ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ATHENS UNIVERSITY OF ECONOMICS AND BUSINESS

Λειτουργικά Συστήματα

Ενότητα # 9: Το ΛΣ Windows

Διδάσκων: Γεώργιος Ξυλωμένος

Τμήμα: Πληροφορικής

BY NC ND

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο

ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΕΚΠΑΙΔΕΥΣΗ ΚΑΙ ΔΙΑ ΒΙΟΥ ΜΑΘΗΣΗ
επένδυση στην κοινωνία της γνώσης
ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ & ΘΡΗΣΚΕΥΜΑΤΩΝ, ΠΟΛΙΤΙΣΜΟΥ & ΑΘΛΗΤΙΣΜΟΥ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ

ΕΣΠΑ 2007-2013
πρόγραμμα για την ανάπτυξη
ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΩΝΙΚΟ ΤΑΜΕΙΟ

Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Χρηματοδότηση

- Το παρόν εκπαιδευτικό υλικό έχει αναπτυχθεί στα πλαίσια του εκπαιδευτικού έργου του διδάσκοντα.
- Το έργο «**Ανοικτά Ακαδημαϊκά Μαθήματα στο Οικονομικό Πανεπιστήμιο Αθηνών**» έχει χρηματοδοτήσει μόνο τη αναδιαμόρφωση του εκπαιδευτικού υλικού.
- Το έργο υλοποιείται στο πλαίσιο του Επιχειρησιακού Προγράμματος «Εκπαίδευση και Δια Βίου Μάθηση» και συγχρηματοδοτείται από την Ευρωπαϊκή Ένωση (Ευρωπαϊκό Κοινωνικό Ταμείο) και από εθνικούς πόρους.

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο

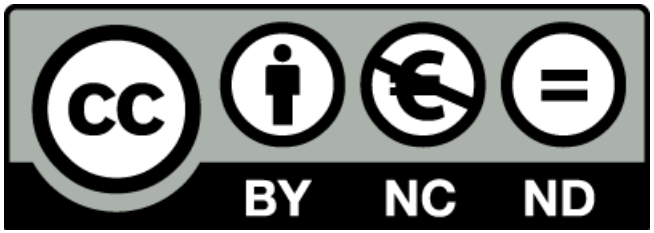
ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΕΚΠΑΙΔΕΥΣΗ ΚΑΙ ΔΙΑ ΒΙΟΥ ΜΑΘΗΣΗ
επένδυση στην κοινωνία της γνώσης
ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ & ΘΡΗΣΚΕΥΜΑΤΩΝ, ΠΟΛΙΤΙΣΜΟΥ & ΑΘΛΗΤΙΣΜΟΥ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ

ΕΣΠΑ 2007-2013
πρόγραμμα για την ανάπτυξη
ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΩΝΙΚΟ ΤΑΜΕΙΟ

Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Άδειες Χρήσης

- Το παρόν εκπαιδευτικό υλικό υπόκειται σε άδειες χρήσης Creative Commons.
- Οι εικόνες προέρχονται από το βιβλίο «Σύγχρονα Λειτουργικά Συστήματα», A.S. Tanenbaum, 3η έκδοση, 2009, Εκδόσεις Κλειδάριθμος.



Σκοποί ενότητας

- Κατανόηση της ιστορικής εξέλιξης των Windows και της διαφοροποίησής τους από το UNIX
- Εισαγωγή στη βασική δομή, σχεδίαση και μοντέλο προγραμματισμού των Windows
- Κατανόηση του τρόπου με τον οποίο οι γενικές αρχές ΛΣ εφαρμόζονται στα Windows στους τομείς των διεργασιών, διαχείρισης μνήμης, εισόδου / εξόδου, συστήματος αρχείων και ασφάλειας

Περιεχόμενα ενότητας

- Ιστορία
- Προγραμματισμός
- Δομή συστήματος
- Διεργασίες και νήματα
- Διαχείριση μνήμης
- Είσοδος / έξοδος
- Σύστημα αρχείων
- Ασφάλεια

ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ATHENS UNIVERSITY OF ECONOMICS AND BUSINESS

Ιστορία

Μάθημα: Λειτουργικά Συστήματα, **Ενότητα # 9:** Το ΛΣ Windows

Διδάσκων: Γιώργος Ξυλωμένος, **Τμήμα:** Πληροφορικής

CC BY NC ND

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο

ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΕΚΠΑΙΔΕΥΣΗ ΚΑΙ ΔΙΑ ΒΙΟΥ ΜΑΘΗΣΗ
επένδυση στην κοινωνία της γνώσης
ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ & ΘΡΗΣΚΕΥΜΑΤΩΝ, ΠΟΛΙΤΙΣΜΟΥ & ΑΘΛΗΤΙΣΜΟΥ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ

ΕΣΠΑ 2007-2013
πρόγραμμα για την ανάπτυξη
ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΩΝΙΚΟ ΤΑΜΕΙΟ

Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Ιστορία των Windows (1 από 2)

- Τρεις γενιές ΛΣ της Microsoft
- MS-DOS
  - Γραμμή διαταγών και ένας χρήστης
- Windows με βάση το MS-DOS
  - Γραφικό περιβάλλον αλλά ίδιο εσωτερικό
- Windows NT
  - Νέα σχεδίαση που εξελίσσεται ως σήμερα

Ιστορία των Windows (2 από 2)

Έτος	MS-DOS	Windows βασισμένα στο MS-DOS	Windows βασισμένα στα NT	Σημειώσεις
1981	MS-DOS 1.0			Πρώτη έκδοση για τον IBM PC
1983	MS-DOS 2.0			Υποστήριξη PC/XT
1984	MS-DOS 3.0			Υποστήριξη PC/AT
1990		Windows 3.0		Δέκα εκατομμύρια αντίτυπα σε 2 χρόνια
1991	MS-DOS 5.0			Προσθήκη διαχείρισης μνήμης
1992		Windows 3.1		Μόνο για τον 286 και μεταγενέστερους επεξεργαστές
1993			Windows NT 3.1	
1995	MS-DOS 7.0	Windows 95		MS-DOS ενσωματωμένο στα Win 95
1996			Windows NT 4.0	
1998		Windows 98		
2000	MS-DOS 8.0	Windows Me	Windows 2000	Τα Win Me ήταν χειρότερα από τα Win 98
2001			Windows XP	Αντικατέστησαν τα Windows 98
2006			Windows Vista	

Ημερομηνίες κυκλοφορίας συστημάτων

MS-DOS (1 από 2)

- Λειτουργικό του πρώτου IBM PC
  - Η IBM έφτιαξε τον PC πάνω στον 8088
  - Ζήτησε από τη Microsoft τη γλώσσα BASIC
    - Πολύ επιτυχημένη σε μηχανές 8080 και Z-80
  - Το ΛΣ θα προερχόταν από την Digital Research
    - Παραλλαγή του CP-M για 8088
  - Τελικά η IBM στράφηκε πάλι στην Microsoft
    - Η Microsoft αγόρασε ένα ΛΣ και το μετέφερε στον PC

MS-DOS (2 από 2)

- Χαρακτηριστικά του MS-DOS
  - Σύστημα 16 bit με διευθύνσεις 20 bit
    - Λόγω των επεξεργαστών 8088/8086
  - Διεπαφή γραμμής διαταγών (όπως στο CP/M)
  - Κατάλληλο για έναν χρήστη
    - Δεν παρείχε καμία έννοια προστασίας
  - Εξελίχθηκε για νέους επεξεργαστές
  - Κατά βάση όμως ήταν το ίδιο σύστημα

Windows σε MS-DOS (1 από 2)

- Windows 1, 2 και 3
  - Γραφική διεπαφή πάνω από το MS-DOS
    - Επιρροές από SRI, PARC και Apple
  - Τα Windows 1 και 2 είχαν μικρό αντίκτυπο
  - Τα Windows 3 είχαν μεγάλη επιτυχία
    - Εκμετάλλευση χαρακτηριστικών του 80386
    - Περιορισμένος πολυπρογραμματισμός
    - Η έκδοση 3.11 είχε αρκετές δυνατότητες δικτύωσης

Windows σε MS-DOS (2 από 2)

- Windows 95
  - Πολλές νέες δυνατότητες
    - Εικονική μνήμη
    - Πραγματικός πολυπρογραμματισμός
    - Διεπαφές προγραμματισμού 32 bit
  - Περιορισμένη ασφάλεια λόγω MS-DOS
    - Μικρή διάκριση χρήστη / συστήματος
  - Εξελίχθηκε σε Windows 98 και Me

Windows NT (1 από 8)

- Ανάγκη ανασχεδιασμού των Windows
  - Υπέρβαση περιορισμών του MS-DOS
  - Ανταγωνιστικό με συστήματα UNIX
  - Δυνατότητα εκτέλεσης σε συστήματα RISC
- Δημιουργία ομάδας New Technology (NT)
  - Επικεφαλής ο Dave Cutler από τη DEC
  - Σχεδίαση συστήματος 32 bit
  - Φορητότητα, αξιοπιστία και ασφάλεια

Windows NT (2 από 8)

Έτος	Λειτουργικό σύστημα DEC	Χαρακτηριστικά
1973	RSX-11M	16 bit, πολυχρηστικό, πραγματικού χρόνου, εναλλαγή
1978	VAX/VMS	32 bit, εικονική μνήμη
1987	VAXELAN	Πραγματικού χρόνου
1988	PRISM/Mica	Ακυρώθηκε για το MIPS/Ultrix

- Ομοιότητες NT με VMS/Mica
  - Ο David Cutler είχε μεγάλη εμπειρία στην DEC
  - Εμπλοκή DEC και Microsoft στα δικαστήρια
    - Κατηγορίες παραβίασης πνευματικής ιδιοκτησίας
    - Τελικά έγινε εξωδικαστικός συμβιβασμός
    - Τα NT απέκτησαν υποστήριξη για DEC Alpha

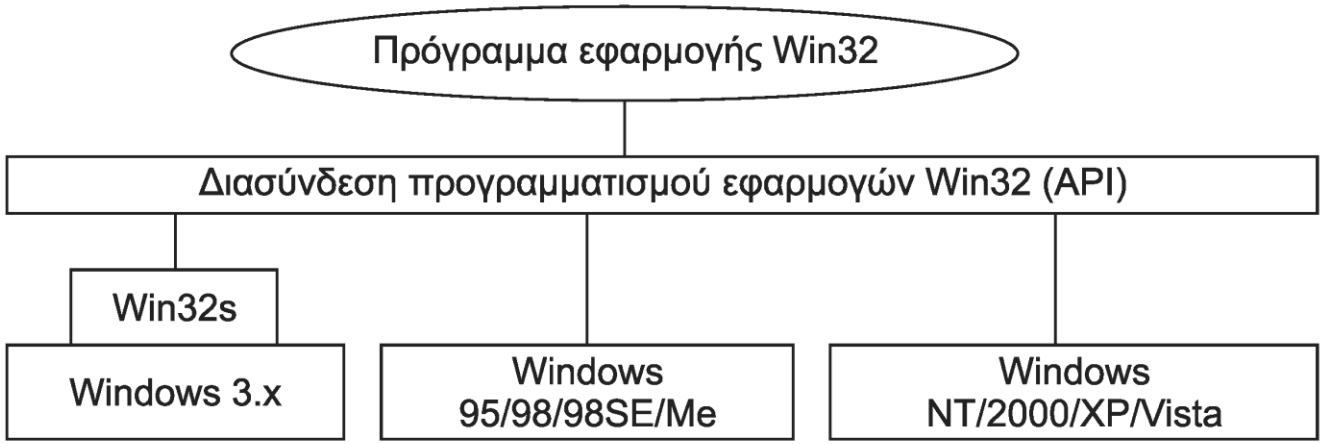
Windows NT (3 από 8)

- Διαφορές Windows NT από UNIX
  - Το UNIX εξελίχθηκε τη δεκαετία του 70
    - Μηχανές 16 bit χωρίς εικονική μνήμη
    - Εναλλαγή διεργασιών μεταξύ δίσκου/μνήμης
  - Τα NT σχεδιάστηκαν τη δεκαετία του 90
    - Μηχανές 32 bit με υλικό προστασίας
    - Χρονοπρογραμματισμός νημάτων
    - Δυναμική σύνδεση με βιβλιοθήκες

Windows NT (4 από 8)

- Windows NT 3.1 για x86, Alpha, MIPS
  - Ίδιος αριθμός έκδοσης με Windows 3.1
  - Χρήση API Win32 (αντί για Win32s)
  - Προβλήματα: πιο βαριά, λιγότερο συμβατά
    - Τα Windows 95 είχαν API Win32 και συμβατότητα
  - NT 3.51: Καλύτερη δικτύωση και PowerPC
- Windows NT 4.0
  - Ίδια γραφική διασύνδεση με Windows 95

Windows NT (5 από 8)



- Συμβατότητα εφαρμογών
  - Κοινή διεπαφή για όλες τις εφαρμογές 32 bit
    - Τα Windows 3.x είχαν περιορισμένη έκδοση
  - Εύκολη μεταφορά από Windows 95 σε NT
    - Για την ίδια αρχιτεκτονική επεξεργαστή

Windows NT (6 από 8)

- Windows 2000: μόνο για x86
  - Στόχος: συνένωση Windows NT και 98
    - Τελικά κυκλοφόρησαν και τα Windows Me
  - Διευθέτηση και άμεση λειτουργία (PnP)
  - Δικτυακή υπηρεσία καταλόγου (AD)
- Windows XP: το τέλος του MS-DOS
  - Πιο φιλική διεπαφή, μεγαλύτερη συμβατότητα
  - Μεταγενέστερη έκδοση διακομιστών (Server 2003)
    - Υποστήριξη IA-64 και x64

Windows NT (7 από 8)

Έτος	Έκδοση πελάτη	Έτος	Έκδοση διακομιστή
1996	Windows NT	1996	Windows NT Server
1999	Windows 2000	1999	Windows 2000 Server
2001	Windows XP	2003	Windows Server 2003
2006	Windows Vista	2007	Windows Server 2008

- Windows Vista: νέα αλλαγή διεπαφής
  - Ενίσχυση ασφάλειας και απόδοσης
  - Μεταγενέστερη έκδοση διακομιστών (Server 2008)
    - Ο πυρήνας είναι ο ίδιος
  - Τα Windows 7/Server 2008R2 είναι πολύ παρόμοια

Windows NT (8 από 8)

Περιοχή πυρήνα	Linux	Vista
Χρονοπρογραμματιστής CPU	50000	75000
Υποδομή Ε/Ε	45000	60000
Εικονική μνήμη	25000	175000

- Θέματα με τα Windows Vista
  - Πολύ φιλόδοξο εγχείρημα για να πετύχει
    - 70 εκατομμύρια γραμμές κώδικα!
    - Στην πορεία άλλαξαν βασικά στοιχεία σχεδίασης
  - 1600 βιβλιοθήκες DLL και 400 EXE στο system32
    - Και όλα τα προγράμματα από προηγούμενες εκδόσεις
  - Έμφαση σε απόδοση και πρόσθετες λειτουργίες

ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ATHENS UNIVERSITY OF ECONOMICS AND BUSINESS

Προγραμματισμός

Μάθημα: Λειτουργικά Συστήματα, **Ενότητα # 9:** Το ΛΣ Windows

Διδάσκων: Γιώργος Ξυλωμένος, **Τμήμα:** Πληροφορικής

CC BY NC ND

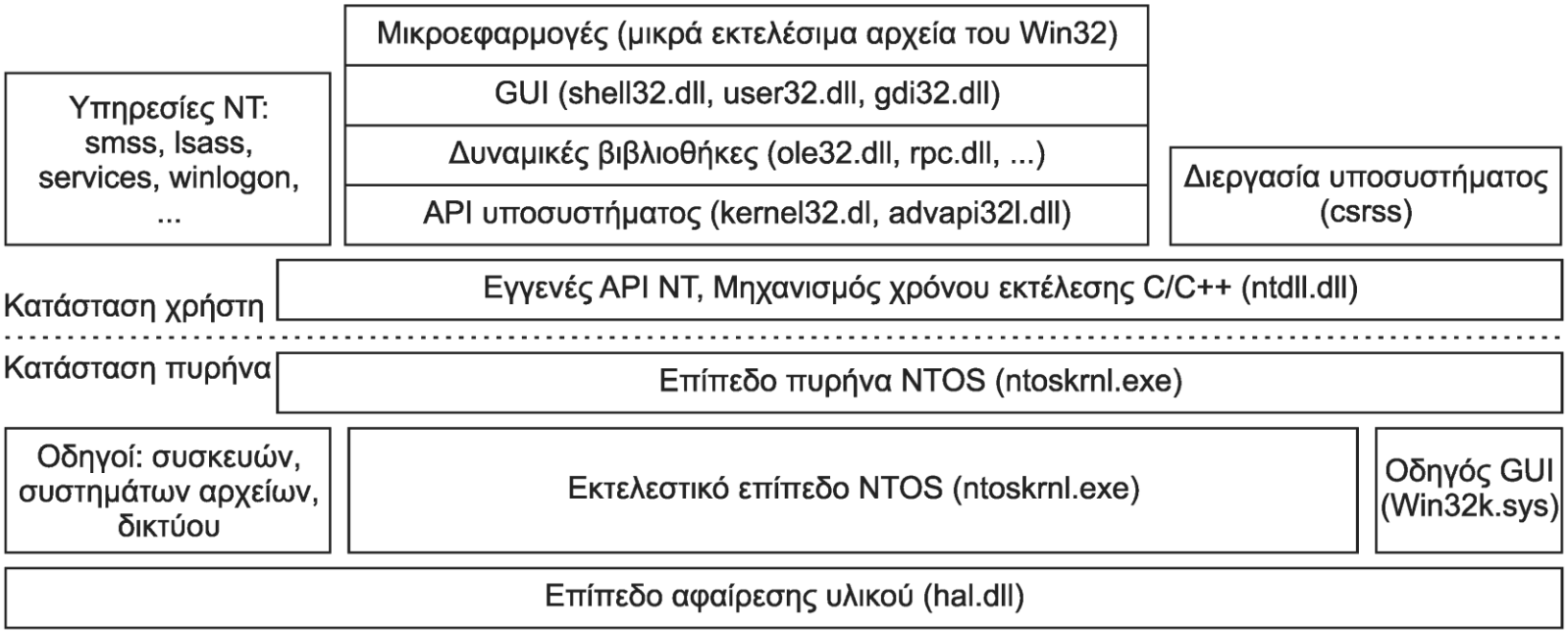
Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο

ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΕΚΠΑΙΔΕΥΣΗ ΚΑΙ ΔΙΑ ΒΙΟΥ ΜΑΘΗΣΗ
επένδυση στην κοινωνία της γνώσης
ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ & ΘΡΗΣΚΕΥΜΑΤΩΝ, ΠΟΛΙΤΙΣΜΟΥ & ΑΘΛΗΤΙΣΜΟΥ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ

ΕΣΠΑ 2007-2013
πρόγραμμα για την ανάπτυξη
ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΩΝΙΚΟ ΤΑΜΕΙΟ

Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Δομή API (1 από 5)

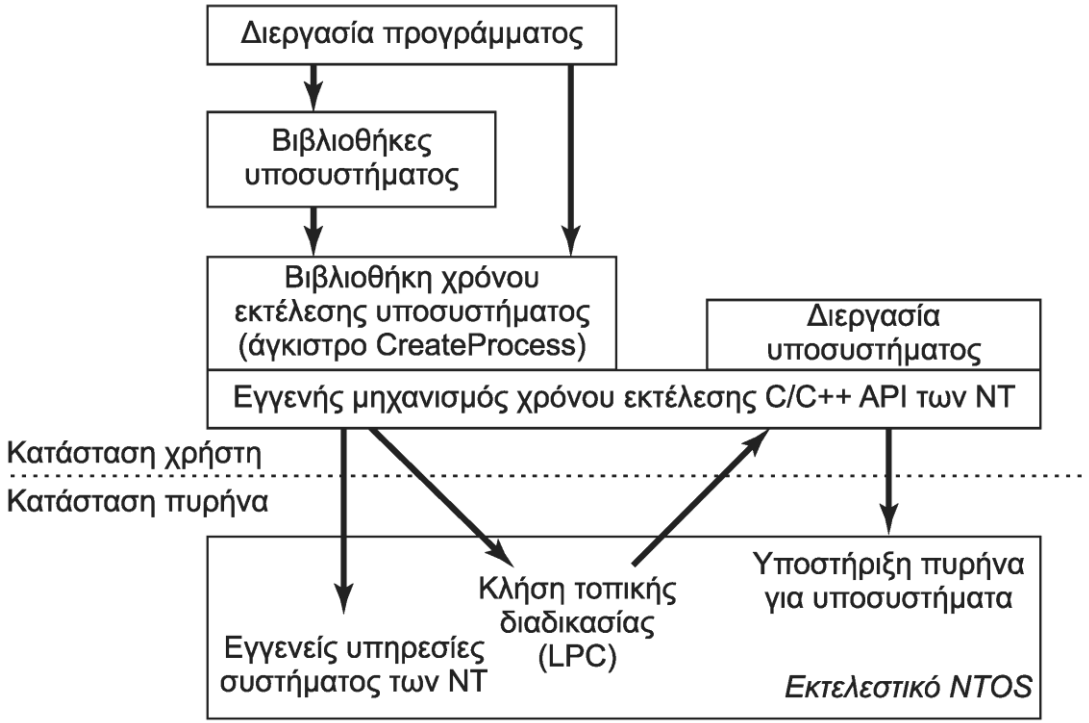


- Κλήσεις συστήματος των Windows
  - Το βασικό επίπεδο είναι ο πυρήνας (ntoskrnl.exe)
  - Χρησιμοποιείται μόνο εσωτερικά στη Microsoft

Δομή API (2 από 5)

- API των Windows
  - Ορισμένα API υλοποιούνται από DLL
  - Άλλα API είναι διεργασίες επιπέδου χρήστη
    - Χρήση RPC για κλήση τους
- Υποσυστήματα - προσωπικότητες
  - Αρχικά είχαμε OS/2, POSIX και Win32
    - Το OS/2 καταργήθηκε, το POSIX σχεδόν
    - Η βασική προσωπικότητα είναι το Win32

Δομή API (3 από 5)



- Δομή υποσυστήματος
  - Διεργασία και βιβλιοθήκες υποσυστήματος
  - Υποστήριξη χρόνου εκτέλεσης και πυρήνα

Δομή API (4 από 5)

- Συστατικά υποσυστήματος
  - Οι βιβλιοθήκες έχουν κλήσεις υψηλού επιπέδου
  - Τοπικές κλήσεις προς διεργασία υποσυστήματος
    - Διεκπεραίωση LPC μέσω του πυρήνα
  - Η CreateProcess εντοπίζει το υποσύστημα
    - Εκκίνηση διεργασίας υποσυστήματος (αν χρειάζεται)
    - Το υποσύστημα φορτώνει τη διεργασία
  - Η διεργασία υποσυστήματος καλεί το NT API

Δομή API (5 από 5)

- Υποσύστημα Win32
  - Υλοποιείται από τη διεργασία csrss.exe
    - Ξεκινάει αυτόματα από τη διεργασία smss.exe
- Προγραμματιστικά μοντέλα
  - Το Win32 είναι πολύ περίπλοκο
  - Τα .NET/WinFX είναι πιο χρηστικά
    - Κρύβουν το Win32 πίσω από βιβλιοθήκη τάξεων
    - Προσθέτουν τις δυνατότητες του CLR

Το NT API (1 από 4)

Κατηγορία αντικειμένου	**Παραδείγματα**
Συγχρονισμός	Σηματοφόροι, mutex, συμβάντα, θύρες IPC, ουρές ολοκλήρωσης E/E (I/O completion queues)
E/E	Αρχεία, συσκευές, οδηγοί, χρονόμετρα
Πρόγραμμα	Εργασίες, διεργασίες, νήματα, ενότητες, σκυτάλες (tokens)
Win32 GUI	Επιφάνειες εργασίας, επανακλήσεις εφαρμογών (application callbacks)

- Κλήσεις συστήματος του NT
  - Χρησιμοποιούνται σε πολύ χαμηλό επίπεδο
    - Υπηρεσίες, υποσυστήματα και οδηγοί πυρήνα
  - Ενεργούν σε αντικείμενα του πυρήνα
    - Απόκρυψη υλοποίησης αλλά όχι κληρονομικότητα

Το NT API (2 από 4)

- Αντικείμενα του NT API
  - Η δημιουργία τους επιστρέφει ένα χειριστήριο
  - Το χειριστήριο γενικά είναι ιδιωτικό
    - Μεταβιβάζεται μόνο με προστατευμένο τρόπο
  - Κάθε χειριστήριο έχει περιγραφέα ασφάλειας
    - Περιγράφει τις επιτρεπόμενες λειτουργίες
  - Τα αντικείμενα έχουν τύπο, λειτουργίες και μνήμη
    - Ουσιαστικά παρέχουν διεπαφές χαμηλού επιπέδου

Το NT API (3 από 4)

NtCreateProcess(&ProcHandle, Access, SectionHandle, DebugPortHardie, ExceptPortHandle, ...)
NtCreateThread(&ThreadHandle, ProcHandle, Access, ThreadContext, CreateSuspended, ...)
NtAllocateVirtualMemory(ProcHandle, Addr, Size, Type, Protection, ...)
NtMapViewOfSection(SectHandle, ProcHandle, Addr, Size, Protection, ...)
NtReadVirtualMemory(ProcHandle, Addr, Size, ...)
NtWriteVirtualMemory(ProcHandle, Addr, Size, ...)
NtCreateFile(&FileHandle, FileNameDescriptor, Access, ...)
NtDuplicateObject(srcProcHandle, srcObjHandle, dstProcHandle, dstObjHandle, ...)

