Principles of 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
- Securing the host involves:
  - Protecting the physical device
  - Securing the operating system software
  - Using security-based software applications
  - Monitoring logs

Securing Devices

- Prevent unauthorized users from gaining physical access to equipment
- Aspects of securing devices
  - Physical access security
  - Host hardware security
  - Mobile device security

Securing Devices (cont'd.)

- Physical security
  - Restricting access to equipment areas
- Hardware locks
  - Standard keyed entry lock provides minimal security
  - Deadbolt locks provide additional security
- Keyed locks can be compromised if keys lost, stolen, or duplicated

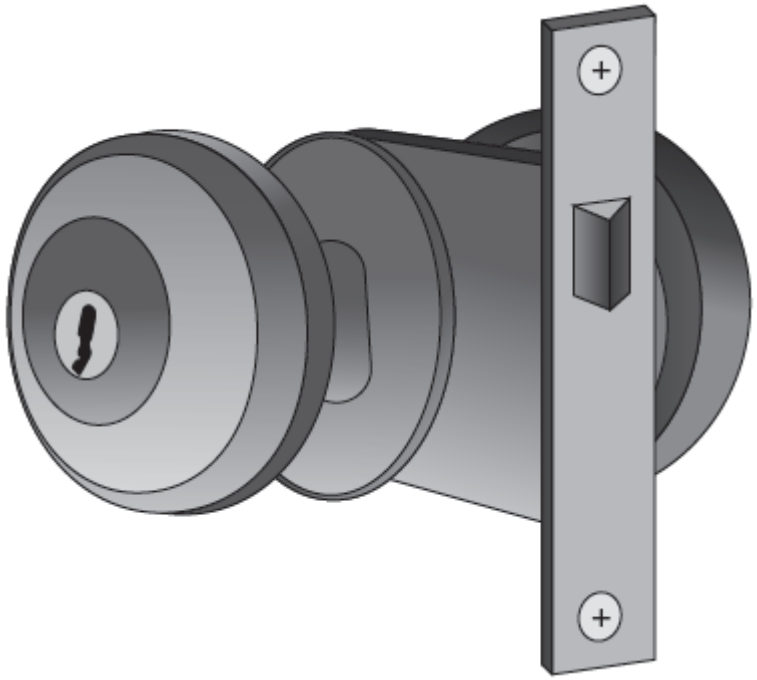

Figure 5-1 Residential keyed entry lock

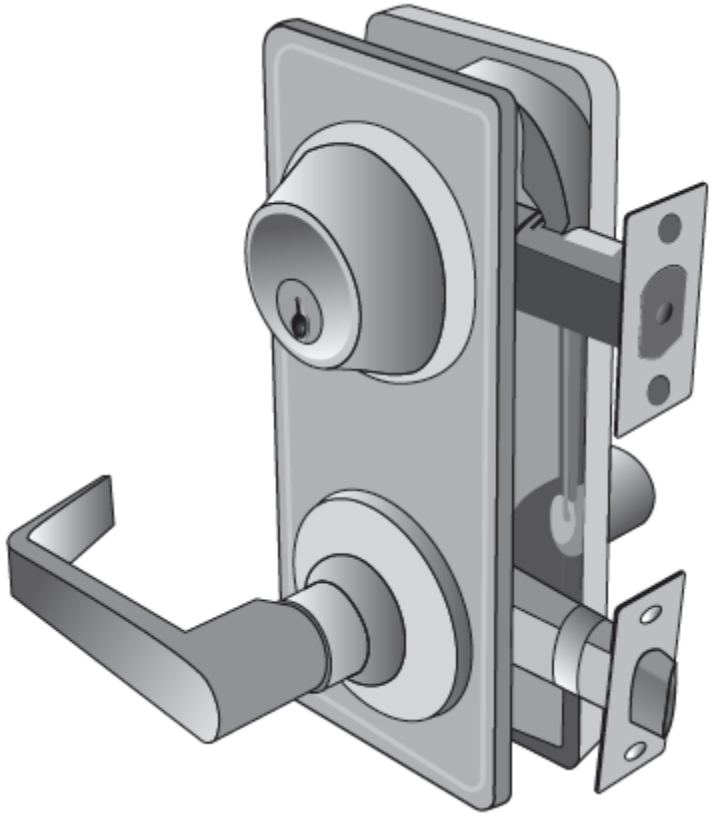

Figure 5-2 Deadbolt lock

Securing Devices (cont'd.)

- Recommended key management procedures
  - Change locks after key loss or theft
  - Inspect locks regularly
  - Issue keys only to authorized users
  - Keep records of who uses and turns in keys
  - Keep track of issued keys
  - Master keys should not have identifying marks

Securing Devices (cont'd.)

