Operating System Security

Operating System Overview

- Operating system: collection of programs that allows user to operate computer hardware
- Three layers:
  - Inner layer
  - Middle layer
  - Outer layer

Operating System Overview (continued)

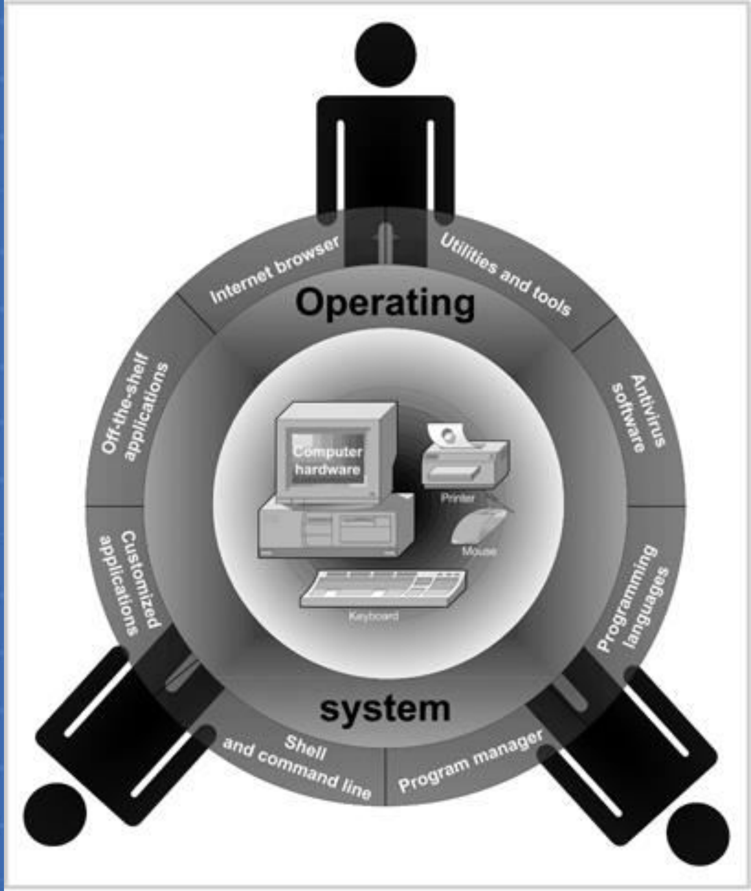


FIGURE 2-1 Three layers of a computer system

Operating System Overview

- Key functions of an operating system:
  - – Multitasking, multisharing
  - – Computer resource management
  - – Controls the flow of activities
  - – Provides a user interface

Operating System Overview (continued)

- Key functions of an operating system (continued):
  - Administers user actions and accounts
  - Runs software utilities and programs
  - Enforce security measures
  - Schedules jobs

The Operating System Security Environment (continued)

