गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS

राष्ट्रीय न्यायिक विज्ञान विश्वविद्यालय
National Forensic Sciences University

Essentials of Cyber Security and Cyber Warfare

Dr. Lokesh Chouhan

Associate Professor

गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS

राष्ट्रीय न्यायालयिक विज्ञान विश्वविद्यालय
(राष्ट्रीय महत्त्व का संस्थान, गृह मंत्रालय, भारत सरकार)

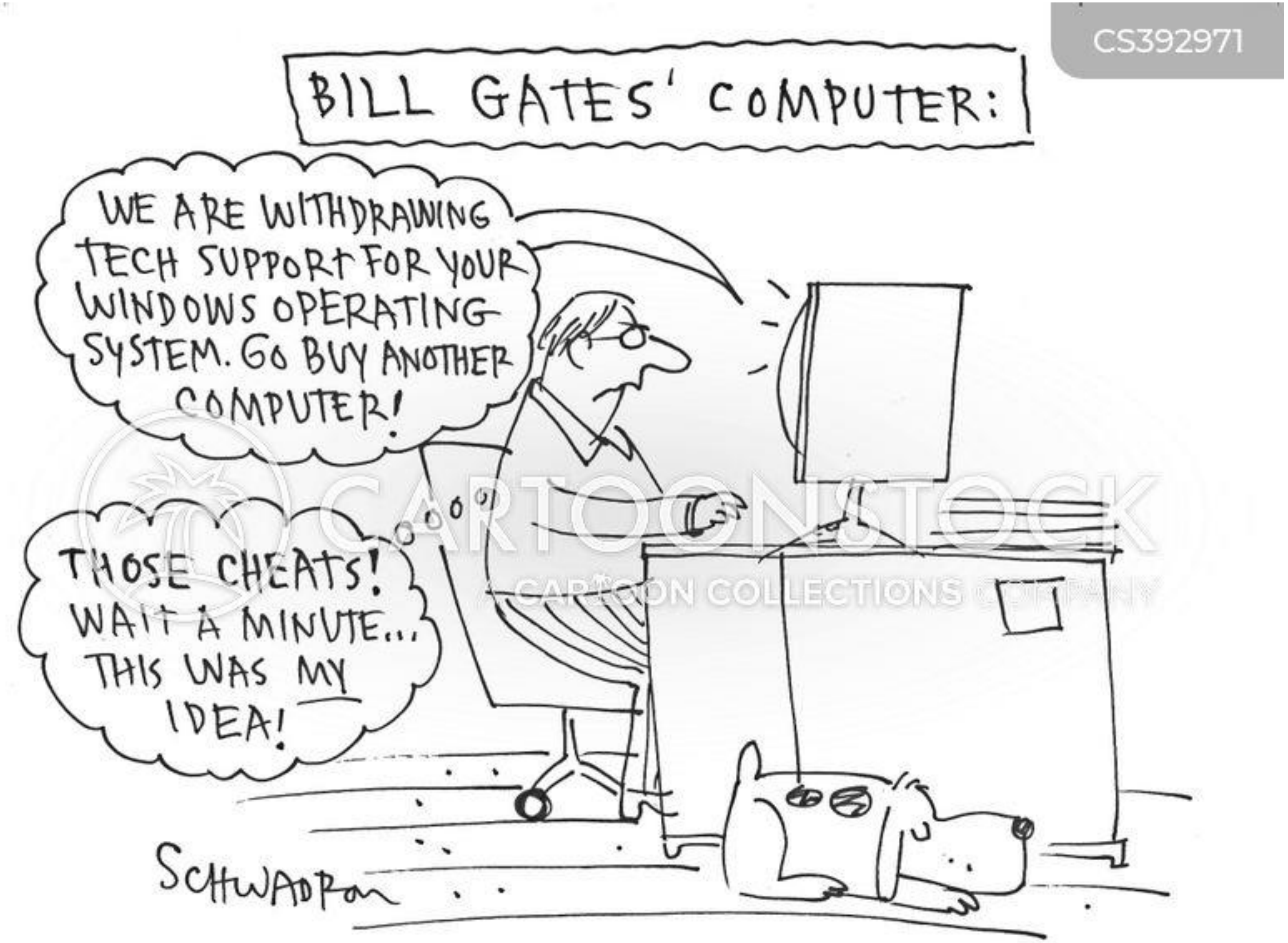
National Forensic Sciences University
(An Institution of National Importance under Ministry of Home Affairs, Government of India)

E-Mail: Lokeshchouhan@gmail.com, Lokesh.chouhan_goa@nfsu.ac.in

Mob: +91-898924399, 9827235155

Unit-1

- **Windows Security**
  - The Windows Security Infrastructure: Three classes of operating system: Client, Server, Embedded, Practical related to Process Hacker, Service Packs, Hotfixes, and Backups: Service packs Email security bulletins, Patch installation, Automatic updates, Windows server update services, Windows backup, System restore, Device driver rollback. Windows Access Controls, NTFS Permissions, Shared Folder Permissions, Registry Key Permissions, Active Directory Permissions, Privileges, BitLocker Drive Encryption, practical related to Microsoft Baseline Security Analyzer. Enforcing.


CS392971
BILL GATES' COMPUTER:
WE ARE WITHDRAWING TECH SUPPORT FOR YOUR WINDOWS OPERATING SYSTEM. GO BUY ANOTHER COMPUTER!
THOSE CHEATS! WAIT A MINUTE... THIS WAS MY IDEA!
SCHWADRON

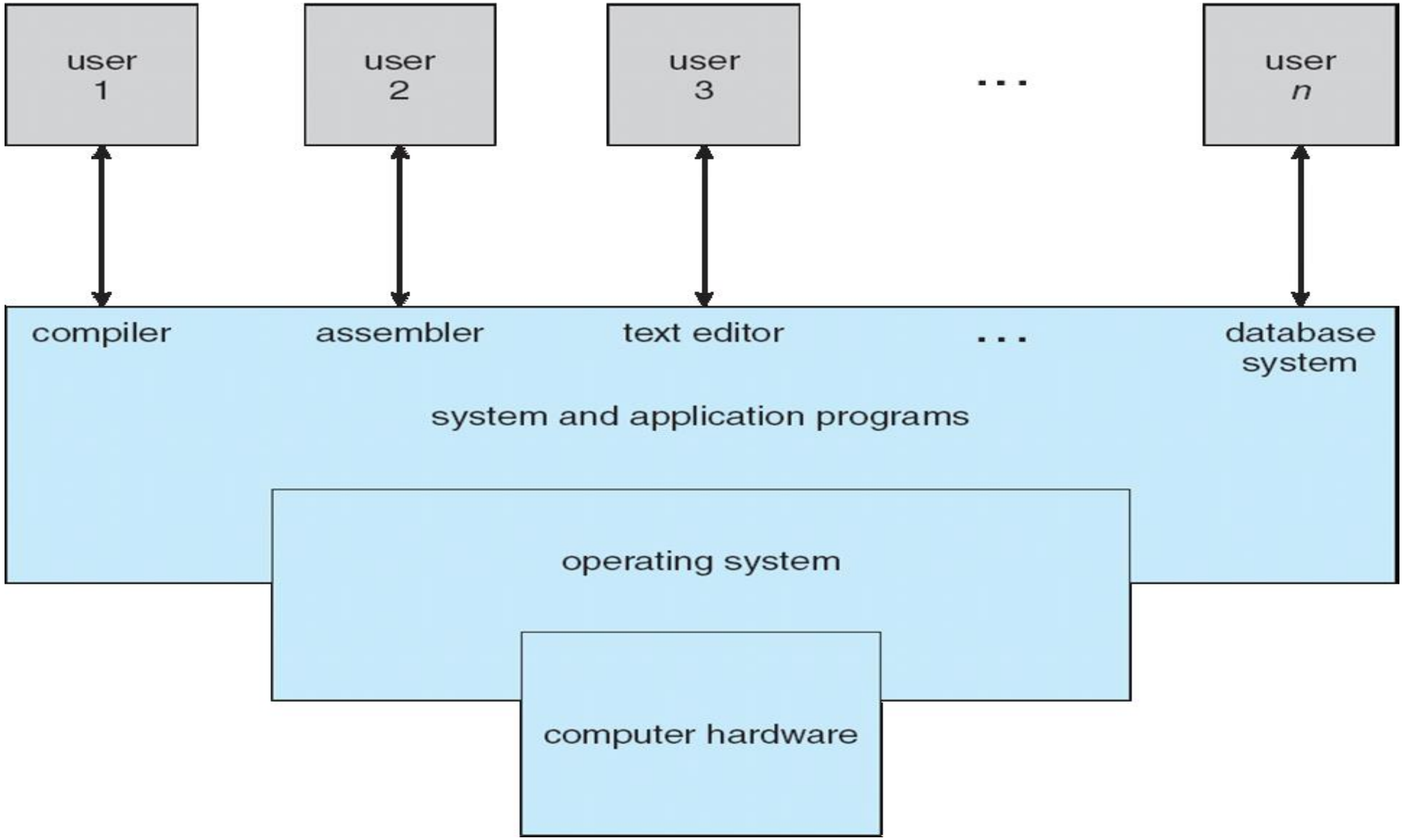
What is an Operating System?

- A program that acts as an intermediary between a user of a computer and the computer hardware
- Operating system **goals**:
  - Execute user programs and make solving user problems easier
  - Make the computer system convenient to use
  - Use the computer hardware in an efficient manner

Computer System Structure

- Computer system can be divided into four components:
  - Hardware – provides basic computing resources
    - CPU, memory, I/O devices
  - Operating system
    - Controls and coordinates use of hardware among various applications and users
  - Application programs – define the ways in which the system resources are used to solve the computing problems of the users
    - Word processors, compilers, web browsers, database systems, video games
  - Users
    - People, machines, other computers

Four Components of a Computer System



What Operating Systems Do

- Depends on the point of view
- Users want convenience, **ease of use** and **good performance**
  - Don’t care about **resource utilization**
- But shared computer such as **mainframe** or **minicomputer** must keep all users happy
- Users of dedicate systems such as **workstations** have dedicated resources but frequently use shared resources from **servers**
- Handheld computers are resource poor, optimized for usability and battery life
- Some computers have little or no user interface, such as embedded computers in devices and automobiles

Operating System Definition

- OS is a **resource allocator**
  - – Manages all resources
  - – Decides between conflicting requests for efficient and fair resource use
- OS is a **control program**
  - – Controls execution of programs to prevent errors and improper use of the computer

Operating System Definition (Cont.)

