Privilege Separation

Dimitris Mitropoulos
dimitro@di.uoa.gr

πως μπορούμε να καθορίζουμε
ποιός έχει πρόσβαση σε τι

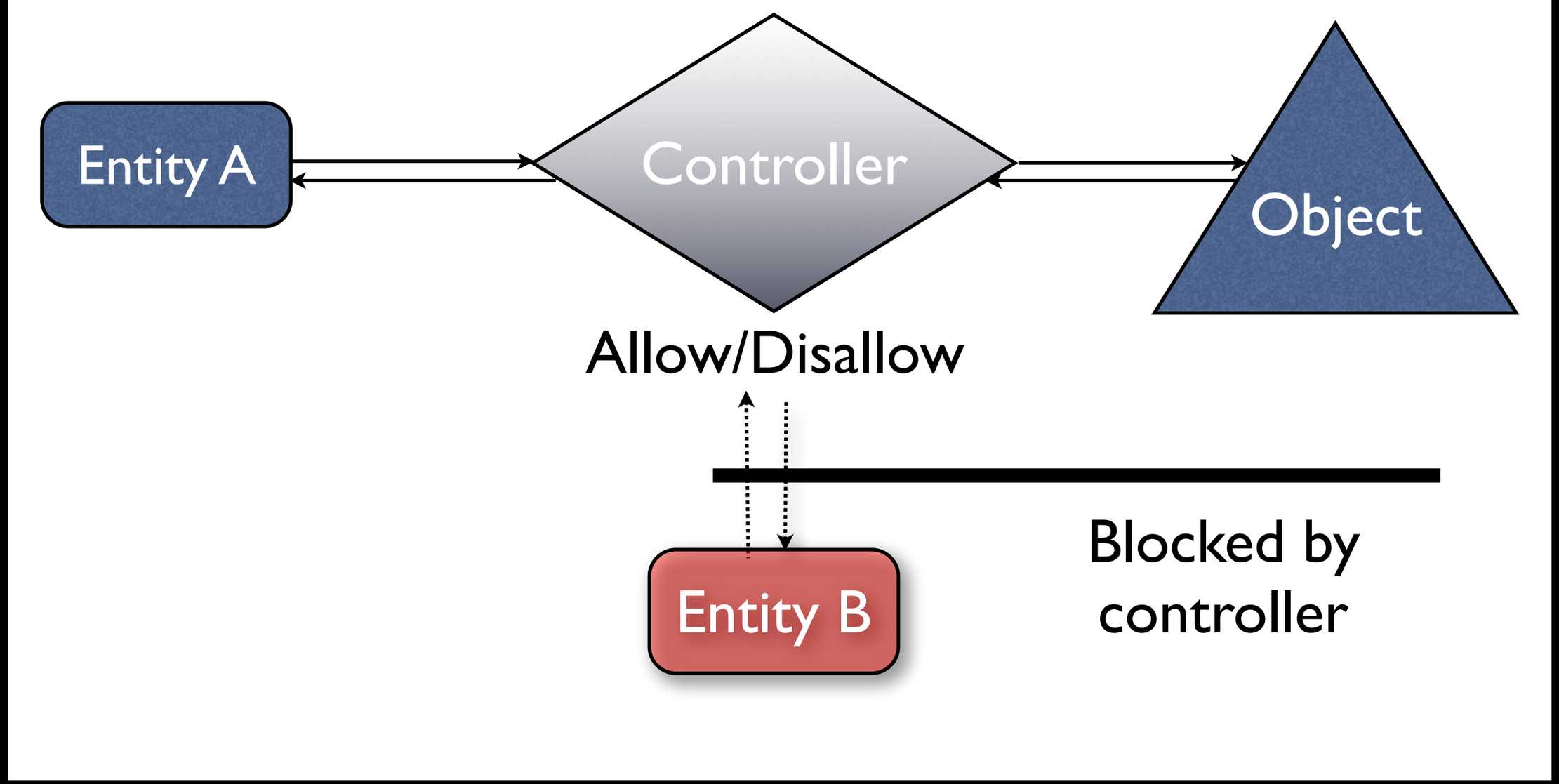
Separation Layers
Επίπεδα Διαχωρισμού

