

UCS1704 – Management and Ethical Practices

UNIT – V
Access Control



Access Control

- The process by which resources or services are granted or denied on a computer system or network
- There are four standard access control models as well as specific practices used to enforce access control

Access Control Terminology

- **Identification**
 - A user accessing a computer system would present credentials or identification, such as a username
- **Authentication**
 - Checking the user's credentials to be sure that they are authentic and not fabricated, usually using a password
- **Authorization**
 - Granting permission to take the action
- A computer user is granted **access**
 - To only certain services or applications in order to perform their duties
- **Custodian**
 - The person who reviews security settings
 - Also called **Administrator**

Access Control Terminology (continued)

Action	Description	Scenario Example	Computer Process
Identification	Review of credentials	Delivery person shows employee badge	User enters username
Authentication	Validate credentials as genuine	Megan reads badge to determine it is real	User provides password
Authorization	Permission granted for admittance	Megan opens door to allow delivery person in	User authorized to log in
Access	Right given to access specific resources	Delivery person can only retrieve box by door	User allowed to access only specific data

Table 7-1 Basic steps in access control

Access Control Terminology (continued)

- Computer access control can be accomplished by one of three entities: hardware, software, or a policy
- Access control can take different forms depending on the resources that are being protected
- Other terminology is used to describe how computer systems impose access control:
 - **Object** – resource to be protected
 - **Subject** – user trying to access the object
 - **Operation** – action being attempted

Access Control Terminology (continued)

Role	Description	Duties	Example
Owner	Person responsible for the information	Determines the level of security needed for the data and delegates security duties as required	Determines that file SALARY.XLSX can be read only by department managers
Custodian	Individual to whom day-to-day actions have been assigned by the owner	Periodically reviews security settings and maintains records of access by end users	Sets and reviews security settings on SALARY.XLSX
End User	User who accesses information in the course of routine job responsibilities	Follows organization's security guidelines and does not attempt to circumvent security	Opens SALARY.XLSX

Table 7-2 Roles in access control

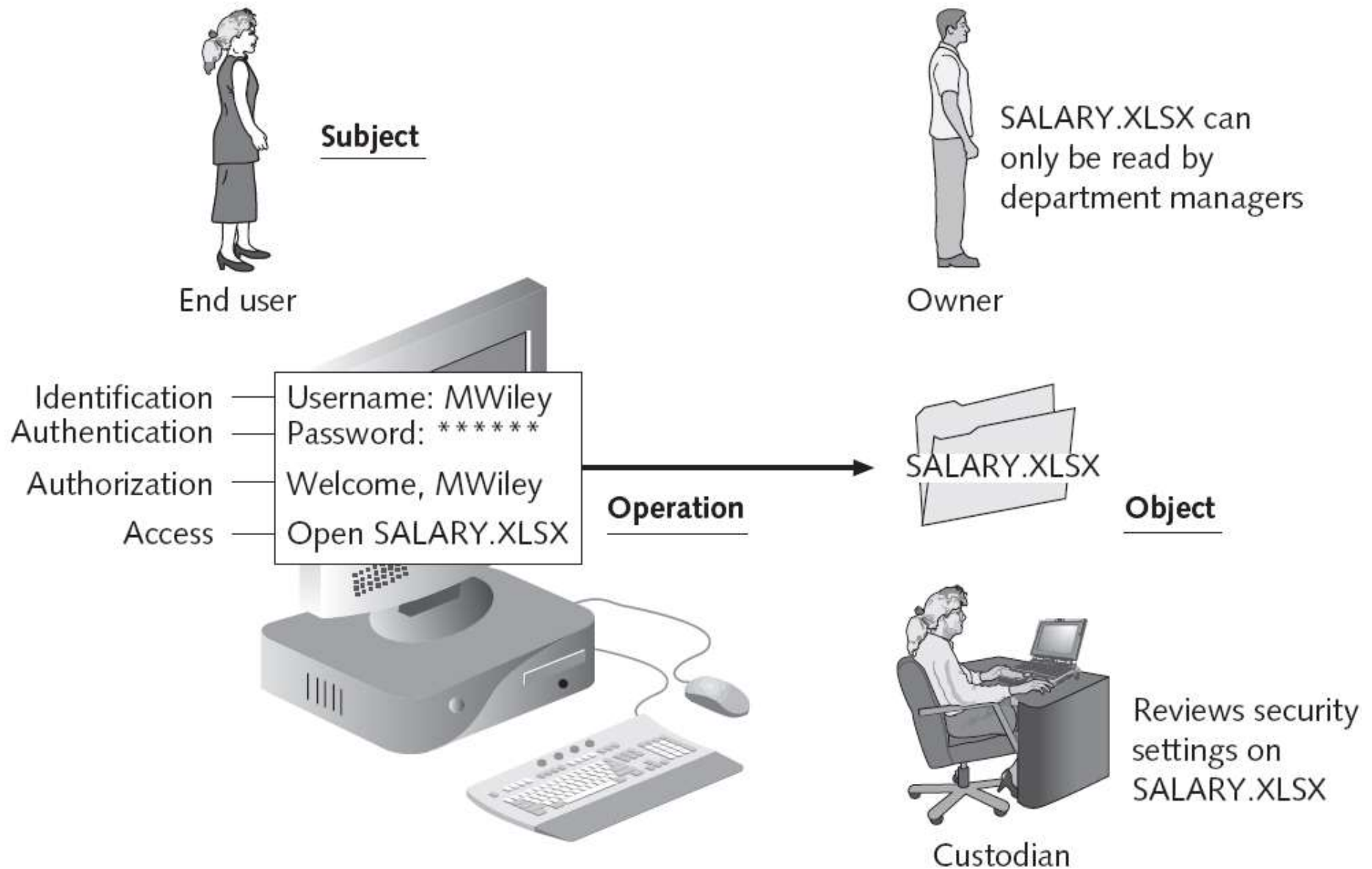


Figure 7-1 Access control process and terminology

Access Control Models

- Mandatory Access Control
- Discretionary Access Control
- Role-Based Access Control
- Rule-Based Access Control

Mandatory Access Control (MAC) model

- Most restrictive model—used by the military
- Objects and subjects are assigned access levels
- Unclassified, Classified, Secret, Top Secret
- The end user cannot implement, modify, or transfer any controls

Discretionary Access Control (DAC) model

- The least restrictive--used by Windows computers in small networks
- A subject has total control over any objects that he or she owns
- Along with the programs that are associated with those objects
- In the DAC model, a subject can also change the permissions for other subjects over objects

