

Ε Κ Δ Ο Σ Ε Ι Σ Κ Λ Ε Ι Δ Α Ρ Ι Θ Μ Ο Σ

ΑΣΦΑΛΕΙΑ ΥΠΟΛΟΓΙΣΤΩΝ

ΑΡΧΕΣ ΚΑΙ ΠΡΑΚΤΙΚΕΣ

3η αμερικανική έκδοση



William Stallings • Lawrie Brown



Κεφάλαιο 4

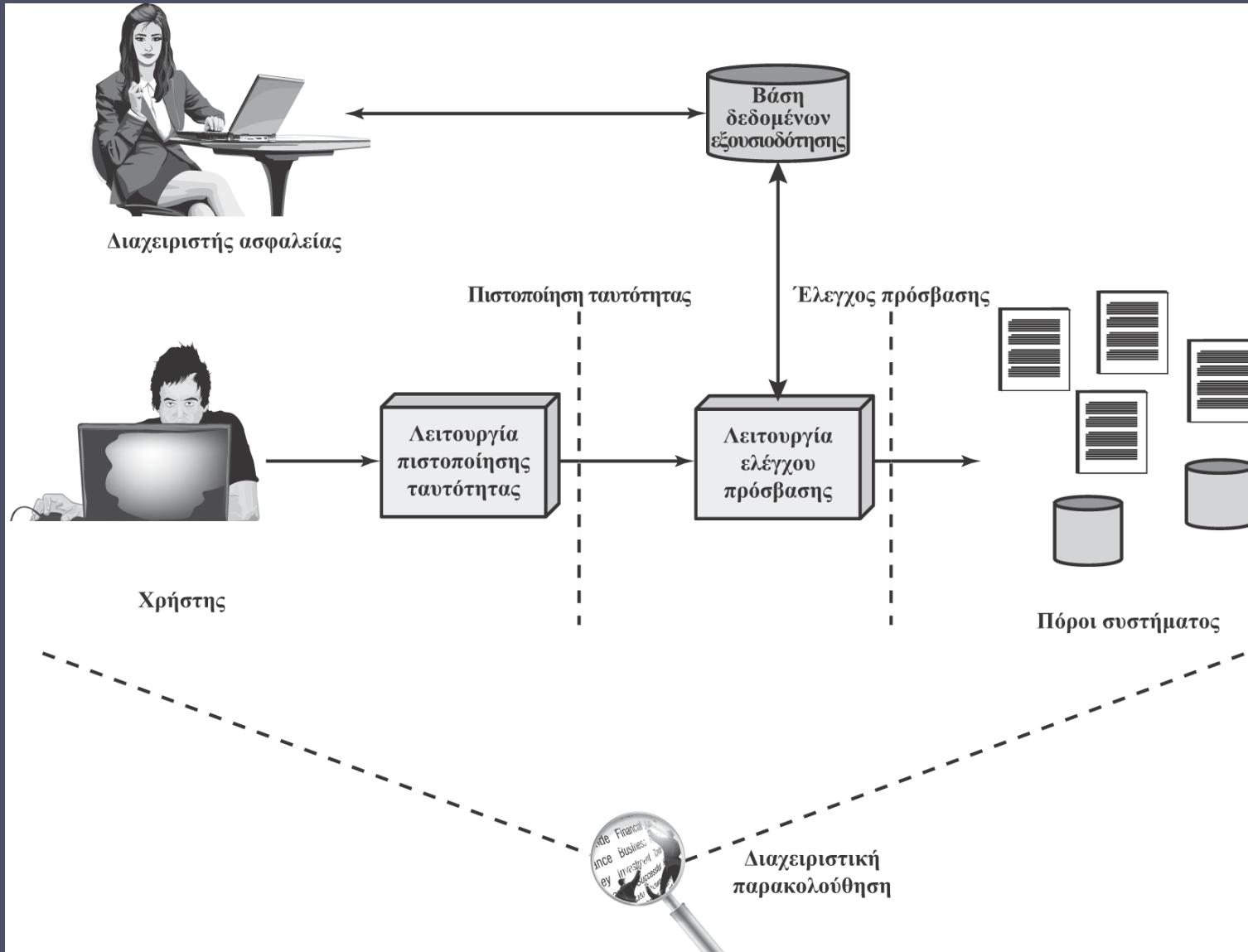
Έλεγχος πρόσβασης

Αρχές ελέγχου πρόσβασης

Στο έγγραφο RFC 4949 η ασφάλεια υπολογιστών ορίζεται ως εξής:

«Μέτρα που υλοποιούν και εγγυώνται υπηρεσίες ασφαλείας σε ένα υπολογιστικό σύστημα, και συγκεκριμένα εκείνα που εγγυώνται την υπηρεσία ελέγχου πρόσβασης.»