- Recommended key management procedures (cont'd.)
  - Secure unused keys in locked safe
  - Set up key monitoring procedure
  - Mark duplicate master keys with "Do not duplicate"
    - Wipe out manufacturer's serial number to prevent duplicates from being ordered

Securing Devices (cont'd.)

- 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

Figure 5-3 Cipher lock

Securing Devices (cont'd.)

- Alternative access method: physical token
  - ID badge may contain bearer's photo
  - ID badge emits a signal identifying the owner
  - Proximity reader receives signal
- RFID tags
  - Can be affixed inside ID badge
  - Read by an RFID proximity reader
    - Badge can remain in bearer's pocket

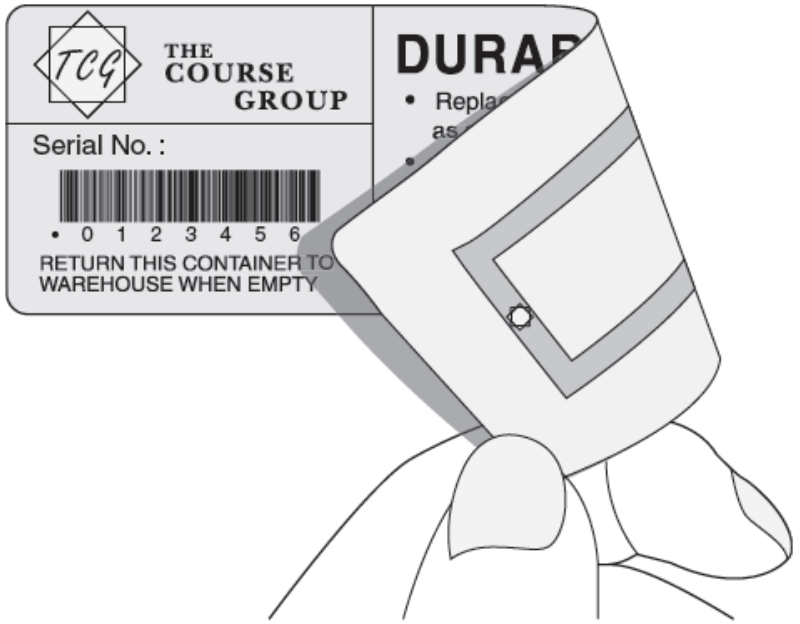

Figure 5-4 RFID tag

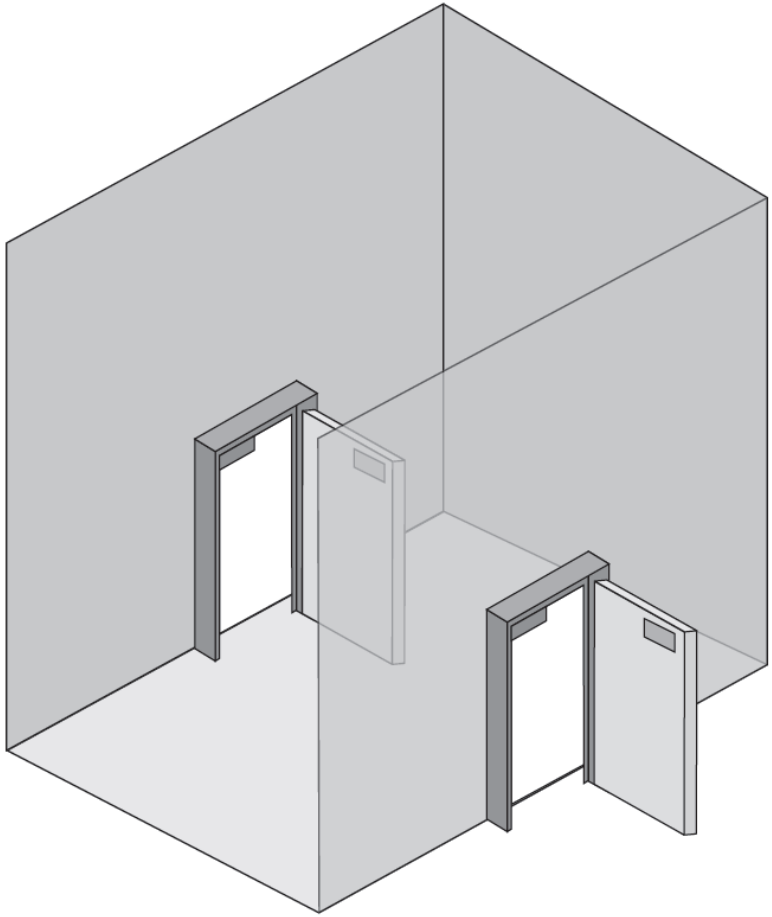

Figure 5-5 Mantrap

Securing Devices (cont'd.)

- Access list
  - Record of individuals who have permission to enter secure area
  - Records time they entered and left
- Mantrap
  - Separates a secured from a nonsecured area
  - Device monitors and controls two interlocking doors
    - Only one door may open at any time

Securing Devices (cont'd.)