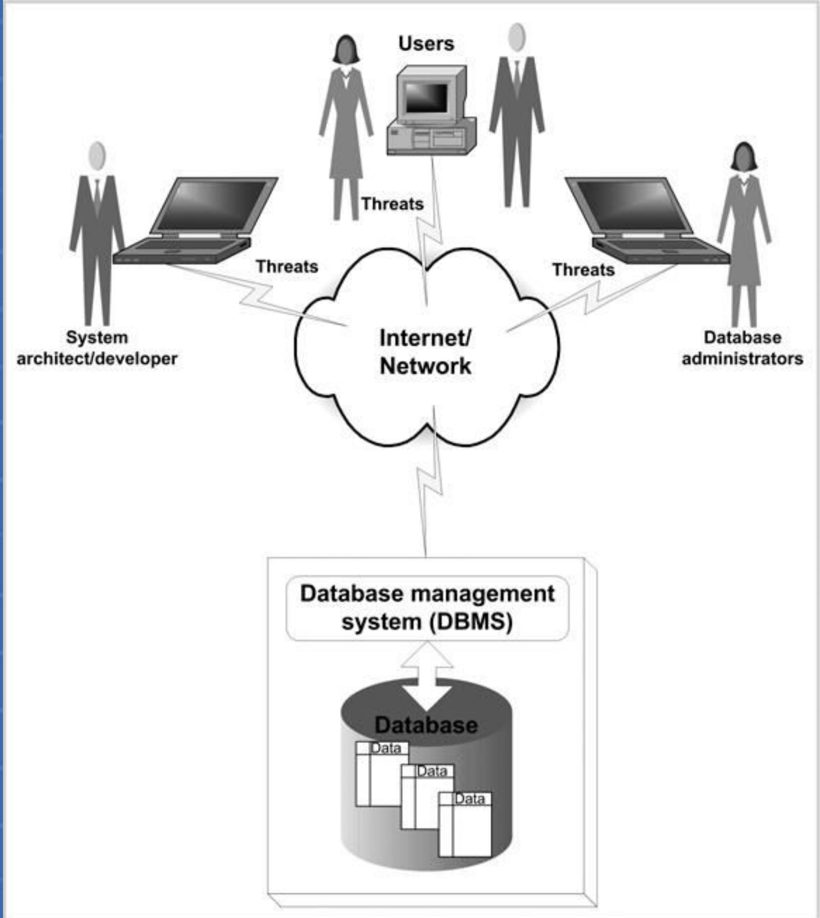


FIGURE 2-2 Database security environment

The Components of an Operating System Security Environment

- Used as access points to the database
- Three components:
  - Memory
  - Services
