UNIVERSITI TEKNIKAL MALAYSIA MELAKA

Fakulti Teknologi Maklumat dan Komunikasi

Network Security Administration and Management

BITS 3353

Lecture 7: Host, Application and Data Security

Objectives

- List the steps for securing a host computer
- Define application security
- Explain how to secure data using loss prevention

Securing the Host

- Three important elements to secure

HOST (Network server or client)	APPLICATIONS	DATA

Host Security

- **Host Security** refers to securing the operating system, filesystem and the resources of the **Host** from unauthorized access or modification or destruction.
- Securing the host involves

1. Protecting the physical devices
2. Securing the operating system software
3. Using security-based software applications
4. Monitoring logs

Securing Devices

WHY? Prevent unauthorized users from gaining physical access to equipment

Level of security control

Technical control

- controls that are carried out or managed by devices

Administrative control

- processes for developing and ensuring that policies and procedures are carried out.
- the actions that users *may do*, *must do*, or *cannot do*.

Securing Devices

Control name	Description	When it occurs	Example
Deterrent control	Discourage attack	Before attack	Signs indicating that the area is under video surveillance
Preventive control	Prevent attack	Before attack	Security awareness training for all users
Detective control	Identify attack	During attack	Installing motion detection sensors
Compensating control	Alternative to normal control	During attack	An infected computer is isolated on a different network
Corrective control	Lessen damage from attack	After attack	A virus is cleaned from an infected server

Activity phase controls

Securing Devices

WHY? Prevent unauthorized users from gaining access to equipment

SECURING DEVICES:

External Perimeter Defenses - designed to restrict access to the areas in which equipment is located

Internal physical access security - focused on the interior of the area.

Hardware security - physical security that specifically involves protecting the hardware of the host system, particularly portable laptops and tablet computers that can easily be stolen.

External Perimeter Defenses

Barriers

•Fencing

– Passive security elements

Barrier around secured area

–Modern perimeter fences are equipped with other deterrents

Securing Devices

Technology	Description	Comments
Anti-climb paint	A nontoxic petroleum gel-based paint that is thickly applied and does not harden, making any coated surface very difficult to climb	Typically used on poles, downpipes, wall tops, and railings above head height (8 feet or 2.4 meters)
Anti-climb collar	Spiked collar that extends horizontally for up to 3 feet (1 meter) from the pole to prevent anyone from climbing; serves as both a practical and visual deterrent	Spiked collars are for protecting equipment mounted on poles like CCTV or in areas where climbing a pole can be an easy point of access over a security fence
Roller barrier	Independently rotating large cups (with a diameter of 5 inches or 115 millimeters) affixed to the top of a fence prevent the hands of intruders from gripping the top of a fence to climb over it	Often found around public grounds and schools where a nonaggressive barrier is important
Rotating spikes	Installed at the top of walls, gates, or fences; the tri-wing spike collars rotate around a central spindle	Can be painted to blend into fencing

Fencing deterrents

External Perimeter Defenses

Guards

- Active security elements
- Some guards are responsible for monitoring activity that is captured by a video camera

Video surveillance

–Closed-circuit television (CCTV)