- Ορισμένες κλήσεις του NT API
  - Δημιουργία διεργασίας με χειριστήριο μνήμης
  - Δημιουργία νήματος με χειριστήριο διεργασίας
  - Μπορούμε να επηρεάσουμε άλλες διεργασίες
    - Αρκεί να έχουμε χειριστήριο προς αυτές

Το NT API (4 από 4)

- Χειριστήρια και ονόματα
  - Κεντρικός διαχειριστής αντικειμένων του NT
  - Υποστηρίζει χώρο ονομάτων αντικειμένων
    - Από το όνομα μπορούμε να πάρουμε χειριστήριο
    - Ιεραρχική δομή καταλόγου για αντικείμενα
  - Ο χώρος ονομάτων δημιουργείται στη μνήμη
    - Συμπληρώνεται όπως εκτελείται το σύστημα
    - Μόνιμα αντικείμενα για συγχρονισμό και κοινή μνήμη

Το Win32 API (1 από 5)

Κλήση Win32	Κλήση εγγενούς API των NT
CreateProcess	NtCreateProcess
CreateThread	NtCreateThread
SuspendThread	NtSuspendThread
CreateSemaphore	NtCreateSemaphore
ReadFile	NtReadFile
DeleteFile	NtSetInformationFile
CreateFileMapping	NtCreateSection
VirtualAlloc	NtAllocateVirtualMemory
MapViewOfFile	NtMapViewOfSection
DuplicateHandle	NtDuplicateObject
CloseHandle	NtClose

- Το δημόσιο API των Windows
  - Υπερκαλύπτει τη λειτουργικότητα του NT API

Το Win32 API (2 από 5)

- Μετατροπή από Win32 σε NT
  - Μετατροπή ονομάτων συσκευών
  - Μετατροπή ονομάτων αρχείων σε χειριστήρια
  - Μετατροπή ANSI σε Unicode
- Windows σε Windows (WOW)
  - Απεικόνιση κλήσεων για συμβατότητα
  - WOW32: εκτέλεση κώδικα 16 bit σε 32 bit
  - WOW64: εκτέλεση κώδικα 32 bit σε 64 bit

Το Win32 API (3 από 5)

- Φιλοσοφία του Win32
  - Συνεχής προσθήκη λειτουργικότητας
  - Πολλοί τρόποι να κάνεις το ίδιο πράγμα
  - Ανάμιξη κλήσεων χαμηλού και υψηλού επιπέδου
- Χαρτογράφηση αρχείων στη μνήμη
  - Δέσμευση διευθύνσεων για μεταγενέστερη χρήση
  - Δημιουργία χαρτογραφήσεων αρχείων ή μνήμης
    - Μπορούν να μοιράζονται από διεργασίες
  - Αντιστοίχιση όψεων χαρτογραφήσεων σε διευθύνσεις

Το Win32 API (4 από 5)

- Ιδιαιτερότητες συστήματος αρχείων
  - Πολλά ρεύματα δεδομένων ανά αρχείο
  - Κρυπτογράφηση αρχείων και μονάδων
  - Ενοποίηση μονάδων δίσκου
  - Ενημέρωση σε αλλαγές αρχείων/καταλόγων
- Ασύγχρονο μοντέλο εισόδου / εξόδου
  - Διάφοροι μέθοδοι συγχρονισμού μετά την Ε/Ε
  - Δυνατότητα χρήσης σύγχρονης Ε/Ε

Το Win32 API (5 από 5)

- Μοντέλο ασφάλειας
  - Κάθε νήμα έχει μία σκυτάλη με προνόμια
  - Κάθε αντικείμενο έχει μία ACL για έλεγχο
- Χώρος ονομάτων του Win32
  - Παρόμοιος με το MS-DOS (π.χ. C:\)
  - Τα NT έχουν πιο εκτεταμένο χώρο ονομάτων
    - \Device\HarddiskVolume1 = \DosDevices\C:
- Πάρα πολλές κλήσεις για το GUI

Μητρώο (1 από 3)

- Μητρώο (registry) των Windows
  - Ειδική μορφή συστήματος αρχείων
  - Μέρος του χώρου ονομάτων των NT
  - Αποτελείται από ανεξάρτητες κυψέλες
    - Κάθε κυψέλη αποθηκεύεται στο δίσκο εκκίνησης
  - Η κυψέλη SYSTEM φορτώνεται με την εκκίνηση
    - Βασικοί οδηγοί και λογισμικό εκκίνησης
  - Οι υπόλοιπες κυψέλες φορτώνονται στη συνέχεια

Μητρώο (2 από 3)

Αρχείο κυψέλης	Αναρτημένο όνομα	Χρήση
SYSTEM	HKLM TEM	Πληροφορίες διευθέτησης του λειτουργικού συστήματος που χρησιμοποιούνται από τον πυρήνα
HARDWARE	HKLM DWARE	Κυψέλη στη μνήμη, όπου καταγράφεται το υλικό που έχει εντοπιστεί
BCD	HKLM BCD	Βάση Δεδομένων Διευθέτησης Εκκίνησης (Boot Configuration Database)
SAM	HKLM	Πληροφορίες σύνδεσης τοπικού χρήστη
SECURITY	HKLM URITY	Λογαριασμός lsass και άλλες πληροφορίες ασφαλείας
DEFAULT	HKEY_USERS.DEFAULT	Προεπιλεγμένη κυψέλη για νέους χρήστες
NTUSER.DAT	HKEY_USERS <user id>	Κυψέλη συγκεκριμένου χρήστη, που διατηρείται στον προσωπικό του κατάλογο
SOFTWARE	HKLM TWARE	Κλάσεις εφαρμογών καταχωρισμένες από το μοντέλο COM
COMPONENTS	HKLM NENTS	Δηλώσεις και εξαρτήσεις για συστατικά του συστήματος

Κυψέλες των Windows

Μητρώο (3 από 3)

- Το μητρώο είναι εξαιρετικά περίπλοκο
  - Περιέχει πληροφορίες διάρθρωσης για τα πάντα
  - Εύκολο να δημιουργήσει προβλήματα
- Κλήσεις χειρισμού του μητρώου

Συνάρτηση Win32 API	**Περιγραφή**
RegCreateKeyEx	Δημιουργία νέου κλειδιού στο μητρώο
RegDeleteKey	Διαγραφή κλειδιού του μητρώου
RegOpenKeyEx	Άνοιγμα κλειδιού για τη λήψη ενός χειριστηρίου γι' αυτό
RegEnumKeyEx	Απαρίθμηση των δευτερευόντων κλειδιών που ανήκουν στο κλειδί του χειριστηρίου
RegQueryValueEx	Αναζήτηση των δεδομένων της τιμής που περιέχει ένα κλειδί

Δομή συστήματος

Μάθημα: Λειτουργικά Συστήματα, **Ενότητα # 9:** Το ΛΣ Windows

Διδάσκων: Γιώργος Ξυλωμένος, **Τμήμα:** Πληροφορικής

CC BY NC ND

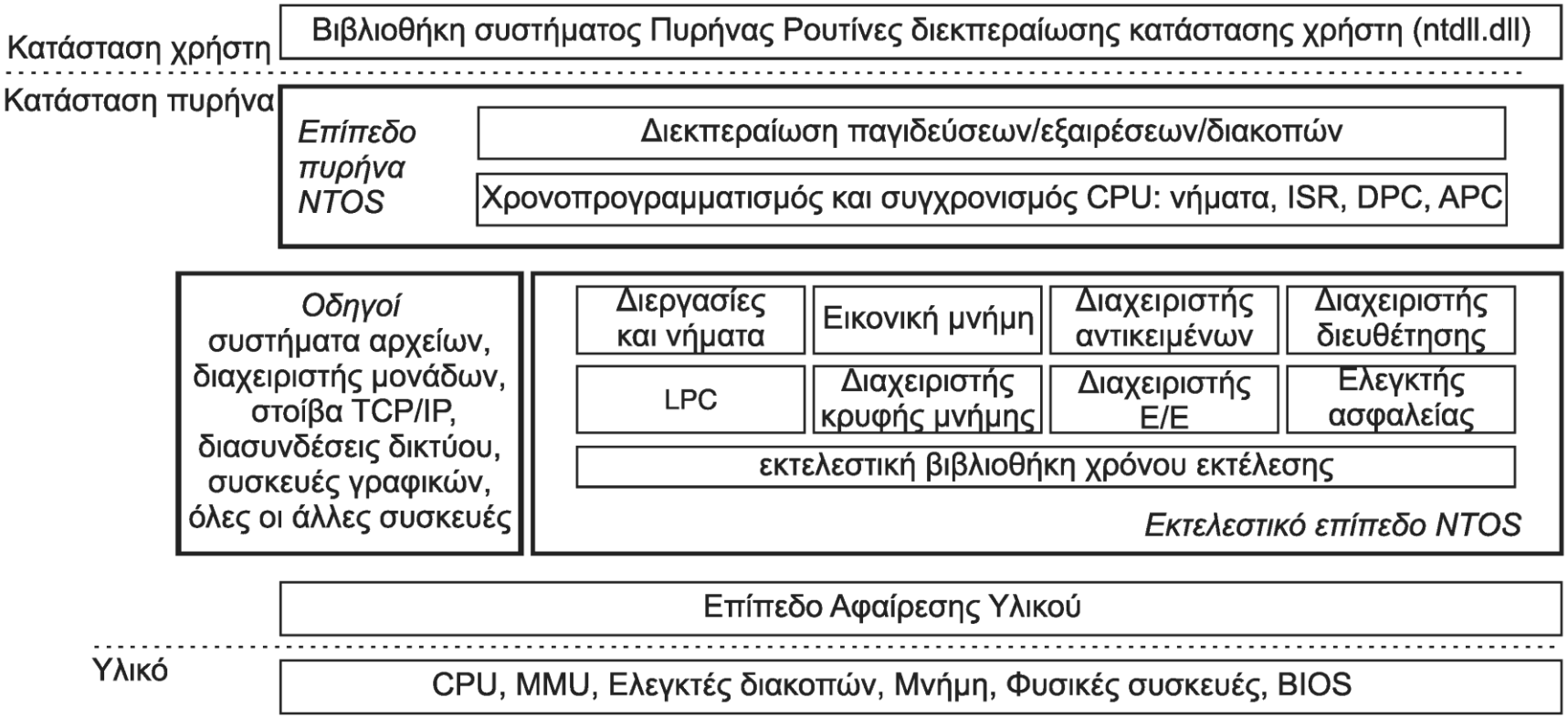
Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο

ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΕΚΠΑΙΔΕΥΣΗ ΚΑΙ ΔΙΑ ΒΙΟΥ ΜΑΘΗΣΗ
επένδυση στην κοινωνία της γνώσης
ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ & ΘΡΗΣΚΕΥΜΑΤΩΝ, ΠΟΛΙΤΙΣΜΟΥ & ΑΘΛΗΤΙΣΜΟΥ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ

ΕΣΠΑ 2007-2013
πρόγραμμα για την ανάπτυξη
ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΩΝΙΚΟ ΤΑΜΕΙΟ

Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Δομή ΛΣ (1 από 3)



Επίπεδα του ΛΣ

Δομή ΛΣ (2 από 3)

- Ο βασικός κώδικας είναι στο ntoskrnl.exe
- Διακρίνεται σε δύο επίπεδα
  - Εκτελεστικό (executive): όλες οι υπηρεσίες
  - Πυρήνας (kernel): λειτουργίες χαμηλού επιπέδου
  - Υπόλοιπες υπηρεσίες σε επίπεδο χρήστη
- Είσοδος στον πυρήνα μέσω ntdll.dll
  - Παρέχει υπηρεσίες και για τον πυρήνα
  - Περιέχεται στην εικονική μνήμη των διεργασιών

Δομή ΛΣ (3 από 3)

- Επίπεδο αφαίρεσης υλικού (HAL)
  - Ενιαίος τρόπος χειρισμού συσκευών και DMA
  - Απόκρυψη διαφορών BIOS και chipset
- Οδηγοί συσκευών
  - Συσκευές και άλλα συμπληρώματα του πυρήνα
    - Συστήματα αρχείων και πρωτόκολλα
    - Αντιβιοτικά και διαχείριση δικαιωμάτων
  - Δυναμική φόρτωση και σύνδεση με πυρήνα

Αφαίρεση υλικού (1 από 2)

- Πόσο φορητά είναι τα Windows;
  - Μόνο 1-2% του κώδικα είναι assembly
  - Ο κώδικας σε C όμως δεν είναι πάντα φορητός
  - Πολλές λεπτομέρειες δεν αποκρύπτονται
    - Μορφή πίνακα σελίδων
    - Διαθέσιμες λειτουργίες συγχρονισμού
  - Το HAL κρύβει λεπτομέρειες σε μία αρχιτεκτονική
    - Διαφορές σε chipset και έκδοση επεξεργαστή

Αφαίρεση υλικού (2 από 2)

- Ε/Ε με θύρες ή με χαρτογράφηση στη μνήμη;
  - Το HAL παρέχει ρουτίνες WRITE_PORT_UCHAR
  - Απεικονίζονται σε κατάλληλες λειτουργίες
  - Ο οδηγός συσκευής χρησιμοποιεί τις ρουτίνες αυτές
- Εμφάνιση συσκευών σε κοινό χώρο διευθύνσεων
- Ενιαίος χειρισμός διακοπών και DMA
- Διαχείριση ρολογιών και χρονομέτρων
- Υλοποίηση κλειδωμάτων περιστροφής

Επίπεδο πυρήνα

- Αφαιρέσεις για διαχείριση του επεξεργαστή
  - Διακοπές, παγίδες και εξαιρέσεις
  - Νήματα: χρονοπρογραμματισμός, συγχρονισμός
    - Οι δομές δεδομένων υλοποιούνται στο εκτελεστικό
    - Επιλογή επόμενου νήματος προς εκτέλεση
    - Αλλαγή συμφραζομένων αν χρειάζεται
  - Αντικείμενα ελέγχου (control)
  - Αντικείμενα διεκπεραίωσης (dispatcher)

Καθυστερημένες κλήσεις (1 από 2)

- Αντικείμενα ελέγχου του πυρήνα
  - Νήματα, διακοπές, χρονόμετρα, συγχρονισμός
  - Αντικείμενα DPC και APC
- ISR: ρουτίνα εξυπηρέτησης διακοπής
  - Εκτελείται με προτεραιότητα διακοπής 3 και άνω
  - Υλοποιεί μόνο το κρίσιμο τμήμα της διακοπής
  - Η υπόλοιπή επεξεργασία γίνεται μέσω DPC
    - Προσθήκη αντικειμένου DPC σε ουρά επεξεργαστή

Καθυστερημένες κλήσεις (2 από 2)

- Καθυστερημένη κλήση διαδικασίας (DPC)
  - Ολοκληρώνει την επεξεργασία μίας διακοπής
  - Αντιστοιχεί σε διακοπή προτεραιότητας 2
    - Εξυπηρετείται όταν τελειώσουν όλες οι άλλες ISR
    - Η ISR επιπέδου 2 εκτελεί όλη την ουρά των DPC
  - Παράδειγμα: πληκτρολόγιο
    - Η ISR αντιγράφει τον κωδικό πλήκτρου
    - Η DPC επεξεργάζεται τους κωδικούς αργότερα

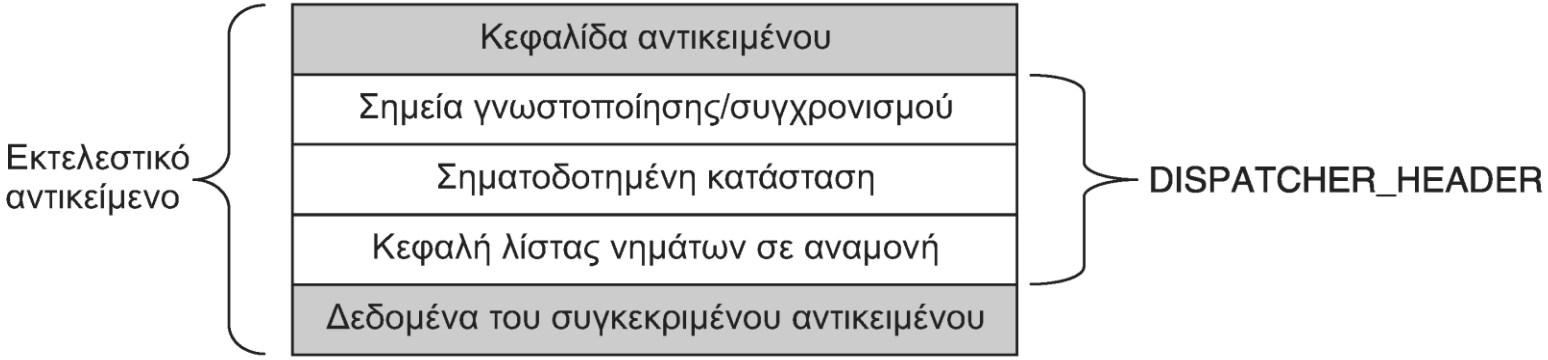
Ασύγχρονες κλήσεις (1 από 2)

- Ασύγχρονη κλήση διαδικασίας (APC)
  - Καλείται όταν ολοκληρωθεί η λειτουργία Ε/Ε
    - Μπαίνει σε ουρά με αίτηση της DPC
    - Η DPC εκτελείται σε όποιο νήμα είναι ενεργό
    - Η APC εκτελείται για λογαριασμό του παραλήπτη
  - Παρόμοια με χειριστή σημάτων στο UNIX
    - Εκτελείται όμως σε επίπεδο πυρήνα
    - Βλέπει τη μνήμη και του πυρήνα και του χρήστη

Ασύγχρονες κλήσεις (2 από 2)

- APC σε επίπεδο χρήστη
  - Η εφαρμογή ορίζει την APC που επιθυμεί
  - Στη συνέχεια μπλοκάρει σε Ε/Ε
  - Όταν ολοκληρωθεί η Ε/Ε καλείται η APC
  - Παρόμοια με επανάκληση από τον πυρήνα
- Χρήση APC από τον πυρήνα
  - Παράδειγμα: ελεγχόμενος τερματισμός νημάτων
    - Η APC παραδίδεται μόνο εκτός κρίσιμων περιοχών

Αντικείμενα διεκπεραίωσης (1 από 2)



- Αντικείμενο με δομή dispatcher_header
  - Διάφορα αντικείμενα όπου έχουμε συγχρονισμό
    - Σηματοφορείς, mutex, συμβάντα, χρονόμετρα
    - Αλλά και αρχεία, διεργασίες, νήματα, θύρες IPC
  - Σημαία κατάστασης, ουρά νημάτων σε αναμονή

Αντικείμενα διεκπεραίωσης (2 από 2)

- Αναμονή σε αντικείμενα διεκπεραίωσης
  - Ενιαίος μηχανισμός για συγχρονισμό
    - Όταν συμβεί κάτι, ξυπνάει το νήμα
  - Κλήση WaitForMultipleObjects
    - Επιτρέπει αναμονή σε πολλά χειριστήρια
- Δύο είδη αντικειμένων διεκπεραίωσης
  - Γνωστοποίησης: ξυπνάνε όλα τα νήματα
  - Συγχρονισμού: ξυπνάει μόνο το πρώτο νήμα

Εκτελεστικό επίπεδο (1 από 4)

- (Σχετικά) Φορητό τμήμα του λειτουργικού
  - Βασίζεται στις υπηρεσίες του πυρήνα
  - Αποτελείται από διάφορα συστατικά
    - Διαχειριστής Ε/Ε, μνήμης, αντικειμένων
  - Εκτελείται για λογαριασμό κάποιου νήματος
  - Υπάρχουν και νήματα πυρήνα
    - Νήμα που εκτελείται ανά δευτερόλεπτο
    - Δεξαμενή νημάτων υψηλής προτεραιότητας

Εκτελεστικό επίπεδο (2 από 4)

- Διαχειριστής αντικειμένων
  - Διαχείριση μνήμης αντικειμένων
    - Μετρητές χρήσης αντικειμένων
  - Χειριστήρια και ονόματα αντικειμένων
- Διαχειριστής Ε/Ε
  - Βασικές υπηρεσίες συσκευών και οδηγών
    - Υποστήριξη οδηγών επιπέδου χρήστη
  - Συνεργασία με διαχειριστή PnP επιπέδου χρήστη
    - Εντοπισμός και φόρτωση του κατάλληλο οδηγού

Εκτελεστικό επίπεδο (3 από 4)

- Διαχειριστής διεργασιών
  - Διεργασία: μνήμη, νήματα και χειριστήρια
- Διαχειριστής μνήμης
  - Εικονική μνήμη με σελιδοποίηση κατ'απαίτηση
  - Υποστηρίζει και το αρχείο σελιδοποίησης
- Διαχειριστής κρυφής μνήμης
  - Κρυφή μνήμη σελίδων από αρχεία
  - Βασίζεται στην χαρτογράφηση αρχείων στη μνήμη