- Video surveillance
  - Closed-circuit television (CCTV)
    - Video cameras transmit signal to limited set of receivers
    - Cameras may be fixed or able to move
- Fencing
  - Barrier around secured area
  - Modern perimeter fences are equipped with other deterrents

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

Table 5-1 Fencing deterrents

Securing Devices (cont'd.)

- Hardware security
  - 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

Figure 5-6 Cable lock

Securing Devices (cont'd.)

- Mobile device security
  - Many security provisions that apply to laptops apply to mobile devices
- Mobile devices' unique security features
  - Remote wipe / sanitation
    - Data can be remotely erased if device is stolen
  - GPS tracking
    - Can pinpoint location to within 100 meters

Securing Devices (cont'd.)

- Mobile devices' unique security features (cont'd.)
  - Voice encryption
    - Used to mask content of voice communication over a smartphone

Securing the Operating System Software

- Five-step process for protecting operating system
  - Develop the security policy
  - Perform host software baselining
  - Configure operating system security and settings
  - Deploy the settings
  - Implement patch management

Securing the Operating System Software (cont'd.)

- Develop the security policy
  - Document(s) that clearly define organization's defense mechanisms
- 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

Securing the Operating System Software (cont'd.)

- 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 (cont'd.)

- 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

Securing the Operating System Software (cont'd.)

- Operating systems have increased in size and complexity
- New attack tools have made secure functions vulnerable
- Security patch
  - General software update to cover discovered vulnerabilities

Operating system	Number of lines of code
Linux kernel version 2.6	5 million
FreeBSD	9 million
Red Hat Linux version 7	30 million
Microsoft Windows 7	50 million
Mac OS X version 10.4	86 million
Debian version 5.0	324 million

Table 5-2 Estimated size of selected operating systems

Securing the Operating System Software (cont'd.)

- Hotfix addresses specific customer situation
- Service pack accumulates security updates and additional features
- Implement patch management
  - Modern operating systems can perform automatic updates
- Patches can sometimes create new problems
  - Vendor should thoroughly test before deploying

