Information Security (CP3404)

Chapter 4 – Host, Application, and Data Security

Based on the Fifth Edition of:

M. Ciampa:. *CompTIA® Security + Guide to Network Security Fundamentals*

Department of Information Technology, College of Business, Law & Governance

Learning Objectives

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

Outline

Preface

- Basic security starts with protecting host, applications, and data
- Host, which can be either a server or a client on a network, runs applications that process, save, or transport data
- Securing the host involves:
  - Protecting the physical device itself
  - Securing the operating system (OS)
  - Using antimalware software

Securing the Host

Securing Devices

- Security control – Any device or process used to reduce risk
- There are two (2) levels of security controls:
  1. Administrative controls – Processes for developing and ensuring that policies and procedures are carried out
  2. Technical controls – Processes carried out or managed by devices

Subtypes of controls that can be either technical or administrative are called activity phase controls

Securing the Host

Activity Phase Controls

- Deterrent control – Attempts to discourage security violations before they occur
- Preventive controls – Works to prevent the threat from coming into contact with the vulnerability
- Detective control – Designed to identify any threat that has reached the system
- Compensating controls – Controls that provide alternative to normal controls that for some reason cannot be used
- Corrective controls – Controls intended to mitigate or lessen the damage caused by the incident

Securing the Host

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

Table 4-1 Activity phase controls

Securing the Host

Securing Devices (Cont.)

- Securing devices includes:
  - External Perimeter Defenses (e.g., Barriers, Guards, Motion detection devices)
  - Internal Physical Access Security (e.g., Hardware locks, Proximity readers, Access lists, Mantraps, Protected Distribution Systems)
  - Hardware security (e.g., Cable lock, Safe or Locking cabinet)

Securing the Host

External Perimeter Defenses – Barriers

- Different types of passive barriers can be used to restrict unwanted individuals or vehicles from entering secure area
- Fencing – Tall, permanent structure to keep out individuals for maintaining security
- Sign – Explains the area is restricted
- Lighting – Area can be viewed after dark
- Modern perimeter security consists of fence equipped with other deterrents (see Table 4-2)

Securing the Host

Technology	Description	Comments
Anticlimb 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).
Anticlimb collar	Spiked collar that extends horizontally for up to 3 feet (1 meter) from the pole to prevent anyone from climbing it; serves as both a practical and visual deterrent.	Used for protecting equipment mounted on poles like cameras or in areas where climbing a pole can be an easy point of access over a security fence.
Roller barrier	Independently rotating large cups (diameter of 5 inches or 115 millimeters) affixed to the top of a fence prevents 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.	Designed for high-security areas; can be painted to blend into fencing.

Table 4-2 Fencing deterrents

Securing the Host

External Perimeter Defenses – Barricade

- Barricade – Generally designed to block passage of traffic
- Most often used for directing large crowds or restricting vehicular traffic and are generally not designed to keep out individuals
- Barricades are usually not as tall as fences and can more easily be circumvented by climbing over them
- Temporary vehicular traffic barricades are frequently used in construction areas

Securing the Host

External Perimeter Defenses – Guards

- Guards – Whereas barriers act as passive devices, human guards are considered active security elements
- Unlike passive devices, guard can differentiate between an intruder and non-intruder (e.g., someone looking a lost pet)
- Can also make split-second decisions about when necessary to take appropriate action
- Some guards responsible for monitoring activity captured by video camera
- Video surveillance – Uses video cameras to transmit a signal
- Closed circuit television (CCTV) – Video signal to a specific and limited set of receivers

Securing the Host

External Perimeter Defenses – Motion detection

- Motion detection – Determining object's change in position in relation to surroundings
- Movement usually generates an audible alarm to warn guard of an intruder
- Can be performed using different methods (see Table 4-3)

Securing the Host

Method	Example
Visual	CCTV
Radio frequency	Radar, microwave
Vibration	Seismic sensors
Sound	Microphones
Magnetism	Magnetic sensors
Infrared	Passive and active infrared light sensors

Table 4-3 Motion detection methods

Securing the Host

Internal Physical Access Security

- External perimeter defenses designed to keep intruder from entering area
- Yet if intruder defeats external perimeter defenses, then must face internal physical access security (focused on interior)

Securing the Host

Internal Physical Access Security – Hardware Locks

- Door locks in commercial buildings different from residential door locks (See Figure 4-1)
- Deadbolt lock – Extends solid metal bar into door frame for extra security
- Much more difficult to defeat than keyed entry locks:
  - Cannot be broken from the outside like a preset lock
  - Extension of bar prevents credit card from being inserted to *jimmy* it open
  - Requires key be used to both open and lock door