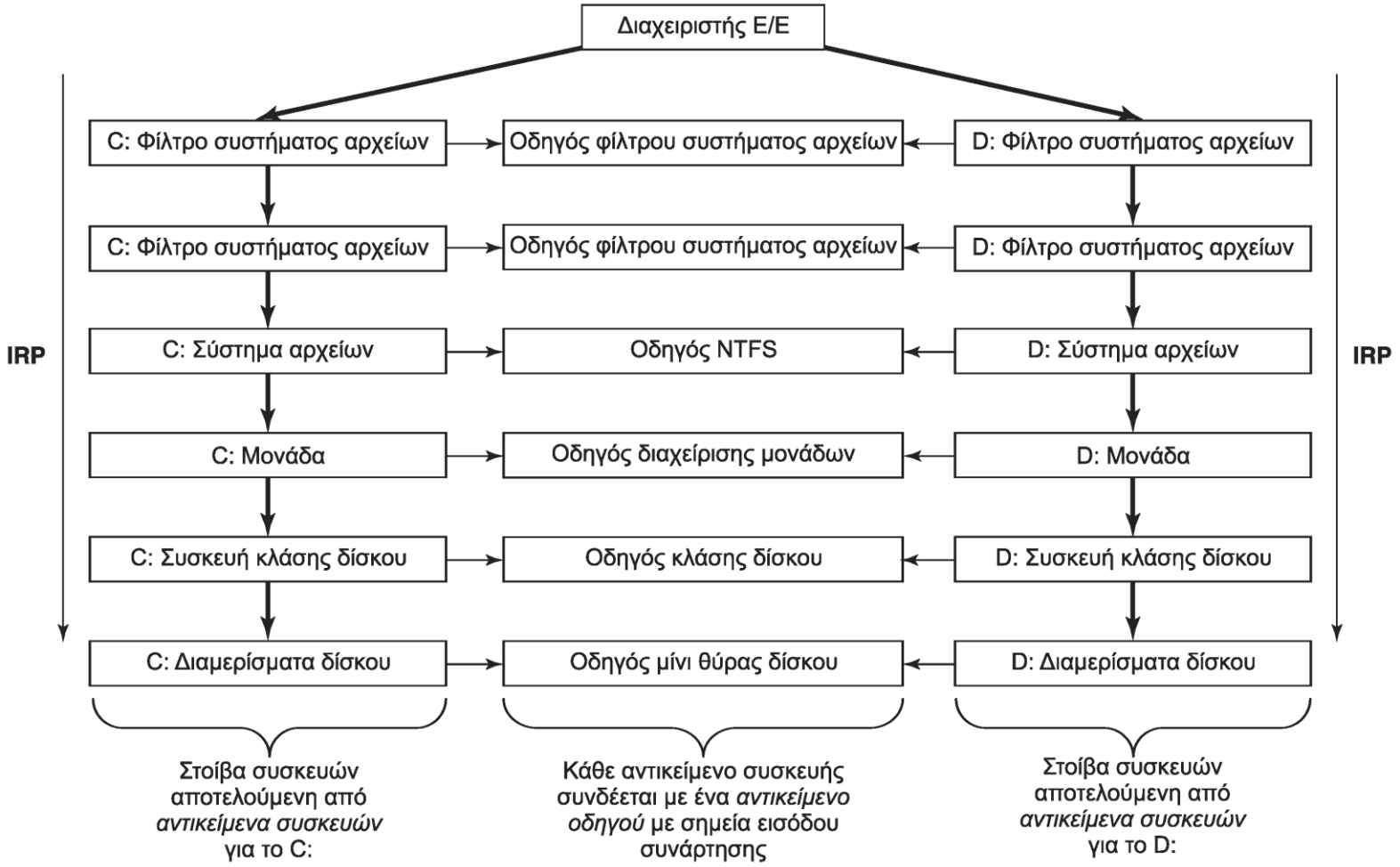
Εκτελεστικό επίπεδο (4 από 4)

- Ελεγκτής αναφορών ασφαλείας
  - Υλοποιεί κεντρικά τους ελέγχους αναφορών
- Διαχειριστής διευθέτησης
  - Υλοποιεί το μητρώο
- Τοπικές κλήσεις διαδικασιών (LPC)
  - Επικοινωνία διεργασιών στο ίδιο σύστημα
    - Χρήση και για τοπικές RPC
    - Επικοινωνία βιβλιοθήκης με διεργασία υποσυστήματος

Οδηγοί συσκευών (1 από 2)

- Γενικός μηχανισμός επέκτασης πυρήνα
  - Και τα συστήματα αρχείων είναι οδηγοί
- Κάθε συσκευή έχει μία στοίβα (device stack)
  - Αποτελείται από ιδιωτικά αντικείμενα συσκευής
    - Συνδέονται με οδηγούς κοινής χρήσης
    - Ορισμένοι οδηγοί λειτουργούν ως φίλτρα
    - Παράδειγμα: κρυπτογραφία, συμπίεση
    - Οδηγός κλάσης (π.χ. USB) και μίνι θύρα (συσκευή)

Οδηγοί συσκευών (2 από 2)



Εκκίνηση (1 από 2)

- Βήματα εκκίνησης
  - Το BIOS φορτώνει το MBR του βασικού δίσκου
  - Το MBR φορτώνει το BootMgr από το δίσκο
  - Μετά από αδράνεια/αναμονή WinResume.exe
  - Για νέα εκκίνηση WinLoad.exe
  - Φόρτωση πυρήνα/εκτελεστικού και HAL
  - Φόρτωση κυψέλης SYSTEM και βασικού Win32
  - Φόρτωση οδηγών εκκίνησης (στην SYSTEM)

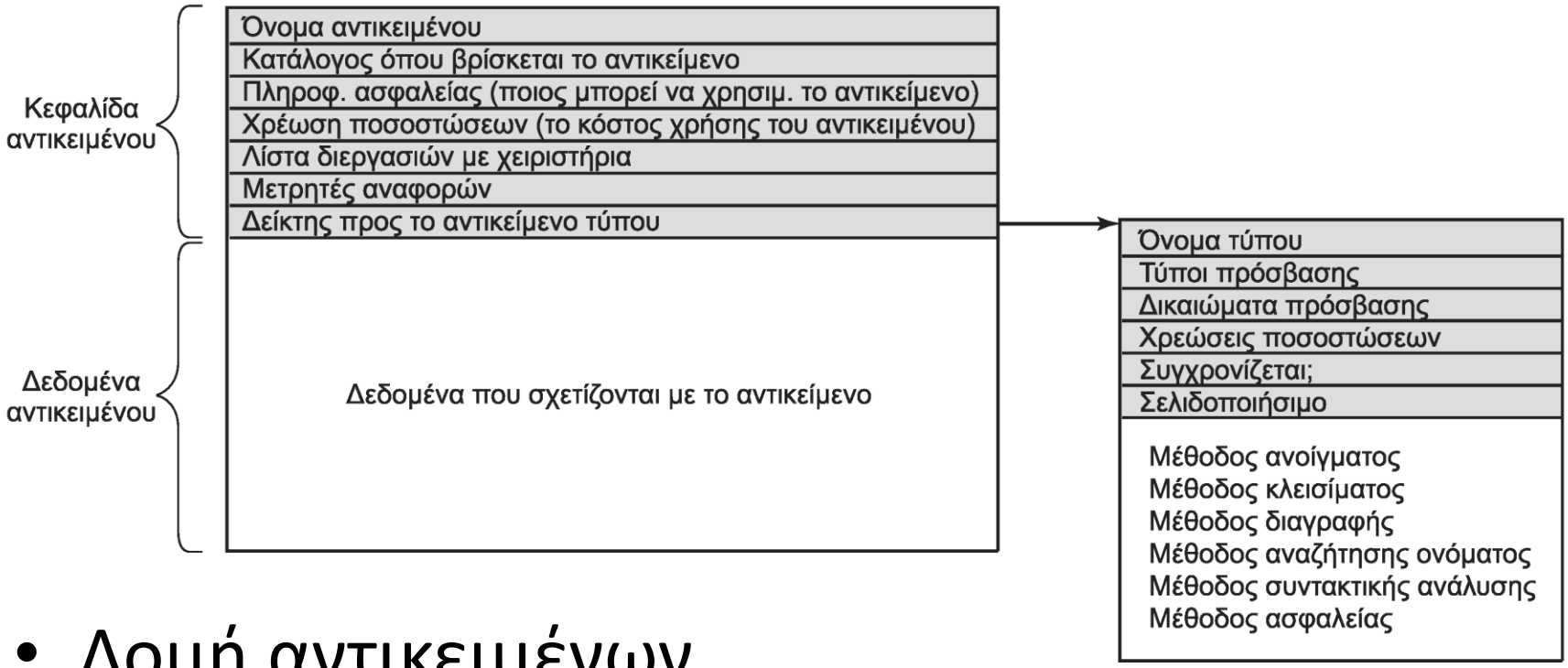
Εκκίνηση (2 από 2)

- Αρχικοποίηση λειτουργικού
  - Αρχικοποίηση HAL, πυρήνα, εκτελεστικού
  - Σύνδεση οδηγών και ενημέρωση SYSTEM
  - Δημιουργία διεργασίας smss.exe
- Ειδικές μορφές εκκίνησης
  - Με τελευταία λειτουργική διάρθρωση
  - Με ασφαλή τρόπο λειτουργίας
  - Με κονσόλα ανάκαμψης (γραμμή διαταγών)

Διαχειριστής αντικειμένων (1 από 3)

- Ενιαία διεπαφή διαχείρισης πόρων
  - Αρχεία, διεργασίες, νήματα, …
    - Δομές δεδομένων που παριστάνουν πόρους
    - Δημιουργούνται δυναμικά στη μνήμη του πυρήνα
    - Ακόμη και οι τύποι αντικειμένων είναι δυναμικοί
  - Υποστήριξη χειριστηρίων και ονομάτων
    - Τα χειριστήρια χρησιμοποιούνται στις κλήσεις
    - Προαιρετικά μπορούμε να έχουμε και ονόματα

Διαχειριστής αντικειμένων (2 από 3)

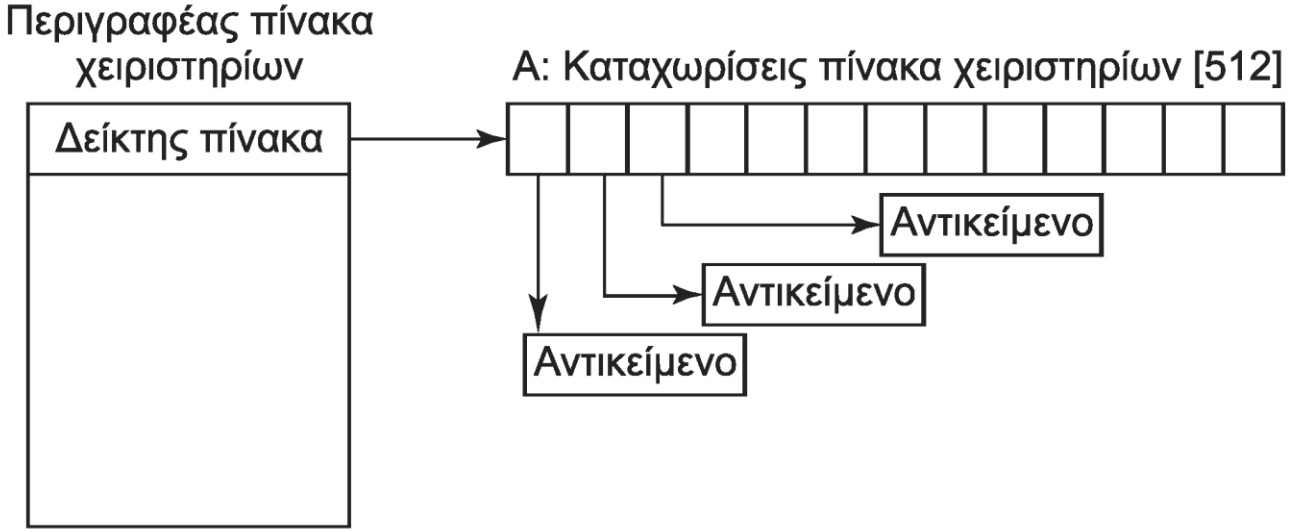


- Δομή αντικειμένων
  - Κοινή κεφαλίδα αντικειμένων
  - Δεδομένα αντικειμένου

Διαχειριστής αντικειμένων (3 από 3)

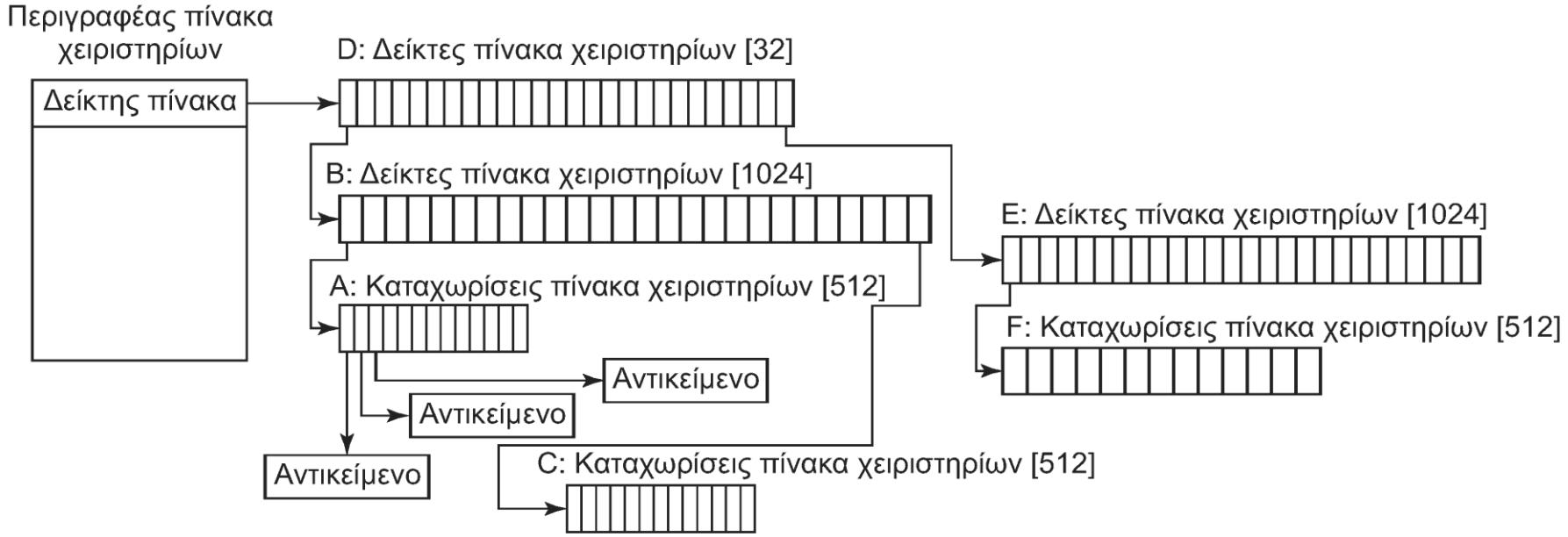
- Μνήμη αντικειμένων
  - Σελιδοποιήσιμη και μη σελιδοποιήσιμη
    - Μη σελιδοποιήσιμη για χειριστές διακοπών
    - Γενικά όπου δεν θέλουμε σφάλματα σελίδας
- Πεδίο χρέωσης (quota) στην κεφαλίδα
  - Ο χρήστης έχει όρια χρεώσεων
- Μετρητής αναφορών στην κεφαλίδα
  - Αποφυγή πρόωρης απελευθέρωσης αντικειμένου

Χειριστήρια (1 από 3)



- Χειριστήριο: αναφορά σε αντικείμενο πυρήνα
  - Οι δείκτες είναι επικίνδυνοι
  - Ο διαχειριστής αντικειμένων δημιουργεί αναφορές
  - Κάθε διεργασία έχει πίνακα χειριστηρίων

Χειριστήρια (2 από 3)



- Πίνακες χειριστηρίων πολλών επιπέδων
  - Για διεργασίες με πάρα πολλά χειριστήρια
- Χωριστός πίνακας για τον ίδιο τον πυρήνα

Χειριστήρια (3 από 3)

- Δημιουργία χειριστηρίων
  - Η διεργασία εκτελεί κάποια κλήση Win32
  - Τελικά εκτελείται μία κλήση συστήματος
  - Παράγεται ένα χειριστήριο 64 bit
    - Μπαίνει στον πίνακα χειριστηρίων της διεργασίας
    - Ο χρήστης παίρνει τη θέση του χειριστηρίου (32 bit)
  - Πρώτα 29 bit: δείκτης σε αντικείμενο
    - Τα 3 τελευταία bit είναι σημαίες
  - Επόμενα 32 bit: δικαιώματα στο αντικείμενο

Ονόματα αντικειμένων (1 από 10)

- Γιατί να έχουμε και ονόματα;
  - Ευκολότερος καταμερισμός αντικειμένων
    - Αλλιώς πρέπει να έχουμε χειριστήρια σε διεργασίες
  - Διατήρηση αντικειμένων στη μνήμη
    - Συσκευές και οδηγοί
  - Μπορούμε να δίνουμε ονόματα σε αντικείμενα
  - Ιεραρχικός χώρος ονομάτων
  - Το αντικείμενο πρέπει να υποστηρίζει ονόματα

Ονόματα αντικειμένων (2 από 10)

Διαδικασία	Πότε καλείται	Σημειώσεις
Open	Για κάθε νέο χειριστήριο	Χρησιμοποιείται σπάνια
Parse	Για τύπους αντικειμένων που επεκτείνουν το χώρο ονομάτων	Χρησιμοποιείται για αρχεία και κλειδιά του μητρώου
Close	Όταν κλείνει το τελευταίο χειριστήριο	Εκκαθάριση ορατών παρενεργειών
Delete	Κατά την τελευταία αποαναφοροποίηση (dereference) δείκτη	Το αντικείμενο πρόκειται να διαγραφεί σύντομα
Security	Λήψη ή ρύθμιση περιγραφέα ασφαλείας αντικειμένου	Προστασία
QueryName	Λήψη ονόματος αντικειμένου	Χρησιμοποιείται σπάνια έξω από τον πυρήνα

- Διαδικασίες που ορίζει ένα αντικείμενο
  - Επανακλήσεις από τον διαχειριστή αντικειμένων
  - Διάκριση κλεισίματος και διαγραφής

Ονόματα αντικειμένων (3 από 10)

- Parse: επέκταση χώρου ονομάτων
  - Ένα φύλλο της ιεραρχίας μπορεί να έχει parse
  - Στην parse περνάμε το υπόλοιπο όνομα
    - Παράδειγμα: αντικείμενα αρχείων
    - Το φύλλο παριστάνει ένα σύστημα αρχείων
    - Η parse χειρίζεται το όνομα του αρχείου
    - Οδηγεί σε δημιουργία αντικειμένου αρχείου
- Γενικές κλήσεις για όλα τα αντικείμενα

Ονόματα αντικειμένων (4 από 10)

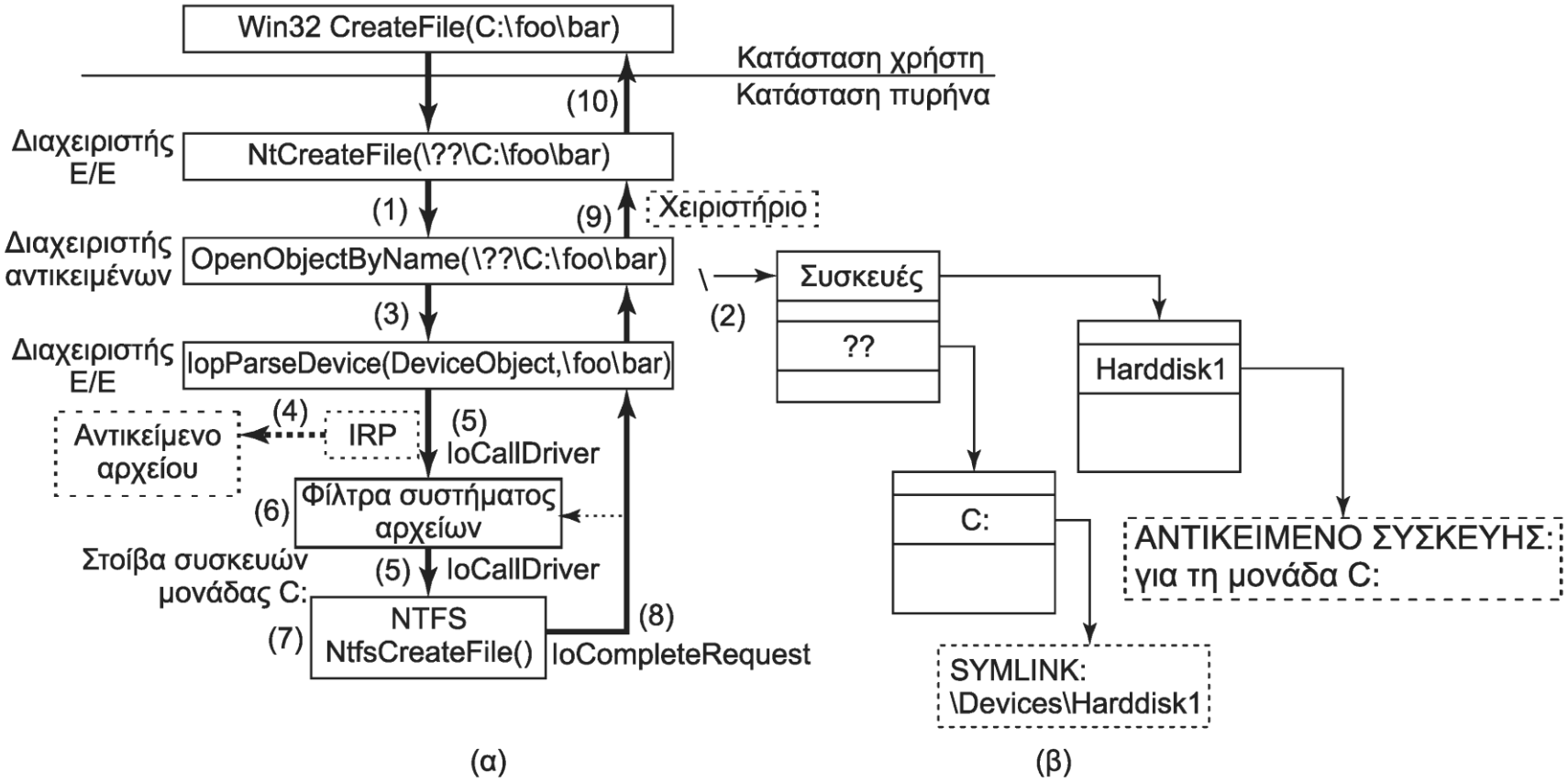
Κατάλογος	Περιεχόμενα
??	Αφετηρία αναζήτησης συσκευών MS-DOS όπως η μονάδα C:
DosDevices (Συσκευές DOS)	Επίσημο όνομα του ??, αλλά στην πραγματικότητα είναι ένας συμβολικός σύνδεσμος προς το ??
Device (Συσκευή)	Όλες οι εντοπισμένες συσκευές Ε/Ε
Driver (Οδηγός)	Αντικείμενα που αντιστοιχούν σε κάθε φορτωμένο οδηγό συσκευής
ObjectTypes (Τύποι αντικειμένων)	Οι τύποι αντικειμένων, όπως αυτοί της Εικόνας 11-22
Windows (Παράθυρα)	Αντικείμενα για την αποστολή μηνυμάτων σε όλα τα παράθυρα του GUI του Win32
BaseNamedObjects (Βασικά επώνυμα αντικείμενα)	Δημιουργημένα από το χρήστη αντικείμενα του Win32, όπως σηματοφόροι, mutex, κλπ.
Arcname	Ονόματα διαμερισμάτων που εντόπισε ο φορτωτής εκκίνησης (boot loader)
NLS	Αντικείμενα υποστήριξης εθνικών γλωσσών
FileSystem (Σύστημα αρχείων)	Αντικείμενα οδηγών συστήματος αρχείων και αντικείμενα αναγνώρισης του συστήματος αρχείων
Security (Ασφάλεια)	Αντικείμενα που ανήκουν στο σύστημα ασφαλείας
KnownDLLs (Γνωστές DLL)	Κοινόχρηστες από κλειδιά βιβλιοθήκες που ανοίγουν νωρίς και διατηρούνται ανοιχτές

- Μέρος του χώρου ονομάτων των Windows

Ονόματα αντικειμένων (5 από 10)