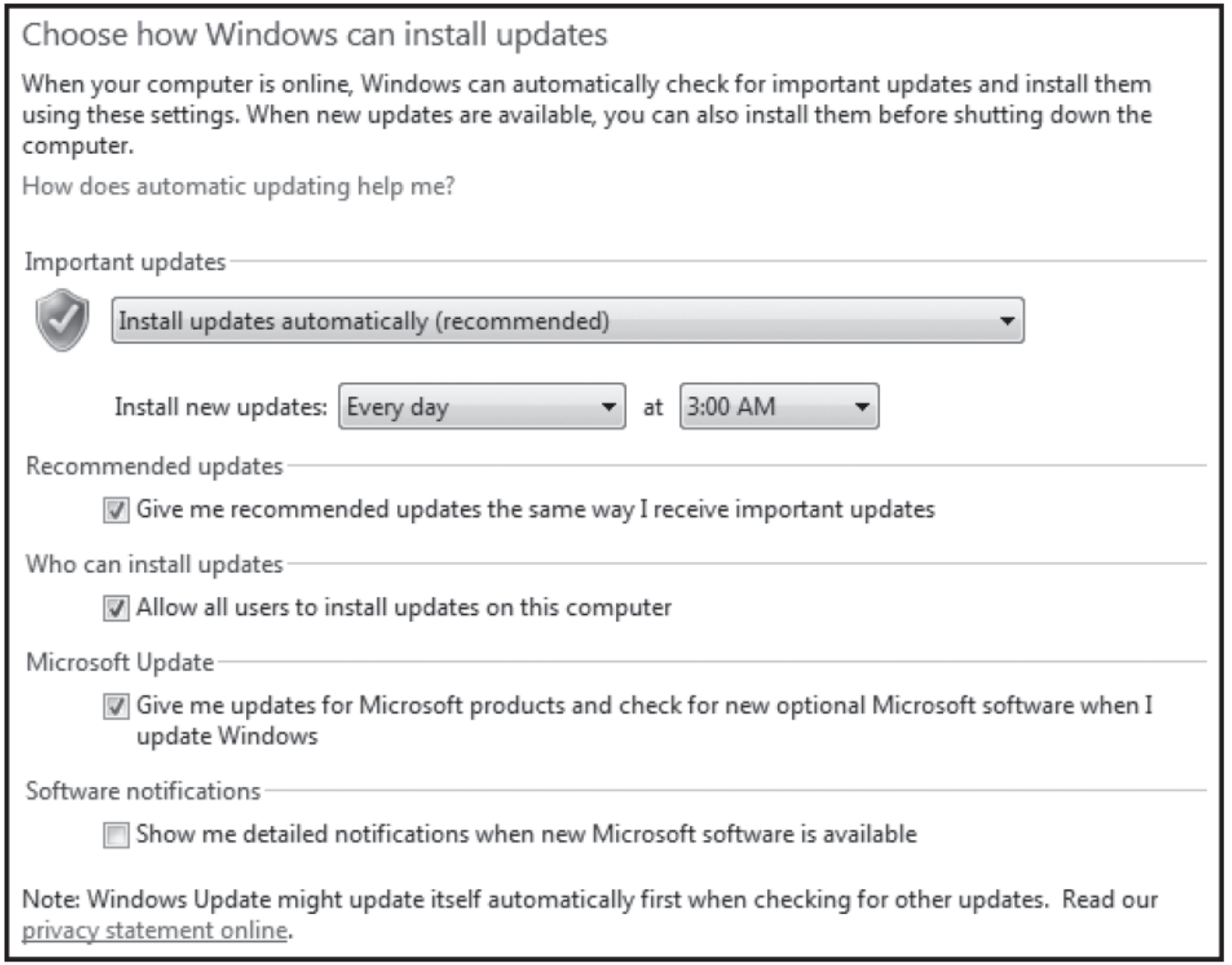

Figure 5-7 Microsoft Windows 7 automatic update options

Securing the Operating System Software (cont'd.)

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

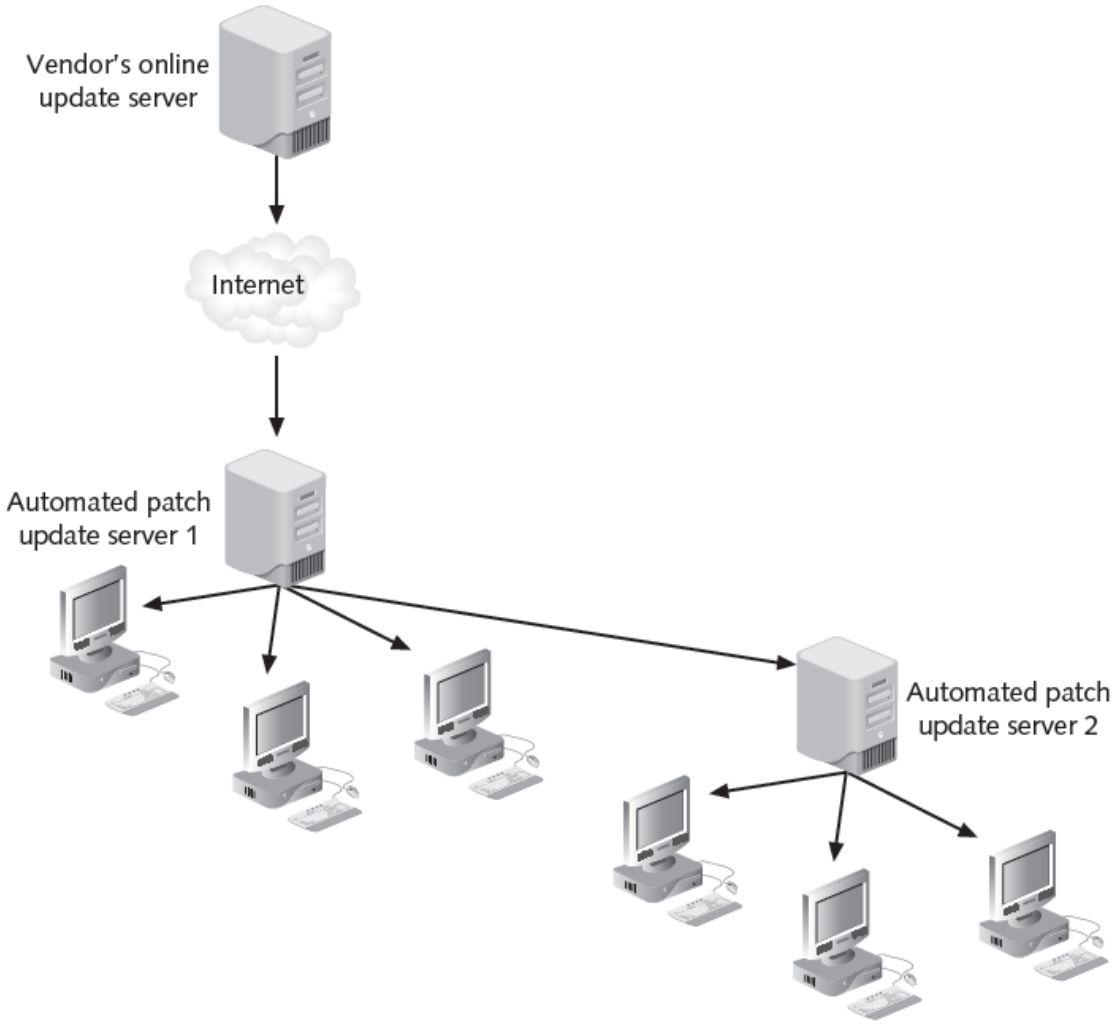

Figure 5-8 Automated patch update service

Securing with Anti-Malware Software

- 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

Anti-Spam

- 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

Pop-up Blockers and Anti-Spyware

- 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 Firewalls

- 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
- Microsoft Windows 7 firewall
  - Three designations for networks: public, home, or work
  - Users can configure settings for each type separately

Monitoring System Logs

- Log: record of events that occur
- Log entries
  - Contain information related to a specific event
- Audit log can track user authentication attempts
- Access log can provide details about requests for specific files
- Monitoring system logs
  - Useful in determining how an attack occurred and whether successfully resisted

Monitoring System Logs (cont'd.)