Εικόνα 4.1 Σχέση μεταξύ του ελέγχου πρόσβασης και άλλων λειτουργιών της ασφάλειας

Πολιτικές ελέγχου πρόσβασης

- Διακριτικός έλεγχος πρόσβασης (discretionary access control, DAC)
 - Ελέγχει την πρόσβαση με βάση την ταυτότητα του αιτούντος και κανόνες πρόσβασης (εξουσιοδοτήσεις) οι οποίοι ορίζουν τι επιτρέπεται (ή δεν επιτρέπεται) να κάνουν οι αιτούντες
- Υποχρεωτικός έλεγχος πρόσβασης (mandatory access control, MAC)
 - Ελέγχει την πρόσβαση συγκρίνοντας ετικέτες ασφαλείας με εξουσιοδοτήσεις ασφαλείας
- Έλεγχος πρόσβασης βασισμένος σε ρόλους (role-based access control, RBAC)
 - Ελέγχει την πρόσβαση με βάση τους ρόλους που έχουν οι χρήστες εντός του συστήματος, καθώς και κανόνες που ορίζουν τους τύπους της επιτρεπόμενης πρόσβασης για χρήστες με δεδομένους ρόλους
- Έλεγχος πρόσβασης βασισμένος σε ιδιότητες (attribute-based access control, ABAC)
 - Ελέγχει την πρόσβαση με βάση ιδιότητες του χρήστη, του πόρου που πρέπει να προσπελαστεί, καθώς και των τρεχουσών περιβαλλοντικών συνθηκών

Υποκείμενα, αντικείμενα και δικαιώματα πρόσβασης

Υποκείμενο

Οντότητα που έχει τη δυνατότητα να προσπελάζει αντικείμενα

Τρεις κατηγορίες

- Κάτοχος (owner)
- Ομάδα (group)
- Κόσμος (world)

Αντικείμενο

Πόρος ελεγχόμενης πρόσβασης

Οντότητα που περιέχει ή/και λαμβάνει πληροφορίες

Δικαίωμα πρόσβασης

Περιγράφει τον τρόπο με τον οποίο ένα υποκείμενο μπορεί να προσπελάσει ένα αντικείμενο

Περιλαμβάνει τα εξής:

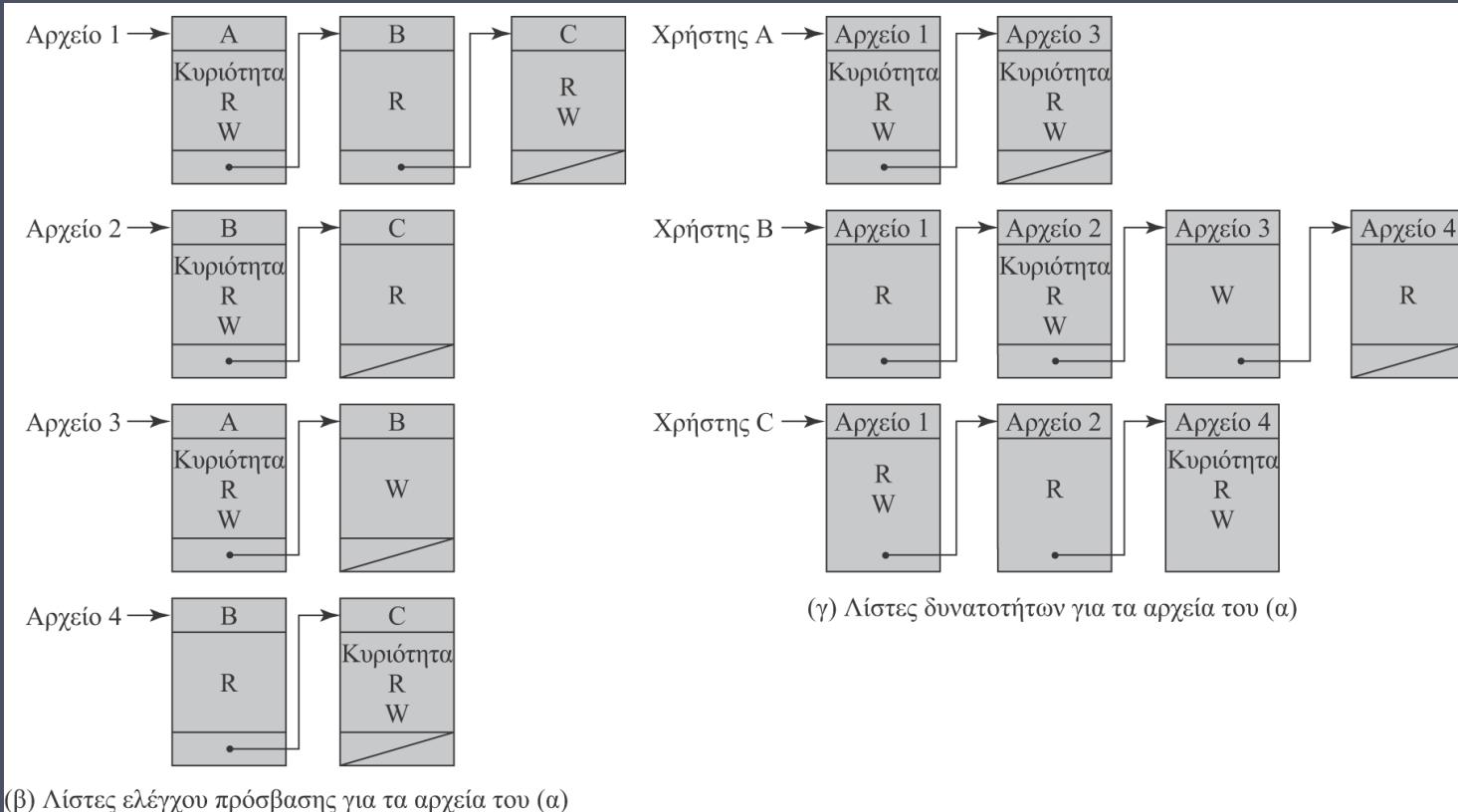
- Ανάγνωση (read)
- Εγγραφή (write)
- Εκτέλεση (execute)
- Διαγραφή (delete)
- Δημιουργία (create)
- Αναζήτηση (search)

Διακριτικός έλεγχος πρόσβασης (DACP)

- Σύστημα στο οποίο μια οντότητα μπορεί να επιτρέψει σε άλλες οντότητες να προσπελάσουν κάποιον πόρο
- Συχνά παρέχεται με χρήση μιας μήτρας πρόσβασης (access matrix)
 - Η μία διάσταση της μήτρας αποτελείται από καθορισμένα υποκείμενα που μπορούν να προσπελάσουν τα δεδομένα που περιέχονται στους πόρους
 - Η άλλη διάσταση περιέχει τα αντικείμενα που μπορούν να προσπελαστούν
- Κάθε στοιχείο της μήτρας υποδεικνύει τα δικαιώματα πρόσβασης ενός συγκεκριμένου υποκειμένου για ένα συγκεκριμένο αντικείμενο

		ANTIKEIMENA			
		Αρχείο 1	Αρχείο 2	Αρχείο 3	Αρχείο 4
Χρήστης A	Χρήστης A	Κυριότητα Ανάγνωση (R) Εγγραφή (W)		Κυριότητα Ανάγνωση (R) Εγγραφή (W)	
	Χρήστης B	Ανάγνωση (R)	Κυριότητα Ανάγνωση (R) Εγγραφή (W)	Εγγραφή (W)	Ανάγνωση (R)
	Χρήστης C	Ανάγνωση (R) Εγγραφή (W)	Ανάγνωση (R)		Κυριότητα Ανάγνωση (R) Εγγραφή (W)