- Χειριστήρια και δείκτες
  - Κάθε αντικείμενο έχει δύο μετρητές αναφορών
  - Κάθε χειριστήριο αντιστοιχεί σε έναν δείκτη
  - Υπάρχουν και δείκτες χωρίς χειριστήρια
    - Το αντικείμενο διατηρείται χωρίς αναφορές χρήστη
- Προβλήματα νημάτων με τα χειριστήρια
  - Εύκολο να γίνουν σφάλματα
  - Εκχώρηση χειριστηρίων με FIFO αντί για LIFO

Ονόματα αντικειμένων (6 από 10)



Παράδειγμα χρήσης αντικειμένου συσκευής

Ονόματα αντικειμένων (7 από 10)

- Δημιουργία αρχείου βήμα προς βήμα
  - Κλήση CreateFile σε επίπεδο Win32
  - Κλήση NtCreateFile στον πυρήνα
    - Μετατροπή ονόματος σε μορφή NT (\??\...)
  - Κλήση OpenObjectByName
    - Το όνομα αντιστοιχεί σε αντικείμενο συσκευής
    - Το αντικείμενο είναι φύλλο με διαδικασία parse
  - Κλήση IopParseDevice με συσκευή και όνομα

Ονόματα αντικειμένων (8 από 10)

- Δημιουργία αρχείου βήμα προς βήμα
  - Δημιουργία πακέτου αίτησης Ε/Ε (IRP)
  - Αποστολή IRP στη στοίβα Ε/Ε
    - Περνάει από φίλτρα, π.χ. αντιβιοτικό αρχείων
  - Τελικά καλείται η NtfsCreateFile (για NTFS)
  - Δημιουργία αντικειμένου αρχείου
  - Αποστολή αντικειμένου στη στοίβα Ε/Ε
  - Δημιουργία και επιστροφή χειριστηρίου στο χρήστη

Ονόματα αντικειμένων (9 από 10)

Τύπος	Περιγραφή
Διεργασία (process)	Διεργασία χρήστη
Νήμα (thread)	Νήμα μέσα σε μια διεργασία
Σηματοφόρος (semaphore)	Σηματοφόρος καταμέτρησης που χρησιμοποιείται για διαδιεργασιακό συγχρονισμό
Mutex	Δυαδικός σηματοφόρος που χρησιμοποιείται για την είσοδο σε κρίσιμη περιοχή
Συμβάν (event)	Αντικείμενο συγχρονισμού που βρίσκεται σε μόνιμη κατάσταση (σηματοδοτημένο/όχι)
Θύρα ALPC (ALPC port)	Μηχανισμός μεταβίβασης μηνυμάτων μεταξύ διεργασιών
Χρονόμετρο (timer)	Αντικείμενο που επιτρέπει σε ένα νήμα να "κοιμηθεί" για συγκεκριμένο χρονικό διάστημα
Ουρά (queue)	Αντικείμενο που χρησιμοποιείται για τη γνωστοποίηση της ολοκλήρωσης ασύγχρονης Ε/Ε

- Τύποι αντικειμένων Windows
  - Μπορούν να προστεθούν νέοι

Ονόματα αντικειμένων (10 από 10)

Ανοιχτό αρχείο (open file)	Αντικείμενο συσχετισμένο με ένα ανοιχτό αρχείο
Σκυτάλη πρόσβασης (access token)	Περιγραφέας ασφαλείας για κάποιο αντικείμενο
Προφίλ (profile)	Δομή δεδομένων που χρησιμοποιείται για την ανάλυση της χρήσης της CPU
Ενότητα (section)	Αντικείμενο που χρησιμοποιείται για την αναπαράσταση χαρτογραφήσιμων αρχείων
Κλειδί (key)	Κλειδί μητρώου, που χρησιμοποιείται για τη σύνδεση του μητρώου με το χώρο ονομάτων του διαχειριστή αντικειμένων
Κατάλογος αντικειμένων (object directory)	Κατάλογος για την ομαδοποίηση αντικειμένων μέσα στο διαχειριστή αντικειμένων
Συμβολικός σύνδεσμος (symbolic link)	Δείκτης προς ένα άλλο αντικείμενο του διαχειριστή αντικειμένων μέσω του ονόματος διαδρομής
Συσκευή (device)	Αντικείμενο συσκευής Ε/Ε για μια φυσική συσκευή, δίαυλο, οδηγό, ή παρουσία μονάδας
Οδηγός συσκευής (device driver)	Κάθε φορτωμένος οδηγός συσκευής διαθέτει το δικό του αντικείμενο

- Τύποι αντικειμένων Windows (συνέχεια)

Επίπεδο χρήστη (1 από 3)

- Μέρος του ΛΣ είναι σε επίπεδο χρήστη
  - Υποσυστήματα, DLL, υπηρεσίες χρήστη
- Υποσυστήματα περιβάλλοντος
  - Επιτρέπουν διαφορετικές προσωπικότητες
  - Τελικά μόνο η προσωπικότητα Win32 επιβίωσε
- Βιβλιοθήκες δυναμικής σύνδεσης (DLL)
  - Επιτρέπουν καταμερισμό κώδικα
  - Κίνδυνος από διαφορές στις εκδόσεις

Επίπεδο χρήστη (2 από 3)

- Υλοποίηση DLL
  - Ο μεταγλωττιστής δεν εισάγει άμεσες κλήσεις
    - Παραγωγή Πίνακα Διευθύνσεων Εισαγωγής (IAT)
  - Συμπλήρωση IAT με τη φόρτωση του κώδικα
    - Δημιουργία γράφου εξαρτήσεων των DLL
    - Εκτέλεση κώδικα αρχικοποίησης του DLL
    - Κίνδυνος αδιεξόδου λόγω κυκλικών αναφορών
  - Δυνατότητα συνύπαρξης εκδόσεων DLL

Επίπεδο χρήστη (3 από 3)

- Υπηρεσίες επιπέδου χρήστη
  - Συμπληρώνουν τον πυρήνα
    - Παράδειγμα: lsass.exe για πιστοποίηση ταυτότητας
  - Σημαντικό κόστος χρήσης
    - Μεταγωγή συμφραζομένων δύο φορές
    - Δύσκολη πρόσβαση στη μνήμη του χρήστη
  - Δυνατότητα εκτέλεσης στην ίδια διεργασία
    - Η svchost εκτελεί πολλές υπηρεσίες συστήματος
    - Εκτελούνται με τα ίδια προνόμια και μοιράζονται νήματα

Διεργασίες και νήματα

Μάθημα: Λειτουργικά Συστήματα, **Ενότητα # 9:** Το ΛΣ Windows

Διδάσκων: Γιώργος Ξυλωμένος, **Τμήμα:** Πληροφορικής

CC BY NC ND

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο
ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΕΚΠΑΙΔΕΥΣΗ ΚΑΙ ΔΙΑ ΒΙΟΥ ΜΑΘΗΣΗ
επένδυση στην κοινωνία της γνώσης
ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ & ΘΡΗΣΚΕΥΜΑΤΩΝ, ΠΟΛΙΤΙΣΜΟΥ & ΑΘΛΗΤΙΣΜΟΥ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ
ΕΣΠΑ 2007-2013
πρόγραμμα για την ανάπτυξη
ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΩΝΙΚΟ ΤΑΜΕΙΟ
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

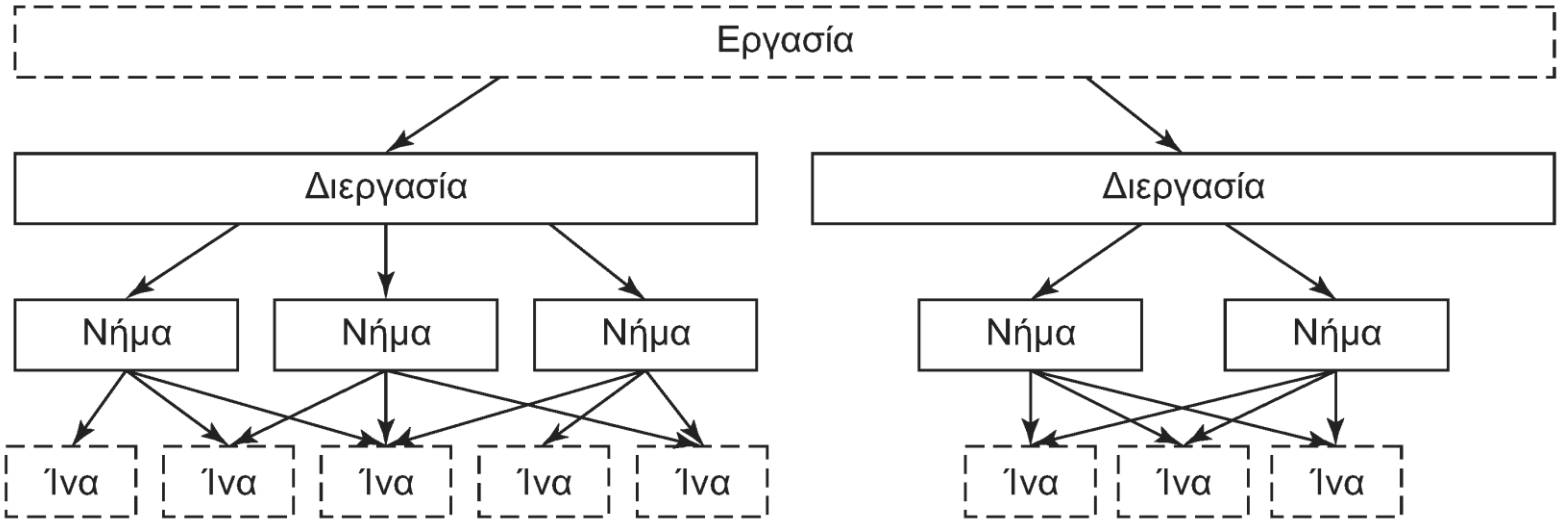
Έννοιες διεργασιών (1 από 5)

- Διεργασίες: αποδέκτες προγραμμάτων
  - Εικονικός χώρος μνήμης, χειριστήρια, νήματα
  - Μπλοκ περιβάλλοντος διεργασίας (PEB)
    - Λίστα φορτωμένου κώδικα
    - Περιβάλλον, κατάλογος, σωροί
- Νήματα: χρονοπρογραμματισμός
  - Στοίβα πυρήνα και χρήστη
  - Μπλοκ περιβάλλοντος νήματος (TEB)
    - Τοπική αποθήκευση νήματος

Έννοιες διεργασιών (2 από 5)

- Κοινόχρηστα δεδομένα χρήστη
  - Κοινή σε πυρήνα και όλες τις διεργασίες
  - Μόνο ο πυρήνας την γράφει
    - Πληροφορίες ώρας, έκδοσης, φυσικής μνήμης
- Διεργασίες
  - Ο δημιουργός έχει χειριστήριο για τη διεργασία
    - Δυνατότητα αλλαγής μνήμης, αντιγραφής χειριστηρίων
    - Ρητός χειρισμός διεργασίας σε αντίθεση με τη fork()

Έννοιες διεργασιών (3 από 5)



- Εργασίες (jobs)
  - Ομαδοποίηση διεργασιών σε εργασίες
  - Χρήση για κοινή διαχείριση πόρων
    - Κατάλληλες για επεξεργασία δέσμης

Έννοιες διεργασιών (4 από 5)

Όνομα	Περιγραφή	Σημειώσεις
Εργασία	Συλλογή διεργασιών που μοιράζονται ποσοστώσεις και όρια	Χρησιμοποιείται σπάνια
Διεργασία	Αποδέκτης για τη δέσμευση πόρων	
Νήμα	Οντότητα που χρονοπρογραμματίζεται από τον πυρήνα	
Ίνα	Ελαφρό νήμα του οποίου η διαχείριση γίνεται εξολοκλήρου στο χώρο χρήστη	Χρησιμοποιείται σπάνια

- Ίνες (fibers)
  - Τα νήματα απεικονίζονται σε ίνες
  - Αλλαγή ίνας σε επίπεδο χρήστη
    - Ο πυρήνας και οι βιβλιοθήκες τις αγνοούν
    - Χρήση για μεταφορά κώδικα από άλλα συστήματα

Έννοιες διεργασιών (5 από 5)

- Νήματα
  - Ίδιος χώρος αναγνωριστικών με διεργασίες (!)
  - Χρήση στοίβας πυρήνα σε κλήσεις συστήματος
    - Αποθήκευση καταχωρητών στη βάση της στοίβας
  - Η διαχείριση πόρων είναι θέμα διεργασίας
    - Όλα τα νήματα βλέπουν τα ίδια χειριστήρια
- Διεργασία συστήματος: νήματα πυρήνα
  - Κώδικας πυρήνα ανεξάρτητος από χρήστες
    - Παράδειγμα: νήματα διαχείρισης μνήμης

Δημιουργία διεργασιών

- Δημιουργία διεργασίας: CreateProcess
  - Εκτελέσιμο αρχείο, γραμμή διαταγών, περιβάλλον
    - Τα Win32 δεν επεκτείνουν τη γραμμή διαταγών
  - Και πολλές άλλες παράμετροι
    - Ασφάλεια, χρονοπρογραμματισμός, χειριστήρια, GUI
    - Ρητός χειρισμός των ρυθμίσεων της διεργασίας
  - Επιστρέφει χειριστήρια/ID για διεργασία/νήμα
  - Υλοποιείται με απλούστερες κλήσεις των NT

Επικοινωνία διεργασιών

- Αγωγοί (pipes): είτε byte είτε μηνυμάτων
  - Υπάρχουν και επώνυμοι αγωγοί
- Ταχυδρομικές θυρίδες (mailslots)
  - Αγωγοί αλλά με πολλούς παραλήπτες
- Υποδοχές τύπου Berkeley
- Απομακρυσμένες κλήσεις διαδικασιών (RPC)
  - Χρήση και στην ίδια μηχανή μέσω LPC
- Καταμερισμένα αντικείμενα: κοινή μνήμη

Συγχρονισμός (1 από 4)

- Σηματοφόροι: CreateSemaphore
  - Κοινή χρήση είτε με χειριστήριο είτε με όνομα
  - ReleaseSemaphore αντί για up
  - WaitForSingleObject αντί για down
    - Εναλλακτικά, WaitForMultipleObjects
- Mutex: σηματοφόροι χωρίς μετρητές
  - ReleaseMutex για απελευθέρωση
  - Ίδιες κλήσεις με σηματοφόρους για αναμονή

Συγχρονισμός (2 από 4)

- Κρίσιμες περιοχές
  - Χρήση μόνο μέσα σε μία διεργασία
  - EnterCriticalSection και LeaveCriticalSection
    - Χρήση κλειδωμάτων περιστροφής
    - Μπλοκάρισμα στον πυρήνα όταν είναι απαραίτητο
- Συμβάντα (events)
  - Σηματοδοτημένα ή μη σηματοδοτημένα
  - SetEvent για σηματοδότηση
  - WaitForSingleObject για αναμονή

Συγχρονισμός (3 από 4)

- Δύο είδη συμβάντων
  - Διαφέρουν στο τι γίνεται όταν σηματοδοτηθούν
  - Γνωστοποίησης: ελευθερώνονται όλα τα νήματα
  - Συγχρονισμού: ελευθερώνεται ένα νήμα
- Δύο είδη σηματοδότησης
  - PulseEvent: αν δεν περιμένει κανείς, χάνεται
  - SetEvent: η σηματοδότηση παραμένει ενεργή

Συγχρονισμός (4 από 4)

Συνάρτηση Win32 API	Περιγραφή
CreateProcess	Δημιουργεί μια νέα διεργασία
CreateThread	Δημιουργεί ένα νέο νήμα μέσα σε μια υπάρχουσα διεργασία
CreateFiber	Δημιουργεί μια νέα ίνα
ExitProcess	Τερματίζει την τρέχουσα διεργασία και όλα τα νήματά της
ExitThread	Τερματίζει αυτό το νήμα
ExitFiber	Τερματίζει αυτή την ίνα
SwitchToFiber	Εκτελεί μια διαφορετική ίνα στο τρέχον νήμα
SetPriorityClass	Καθορίζει την κατηγορία προτεραιότητας για μια διεργασία
SetThreadPriority	Καθορίζει την προτεραιότητα ενός νήματος
CreateSemaphore	Δημιουργεί ένα νέο σηματοφόρο
CreateMutex	Δημιουργεί ένα νέο mutex
OpenSemaphore	Ανοίγει έναν υπάρχοντα σηματοφόρο
OpenMutex	Ανοίγει ένα υπάρχον mutex
WaitForSingleObject	Μπλοκάρεται περιμένοντας ένα σηματοφόρο, mutex, κλπ.
WaitForMultipleObjects	Μπλοκάρεται περιμένοντας ένα σύνολο αντικειμένων των οποίων παρέχονται τα χειριστήρια
PulseEvent	Ορίζει ένα συμβάν ως σηματοδοτημένο και μετά ως μη σηματοδοτημένο
ReleaseMutex	Αποδεσμεύει ένα mutex ώστε να μπορεί να το αποκτήσει ένα άλλο νήμα
ReleaseSemaphore	Αυξάνει το μετρητή σηματοφόρων κατά 1
EnterCriticalSection	Αποκτά το κλείδωμα για μια κρίσιμη περιοχή
LeaveCriticalSection	Αποδεσμεύει το κλείδωμα για μια κρίσιμη περιοχή

Υλοποίηση διεργασιών (1 από 3)

- Κλήση CreateProcess στο Win32
- Μετατροπή ονόματος αρχείου σε όνομα NT
- Κλήση της NtCreateUserProcess
- Δημιουργία αντικειμένου ενότητας με εικόνα
- Δημιουργία αντικειμένου διεργασίας
- Δημιουργία χώρου διευθύνσεων
- Δημιουργία πίνακα χειριστηρίων

Υλοποίηση διεργασιών (2 από 3)

- Χαρτογράφηση ενότητας και κοινής σελίδας
- Δημιουργία PEB διεργασίας
- Εκχώρηση εικονικής μνήμης
- Εκχώρηση ταυτότητας διεργασίας
- Δημιουργία TEB νήματος
- Προσθήκη διεργασίας σε δομές πυρήνα
- Επιστροφή από NtCreateUserProcess

Υλοποίηση διεργασιών (3 από 3)

- Σε περίπτωση αποτυχίας
  - Έλεγχος αν η διεργασία θέλει άλλο υποσύστημα
    - Παράδειγμα: WOW64
- Εγγραφή διεργασίας στο υποσύστημα Win32
  - Εμφάνιση δείκτη με κλεψύδρα στην οθόνη
- Τροποποίηση δικαιωμάτων (αν χρειάζεται)
- Προσθήκη βιβλιοθηκών συμβατότητας
- Κλήση NtResumeThread για εκκίνηση νήματος

Χρονοπρογραμματισμός (1 από 10)

- Περιπτώσεις κλήσεις χρονοπρογραμματιστή
  - Μπλοκάρισμα εκτελούμενου νήματος
    - Αναγκαστική κλήση του χρονοπρογραμματιστή
  - Σηματοδότηση ενός αντικειμένου
    - Έλεγχος για νήμα υψηλότερης προτεραιότητας
  - Εξάντληση κβάντου
    - Προκαλείται από διακοπή ρολογιού
    - Μπορεί να συνεχίσει και η ίδια διεργασία

Χρονοπρογραμματισμός (2 από 10)

- Περιπτώσεις κλήσεις χρονοπρογραμματιστή
  - Ολοκλήρωση λειτουργίας Ε/Ε
  - Λήξη προθεσμίας αναμονής
    - Η ISR προσθέτει μία DPC στην ουρά
    - Η DPC θα καλέσει τον χρονοπρογραμματιστή
    - Έλεγχος για νήμα υψηλότερης προτεραιότητας
- Αλγόριθμος χρονοπρογραμματισμού
  - Δύο είδη προτεραιοτήτων

Χρονοπρογραμματισμός (3 από 10)

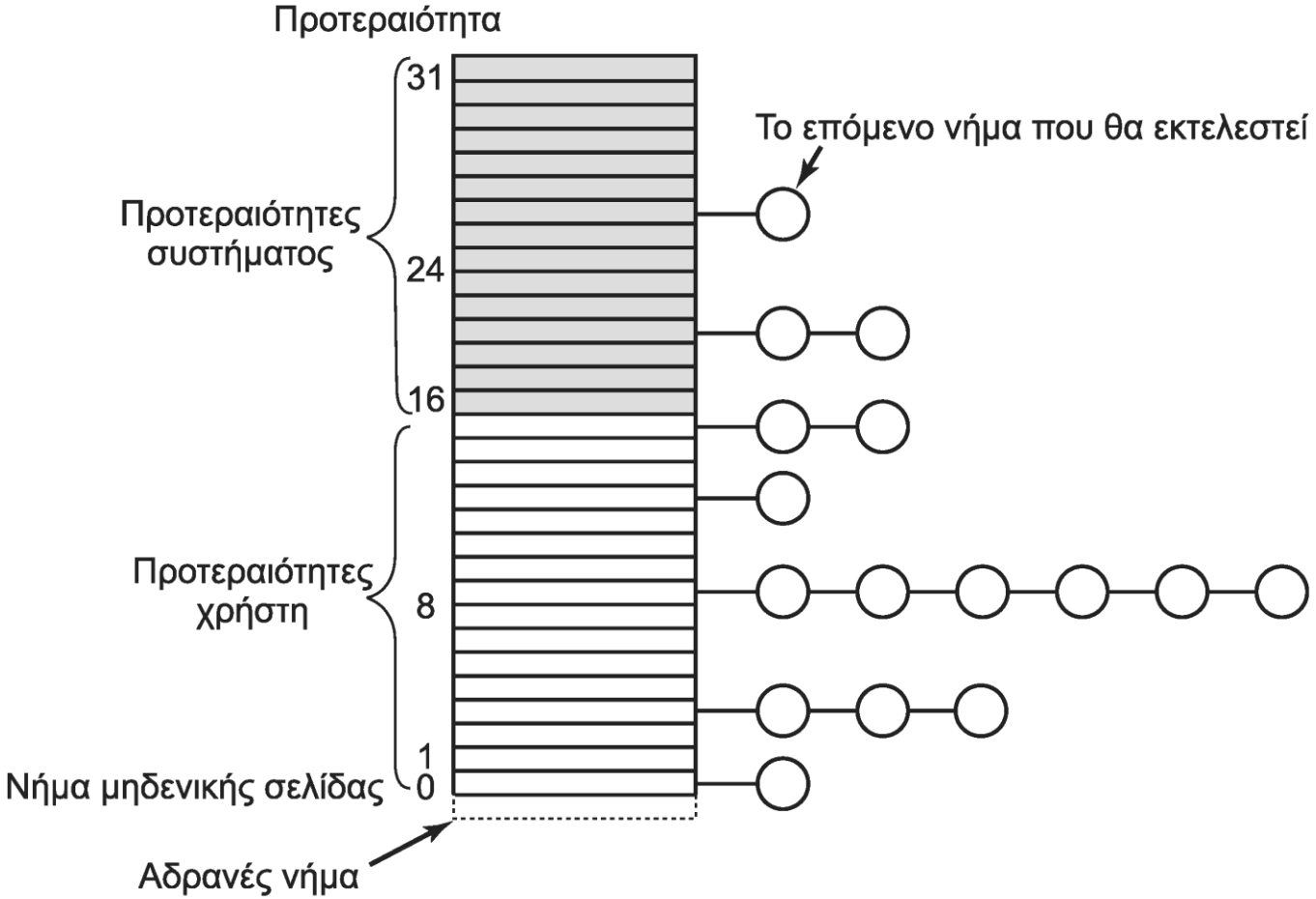
- Κατηγορία προτεραιότητας: SetPriorityClass
  - Βασική προτεραιότητα νημάτων διεργασίας
  - Πραγματικού χρόνου έως αδρανής
- Προτεραιότητα νήματος: SetThreadPriority
  - Σχετική προτεραιότητα νημάτων διεργασίας
  - Χρονικά κρίσιμη ως αδρανής
- Συνδυασμός για παραγωγή τιμής 1-31
  - Βασική προτεραιότητα νήματος