•Video cameras transmit signal to limited set of receivers

•Cameras may be fixed or able to move

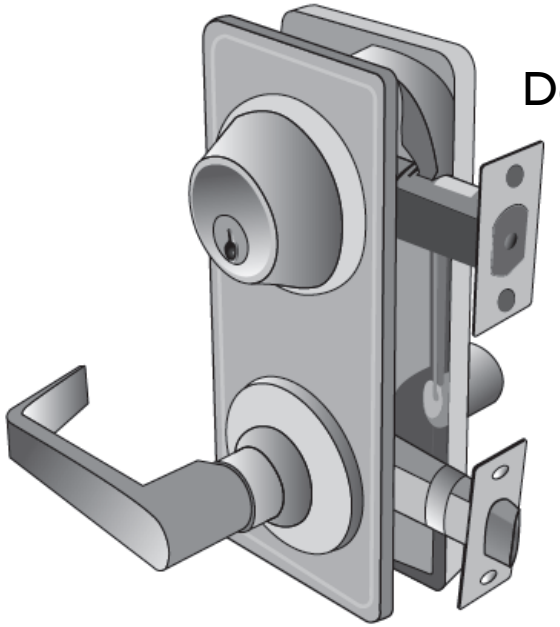
Internal Physical Access Security

Hardware Locks

- Hardware locks for doors in residences generally fall into four categories.
  - Keyed entry lock
  - Privacy lock
  - Patio lock
  - Passage lock

Residential keyed entry lock

- The standard keyed entry lock
- security is minimal



Deadbolt lock

- more difficult to defeat than keyed entry locks.
- Extends a solid metal bar into the door frame for extra security

Internal Physical Access Security

CIPHER LOCK

–More sophisticated alternative to key lock

–Combination sequence necessary to open door

–Can be programmed to allow individual's code to give access at only certain days or times

–Records when door is opened and by which code

–Can be vulnerable to shoulder surfing

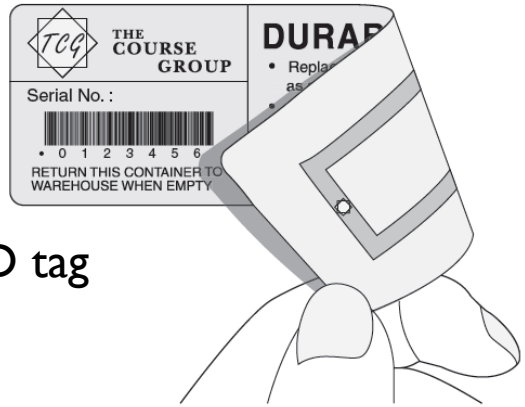
–Often used in conjunction with tailgate sensor

Cipher lock

Internal Physical Access Security

Proximity Readers

- ID Badge
  - contained a photograph of the bearer and were visually screened by security guards.
  - ID badges were *magnetic stripe cards* that were "swiped" or contained a *barcode* identifier that was "scanned" to identify the user.



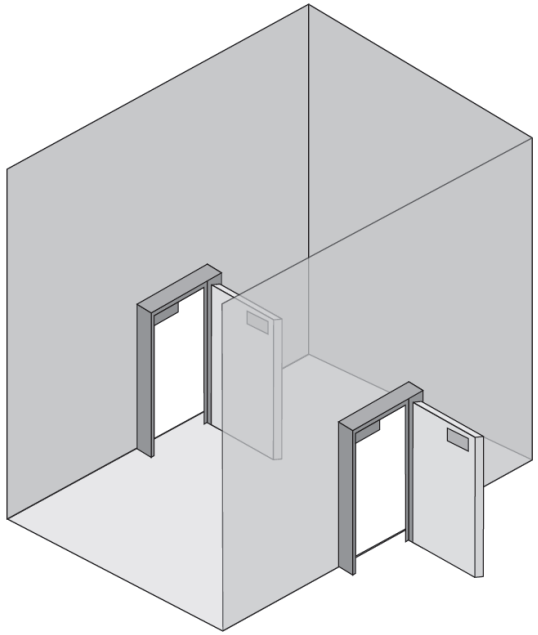
RFID tag

RFID tags
–Can be affixed inside ID badge
–Read by an RFID proximity reader
•Badge can remain in bearer's pocket

Internal Physical Access Security

Mantrap

–Separates a secured from a nonsecured area
–Device monitors and controls two interlocking doors
•Only one door may open at any time



Mantrap

Hardware Security

Cable Lock

- Physical security protecting host system hardware
- Portable devices have steel bracket security slot
  - -Cable lock inserted into slot and secured to device
  - -Cable connected to lock secured to desk or immobile object

