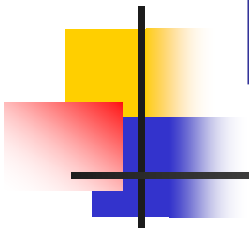


CS423 Operating Systems Security



Multi-level Security

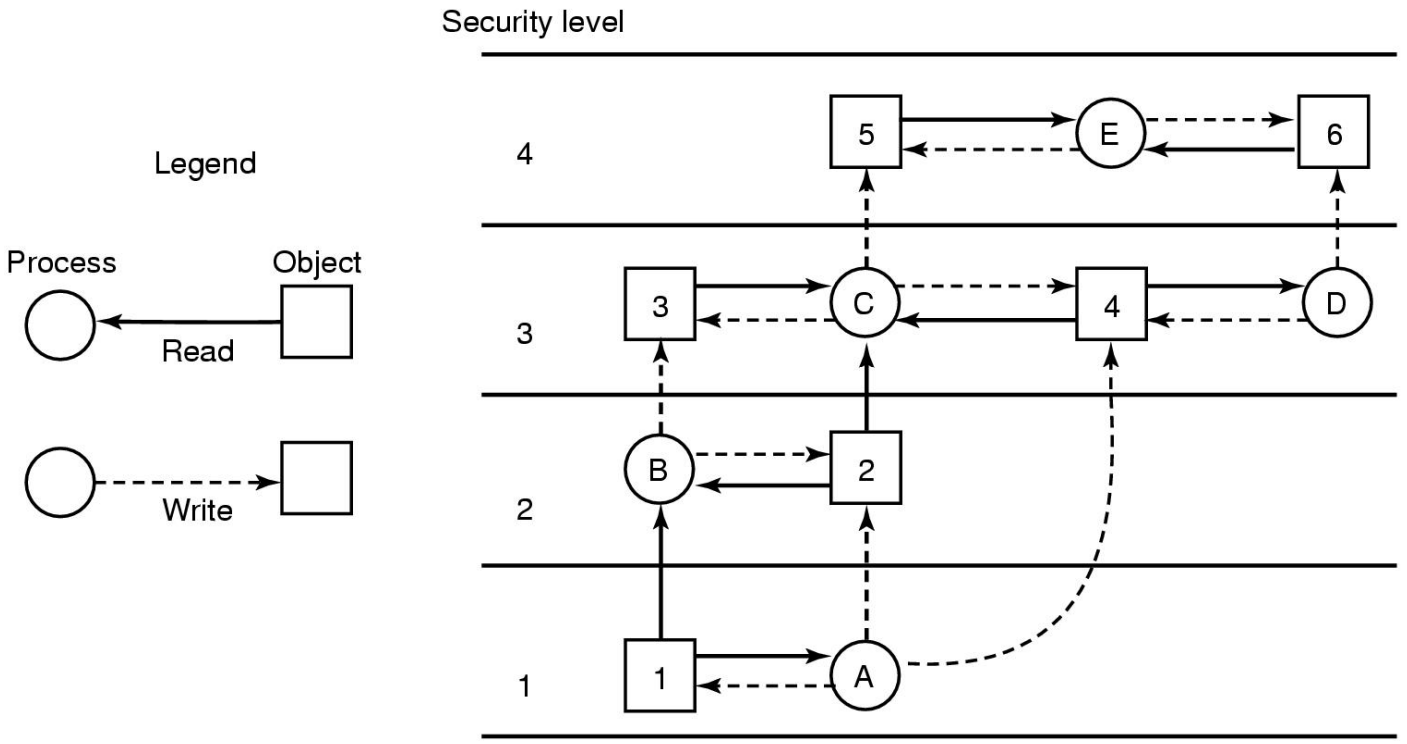
Rules for the Bell-La Padula model:

The simple security principle: 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.