Χρονοπρογραμματισμός (4 από 10)

		Κατηγορίες προτεραιοτήτων για τις διεργασίες Win32					
Win32 Προτεραιότητες νημάτων		Πραγμα-τικού χρόνου	Υψηλή	Υψηλότε-ρη από την κανο-νική	Κανονική	Χαμηλότε-ρη από την κανο-νική	Αδρανής
	Χρονικά κρίσιμη	31	15	15	15	15	15
	Ανώτατη	26	15	12	10	8	6
	Υψηλότερη από την κανονική	25	14	11	9	7	5
	Κανονική	24	13	10	8	6	4
	Χαμηλότερη από την κανονική	23	12	9	7	5	3
	Κατώτατη	22	11	8	6	4	2
	Αδρανής	16	1	1	1	1	1

Υπολογισμός βασικής προτεραιότητας

Χρονοπρογραμματισμός (5 από 10)



Σύστημα πολλαπλών ουρών Windows

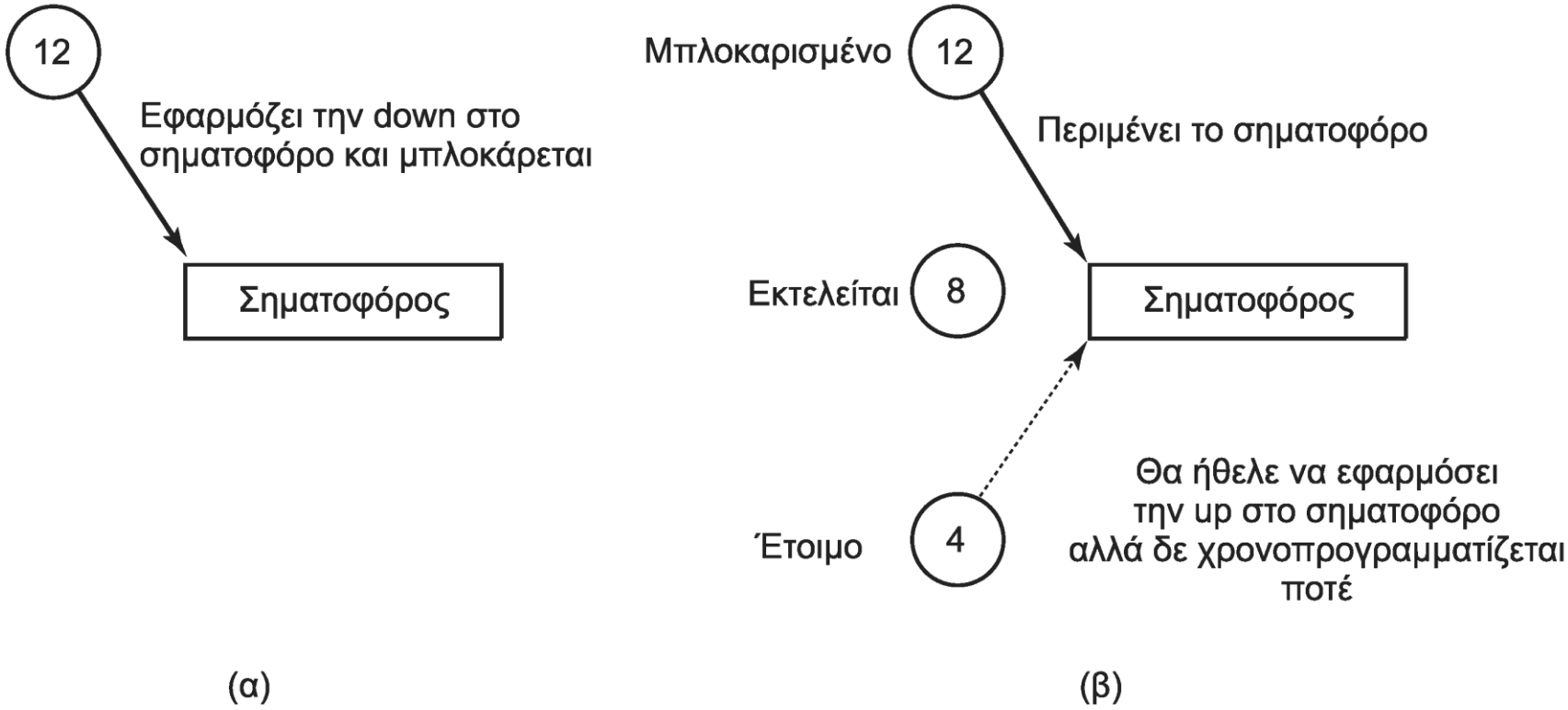
Χρονοπρογραμματισμός (6 από 10)

- Υλοποίηση ουρών προτεραιότητας
  - Εκτέλεση πάντα της υψηλότερης προτεραιότητας
  - Εκ περιτροπής εκτέλεση σε κάθε προτεραιότητα
  - Επίπεδα 16-31: πραγματικού χρόνου
    - Τρέχουν αμέσως μετά από ISR και DPC
  - Επίπεδα 1-15: διεργασίες χρηστών
  - Επίπεδο 0: νήμα μηδενισμού σελίδων
  - Επίπεδο -1: αδρανές νήμα

Χρονοπρογραμματισμός (7 από 10)

- Πραγματική προτεραιότητα νήματος
  - Ξεκινάει από τη βασική προτεραιότητα
  - Αύξηση σε κάθε τερματισμό λειτουργίας Ε/Ε
    - +1 για δίσκο, +6 πληκτρολόγιο, +8 κάρτα ήχου
    - Δεν περνάει ποτέ το 15 όμως
  - Αύξηση μετά από αναμονή συγχρονισμού
    - +2 στο προσκήνιο, +1 στο παρασκήνιο
  - -1 σε κάθε λήξη κβάντου
    - Μέχρι τη βασική προτεραιότητα όμως

Χρονοπρογραμματισμός (8 από 10)



- Αντιστροφή προτεραιοτήτων
  - Η 8 εκτελείται πριν την 12 λόγω της 4

Χρονοπρογραμματισμός (9 από 10)

- Αντιμετώπιση αντιστροφής προτεραιοτήτων
  - Παρακολούθηση χρόνου αναμονής νήματος
  - Μετά από κάποιο όριο, πάει στο επίπεδο 15
    - Μένει εκεί για δύο κβάντα
    - Μετά επιστρέφει εκεί που ήταν
- Ιδανικός επεξεργαστής νήματος
  - Χρήσιμο σε συστήματα NUMA
  - Το νήμα εκτελείται εκεί που είναι η μνήμη του

Χρονοπρογραμματισμός (10 από 10)

- Μέγεθος κβάντου
  - Στους πελάτες είναι 20 msec
  - Στους διακομιστές είναι 120 msec
  - Μπορεί να πολλαπλασιαστεί από τον διαχειριστή
- Προτεραιότητα διεργασίας προσκηνίου
  - Έστω ότι ένα παράθυρο έρχεται στο προσκήνιο
  - Όλα του τα νήματα έχουν αυξημένο κβάντο
    - Βελτίωση της εμπειρίας του χρήστη

ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ATHENS UNIVERSITY OF ECONOMICS AND BUSINESS

Διαχείριση μνήμης

Μάθημα: Λειτουργικά Συστήματα, **Ενότητα # 9:** Το ΛΣ Windows

Διδάσκων: Γιώργος Ξυλωμένος, **Τμήμα:** Πληροφορικής

CC BY NC ND

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο

ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΕΚΠΑΙΔΕΥΣΗ ΚΑΙ ΔΙΑ ΒΙΟΥ ΜΑΘΗΣΗ
επένδυση στην κοινωνία της γνώσης
ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ & ΘΡΗΣΚΕΥΜΑΤΩΝ, ΠΟΛΙΤΙΣΜΟΥ & ΑΘΛΗΤΙΣΜΟΥ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ

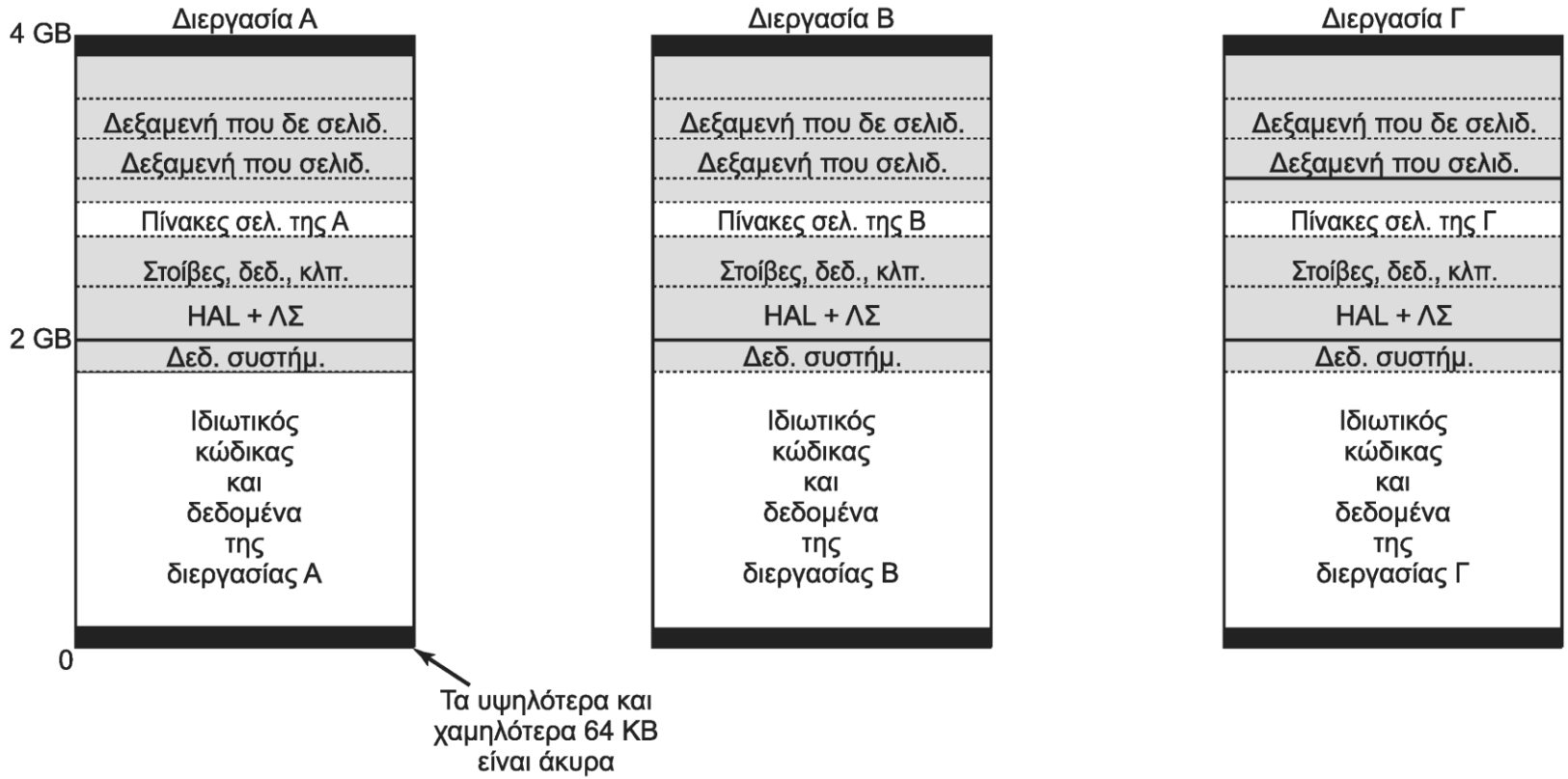
ΕΣΠΑ 2007-2013
πρόγραμμα για την ανάπτυξη
ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΩΝΙΚΟ ΤΑΜΕΙΟ

Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Χώροι διευθύνσεων (1 από 2)

- Χώρος διευθύνσεων διεργασίας
  - 32 bit: 2 GB χρήστης + 2 GB πυρήνας
    - 3 GB χρήστης στις εκδόσεις διακομιστή
  - 64 bit: 4 GB και σε διεργασίας 32 bit (WOW64)
  - Μέγεθος σελίδας 4 KB ή (σπάνια) 4 MB
  - Δεν χρησιμοποιούνται 64+64KB στα άκρα
    - Εντοπισμός συνήθως προβλημάτων με δείκτες
  - Ο πυρήνας είναι κοινός σε όλες τις διεργασίες

Χώροι διευθύνσεων (2 από 2)



- Τυπικοί χάρτες μνήμης διεργασιών
  - Ίδιος χάρτης μνήμης και σε κατάσταση πυρήνα

Εκχώρηση εικονικής μνήμης

- Τρεις καταστάσεις σελίδων
  - Άκυρη: δεν αντιστοιχεί σε ενότητα μνήμης
  - Κατακυρωμένη: αντιστοιχεί σε ενότητα
    - Σφάλμα σελίδας οδηγεί σε προσκόμιση της σελίδας
    - Ήπιο σφάλμα αν είναι διαθέσιμη στην κρυφή μνήμη
  - Δεσμευμένη: θα χρειαστεί στο μέλλον
    - Οι σελίδες στοίβας είναι δεσμευμένες
    - Όσο μεγαλώνει η στοίβα γίνονται κατακυρωμένες

Αρχεία σελιδοποίησης (1 από 2)

- Χρήση για μη χαρτογραφημένες σελίδες
  - Δέσμευση χώρου μόνο όταν εκτοπίζονται
    - Με αρκετή μνήμη δεν χρειάζεται τέτοιο αρχείο
    - Χρήσιμο σε ενσωματωμένα συστήματα
  - Ομαδοποίηση εκτοπισμένων σελίδων
    - Εκχώρηση γειτονικών θέσεων στο δίσκο
    - Ομαδική εγγραφή των σελίδων
  - Η εκχώρηση μένει μέχρι να γραφτεί η σελίδα
    - Στη φόρτωση η σελίδα σημειώνεται ως μόνο ανάγνωσης

Αρχεία σελιδοποίησης (2 από 2)

- Υποστήριξη έως 16 αρχείων
  - Σε διαφορετικούς δίσκους για απόδοση
  - Καλύτερα να δεσμεύεται χώρος από την αρχή
- Παρακολούθηση μέσω πίνακα σελίδων
- Δεν χρησιμοποιείται για όλες τις σελίδες
  - Προγράμματα και DLL διαβάζονται από το δίσκο
  - Τα χαρτογραφημένα αρχεία είναι στο δίσκο

Πολύ μεγάλες μνήμες

- Εναλλαγή σειράς (bank switching)
  - Εναλλαγή τμημάτων φυσικής μνήμης
    - Φυσική μνήμη >> χώρου διευθύνσεων
  - Συνηθισμένο σε συστήματα 16/20 bit
    - 8088/8086 και συμβατοί επεξεργαστές
  - Τελικά χρειάστηκε και σε συστήματα 32 bit
    - PAE: διευθύνσεις 36 bit σε μηχανή 32 bit
    - Λέγεται Επεκτάσεις Διευθύνσεων σε Παράθυρα (AWE)

Κλήσεις διαχείρισης μνήμης

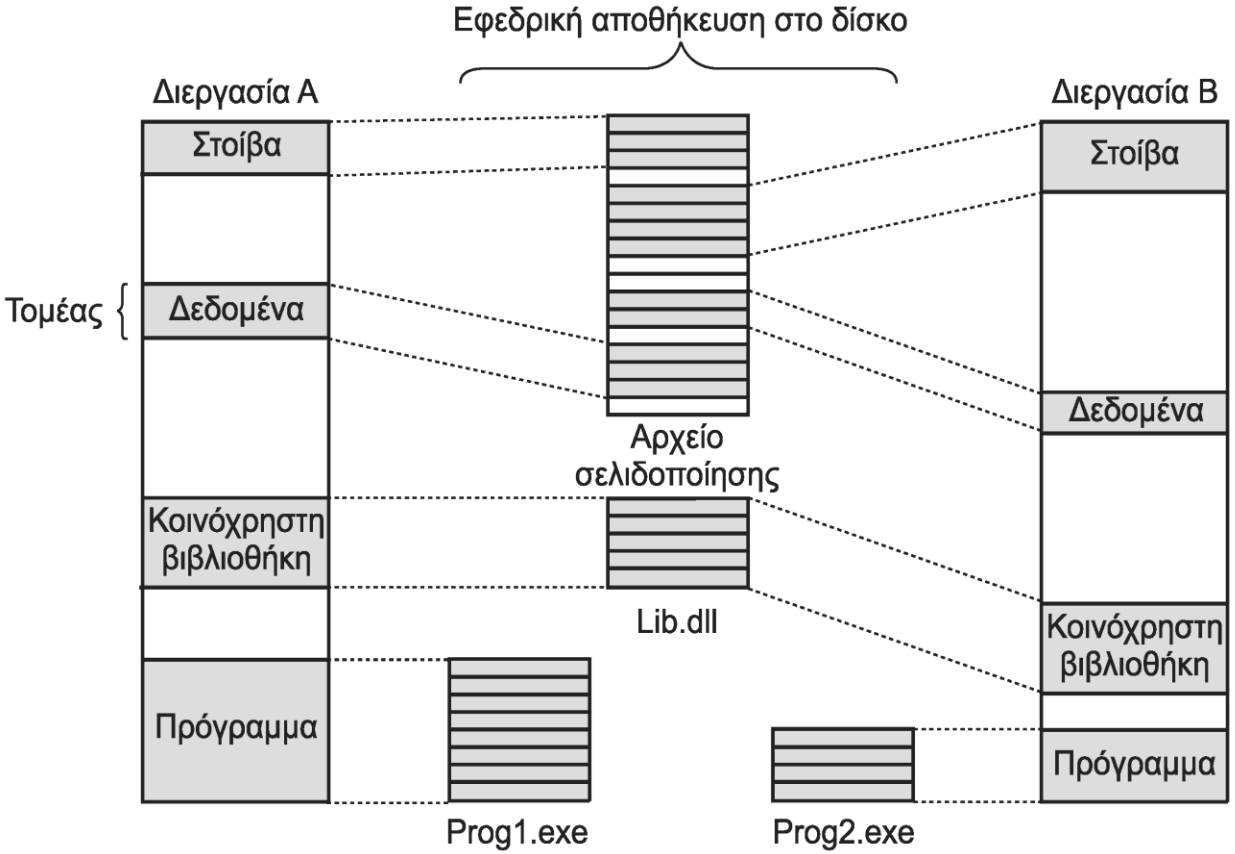
Συνάρτηση Win32 API	Περιγραφή
VirtualAlloc	Δεσμεύει ή κατακυρώνει μια περιοχή
VirtualFree	Αποδεσμεύει ή καταργεί την κατακύρωση μιας περιοχής
VirtualProtect	Αλλάζει την προστασία ανάγνωσης/εγγραφής/εκτέλεσης μιας περιοχής
VirtualQuery	Διερευνά την κατάσταση μιας περιοχής
VirtualLock	Κάνει μια περιοχή παραμένουσα στη μνήμη (απενεργοποιεί τη σελιδοποίησή της)
VirtualUnlock	Κάνει μια περιοχή σελιδοποιήσιμη με το συνηθισμένο τρόπο
CreateFileMapping	Δημιουργεί ένα αντικείμενο χαρτογράφησης αρχείου και (προαιρετικά) του δίνει ένα όνομα
MapViewOfFile	Χαρτογραφεί ένα αρχείο (ή μέρος του) στο χώρο διευθύνσεων
UnmapViewOfFile	Αφαιρεί ένα χαρτογραφημένο αρχείο από το χώρο διευθύνσεων
OpenFileMapping	Ανοίγει ένα αντικείμενο χαρτογράφησης αρχείου που έχει δημιουργηθεί

- Λειτουργούν σε συνεχόμενες περιοχές
  - Ακέραιο πλήθος σελίδων, αρχή σε όριο 64 KB

Υλοποίηση μνήμης (1 από 2)

- Ενιαίος γραμμικός χώρος διευθύνσεων
  - Συνήθως σελίδες 4 KB
  - Δυνατότητα σελίδων 4 MB
    - Καλύτερη αξιοποίηση TLB
    - Μικρότεροι πίνακες σελίδων ενός επιπέδου
    - Κατάλληλο για πολύ μεγάλες εφαρμογές
  - Για κάθε περιοχή έχουμε έναν VAD
    - Διευθύνσεις, αρχείο και απόσταση, προνόμια
    - Οργάνωση VAD σε ισορροπημένο δένδρο

Υλοποίηση μνήμης (2 από 2)



Κάθε διεργασία ορίζεται από τα VAD της

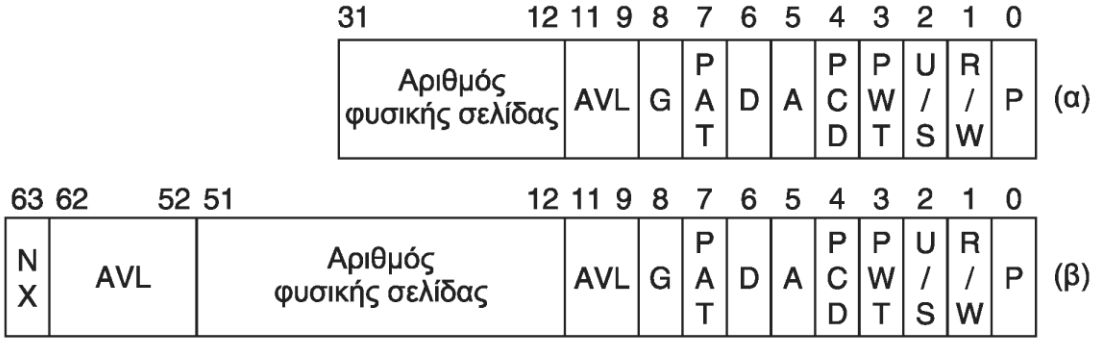
Σφάλματα σελίδας (1 από 6)

- Προσελιδοποίηση: τεχνολογία SuperFetch
  - Το σύστημα παρακολουθεί τις αναφορές σελίδων
  - Όταν ξεκινά μία διεργασία φορτώνει τις σελίδες
    - Επιπλέον φορτώνουμε ένα ολόκληρο μπλοκ δίσκου
  - Οι σελίδες μπαίνουν στη λίστα αναμονής
    - Αν χρησιμοποιηθούν, μπαίνουν στον πίνακα σελίδων
- Σελίδες που είναι ήδη στη μνήμη
  - Εκτελέσιμα αρχεία ή DLL
  - Αντιγραφή κατά την εγγραφή για δεδομένα

Σφάλματα σελίδας (2 από 6)

- Μη χαρτογραφημένες σελίδες
  - Οι σελίδες είναι πάντα μηδενισμένες
    - Για να μην διαβάζουμε δεδομένα άλλων
- Διαχείριση σφάλματος σελίδας
  - Ο πυρήνας δημιουργεί περιγραφή σφάλματος
  - Ο διαχειριστής μνήμης ελέγχει την προσπέλαση
    - Η σελίδα πρέπει να είναι κατακυρωμένη
  - Εντοπισμός του VAD της σελίδας

Σφάλματα σελίδας (3 από 6)



NX-No eXecute (Όχι εκτέλεση)
AVL-AVaiLable to the OS (Διαθέσιμη στο ΛΣ)
G-Global page (Καθολική σελίδα)
PAT-Page Attribute Table (Πίνακας Χαρακτηριστικών Σελίδας)
D-Dirty (Τροποποιημένο/"Βρώμικο")
A-Accessed (Προσπελασμένη)
PCD-Page Cache Disable (Απενεργοποίηση κρυφής μνήμης σελίδων)
PWT-Page Write-Through (Ταυτόχρονη εγγραφή σελίδας)
U/S-User/Supervisor (Χρήστης/Επόπτης)
R/W-Read/Write access (Πρόσβαση για ανάγνωση/εγγραφή)
P-Present (Παρούσα) ή Valid (Έγκυρη)