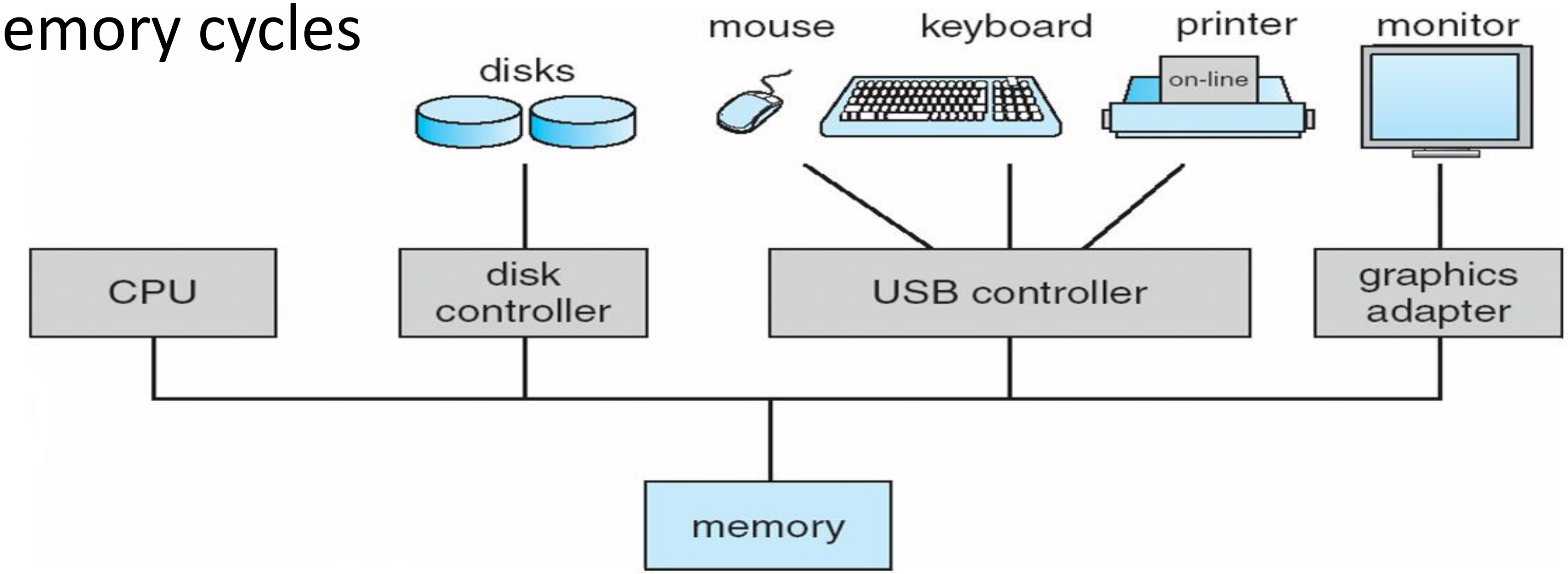
- No universally accepted definition
- "Everything a vendor ships when you order an operating system" is a good approximation
  - But varies wildly
- "The one program running at all times on the computer" is the **kernel**.
- Everything else is either
  - a system program (ships with the operating system) , or
  - an application program.

Computer Startup

- **bootstrap program** is loaded at power-up or reboot
  - Typically stored in ROM or EPROM, generally known as **firmware**
  - Initializes all aspects of system
  - Loads operating system kernel and starts execution

Computer System Organization

- Computer-system operation
  - One or more CPUs, device controllers connect through common bus providing access to shared memory
  - Concurrent execution of CPUs and devices competing for memory cycles



Computing Environments - Mobile

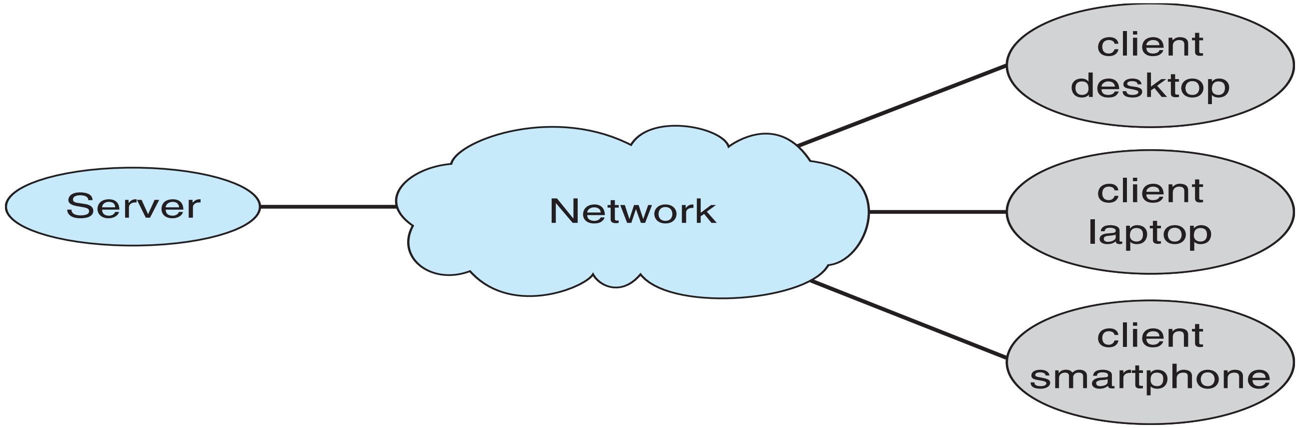
- Handheld smartphones, tablets, etc
- What is the functional difference between them and a “traditional” laptop?
- Extra feature – more OS features (GPS, gyroscope)
- Allows new types of apps like ***augmented reality***
- Use IEEE 802.11 wireless, or cellular data networks for connectivity
- Leaders are **Apple iOS** and **Google Android**

Computing Environments – Distributed

- Distributed computiing
  - Collection of separate, possibly heterogeneous, systems networked together
    - **Network** is a communications path, **TCP/IP** most common
      - **Local Area Network** (**LAN**)
      - **Wide Area Network** (**WAN**)
      - **Metropolitan Area Network** (**MAN**)
      - **Personal Area Network** (**PAN**)
  - **Network Operating System** provides features between systems across network
    - Communication scheme allows systems to exchange messages
    - Illusion of a single system

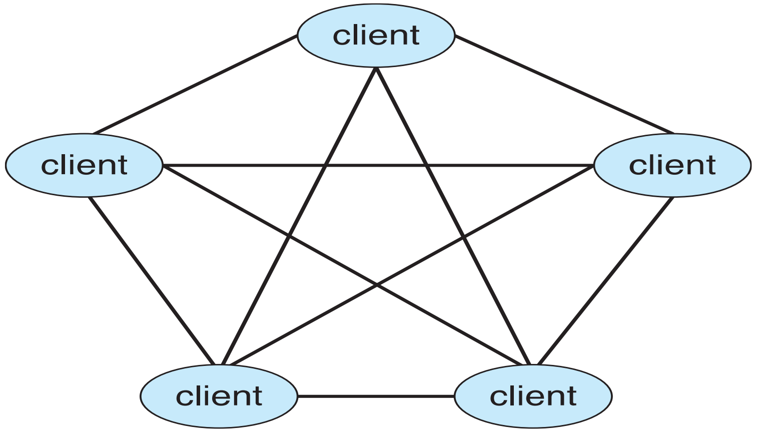
Computing Environments – Client-Server

- Client-Server Computing
  - Dumb terminals supplanted by smart PCs
  - Many systems now **servers**, responding to requests generated by **clients**
    - **Compute-server system** provides an interface to client to request services (i.e., database)
    - **File-server system** provides interface for clients to store and retrieve files



Computing Environments - Peer-to-Peer

- Another model of distributed system
- P2P does not distinguish clients and servers
  - Instead all nodes are considered peers
  - May each act as client, server or both
  - Node must join P2P network
    - Registers its service with central lookup service on network, or
    - Broadcast request for service and respond to requests for service via ***discovery protocol***
  - Examples include Napster and Gnutella, **Voice over IP** (**VoIP**) such as Skype



Computing Environments - Virtualization

- Allows operating systems to run applications within other OSes
  - – Vast and growing industry
- **Emulation** used when source CPU type different from target type (i.e. PowerPC to Intel x86)
  - – Generally slowest method
  - – When computer language not compiled to native code – **Interpretation**
- **Virtualization** – OS natively compiled for CPU, running **guest** OSes also natively compiled
  - – Consider VMware running WinXP guests, each running applications, all on native WinXP **host** OS
  - – **VMM** (virtual machine Manager) provides virtualization services

Protection and Security

- **Protection** – any mechanism for controlling access of processes or users to resources defined by the OS
- **Security** – defense of the system against internal and external attacks
  - Huge range, including denial-of-service, worms, viruses, identity theft, theft of service

Protection and Security

- Systems generally first distinguish among users, to determine who can do what
  - User identities (**user IDs**, security IDs) include name and associated number, one per user
  - User ID then associated with all files, processes of that user to determine access control
  - Group identifier (**group ID**) allows set of users to be defined and controls managed, then also associated with each process, file
  - **Privilege escalation** allows user to change to effective ID with more rights

Process Management

- **A process is a program in execution**. It is a unit of work within the system. Program is a ***passive entity***, process is an ***active entity***.
- Process needs resources to accomplish its task
  - CPU, memory, I/O, files
  - Initialization data
- Process termination requires reclaim of any reusable resources
- Single-threaded process has one **program counter** specifying location of next instruction to execute
  - Process executes instructions sequentially, one at a time, until completion

Process Management

- Multi-threaded process has one program counter per thread
- Typically system has many processes, some user, some operating system running concurrently on one or more CPUs
  - Concurrency by multiplexing the CPUs among the processes / threads

Process Management Activities

The operating system is responsible for the following activities in connection with process management:

- Creating and deleting both user and system processes
- Suspending and resuming processes
- Providing mechanisms for process synchronization
- Providing mechanisms for process communication
- Providing mechanisms for deadlock handling

Process Management Activities

Access control refers to **security features that control who can access resources in the operating system**.

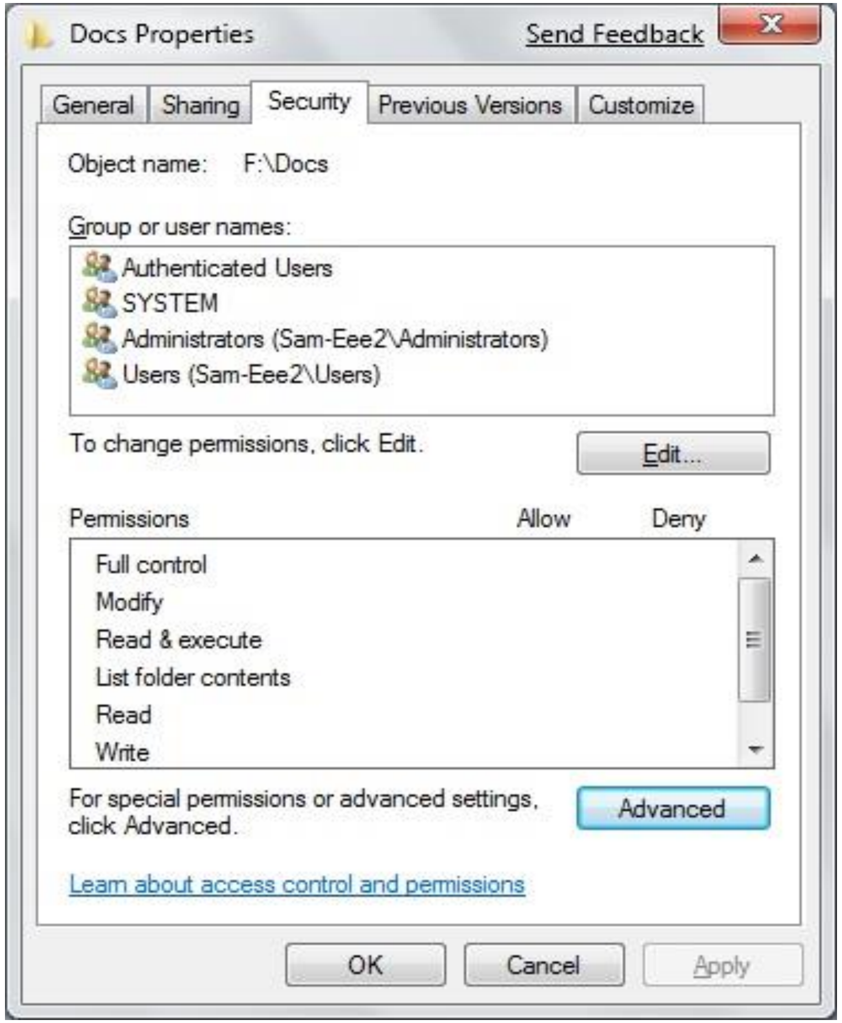
Logical Access Control Methods

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



Object name: F:\Docs

Group or user names:

Authenticated Users
SYSTEM
Administrators (Sam-Eee2\Administrators)
Users (Sam-Eee2\Users)

To change permissions, click Edit.

Full control
Modify
Read & execute
List folder contents
Read
Write

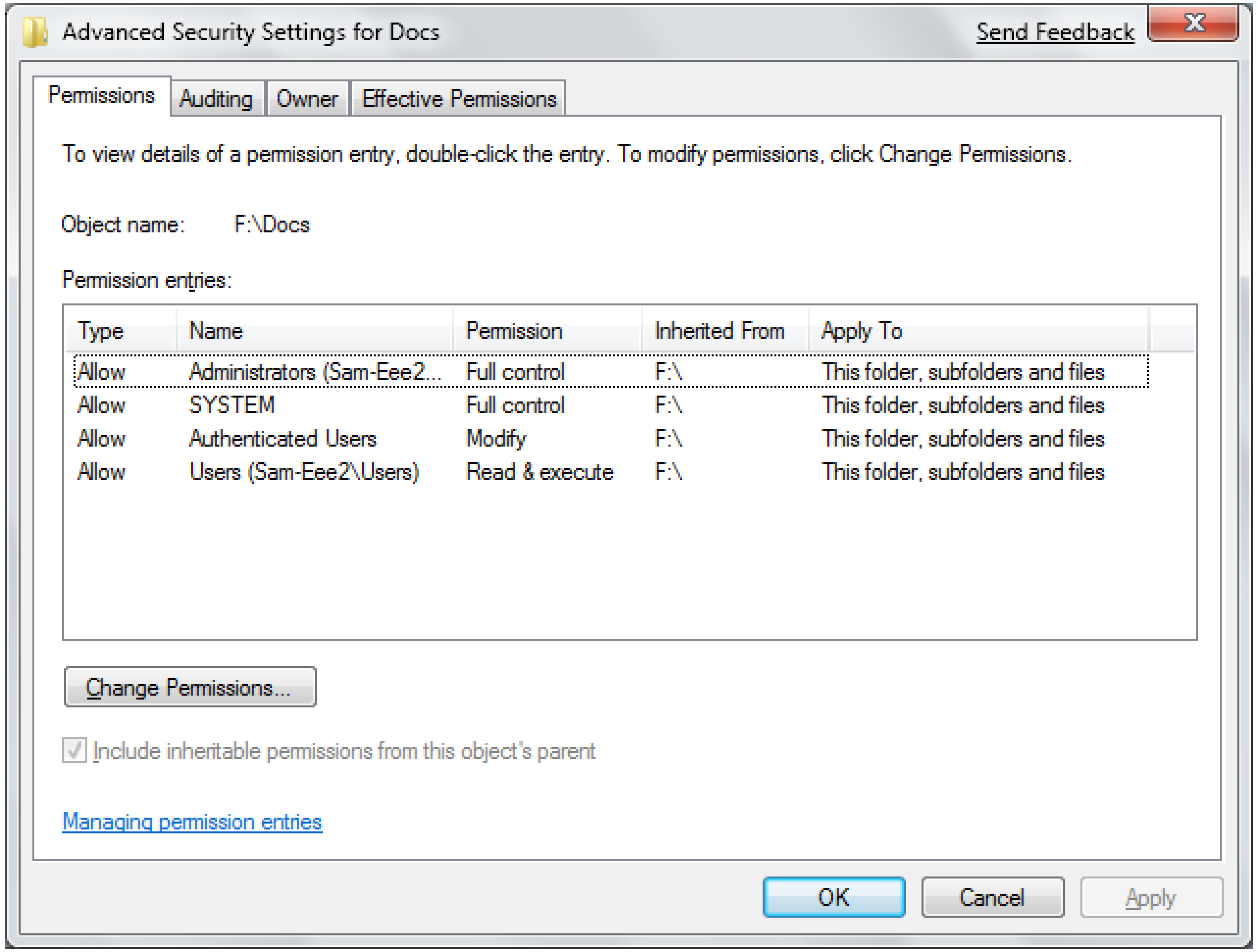
For special permissions or advanced settings, click Advanced.

Learn about access control and permissions

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



To view details of a permission entry, double-click the entry. To modify permissions, click Change Permissions.

Object name: F:\Docs

Permission entries:

Type	Name	Permission	Inherited From	Apply To
Allow	Administrators (Sam-Eee2...	Full control	F:\	This folder, subfolders and files
Allow	SYSTEM	Full control	F:\	This folder, subfolders and files
Allow	Authenticated Users	Modify	F:\	This folder, subfolders and files
Allow	Users (Sam-Eee2\Users)	Read & execute	F:\	This folder, subfolders and files

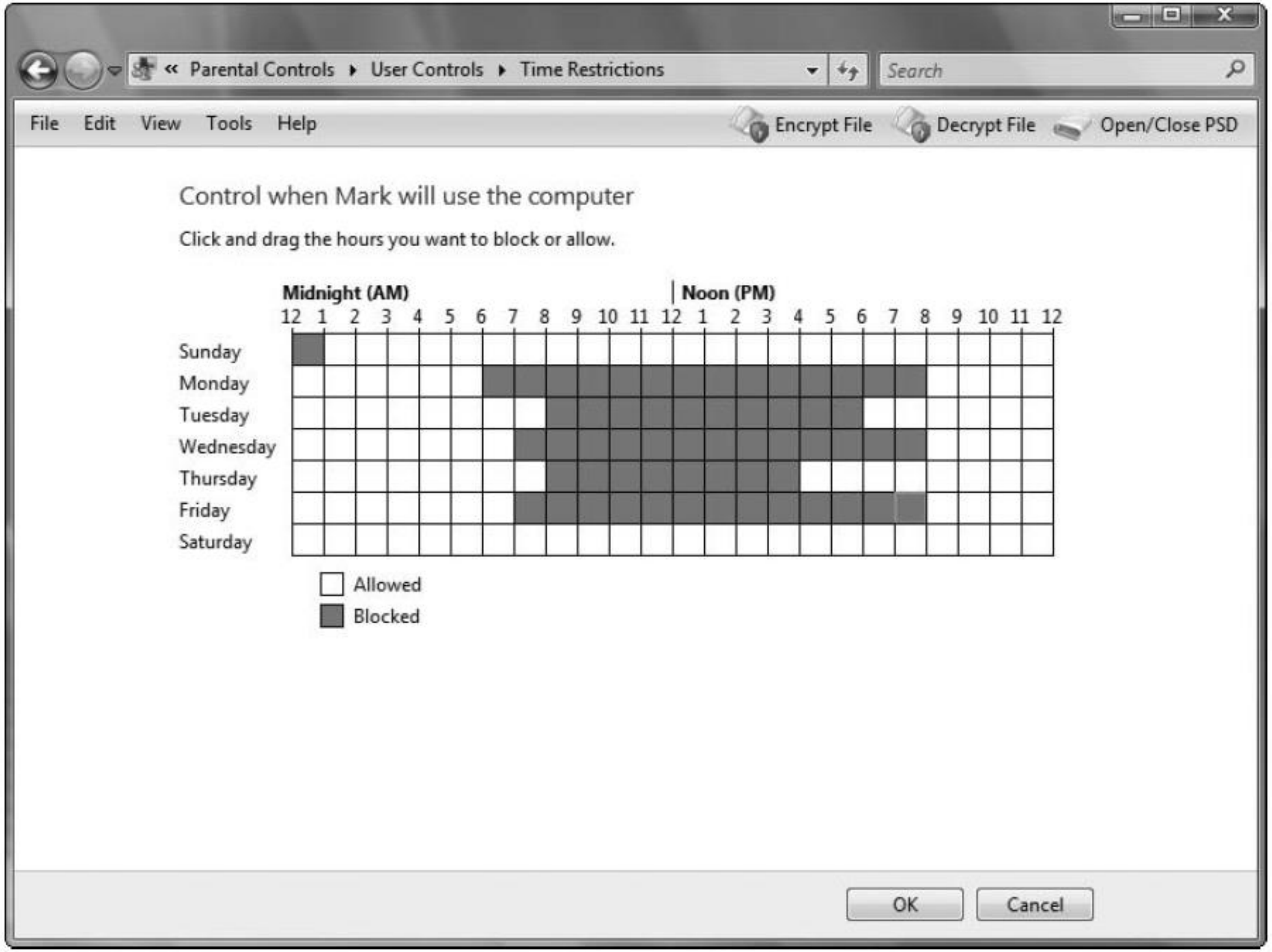
☑ Include inheritable permissions from this object's parent

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



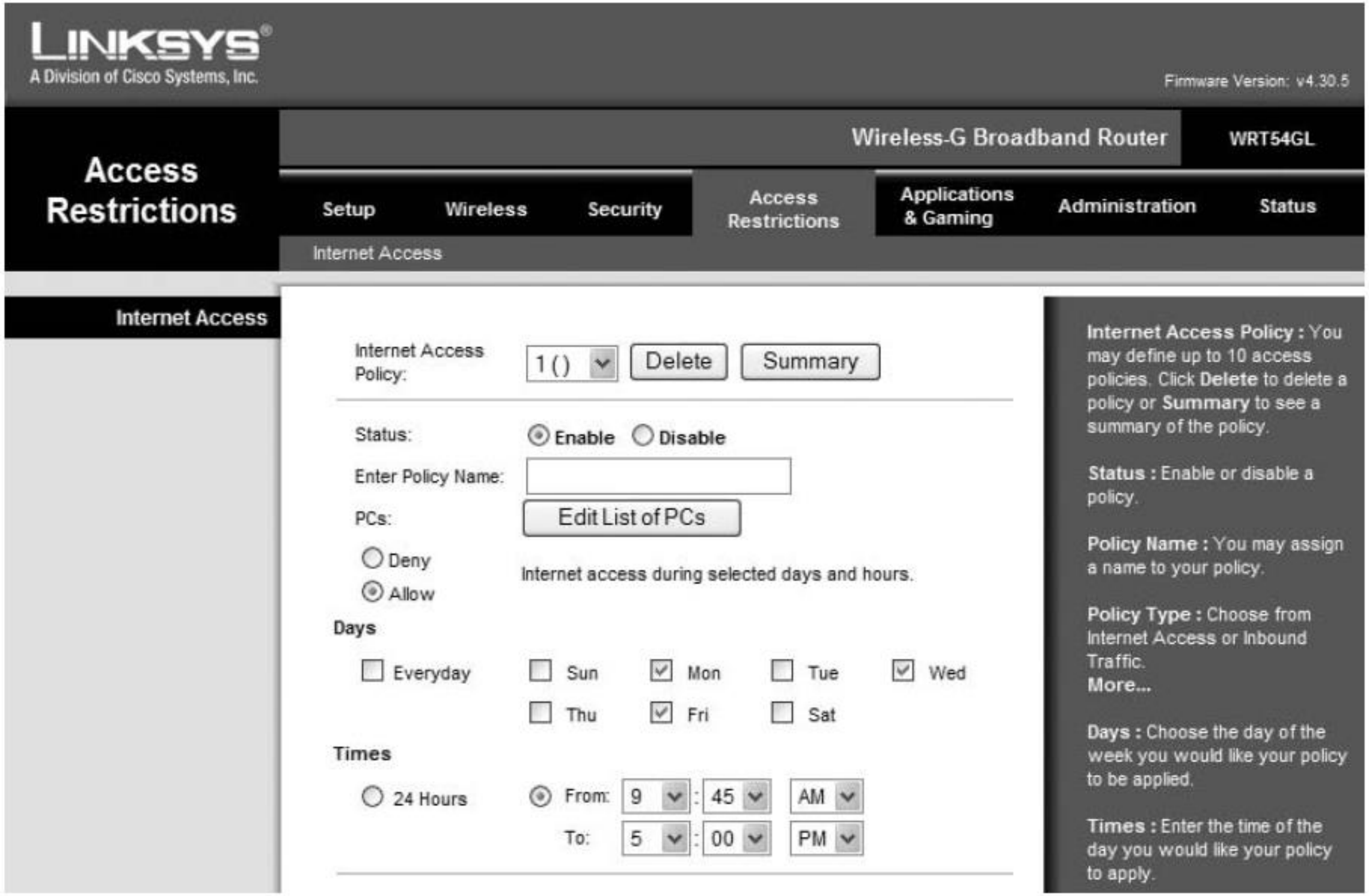
Control when Mark will use the computer

Click and drag the hours you want to block or allow.

	Midnight (AM) 12	1	2	3	4	5	6	7	8	9	10	11	Noon (PM) 12	1	2	3	4	5	6	7	8	9	10	11
Sunday	■	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
Monday	□	□	□	□	□	□	■	■	■	■	■	■	■	■	■	■	■	■	■	■	□	□	□	□
Tuesday	□	□	□	□	□	□	□	□	■	■	■	■	■	■	■	■	■	■	□	□	□	□	□	□
Wednesday	□	□	□	□	□	□	□	■	■	■	■	■	■	■	■	■	■	■	■	■	□	□	□	□
Thursday	□	□	□	□	□	□	□	□	■	■	■	■	■	■	■	■	□	□	□	□	□	□	□	□
Friday	□	□	□	□	□	□	□	■	■	■	■	■	■	■	■	■	■	■	■	■	□	□	□	□
Saturday	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□

□ Allowed
■ Blocked

Figure 7-5 Windows Vista Parental Controls



Internet Access Policy: 1 ()

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.

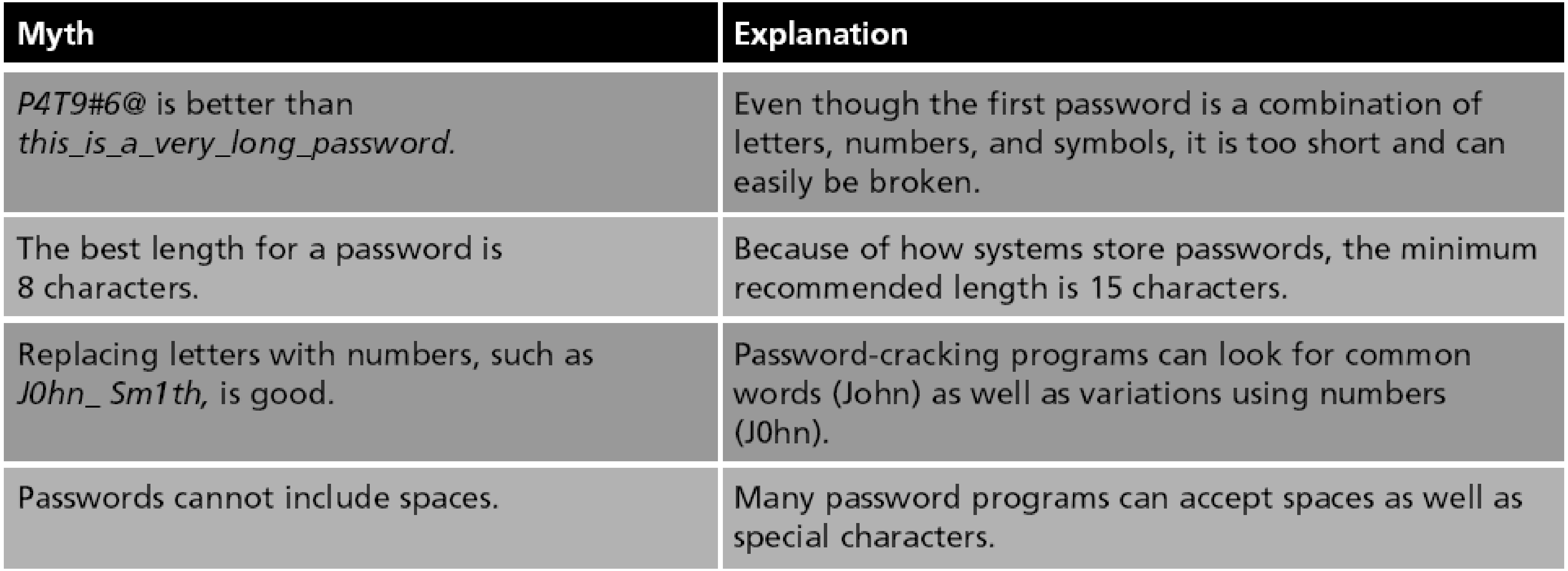
Times : Enter the time of the day you would like your policy to apply.

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
P4T9#6@ is better than *this_is_a_very_long_password.*	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 *J0hn_ Sm1th,* 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.

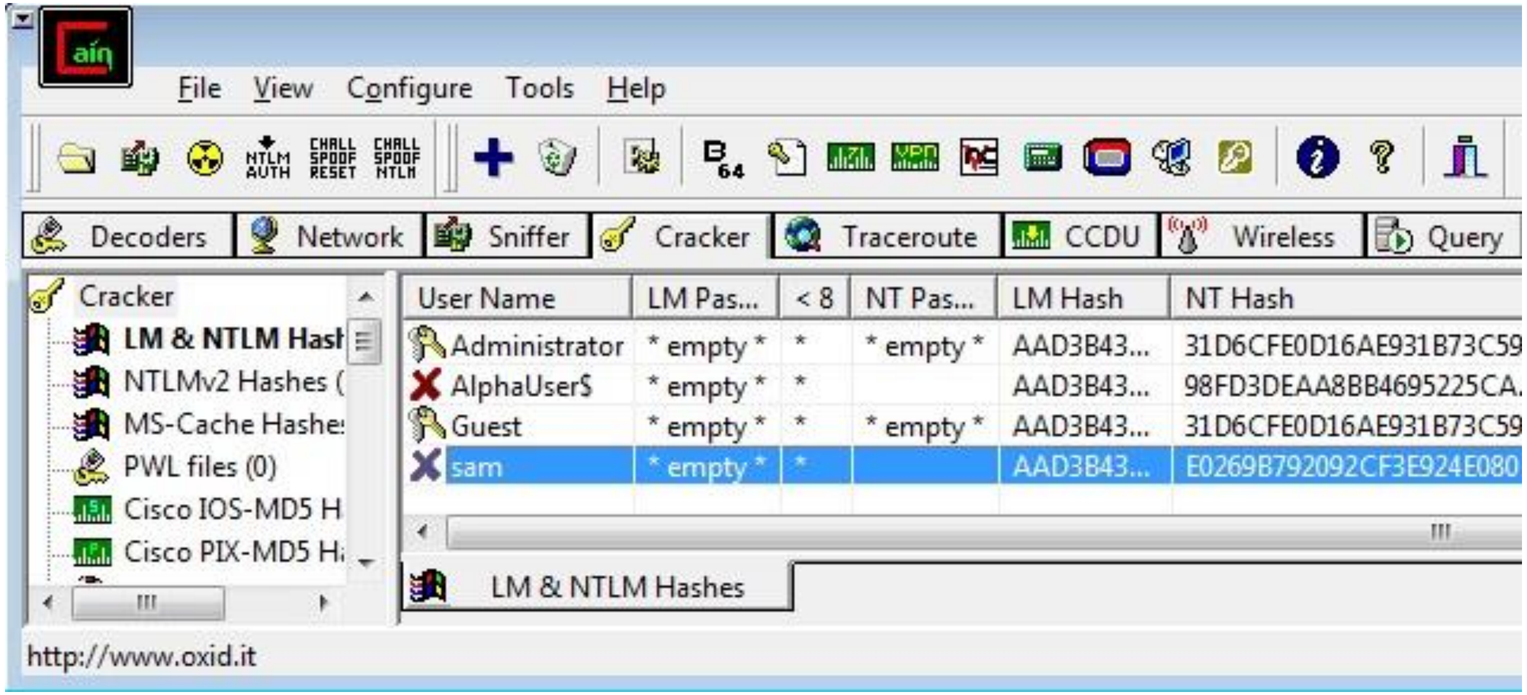
Table 7-4 Common password myths

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"



User Name	LM Pas...	< 8	NT Pas...	LM Hash	NT Hash
Administrator	* empty *	*	* empty *	AAD3B43...	31D6CFE0D16AE931B73C59
AlphaUser$	* empty *	*		AAD3B43...	98FD3DEAA8BB4695225CA.
Guest	* empty *	*	* empty *	AAD3B43...	31D6CFE0D16AE931B73C59
sam	* empty *	*		AAD3B43...	E0269B792092CF3E924E080

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

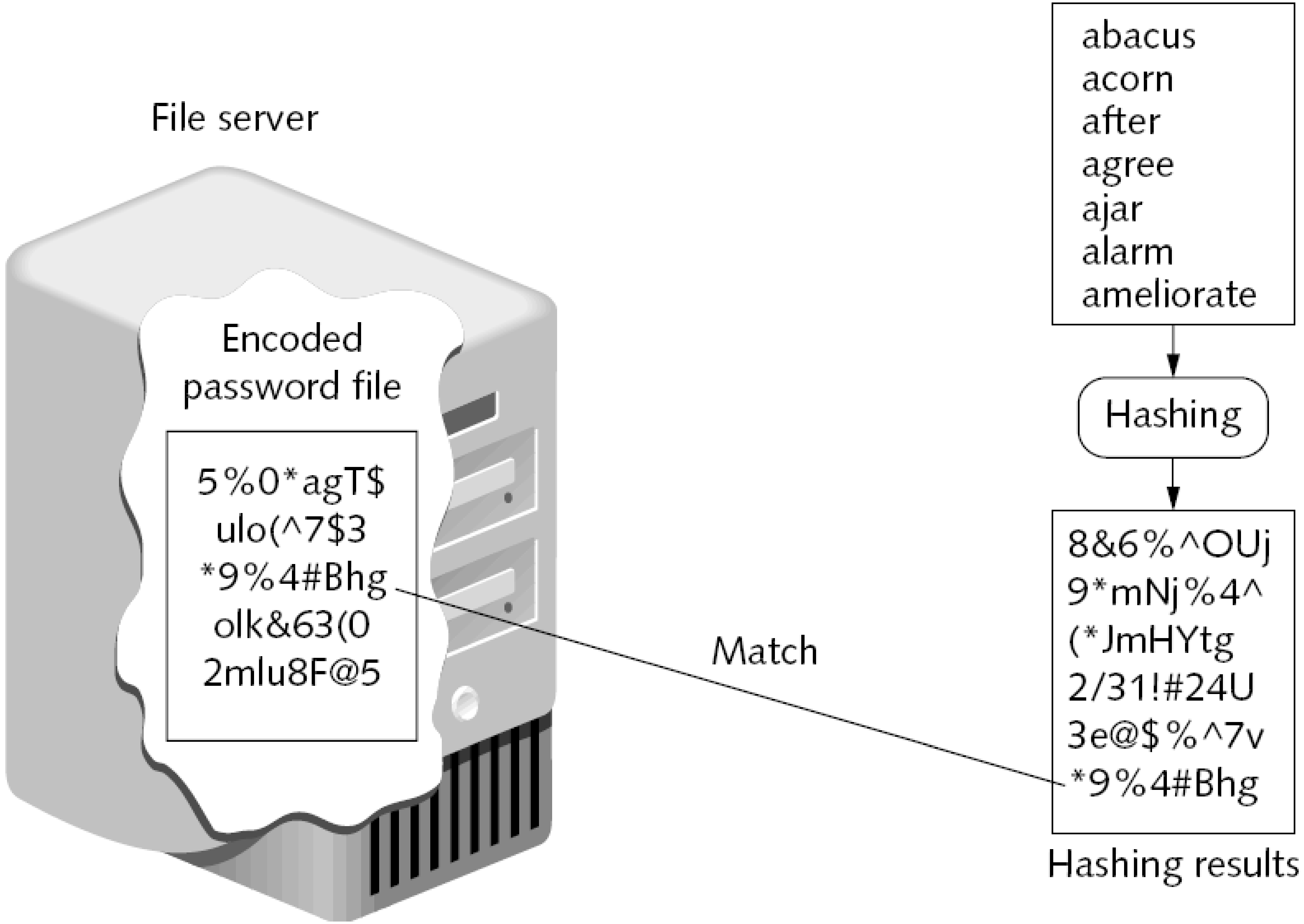
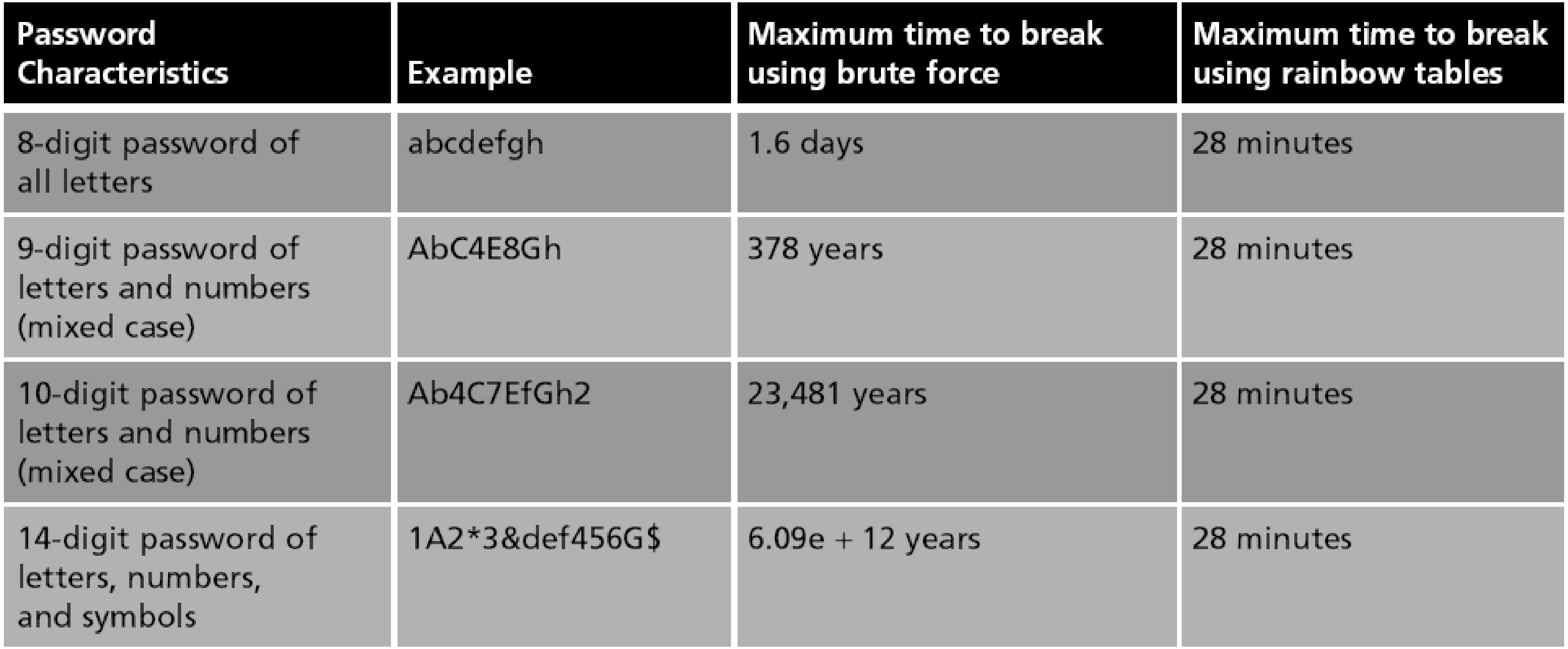


Figure 7-7 Dictionary attack

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)

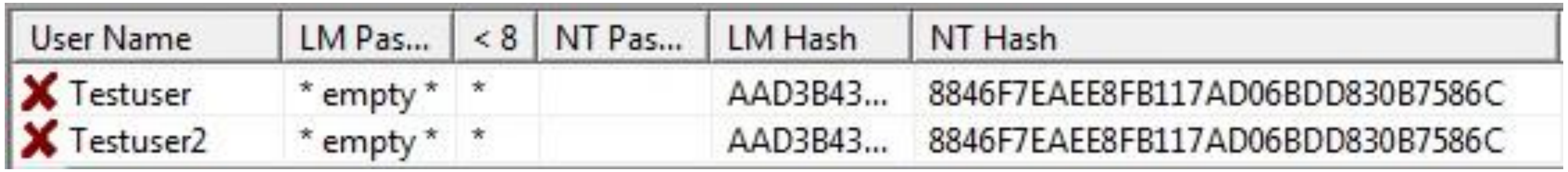
- One reason for the success of rainbow tables is how older Microsoft Windows operating systems hash passwords
- A defense against breaking encrypted passwords with rainbow tables
  - Hashing algorithm should include a random sequence of bits as input along with the user-created password
- These random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

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

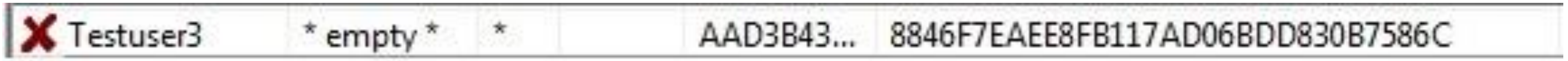
Demonstration

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



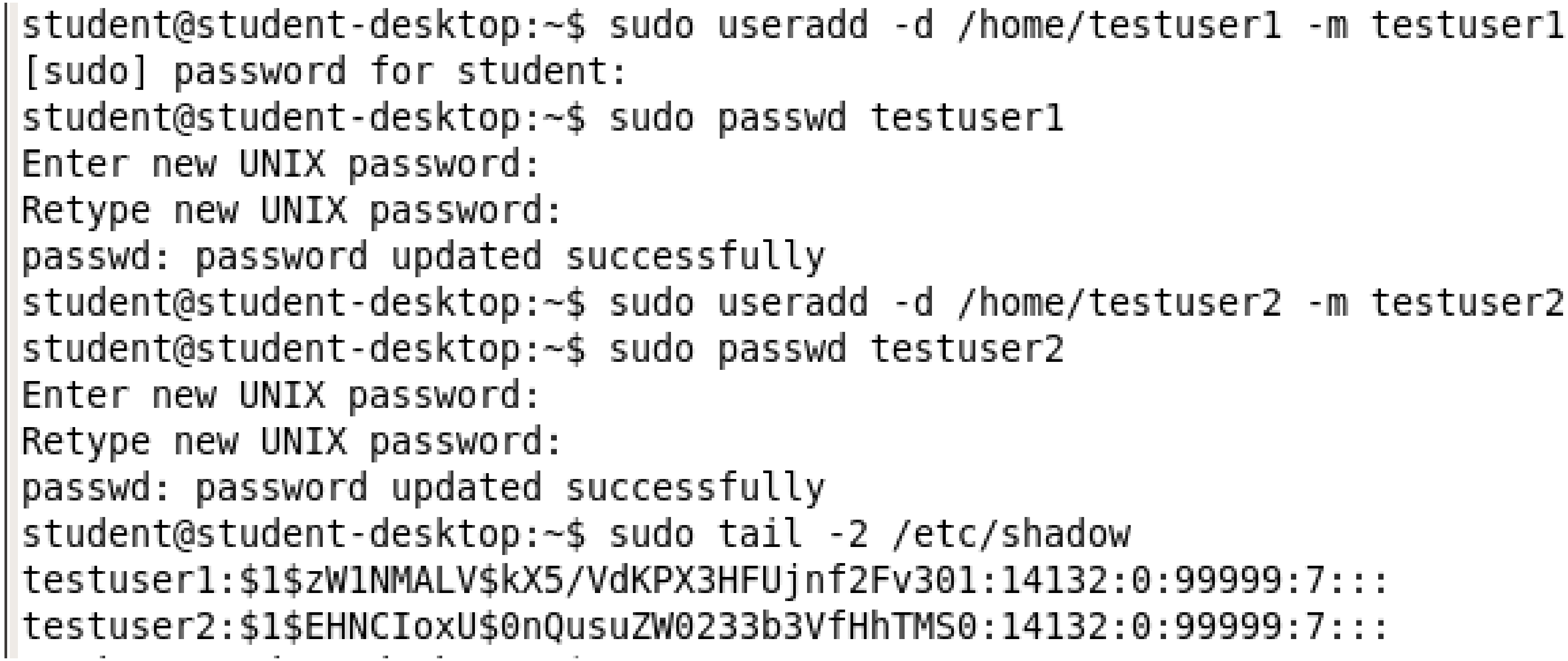
User Name	LM Pas...	< 8	NT Pas...	LM Hash	NT Hash
✗ Testuser	* empty *	*		AAD3B43...	8846F7EAEE8FB117AD06BDD830B7586C
✗ Testuser2	* empty *	*		AAD3B43...	8846F7EAEE8FB117AD06BDD830B7586C

- This hash is from a different Windows 7 Beta machine



✗ Testuser3	* empty *	*		AAD3B43...	8846F7EAEE8FB117AD06BDD830B7586C

Linux Salts its Hashes



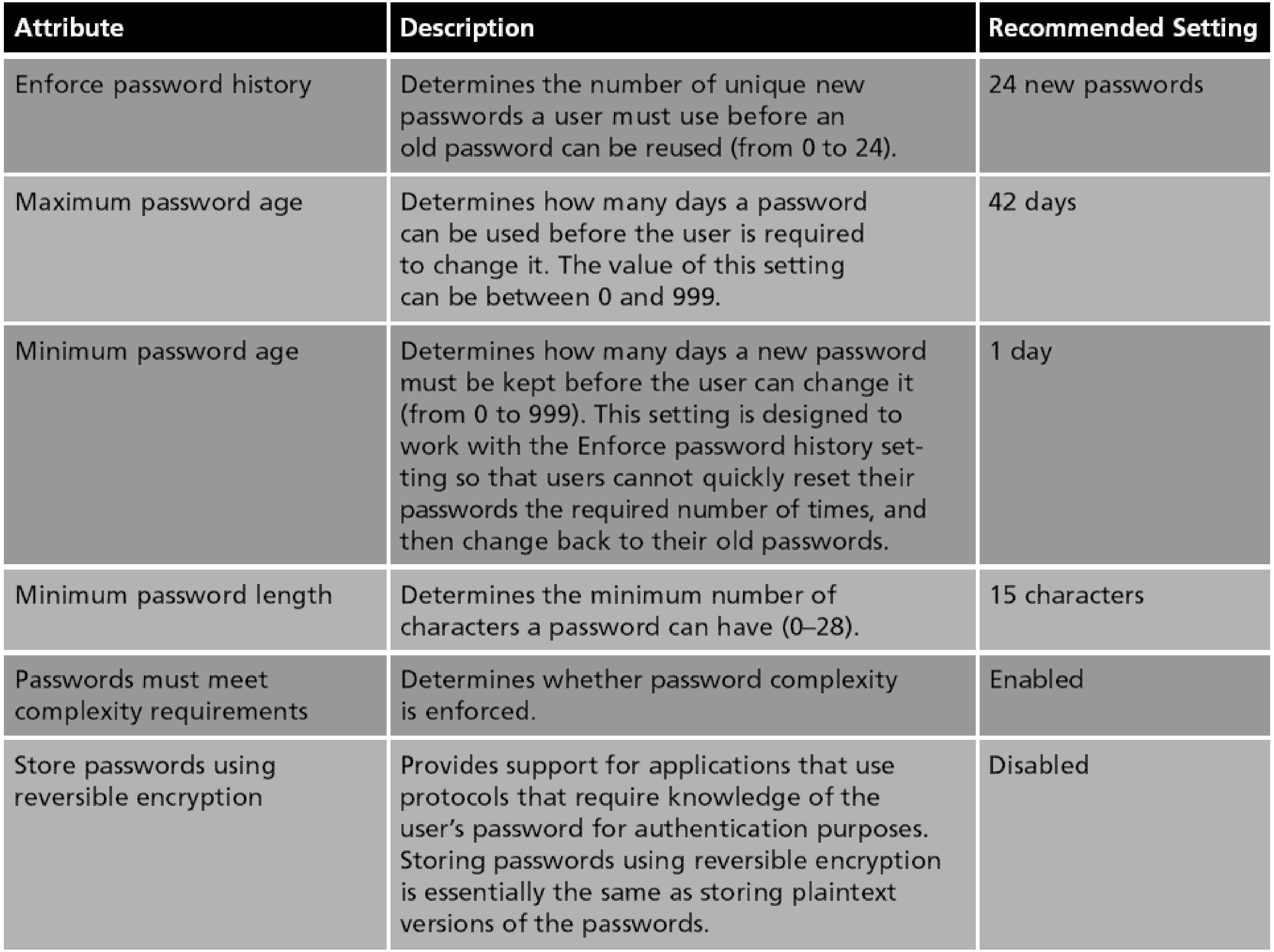
```
student@student-desktop:~$ sudo useradd -d /home/testuser1 -m testuser1
[sudo] password for student:
student@student-desktop:~$ sudo passwd testuser1
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
student@student-desktop:~$ sudo useradd -d /home/testuser2 -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

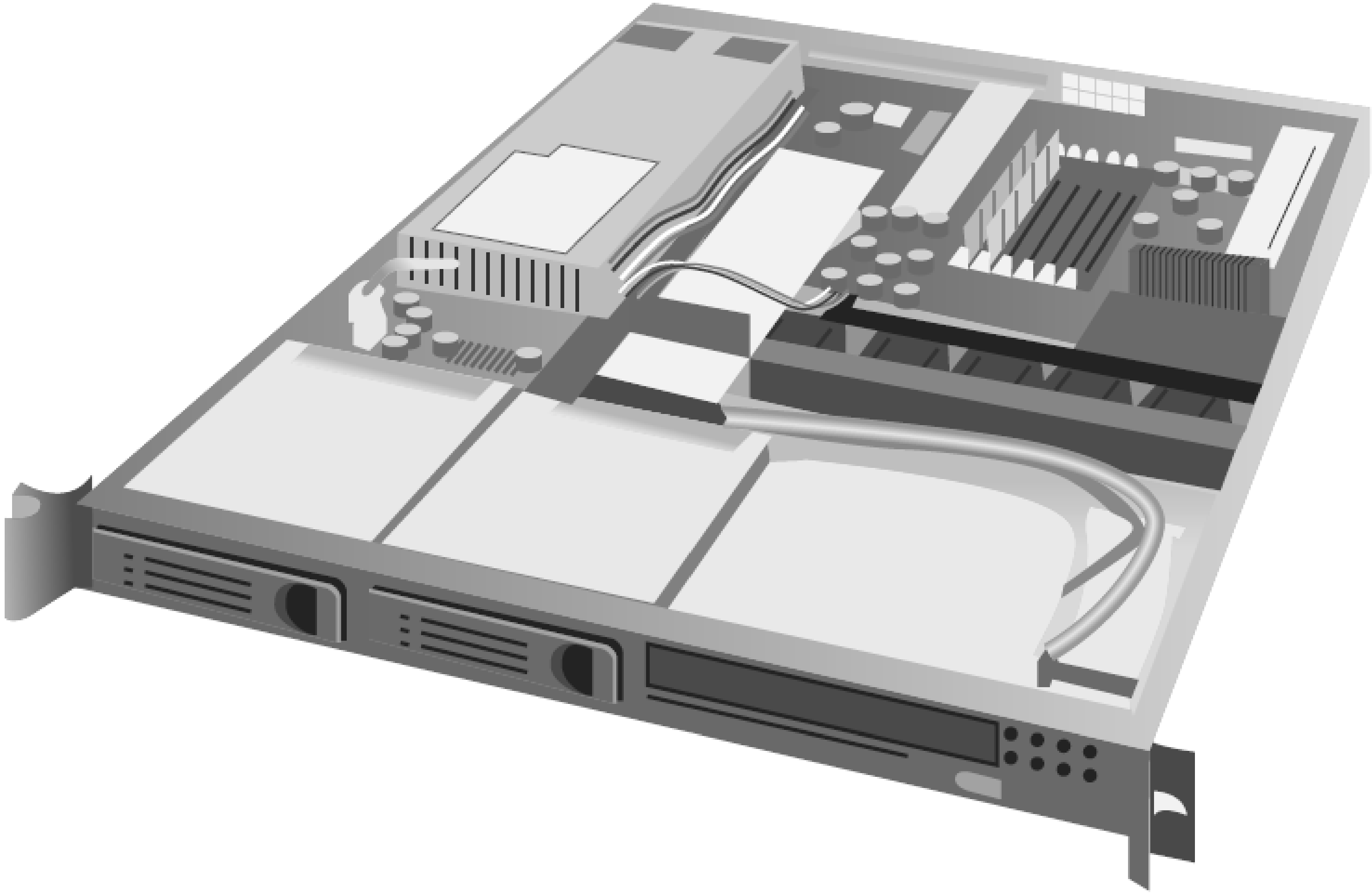


Figure 7-8 Rack-mounted server

KVM Switch

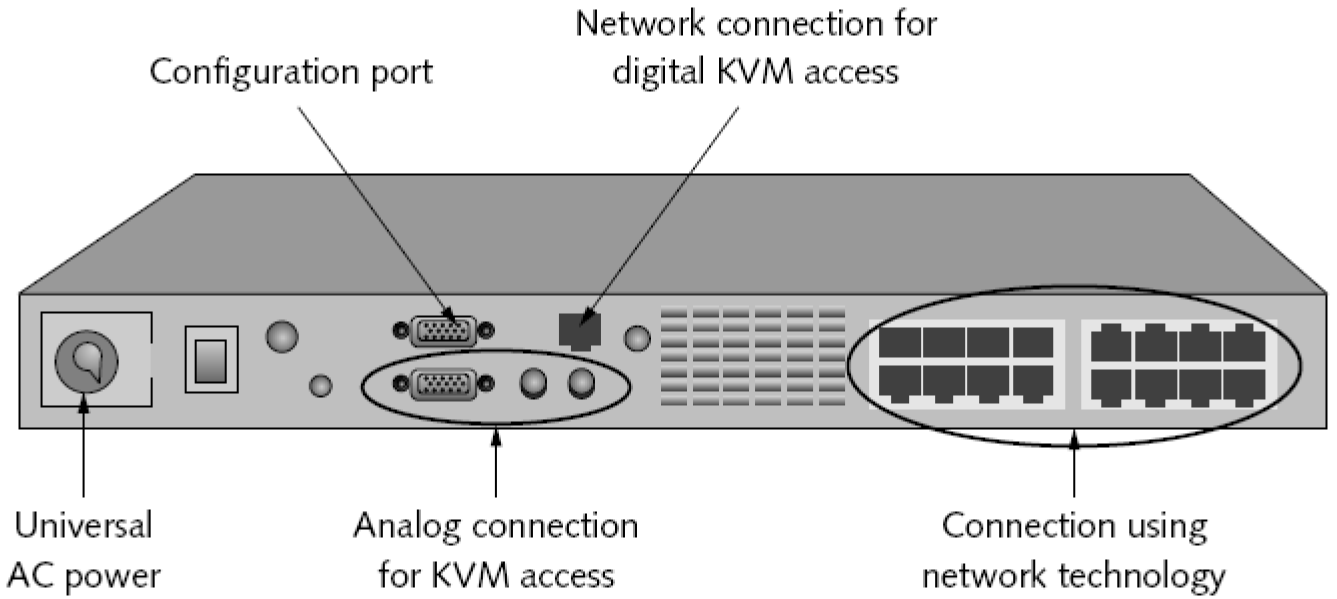
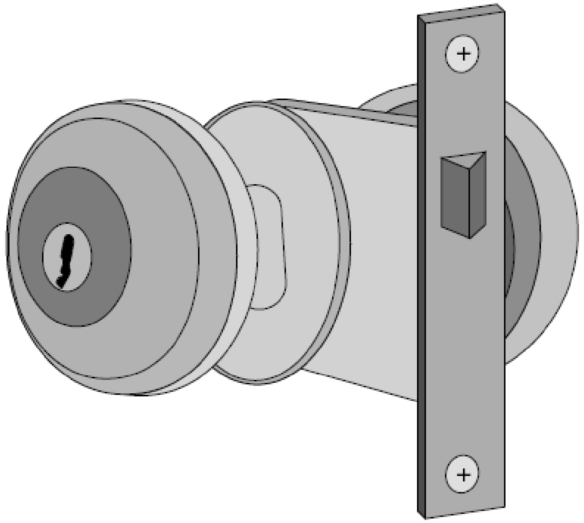

Configuration port
Network connection for digital KVM access
Universal AC power
Analog connection for KVM access
Connection using network technology

Figure 7-9 KVM switch

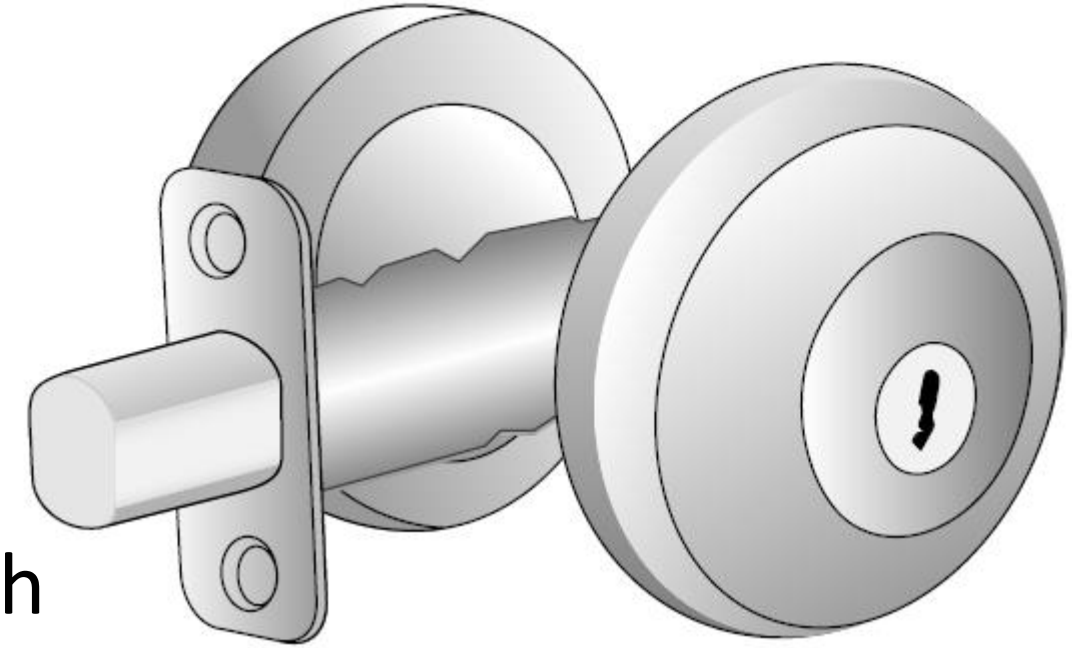
Door Security