  - Files

The Components of an Operating System Security Environment (continued)

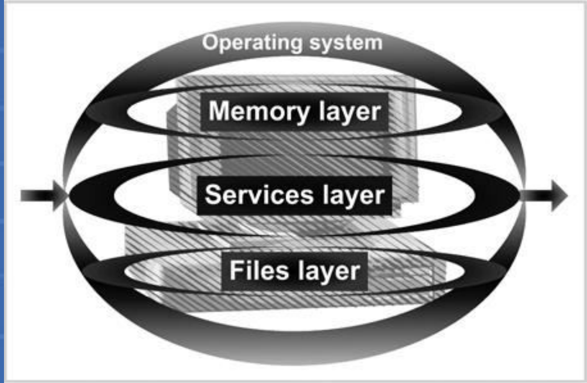


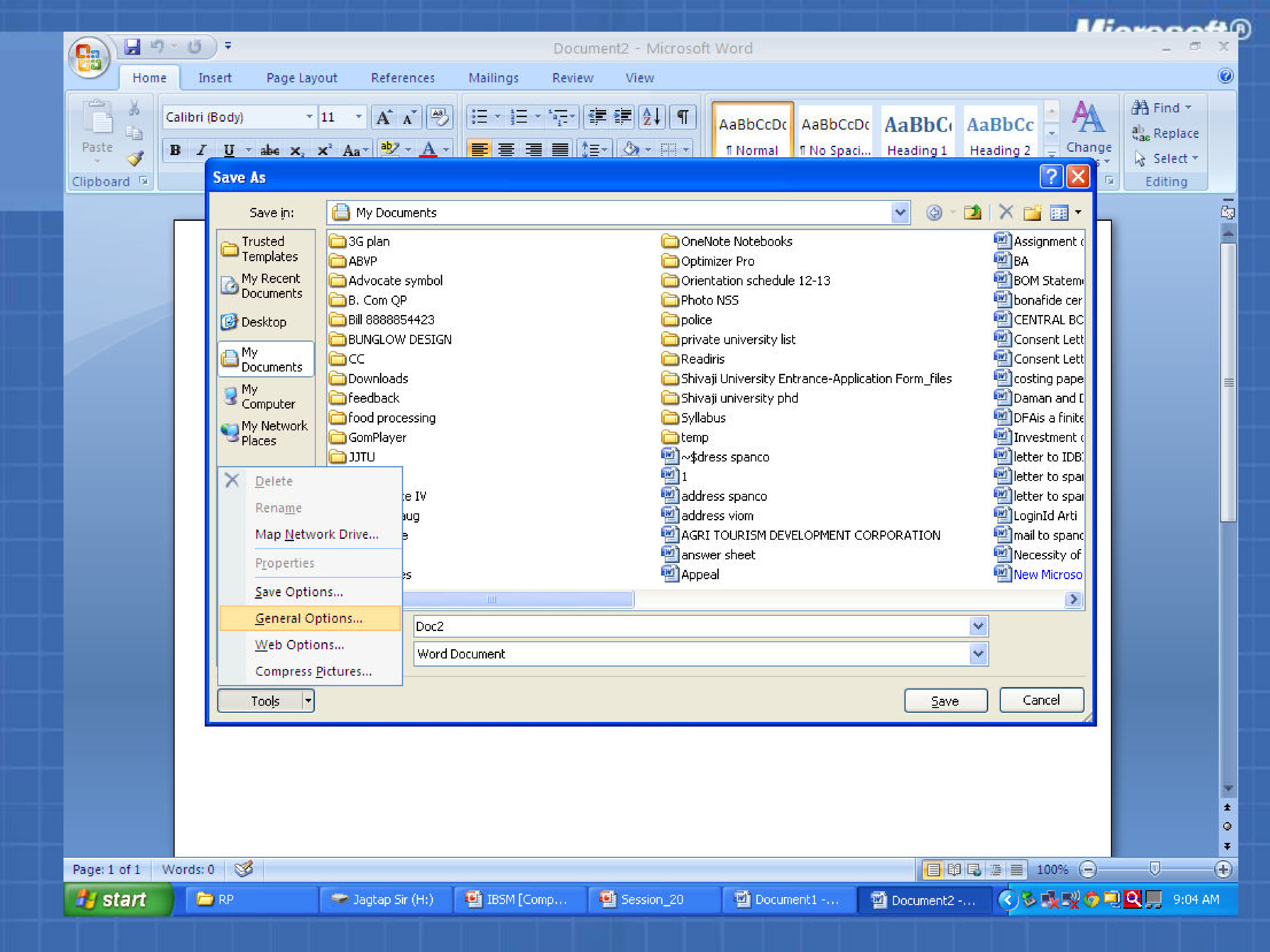
FIGURE 2-3 Operating system security environment

