

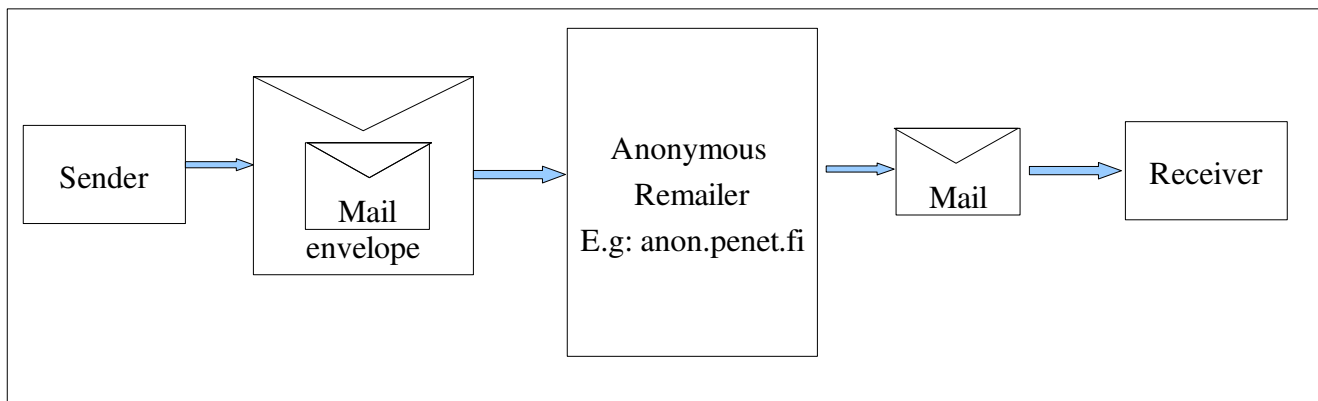
Famous Security Bugs:

1. Wireless WEP off by default:

- Earlier for most wireless routers has WEP(Wireless Equivalent Privacy) was off by default.
- Major security loophole. Silent Failure
- Breaks : **Failure by Default** principle.

2. Anonymous Remailer:

- Used to send anonymous E-mails that is to hide sender's identity.



- Sender sends email message encrypted in an envelope which can be only decrypted by remailer.
- Anonymous remailer forwards an incoming mail without revealing the source for that mail.
- It is possible to identify the sender by breaking into anonymous remailer.
- Anonymous remailer is fallible.
- Breaks : **Separation of privilege** principle.
- Solution: use multiple anonymous remailer (using cascading) to hide sender's identity.
- It is unlikely to break through all anonymous remailers to reveal sender's identity.

3. Canonicalization:

- It's a web server attack.
- Web sever has two sections,
public readable files and
private files which are accessible within organization based to authentication.
- Webserver configuration file (example):

public : /var/www/*

private : /var/intranet/*

- If attacker can use path like '/var/www/./intranet/secrete-file' to get access to a vital private information.
- Since web servers rules are defined using regular expression and wild cards, vulnerability depends on implementation.
- Violates : **complete mediation** principle
- Possible solutions:
 1. Defines explicit list of files which are world readable. But this is tedious and does not help in case of dynamically generated web pages.
 2. Apache now uses .htaccess file per directory. This file defines access for each directory and this file resides in the same directory. So no matter how attacker specifies the path, correct authentication rules will be read.

4. Network File system (NFS):

- This is a protocol used for accessing remote files as if they are local.
- When NFS client sends mount request to NFS server, server performs the authentication based on the policies and then sends a 32 bit root file handle to client.
- Further access to files only requires root file handle and server does not refer to any policies during file open, read, write, etc
- Easy to access private information by guessing file handle which is only 32 bit.
- Violates : **complete mediation** principle

5. Tracker Beaming

- Attack on a popular FTP server(wuftp) written by Washington University
- FTP server has 2 modes : nobody and root
- Mostly FTP server runs in nobody mode and occasionally uses root mode for some privileged operations.

The code which switches from nobody to root mode was:

```
setuid() // uid of root on Unix OS is 0
//do the privilege operation
setuid(-1)

sgoob() //out of band handler
{
    // not written to run as root
}
```

- The TCP has special Out of Band packet delivery mechanism which is used to send out of order packets. Arrival of such packet was indicated using interrupt.
- If attacker send an out of band TCP packet when FTP server is doing some privilege

operation, then FTP server will get interrupted when it is running as root.