Καταχωρίσεις πίνακα σελίδων

Σφάλματα σελίδας (4 από 6)

- Μέγεθος καταχωρίσεων σελίδων
  - 32 ή 64 bit ανάλογα με αρχιτεκτονική
    - 64 bit όταν χρησιμοποιείται PAE
- Πέντε είδη σφαλμάτων σελίδας
- Μοιραία σφάλματα
  - Η σελίδα δεν είναι κατακυρωμένη
  - Η σελίδα δεν είναι προσπελάσιμη
    - Συνήθως τερματισμός διεργασίας

Σφάλματα σελίδας (5 από 6)

- Σελίδας αντιγραφής κατά την εγγραφή
  - Δημιουργία αντιγράφου της σελίδας
- Αύξηση μεγέθους στοίβας
  - Επιστρέφει μηδενισμένη σελίδα
  - Αρκεί να έχουν δεσμευθεί αρκετές σελίδες
- Μη χαρτογραφημένης σελίδας
  - Ήπιο σφάλμα: η σελίδα είναι στη μνήμη
  - Αυστηρό σφάλμα: η σελίδα είναι στο δίσκο

Σφάλματα σελίδας (6 από 6)

- Αφαίρεση σελίδων από πίνακα
  - Μπορεί να πάει σε τρεις διαφορετικές λίστες
  - Ελεύθερες: δεν θα χρειαστεί ξανά
    - Στοίβα διεργασίας που τερμάτισε
  - Τροποποιημένες: πρέπει να γραφτεί στο δίσκο
  - Αναμονής: δεν χρειάζεται να γραφτεί στο δίσκο
    - Οι τροποποιημένες πάνε εκεί όταν γραφούν
  - Οι δύο τελευταίες λειτουργούν ως κρυφή μνήμη

Αντικατάσταση σελίδων (1 από 2)

- Σύνολο εργασίας διεργασίας
  - Σελίδες διεργασίας στη μνήμη
    - Αλλάζει κατά την εκτέλεση της διεργασίας
  - Ελάχιστο και μέγιστο μέγεθος
    - Τα όρια είναι ελαστικά
  - Αρχικά κάθε διεργασία έχει τα ίδια όρια
    - 20-50 και 45-345 σελίδες ανάλογα με τη μνήμη
  - Περιορισμός στα όρια σε έλλειψη μνήμης

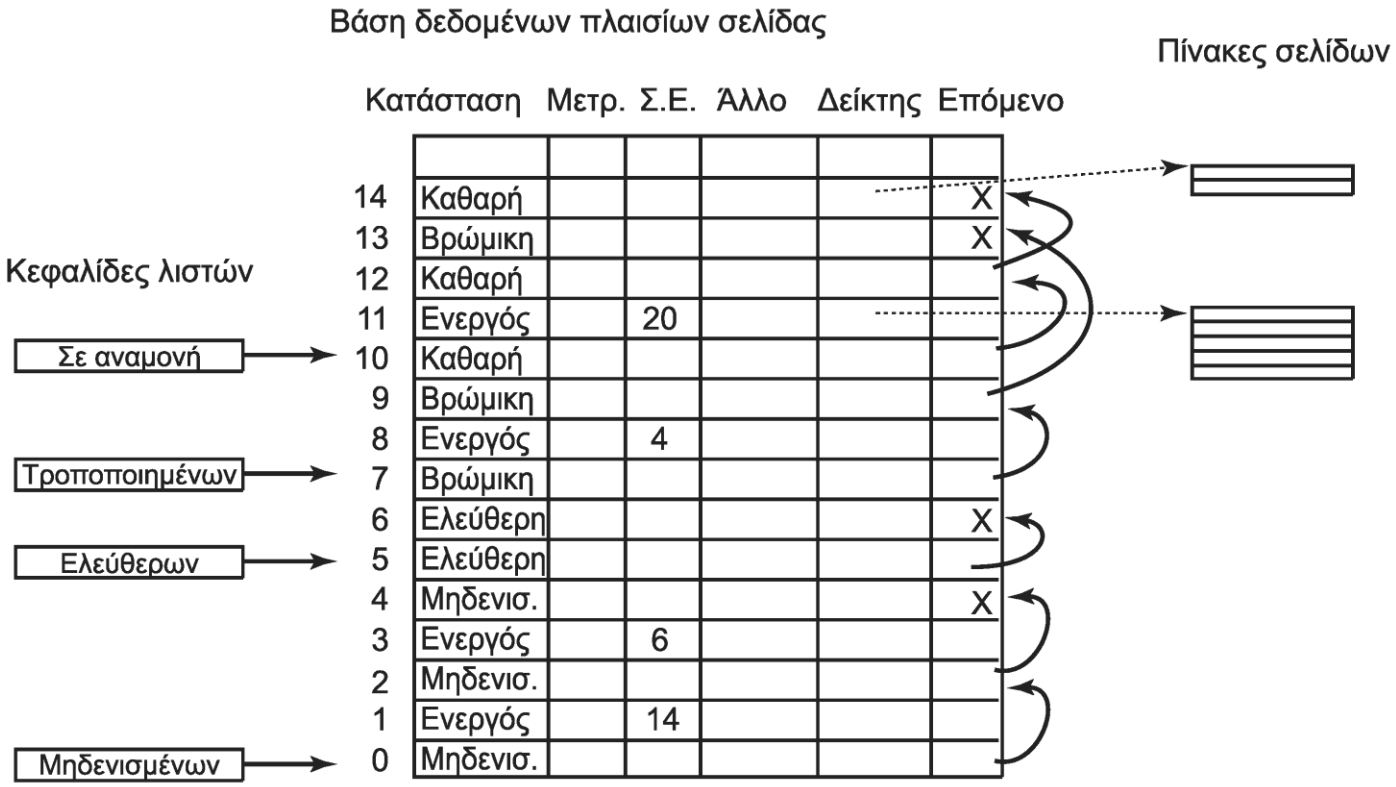
Αντικατάσταση σελίδων (2 από 2)

- Ο αλγόριθμος εξαρτάται από το χώρο
- Αρκετή διαθέσιμη μνήμη
  - Παρακολούθηση ηλικίας διεργασίας
- Μικρή πίεση μνήμης
  - Οι μεγάλες διεργασίες δεν μεγαλώνουν
    - Αντικατάσταση των σελίδων τους
- Μεγάλη πίεση μνήμης
  - Οι διεργασίες περιορίζονται στα όριά τους

Φυσική μνήμη (1 από 4)

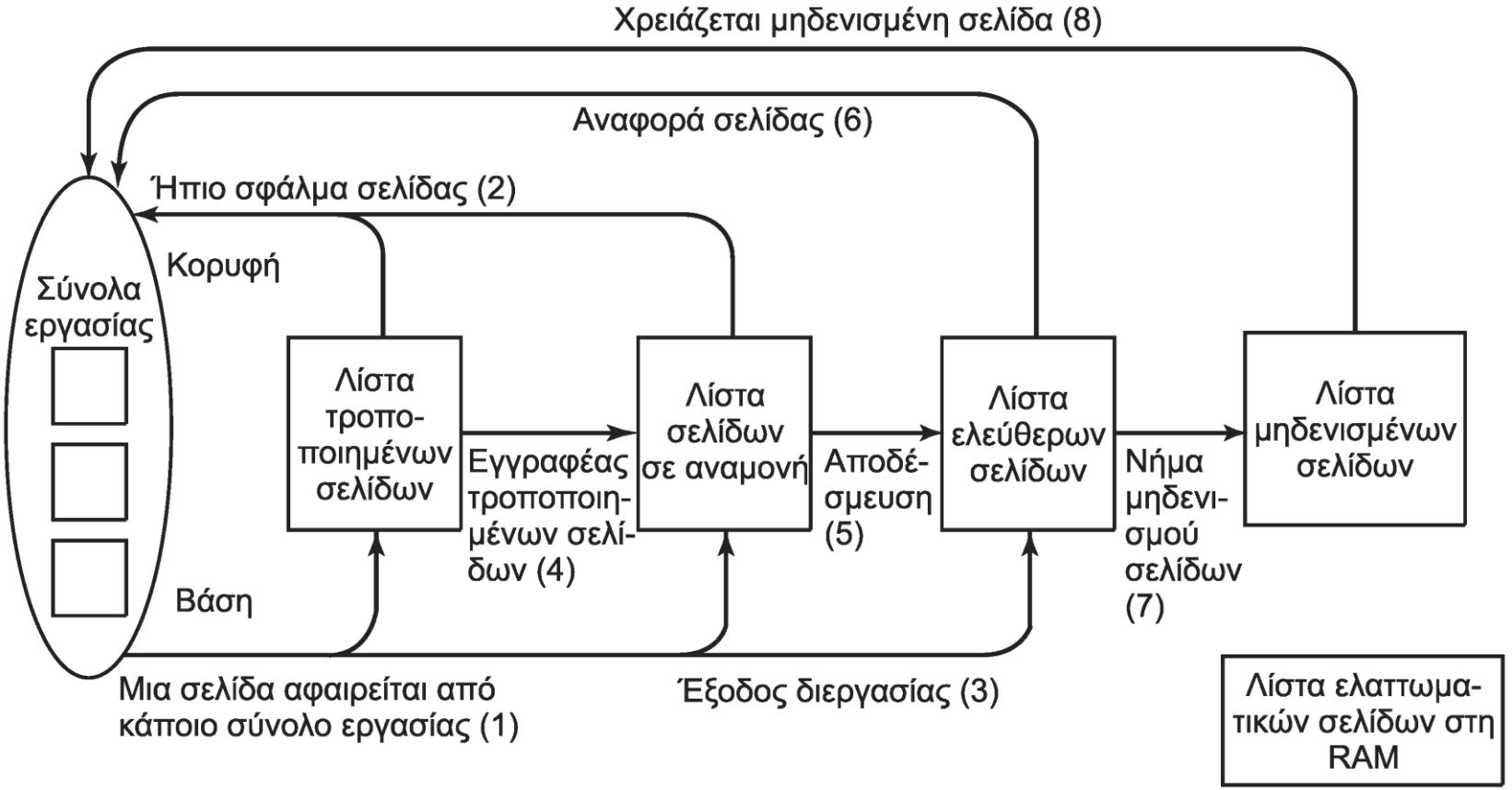
- Λίστα μηδενισμένων σελίδων
  - Για σελίδες που δεν φορτώνονται με δεδομένα
    - Μερικώς γεμάτες, σωρό, στοίβα
  - Ο μηδενισμός γίνεται στο παρασκήνιο
- Βάση δεδομένων αριθμών πλαισίων σελίδας
  - Πίνακας με όλα τα πλαίσια φυσικής μνήμης
  - Σταθερό μήκος καταχωρίσεων
  - Διαφορετικά στοιχεία σε κάθε καταχώρηση

Φυσική μνήμη (2 από 4)



- Βάση δεδομένων αριθμών πλαισίων σελίδας
  - Οργάνωση των πλαισίων σε λίστες

Φυσική μνήμη (3 από 4)



Κύκλος ζωής σελίδων

Φυσική μνήμη (4 από 4)

- Νήματα συστήματος για διαχείριση μνήμης
  - Διαχειριστής συνόλου ισορροπίας
    - Ψάχνει για αδρανείς διεργασίες
  - Εγγραφέας χαρτογραφημένων σελίδων
    - Μπορεί να χρειαστεί να μεγαλώσει το αρχείο
  - Εγγραφές τροποποιημένων σελίδων
    - Χρησιμοποιεί τα αρχεία σελιδοποίησης
  - Νήμα μηδενισμού σελίδων

Κρυφή μνήμη ΛΣ (1 από 3)

- Κρυφή μνήμη μπλοκ αρχείων
  - Χρήση εικονικών διευθύνσεων μπλοκ
    - Θέση μπλοκ στο αρχείο, όχι στη συσκευή
  - Οι αποθηκευμένες περιοχές λέγονται όψεις
    - Ο διαχειριστής κρυφής μνήμης επιλέγει όψεις
    - Ο διαχειριστής μνήμης χειρίζεται τις σελίδες
  - Χρήση μηδενικών σελίδων για κενά στα αρχεία
    - Αποφυγή ανάγνωσης δεδομένων τρίτων

Κρυφή μνήμη ΛΣ (2 από 3)

- Λειτουργία διαχειριστή κρυφής μνήμης
  - Έστω ότι γίνεται αναφορά σε ένα αρχείο
  - Χαρτογράφηση 256 KB στη μνήμη
    - Αν το μπλοκ ζητηθεί, διαβάζεται από το δίσκο
    - Αυτό είναι αρμοδιότητα του διαχειριστή μνήμης
  - Χρήση και για κανονικά χαρτογραφημένα αρχεία
  - Δυνατότητα παράκαμψης της κρυφής μνήμης
    - Αφήνει 3 GB εικονικής μνήμης στις εφαρμογές

Κρυφή μνήμη ΛΣ (3 από 3)

- Τεχνολογία ReadyBoost
  - Χρήση μνήμης flash ως κρυφής μνήμης
  - Συμπίεση και κρυπτογράφηση δεδομένων
  - Αποθήκευση με ταυτόχρονη εγγραφή
    - Αποφυγή προβλημάτων σε αφαίρεση flash
    - Μπορεί να αποφευχθεί με ενσωματωμένη flash
- Τεχνολογία ReadyBoot
  - Χρήση μνήμης flash για επιτάχυνση εκκίνησης

ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ATHENS UNIVERSITY OF ECONOMICS AND BUSINESS

Είσοδος / έξοδος

Μάθημα: Λειτουργικά Συστήματα, **Ενότητα # 9:** Το ΛΣ Windows

Διδάσκων: Γιώργος Ξυλωμένος, **Τμήμα:** Πληροφορικής

CC BY NC ND

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο

ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΕΚΠΑΙΔΕΥΣΗ ΚΑΙ ΔΙΑ ΒΙΟΥ ΜΑΘΗΣΗ
επένδυση στην κοινωνία της γνώσης
ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ & ΘΡΗΣΚΕΥΜΑΤΩΝ, ΠΟΛΙΤΙΣΜΟΥ & ΑΘΛΗΤΙΣΜΟΥ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ

ΕΣΠΑ 2007-2013
πρόγραμμα για την ανάπτυξη
ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΩΝΙΚΟ ΤΑΜΕΙΟ

Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Έννοιες Ε/Ε (1 από 4)

- Διαχειριστής τοποθέτησης και λειτουργίας (PnP)
  - Απαρίθμηση διαύλου
    - Είτε στην εκκίνηση (PCI) είτε δυναμικά (USB)
    - Αποστολή αίτησης σε κάθε υποδοχή του διαύλου
    - Κάθε συσκευή δίνει το αναγνωριστικό της
  - Διάρθρωση συσκευών
    - Κατανομή επιπέδων διακοπών
    - Δημιουργία αντικειμένων οδηγών
    - Δημιουργία αντικειμένων συσκευών

Έννοιες Ε/Ε (2 από 4)

- Φόρτωση υπόλοιπων οδηγών
  - Οδηγοί που δεν αντιστοιχούν σε συσκευές
    - Συστήματα αρχείων, αντιβιοτικά
    - Δεν μπορούν να φορτωθούν με PnP
  - Φόρτωση κατά την εκκίνηση
    - Χρήση αρχείων διάρθρωσης
  - Φόρτωση όταν χρειαστούν
    - Παράδειγμα: με την ανάρτηση συστήματος αρχείων

Έννοιες Ε/Ε (3 από 4)

- Δυναμικοί δίσκοι και λογικές μονάδες
  - Αποτελούνται από πολλά διαμερίσματα
    - Ακόμη και σε διαφορετικούς δίσκους
- Σκιώδη αντίγραφα μονάδων
  - Στιγμιότυπα μονάδων σε διάφορες στιγμές
  - Επαναφορά παλιάς κατάστασης
  - Εφεδρικά αντίγραφα σε συνεπή κατάσταση
    - Οι εφαρμογές διακόπτουν την κατάλληλη στιγμή
    - Λαμβάνεται στιγμιότυπο για το εφεδρικό αντίγραφο

Έννοιες Ε/Ε (4 από 4)

- Ασύγχρονη Ε/Ε: πολλοί τρόποι αναμονής
  - Αναμονή σε αντικείμενο συμβάντος
  - Προσθήκη συμβάντος ολοκλήρωσης σε ουρά
  - Διαδικασία επανάκλησης στο τέλος
  - Παρακολούθηση θέσης στη μνήμη
- Προτεραιότητες Ε/Ε
  - Υψηλή: διαχειριστής μνήμης
  - Χαμηλή: αντιβιοτικά, συντήρηση δίσκου

Κλήσεις Ε/Ε (1 από 3)

- Κλήσεις συστήματος διαχειριστή Ε/Ε
  - Άνοιγμα, κλείσιμο, ανάγνωση, εγγραφή, ioctl
  - Επιπλέον PnP και διαχείριση ισχύος
  - Στο Win32 κλήσεις ανάλογα με τη συσκευή
    - Απεικονίζονται σε απλούστερες κλήσεις NT
  - Πολλές παράμετροι και παραλλαγές
    - Παράδειγμα: τρόπος ενημέρωσης τέλους κλήσης
    - Απαραίτητο για ασύγχρονες κλήσεις

Κλήσεις Ε/Ε (2 από 3)

- Ιδιαιτερότητες κλήσεων Ε/Ε
  - Ίδια κλήση για δημιουργία/άνοιγμα αρχείου
  - Ανάγνωση/εγγραφή ορίζουν το δείκτη στο αρχείο
  - Ειδικές κλήσεις για παροχή πληροφοριών
    - Πιθανόν και για αλλαγή πληροφοριών
  - Δυνατότητα ειδοποίησης σε αλλαγές
    - Απλή επέκταση των ασύγχρονων κλήσεων
  - Κλείδωμα περιοχών αρχείων με κλειδί

Κλήσεις Ε/Ε (3 από 3)

Κλήση συστήματος για Ε/Ε	Περιγραφή
NtCreateFile	Άνοιγμα νέων ή υπαρχόντων αρχείων και συσκευών
NtReadFile	Ανάγνωση από αρχείο ή συσκευή
NtWriteFile	Εγγραφή σε αρχείο ή συσκευή
NtQueryDirectoryFile	Αίτηση πληροφοριών σχετικά με έναν κατάλογο και τα αρχεία του
NtQueryVolumeInformationFile	Αίτηση πληροφοριών σχετικά με μια μονάδα
NtSetVolumeInformationFile	Τροποποίηση πληροφοριών μονάδας
NtNotifyChangeDirectoryFile	Ολοκλήρωση όταν τροποποιείται οποιοδήποτε αρχείο του καταλόγου ή του υποδένδρου
NtQueryIInformationFile	Αίτηση πληροφοριών σχετικά με ένα αρχείο
NtSetInformation File	Τροποποίηση πληροφοριών αρχείου
NtLockFile	Κλείδωμα μιας περιοχής byte σε ένα αρχείο
NtUnlockFile	Αφαίρεση κλειδώματος περιοχής
NtFsControlFile	Διάφορες λειτουργίες σε ένα αρχείο
NtFlushBuffersFile	Εκκένωση των προσωρινών μνημών αρχείου από τη μνήμη στο δίσκο
NtCancelIoFile	Ακύρωση εκκρεμών λειτουργιών Ε/Ε για ένα αρχείο
NtDeviceIoControlFile	Ειδικές λειτουργίες σε μια συσκευή

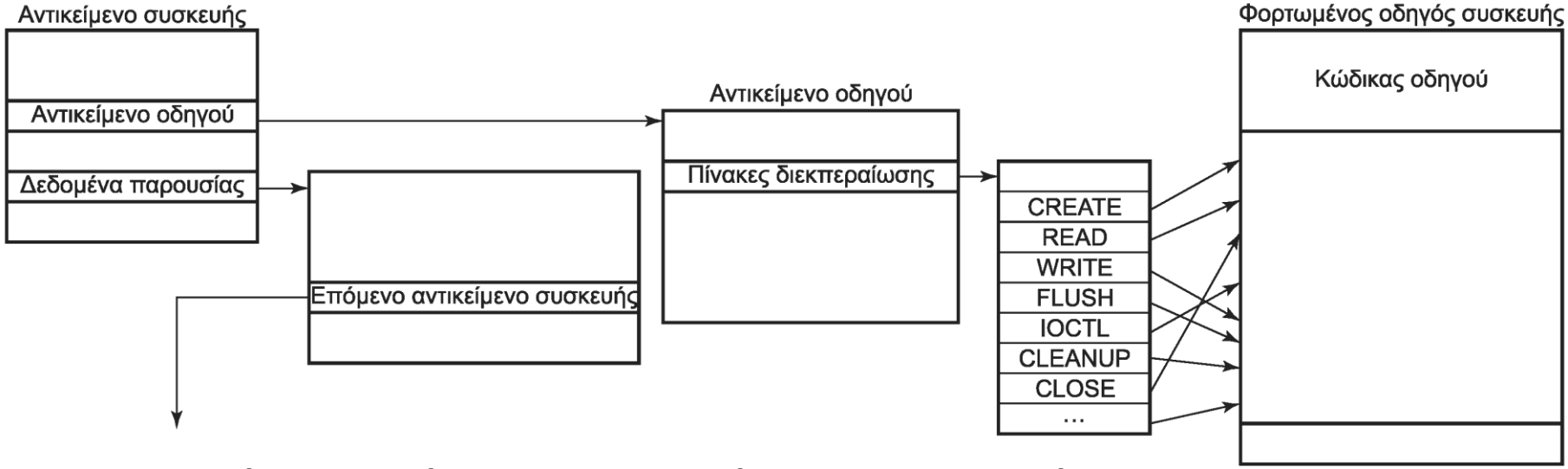
Οδηγοί συσκευών (1 από 3)

- Μοντέλο οδηγών των Windows (WDM)
  - Συμβατό με Windows 98 και 2000
    - Επέτρεπε χρήση οδηγών και στα δύο συστήματα
  - Βοήθημα επαλήθευσης οδηγών (verifier.exe)
    - Χρήσιμο στους διαχειριστές για έλεγχο οδηγών
- Θεμελίωση οδηγών των Windows (WDF)
  - Απλοποιημένο μοντέλο πάνω από το WDM
  - UMDF για οδηγούς επιπέδου χρήστη
  - KMDF για οδηγούς επιπέδου πυρήνα

Οδηγοί συσκευών (2 από 3)