- 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 and lock the door



Lock Best Practices

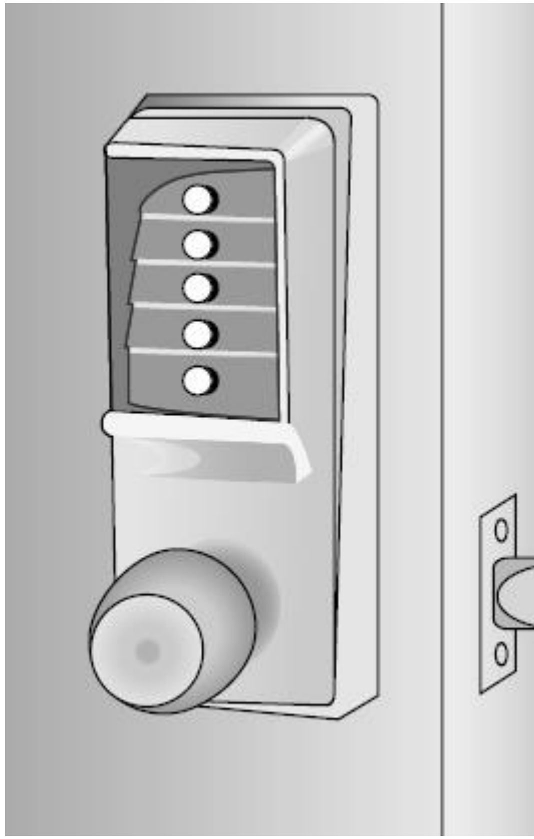
- Change locks immediately upon loss or theft of keys
- Inspect all locks on a regular basis
- Issue keys only to authorized persons
- Keep records of who uses and turns in keys
- Keep track of keys issued, with their number and identification
- Master keys should not have any marks identifying them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

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 and by which code
- Cipher locks are typically connected to a networked computer system
  - – Can be monitored and controlled from one central location



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)

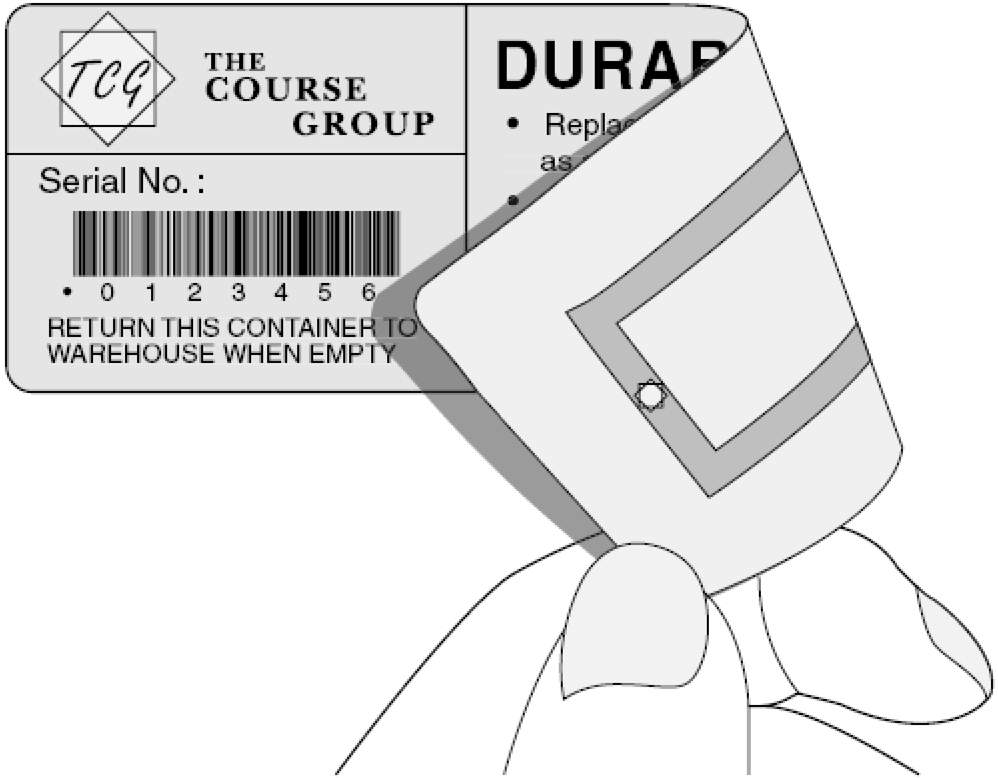
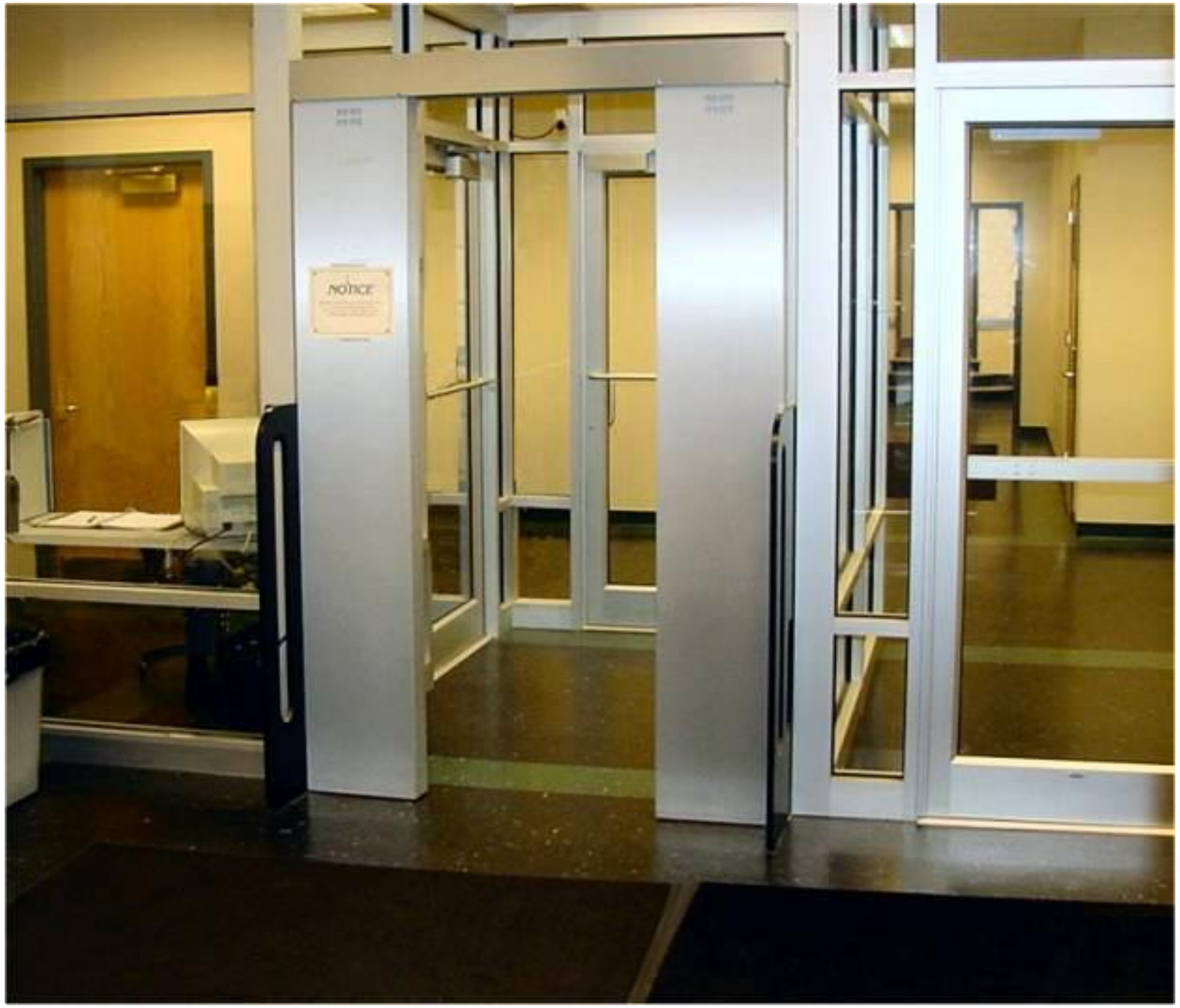


Figure 7-13 RFID tag

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 documents

Dr. Lokesh Chouhan
NFSU Goa
Lokesh.chouhan_goa@nfsu.ac.in