- Now the Out of band interrupt handler is not written to run as a root. Moreover it was written in a manner that it break the execution sequence and hence after interrupt handler control does not return to same place therefore FTP server never switches back to normal (nobody) mode. So now all private data on server is accessible to attacker.
- Violates : **Least Privilege** principle
: **Economy of Mechanism** Principle

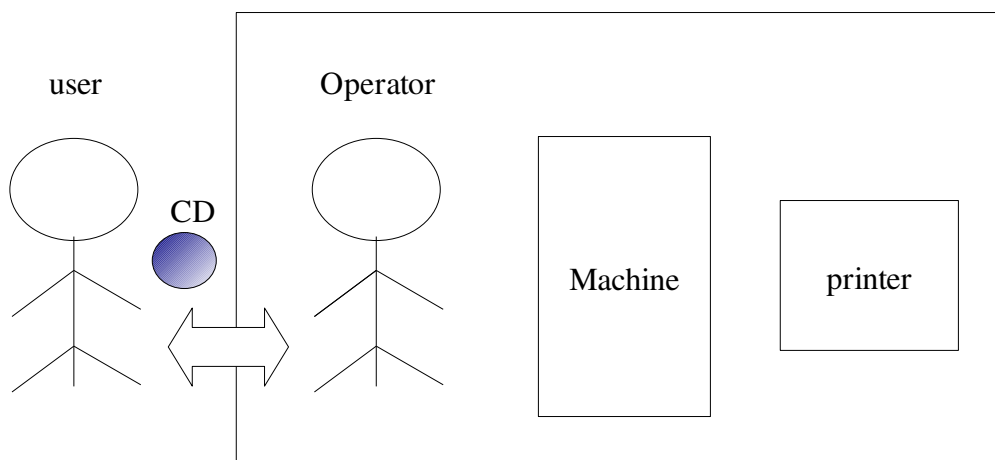
6. Related to Internet Explorer(IE)

- IE's html rendering facility was available to other application as DLL.
- In browser mode, javascript engine has limited access to local file system but in other modes it has complete access to local file systems
- Eudora Mail client : uses IE DLL to display email messages.
- Javascript engine has complete access to file system while displaying mails and Attacker exploited this loophole.
- Example of security loophole, after integration of two applications which are secure while running independently.
- Violates : **Least shared mechanism** principle
: **Open Design** Principle
: **Complete mediation** Principle

Trends in Computer Science:

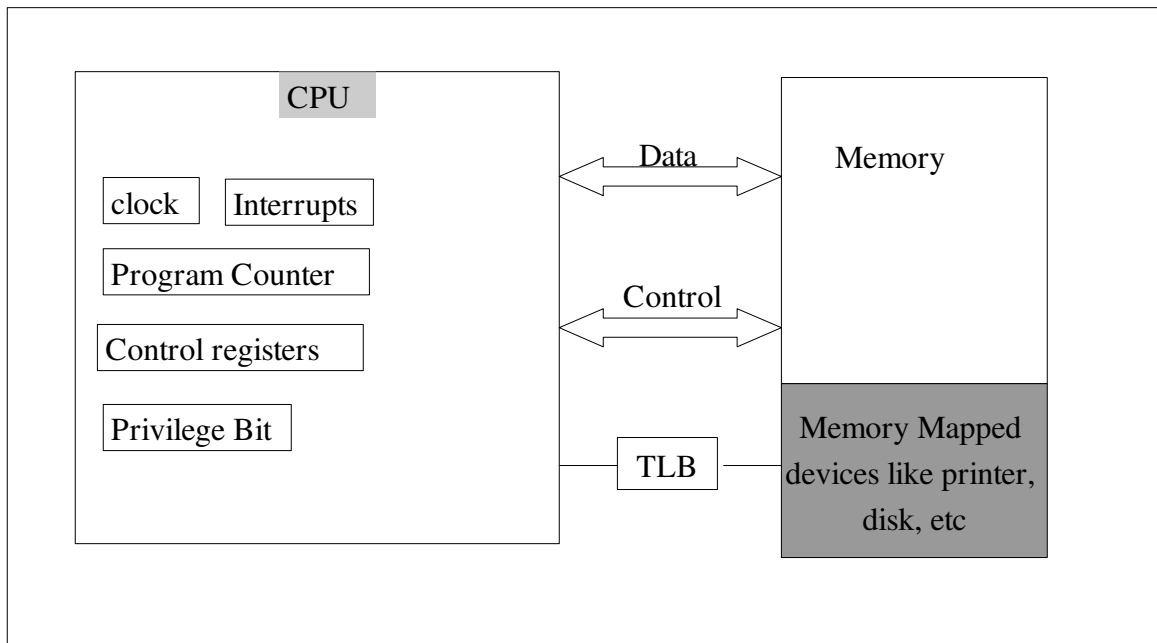
Isolation --> Multiprogramming --> RPC (Remote Procedure Calls) --> Mobile Code --> Mashups

Highly Secure Systems:



- User gives CD to operator, and then operator prints the user data and hands it back to user
- For each user, operator first restarts the machine
- Each user is allowed to use the machine for maximum 1 hour at a time.
- Assumption:
 1. Operator is infallible.
 2. Room is secure
 3. Room has visual privacy
- Pretty much secure system
- Satisfies security goals: Confidentiality, Integrity & Availability

Real Simple Machine (Hardware)



- All devices are memory mapped
- TLB (translation Lookaside Buffer): It contains the virtual to physical address mapping.
- Privilege mode : 0 => high , 1 => low
- Access to TLB, interrupt control, etc if privilege mode is 0.
- OS will run in privilege 0 mode.
- Supports multiple programs.