Tanenbaum, Modern Operating Systems, Prentice-Hall, Inc. All rights reserved. 0-13-**6006639**

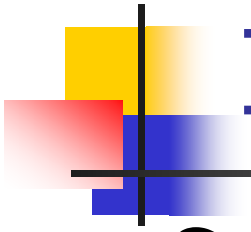
Information Flow



The Bell-La Padula multilevel security model.

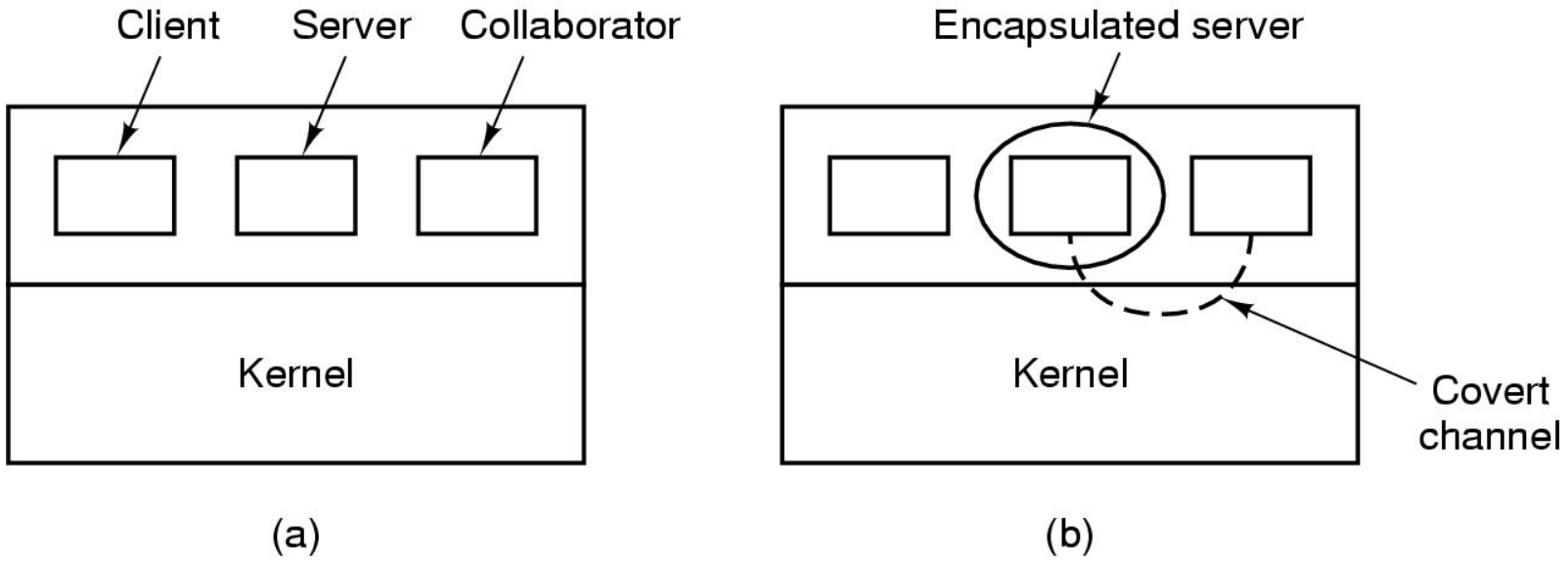
Tanenbaum, Modern Operating Systems, Prentice-Hall, Inc. All rights reserved. 0-13-**6006639**

Is This Enough to Prevent Information Leaks?



- Consider two processes of different security levels on the same machine
- Can an "un-loyal" high-security process leak information to a low-security process?
  - Remember:
    - The high-security process cannot write objects at a security level lower than itself
    - The low-security process cannot read objects at a level higher than itself (which means it cannot read any objects written by the higher-security process)