(α) Μήτρα πρόσβασης



Εικόνα 4.2 Παράδειγμα δομών ελέγχου πρόσβασης

Υποκείμενο	Κατάσταση πρόσβασης	Αντικείμενο
A	Κυριότητα	Αρχείο 1
A	Ανάγνωση	Αρχείο 1
A	Εγγραφή	Αρχείο 1
A	Κυριότητα	Αρχείο 3
A	Ανάγνωση	Αρχείο 3
A	Εγγραφή	Αρχείο 3
B	Ανάγνωση	Αρχείο 1
B	Κυριότητα	Αρχείο 2
B	Ανάγνωση	Αρχείο 2
B	Εγγραφή	Αρχείο 2
B	Εγγραφή	Αρχείο 3
B	Ανάγνωση	Αρχείο 4
C	Ανάγνωση	Αρχείο 1
C	Εγγραφή	Αρχείο 1
C	Ανάγνωση	Αρχείο 2
C	Κυριότητα	Αρχείο 4
C	Ανάγνωση	Αρχείο 4
C	Εγγραφή	Αρχείο 4

Πίνακας 4.1

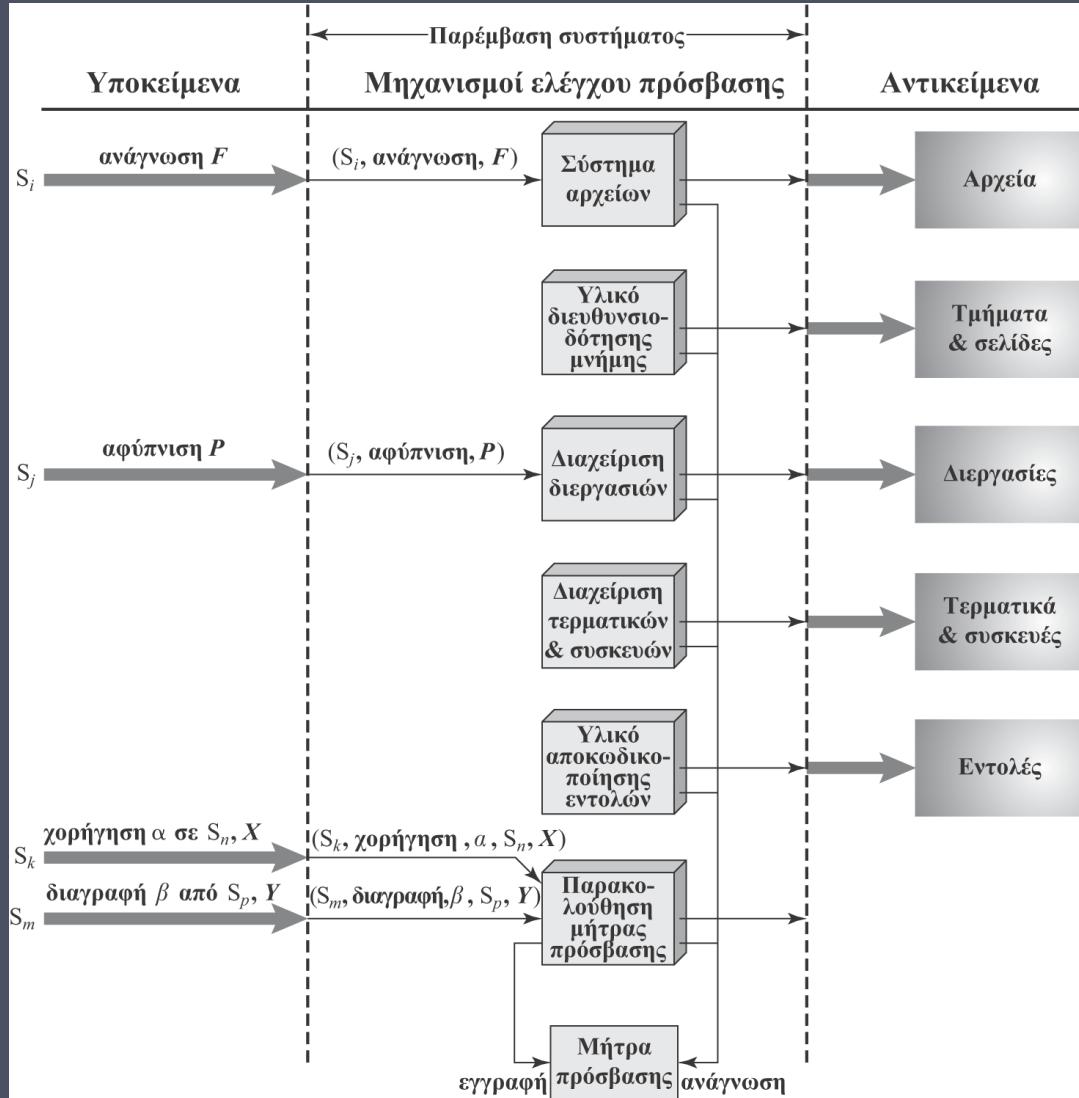
Πίνακας εξουσιοδοτήσεων για τα αρχεία της Εικόνας 4.2

