Security (Part 2)

Operating Systems

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.

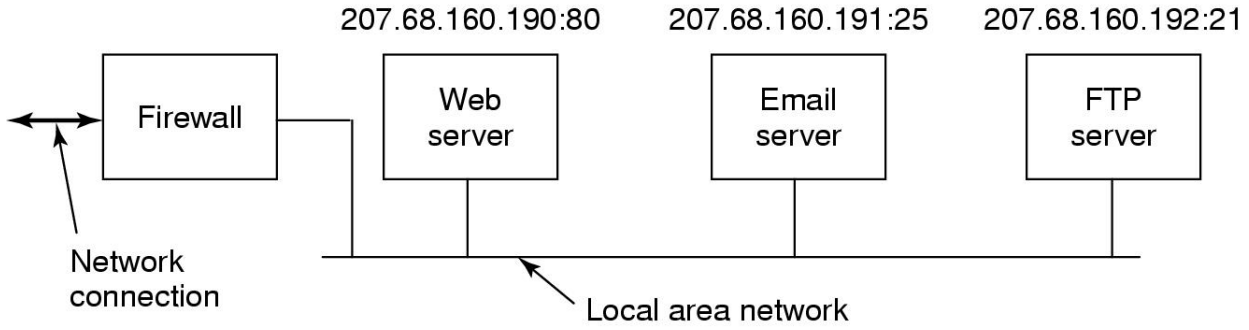
Types of Viruses

- 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

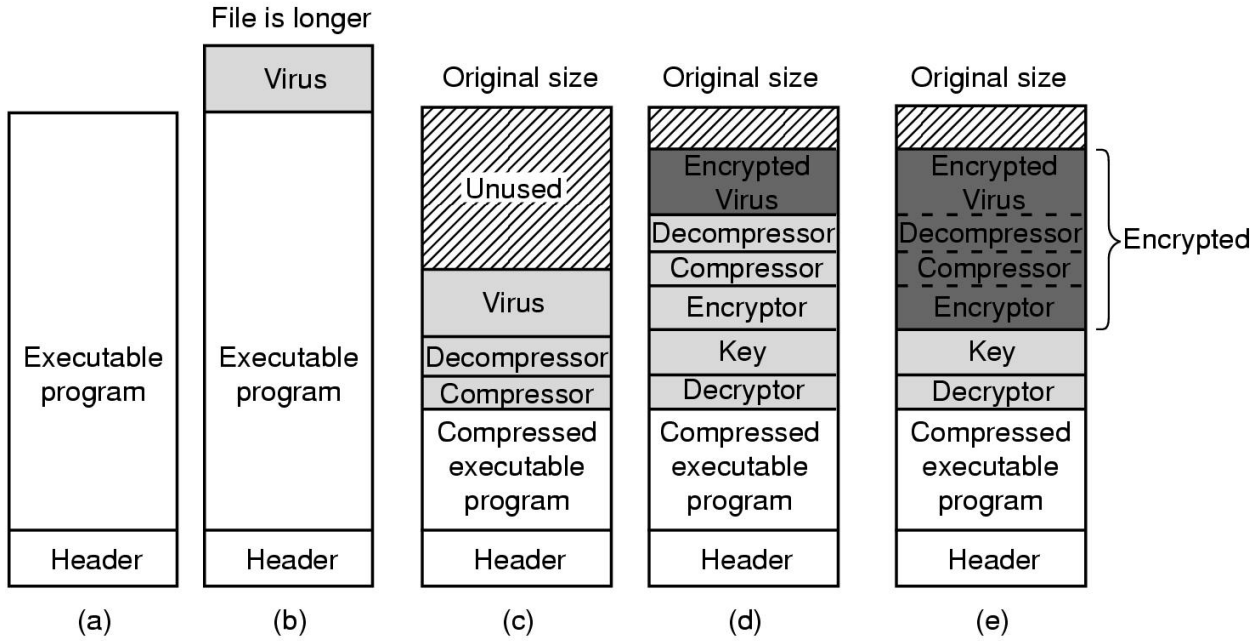
Firewalls



- 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.