- Laptops may be placed in a safe
- Locking cabinets
  - -Can be prewired for power and network connections
  - -Allow devices to charge while stored

Cable lock

Securing the Operating System
Software: Security through configuration

Security through configuration

1. Develop the security policy
2. Perform host software baselining
3. Configure operating system security and settings
4. Deploy the settings
5. Implement patch management

1 Develop the security policy

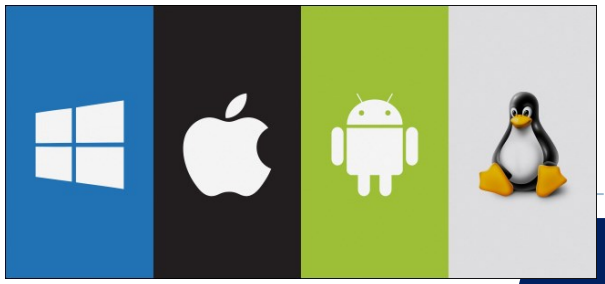
–Document(s) that clearly define organization's defense mechanisms

2 Perform host software baselining

–Baseline: standard or checklist against which systems can be evaluated
–Configuration settings that are used for each computer in the organization

3 Configure operating system security and settings

–Hundreds of different security settings can be manipulated
–Typical configuration baseline
•Changing insecure default settings
•Eliminating unnecessary software, services, protocols
•Enabling security features such as a firewall



Securing the Operating System Software

4 Deploy the settings

–Security template: collections of security configuration settings
–Process can be automated

•Group policy
–Windows feature providing centralized computer management
–A single configuration may be deployed to many users