DAC Has Two Significant Weaknesses

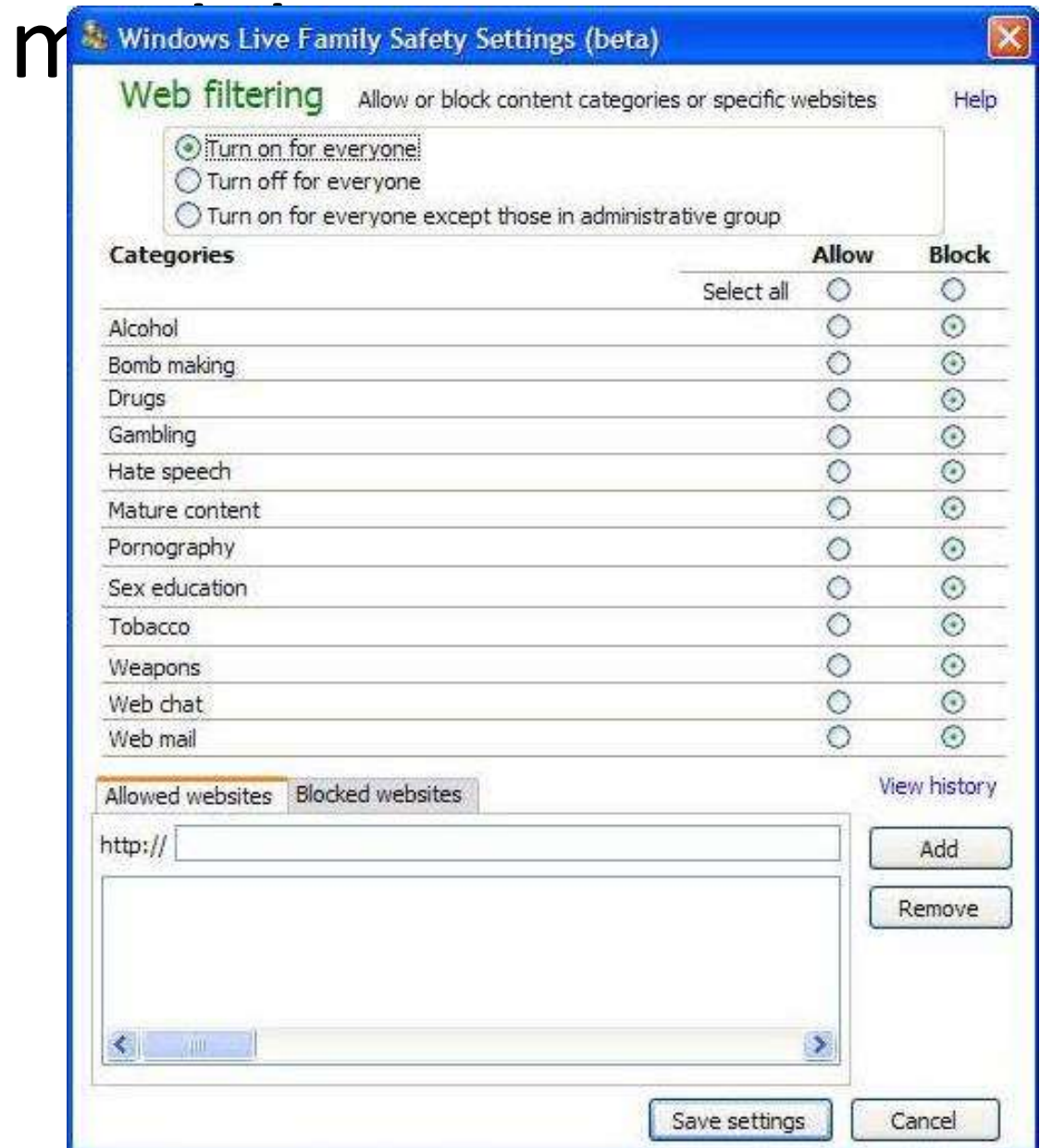
- It relies on the end-user subject to set the proper level of security
- A subject's permissions will be “inherited” by any programs that the subject executes

Role Based Access Control (RBAC) model

- Sometimes called **Non-Discretionary Access Control**
- Used in Windows corporate domains
- Considered a more “real world” approach than the other models
- Assigns permissions to particular roles in the organization, such as “Manager” and then assigns users to that role
- Objects are set to be a certain type, to which subjects with that particular role have access

Rule Based Access Control (RBAC)

- Also called the **Rule-Based Role-Based Access Control (RB-RBAC)** model or **automated provisioning**
- Controls access with **rules** defined by a custodian
 - Example: Windows



Access Control Models (continued)

Name	Restrictions	Description
Mandatory Access Control (MAC)	End user cannot set controls	Most restrictive model
Discretionary Access Control (DAC)	Subject has total control over objects	Least restrictive model
Role Based Access Control (RBAC)	Assigns permissions to particular roles in the organization and then users are assigned to roles	Considered a more "real world" approach
Rule Based Access Control (RBAC)	Dynamically assigns roles to subjects based on a set of rules defined by a custodian	Used for managing user access to one or more systems

Table 7-3 Access control models

Best Practices for Access Control

- **Separation of duties**
 - No one person should control money or other essential resources alone
 - Network administrators often have too much power and responsibility
- **Job rotation**
 - Individuals are periodically moved from one job responsibility to another

Best Practices for Access Control

- **Least privilege**
 - Each user should be given only the minimal amount of privileges necessary to perform his or her job function
- **Implicit deny**
 - If a condition is not explicitly met, access is denied
 - For example, Web filters typically block unrated sites

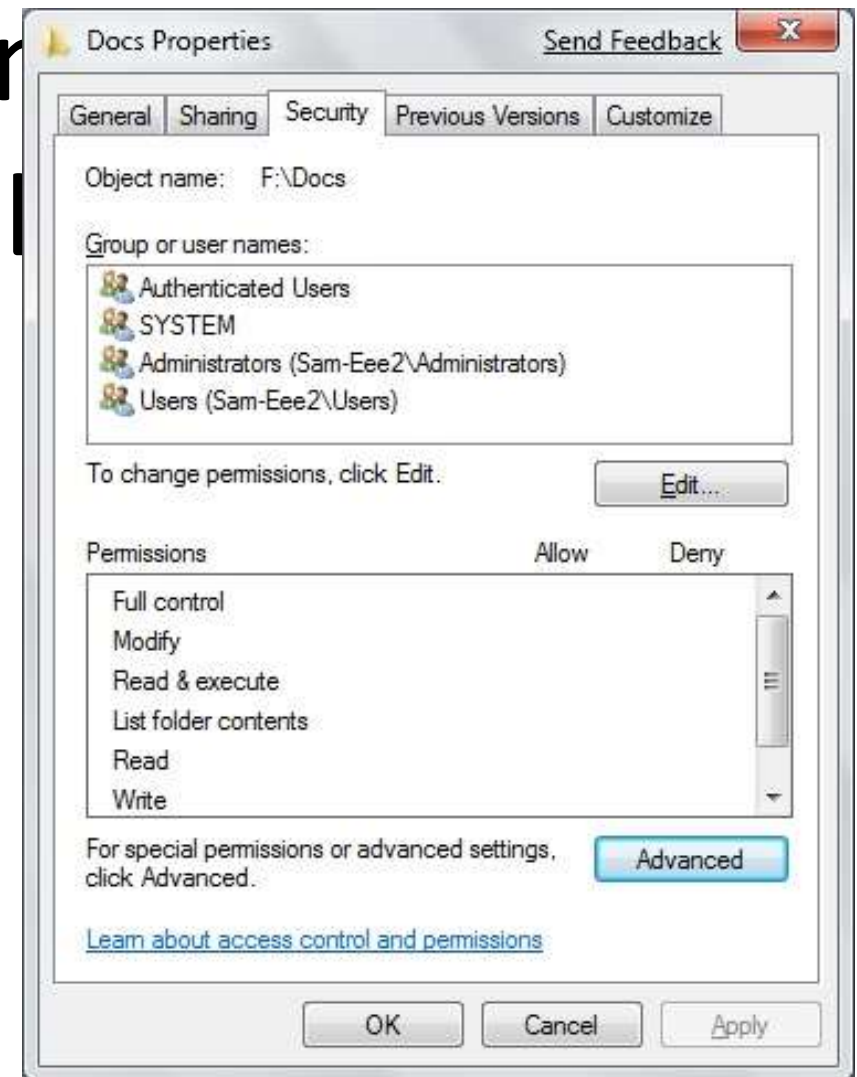
Logical Access Control Methods

Access Control Methods

- The methods to implement access control are divided into two broad categories
 - **Physical access control** and
 - **Logical access control**
- Logical access control includes
 - Access control lists (ACLs)
 - Group policies
 - Account restrictions
 - Passwords