ANTIKEIMENA

Υποκείμενα			Αρχεία		Διεργασίες		Μονάδες δίσκου		
	S ₁	S ₂	S ₃	F ₁	F ₂	P ₁	P ₂	D ₁	D ₂
ΥΠΟΚΕΙΜΕΝΑ	S ₁	έλεγχος	κάτοχος	κάτοχος έλεγχος	ανάγνωση*	ανάγνωση κάτοχος	αφύπνιση	αφύπνιση	αναζή- τηση
	S ₂		έλεγχος		εγγραφή*	εκτέλεση			κάτοχος
	S ₃			έλεγχος		εγγραφή	διακοπή		αναζή- τηση*

* σημαία αντιγραφής ενεργοποιημένη

Εικόνα 4.3 Επεκτεταμένη μήτρα ελέγχου πρόσβασης



Εικόνα 4.4 Οργάνωση της λειτουργίας ελέγχου πρόσβασης

Πίνακας 4.2

Εντολές συστήματος ελέγχου πρόσβασης

Κανόνας	Εντολή (από S_0)	Εξουσιοδότηση	Ενέργεια
R1	μεταβίβαση $\left\{ \alpha^* \atop \alpha \right\}$ σε S, X	‘ α^* ’ στο $A[S_0, X]$	αποθήκευση $\left\{ \alpha^* \atop \alpha \right\}$ στο $A[S, X]$
R2	χορήγηση $\left\{ \alpha^* \atop \alpha \right\}$ σε S, X	‘κάτοχος’ στο $A[S_0, X]$	αποθήκευση $\left\{ \alpha^* \atop \alpha \right\}$ στο $A[S, X]$
R3	διαγραφή α από S, X	‘έλεγχος’ στο $A[S_0, S]$ ή ‘κάτοχος’ στο $A[S_0, X]$	διαγραφή α από το $A[S, X]$
R4	$w \leftarrow$ ανάγνωση S, X	‘έλεγχος’ στο $A[S_0, S]$ ή ‘κάτοχος’ στο $A[S_0, X]$	αντιγραφή του $A[S, X]$ στο w
R5	δημιουργία αντικειμένου X	Καμία	προσθήκη στήλης για το X στη μήτρα A , αποθήκευση ‘κάτοχος’ στο $A[S_0, X]$
R6	καταστροφή αντικειμένου X	‘κάτοχος’ στο $A[S_0, X]$	διαγραφή στήλης για το X από τη μήτρα A
R7	δημιουργία αντικειμένου S	Καμία	προσθήκη γραμμής για το S στη μήτρα A , εκτέλεση δημιουργία αντικειμένου S , αποθήκευση ‘έλεγχος’ στο $A[S, S]$
R8	καταστροφή αντικειμένου S	‘κάτοχος’ στο $A[S_0, S]$	διαγραφή γραμμής για το S από την A , εκτέλεση καταστροφή αντικειμένου S



Περιοχές προστασίας

- Ένα σύνολο αντικειμένων και τα σχετικά δικαιώματα πρόσβασης
- Περισσότερη ευελιξία κατά τη συσχέτιση δυνατοτήτων με περιοχές προστασίας
- Κάθε γραμμή της μήτρας πρόσβασης ορίζει μια περιοχή προστασίας
- Ένας χρήστης μπορεί να δημιουργήσει διεργασίες που έχουν ένα υποσύνολο των δικαιωμάτων πρόσβασης του χρήστη
- Η συσχέτιση μεταξύ διεργασίας και περιοχής μπορεί να είναι στατική ή δυναμική
- Σε κατάσταση χρήστη (user mode), απαγορεύεται η χρήση ορισμένων προστατευμένων περιοχών της μνήμης και δεν μπορούν να εκτελούνται ορισμένες εντολές
- Σε κατάσταση πυρήνα (kernel mode), μπορούν να εκτελούνται προνομιακές εντολές και να προσπελάζονται προστατευμένες περιοχές της μνήμης