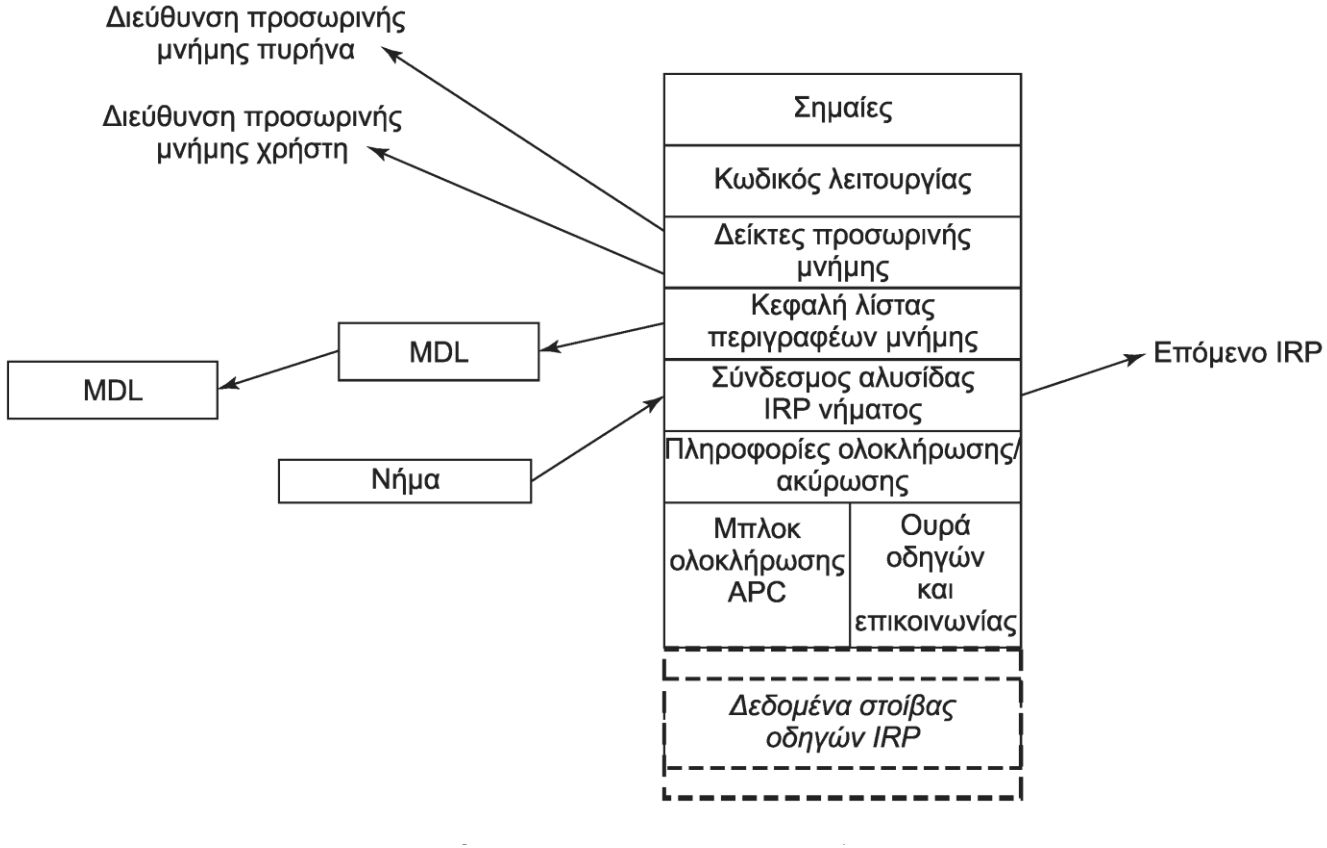
- Αντικείμενα συσκευών
  - Παριστάνουν συσκευές και όχι μόνο
    - Συστήματα αρχείων, πρωτόκολλα, …
  - Οργάνωση σε στοίβες συσκευών
- Κλήση της IoCallDriver από το διαχειριστή Ε/Ε
  - Δίνεται αντικείμενο IRP και αντικείμενο συσκευής
    - Το IRP αναφέρει τις λειτουργίες προς εκτέλεση
  - Εντοπισμός αντικειμένου οδηγού

Οδηγοί συσκευών (3 από 3)



- Σε κάθε επίπεδο καλείται ο οδηγός
  - Πίνακας διεκπεραίωσης στο αντικείμενο οδηγού
  - Κλήση της λειτουργίας που αναφέρει το IRP
- Τρεις δυνατότητες στο τέλος της κλήσης
  - Επόμενο επίπεδο, ολοκλήρωση ή εκκρεμότητα

Πακέτα αιτήσεων Ε/Ε (1 από 2)

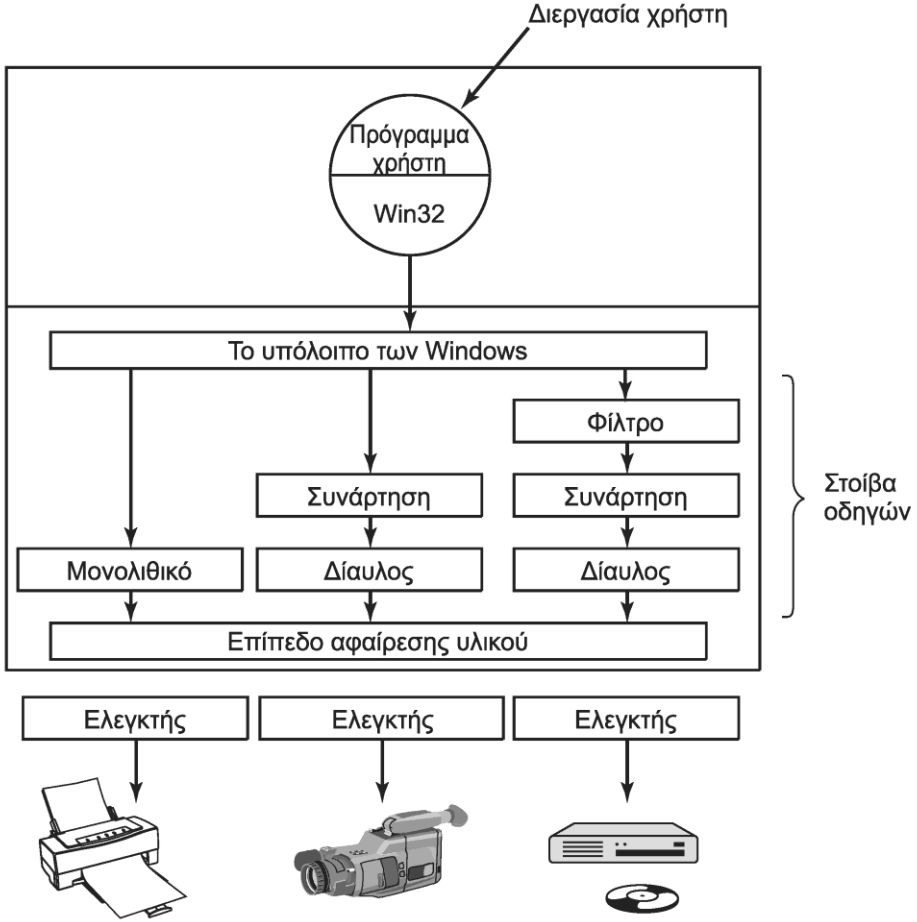


Μορφή πακέτου αίτησης Ε/Ε (IRP)

Πακέτα αιτήσεων Ε/Ε (2 από 2)

- Δεδομένα στοίβας οδηγών
  - Χώρος δεδομένων για κάθε οδηγό της στοίβας
    - Παράδειγμα: ρουτίνα που θα κληθεί στην ολοκλήρωση
  - Στην ολοκλήρωση ανεβαίνουμε στη στοίβα
    - Κλήση ρουτίνας ολοκλήρωσης σε κάθε επίπεδο
  - Ο διαχειριστής γνωρίζει το μέγεθος της στοίβας
    - Απαραίτητο για εκχώρηση αρκετής μνήμης στο IRP
- MDL: φυσικές σελίδες για DMA

Στοίβες συσκευών (1 από 4)



Παράδειγμα στοίβας συσκευών

Στοίβες συσκευών (2 από 4)

- Η στοίβα είναι προαιρετική
  - Μπορεί να υπάρχει ένας μόνος οδηγός
- Τυπικές δομές στοίβας οδηγών
  - Διαχωρισμός διαύλου από συσκευή
    - Ένας οδηγός για το δίαυλο PCI
    - Άλλος οδηγός για την ίδια τη συσκευή
  - Εισαγωγή φίλτρων στη στοίβα
    - Συμπίεση και αποσυμπίεση δεδομένων

Στοίβες συσκευών (3 από 4)

- Προβλήματα με οδηγούς συσκευών
  - Οι οδηγοί επιπέδου πυρήνα είναι επικίνδυνοι
    - Μοιράζονται το χώρο διευθύνσεων του πυρήνα
    - Εκτελούνται με προνόμια επόπτη
  - Το μοντέλο Ε/Ε είναι ισχυρό αλλά περίπλοκο
    - Ασύγχρονο μοντέλο σε πολυνηματικό σύστημα
    - Δυναμική εισαγωγή/εξαγωγή συσκευών
    - Δύσκολα οι προγραμματιστές αποφεύγουν τα λάθη

Στοίβες συσκευών (4 από 4)

- Διαχειριστής ισχύος
  - Κλείνει ή υποβαθμίζει μέρη του συστήματος
    - Μείωση συχνότητας λειτουργίας επεξεργαστή
    - Διακοπή λειτουργίας πυρήνων/επεξεργαστών
  - Κατάσταση αδράνειας (hibernation)
    - Αντιγραφή μνήμης στο δίσκο
    - Ελαχιστοποίηση κατανάλωσης ενέργειας
  - Κατάσταση αναμονής (standby)
    - Ενέργεια μόνο για ανανέωση δυναμικής μνήμης
    - Κίνδυνος απώλειας αν τελειώσει η μπαταρία

Σύστημα αρχείων

Μάθημα: Λειτουργικά Συστήματα, **Ενότητα # 9:** Το ΛΣ Windows

Διδάσκων: Γιώργος Ξυλωμένος, **Τμήμα:** Πληροφορικής

CC BY NC ND

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο
ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΕΚΠΑΙΔΕΥΣΗ ΚΑΙ ΔΙΑ ΒΙΟΥ ΜΑΘΗΣΗ
επένδυση στην κοινωνία της γνώσης
ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ & ΘΡΗΣΚΕΥΜΑΤΩΝ, ΠΟΛΙΤΙΣΜΟΥ & ΑΘΛΗΤΙΣΜΟΥ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ
ΕΣΠΑ 2007-2013
πρόγραμμα για την ανάπτυξη
ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΩΝΙΚΟ ΤΑΜΕΙΟ
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Έννοιες αρχείων (1 από 3)

- Συστήματα αρχείων των Windows
  - FAT-16/FAT-32: χωρίς προστασία, για συμβατότητα
  - NTFS: το σύστημα αρχείων των NT
    - Μεγάλοι δίσκοι, ασφάλεια, λειτουργικότητα
- Ονόματα αρχείων
  - Έως 255 χαρακτήρες Unicode
  - Διαδρομές έως 32767 χαρακτήρες
  - Διακρίνει και διατηρεί πεζά-κεφαλαία
    - Το Win32 διατηρεί αλλά δεν διακρίνει πεζά-κεφαλαία

Έννοιες αρχείων (2 από 3)

- Χαρακτηριστικά και ρεύματα
  - Κάθε αρχείο αποτελείται από χαρακτηριστικά
  - Κάθε χαρακτηριστικό είναι ένα ρεύμα byte
  - Συνήθως τρία χαρακτηριστικά
    - Όνομα, αναγνωριστικό, ανώνυμα δεδομένα
    - Αναφορά με όνομα:ρεύμα
  - Στα Mac τα αρχεία έχουν 2 ρεύματα δεδομένων
    - Στα Windows τα πολλά ρεύματα χάνονται εύκολα

Έννοιες αρχείων (3 από 3)

- Ιεραρχικός χώρος ονομάτων
  - Διαχωρισμός με \ αντί για /
  - Τα ευρετήρια «.» και «..» είναι συμβάσεις
  - Σκληροί σύνδεσμοι για το σύστημα POSIX
  - Συμβολικοί σύνδεσμοι για διαχειριστές
    - Σημεία συντακτικής επανανάλυσης
  - Συμπίεση, κρυπτογράφηση, αραιά αρχεία
  - Ανοχή σε σφάλματα, τήρηση ημερολογίου

Δομή συστήματος αρχείων (1 από 8)

- Μονάδα (volume) NTFS
  - Αντιστοιχεί σε διαμέρισμα δίσκου
    - Μπορεί να συνδέει πολλά διαμερίσματα
    - Και σε διαφορετικούς δίσκους
  - Γραμμική ακολουθία μπλοκ (συστοιχιών)
    - Μέγεθος μπλοκ από 512 byte έως 64 KB
    - Συνήθως χρήση μπλοκ 4 KB
  - Διευθύνσεις μπλοκ 64 bit

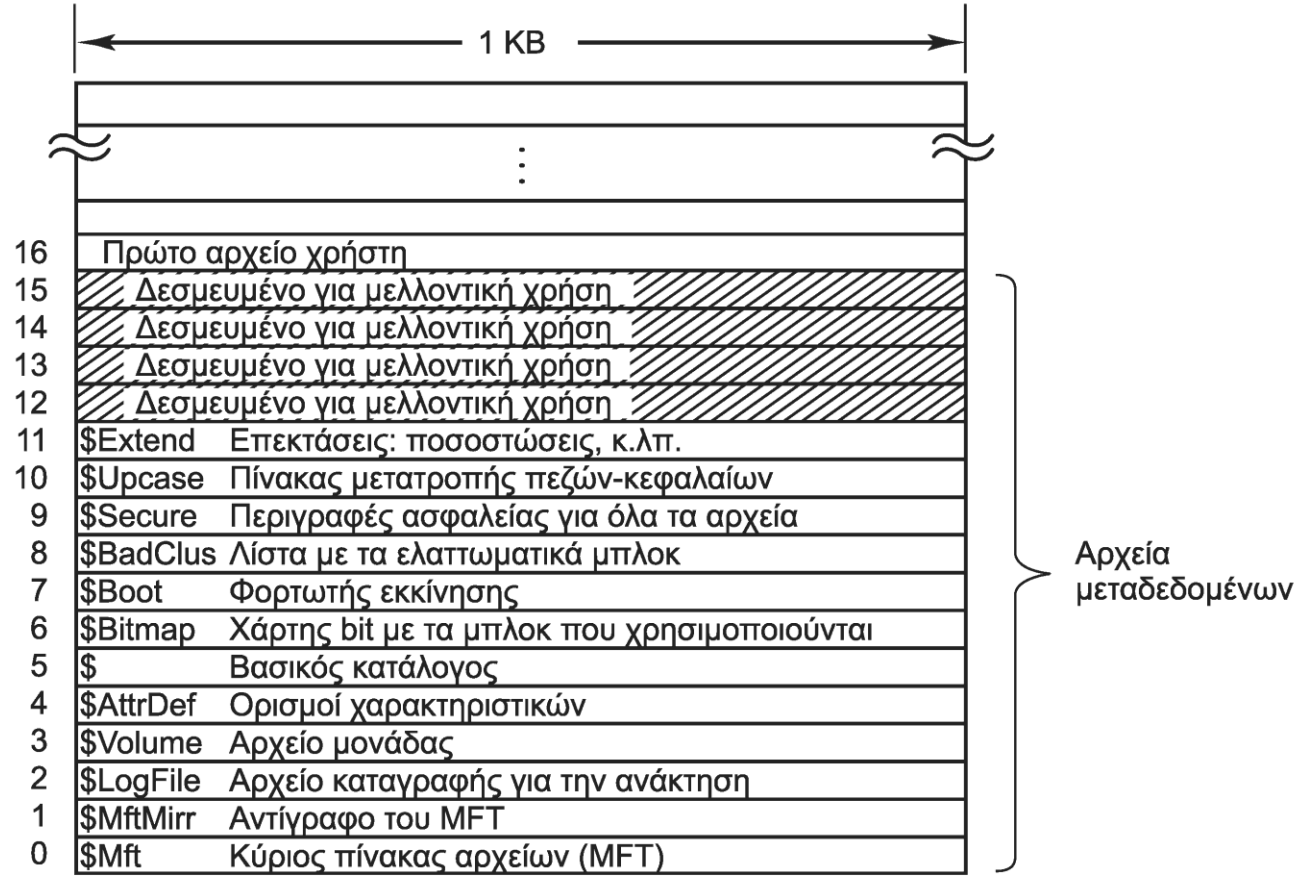
Δομή συστήματος αρχείων (2 από 8)

- Κύριος πίνακας αρχείων (MFT)
  - Γραμμική ακολουθία εγγραφών 1 KB
  - Κάθε εγγραφή περιγράφει ένα αρχείο ή κατάλογο
    - Χαρακτηριστικά αρχείου και διευθύνσεις μπλοκ
    - Πρόσθετες εγγραφές για πολύ μεγάλα αρχεία
  - Χάρτης bit για παρακολούθηση θέσεων MFT
  - Αποθηκεύεται οπουδήποτε στο δίσκο
  - Μεγαλώνει μέχρι 2^{48} εγγραφές

Δομή συστήματος αρχείων (3 από 8)

- Εγγραφές MFT
  - Ακολουθία ζευγών (κεφαλίδα, τιμή)
    - Ζεύγη σταθερού και μεταβλητού μεγέθους
  - Οι μικρές κεφαλίδες είναι μέσα στο MFT
  - Οι μεγάλες αποθηκεύονται αλλού
- Οι πρώτες 16 εγγραφές είναι δεσμευμένες
  - Αρχεία μεταδεδομένων του NTFS
  - Αρχίζουν με $ για να διακρίνονται

Δομή συστήματος αρχείων (4 από 8)



Βασικές καταχωρήσεις του MFT

Δομή συστήματος αρχείων (5 από 8)

- $Mft: το ίδιο το αρχείο με το MFT
  - Το πρώτο μπλοκ αναφέρεται στο μπλοκ εκκίνησης
  - Από εκεί διαβάζουμε όλο το MFT
- Κωδικοποίηση εγγραφών MFT
  - Μαγικός αριθμός για έλεγχο
  - Αριθμός σειράς που αλλάζει σε νέα χρήση
  - Μετρητής αναφορών στο αρχείο
  - Μήκος χρησιμοποιημένης εγγραφής

Δομή συστήματος αρχείων (6 από 8)

Χαρακτηριστικό	Περιγραφή
Πρότυπες πληροφορίες	Bit σημαιών, ημερομηνίες, κλπ.
Όνομα αρχείου	Όνομα αρχείου σε Unicode· μπορεί να επαναλαμβάνεται σε μορφή MS-DOS
Περιγραφέας ασφαλείας	Παρωχημένο. Οι πληροφορίες ασφαλείας βρίσκονται τώρα στην $Extend$Secure
Λίστα χαρακτηριστικών	Θέση πρόσθετων εγγραφών MFT, αν χρειάζονται
Ταυτότητα αντικειμένου	Αναγνωριστικό αρχείου των 64 bit που είναι μοναδικό σε αυτή τη μονάδα
Σημείο συντακτικής επανανάλυσης	Χρησιμοποιείται για ανάρτηση συστημάτων αρχείων και συμβολικούς συνδέσμους
Όνομα μονάδας	Το όνομα αυτής της μονάδας (χρησιμοποιείται μόνο στη $Volume)
Πληροφορίες μονάδας	Έκδοση της μονάδας (χρησιμοποιείται μόνο στη $Volume)
Αφετηρία αριθμοδείκτη	Χρησιμοποιείται για τους καταλόγους
Εκχώρηση αριθμοδείκτη	Χρησιμοποιείται για πολύ μεγάλους καταλόγους
Χάρτης bit	Χρησιμοποιείται για πολύ μεγάλους καταλόγους
Ρεύμα βοηθητικών εφαρμογών καταγραφής	Ελέγχει τις καταγραφές στο $LogFile
Δεδομένα	Ρεύμα δεδομένων· μπορεί να επαναλαμβάνεται

Βασικά χαρακτηριστικά εγγραφών MFT

Δομή συστήματος αρχείων (7 από 8)

- Μορφή χαρακτηριστικών
  - Αναγνωριστικό χαρακτηριστικού
  - Μήκος χαρακτηριστικού
  - Θέση τιμής χαρακτηριστικού
    - Μη διαμένον χαρακτηριστικό: αποθηκεύεται αλλού
    - Απαιτεί μεγαλύτερη κεφαλίδα
    - Περιέχει τη διεύθυνση τις τιμής στο δίσκο
  - Μπορεί να μην χωράνε ούτε οι κεφαλίδες
    - Τότε χρησιμοποιούνται πρόσθετες εγγραφές MFT

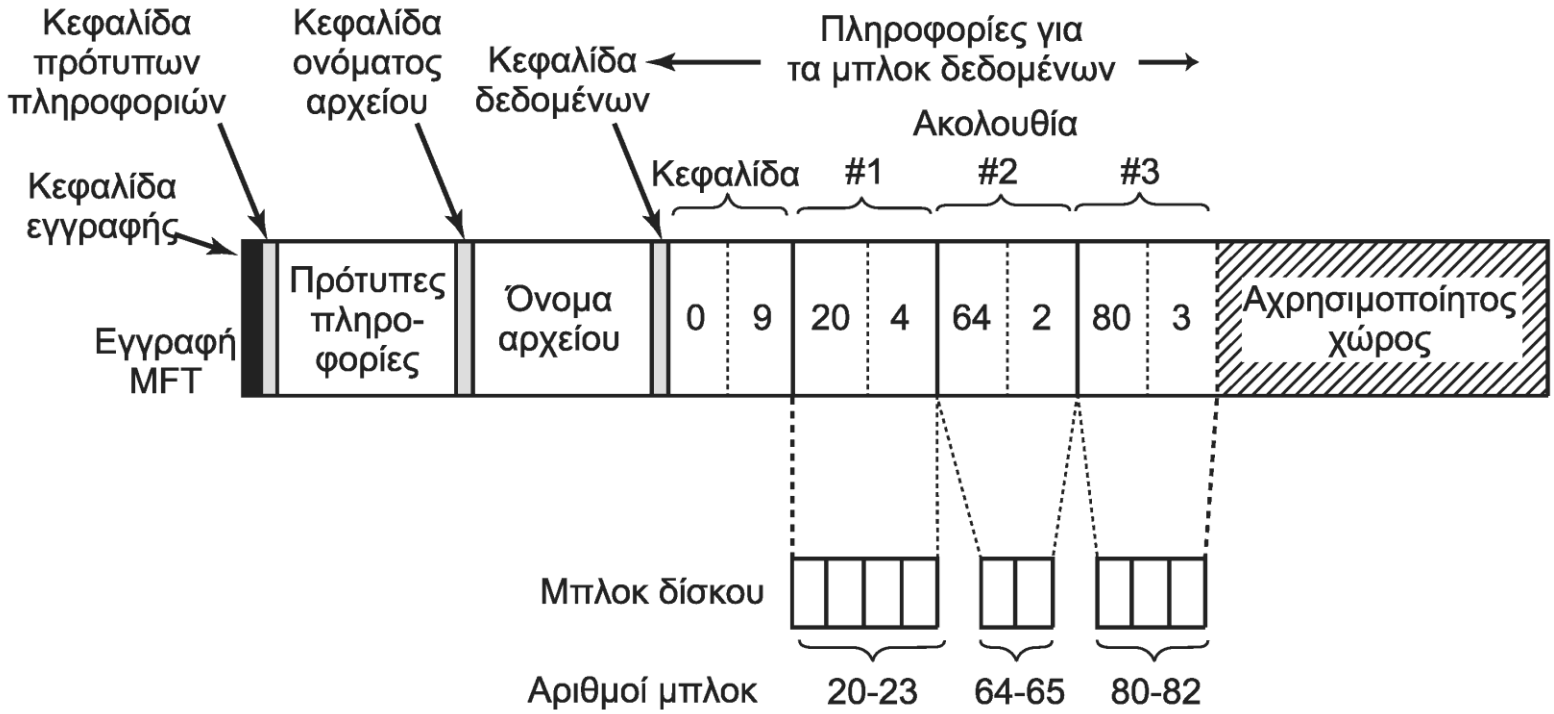
Δομή συστήματος αρχείων (8 από 8)

- Παραπομπή σε άλλο αρχείο για ασφάλεια
  - Επιτρέπει την επαναχρησιμοποίηση πολιτικών
- Αποθήκευση καταλόγων με μορφή λίστας
  - Οι μεγάλοι κατάλογοι αλλάζουν σε B+ δένδρα
- Προεπιλεγμένο ρεύμα δεδομένων: ανώνυμο
  - Πρόσθετα ρεύματα δεδομένων έχουν όνομα
    - Ακολουθούν οι διευθύνσεις των μπλοκ
    - Μικρά ρεύματα αποθηκεύονται στο ίδιο το MFT