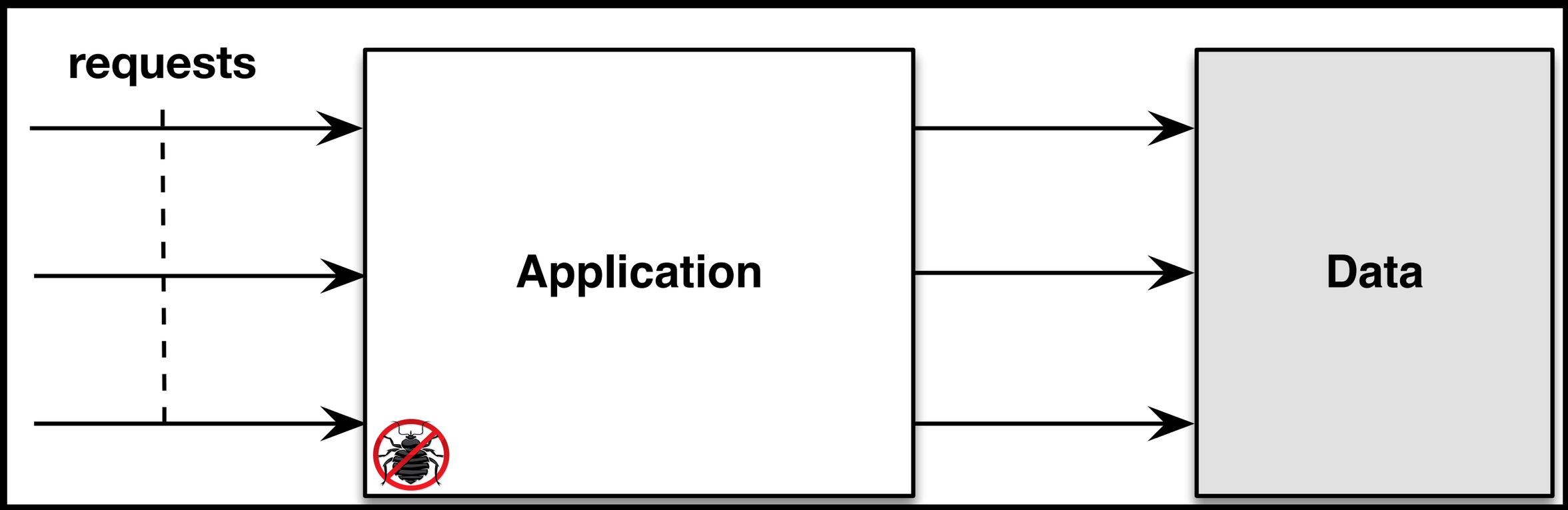
Ο διαχωρισμός αντικειμένων μπορεί να γίνει:

1. Σε φυσικό επίπεδο (διαφορετικές συσκευές),
2. Σε λογικό (λ.χ. Access Control Lists) και
3. Σε κρυπτογραφικό.