Έλεγχος πρόσβασης σε αρχεία του UNIX

Η διαχείριση αρχείων του UNIX γίνεται με χρήση κόμβων inode (index nodes, κόμβοι ευρετηρίου)

- Δομές ελέγχου οι οποίες περιέχουν τις βασικές πληροφορίες που απαιτούνται για ένα συγκεκριμένο αρχείο
- Με έναν κόμβο inode μπορούν να συσχετίζονται πολλά ονόματα αρχείων
- Ένας ενεργός κόμβος inode συσχετίζεται με ακριβώς ένα αρχείο
- Ιδιότητες (attributes) αρχείων, δικαιώματα πρόσβασης και άλλες πληροφορίες ελέγχου αποθηκεύονται στον κόμβο inode
- Στον σκληρό δίσκο υπάρχει ένας πίνακας, ή λίστα, κόμβων inode, ο οποίος περιέχει τους κόμβους inode για όλα τα αρχεία του συστήματος αρχείων
- Κατά το άνοιγμα ενός αρχείου, ο σχετικός κόμβος inode μεταφέρεται στην κύρια μνήμη και αποθηκεύεται σε έναν πίνακα κόμβων inode ο οποίος παραμένει στη μνήμη

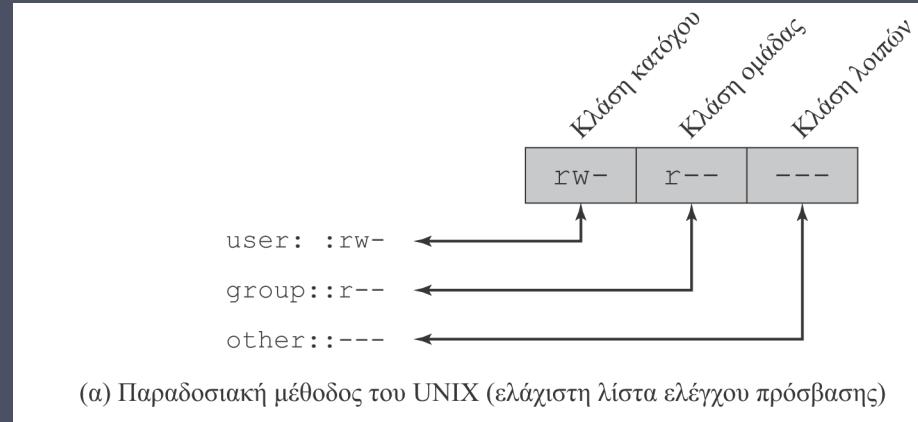
Οι κατάλογοι είναι δομημένοι σε ένα ιεραρχικό δένδρο

- Κάθε κατάλογος μπορεί να περιέχει αρχεία ή/και άλλους καταλόγους
- Περιέχει ονόματα αρχείων συν τους δείκτες προς τους συσχετιζόμενους κόμβους inode

UNIX

Έλεγχος πρόσβασης σε αρχεία

- Μοναδικό αναγνωριστικό χρήστη (user ID)
- Μέλος μιας κύριας ομάδας που διαθέτει δικό της αναγνωριστικό ομάδας (group ID)
- Κάθε αρχείο ανήκει σε μια συγκεκριμένη ομάδα
- 12 bit προστασίας
 - Καθορίζουν δικαιώματα ανάγνωσης, εγγραφής και εκτέλεσης για τον κάτοχο του αρχείου, για τα άλλα μέλη της ομάδας, και για όλους τους λοιπούς χρήστες
- Τα bit του κατόχου και της ομάδας, καθώς και τα bit προστασίας, αποτελούν κομμάτι του κόμβου inode του αρχείου