- Logs that record all activity from network devices or programs:
  - Used in operations, general audits, and demonstrating regulatory compliance
- Logs for system security
  - Operating system logs
  - Security application logs

Monitoring System Logs (cont'd.)

- System event logs record:
  - Client requests and server responses
  - Usage information
  - Account information
  - Operational information
- Security application logs
  - Anti-virus software log
  - Automated patch update service log

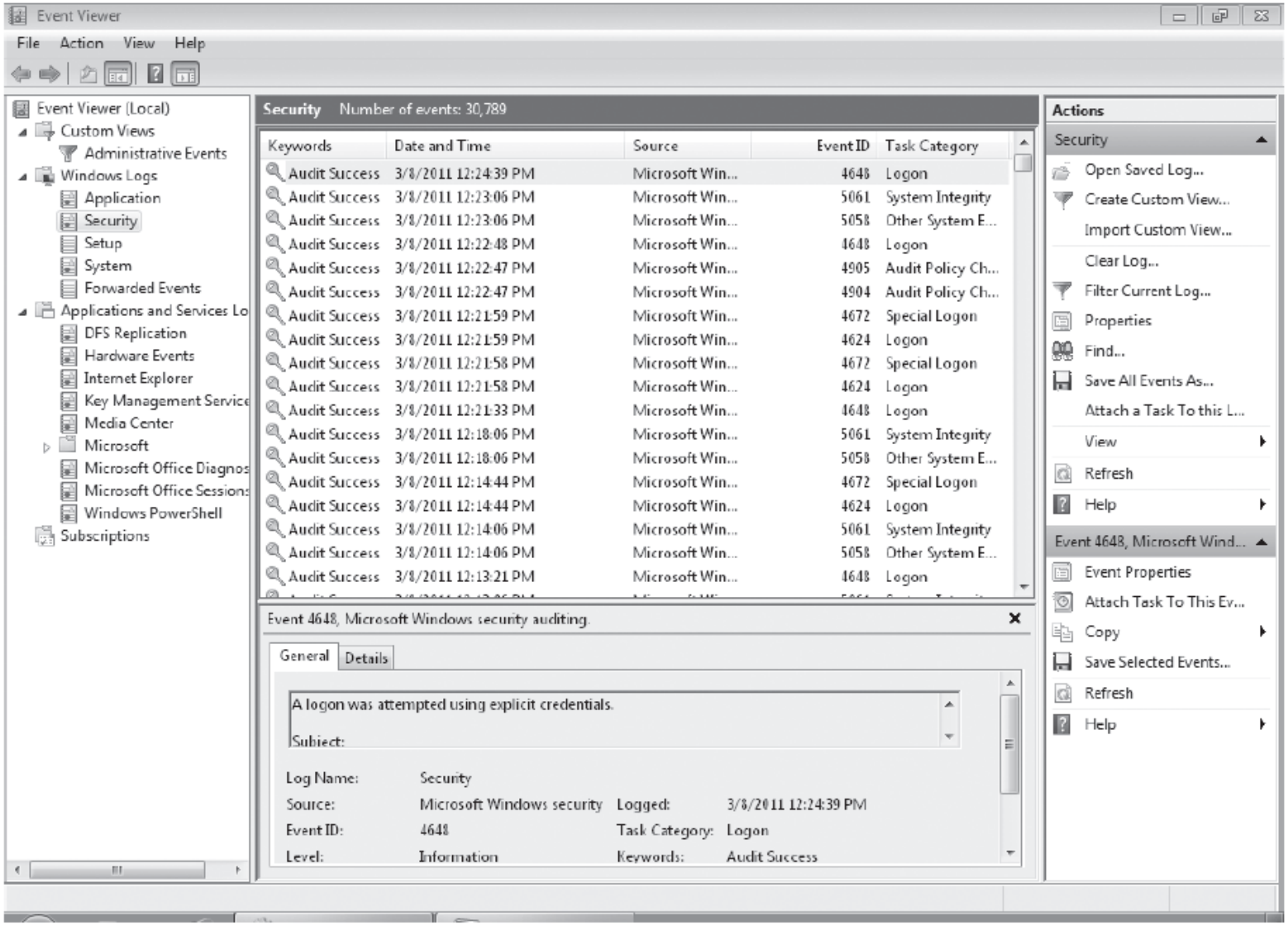

Figure 5-9 Microsoft system event and audit record log viewer

Monitoring System Logs (cont'd.)

- 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

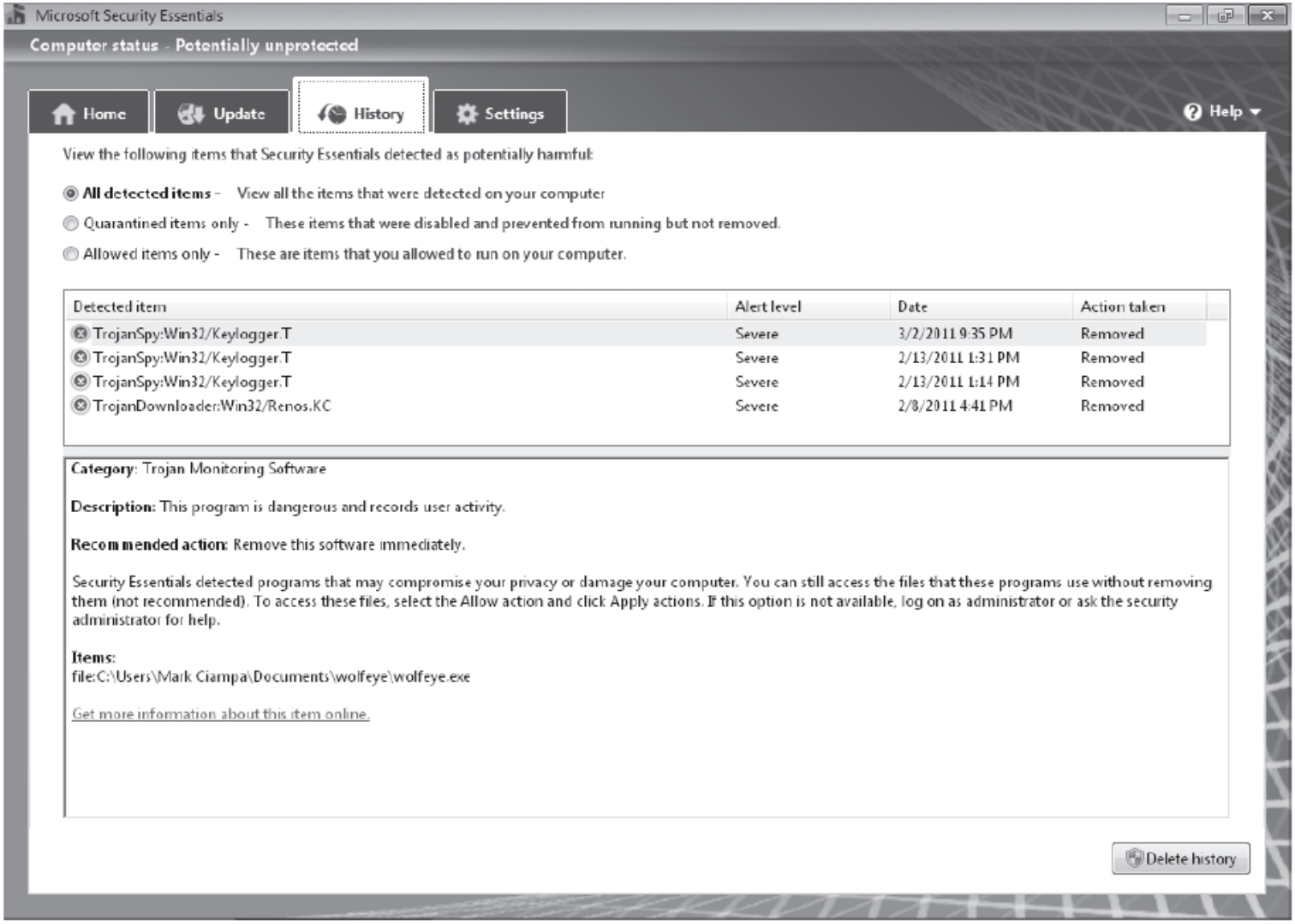

Figure 5-10 Anti-virus log

Application Security

- Aspects of securing applications
  - Application development security
  - Application hardening
  - Patch management

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

Application Development Security (cont'd.)

- Secure coding concepts
  - Coding standards increase applications' consistency, reliability, and security
  - Coding standards useful in code review process
- Errors (exceptions)
  - Faults that occur while application is running
  - Response should be based on the error
  - Improper handling can lead to application failure or insecurity

Application Development Security (cont'd.)

- Error handling practices to avoid
  - Failing to check return codes or handle exceptions
    - Or improperly checking them
  - Handling all return codes or exceptions in the same manner
  - Divulging potentially sensitive data in error information

Application Development Security (cont'd.)

- Verify user responses to the application
  - Could cause program to abort
  - Necessary to check for XSS, SQL, or XML injection attacks
- Input validation
  - Performed after data entered but before destination is known
  - Not possible to know which characters are potentially harmful

Application Development Security (cont'd.)

- Escaping (output encoding)
  - Preferred method for trapping user responses
  - Ensures characters are treated as data
    - Not relevant to the application
- Fuzz testing (fuzzing)
  - Software technique that deliberately provides invalid, unexpected, or random data inputs
  - Monitor to ensure all errors are trapped

Application Development Security (cont'd.)

- Application hardening
  - Intended to prevent exploiting vulnerabilities

Attack	Description	Defense
Executable files attack	Trick the vulnerable application into modifying or creating executable files on the system	Prevent the application from creating or modifying executable files for its proper function
System tampering	Use the vulnerable application to modify special sensitive areas of the operating system (Microsoft Windows Registry keys, system startup files, and so on.) and take advantage of those modifications	Do not allow applications to modify special areas of the OS
Process spawning control	Trick the vulnerable application into spawning executable files on the system	Taking away the process spawning ability from the application

Table 5-3 Attacks based on application vulnerabilities

Application Development Security (cont'd.)

- Patch management
  - Rare until recently
  - Users unaware of the existence of patches or where to acquire them
  - More application patch management systems are being developed today

Securing Data

- Work today involves electronic collaboration
  - Data must flow freely
  - Data security is important
- Data loss prevention
  - System of security tools used to recognize and identify critical data and ensure it is protected
  - Goal: protect data from unauthorized users

Securing Data (cont'd.)

- Data loss prevention typically examines:
  - Data in use (example: being printed)
  - Data in motion (being transmitted)
  - Data at rest (stored)
- Content inspection
  - Security analysis of transaction
  - Takes context into account

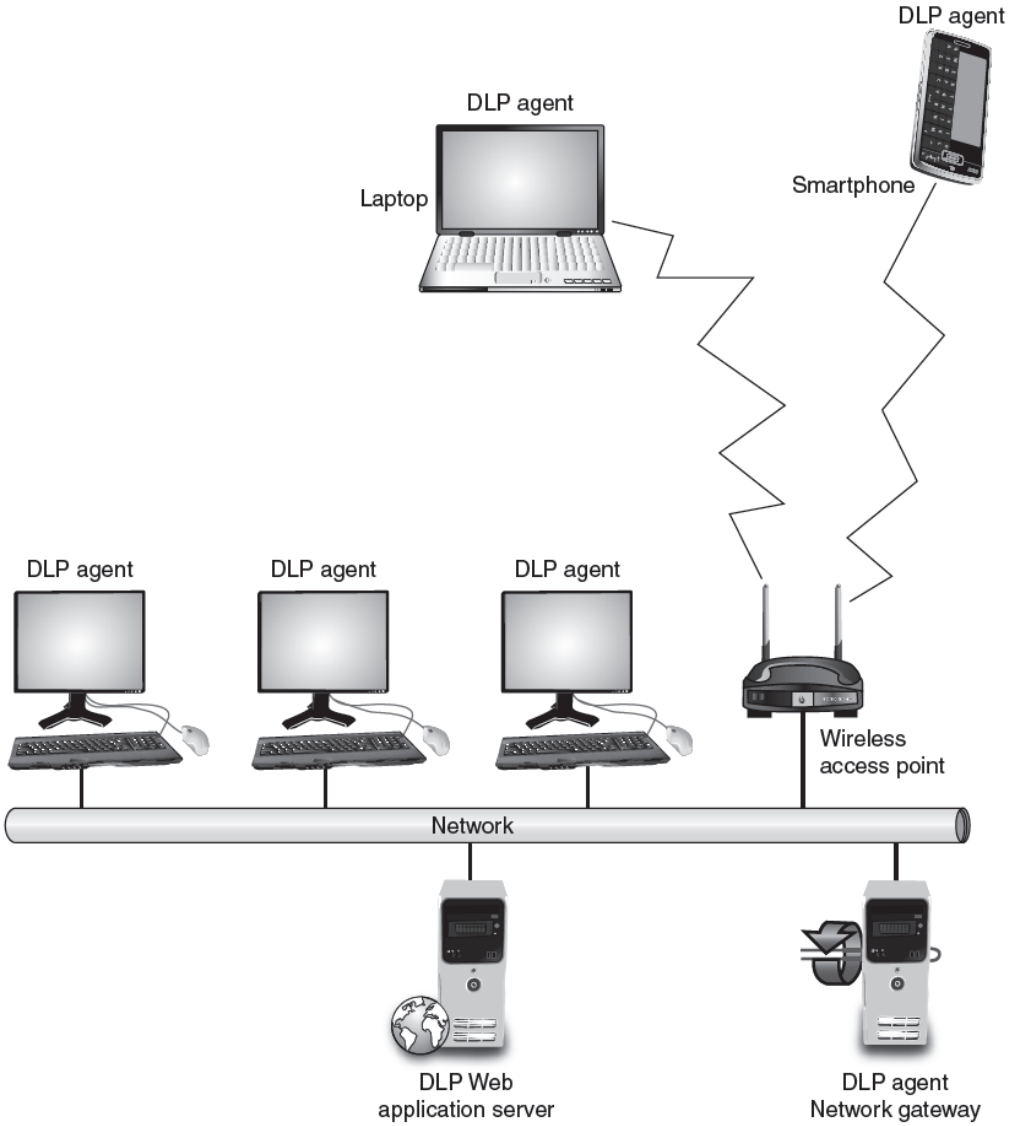

Figure 5-11 DLP architecture

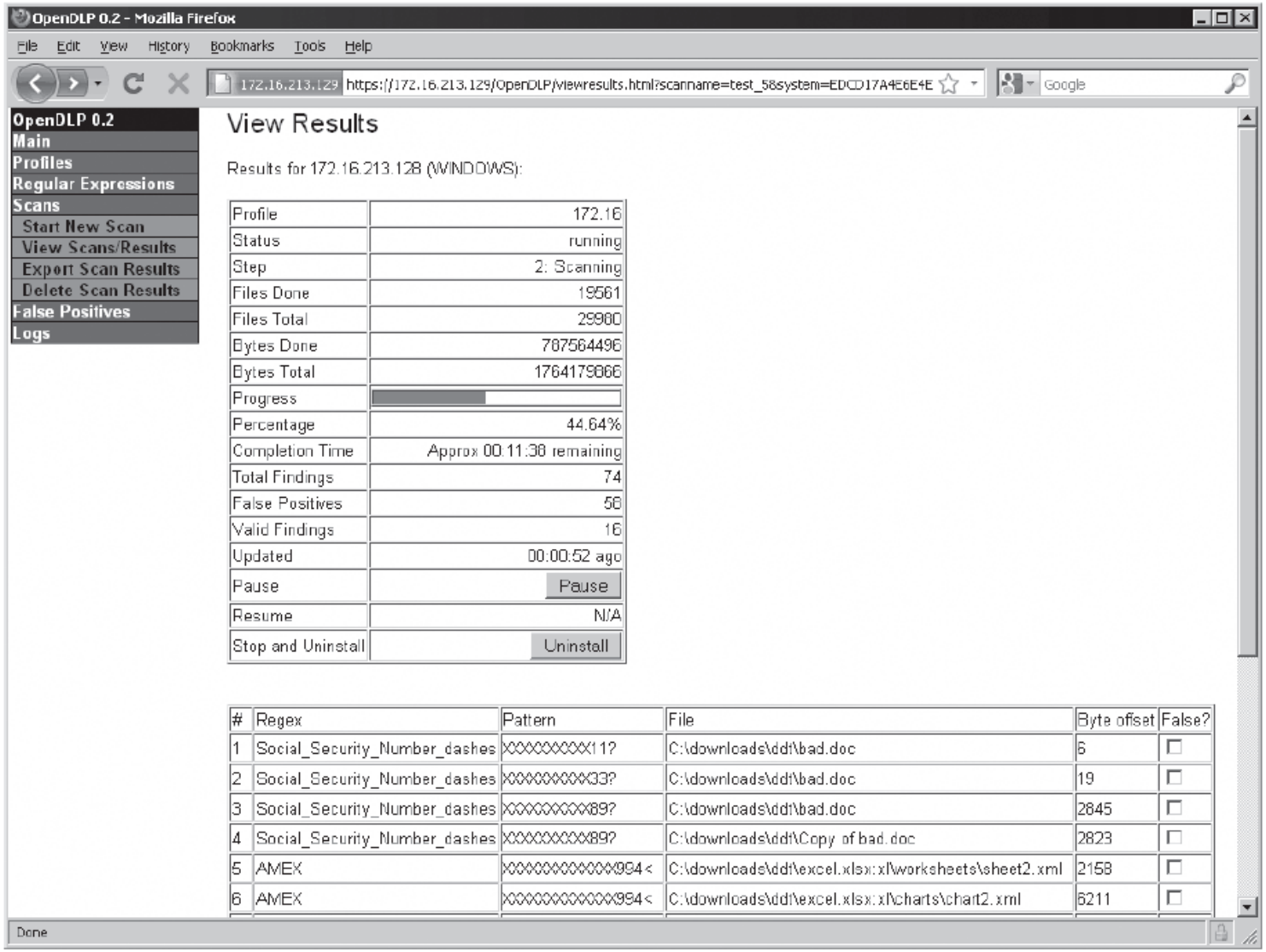

Figure 5-12 DLP report

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

Summary (cont'd.)

- 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