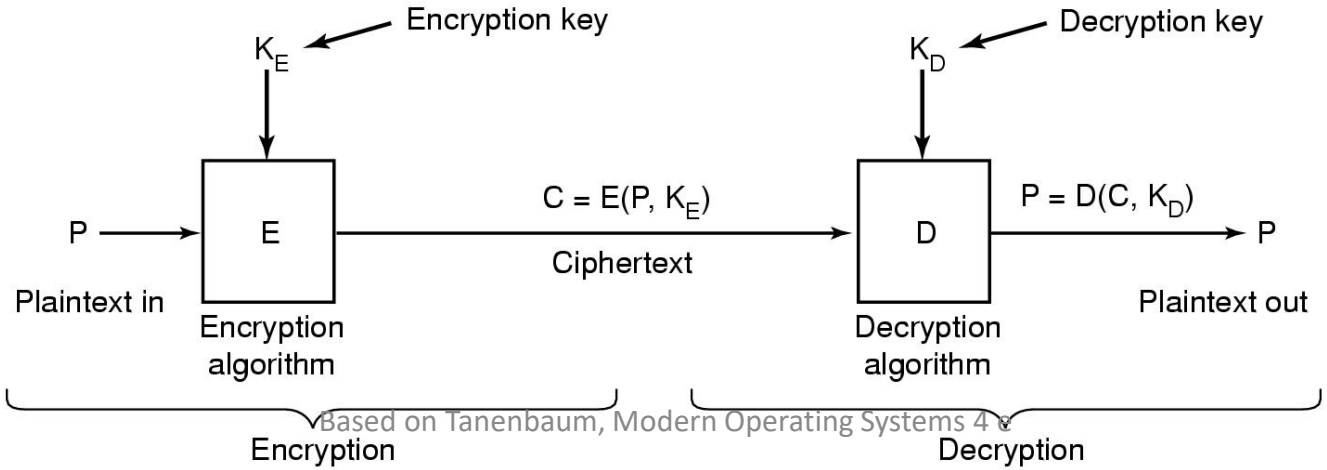
Antivirus

- 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.

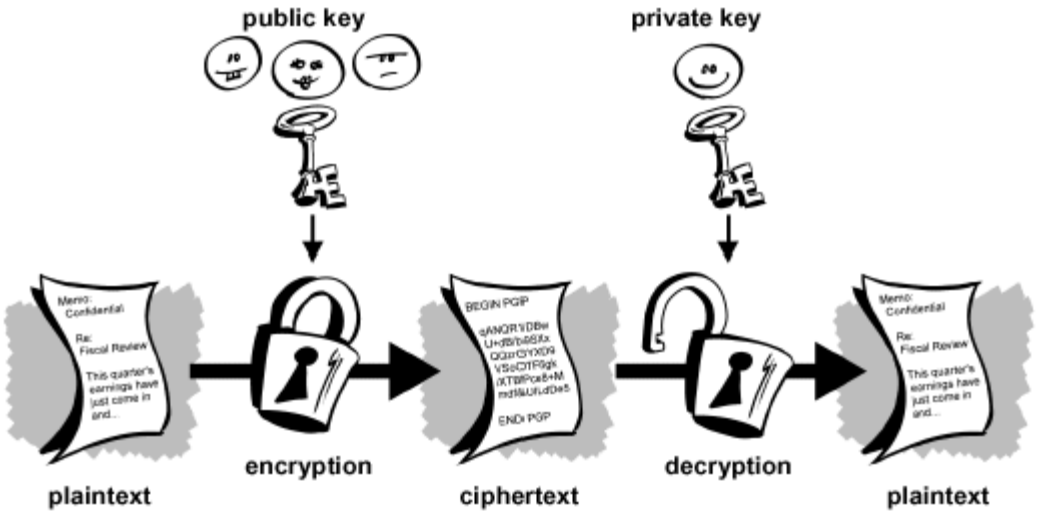
Public-Key Cryptography

- 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 × 3141592653589`?
- Decryption without the key requires you to perform a hard operation, such as what is the square root of `9869604401089358618834490999876151135313699407240790626413349383064462809`?
- 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

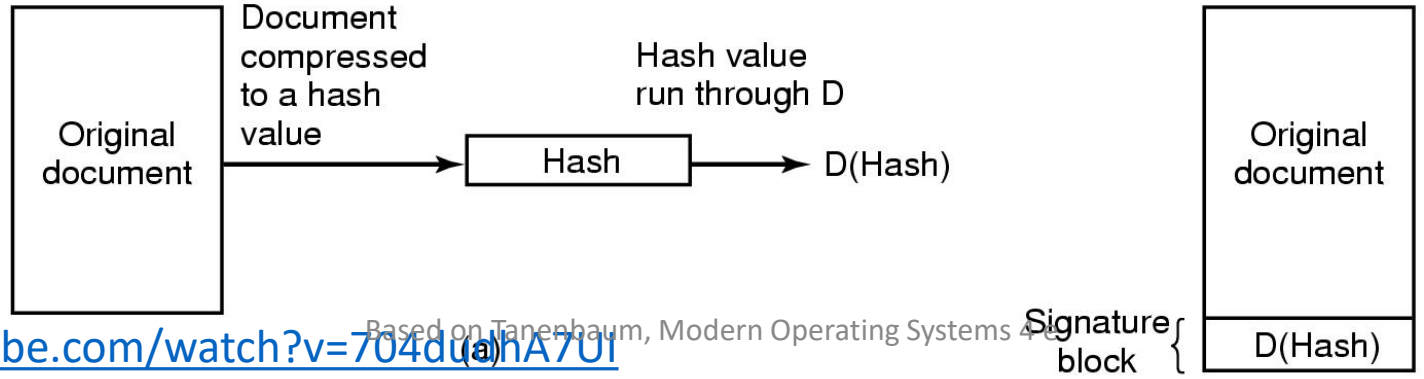
Public-Key Cryptography

- 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

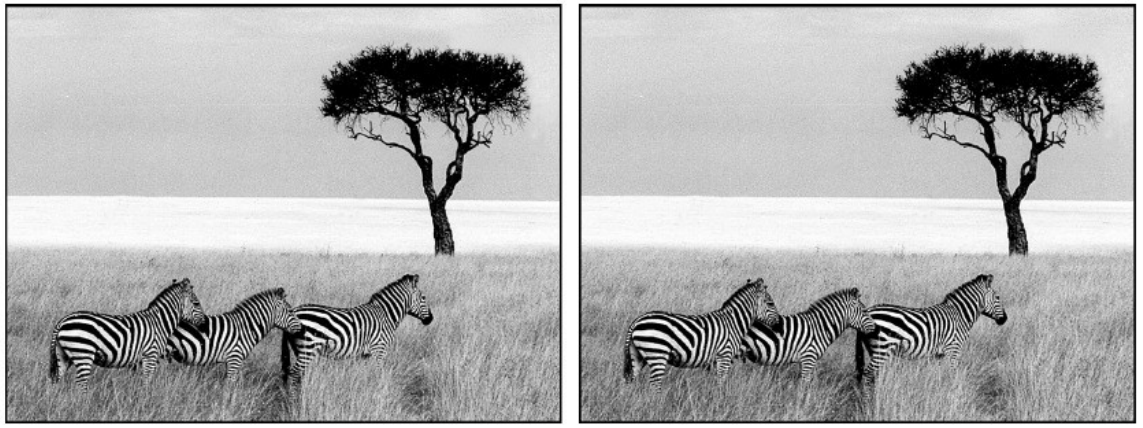
- Digital signatures make it possible to sign emails and other digital documents in such a way that they cannot be repudiated by the sender later.
- One common way is to first run the document through a one-way cryptographic hashing algorithm that is very hard to invert.
- The hashing function typically 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