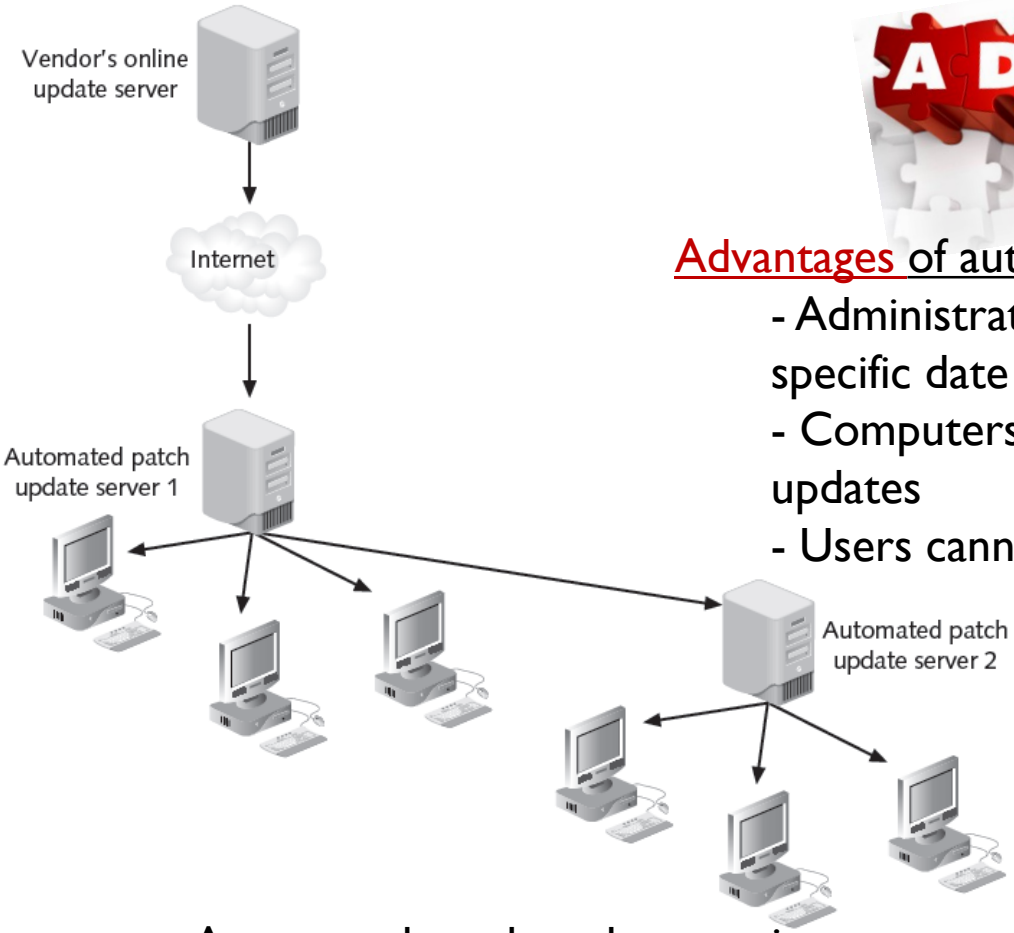
5 Implement Patch Management

–Modern operating systems can perform automatic updates

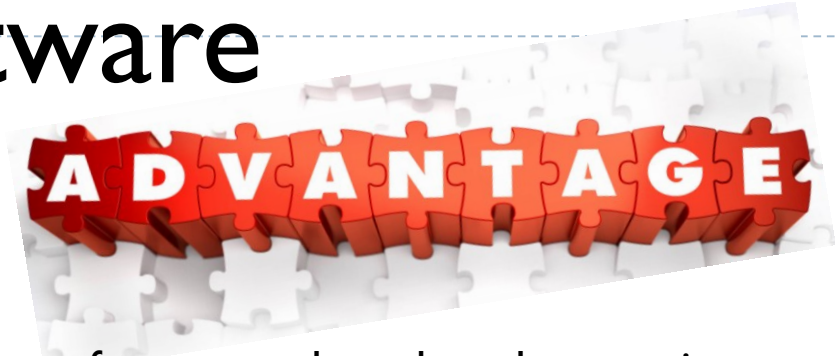
•Patches can sometimes create new problems
–Vendor should thoroughly test before deploying

• Automated patch update service
–Manage patches locally rather than rely on vendor's online update service

Securing the Operating System Software



Automated patch update service



Advantages of automated patch update service

- Administrators can force updates to install by specific date
- Computers not on the Internet can receive updates
- Users cannot disable or circumvent updates

Securing the Operating System
Software: Securing with Antimalware

ANTI-VIRUS

–Software that examines a computer for infections
–Scans new documents that might contain viruses
–Searches for known virus patterns

Weakness of anti-virus
–Vendor must continually search for new viruses, update and distribute signature files to users
•Alterative approach: **code emulation**
–Questionable code executed in virtual environment

ANTISPAM

- Spammers can distribute malware through email attachments
- Spam can be used for social engineering attacks
- Spam filtering methods

–Bayesian filtering

–Local host filtering

- Blacklist
- Whitelist

–Blocking certain file attachment types

Securing the Operating System
Software: Securing with Antimalware

POP-UP

–Small window appearing over Web site
–Usually created by advertisers

POP-UP BLOCKERS

–Separate program as part of anti-spyware package
–Incorporated within a browser
–Allows user to limit or block most pop-ups
–Alert can be displayed in the browser
•Gives user option to display pop-up

HOST-BASED FIREWALL

–Designed to prevent malicious packets from entering or leaving computers

–May be hardware or software-based

–Host-based software firewall runs on local system

Application-based firewall

- Application running on a host computer may need to send and receive transmissions that normally would be blocked by the firewall.
- More secure than opening a port on the firewall

Host Security

- **Host Security** refers to securing the operating system, filesystem and the resources of the **Host** from unauthorized access or modification or destruction.
- Securing the host involves

1. Protecting the physical devices
2. Securing the operating system software
3. Using security-based software applications
4. Monitoring logs

Monitoring System Logs

LOG record of events that occur

SECURITY LOG reveal the types of attacks that are being directed at the network and if any of the attacks were successful

