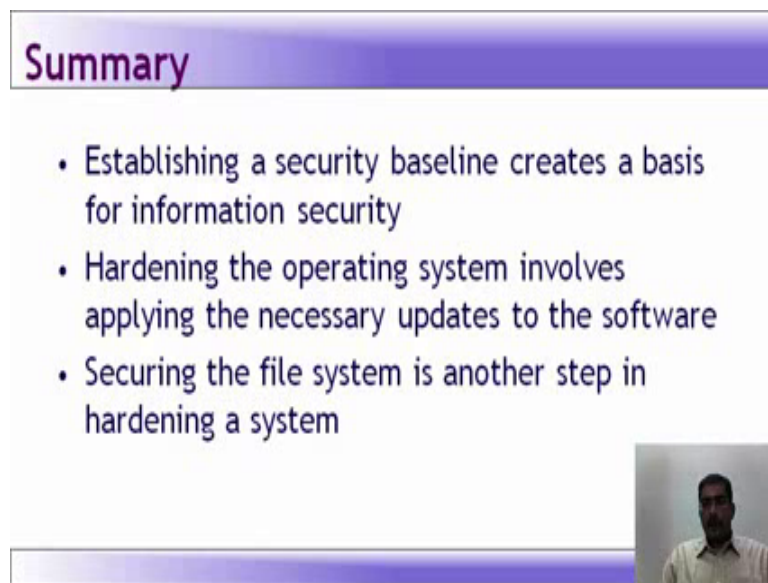
Rule	Transport Protocol	Protocol	Source IP	Source Port	Destination IP	Destination Port	Action	Time	Track
1	TCP	HTTP out-bound	198.146.118.0/24	Any	Any	80	Allow	Any	No
2	TCP	HTTP inbound	206.23.19.40	80	198.146.118.0/2	80	Deny	Any	Yes



A very simple ruled based is shown here; it is a sample only. Now if you see the rule number 1 transport protocol is TCP the protocol used this http out bound traffic the source IP is given the full sub net. Source port from any port, destination IP to any destination port is 80, action is allowed, time is any time no restrictions from time, and the final says track no, do not track. Now for the inbound the second one is for the

inbound connections, so TCP is that 206.23.19.40; source port is 80 destination IP is also given there, destination port is given there, so if it originates from that the action is denied the time is any time that particular connection can be denied, and you want a track that yes. So in simplistic terms, this is how a rule base looks like. So you an organization will have several rules like this that have been configured to permit or to deny access to certain ports or services or based on IPs so that criteria can be varied depending upon the requirements.

(Refer Slide Time: 14:50)



## Summary

- Establishing a security baseline creates a basis for information security
- Hardening the operating system involves applying the necessary updates to the software
- Securing the file system is another step in hardening a system

We almost to the end of the module; now the summary of what we discussed now is establishing a security base line creates a basis for information security. Hardening the operating system involves applying the necessary updates to the software. Securing the file system is another step in hardening the system.

(Refer Slide Time: 15:18)

## Summary (continued)

- Applications and operating systems must be hardened by installing the latest patches and updates
- Servers, such as Web servers, mail servers, FTP servers, DNS servers, NNTP servers, print/file servers, and DHCP servers, must be hardened to prevent attackers from corrupting them or using the server to launch other attacks



Applications and operating systems must be hardened by installing the latest patches and updates. Servers, such as web servers, mail servers, FTP servers, DNS servers, NNTP servers, print or file servers, DHCP servers so any kind email servers must be hardened to prevent attackers from corrupting them or using the server to launch other attacks.

(Refer Slide Time: 15:46)

## Cold Boot Attacks

**Lest We Remember:**  
Cold Boot Attacks on Encryption Keys

[citp.princeton.edu/memory](http://citp.princeton.edu/memory)

<https://www.youtube.com/watch?v=Ej-Nr7>



This lest we remember cold boot attacks on encryption keys is a fantastic video on how the cold boot attacks happened or how information is removed from a memory when the system is on. I would suggest that this is less than ten minute video where an actual demonstration happens. So I would suggest that you go through this, understand the kind of method that are coming into force now days as technology increases or improves day



by day the attack also gets more sophisticated day by day. This cold boot attack will actually tell you how innovative the attackers also happen as the technology progresses. We now at the end of module five, and I hope that you had an enriching session, if you have any queries on the subject please post them on forum, we will try to answer to the best of your satisfaction; I meet you again in module six.