Παραδοσιακός έλεγχος πρόσβασης σε αρχεία του UNIX

- «Set user ID»(SetUID, ορισμός αναγνωριστικού χρήστη)
- «Set group ID»(SetGID, ορισμός αναγνωριστικού ομάδας)
 - Κατά τη λήψη αποφάσεων ελέγχου πρόσβασης, το σύστημα χρησιμοποιεί προσωρινά τα δικαιώματα του κατόχου/ομάδας του αρχείου παράλληλα με τα δικαιώματα του πραγματικού χρήστη
 - Επιτρέπει σε προνομιακά προγράμματα να αποκτήσουν πρόσβαση σε αρχεία/πόρους που δεν είναι προσπελάσιμα από άλλους χρήστες
- Bit «sticky»
 - Όταν εφαρμόζεται σε καταλόγους, καθορίζει ότι μόνο ο κάτοχος οποιουδήποτε αρχείου του καταλόγου μπορεί να μετονομάσει, μετακινήσει, ή διαγράψει το συγκεκριμένο αρχείο
- «Υπερχρήστης» (superuser)
 - Δεν υπόκειται στους συνήθεις περιορισμούς του ελέγχου πρόσβασης
 - Διαθέτει δικαιώματα πρόσβασης σε όλο το σύστημα