Κατανομή χώρου (1 από 6)

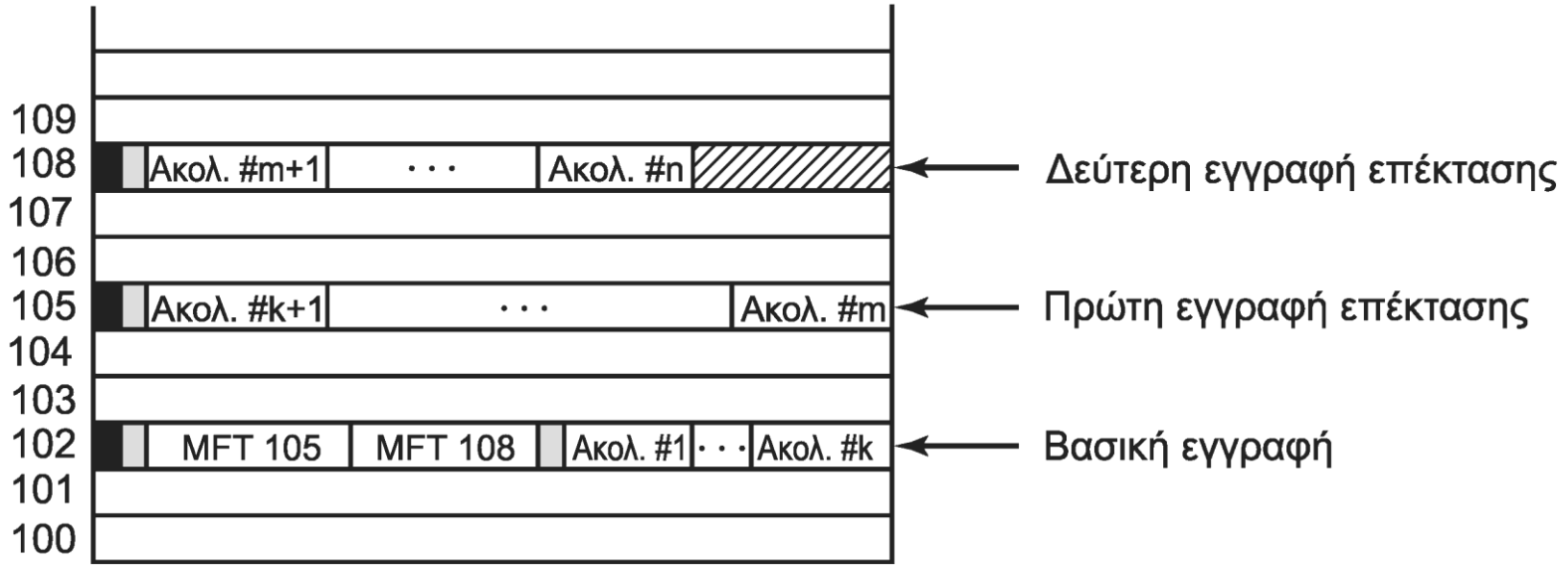
- Προσπάθεια κατανομής γειτονικών μπλοκ
  - Αύξηση απόδοσης λόγω αποφυγής αναζητήσεων
- Ακολουθία εγγραφών περιγραφής ρεύματος
  - Κάθε εγγραφή δείχνει λογικά συνεχόμενα μπλοκ
    - Μπορεί να έχουμε κενά με μηδενικές τιμές
  - Κεφαλίδα εγγραφής: αρχή ροής, τέλος ροής + 1
    - Σχετικές διευθύνσεις από την αρχή του αρχείου
  - Ζεύγη διευθύνσεων: πρώτο μπλοκ, πλήθος
    - Σχετικές διευθύνσεις από την αρχή της μονάδας

Κατανομή χώρου (2 από 6)



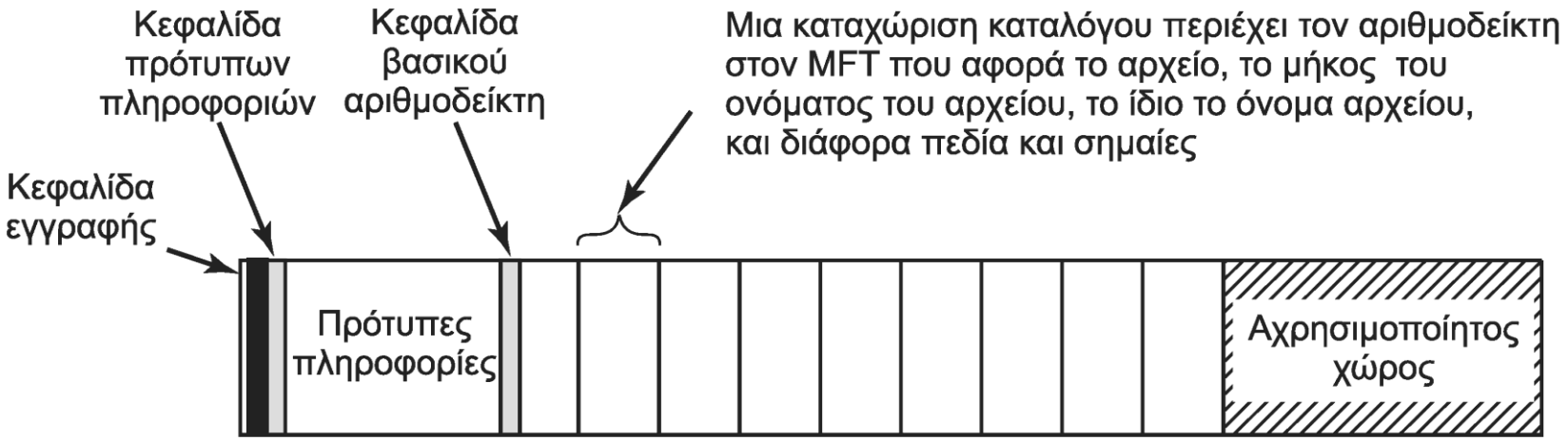
- Παράδειγμα: αρχείο με 9 λογικά μπλοκ
  - Λίστα με τρεις ακολουθίες φυσικών μπλοκ

Κατανομή χώρου (3 από 6)



- Παράδειγμα: πολύ μεγάλο αρχείο
  - Η βασική εγγραφή (102) δείχνει άλλες δύο
  - Οι δείκτες κατανέμονται σε τρεις εγγραφές

Κατανομή χώρου (4 από 6)



- Μορφή εγγραφής καταλόγου
  - Ακολουθία καταχωρίσεων για αρχεία
    - Δείκτης αρχείου στο MFT, μήκος ονόματος και όνομα
    - Γραμμική αναζήτηση ονομάτων
    - Οι μεγάλοι κατάλογοι οργανώνονται σε B+ δένδρα

Κατανομή χώρου (5 από 6)

- Άνοιγμα αρχείου
  - Έχουμε δει την ανάλυση ονόματος μέχρι το NTFS
  - Το NTFS λαμβάνει ένα IRP με το όνομα \foo\bar
  - Ανάγνωση ρίζας από MFT και εντοπισμός foo
  - Ανάγνωση foo και εντοπισμός bar
  - Έλεγχος αν επιτρέπεται η πρόσβαση
  - Ολοκλήρωση αντικειμένου αρχείου
  - Ο χρήστης παίρνει χειριστήριο για τη συνέχεια

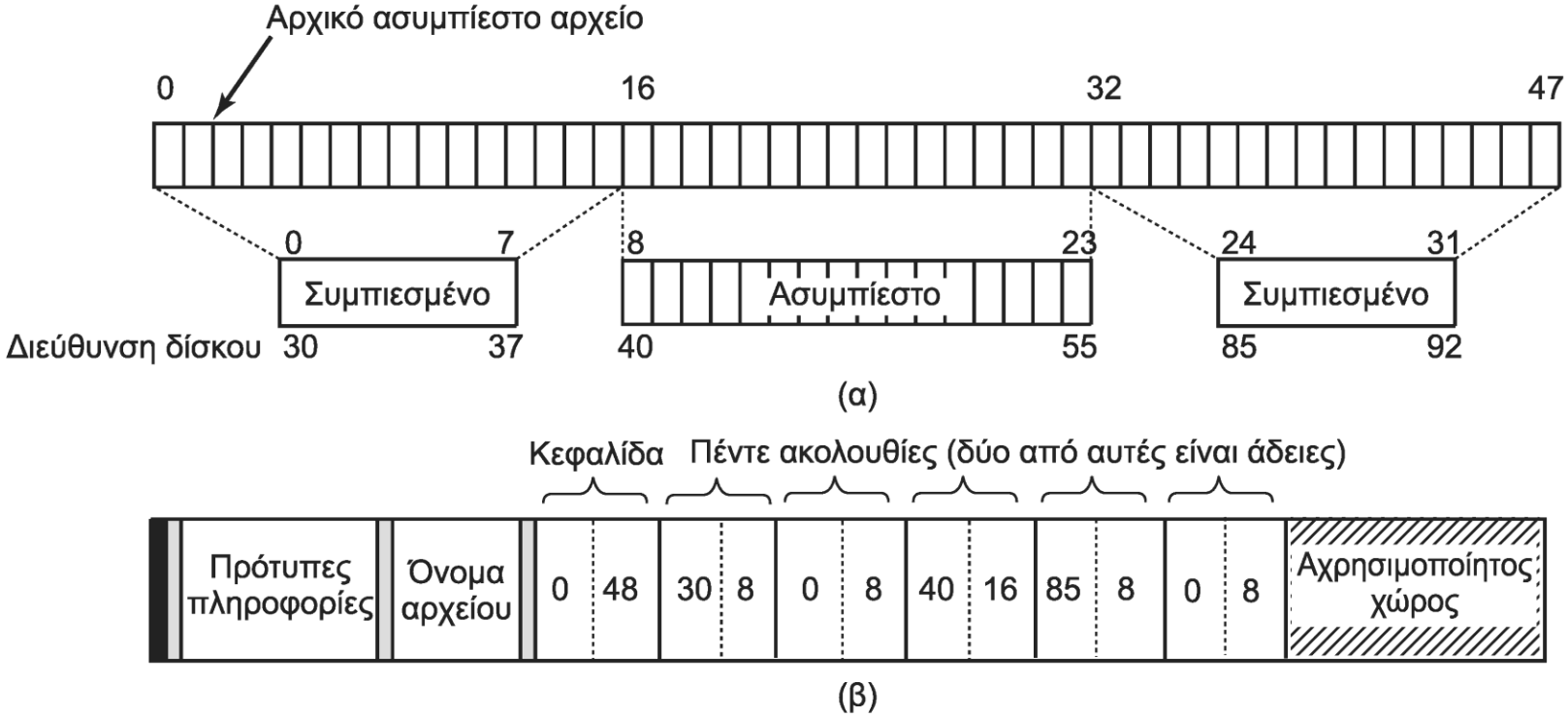
Κατανομή χώρου (6 από 6)

- Σημεία συντακτικής επανανάλυσης (reparse)
  - Ειδική σημείωση σε αρχείο/κατάλογο
    - Συνοδεύεται από κάποια δεδομένα
  - Επιστρέφουν αποτυχία κατά την ανάλυση
    - Στο IRP επιστρέφονται τα δεδομένα
  - Ο διαχειριστής αντικειμένων ξεκινά ξανά
    - Χρήση των δεδομένων ως νέο όνομα
  - Υλοποίηση ανάρτησης, συμβολικών συνδέσμων

Συμπίεση αρχείων (1 από 2)

- Δημιουργία συμπιεσμένων αρχείων
  - Συμπίεση/αποσυμπίεση από το NTFS
  - Δεν είναι εμφανής στις διεργασίες
  - Λειτουργεί σε ομάδες 16 μπλοκ
    - Εξετάζουμε 16 λογικά συνεχόμενα μπλοκ
    - Δοκιμάζουμε να τα συμπιέσουμε
    - Αν έχουμε <=15 μπλοκ, γράφονται συμπιεσμένα
    - Επαναλαμβάνουμε μέχρι το τέλος του αρχείου

Συμπίεση αρχείων (2 από 2)



- Διάκριση συμπιεσμένων περιοχών
  - Δεύτερη εγγραφή με απόσταση μηδέν

Τήρηση ημερολογίου

- Δύο τρόποι παρακολούθησης αλλαγών
- Κλήση NtNotifyChangeDirectoryFile
  - Περνάμε μια περιοχή μνήμης και ένα αρχείο
  - Επιστρέφει τις αλλαγές στο αρχείο
    - Ελπίζουμε να χωράνε όλες στην περιοχή
- Ημερολόγιο αλλαγών του NTFS
  - Λίστα όλων των αλλαγών σε αρχεία
  - Αποθήκευση σε πολύ μεγάλο αρχείο ημερολογίου

Ασφάλεια

Μάθημα: Λειτουργικά Συστήματα, **Ενότητα # 9:** Το ΛΣ Windows

Διδάσκων: Γιώργος Ξυλωμένος, **Τμήμα:** Πληροφορικής

CC BY NC ND

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο

ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΕΚΠΑΙΔΕΥΣΗ ΚΑΙ ΔΙΑ ΒΙΟΥ ΜΑΘΗΣΗ
επένδυση στην κοινωνία της γνώσης
ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ & ΘΡΗΣΚΕΥΜΑΤΩΝ, ΠΟΛΙΤΙΣΜΟΥ & ΑΘΛΗΤΙΣΜΟΥ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ

ΕΣΠΑ 2007-2013
πρόγραμμα για την ανάπτυξη
ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΩΝΙΚΟ ΤΑΜΕΙΟ

Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Απαιτήσεις ασφάλειας (1 από 2)

- Τα NT σχεδιάστηκαν για ασφάλεια C2
  - Πρότυπο του DoD των ΗΠΑ
  - Δεν υλοποιείται πια κατά 100%
- Ασφαλής σύνδεση χωρίς παραπλάνηση
  - Όλοι οι χρήστες πρέπει να δώσουν συνθηματικό
  - Χρήση CTRL-ALT-DEL πριν τη σύνδεση
    - Ενεργοποιεί πάντα το λειτουργικό σύστημα
    - Δεν απενεργοποιείται από εφαρμογές χρήστη

Απαιτήσεις ασφάλειας (2 από 2)

- Διακριτικοί έλεγχοι πρόσβασης
  - Ο ιδιοκτήτης επιλέγει τρόπο πρόσβασης
- Έλεγχοι προνομιακής πρόσβασης
  - Ο υπερχρήστης μπορεί να παρακάμψει ελέγχους
- Προστασία χώρου διευθύνσεων διεργασίας
- Μηδενισμός νέων σελίδων
- Ελεγκτική παρακολούθηση ασφάλειας
  - Αρχείο καταγραφής συμβάντων

Έννοιες ασφάλειας (1 από 4)

- Κάθε ομάδα έχει ταυτότητα ασφάλειας (SID)
  - Κεφαλίδα και τυχαίος αριθμός για μοναδικότητα
  - Οι διεργασίες έχουν μία σκυτάλη πρόσβασης
    - Περιέχει το SID του ιδιοκτήτη και άλλες πληροφορίες
    - Προεπιλεγμένη ACL για νέα αντικείμενα
    - Ειδικά προνόμια του χρήστη (τύπου υπερχρήστη)
    - Δυνατότητα μίμησης και περιορισμένων προνομίων

Κεφαλίδα	Χρόνος λήξης προθεσμίας	Ομάδες	Προεπιλεγμένο CACL	SID χρήστη	SID ομάδας	Περιορισμένα SID	Προνόμια	Επίπεδο μίμησης	Επίπεδο ακεραιότητας

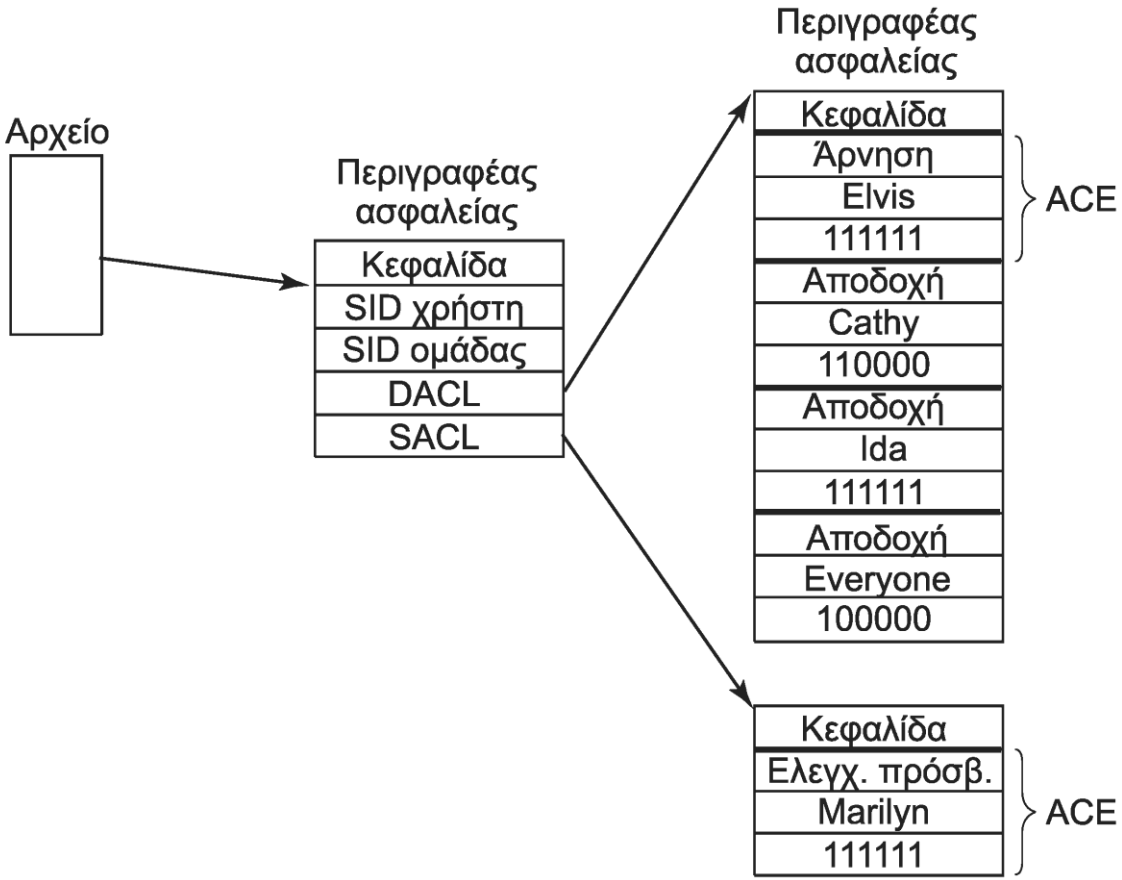
Έννοιες ασφάλειας (2 από 4)

- Δημιουργία σκυτάλης στη σύνδεση
  - Οι διεργασίες την κληρονομούν
  - Όλα τα νήματα έχουν την ίδια
- Μηχανισμός μίμησης (impersonation)
  - Δυνατότητα απόκτησης άλλης σκυτάλης
    - Το νήμα αποκτά διαφορετικά προνόμια
  - Παράδειγμα: πελάτης περνά σκυτάλη σε διακομιστή
    - Δυνατότητα προσπέλασης αρχείων πελάτη

Έννοιες ασφάλειας (3 από 4)

- Περιγραφέας ασφάλειας αντικειμένου
  - Περιορίζει την πρόσβαση στο αντικείμενο
  - DACL: δικαιώματα χρήσης αντικειμένου
    - Λίστα στοιχείων ελέγχου πρόσβασης (ACE)
    - Κάθε ACE έχει SID και χάρτη δικαιωμάτων
    - Μπορεί να είναι αποδοχής ή άρνησης
  - SACL: ενέργειες που καταγράφονται
    - Ίδια μορφή με την DACL

Έννοιες ασφάλειας (4 από 4)



Παράδειγμα περιγραφέα ασφάλειας

Κλήσεις ασφάλειας

Συνάρτηση Win32 API	Περιγραφή
InitializeSecurityDescriptor	Προετοιμασία νέου περιγραφέα ασφαλείας για χρήση
LookupAccountSid	Αναζήτηση SID δεδομένου ονόματος χρήστη
SetSecurityDescriptorOwner	Καταχώριση SID ιδιοκτήτη στον περιγραφέα ασφαλείας
SetSecurityDescriptorGroup	Καταχώριση SID ομάδας στον περιγραφέα ασφαλείας
InitializeAcl	Αρχικές τιμές σε DACL ή SACL
AddAccessAllowedAce	Προσθήκη νέας ACE σε DACL ή SACL, που επιτρέπει την πρόσβαση
AddAccessDeniedAce	Προσθήκη νέας ACE σε DACL ή SACL, που απαγορεύει την πρόσβαση
DeleteAce	Διαγραφή ACE από DACL ή SACL
SetSecurityDescriptorDacl	Προσάρτηση DACL σε έναν περιγραφέα ασφαλείας

- Κλήσεις διαχείρισης περιγραφέων ασφάλειας
  - Αντιστοίχιση περιγραφέα κατά δημιουργία
  - Αλλιώς κληρονομείται από τη διεργασία

Υλοποίηση ασφάλειας (1 από 3)

- Αρχικοποίηση ασφάλειας
  - Σύνδεση με διεργασία winlogon
  - Πιστοποίηση ταυτότητας με διεργασία lsass
  - Δημιουργία νέου φλοιού GUI (explorer)
    - Χρήση της κατάλληλης σκυτάλης πρόσβασης
- Έλεγχος ασφάλειας στο άνοιγμα αντικειμένων
  - Κεντρικός ελεγκτής αναφορών ασφάλειας
  - Σύγκριση ζητούμενων με επιτρεπτά δικαιώματα
    - Ισχύει η πρώτη καταχώριση της ACL που ταιριάζει

Υλοποίηση ασφάλειας (2 από 3)

- Περιορισμένοι έλεγχοι στη συνέχεια
  - Μόνο αν η λειτουργία είχε ελεγχθεί αρχικά
  - Δεν ελέγχεται ξανά η DACL σε κάθε πρόσβαση
  - Εγγραφή στο ημερολόγιο ανάλογα με SACL
- SID επιπέδου ακεραιότητας
  - Περιέχονται σε σκυτάλη και SACL
  - Δεν επιτρέπουν υπέρβαση δικαιωμάτων
    - Ανεξάρτητα από το τι λέει η DACL

Υλοποίηση ασφάλειας (3 από 3)

- Απαγόρευση εκτέλεσης (NX)
  - Σελίδες με απαγόρευση εκτέλεσης κώδικα
    - Αποφυγή προβλημάτων υπερχείλισης στοίβας
- Υπογραφή κώδικα πυρήνα (για οδηγούς)
- Φόρτωση κώδικα σε τυχαίες διευθύνσεις
- Έλεγχος λογαριασμού χρήστη (UAC)
  - Εμφάνιση ειδικής οθόνης για το διαχειριστή
    - Ο χρήστης πρέπει να εγκρίνει την πρόσβαση

Τέλος Ενότητας #9

Μάθημα: Λειτουργικά Συστήματα, **Ενότητα # 9:** Το ΛΣ Windows

Διδάσκων: Γιώργος Ξυλωμένος, **Τμήμα:** Πληροφορικής

CC BY NC ND

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο
ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΕΚΠΑΙΔΕΥΣΗ ΚΑΙ ΔΙΑ ΒΙΟΥ ΜΑΘΗΣΗ
επένδυση στην κοινωνία της γνώσης
ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ & ΘΡΗΣΚΕΥΜΑΤΩΝ, ΠΟΛΙΤΙΣΜΟΥ & ΑΘΛΗΤΙΣΜΟΥ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ
ΕΣΠΑ 2007-2013
πρόγραμμα για την ανάπτυξη
ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΩΝΙΚΟ ΤΑΜΕΙΟ
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης