

Secure OS

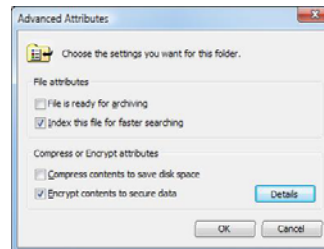
Standard OS Security

Your regular laptop OS provides several security features

- File access permissions
- Separate accounts with passwords
 - Separate home directory
 - Lesser privileged accounts
- Ability to encrypt files transparently

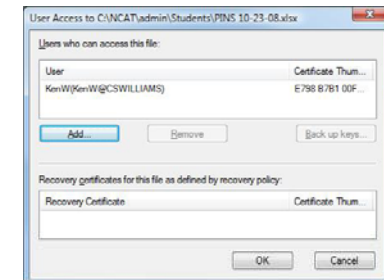
Windows File Encryption

- Windows can encrypt the contents of a file
- Encryption and decryption happens automatically without input from the user
- Access to the encryption keys is based on the user's password

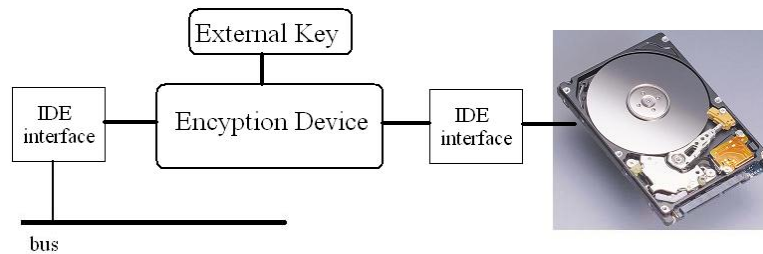


Windows Encryption Recovery

- If an administrator changes a user's password, they will lose access to encrypted files
- Windows supports Recovery Certificates that can allow access if the user previously allowed this



Hardware Disk Encryption



Commercial Products

Internal IDE PCI Hard Drive Encryption Add-On Card with DES 40-bit



Internal IDE PCI Hard Drive Encryption Add-On Card with DES 40-bit Encryption

Item# PCI-40BIT

Regular price: \$99.98

Sale price: \$59.98





Availability: Usually ships the next business day.

[Add to cart](#)

Windows Security Center



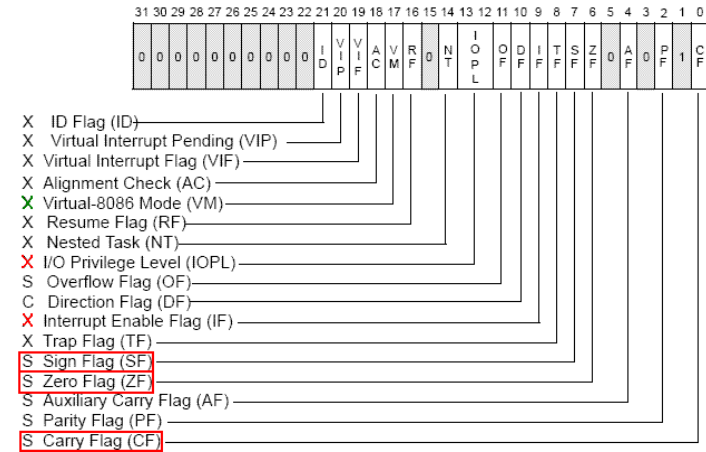
User Account Control

- User Account Control (UAC) asks permission or an admin password before performing actions that could potentially affect your system
-  Windows needs your permission to continue
-  Program needs your permission to continue
-  Unidentified program wants access
-  This program has been blocked
- *Many users consider UAC to be annoying*

Pentium Protection

- Protection bits give 4 levels of privilege
 - 0 most protected, 3 least
 - Use of levels software dependent
 - Usually level 3 for applications, level 1 for O/S and level 0 for kernel (level 2 not used)
 - Level 2 may be used for apps that have internal security e.g. database
 - Some instructions only work in level 0

Intel Status Register



Memory Separation

- All memory allocation schemes we discussed prevent one user from accessing the memory of another
- Base address registers have limit registers
- Each user has their own page table in a virtual memory system. Users cannot address the memory of another user.

Security Oriented OS

- There are several operating systems whose focus is enhanced security
- Some OS are designed to enforce mandatory access control policies
- Security-Enhanced Linux (SELinux) is a set of modifications to regular Linux to support access control security policies including mandatory access control

Marking

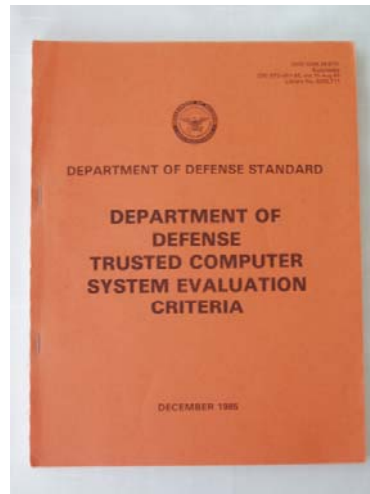
- All objects (such as files) in a secure operating system are marked with a security level
- An object's security level is set when the object is created and cannot be changed
- The OS is responsible for maintaining an object's security level
- When a user's account is entered in the system, the administrator sets their security level

Trusted Computer System Evaluation Criteria

- Trusted Computer System Evaluation Criteria (TCSEC) is a Department of Defense standard that sets basic requirements for assessing the effectiveness of computer security controls
- Created in 1983 and replaced by the international Common Criteria standard in 2005

Orange Book

- The TCSEC standard is informally known as the Orange book
- One of the Rainbow Series of U.S. government security publications



TCSEC Policy Objectives

- The security policy must be explicit, well-defined and enforced by the computer system
- **Mandatory Access Control** – The Bell-LaPadula Model must be enforced
- **Discretionary Security Policy** – Allow users to specify who may access an object and how

TCSEC Accountability Requirements

Regardless of policy the system must enforce

- **Identification** - The ability to recognize an individual user
- **Authentication** - The verification of an individual user's authorization to specific information
- **Auditing** - Audit information must be kept and protected so that actions affecting security can be traced to the individual

TCSEC Assurance

- The computer system must contain hardware/software mechanisms that can be independently evaluated to provide sufficient assurance that the system enforces the above requirements

TCSEC Classes

- **A** — Verified protection
 - A1 — Verified Design
- **B** — Mandatory protection
 - B1 — Labeled Security Protection
 - B2 — Structured Protection
 - B3 — Security Domains
- **C** — Discretionary protection
 - C1 — Discretionary Security Protection
 - C2 — Controlled Access Protection
- **D** — Minimal protection

Common Criteria

- Common Criteria for Information Technology Security Evaluation is an international standard for computer security certification
- Evolved from previous U.S., Canadian and European standards

Evaluation Assurance Level

- The Evaluation Assurance Level (EAL) is a numerical rating describing the depth and rigor of an evaluation
- EAL 1 is the most basic and EAL 7 the most stringent
- Higher EALs do not necessarily imply “better security”, only more extensively verified

Common Criteria Testing Laboratories

- Common Criteria Testing Laboratories (CCTL) certify that a product meets specifications
- In the US, the National Institute of Standards and Technology (NIST) and the National Voluntary Laboratory Accreditation Program accredits Laboratories

Why have International Standards?

- If a device has been certified to meet the standard, people building secure systems can feel safe to use it
- Without standards, people can make claims about their security without any basis for accuracy

Criticisms of Common Criteria

- Evaluation is a costly process (often measured in hundreds of thousands of US dollars)
- Evaluation focuses primarily on assessing the documentation, not on the product itself
- It takes so long to prepare the evidence and get certified that the product may be obsolete