Log entries

- Contain information related to a specific event

  -Access log can provide details about requests for specific files

  -Audit log can track user authentication attempts

  - System event logs can document any unsuccessful events and the most significant successful events

Monitoring System Logs

Device	Explanation
Firewalls	Firewall logs can be used to determine whether new IP addresses are attempting to probe the network and if stronger firewall rules are necessary to block them. Outgoing connections, incoming connections, denied traffic, and permitted traffic should all be recorded.
Network intrusion detection systems (NIDS) and network intrusion prevention systems (NIPS)	Intrusion detection and intrusion prevention systems record detailed security log information on suspicious behavior as well as any attacks that are detected. In addition, these logs also record any actions NIPS used to stop the attacks.
Web servers	Web servers are usually the primary target of attackers. These logs can provide valuable information about the type of attack that can help in configuring good security on the server.
DHCP servers	DHCP server logs can identify new systems that mysteriously appear and then disappear as part of the network. They can also show what hardware device had which IP address at a specific time.
VPN concentrators	VPN logs can be monitored for attempted unauthorized access to the network.
Proxies	As intermediate hosts through which websites are accessed, these devices keep a log of all URLs that are accessed through them. This information can be useful when determining if a zombie is "calling home."
Domain Name System (DNS)	A DNS log can create entries in a log for all queries that are received. Some DNS servers also can create logs for error and alert messages.
Email servers	Email servers can show the latest malware attacks that are being launched through the use of attachments.
Routers and switches	Router and switch logs provide general information about network traffic.

Device logs with beneficial security data

Monitoring System Logs

Benefits of monitoring system logs

- Identify security incidents, policy violations, fraudulent activity
- Provide information shortly after event occurs
- Provide information to help resolve problems
- Help identify operational trends and long-term problems
- Provide documentation of regulatory compliance

Application Security

- Application security is the process of making apps more secure by finding, fixing, and enhancing the security of apps.
- Much of this happens during the development phase, but it includes tools and methods to protect apps once they are deployed.

Aspects of securing applications

Application development security

Application hardening

Patch management

Application Security : Application Development Security

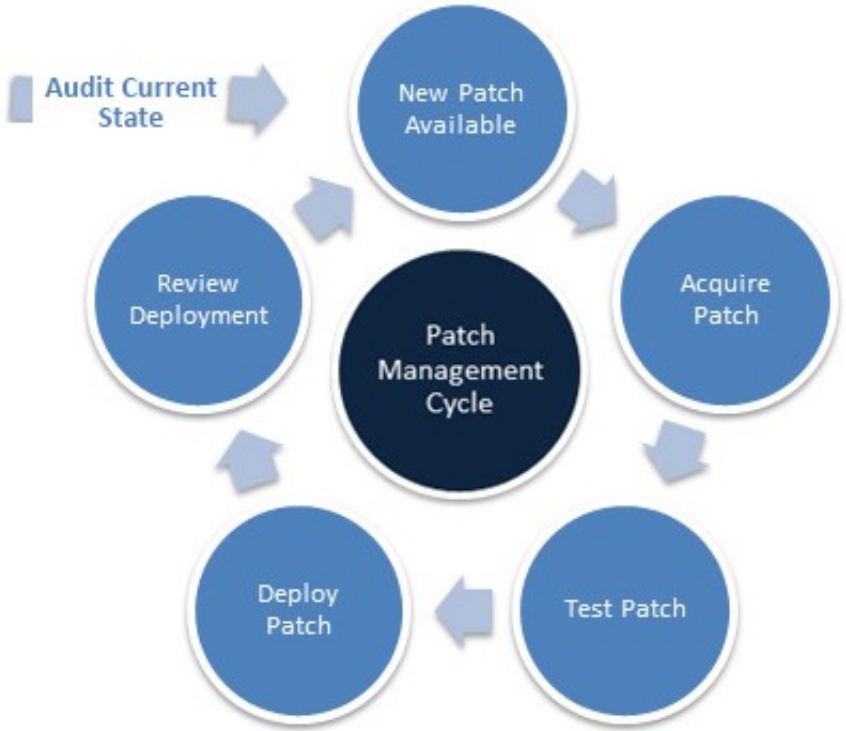
- Security for applications must be considered through all phases of development cycle
- Application configuration baselines
  - –Standard environment settings can establish a secure baseline
  - –Includes each development system, build system, and test system
  - –Must include system and network configurations
- Secure coding concepts
  - –Coding standards increase applications' consistency, reliability, and security
  - –Coding standards useful in code review process
- Errors and Exception Handling
  - –Faults that occur while application is running
  - –Response should be based on the error
  - –Improper handling can lead to application failure or insecurity