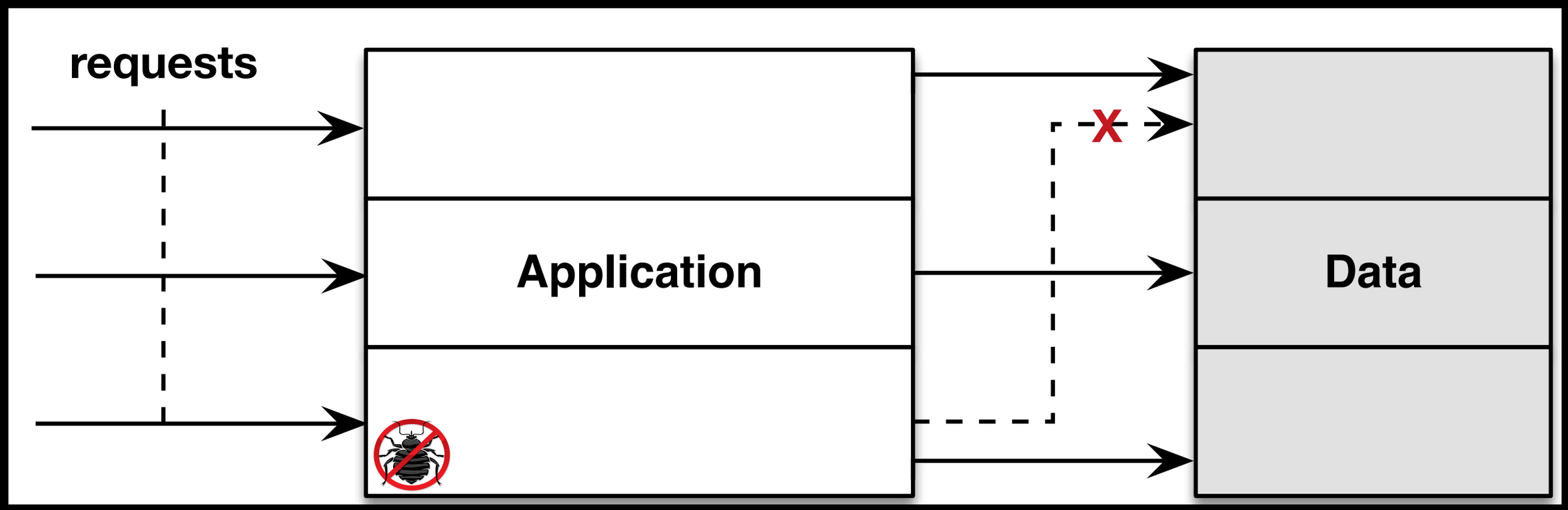
Logical Access Control

Έλεγχος Προσπέλασης





διαίρεση ενός συστήματος σε διαφορετικά μέρη, που το
κάθε ένα θα έχει διαφορετικά προνόμια

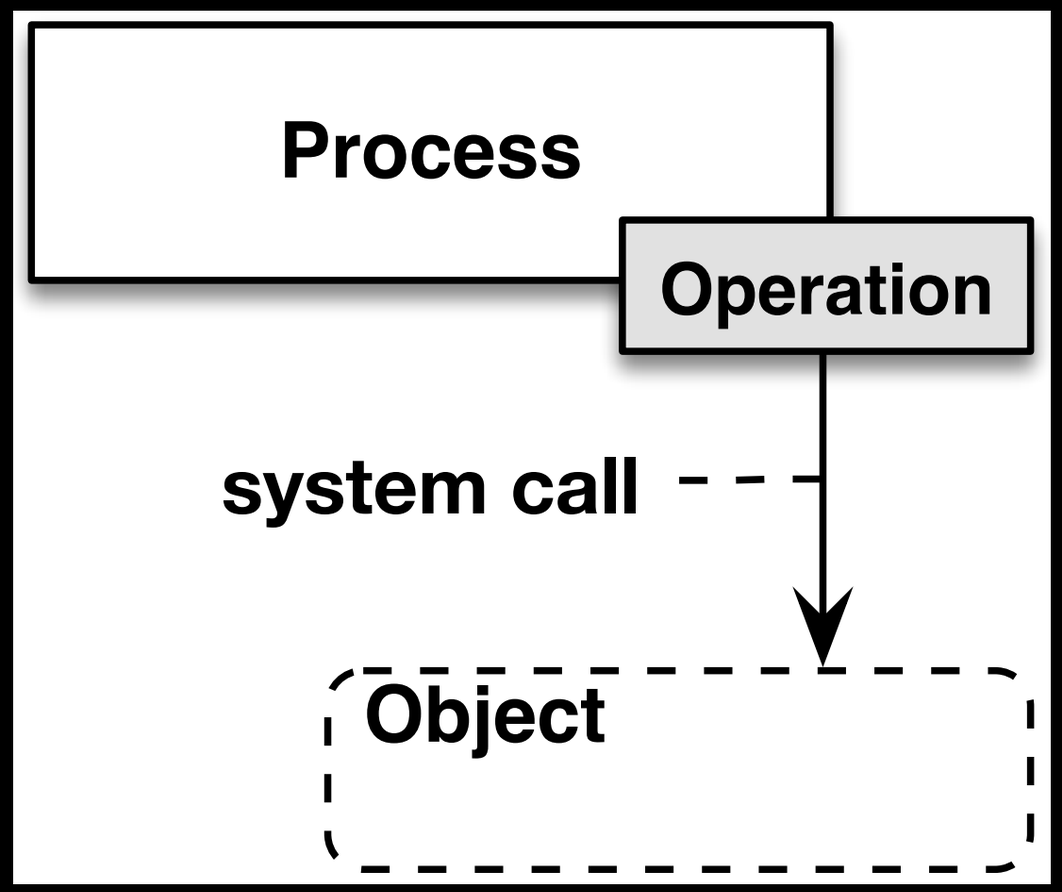


μια σωστή κατανομή προνομίων μπορεί να προστατέψει τα
δεδομένα μιας εφαρμογής ακόμα και αν αυτή περιέχει αδυναμίες

