Security

ICT 41203 Operating Systems

Nimal Skandhakumar

Faculty of Technology
University of Sri Jayewardenepura

2018/12/03

The Security Environment

- **Confidentiality** - if the owner of data decides to make available only to certain people and no others, the system should guarantee that release of the data to unauthorised people never occurs
- **Integrity** - unauthorised users should not be able to modify any data (changing the data, removing data and adding false data) without the owner's permission
- **Availability** - nobody can disturb the system to make it unusable, such as in the form of **denial-of-service** attacks that are increasingly common

Goal	Threat
Confidentiality	Exposure of data
Integrity	Tampering with data
Availability	Denial of service

Intruders

- Common categories:
  - Casual prying by nontechnical users.
  - Snooping by insiders.
  - Determined attempts to make money.
  - Commercial or military espionage.

Operating System Security

- Often the ways to compromise the security of a computer system are not very sophisticated.
  - E.g. easy to guess passwords, writing down passwords
- Exploiting such behaviours of humans, social engineering, is a significant challenge.
  - E.g. requirement to frequent password change vs. writing down passwords
- However, operating systems should also account for targeted attacks that are more sophisticated in nature, targeting the security framework of operating systems.

Operating System Security

- Passive attacks
  - try to steal information passively
  - sniff the network traffic and tries to break the encryption to get to the data
- Active attacks
  - try to make a computer program misbehave
  - take control of a user's Web browser to make it execute malicious code

Operating System Security

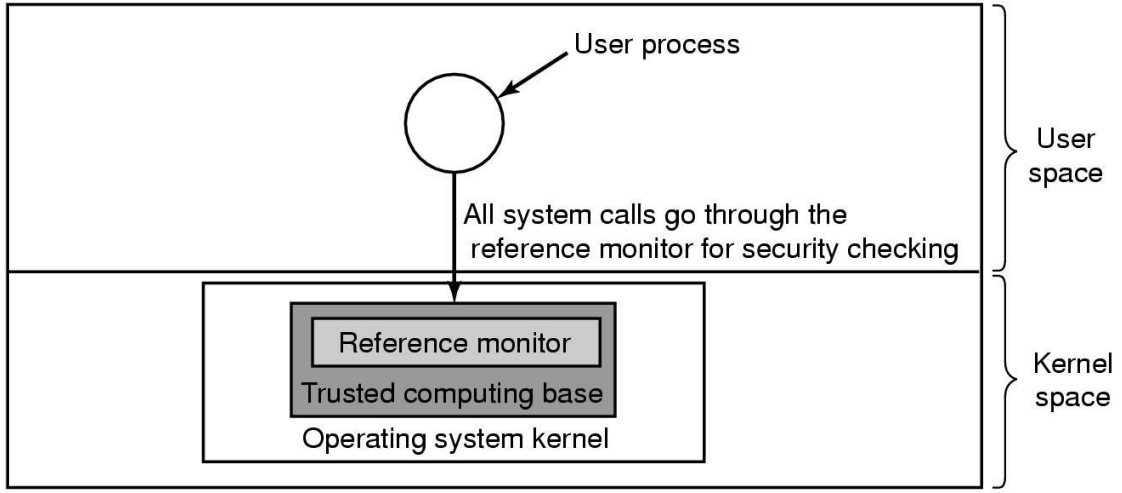
- **Cryptography**
  - shuffling a message or file in such a way that it becomes hard to recover the original data unless you have the key
  - to transmit data securely over the network, to store files securely on disk, to scramble the passwords in a password file, etc.
- Software **hardening**
  - adds protection mechanisms to programs to make it hard for attackers to make them misbehave
  - to prevent attackers from injecting new code into running software, to make sure that each process has exactly those privileges it needs to do what it is supposed to do and no more, etc.

Can we build secure systems?

- Is it possible to build a secure computer system?
  - In principle, software can be free of bugs and we can even verify that it is secure—as long as that software is not too large or complicated.
  - Unfortunately, computer systems today are horrendously complicated.
- If so, why is it not done?
  - People are not willing to leave what they are using, even if it's not secure
  - The only known way to build a secure system is to keep it simple. Features are the enemy of security.
  - But, today's feature-rich software have more complexity, more code, more bugs, and more security errors.

Trusted Computing Base (TCB)

- In the security world, people often talk about **trusted systems** rather than secure systems.
- These are systems that have formally stated security requirements and meet these requirements.
- At the heart of every trusted system is a minimal **TCB** (**Trusted Computing Base**) consisting of the hardware and software necessary for enforcing all the security rules.
- If the trusted computing base is working to specification, the system security cannot be compromised, no matter what else is wrong.