Application Security : Application Hardening

- Application hardening is the process of securing an application against local and internet-base attacks.
- Application hardening is possible by removing the functions or components that you don't require. You can restrict access and make sure the application is kept up-to-date with patches.

Application Security : Patch Management

Patch management is the process that helps acquire, test and install multiple patches (code changes) on existing applications and software tools on a computer, enabling systems to stay updated on existing patches and determining which patches are the appropriate ones.



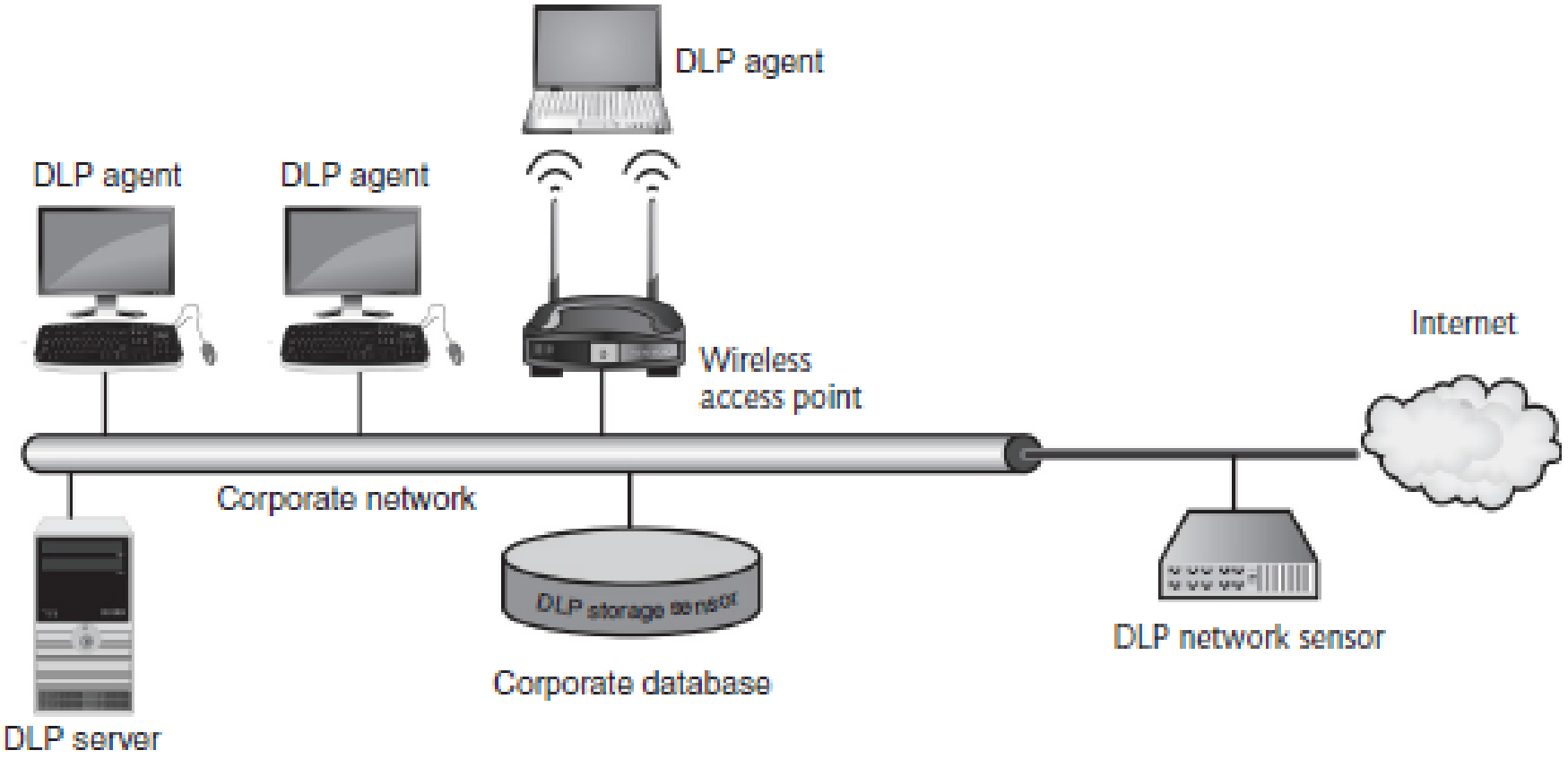
Securing Data

- Work today involves electronic collaboration
  - –Data must flow freely
  - –Data security is important

Data Loss Prevention

- Data Loss Prevention is a system of security tools used to recognize and identify critical data and ensure it is protected

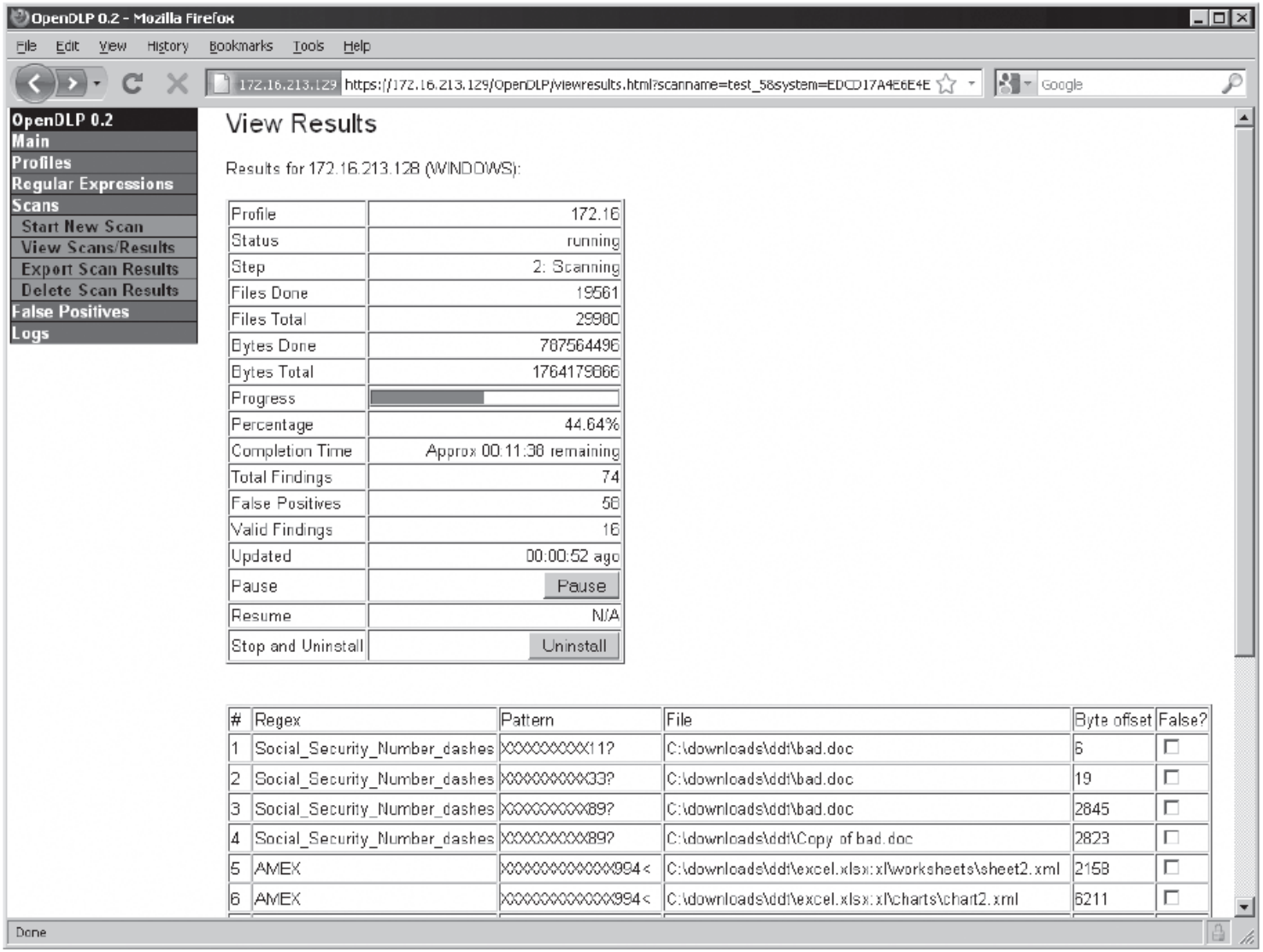
- **Goal**: protect data from unauthorized users
- Data loss prevention typically examines:
  - –Data in use (example: being printed)
  - –Data in motion (being transmitted)
  - –Data at rest (stored)



DLP architecture

Summary

- Physical access security includes door locks of various types
- Portable devices can be secured with a cable lock
- Remote wipe / sanitation can erase device contents from a distance if stolen
- Security policy must be created, then a baseline can be established
- Third-party anti-malware software can provide added security
- Monitoring system logs is useful in determining how an attack occurred
- Protecting applications that run on hardware
  - Create configuration baselines
  - Secure coding concepts
- Data loss prevention (DLP) can identify critical data, monitor and protect it
  - Works through content inspection


OpenDLP 0.2 - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://172.16.213.129/OpenDLP/viewresults.html?scanname=test_5&system=EDCD17A4E6E4E
Google
OpenDLP 0.2
Main
Profiles
Regular Expressions
Scans
Start New Scan
View Scans/Results
Export Scan Results
Delete Scan Results
False Positives
Logs
View Results
Results for 172.16.213.128 (WINDOWS):
Profile 172.16
Status running
Step 2: Scanning
Files Done 19561
Files Total 29980
Bytes Done 787564496
Bytes Total 1764179866
Progress
Percentage 44.64%
Completion Time Approx 00:11:38 remaining
Total Findings 74
False Positives 58
Valid Findings 16
Updated 00:00:52 ago
Pause Pause
Resume N/A
Stop and Uninstall Uninstall
Regex Pattern File Byte offset False?
1 Social_Security_Number_dashes XXXXXXXXX11? C:\downloads\ddl\bad.doc 6
2 Social_Security_Number_dashes XXXXXXXXX33? C:\downloads\ddl\bad.doc 19
3 Social_Security_Number_dashes XXXXXXXXX89? C:\downloads\ddl\bad.doc 2845
4 Social_Security_Number_dashes XXXXXXXXX89? C:\downloads\ddl\Copy of bad.doc 2823
5 AMEX XXXXXXXXXXXX994< C:\downloads\ddl\excel.xlsx:xl\worksheets\sheet2.xml 2158
6 AMEX XXXXXXXXXXXX994< C:\downloads\ddl\excel.xlsx:xl\charts\chart2.xml 6211
Done

DLP report