Services

- Main component of operating system security environment
- Operating system core utilities
- Used to gain access to the OS and its features
- Include
  - User authentication
  - Remote access
  - Administration tasks
  - Password policies

Files

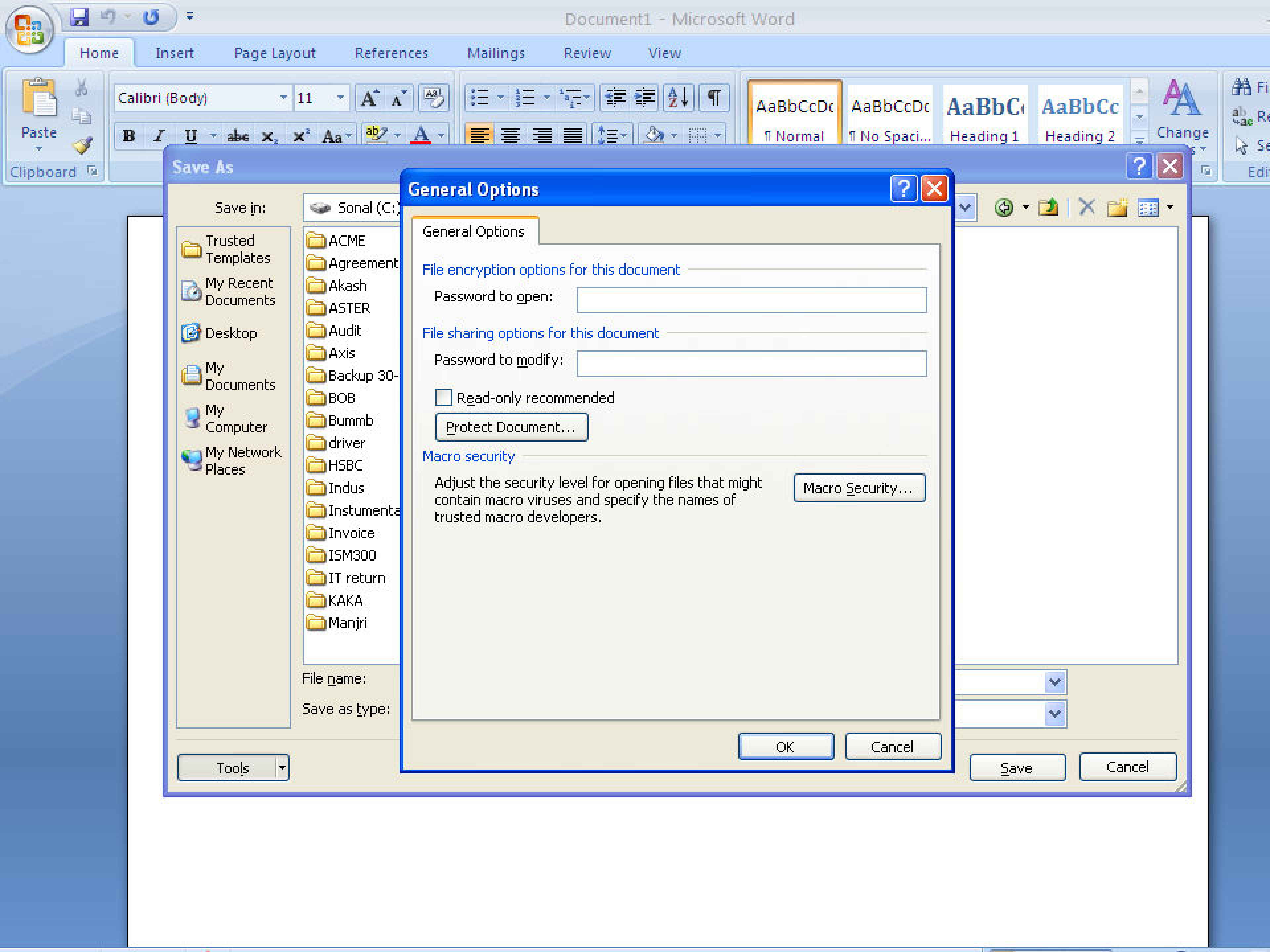
- Common threats:
  - File permission
  - File sharing
- Files must be protected from unauthorized reading and writing actions
- Data resides in files; protecting files protects data
- Read, write, and execute privileges



Save in: My Documents

Doc2

Word Document



General Options

General Options

File encryption options for this document

Password to open:

File sharing options for this document

Password to modify:

☐ Read-only recommended

Protect Document...

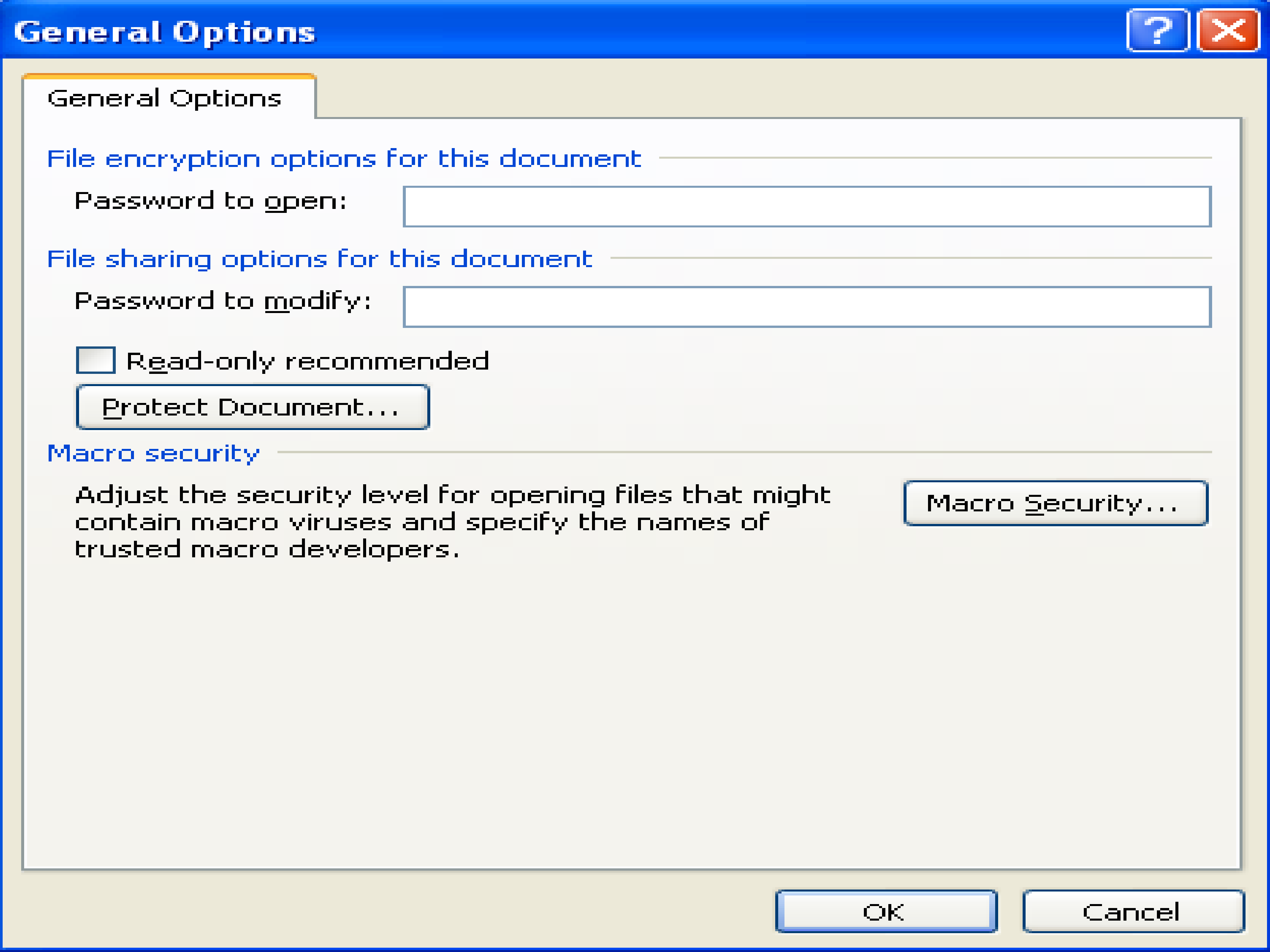
Macro security

Adjust the security level for opening files that might contain macro viruses and specify the names of trusted macro developers.

Macro Security...

OK

Cancel



General Options

General Options

File encryption options for this document

Password to open:

File sharing options for this document

Password to modify:

□ Read-only recommended

Protect Document...

Macro security

Adjust the security level for opening files that might contain macro viruses and specify the names of trusted macro developers.

Macro Security...

OK

Cancel

File Transfer

- FTP (File Transfer Protocol):
  - Internet service for transferring files from one computer to another
  - Transmits usernames and passwords in plaintext
  - Root account cannot be used with FTP
  - Anonymous FTP: ability to log on to the FTP server without being authenticated

File Transfer (continued)

- Best practices:
  - Use Secure FTP utility if possible
  - Make two FTP directories:
    - One for uploads with write permissions only
    - One for downloads with read permissions only
  - Use specific accounts with limited permissions
  - Log and scan FTP activities
  - Allow only authorized operators

Sharing Files

- Naturally leads to security risks and threats
- Peer-to-peer programs: allow users to share files over the Internet
- Reasons for blocking file sharing:
  - – Malicious code
  - – Adware and spyware
  - – Privacy and confidentiality
  - – Pornography
  - – Copyright issues

Memory

- Hardware memory available on the system
- Can be corrupted by badly written software
- Two options:
  - Stop using the program
  - Apply a patch (service pack) to fix it
- Can harm data integrity
- Can potentially exploit data for illegal use

Authentication Methods

- Authentication:
  - Verifies user identity
  - Permits access to the operating system
- Physical authentication:
  - Allows physical entrance to company property
  - Magnetic cards and biometric measures
- Digital authentication: verifies user identity by digital means

Digital Authentication Mechanism

- Digital certificates: digital passport that identifies and verifies holder of certificate
- Digital token (security token):
  - Small electronic device
  - Displays a number unique to the token holder; used with the holder's PIN as a password
  - Uses a different password each time

Problems

It may lead to risk in the following situation

1) when customer uses other computer or cyber café

2) when password is lost.

3) when internet and network data is hacked.

4) when customers respond to phishing mail.

5)The current method of using only one factor of authentication definitely has its weaknesses.

6)The fact that a wrong click can cause monetary losses may be a deterrent.

Problems (continue…)

6) One of the measure and unnoticed drawback of online banking is if one is asking for help on internet baking to customer care and if official customer care executive asks for password and provide it to fraudulent. Then one’s money at risk without his/her mistake.

7) The internet is supposed to make things faster but there can be unnecessary delay due to technical difficulties.