Access Control List (ACL)

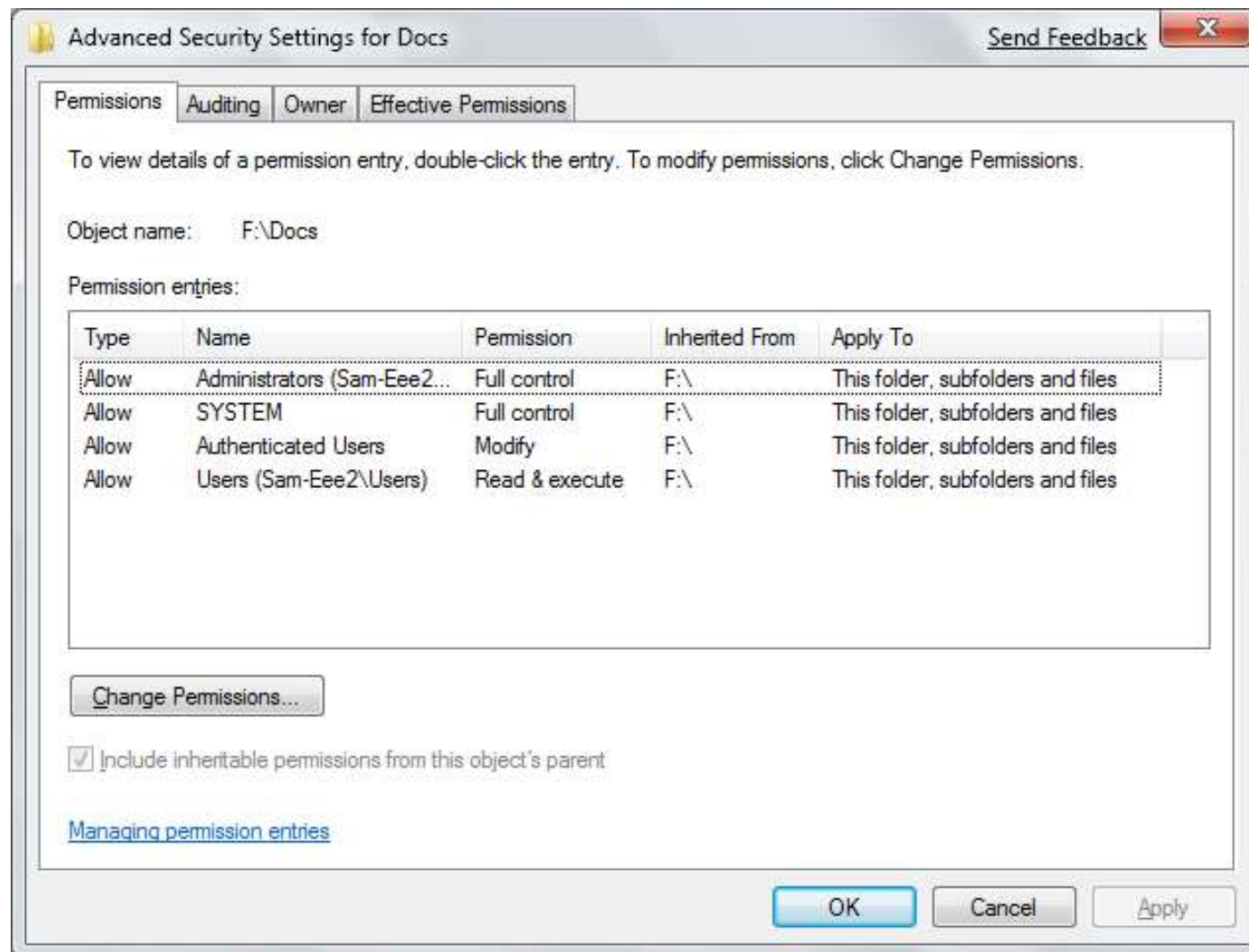
- A set of permissions attached to an object
- Specifies which subjects are allowed to access the object
- And what operations they can perform on it
- Every file and folder has an ACL
- **Access control entry (ACE)**
 - Each entry in the ACL table in the Microsoft Windows, Linux, and Mac OS X operating systems



Windows Access Control Entries (ACEs)

- In Windows, the ACE includes
 - Security identifier (SID) for the user or group
 - Access mask that specifies the access rights controlled by the ACE
 - A flag that indicates the type of ACE
 - A set of flags that determine whether objects can inherit permissions

Advanced Security Settings in Windows 7 Beta



Group Policy

- A Microsoft Windows feature that provides centralized management and configuration of computers and remote users
- Using the Microsoft directory services known as Active Directory (AD)
- Group Policy is used in corporate domains to restrict user actions that may pose a security risk
- Group Policy settings are stored in **Group Policy Objects (GPOs)**

Account Restrictions

- **Time of day restrictions**
 - Limit when a user can log on to a system
 - These restrictions can be set through a Group Policy
 - Can also be set on individual systems
- **Account expiration**
 - The process of setting a user's account to expire
 - Orphaned accounts are user accounts that remain active after an employee has left an organization
 - Can be controlled using account expiration

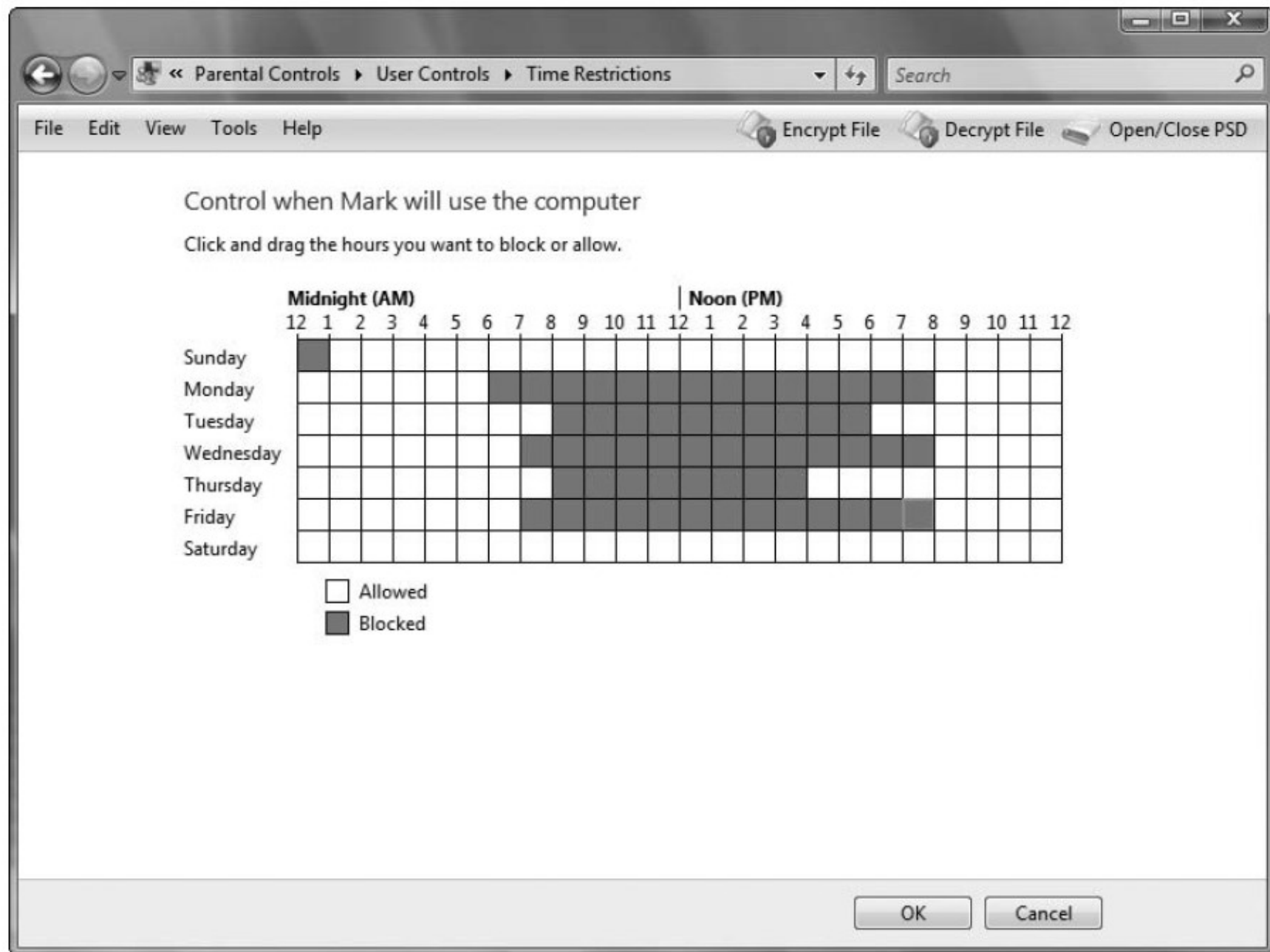


Figure 7-5 Windows Vista Parental Controls

LINKSYS®

A Division of Cisco Systems, Inc.

Firmware Version: v4.30.5

Access Restrictions

Wireless-G Broadband Router

WRT54GL

Setup

Wireless

Security

Access Restrictions

Applications & Gaming

Administration

Status

Internet Access

Internet Access

Internet Access Policy:

1 ()

Delete

Summary

Status:

☒ Enable
 ☐ Disable

Enter Policy Name:

PCs:

Edit List of PCs

☐ Deny
 ☒ Allow

Internet access during selected days and hours.

Days

☐ Everyday
 ☐ Sun
 ☒ Mon
 ☐ Tue
 ☒ Wed
 ☐ Thu
 ☒ Fri
 ☐ Sat

Times

☐ 24 Hours
 ☒ From:

9

:

45

AM

To:

5

:

00

PM

Internet Access Policy :

You may define up to 10 access policies. Click **Delete** to delete a policy or **Summary** to see a summary of the policy.

Status :

Enable or disable a policy.

Policy Name :

You may assign a name to your policy.

Policy Type :

Choose from Internet Access or Inbound Traffic.

More...

Days :

Choose the day of the week you would like your policy to be applied.

Times :

Enter the time of the day you would like your policy to apply.

Figure 7-6 Wireless access point restrictions

Passwords

- The most common logical access control
- Sometimes referred to as a logical token
- A secret combination of letters and numbers that only the user knows
- A password should never be written down
 - Must also be of a sufficient length and complexity so that an attacker cannot easily guess it (password paradox)

Passwords Myths

Myth	Explanation
<i>P4T9#6@</i> is better than <i>this_is_a_very_long_password</i> .	Even though the first password is a combination of letters, numbers, and symbols, it is too short and can easily be broken.
The best length for a password is 8 characters.	Because of how systems store passwords, the minimum recommended length is 15 characters.
Replacing letters with numbers, such as <i>J0hn_Sm1th</i> , is good.	Password-cracking programs can look for common words (John) as well as variations using numbers (J0hn).
Passwords cannot include spaces.	Many password programs can accept spaces as well as special characters.

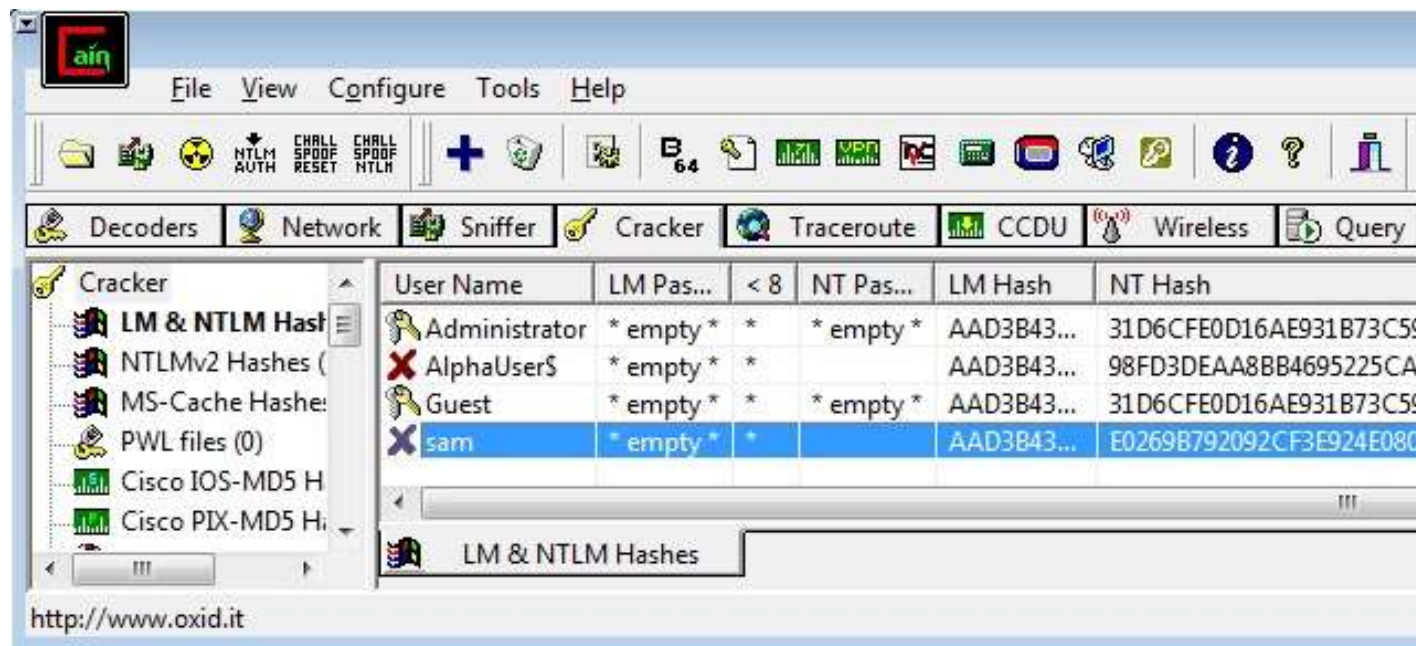
Table 7-4 Common password myths

Attacks on Passwords

- **Brute force attack**
 - Simply trying to guess a password through combining a random combination of characters
- Passwords typically are stored in an encrypted form called a “hash”
 - Attackers try to steal the file of hashed passwords and then break the hashed passwords offline

How to Get the Hashes

- Easy way: Just use Cain
- Cracker tab, right-click, "Add to List"



Attacks on Passwords

- **Dictionary attack**
 - Guess passwords from a dictionary
 - Works if the password is a known common password
- **Rainbow tables**
 - Make password attacks faster by creating a large pregenerated data set of hashes from nearly every possible password combination
 - Works well against Windows passwords because Microsoft doesn't use the **salting** technique when computing hashes

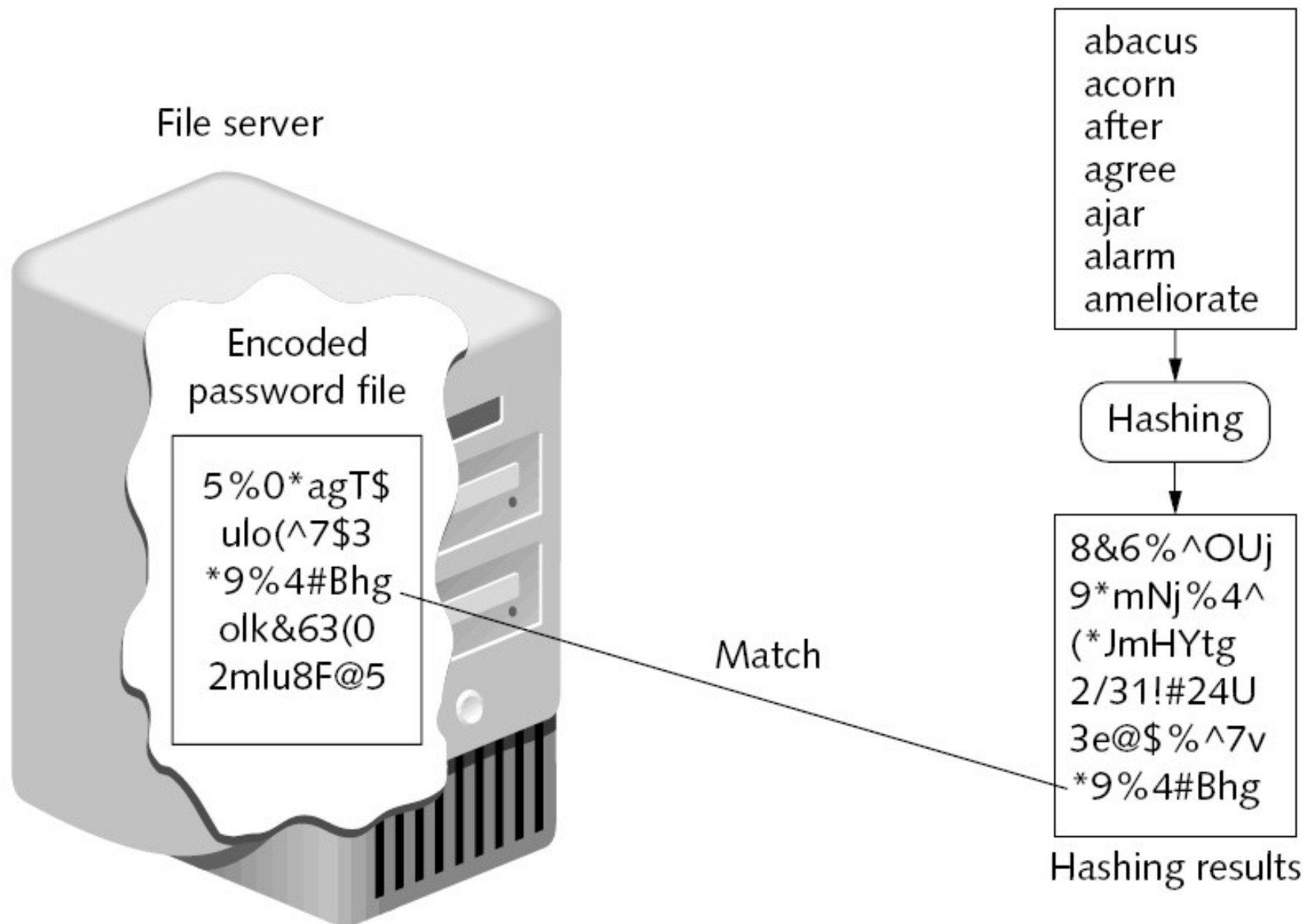


Figure 7-7 Dictionary attack

Rainbow Tables

- Generating a rainbow table requires a significant amount of time
- Rainbow table advantages
 - Can be used repeatedly for attacks on other passwords
 - Rainbow tables are much faster than dictionary attacks
 - The amount of time needed on the attacking machine is greatly reduced

Rainbow Table Attack

Password Characteristics	Example	Maximum time to break using brute force	Maximum time to break using rainbow tables
8-digit password of all letters	abcdefgh	1.6 days	28 minutes
9-digit password of letters and numbers (mixed case)	AbC4E8Gh	378 years	28 minutes
10-digit password of letters and numbers (mixed case)	Ab4C7EfGh2	23,481 years	28 minutes
14-digit password of letters, numbers, and symbols	1A2*3&def456G\$	6.09e + 12 years	28 minutes

Table 7-5 Times to break a hash

Passwords (continued)

- One reason for the success of rainbow tables is how older Microsoft Windows operating systems hash passwords
- A defense against breaking encrypted passwords with rainbow tables
 - Hashing algorithm should include a random sequence of bits as input along with the user-created password
- These random bits are known as a **salt**
 - Make brute force, dictionary, and rainbow table

No Salt!

- To make hashing stronger, add a random "Salt" to a password before hashing it
- Windows doesn't salt its hash!
- Two accounts with the same password hash to the same result, even in Windows 7 Beta!
- This makes it possible to speed up password cracking with precomputed Rainbow Tables

Demonstration

- Here are two accounts on a Windows 7 Beta machine with the password 'password'

User Name	LM Pas...	< 8	NT Pas...	LM Hash	NT Hash
✗ Testuser	* empty *	*		AAD3B43...	8846F7EAE8FB117AD06BDD830B7586C
✗ Testuser2	* empty *	*		AAD3B43...	8846F7EAE8FB117AD06BDD830B7586C

- This hash is from a different Windows 7 Beta machine

✗ Testuser3	* empty *	*		AAD3B43...	8846F7EAE8FB117AD06BDD830B7586C
-------------	-----------	---	--	------------	---------------------------------

Linux Salts its Hashes

```
student@student-desktop:~$ sudo useradd -d /home/testuser1 -m testuser1
[sudo] password for student:
student@student-desktop:~$ sudo passwd testuser1
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
student@student-desktop:~$ sudo useradd -d /home/testuser2 -m testuser2
student@student-desktop:~$ sudo passwd testuser2
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
student@student-desktop:~$ sudo tail -2 /etc/shadow
testuser1:$1$zW1NMALV$kX5/VdKPX3HFUjnf2Fv301:14132:0:99999:7:::
testuser2:$1$EHNCIoxU$0nQusuZW0233b3VfHhTMS0:14132:0:99999:7:::
```

Password Policy

- A strong password policy can provide several defenses against password attacks
- The first password policy is to create and use strong passwords
- One of the best defenses against rainbow tables is to prevent the attacker from capturing the password hashes
- A final defense is to use another program to help keep track of passwords

Domain Password Policy

- Setting password restrictions for a Windows domain can be accomplished through the Windows Domain password policy
- There are six common domain password policy settings, called password setting objects
 - Used to build a domain password policy

Attribute	Description	Recommended Setting
Enforce password history	Determines the number of unique new passwords a user must use before an old password can be reused (from 0 to 24).	24 new passwords
Maximum password age	Determines how many days a password can be used before the user is required to change it. The value of this setting can be between 0 and 999.	42 days
Minimum password age	Determines how many days a new password must be kept before the user can change it (from 0 to 999). This setting is designed to work with the Enforce password history setting so that users cannot quickly reset their passwords the required number of times, and then change back to their old passwords.	1 day
Minimum password length	Determines the minimum number of characters a password can have (0–28).	15 characters
Passwords must meet complexity requirements	Determines whether password complexity is enforced.	Enabled
Store passwords using reversible encryption	Provides support for applications that use protocols that require knowledge of the user's password for authentication purposes. Storing passwords using reversible encryption is essentially the same as storing plaintext versions of the passwords.	Disabled

Table 7-6 Password objects

Physical Access Control

Physical Access Control

- Physical access control primarily protects computer equipment
 - Designed to prevent unauthorized users from gaining physical access to equipment in order to use, steal, or vandalize it
- Physical access control includes computer security, door security, mantraps, video surveillance, and physical access logs

Physical Computer Security

- Physically securing network servers in an organization is essential
- **Rack-mounted servers**
 - 4.45 centimeters (1.75 inches) tall
 - Can be stacked with up to 50 other servers in a closely confined area
- **KVM (Keyboard, Video, Mouse) Switch**
 - Needed to connect to the servers
 - Can be password-protected

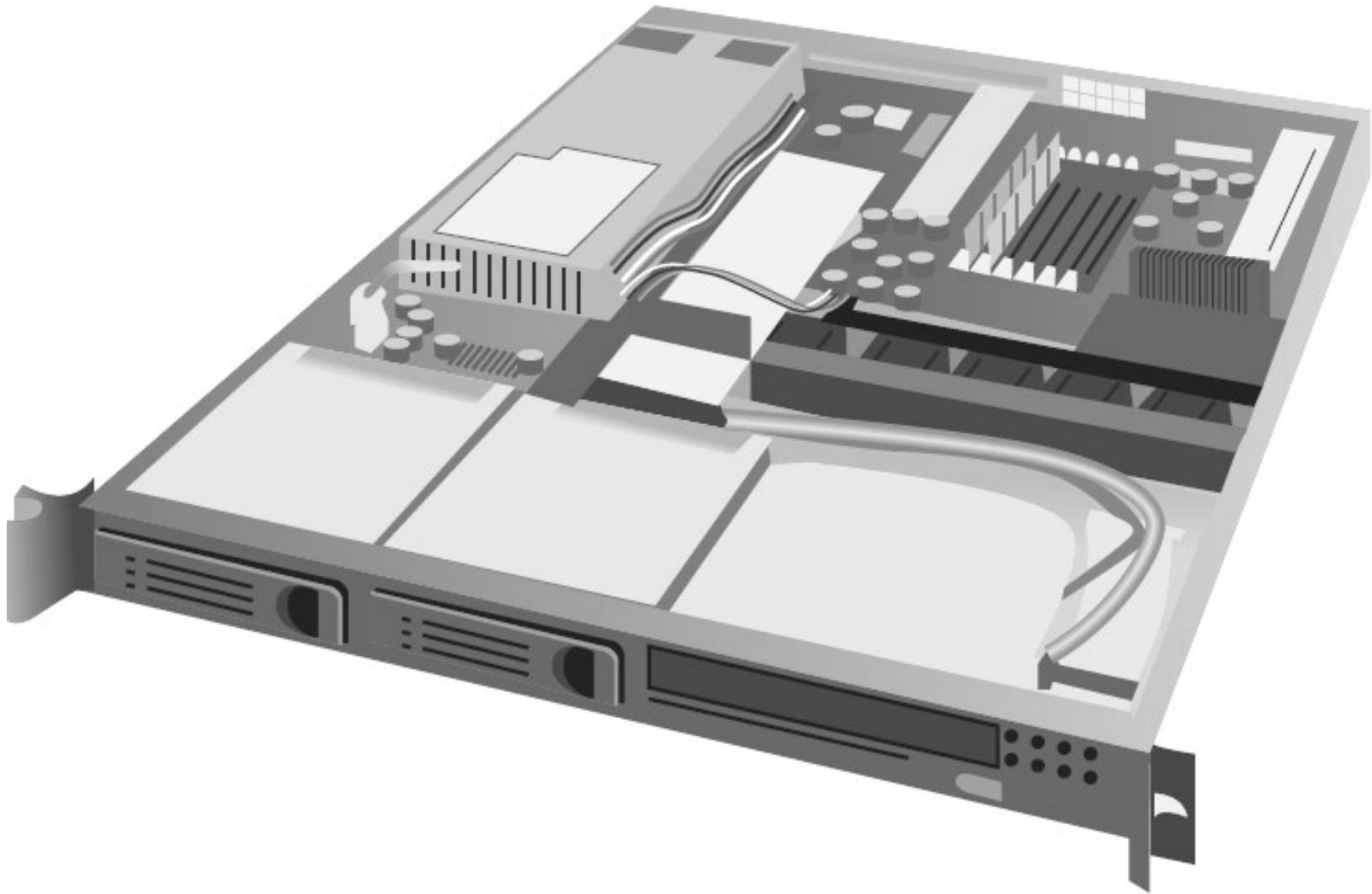


Figure 7-8 Rack-mounted server

KVM Switch

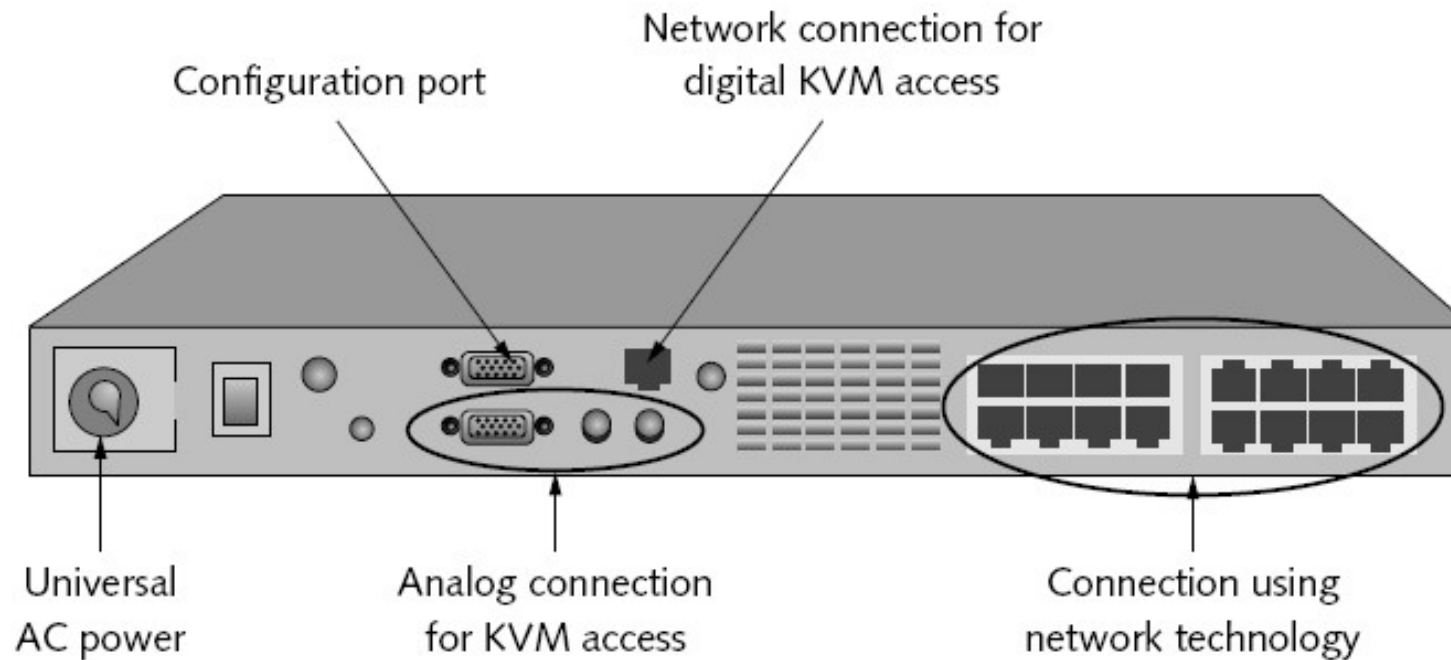
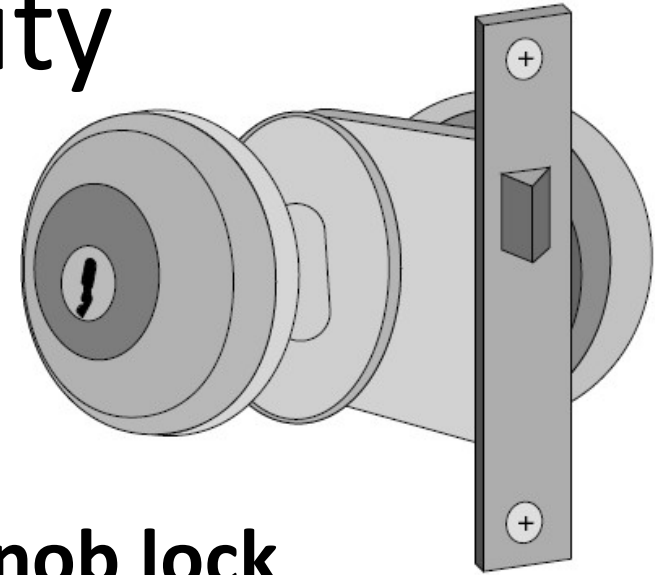


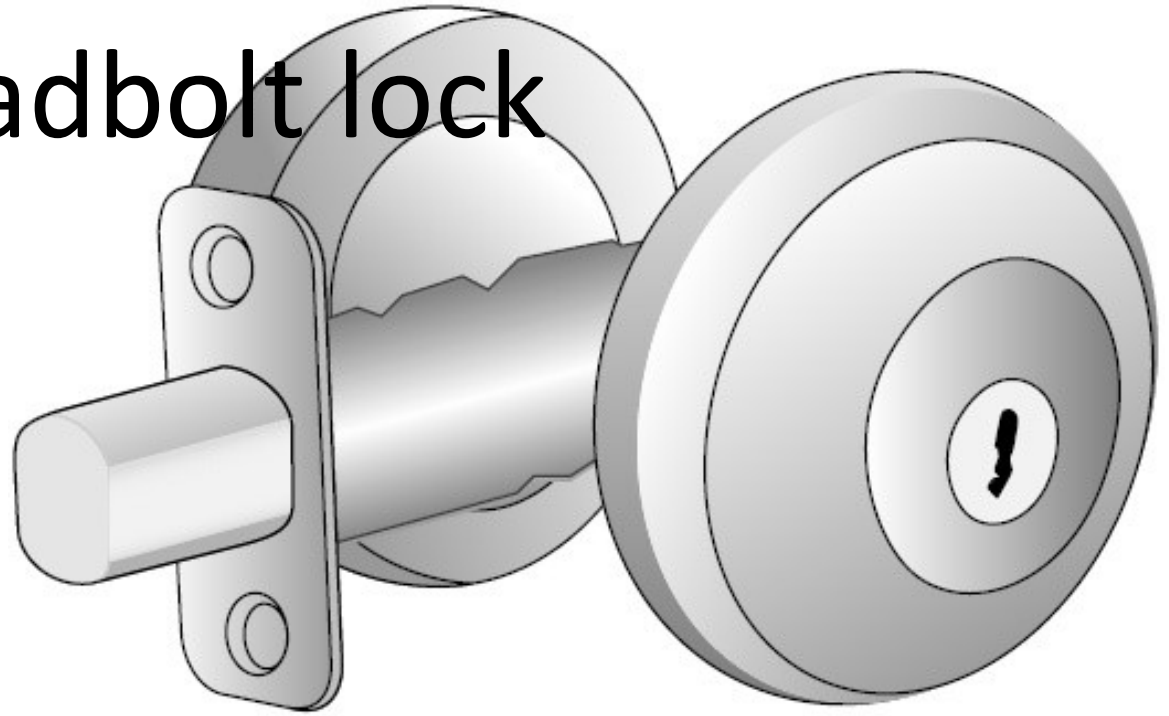
Figure 7-9 KVM switch

Door Security



- Hardware locks
 - **Preset lock**
 - Also known as the **key-in-knob lock**
 - The easiest to use because it requires only a key for unlocking the door from the outside
 - Automatically locks behind the person, unless it has been set to remain unlocked
 - Security provided by a preset lock is minimal

Deadbolt lock



- Extends a solid metal bar into the door frame
- Much more difficult to defeat than preset locks
- Requires that the key be used to both open

Lock Best Practices

- Change locks immediately upon loss or theft of keys
- Inspect all locks on a regular basis
- Issue keys only to authorized persons
- Keep records of who uses and turns in keys
- Keep track of keys issued, with their number and identification
- Master keys should not have any marks identifying them as masters

Lock Best Practices

- Secure unused keys in a locked safe
- Set up a procedure to monitor the use of all locks and keys and update the procedure as necessary
- When making duplicates of master keys, mark them “Do Not Duplicate,” and wipe out the manufacturer’s serial numbers to keep duplicates from being ordered

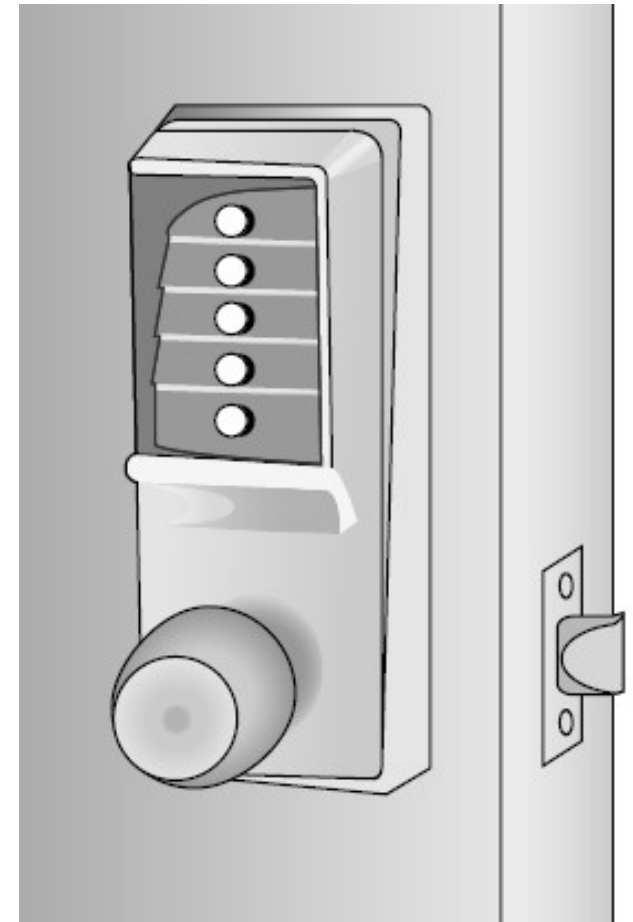
Lockpicking at DEFCON



- See links Ch 7e, 7f

Cipher Lock

- Combination locks that use buttons that must be pushed in the proper sequence to open the door
- Can be programmed to allow only the code of certain individuals to be valid on specific dates and times
- Cipher locks also keep a record of when the door was opened



Cipher Lock Disadvantages

- Basic models can cost several hundred dollars while advanced models can be even more expensive
- Users must be careful to conceal which buttons they push to avoid someone seeing or photographing the combination

Tailgate Sensor

- Uses infrared beams that are aimed across a doorway
- Can detect if a second person walks through the beam array immediately behind (“tailgates”) the first person
 - Without presenting credentials

Physical Tokens

- Objects to identify users
- **ID Badge**
 - The most common types of physical tokens
 - ID badges originally were visually screened by security guards
 - Today, ID badges can be fitted with tiny **radio frequency identification (RFID) tags**
 - Can be read by an RFID transceiver as the user walks through the door with the badge in her pocket

Door Security (continued)

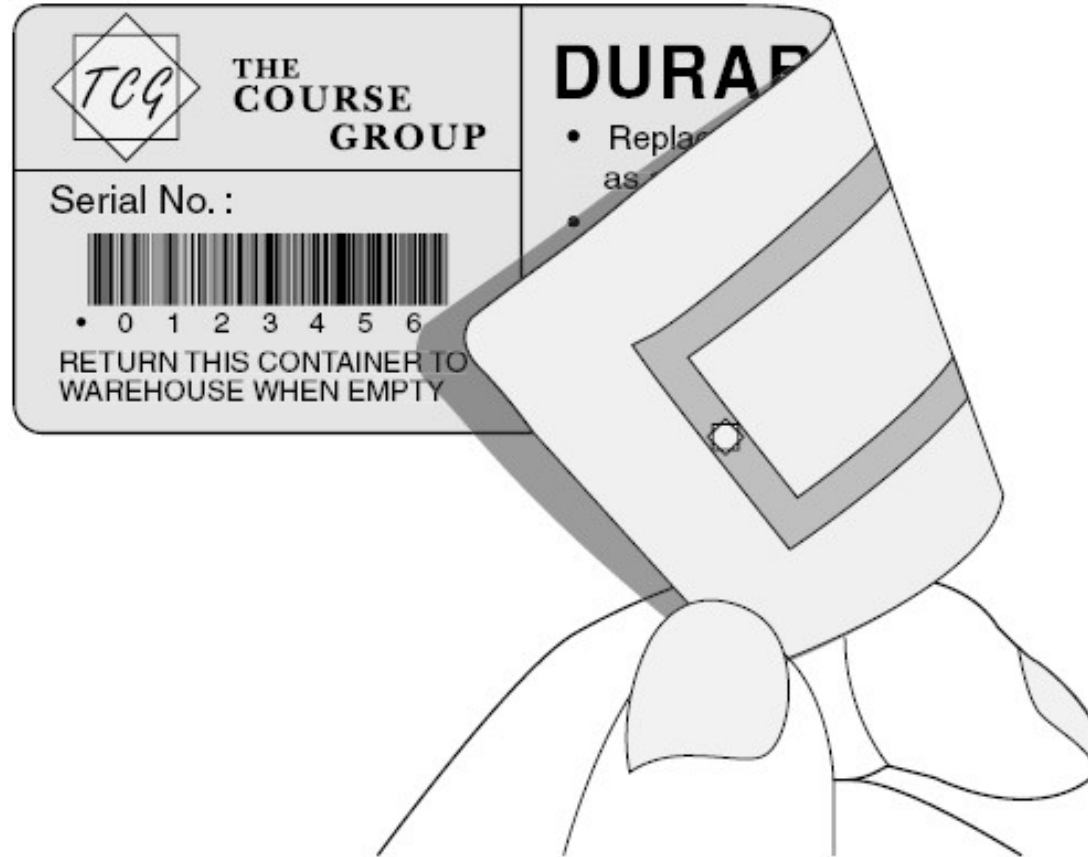


Figure 7-13 RFID tag

Mantrap

- Before entering a secure area, a person must enter the mantrap
 - A small room like an elevator
- If their ID is not valid, they are trapped there until the police arrive
- Mantraps are used at high-security areas where only authorized persons are allowed to enter
 - Such as sensitive data processing areas, cash handling areas, critical research labs, security control rooms, and automated airline passenger entry portals

Mantrap



Video Surveillance

- **Closed circuit television (CCTV)**
 - Using video cameras to transmit a signal to a specific and limited set of receivers
- Some CCTV cameras are fixed in a single position pointed at a door or a hallway
- Other cameras resemble a small dome and allow the security technician to move the camera 360 degrees for a full panoramic view

Physical Access Log

- A record or list of individuals who entered a secure area, the time that they entered, and the time they left the area
- Can also identify if unauthorized personnel have accessed a secure area
- Physical access logs originally were paper documents
 - Today, door access systems and physical tokens can generate electronic log