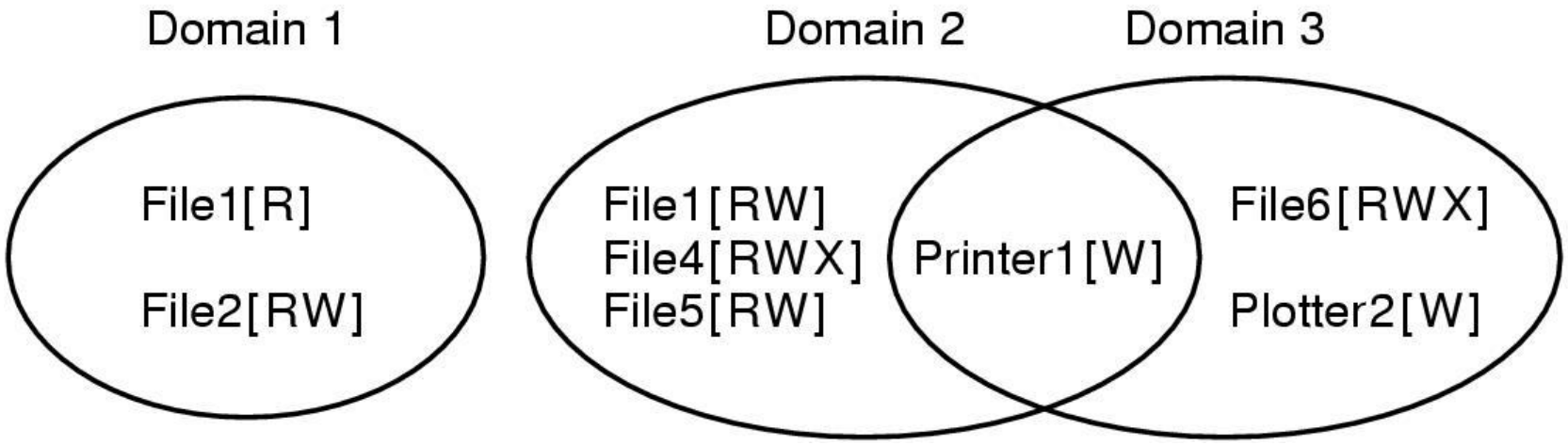


Controlling Access to Resources

- A computer system contains many resources, or ‘‘objects,’’ that need to be protected.
- These objects can be hardware (e.g., CPUs, memory pages, disk drives, or printers) or software (e.g., processes, files, databases, or semaphores).
- A model of what is to be protected and who is allowed to do what is necessary for the operating system.
- There are various models for doing this,
  1. Protection Domains
  2. Access Control Lists
  3. Capabilities

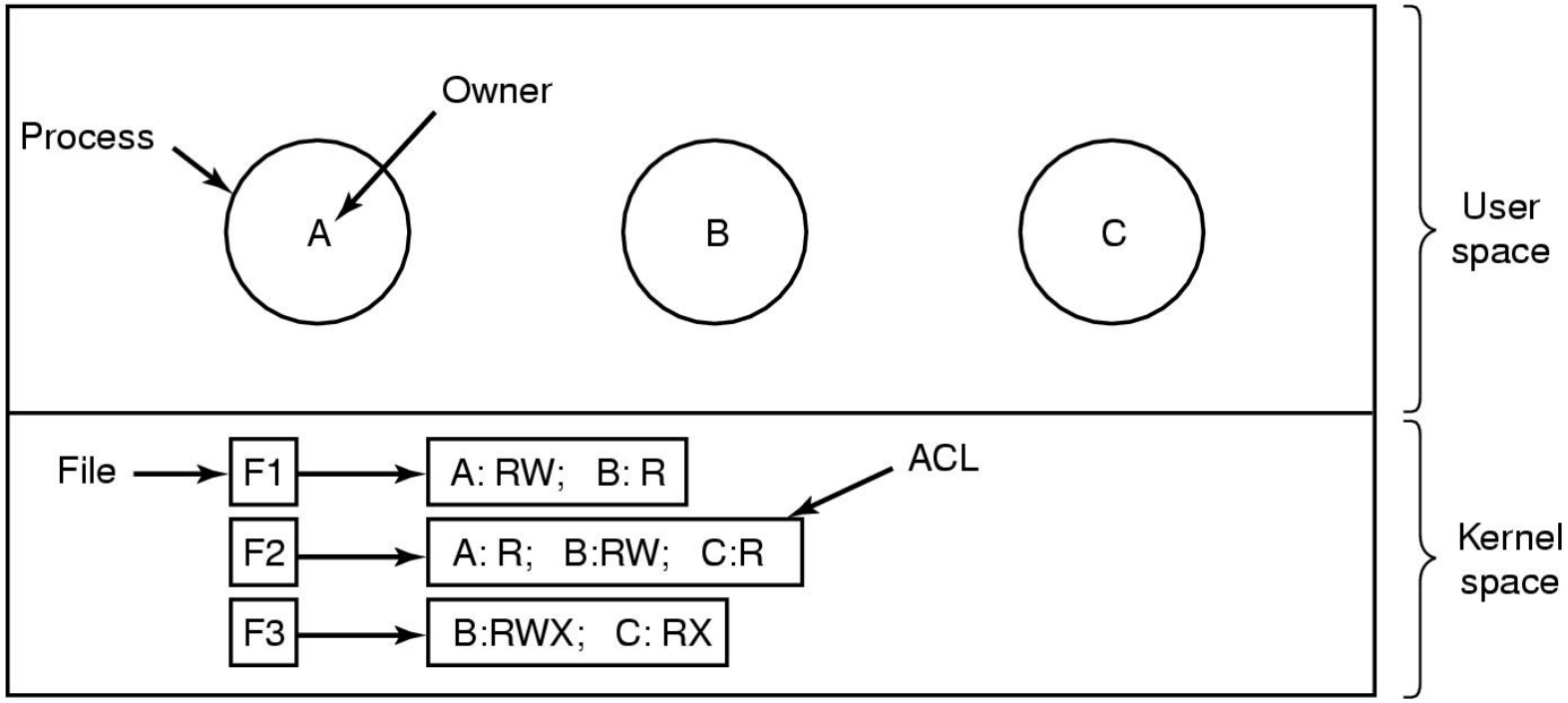
Protection Domains

- A **domain** is a set of (object, rights) pairs.
- Each pair specifies an object and some subset of the operations that can be performed on it.
- A **right** in this context means permission to perform one of the operations.
- E.g. Unix/Linux file permissions with UID/GID



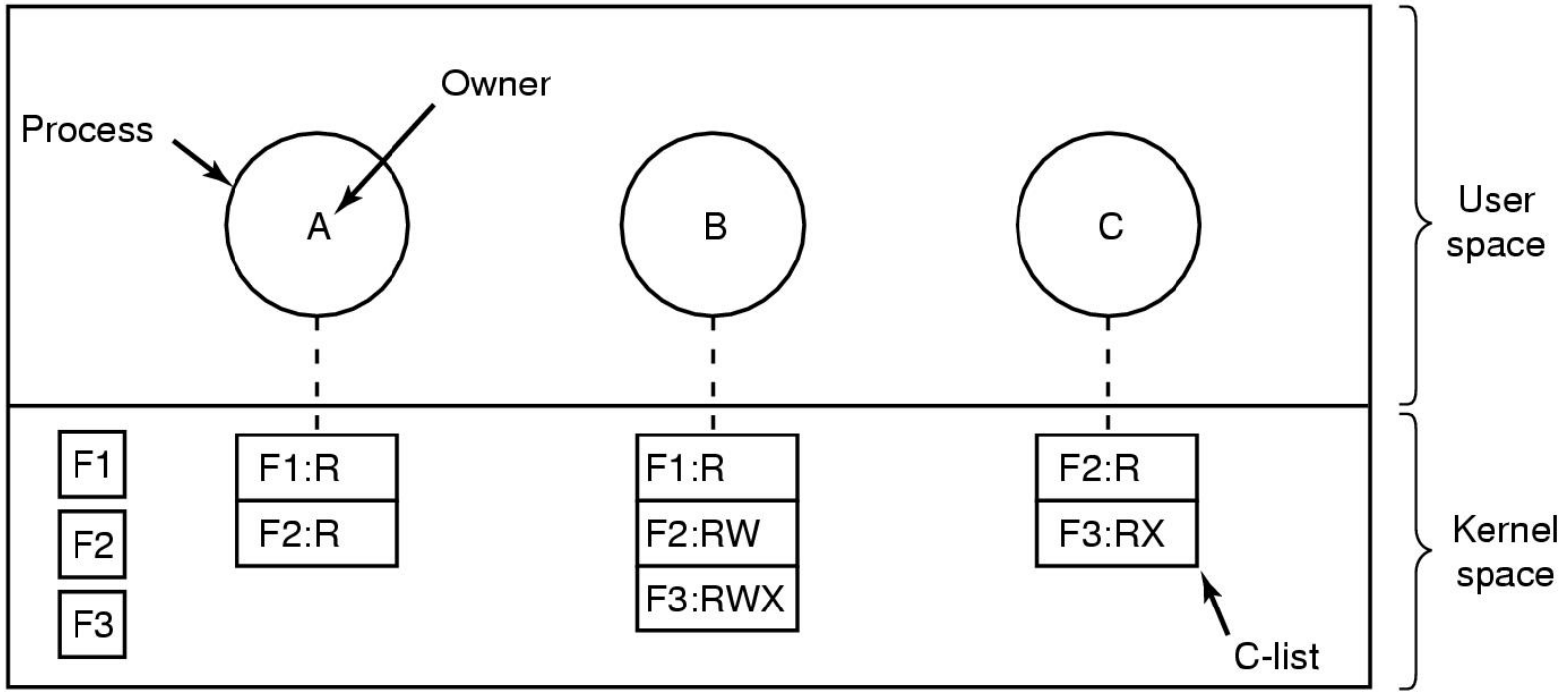
Access Control Lists

- An **Access Control List (ACL)** consists of associating with each object an (ordered) list containing all the domains that may access the object, and how.



Capabilities

- A **capability list** (or **C-list**) is a list of objects associated with each process that may be accessed, along with an indication of which operations are permitted on each, in other words, its domain.

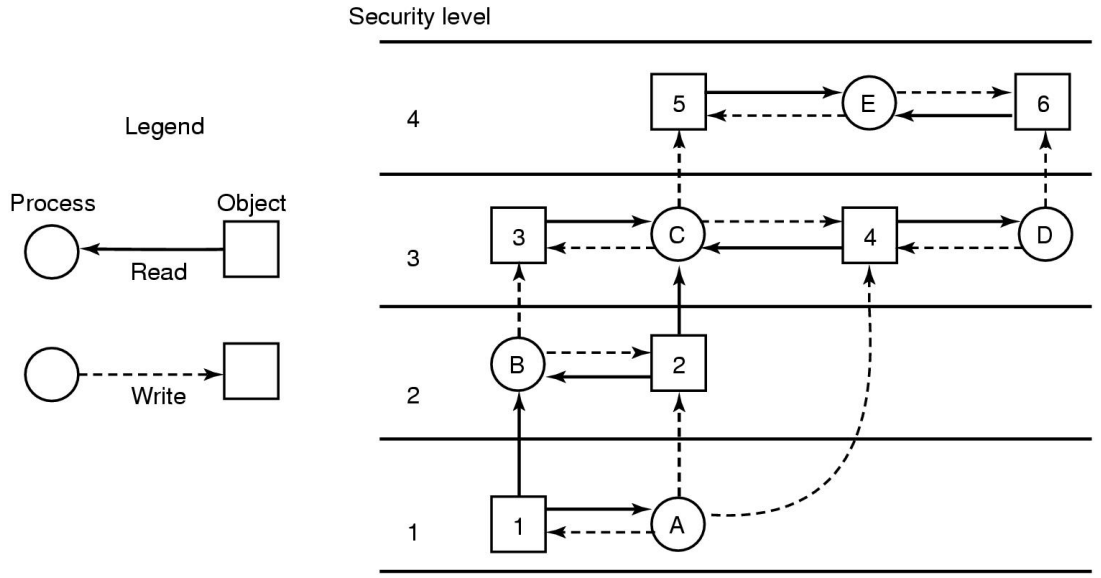


Formal Models of Secure Systems

- **Multilevel Security**
  - **discretionary access control**
    - operating systems allow individual users to determine who may read and write their files and other objects
  - **mandatory access controls**
    - the organization has stated rules about who can see what, and these may not be modified by individuals
  - operating systems must enforce the stated security policies, in addition to the standard discretionary access controls

Formal Models of Secure Systems

- **The Bell-La Padula Model**
- Rules for the Bell-La Padula model:
  - **The simple security property**:
    A process running at security level k can read only objects at its level or lower.
  - **The * property**: A process running at security level k can write only objects at its level or higher.



Formal Models of Secure Systems

- **The Biba Model**
- Rules for the Biba model:
  - **The simple integrity principle**: A process running at security level k can write only objects at its level or lower (no write up).
  - **The integrity * property**: A process running at security level k can read only objects at its level or higher (no read down).

Authentication

- Every *secured* computer system must require all users to be authenticated at login time.
- General principles of authenticating users:
  1. Something the user knows – Known things password, PIN
  2. Something the user has – Physical objects like smartcard, phone
  3. Something the user is – Biomatrices like fingerprint, iris scan

Authentication

- A key problem with password login is the use of weak passwords
- **Challenge-Response Authentication** is a variation on the password idea is to have each new user provide a long list of questions and answers that are then stored on the server securely, and asked for at the time of authentication
- Authentication Using a Physical Object or Authentication Using Biometrics can add additional layer of security to the authentication process

Exploiting Software

- One of the main ways to break into a user's computer is by exploiting vulnerabilities in the software running on the system to make it do something different than the programmer intended.
- These attacks can exploit various aspects of operating systems:
  - Buffer Overflow Attacks
  - Format String Attacks
  - Dangling Pointers
  - Null Pointer Dereference Attacks
  - Integer Overflow Attacks
  - Command Injection Attacks

Insider Attacks

- These are executed by programmers or employees of the company running the computer to be protected or making critical software.
- Logic Bombs
  - a piece of code written by one of a company's (currently employed) programmers and secretly inserted into the production system
  - in the event of their firing and absence of a daily input of password, the system can do any pre-programmed malicious actions
- Back Doors
  - a programmer could add code to the login program to allow anyone to log in using the login name ‘‘zzzzz’’ no matter what was in the password file
- Login Spoofing

Malware

- Malicious Software, commonly spread over the internet
- Can be used for a form of blackmail
- Example: Encrypts files on victim disk, then displays a message like

Greetings from General Encryption

To purchase a decryption key for your hard disk, please send $100 in small unmarked bills to Box 2154, Panama City, Panama.

Thank you. We appreciate your business.

Spyware

- Spyware is software that is stealthily loaded onto a PC without the owner's knowledge and runs in the background doing things behind the owner's back.
- Four common characteristics of spyware:
  1. It hides, so the victim cannot find it easily.
  2. It collects data about the user (Websites visited, passwords, even credit card numbers).
  3. It communicates the collected information back to its distant master.
  4. It tries to survive determined attempts to remove it.

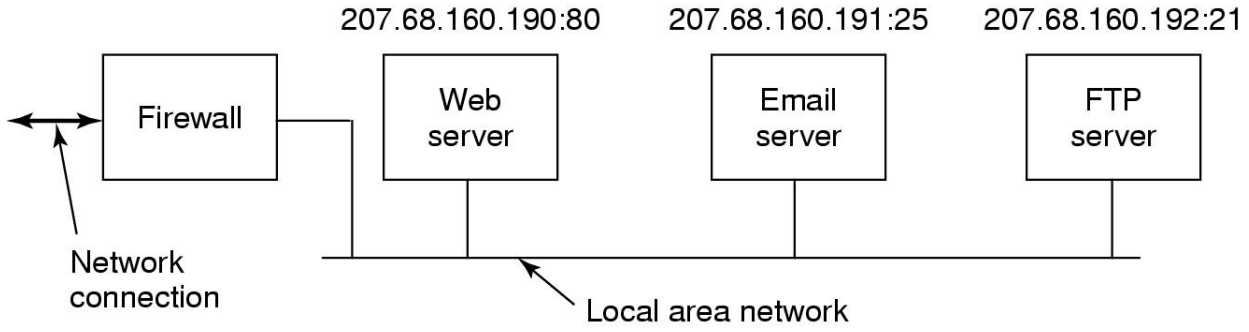
Types of Viruses

- Companion virus
- Executable program virus
- Parasitic virus
- Memory-resident virus
- Boot sector virus
- Device driver virus
- Macro virus
- Source code virus

Defences

- **Defence in depth:**
  - there should be multiple layers of security so that if one of them is breached, there are still others to overcome
- There are various layers of security that can be applied to an OS:
  - Firewalls
  - Anti Virus
  - Code Signing
  - Jailing
  - Model-based Intrusion Detection
  - Sandboxing

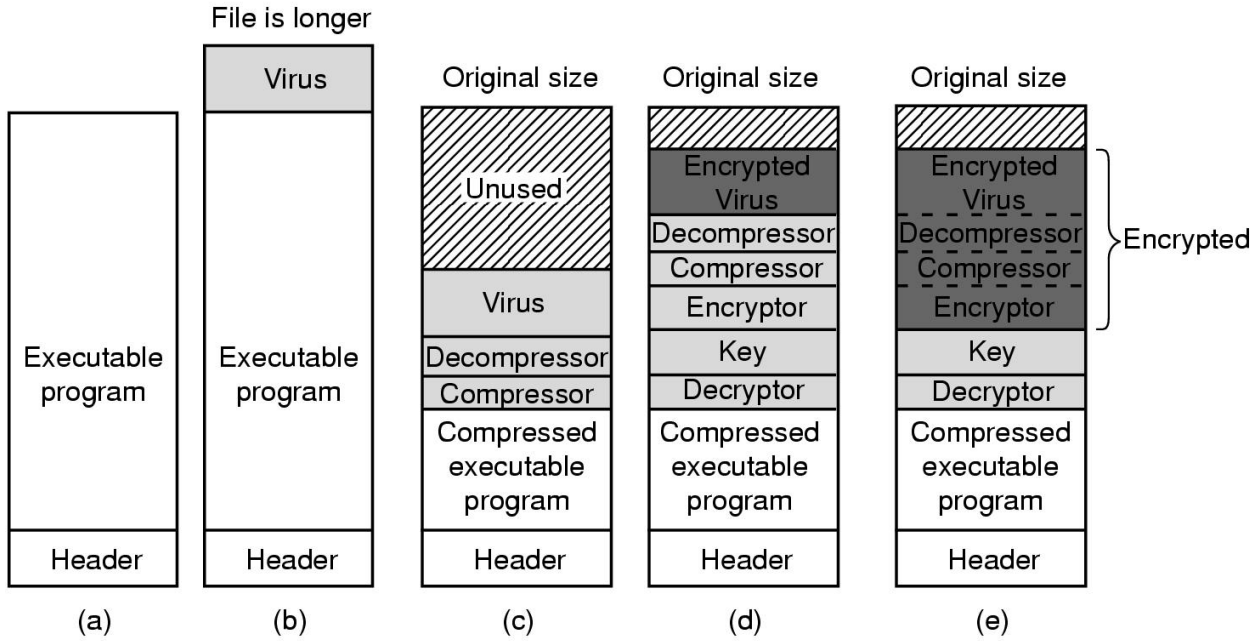
Firewalls



- Being connected to the Internet exposes a computer to two kinds of dangers: incoming and outgoing.
- Thus, mechanisms are needed to keep ‘‘good’’ bits in and ‘‘bad’’ bits out.
- All traffic in or out must go through a **firewall**, where they could be inspected against predefined rules or policies.
- Firewalls come in two basic varieties: hardware and software.
- Firewalls are configured with rules describing what is allowed in and what is allowed out.

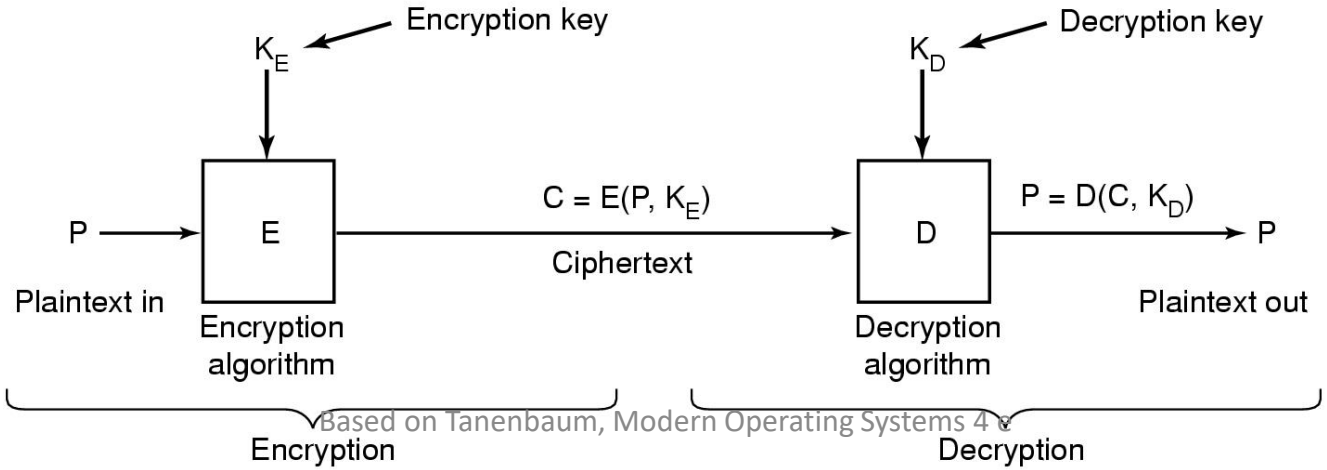
Antivirus

- Have a new virus infect a program that does nothing, often called a **goat file**, to get a copy of the virus in its purest form.
- Make an exact listing of the virus' code and enter it into the database of known viruses.
- Scan every executable file on the disk looking for any of the viruses in the database of known viruses.



Basic Cryptography

- Cryptography plays an important role in security and operating systems use cryptography in many places.
  - Some file systems can encrypt all the data on disk
  - Protocols like IPSec may encrypt and/or sign all network packets
  - Most operating systems scramble authentication passwords
- Take a message or file, called the **plaintext**, and encrypt it into **ciphertext** in such a way that only authorized people know how to convert it back to plaintext.



Secret-Key Cryptography

- Monoalphabetic substitution:
  - Plaintext: `ABCDEFGHIJKLMNOPQRSTUVWXYZ`
  - Ciphertext: `QWERTYUIOPASDFGHJKLZXCVBNM`
  - Plaintext `ATTACK` would be transformed into the ciphertext `QZZQEA`
  - Decryption key: `KXVMCNOPHQRSZYIJADLEGWBUFT`
- Given the encryption key it is easy to find the decryption key.
  - With a small amount of ciphertext, the cipher can be broken.
  - Symmetric-key cryptography
- The basic attack takes advantage of the statistical properties of natural languages.
  - In English, for example, *e* is the most common letter, followed by *t*, *o*, *a*, *n*, *i*, etc. The most common two-letter combinations, called **digrams**, are *th*, *in*, *er*, *re*, and so on.
- Also, sender and receiver must both be in possession of the shared secret key.

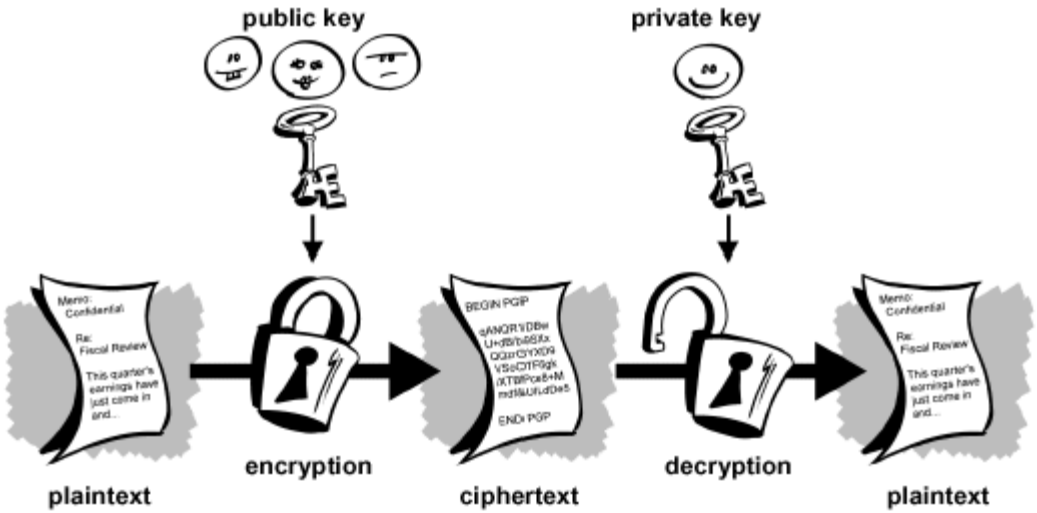
Public-Key Cryptography

- In this system, distinct keys are used for encryption and decryption.
- Given a well-chosen encryption key, it is virtually impossible to discover the corresponding decryption key.
- Encryption makes use of an "easy" operation, such as how much is `3141592653589 79 × 3141592653589 79`?
- Decryption without the key requires you to perform a hard operation, such as what is the square root of `3912571506419387090594828508241`?
- The main problem with public-key cryptography is that it is a thousand times slower than secret-key cryptography.

- Public-Key Cryptography - https://www.youtube.com/watch?v=GSIDS_lvRv4
- Instant Messaging and the Signal Protocol - https://www.youtube.com/watch?v=DXv1boalsDI

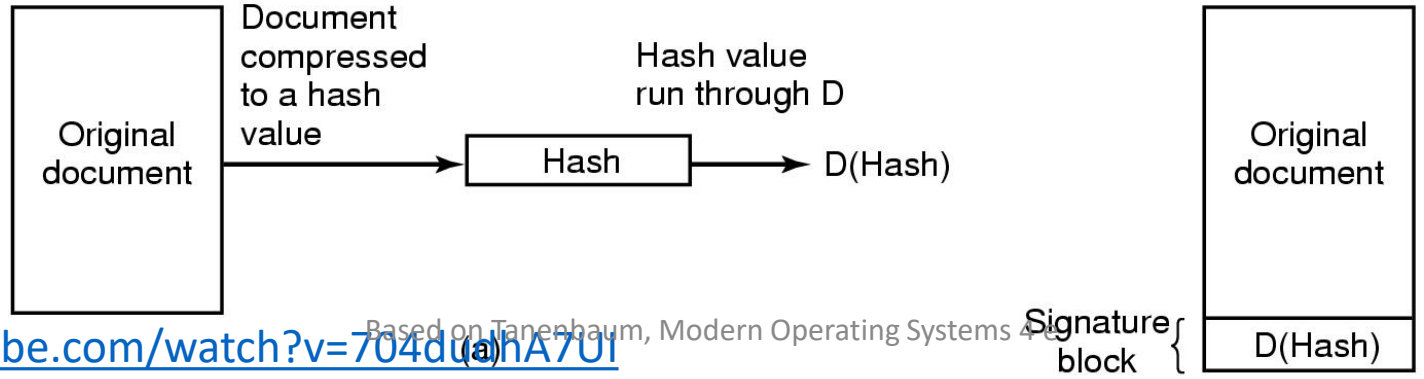
Public-Key Cryptography

- The way public-key cryptography works is that everyone picks a (public key, private key) pair and publishes the public key.
- The public key is the encryption key; the private key is the decryption key.
- To send a secret message to a user, a correspondent encrypts the message with the receiver's public key.
- Since only the receiver has the private key, only the receiver can decrypt the message.



Digital Signatures

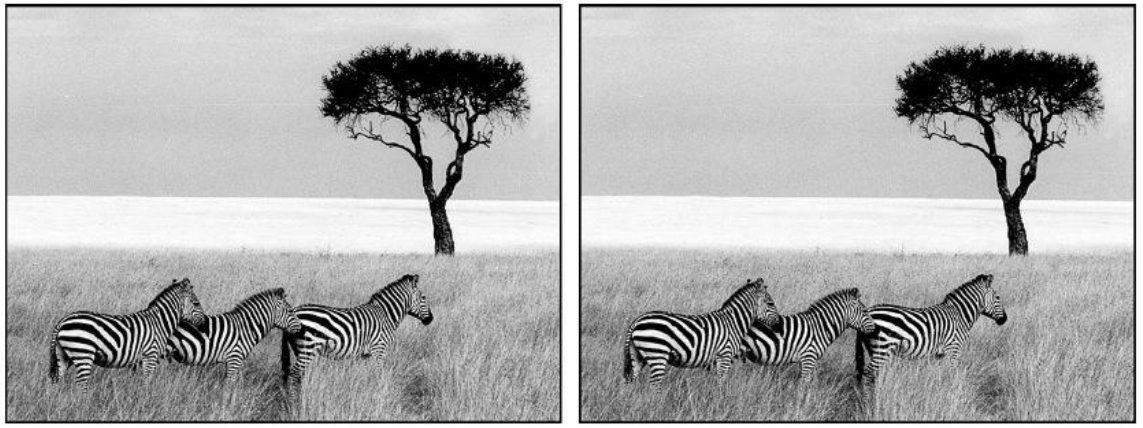
- Digital signatures make it possible to sign emails and other digital documents in such a way that they cannot be repudiated by the sender later.
- One common way is to first run the document through a one-way cryptographic hashing algorithm that is very hard to invert.
- The hashing function typically produces a fixed-length result independent of the original document size.
- The most popular hashing functions used is **SHA-1** (**Secure Hash Algorithm**), which produces a 20-byte result (NIST, 1995).



https://www.youtube.com/watch?v=704duUhA7UI

Steganography

- Steganography is the practice of concealing a file, message, image, or video within another file, message, image, or video.
- Steganography can be used to leak information in a covert way, but it is more common that we want to do the opposite: hide the information from the prying eyes of attackers, without necessarily hiding the fact that we are hiding it.



(a) (b)

- https://www.youtube.com/watch?v=TWEXCYQKyDc