OS Entities

Βασικές Οντότητες Λειτουργικών Συστημάτων

- **Principles** (Αρχές)
- **Subject** (Υποκείμενο):
  process
- **Object** (Αντικείμενο):
  1. Files / Directories
  2. Network / Sockets
  3. File Descriptors
  4. Other Processes
  5. Memory



OS Principles

- **user ID** (32 bit integer)
- **group ID** (32 bit integer)
- Ένα process **συσχετίζεται** με ένα user ID (uid) value και μια λίστα από group ID (guid) values.
- **Superuser principle** (“root”): έχει uid = 0.

Files & Directories

- Λειτουργίες που μας ενδιαφέρουν σε σχέση με τα αρχεία: read, write, execute, change permissions.
- Αντίστοιχα για τα directories: create, remove, rename, lookup, link, unlink, change permissions.

Που βρίσκει όμως το σύστημα αυτά τα δικαιώματα;

the inode struct

- Κάθε αρχείο σε ένα UNIX σύστημα, αντιστοιχεί σε ένα inode.
- Ένα inode με τη σειρά του περιέχει διάφορες πληροφορίες όπως το μέγεθος του αρχείου σε bytes, δείκτες σε disk blocks όπου αποθηκεύονται τα περιεχόμενα του αρχείου, έναν hard link counter κ.α.
- Επίσης περιέχει ένα **uid**, ένα **guid** και μια άλλη **δομή** που καθορίζει τα δικαιώματα που μπορεί να έχουν οι χρήστες σε αυτό το αρχείο.

Ποιά είναι αυτή;

Access Control List

Directory

File 1	o
File 2	o
File 3	o

pointer

File 1 ACL

User A	Read
User B	Read and Write
Other	no access

inode’s ACL

	4	2	1	
Permission Bits	**r**	**w**	**x**	
owner	1	1	0	6
group	1	0	0	4
other	1	0	0	4

Αλλαγή δικαιωμάτων;

Μόνο αν είσαι owner (ή root).

Directories

- Το link και το unlink είναι το αντίστοιχο write. Επίσης, για να κάνουμε rename πρέπει να έχουμε write permissions.
- Εαν έχουμε read permissions μπορούμε να δούμε τι περιέχει μέσα το directory.
- Το lookup είναι το αντίστοιχο του execute. Με το lookup μπορούμε να έχουμε πρόσβαση σε ένα συγκεκριμένο αρχείο ενός directory.

open(“/etc/passwd”)

ποιά δικαιώματα θα πρέπει να έχουμε για να ανοίξουμε με επιτυχία το αρχείο passwd;

Quiz

- Υποθέτουμε πως το DI δημιουργεί ένα group με όλους όσους συσχετίζονται με το μάθημά μας (ΥΣ13) σε ένα μηχάνημα. Επίσης, υπάρχει και ένα group που περιλαμβάνει όλους τους TAs (Teaching Assistants) του τμήματος.
- Πως μπορούμε να δώσουμε πρόσβαση (με όλα τα δικαιώματα) στο αρχείο grades.txt μόνο στους TAs του μαθήματος;

File Descriptors

- Ένας file descriptor, εκπροσωπεί ένα ανοιχτό αρχείο.
- Οι έλεγχοι θα γίνουν την στιγμή του ανοίγματος του αρχείου.
- Αφης στιγμής δημιουργηθεί με επιτυχία ένας file descriptor, το process μπορεί να το επεξεργαστεί το αρχείο ανάλογα.
- Ενας file descriptor μπορεί να περάσει και σε ένα άλλο process (parent σε child).

```c
#include <stdio.h>
#include <sys/types.h>
#include <sys/stat.h>
#include <fcntl.h>
#include <string.h>
#include <errno.h>

int main(int argc, char *argv[])
{
    int fd;

    if(2 != argc)
    {
        printf("\n Usage :  \n");
        return 1;
    }

    errno = 0;
    fd = open(argv[1],O_RDONLY);

    if(-1 == fd)
    {
        printf("\n open() failed with error [%s]\n",strerror(errno));
        return 1;
    }
    else
    {
        printf("\n Open() Successful\n");
        /* open() succeeded, now one can do read operations
           on the file opened since we opened it in read-only
           mode. Also once done with processing, the file needs
           to be closed. Closing a file can be achieved using
           close() function. */
    }

    return 0;
}
```

Processes

- Ενέργειες σε σχέση με τα processes: δημιουργία (**create**), τερματισμός (**kill**), debug (**ptrace**).
- Ένα process δεν μπορεί να κάνει create ένα process με διαφορετικό uid.
- Το ίδιο ισχύει και για το debug.
- Για να κάνει kill ένα process ένα άλλο process, το πρώτο θα πρέπει να έχει το uid που έκανε create το δεύτερο.

Network

- Διαφορετική λογική (άλλωστε η δικτύωση ήρθε αργότερα).
- Ενέργειες: connect, listen, read / write, αποστολή πακέτων.
- Τυπικά, δεν υπάρχει σύνδεση με ένα uid. Ο καθένας μπορεί να ανοίξει μια σύνδεση.

Network
listen

- Στην περίπτωση του listen έχουμε τα ports.
- Για ports με νούμερο μικρότερο του 1024 θα πρέπει το uid να είναι 0 (με άλλα λόγια, τα χρησιμοποιεί μόνο ο root).
- Αυτό μας δίνει την ευκαιρία να αναθέσουμε συγκεκριμένα ports σε συγκεκριμένα services (http - 80).

Αλλιώς τι πρόβλημα μπορεί να υπήρχε;

Memory

- Ένα process δεν μπορεί να δει την μνήμη ενός άλλου process.
- Εξαίρεση αποτελούν οι debuging μηχανισμοί.

Εκχώρηση Ενός id

- Ο root χρήστης θα θέσει το uid σε ένα process χρησιμοποιώντας το system call: **setuid**.
- Αντίστοιχα υπάρχει το setgid και το setgroups.
- Ένα process θα **κληρονομήσει** το uid από το parent process.

Ο χρήστης θα πρέπει να έχει συνδεθεί κάπως…

Login Process

- Έχει uid = 0.
- Τρέχει για να **αυθεντικοποιήσει** έναν χρήστη.
- Τυπικά θα ελένξει εαν το username και το password υπάρχουν σε ένα table που περιέχει όλους τους λογαριασμούς (/etc/passwd).
- Πλεον το αρχείο αυτό δεν περιέχει τα passwords (αυτά βρίσκονται στο /etc/shadow) αλλά περιέχει το uid που χρειάζεται για να το σύστημα για να καλέσει το setuid call με όρισμα το uid.
- Μετά από αυτό θα κληθεί το call exec(/bin/sh) π.χ. έτσι ώστε να τρέξει το shell ως ξεχωριστό process με το πρέπον uid.

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
syslog:x:101:103::/home/syslog:/bin/false
mysql:x:102:105:MySQL Server,,,:/nonexistent:/bin/false
postfix:x:103:109::/var/spool/postfix:/bin/false
dovecot:x:104:111:Dovecot mail server,,,:/usr/lib/dovecot:/bin/false
sshd:x:105:65534::/var/run/sshd:/usr/sbin/nologin
landscape:x:106:113::/var/lib/landscape:/bin/false
eric:x:1000:1000:mixeduperic,,,:/home/eric:/bin/bash
jim:x:1001:1001::/home/jim:/bin/bash
bob:x:1002:1002::/home/bob:/bin/bash
tony:x:1003:1003:Tony Smith,,,:/home/tony:/bin/bash
"/etc/passwd" 29L, 1257C                                      29,1          All
```

Θα μπορούσαμε να κάνουμε elevate τα privileges και να πάμε πάλι στο uid 0;

θέλουμε να κάνουμε install ένα package…

setuid Binaries

- λ.χ. su, sudo.
- Υπάρχει αντίστοιχα ένα bit στο inode που δείχνει εαν είναι ένα binary τέτοιου τύπου ή όχι.
- Πως μπορούμε να προστατευθούμε από την ενδεχόμενη κακόβουλη χρησιμοποίηση αυτών των binaries;

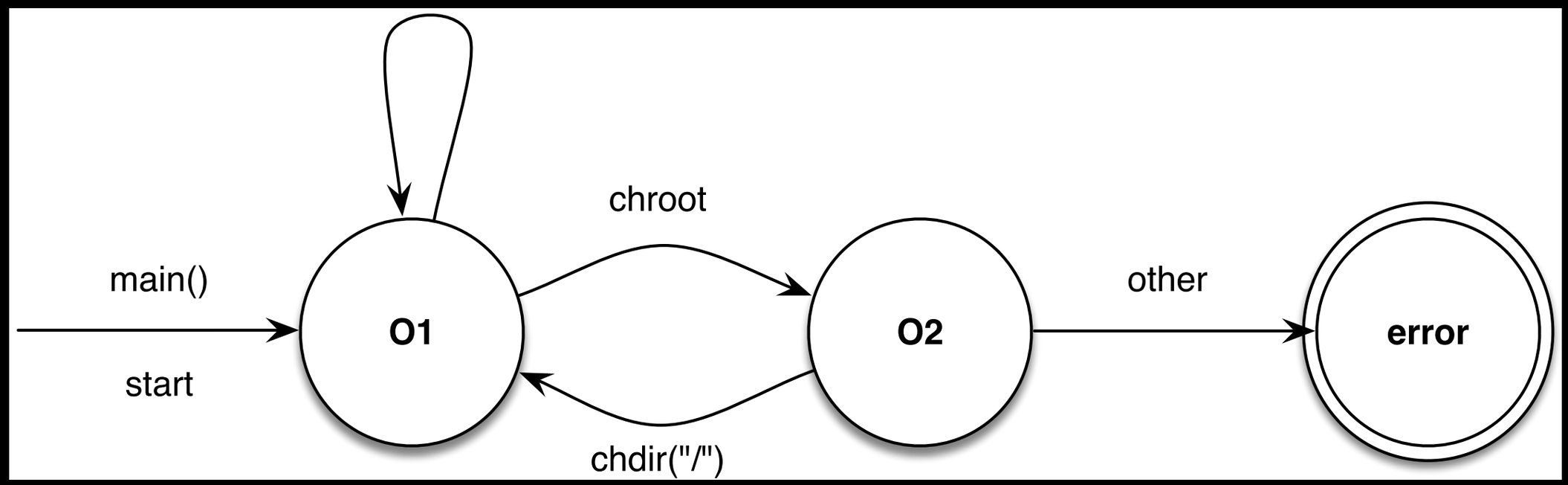
chroot

- Χρησιμοποιώντας το file system namespace.
- Καλώντας: chroot(“/foo”) το root directory θα γίνει:

  / = /foo
- Άρα εάν είχαμε ένα αρχείο x στο /foo/x πλέον το βρίσκουμε στο /x.
- Ο πυρήνας εμποδίζει ενέργειες όπως η:

  /foo/../etc/passwd
- Μορούμε να το παρακάμψουμε;

MOPS



Project 1:
Multiple App Hack
Incident Analysis

```
root@snf-744418:/var/www/eclass/fooakoko.csec.gr# ls -l
total 76
-rw-r--r--  1 fooakoko fooakoko 5581 Mar 27 20:04 CREDITS.txt
-rw-r--r--  1 fooakoko fooakoko 4610 Mar 27 20:04 README.txt
drwxrwxr-x  2 fooakoko www-data 4096 May  2 01:34 config
drwxrwxr-x  9 fooakoko www-data 4096 Apr 22 17:00 courses
drwxr-xr-x  2 fooakoko fooakoko 4096 Mar 27 20:04 images
drwxr-xr-x  8 fooakoko fooakoko 4096 Mar 27 20:04 include
-rw-rw----  2 fooakoko www-data 8662 Mar 27 20:04 index.php
drwxr-xr-x  3 fooakoko fooakoko 4096 Mar 27 20:04 info
drwxr-xr-x 2 fooakoko fooakoko 4096 Mar 27 20:04 install
drwxr-xr-x  5 fooakoko fooakoko 4096 Mar 27 20:04 manuals
drwxr-xr-x 38 fooakoko fooakoko 4096 Mar 27 20:04 modules
-rw-r--r--  1 fooakoko fooakoko  592 Mar 27 20:04 student_view.php
drwxr-xr-x  3 fooakoko fooakoko 4096 Mar 27 20:04 template
drwxr-xr-x  2 fooakoko fooakoko 4096 Mar 27 20:04 upgrade
drwxrwxr-x  5 fooakoko www-data 4096 Apr 20 21:40 video
root@snf-744418:/var/www/eclass/fooakoko.csec.gr#
```

```
  File: 'xxx.csec.gr/index.htm'
  Size: 2651            Blocks: 8          IO Block: 4096   regular file
Device: 700h/1792d      Inode: 17576       Links: 2
Access: (0644/-rw-r--r--)  Uid: ( 1000/  1000)   Gid: ( 1000/  1000)
Access: 2017-04-24 16:50:13.971054628 +0300
Modify: 2017-04-24 15:50:04.238478802 +0300
Change: 2017-04-24 22:05:24.961229798 +0300
 Birth: -
  File: 'xxx.csec.gr/index.htm'
  Size: 2651            Blocks: 8          IO Block: 4096   regular file
Device: 700h/1792d      Inode: 18165       Links: 2
Access: (0644/-rw-r--r--)  Uid: ( 1000/  1000)   Gid: ( 1000/  1000)
Access: 2017-04-24 16:50:24.715846985 +0300
Modify: 2017-04-24 15:50:47.778472483 +0300
Change: 2017-04-24 22:05:24.869232007 +0300
 Birth: -
  File: 'xxx.csec.gr/index.htm'
  Size: 2651            Blocks: 8          IO Block: 4096   regular file
Device: 700h/1792d      Inode: 18166       Links: 2
Access: (0644/-rw-r--r--)  Uid: ( 1000/  1000)   Gid: ( 1000/  1000)
Access: 2017-04-24 16:49:09.776913016 +0300
Modify: 2017-04-24 15:52:23.382459125 +0300
Change: 2017-04-24 22:05:24.037234643 +0300
 Birth: -
  File: 'xxx.csec.gr/index.htm'
  Size: 2651            Blocks: 8          IO Block: 4096   regular file
Device: 700h/1792d      Inode: 18763       Links: 2
Access: (0644/-rw-r--r--)  Uid: ( 1000/  1000)   Gid: ( 1000/  1000)
Access: 2017-04-24 16:50:37.084685789 +0300
Modify: 2017-04-24 15:53:50.190441189 +0300
Change: 2017-04-24 22:05:24.037234643 +0300
```

```
675 IP.IP.IP.IP - - [24/Apr/2017:15:49:27 +0300] "GET /modules/testfile.php?img=2 HTTP/1.1" 200 267 "http://XXXXX.csec.gr/modules/testfile.php" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0"
676 IP.IP.IP.IP - - [24/Apr/2017:15:49:27 +0300] "GET /modules/testfile.php?img=1 HTTP/1.1" 200 266 "http://XXXXX.csec.gr/modules/testfile.php" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0"
677 IP.IP.IP.IP - - [24/Apr/2017:15:49:49 +0300] "POST /modules/testfile.php HTTP/1.1" 200 5022 "http://XXXXX.csec.gr/modules/testfile.php" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0"
678 IP.IP.IP.IP - - [24/Apr/2017:15:49:50 +0300] "GET /modules/testfile.php?img=1 HTTP/1.1" 200 266 "http://XXXXX.csec.gr/modules/testfile.php" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0"
679 IP.IP.IP.IP - - [24/Apr/2017:15:49:50 +0300] "GET /modules/testfile.php?img=2 HTTP/1.1" 200 267 "http://XXXXX.csec.gr/modules/testfile.php" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0"
680 IP.IP.IP.IP - - [24/Apr/2017:15:50:04 +0300] "POST /modules/testfile.php HTTP/1.1" 200 5158 "http://XXXXX.csec.gr/modules/testfile.php" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0"
681 IP.IP.IP.IP - - [24/Apr/2017:15:50:05 +0300] "GET /modules/testfile.php?img=1 HTTP/1.1" 200 266 "http://XXXXX.csec.gr/modules/testfile.php" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0"
682 IP.IP.IP.IP - - [24/Apr/2017:15:50:05 +0300] "GET /modules/testfile.php?img=2 HTTP/1.1" 200 267 "http://XXXXX.csec.gr/modules/testfile.php" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0"
683 IP.IP.IP.IP - - [24/Apr/2017:15:50:14 +0300] "POST /modules/testfile.php HTTP/1.1" 200 4726 "http://XXXXX.csec.gr/modules/testfile.php" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0"
684 IP.IP.IP.IP - - [24/Apr/2017:15:50:16 +0300] "GET /modules/testfile.php?img=1 HTTP/1.1" 200 266 "http://XXXXX.csec.gr/modules/testfile.php" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0"
685 IP.IP.IP.IP - - [24/Apr/2017:15:50:16 +0300] "GET /modules/testfile.php?img=2 HTTP/1.1" 200 267 "http://XXXXX.csec.gr/modules/testfile.php" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0"
686 IP.IP.IP.IP - - [24/Apr/2017:15:50:33 +0300] "POST /modules/testfile.php HTTP/1.1" 200 5110 "http://XXXXX.csec.gr/modules/testfile.php" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0"
687 IP.IP.IP.IP - - [24/Apr/2017:15:50:34 +0300] "GET /modules/testfile.php?img=1 HTTP/1.1" 200 266 "http://XXXXX.csec.gr/modules/testfile.php" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0"
688 IP.IP.IP.IP - - [24/Apr/2017:15:50:34 +0300] "GET /modules/testfile.php?img=2 HTTP/1.1" 200 267 "http://XXXXX.csec.gr/modules/testfile.php" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0"
689 IP.IP.IP.IP - - [24/Apr/2017:15:50:47 +0300] "POST /modules/testfile.php HTTP/1.1" 200 5138 "http://XXXXX.csec.gr/modules/testfile.php" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0"
690 IP.IP.IP.IP - - [24/Apr/2017:15:50:49 +0300] "GET /modules/testfile.php?img=1 HTTP/1.1" 200 266 "http://XXXXX.csec.gr/modules/testfile.php" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0"
691 IP.IP.IP.IP - - [24/Apr/2017:15:50:49 +0300] "GET /modules/testfile.php?img=2 HTTP/1.1" 200 267 "http://XXXXX.csec.gr/modules/testfile.php" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0"
692 IP.IP.IP.IP - - [24/Apr/2017:15:50:55 +0300] "POST /modules/testfile.php HTTP/1.1" 200 4728 "http://XXXXX.csec.gr/modules/testfile.php" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0"
693 IP.IP.IP.IP - - [24/Apr/2017:15:50:58 +0300] "GET /modules/testfile.php?img=1 HTTP/1.1" 200 266 "http://XXXXX.csec.gr/modules/testfile.php" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0"
694 IP.IP.IP.IP - - [24/Apr/2017:15:50:58 +0300] "GET /modules/testfile.php?img=2 HTTP/1.1" 200 267 "http://XXXXX.csec.gr/modules/testfile.php" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0"
695 IP.IP.IP.IP - - [24/Apr/2017:15:51:25 +0300] "POST /modules/testfile.php HTTP/1.1" 200 4997 "http://XXXXX.csec.gr/modules/testfile.php" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0"
696 IP.IP.IP.IP - - [24/Apr/2017:15:51:27 +0300] "GET /modules/testfile.php?img=1 HTTP/1.1" 200 266 "http://XXXXX.csec.gr/modules/testfile.php" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0"
697 IP.IP.IP.IP - - [24/Apr/2017:15:51:27 +0300] "GET /modules/testfile.php?img=2 HTTP/1.1" 200 267 "http://XXXXX.csec.gr/modules/testfile.php" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0"
```

```
112 cd modules/
113 ls
114 mv r57.php testfile.php
115 ls
```


R57

Βιβλιογραφία

R. J. Anderson. Security Engineering: A Guide to Building Dependable Distributed Systems. *John Wiley & Sons, Inc.*, New York, NY, USA, 2001. ISBN 0471389226.

Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone. Handbook of Applied Cryptography, *CRC Press*, ISBN 0849385237.

Andrew S. Tanenbaum. Modern Operating Systems (3rd Edition). *Pearson*, 2007. SBN 0136006639

Hao Chen and David Wagner. MOPS: an infrastructure for examining security properties of software. In *Proceedings of the 9th ACM Conference on Computer and Communications Security (CCS)*, pages 235--244, Washington, DC, November 2002.