Securing the Host

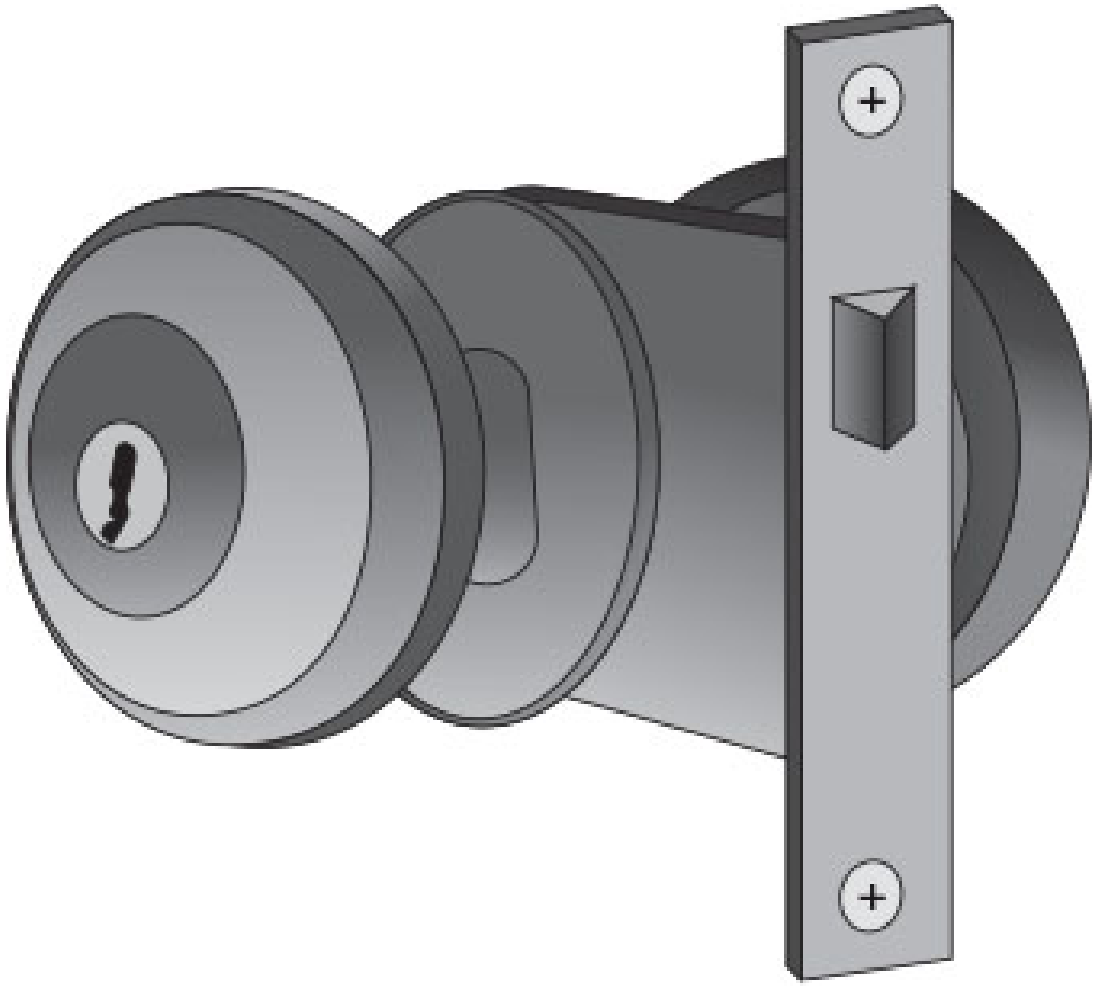

Figure 4-1 Residential keyed entry lock

Securing the Host

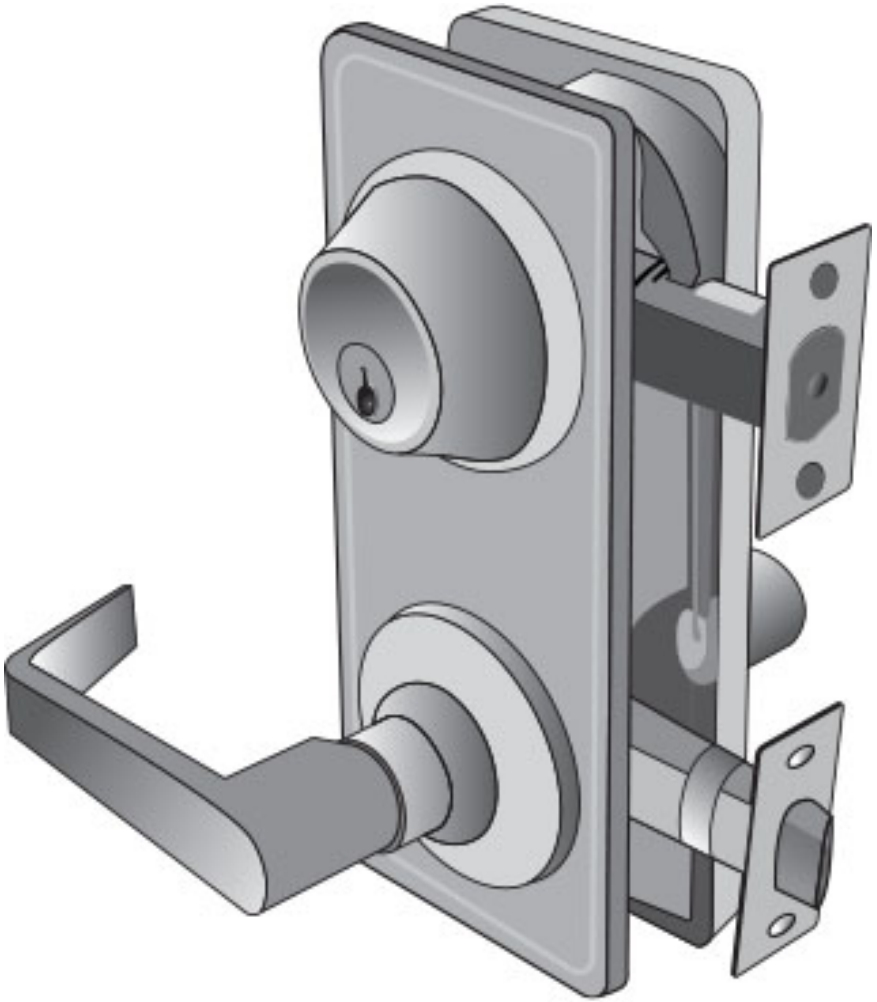

Figure 4-2 Deadbolt lock

Securing the Host

Internal Physical Access Security – Key Management

- Inspect all locks on regular basis to identify physical damage or signs of tampering
- Receive approval of supervisor or other appropriate person before issuing keys
- Keep track of keys issued, to whom, and date
- Require users to sign name when receiving keys
- Master keys not have any marks identifying them as masters
- Secure unused keys in locked safe
- Establish procedure to monitor use locks and keys

Securing the Host

Internal Physical Access Security – Cipher Lock

- 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 (see Figure 4-3)

Securing the Host

Figure 4-3 Cipher lock

Securing the Host

Internal Physical Access Security – Proximity Readers

- Instead of using key or entering a code to open door user can use an object (physical token) for identification
- ID badge – Originally contained photograph of bearer and were visually screened by security guards
- Later ID badges were magnetic stripe cards that were swiped or contained barcode identifier scanned to identify user
- New technologies not require ID badge be visually exposed
- Proximity reader – Device that receives the badge signal
- ID badges detected by proximity reader often fitted with tiny radio frequency identification (RFID) tags

Securing the Host

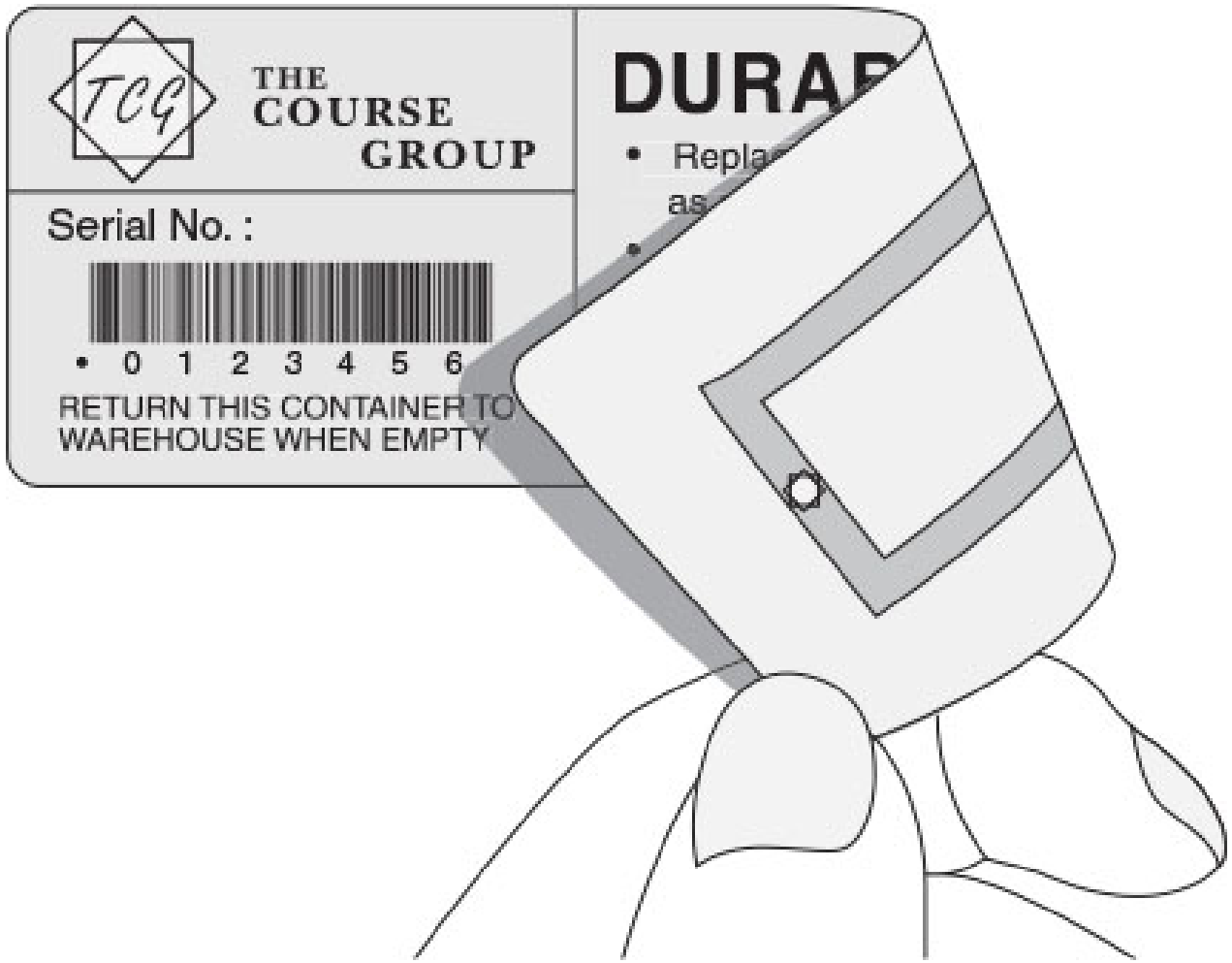

Figure 4-4 RFID tag

Securing the Host

Internal Physical Access Security – Access List & Mantraps

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

Securing the Host

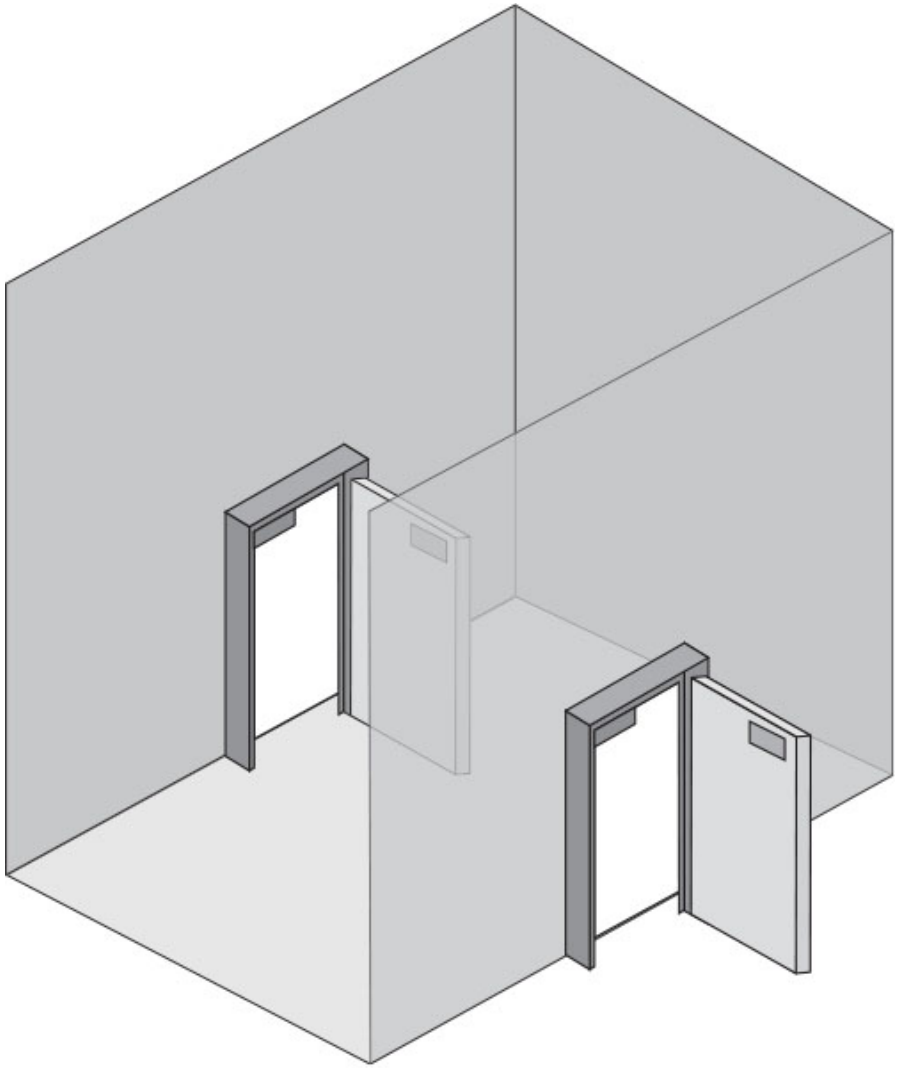

Figure 4-5 Mantrap

Securing the Host

Internal Physical Access Security – Protected Distribution Systems

- Protected distribution system (PDS) – System of cable conduits used to protect classified information being transmitted between two secure areas
- PDS is a standard created by U.S. Department of Defense (DOD) —See Figure 4-6
- Hardened carrier PDS – Connections between different segments are permanently sealed with welds or special sealants
- Alarmed carrier PDS – Carrier system deployed with specialized optical fibers that can sense acoustic vibrations and trigger alarm when intruder attempts to gain access

Securing the Host

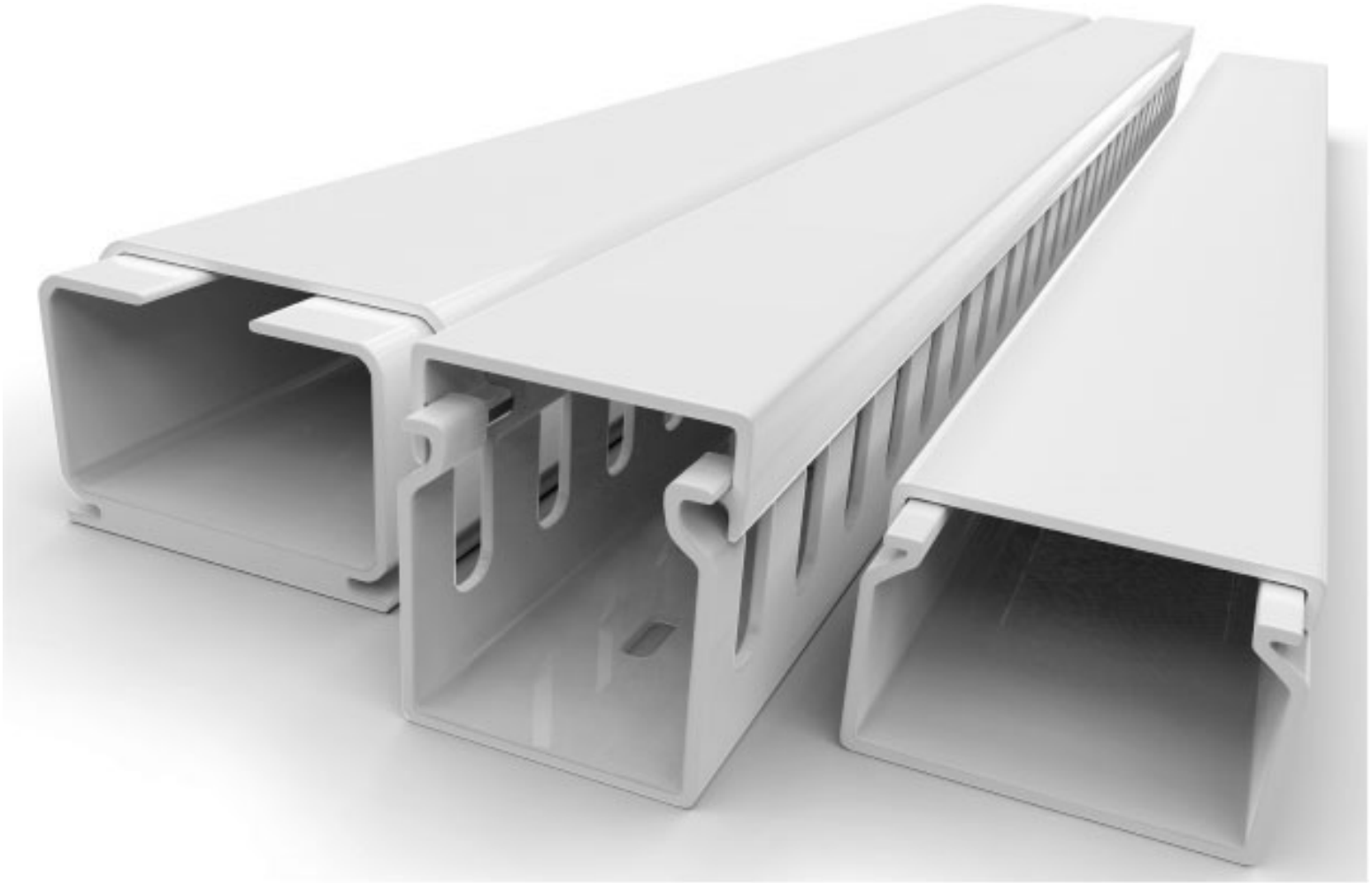

Figure 4-6 Cable conduits

Securing the Host

Hardware Security

- Hardware security – Physical security protecting host system hardware
- Portable devices have steel bracket security slot with Cable lock inserted into slot and secured to device (see Figure 4-7)
- Laptops may be placed in safe or locking cabinets
- Can be prewired for power and network connections to allow devices to charge while stored

Securing the Host

Figure 4-7 Cable lock

Securing the Operating System Software

Securing the Operating System Software

- In addition to protecting the hardware, the operating system software must be protected
- Two (2) approaches to securing operating system
  1. Security through configuration – Properly configure operating system after it has been installed to *fortify* it
  2. Security through design – Tighten security during initial design and coding of operating system.

Securing the Operating System Software

Security Through Configuration

- security of an OS can be enhanced through a five-step process:
  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

Securing the Operating System Software

Security Through Configuration

Develop the Security Policy (Step 1)

- A security policy is a document or a series of documents that clearly defines the defense mechanisms an organization will employ in order to keep information secure
- A security policy for an operating system may outline which security settings must be turned on and how they are to be configured

Securing the Operating System Software

Security Through Configuration

Perform Host Software Baselining (Step 2)

- A baseline is the standard or checklist against which system can be evaluated and audited for their level of security (security posture)
- A host baseline for the OS is configuration settings that will be used for each computer in the organization
- Whereas the security policy determines what must be protected, the baselines are the OS settings that impose how the policy will be enforced

Securing the Operating System Software

Security Through Configuration

Configure Operating System Security Settings (Step 3)

- Modern OSs have hundreds of different security settings that can be manipulated to conform to the baseline, e.g.:
  - Changing insecure default settings (such as allowing Guest accounts)
  - Eliminating unnecessary software, services, protocols (like removing games)
  - Enabling system security features (such as turning on the firewall)

Securing the Operating System Software

Security Through Configuration

Deploy and Manage Security Settings (Step 4)

- In Microsoft Windows a security template is a collection of security configuration settings
- A Microsoft security template can be deployed manually
- Group Policy provides centralized management and configuration of computers and remote users who are using specific Microsoft directory services known as Active Directory (AD)

Securing the Operating System Software

Security Through Configuration

Implement Patch Management (Step 5)

- Operating systems have increased in size and complexity (from 4000 lines in MS-DOS v1.0 to about 90 million lines in Windows 8.1)
- New attack tools have made secure functions vulnerable
- Security patch – General software update to cover discovered vulnerabilities
- Hotfix – Addresses specific customer situation
- Service pack – Accumulates patches, hotfixes, and additional features

Securing the Operating System Software

Security Through Configuration

Implement Patch Management (Step 5) –Cont.

- Modern operating systems can perform automatic updates
- OS interacts with vendor's online update service to automatically download and install patches (depending upon configuration option chosen)
- Patches can sometimes create new problems
- Vendor should thoroughly test before deploying

Securing the Operating System Software

Security Through Configuration

Implement Patch Management (Step 5) –Cont.

- Automated patch update service – Manage patches locally instead using vendor's online update service
- Advantages:
  - (i) Administrators can approve or decline updates for client systems, force updates to install by specific date, and obtain reports on what updates each computer needs.
  - (ii) Administrators can approve updates for *detection* only (allows them see which computers will require update without actually installing it)

Securing the Operating System Software

Security Through Configuration

Implement Patch Management (Step 5) –Cont. Advantages

(iii) Downloading patches from local server instead of using the vendor's online update service can save bandwidth and time because each computer does not have to connect to an external server

(iv) Specific types of updates that organization does not test (hotfixes) can be automatically installed whenever they become available

(v) Users cannot disable or circumvent updates as they can if computer configured to use vendor's online update service

Securing the Operating System Software

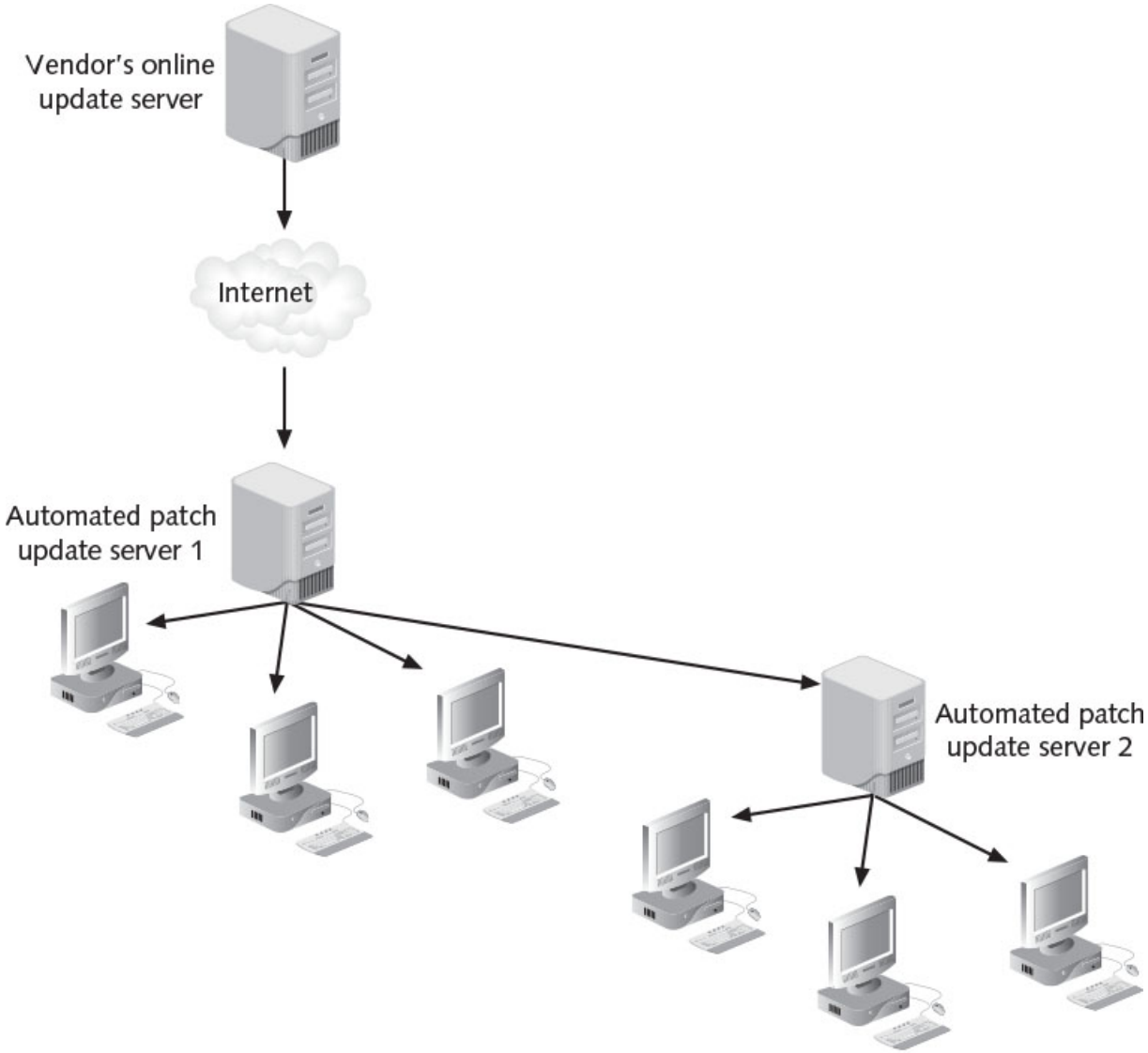

Figure 4-8 Automated patch update service

Securing the Operating System Software

Security Through Design

- Other techniques used instead of managing different security options on an operating system that has already been deployed
- OS hardening – Necessary to tighten security during design and coding of OS (see Table 4-4)
- Trusted OS – Operating system that has been designed through OS hardening

Securing the Operating System Software

Hardening technique	Explanation
Least privilege	Remove all *supervisor* or *administrator* accounts that can bypass security settings and instead split privileges into smaller units to provide the least-privileged unit to a user or process.
Reduce capabilities	Significantly restrict what resources can be accessed and by whom.
Read-only file system	Important operating system files cannot be changed.
Kernel pruning	Remove all unnecessary features that may compromise an operating system.

Table 4-4 OS hardening techniques

Securing the Operating System Software

Security Through Antimalware

- Operating system software continued to add security protections to core set of features
- Third-party antimalware software packages can provide added security
- Antimalware software includes:
  - Antivirus
  - Antispam
  - Popup blockers and antispyware
  - Host-based firewalls

Securing the Operating System Software

Antivirus

- Antivirus (AV) – Software that examines computer for infections
- Static analysis – Scan files by attempting to match known virus patterns against potentially infected files
- Host AV software contains virus scanning engine and database of known virus signatures
- By comparing virus signatures against potentially infected file (*string scanning*) match may indicate infected file

Securing the Operating System Software

Antivirus (cont.)

- Dynamic heuristic detection – Uses variety of techniques to spot characteristics of virus instead of attempting to make matches
- Code emulation – Virtual environment is created that simulates the central processing unit (CPU) and memory of the computer
- Any questionable program code is executed in virtual environment (no actual virus code is executed by the real CPU) to determine if is virus

Securing the Operating System Software

Antispam

- Spammers can distribute malware through email attachments or use for social engineering attacks
- Bayesian filtering – Analyzes every word in each email and determines how frequently a word occurs in *spam* pile compared to *not-spam* pile
- Create lists of senders:
  - Blacklist – Allow everything in unless it appears on the list
  - White list – List of approved senders

Securing the Operating System Software

Popup Blockers and Antispyware

- Pop-up – Small window appearing over web-page usually created by advertisers
- Pop-up blocker – Separate program as part of antispyware package incorporated within browser that allows user to limit or block most pop-ups
- Alert can be displayed in browser and gives user option to display pop-up

Securing the Operating System Software

Host-based Firewalls

- Firewall (packet filter) – Designed prevent malicious packets from entering/leaving
- May be hardware or software-based
- Host-based application firewall – Software firewall runs on local system
- Application running on a host computer may need send and receive transmissions that normally would be blocked by firewall
- Opening the firewall can be created by the user simply by approving application to transmit (called unblocking)

Quick Quiz

1. Controls that are intended to mitigate or lessen the damage caused by the incident are called _____.
   Answer:

Quick Quiz

1. Controls that are intended to mitigate or lessen the damage caused by the incident are called _____.
   Answer: corrective controls

Quick Quiz

1. Controls that are intended to mitigate or lessen the damage caused by the incident are called _____.
   Answer: corrective controls

2. _____ involves restricting access to the areas in which equipment is located.
   Answer:

Quick Quiz

1. Controls that are intended to mitigate or lessen the damage caused by the incident are called _____.
   Answer: corrective controls

2. _____ involves restricting access to the areas in which equipment is located.
   Answer: Physical security

Quick Quiz

1. Controls that are intended to mitigate or lessen the damage caused by the incident are called _____.
   Answer: corrective controls

2. _____ involves restricting access to the areas in which equipment is located.
   Answer: Physical security

3. A(n) _____ device monitors and controls two interlocking doors to a small room.
   Answer:

Quick Quiz

1. Controls that are intended to mitigate or lessen the damage caused by the incident are called _____.
   Answer: corrective controls

2. _____ involves restricting access to the areas in which equipment is located.
   Answer: Physical security

3. A(n) _____ device monitors and controls two interlocking doors to a small room.
   Answer: mantrap

Quick Quiz

1. Controls that are intended to mitigate or lessen the damage caused by the incident are called _____.
   Answer: corrective controls

2. _____ involves restricting access to the areas in which equipment is located.
   Answer: Physical security

3. A(n) _____ device monitors and controls two interlocking doors to a small room.
   Answer: mantrap

4. A(n) _____ is designed to prevent malicious network packets from entering or leaving computers or networks.
   Answer:

Quick Quiz

1. Controls that are intended to mitigate or lessen the damage caused by the incident are called _____.
   Answer: corrective controls

2. _____ involves restricting access to the areas in which equipment is located.
   Answer: Physical security

3. A(n) _____ device monitors and controls two interlocking doors to a small room.
   Answer: mantrap

4. A(n) _____ is designed to prevent malicious network packets from entering or leaving computers or networks.
   Answer: firewall

Quick Quiz

5. Most portable devices, and some computer monitors, have a special steel bracket security slot built into the case, which can be used in conjunction with a:
   (a) U-lock
   (b) safe lock
   (c) shield lock
   (d) cable lock

   Answer:

Quick Quiz

5. Most portable devices, and some computer monitors, have a special steel bracket security slot built into the case, which can be used in conjunction with a:
   (a) U-lock
   (b) safe lock
   (c) shield lock
   (d) cable lock

   Answer: (d)

Quick Quiz

5. Most portable devices, and some computer monitors, have a special steel bracket security slot built into the case, which can be used in conjunction with a:
   (a) U-lock
   (b) safe lock
   (c) shield lock
   (d) cable lock

   Answer: (d)

6. A(n) _____ is a document or series of documents that clearly defines the defense mechanisms an organization will employ in order to keep information secure.

   Answer:

Quick Quiz

5. Most portable devices, and some computer monitors, have a special steel bracket security slot built into the case, which can be used in conjunction with a:
   (a) U-lock
   (b) safe lock
   (c) shield lock
   (d) cable lock

   Answer: (d)

6. A(n) _____ is a document or series of documents that clearly defines the defense mechanisms an organization will employ in order to keep information secure.
   Answer: security policy

Securing Static Environments

Securing Static Environments

- Static environment – Types of devices with microprocessors not designed to be updated
- Embedded system – Computer system with a dedicated function within a larger electrical or mechanical system
  - OS of embedded systems are often stripped-down versions of general-purpose operating systems and may contain many of the same vulnerabilities
- Smartphone – Includes an operating system that allows it to run third-party applications but operating systems have vulnerabilities that attackers can exploit

Securing Static Environments

Securing Static Environments (Cont.)

- Mainframe – Very large computing systems that have significant processing capabilities
- In-vehicle computer systems – Automobile functions that are controlled by microprocessors
- SCADA (supervisory control and data acquisition) – Large-scale industrial-control systems found in military installations, oil pipeline control systems, manufacturing environments, and nuclear power plants

Securing Static Environments

Method	Description
Network segmentation	Keep devices on their own network separated from the regular network.
Security layers	Build security in layers around the device.
Application firewalls	When feasible, install application firewalls on the device's operating system.
Manual updates	Provide a means for manual software updates when automated updates cannot be used.
Firmware version control	Develop a policy that keeps track of updates to firmware.
Control redundancy and diversity	Keep the operating system code as basic as possible to limit overlapping or unnecessary features.

Table 4-5 Static environment defense methods

Application Security

Application Security

- Along with securing the operating system software on hosts and in static environments, is equally need to protect applications that run on the devices
- Application security includes:
  - Application development security
  - Application hardening and patch management

Application Security

Application Development Security

- Security for applications must be considered through all phases of the software life cycle (i.e., design, developmenmt, testing, deployment, and maintenance)
- Application development security involves :
  - Application configuration baselines:
  - Secure coding concepts

Application Security

Application Configuration Baselines

- As with OS baseline, standard environment settings in application development can stablish a secure baseline
- Standard environment should include development system, build system, and test system
- Standardization itself must include system and network configurations

Application Security

Secure Coding Concepts

- Coding standards increase applications' consistency, reliability, and security
- Wrapper functions – A substitute for a regular function that is used in testing
- Secure coding concepts include proper error and exception handling and input validation
- Errors (exceptions) – Faults that occur while application is running

  Fuzz testing (fuzzing) – Software testing technique that deliberately provides invalid, unexpected, or random data as inputs to computer program

Application Security

Secure Coding Concepts

Input Validation

- Verify user responses to application:
  - Could cause program to abort
  - Necessary to check for XSS, SQL, or XML injection attacks
  - Cross-site request forgery (XSRF) – Attack uses the user's web browser settings to impersonate the user
- Input validation – Verifies a user's input to an application and is performed after data entered but before destination is known (i.e., suitable for handling trusted data, rather than injection attacks)

Application Security

Secure Coding Concepts

Input Validation

- Instead of input validation, more drastic approach to preventing SQL injection attacks is avoid using SQL relational databases altogether
- NoSQL – New nonrelational databases that are better tuned for accessing large data sets
- NoSQL databases vs. SQL database – Argument over which database technology is better

Application Security

Application Hardening and Patch Management

- Application hardening is intended to prevent attackers from exploiting vulnerabilities in software applications (See Table 4-6)
- Application 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

Application Security

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, etc.) 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.	Take away the process spawning ability from the application.

Table 4-6 Attacks based on application vulnerabilities

Securing Data

Securing Data

- Work today involves electronic collaboration, so data must flow freely but securely
- Data loss prevention (DLP) – System of security tools used to recognize and identify critical data and ensure it is protected
- DLP examines data in any of its three (3) states:
  1. Data in-use – Data actions being performed by *endpoint devices*
  2. Data in-transit – Actions that transmit the data across a network
  3. Data at-rest – Stored on electronic media

Securing Data

DLP (also called Data Leak Prevention) Techniques

- Content inspection – Security analysis of transaction and takes context into account
- DLP systems also can use *index matching*:
  - Documents identified as needing protection, such as the program source code for a new software application, are analyzed by DLP system
  - Complex computations are conducted based on analysis

Securing Data

DLP Sensors

- DLP network sensors – Installed on perimeter of network to protect data in-transit by monitoring all network traffic
- DLP storage sensors – Sensors on network storage devices are designed to protect data at-rest
- DLP agent sensors – Sensors are installed on each host device (desktop, laptop, tablet, etc.) and protect data in-use (see Figure 4-9)

When a policy violation is detected, different actions can then be taken (See Figure 4-10)