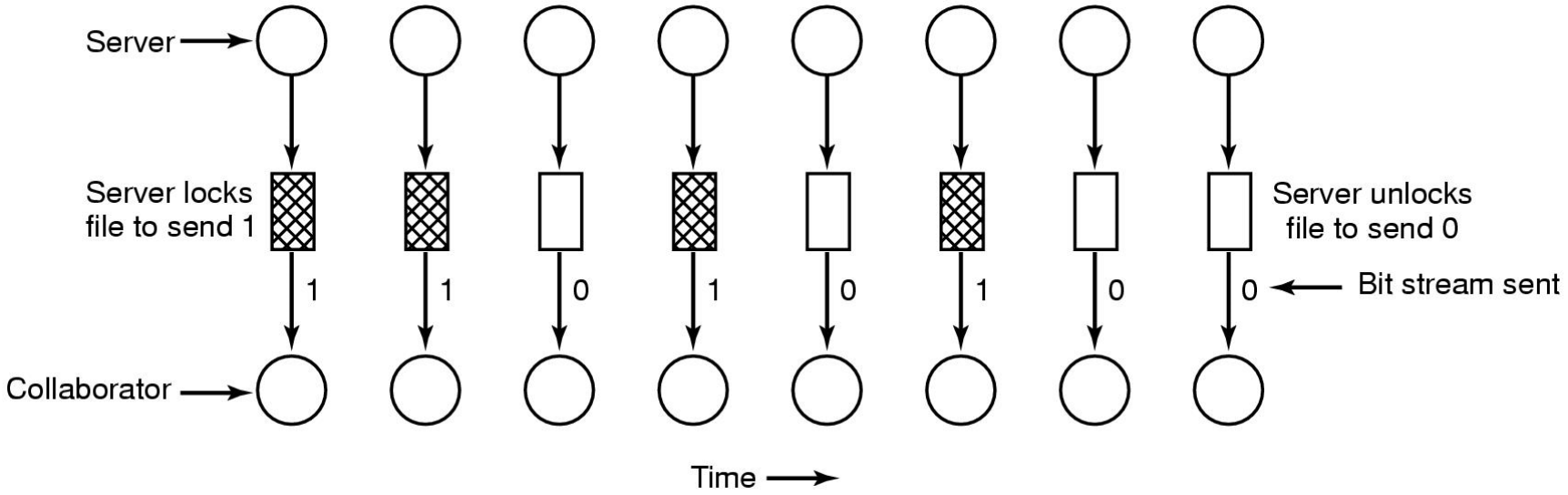
Covert Channels



(a) The client, server, and collaborator processes. (b) The encapsulated server can still leak to the collaborator via covert channels.

Tanenbaum, Modern Operating Systems, Prentice-Hall, Inc. All rights reserved. 0-13-**6006639**

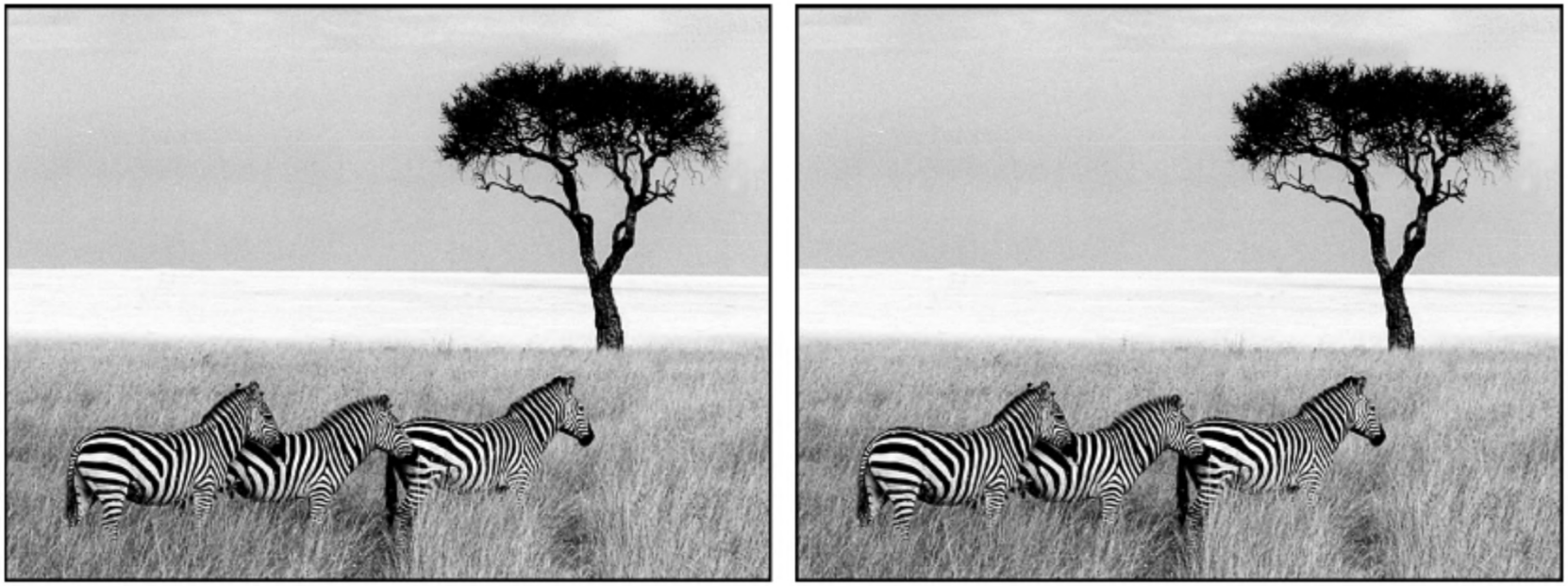
Covert Channels



A covert channel using file locking.

Tanenbaum, Modern Operating Systems, Prentice-Hall, Inc. All rights reserved. 0-13-**6006639**

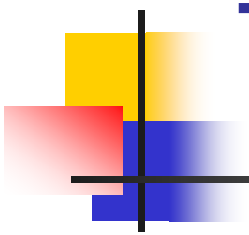
Covert Channels



(a) (b)

(a) Three zebras and a tree. (b) Three zebras, a tree, and the complete text of five plays by William Shakespeare.

Tanenbaum, Modern Operating Systems, Prentice-Hall, Inc. All rights reserved. 0-13-**6006639**



The BIBA Model

Rules for the Biba model:

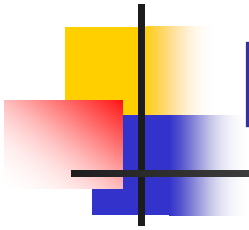
The simple integrity principle: A process running at security level k can write only objects at its level or lower (no write up).

The integrity * property: A process running at security level k can read only objects at its level or higher (no read down).

What does this guarantee?

Tanenbaum, Modern Operating Systems, Prentice-Hall, Inc. All rights reserved. 0-13-**6006639**

User Authentication (to the Machine)



General principles of authenticating users:

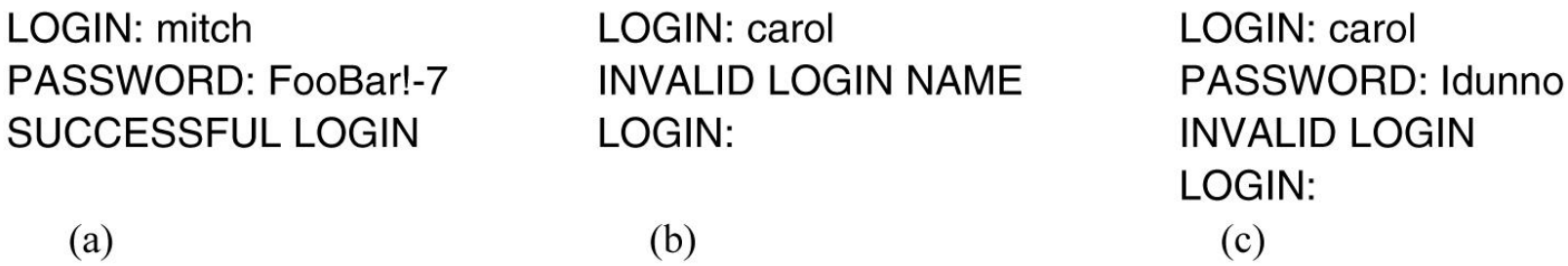
Something the user knows.

Something the user has.

Something the user is.

Tanenbaum, Modern Operating Systems, Prentice-Hall, Inc. All rights reserved. 0-13-**6006639**

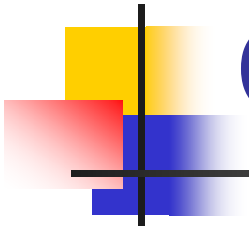
Authentication Using Passwords



(a) A successful login.
(b) Login rejected after name is entered.
(c) Login rejected after name and password are typed.

Tanenbaum, Modern Operating Systems, Prentice-Hall, Inc. All rights reserved. 0-13-**6006639**

Authentication Using Challenge-response



The questions should be chosen so that the user does not need to write them down.

Examples:

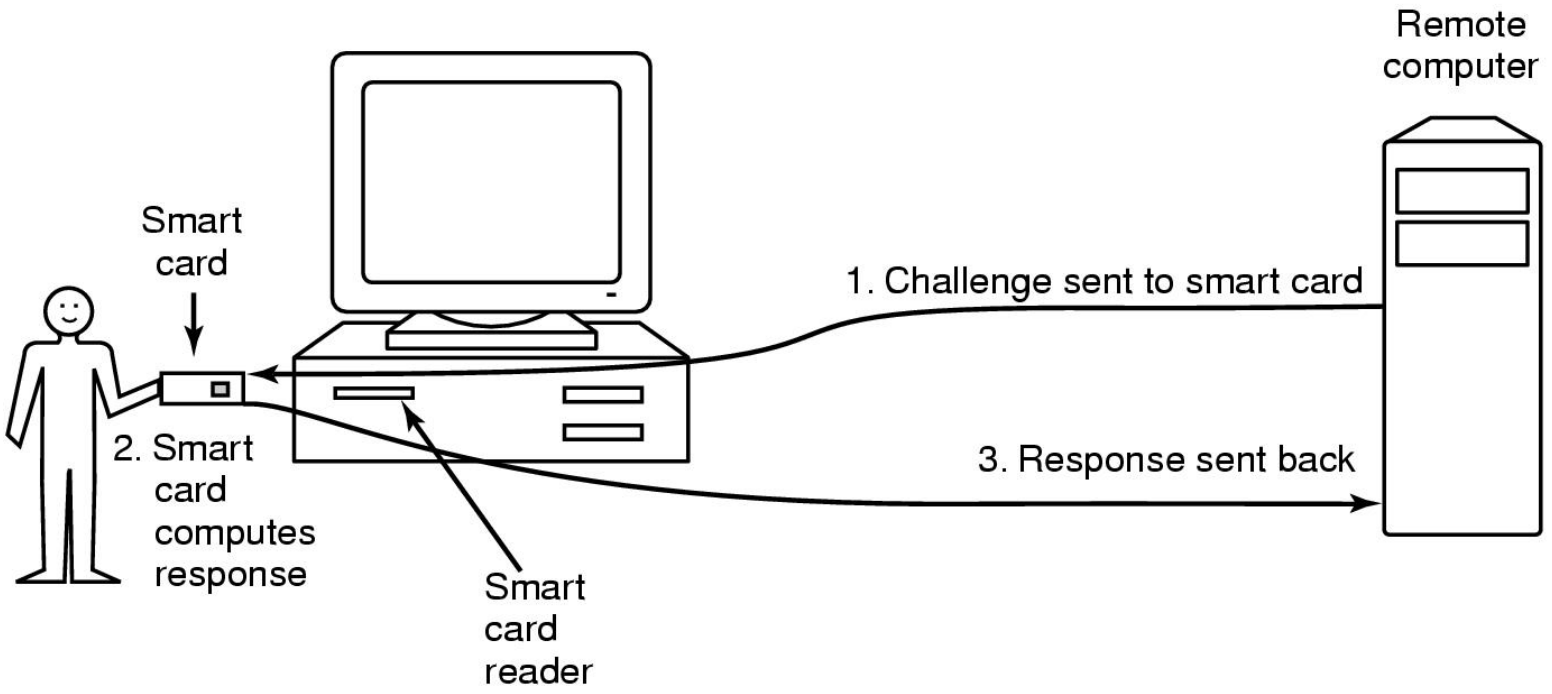
Who is Marjolein's sister?

On what street was your elementary school?

What did Mrs. Woroboff teach?

Tanenbaum, Modern Operating Systems, Prentice-Hall, Inc. All rights reserved. 0-13-**6006639**

Authentication Using A Physical Object



Use of a smart card for authentication.

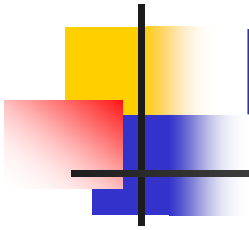
Tanenbaum, Modern Operating Systems, Prentice-Hall, Inc. All rights reserved. 0-13-**6006639**

Authentication Using Biometrics



Tanenbaum, Modern Operating Systems, Prentice-Hall, Inc. All rights reserved. 0-13-**6006639**

Is Authentication Using Biometrics a Good idea?



- Pros?
- Cons?

Is Authentication Using Biometrics a Good idea?

- Pros?
- Cons?
  - Hard to "change the password"



Insider Attacks on Authentication: Trap Doors

```
while (TRUE) {
        printf("login: ");
        get_string(name);
        disable_echoing( );
        printf("password: ");
        get_string(password);
        enable_echoing( );
        v = check_validity(name, password);
        if (v) break;
}
execute_shell(name);
```

(a)

```
while (TRUE) {
        printf("login: ");
        get_string(name);
        disable_echoing( );
        printf("password: ");
        get_string(password);
        enable_echoing( );
        v = check_validity(name, password);
        if (v || strcmp(name, "zzzzz") == 0) break;
}
execute_shell(name);
```

(b)

(a) Normal code. (b) Code with a trap door inserted.

Tanenbaum, Modern Operating Systems, Prentice-Hall, Inc. All rights reserved. 0-13-**6006639**

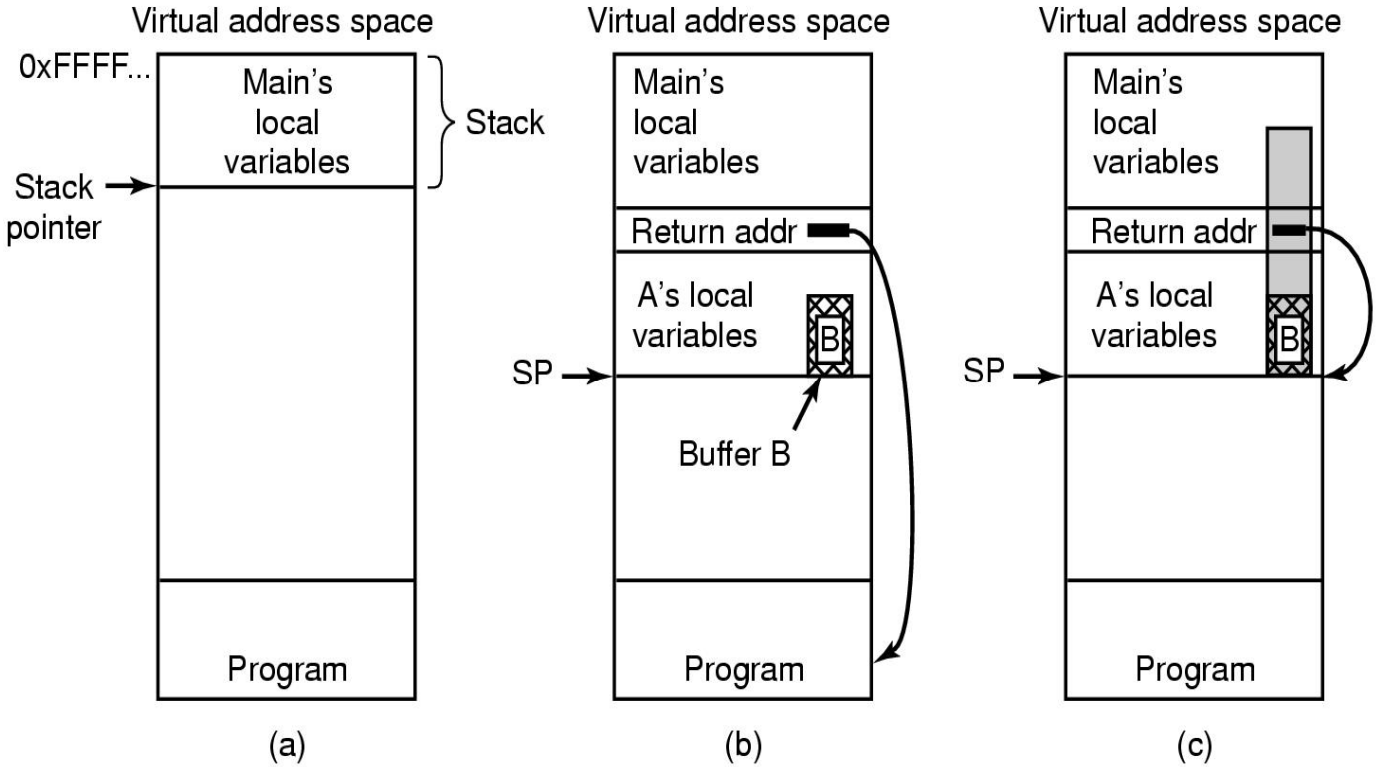
Phishing Attacks and Login Spoofing



(a) Correct login screen. (b) Phony login screen.

Tanenbaum, Modern Operating Systems, Prentice-Hall, Inc. All rights reserved. 0-13-**6006639**

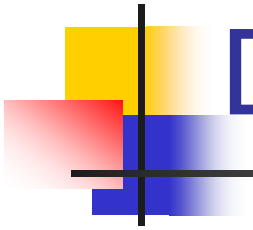
Other Attacks to Gain Unauthorized Access:
Buffer Overflow Attacks



(a) Situation when the main program is running.
(b) After the procedure A has been called.
(c) Buffer overflow shown in gray.

Tanenbaum, Modern Operating Systems, Prentice-Hall, Inc. All rights reserved. 0-13-**6006639**

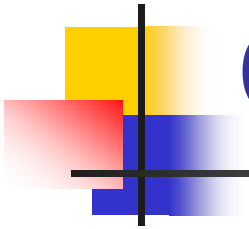
Attacks to Prevent Authorized Access: Denial of Service Attacks



- Attempt to overload the machine (typically with processing of incoming traffic)
- Solution:
  - Network-level: Change the paradigm from push-based to pull-based
  - OS-level: Perform early de-multiplexing and drop unsolicited traffic

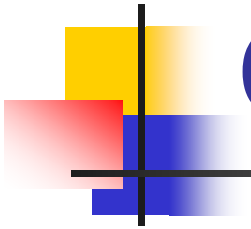
A Pull-based Networking Paradigm?
Named Data Networking

- Data, not machines, have names
- A node expresses "interest" in a given name
- Interest is routed to whoever has the named object (leaving "breadcrumbs" for data to retrace route)
- Data follows "breadcrumbs" back to source, consuming them as it goes
- End result: cannot send unsolicited data (it will be dropped in the absence of "interest")



OS-Level Mechanisms

- Early demultiplexing
  - Classify incoming data from the network card as early as possible
  - Drop the data into separate piles
  - Do not process a pile unless there is interest from the application



Quiz

- Disk requests arrive for the following tracks (head is initially at 40):
  - 30, 43, 42, 65, 15, 16, 34
- In what order are they served with:
  - Shortest seek time first?
  - C-SCAN (serving in increasing order)