Digital Authentication Mechanism

- Digital card:
  - Also known as a security card or smart card
  - Similar to a credit card; uses an electronic circuit instead of a magnetic strip
  - Stores user identification information
- Public Key Infrastructure (PKI):
  - User keeps a private key
  - Authentication firm holds a public key
  - Encrypt and decrypt data using both keys

Authorization

- Process that decides whether users are permitted to perform the functions they request
- Authorization is not performed until the user is authenticated
- Deals with privileges and rights

User Administration

- Create user accounts
- Set password policies
- Grant privileges to users
- Best practices:
  - Use a consistent naming convention
  - Always provide a password to an account and force the user to change it at the first logon
  - Protect passwords
  - Do not use default passwords

User Administration (continued)

- Best practices (continued):
  - Create a specific file system for users
  - Educate users on how to select a password
  - Lock non-used accounts
  - Grant privileges on a per host basis
  - Do not grant privileges to all machines

Password Policies

- First line of defense
- Dictionary attack: permutation of words in dictionary
- Make hard for hackers entering your systems
- Best password policy:
  - Matches your company missions
  - Enforced at all level of the organization

Password Policies (continued)

- Best practices:
  - Password aging
  - Password reuse
  - Password history
  - Password encryption

Password Policies (continued)

- Best practices (continued):
  - Password storage and protection
  - Password complexity
  - Logon retries
  - Single sign-on

Vulnerabilities of Operating Systems

- Top vulnerabilities to Windows systems:
  - Internet Information Services (IIS)
  - Microsoft SQL Server (MSSQL)
  - Windows Authentication
  - Internet Explorer (IE)
  - Windows Remote Access Services

Vulnerabilities of Operating Systems (continued)

- Top vulnerabilities to Windows (continued):
  - Microsoft Data Access Components (MDAC)
  - Windows Scripting Host (WSH)
  - Microsoft Outlook and Outlook Express
  - Windows Peer-to-Peer File Sharing (P2P)
  - Simple Network Management Protocol (SNMP)

Vulnerabilities of Operating Systems (continued)

- Top vulnerabilities to UNIX systems:
  - BIND Domain Name System
  - Remote Procedure Calls (RPC)
  - Apache Web Server
  - General UNIX authentication accounts with no passwords or weak passwords
  - Clear text services

Vulnerabilities of Operating Systems (continued)

- Top vulnerabilities to UNIX systems (continued):
  - Sendmail
  - Simple Network Management Protocol (SNMP)
  - Secure Shell (SSH)
  - Misconfiguration of Enterprise Services NIS/NFS
  - Open Secure Sockets Layer (SSL)

E-mail Security

- Tool must widely used by public
- May be the tool must frequently used by hackers:
  - Viruses
  - Worms
  - Spam
  - Others
- Used to send private and confidential data as well as offensive material

E-mail Security (continued)

- Used by employees to communicate with:
  - Clients
  - Colleagues
  - Friends
- Recommendations:
  - Do not configure e-mail server on the same machine where sensitive data resides
  - Do not disclose technical details about the e-mail server

Computer Technology and Security

Computer Viruses

- Virus
  - Stands for Vital Information Resources Under Siege
  - Is a destructive computer program written to alter the way a computer operates
  - Is written by individuals to cause damage to computers and the data stored on them
- Some Examples of virus are
  - Disk Killer
  - W97M
  - Sunday
  - Cascade
  - Anna Kournikova
  - Lovegate

Antivirus Software

- Antivirus software
  - Is a software to scan the computer for viruses
  - Is used to remove the viruses from the computer if found
- Examples of antivirus software are:
  - Quick Heal
  - Net Protector
  - Avast
  - McAfee
  - VX2000
  - Smartdog

How to Prevent A Virus Attack

- Precautions that you can follow to keep your computer free from viruses are:
  - Scan all floppy disks/pen drives before opening or copying files
  - Install at least one antivirus software and run it regularly
  - Update the antivirus software regularly to check for new viruses
  - Make backup copies to minimize damage if virus attack occur

Hacking

- Hackers or Crackers
  - Are people who access the computers of others without their knowledge
  - They are intelligent programmers, who have high knowledge of computer systems and programming languages

Misusing Personal Information

- Chances of the data being intercepted, deleted or altered by others can happen
  - When data is transferred over a large network
  - In chat rooms and newsgroups, where people often reveal personal details in their interaction with others. People with bad intentions use this information maliciously

Theft of Information

The different types of crimes and criminals that the digital world harbours are:

- Software Piracy
  - Is the illegal copying, distribution, or use of software without the permission of its owner
- Cracking
  - Cracker
    - Break into the computers of other users by means of a network, either for the challenge or for some malicious intention
    - Take advantage of any breach in security on a computer and steal vital information or even cause damage to files and programs

Theft of Information (Contd..)

Stealing Data

- Occurs when data is transferred from one network to another where there is a risk of the information being viewed, deleted, or altered by others
- Occurs when Individuals share their information online or when they buy goods online