Securing Data

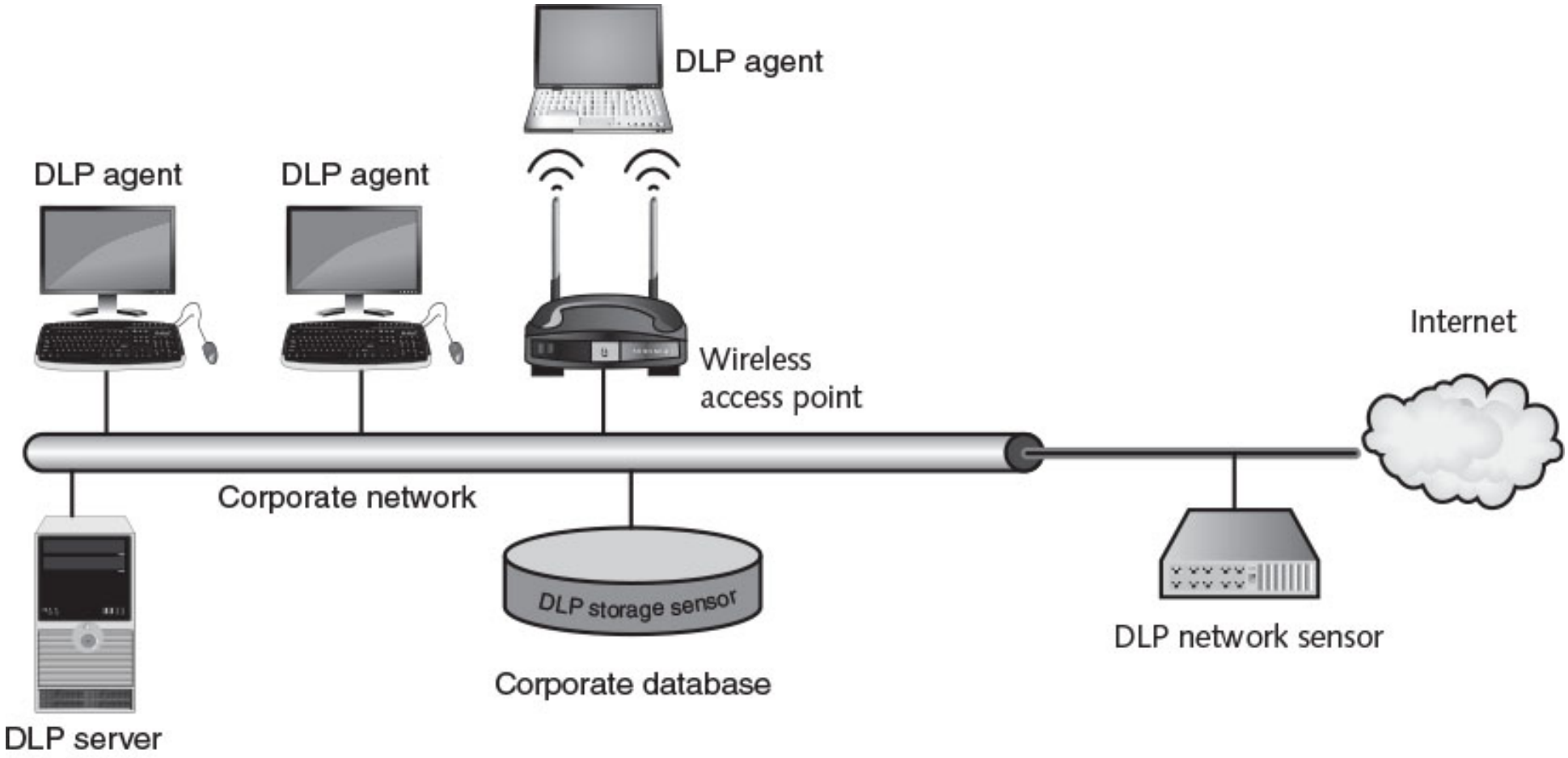

Figure 4-9 DLP architecture

Securing Data

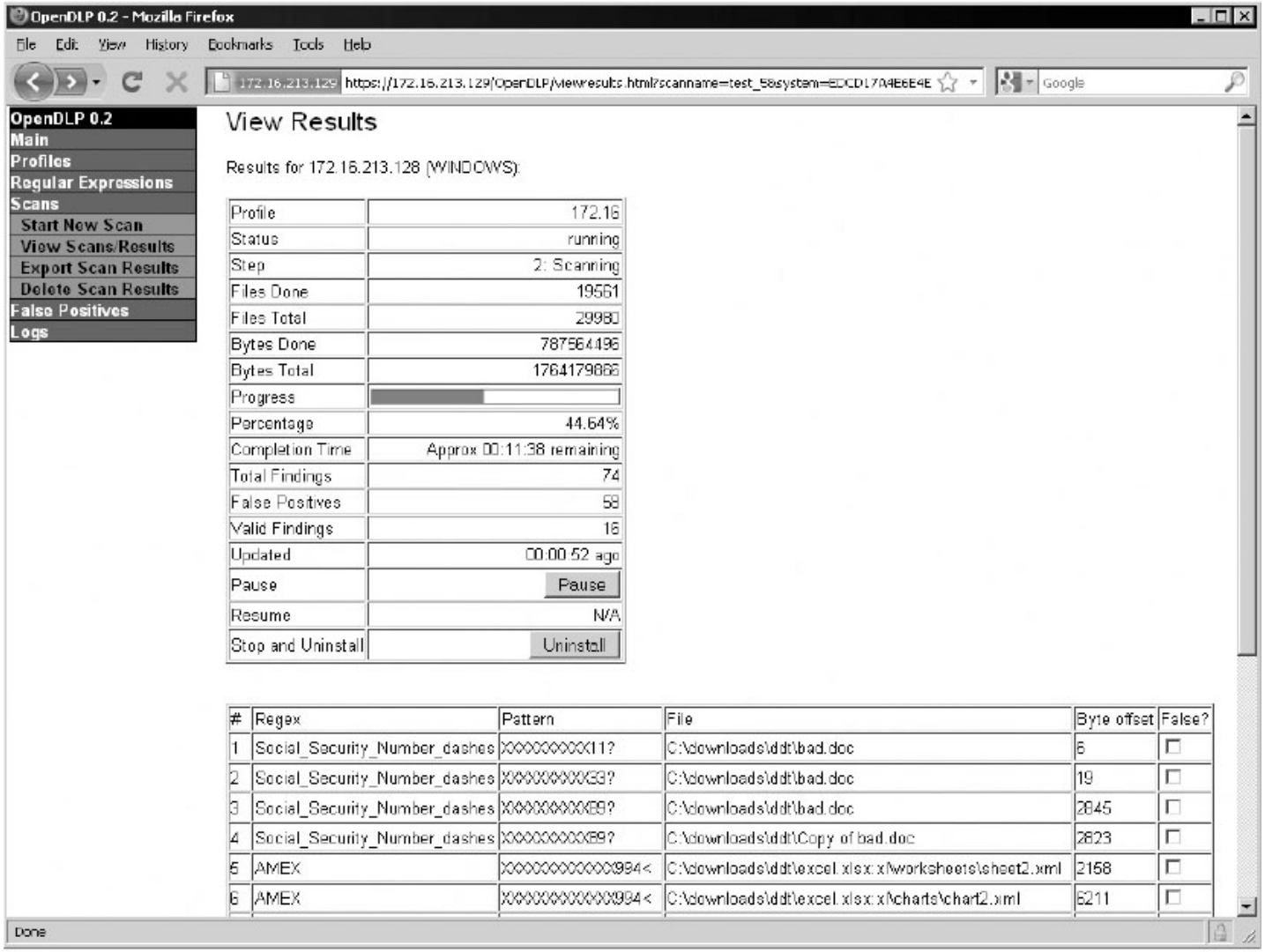

Figure 4-10 DLP report

Source: Google OpenDLP © Andrew Gavin

Quick Quiz

1. A(n) _____ is a computer system with a dedicated function within a larger electrical or mechanical system.
   Answer:

Quick Quiz

1. A(n) _____ is a computer system with a dedicated function within a larger electrical or mechanical system.
   Answer: embedded systems

Quick Quiz

1. A(n) _____ is a computer system with a dedicated function within a larger electrical or mechanical system.
   Answer: embedded systems

2. Application _____ is intended to prevent exploiting vulnerabilities in software applications.
   Answer:

Quick Quiz

1. A(n) _____ is a computer system with a dedicated function within a larger electrical or mechanical system.
   Answer: embedded systems

2. Application _____ is intended to prevent exploiting vulnerabilities in software applications.
   Answer: hardening

Quick Quiz

1. A(n) _____ is a computer system with a dedicated function within a larger electrical or mechanical system.
   Answer: embedded systems

2. Application _____ is intended to prevent exploiting vulnerabilities in software applications.
   Answer: hardening

3. _____ is defined as a security analysis of the transaction within its approved context.
   Answer:

Quick Quiz

1. A(n) _____ is a computer system with a dedicated function within a larger electrical or mechanical system.
   Answer: embedded systems

2. Application _____ is intended to prevent exploiting vulnerabilities in software applications.
   Answer: hardening

3. _____ is defined as a security analysis of the transaction within its approved context.
   Answer: Content inspection

Quick Quiz

1. A(n) _____ is a computer system with a dedicated function within a larger electrical or mechanical system.
   Answer: embedded systems

2. Application _____ is intended to prevent exploiting vulnerabilities in software applications.
   Answer: hardening

3. _____ is defined as a security analysis of the transaction within its approved context.
   Answer: Content inspection

4. When a policy violation is detected by the _____, it is reported back to the DLP server.
   Answer:

Quick Quiz

1. A(n) _____ is a computer system with a dedicated function within a larger electrical or mechanical system.
   Answer: embedded systems

2. Application _____ is intended to prevent exploiting vulnerabilities in software applications.
   Answer: hardening

3. _____ is defined as a security analysis of the transaction within its approved context.
   Answer: Content inspection

4. When a policy violation is detected by the _____, it is reported back to the DLP server.
   Answer: DLP agent