Λίστες ελέγχου πρόσβασης (ACL) στο UNIX

Πολλά σύγχρονα συστήματα UNIX υποστηρίζουν τις λίστες ACL

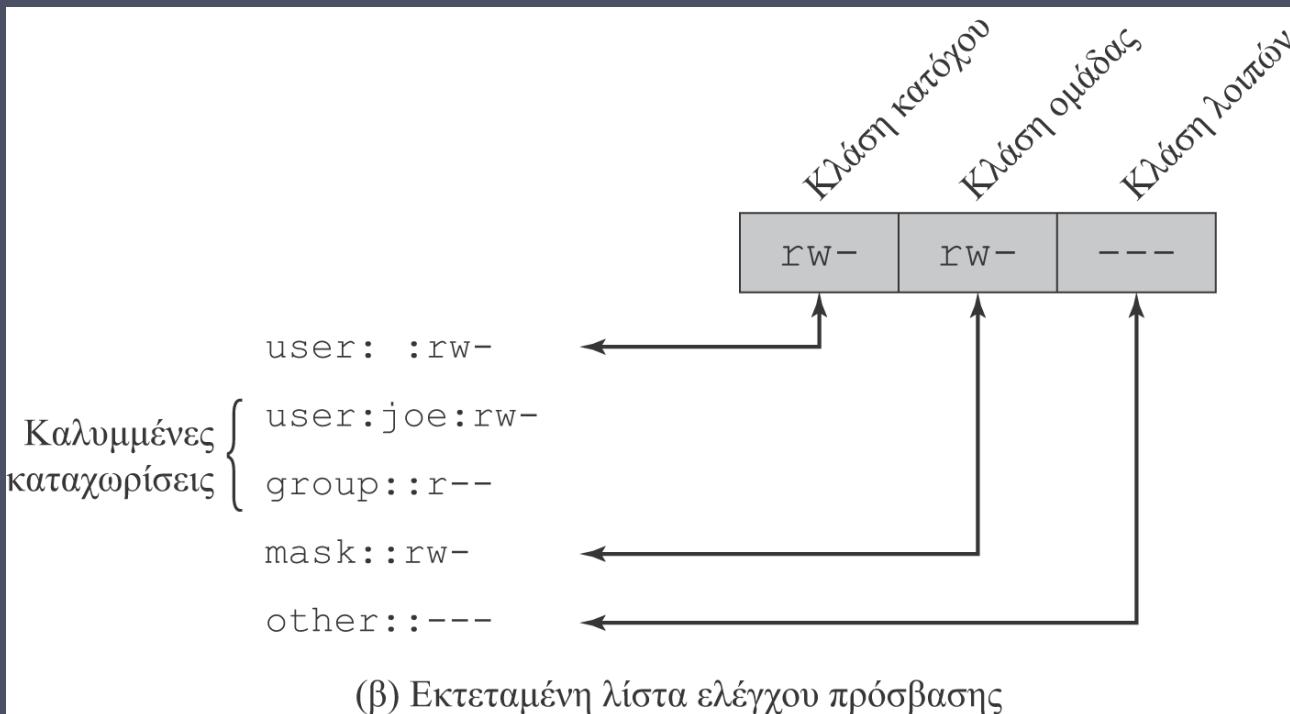
- FreeBSD, OpenBSD, Linux, Solaris

FreeBSD

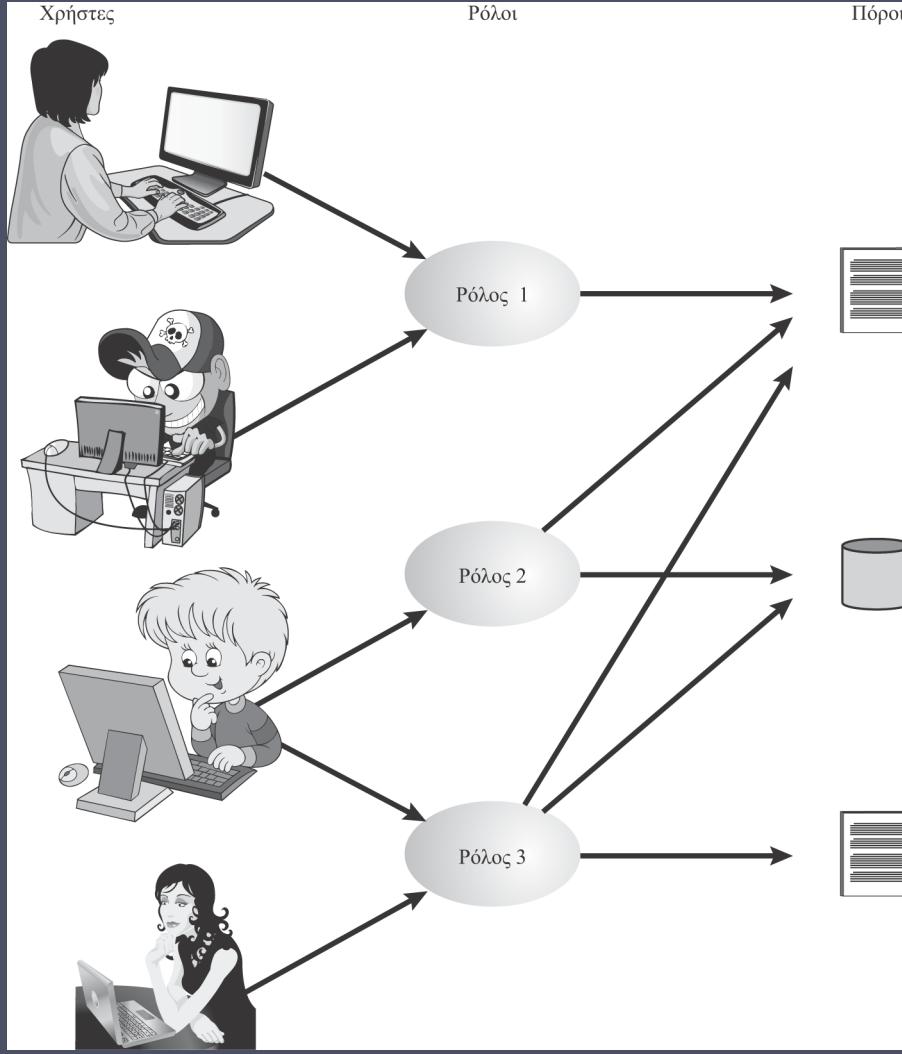
- Η εντολή setfacl αντιστοιχίζει μια λίστα αναγνωριστικών χρηστών και ομάδων
- Ένα αρχείο μπορεί να έχει συσχετιστεί με οποιοδήποτε πλήθος χρηστών και ομάδων
- Τοία bit προστασίας (ανάγνωση, εγγραφή, εκτέλεση)
- Ένα αρχείο δεν χρειάζεται να διαθέτει λίστα ACL
- Πρόσθετο bit προστασίας που υποδεικνύει αν το αρχείο έχει επεκτεταμένη λίστα ACL

Όταν μια διεργασία αιτείται πρόσβαση σε ένα αντικείμενο του συστήματος αρχείων, εκτελούνται δύο βήματα:

- Το βήμα 1 επιλέγει την καταλληλότερη ACL
- Το βήμα 2 ελέγχει αν η καταχώριση που ταιριάζει περιέχει επαρκή δικαιώματα πρόσβασης



Εικόνα 4.5 Έλεγχος πρόσβασης σε αρχεία του UNIX

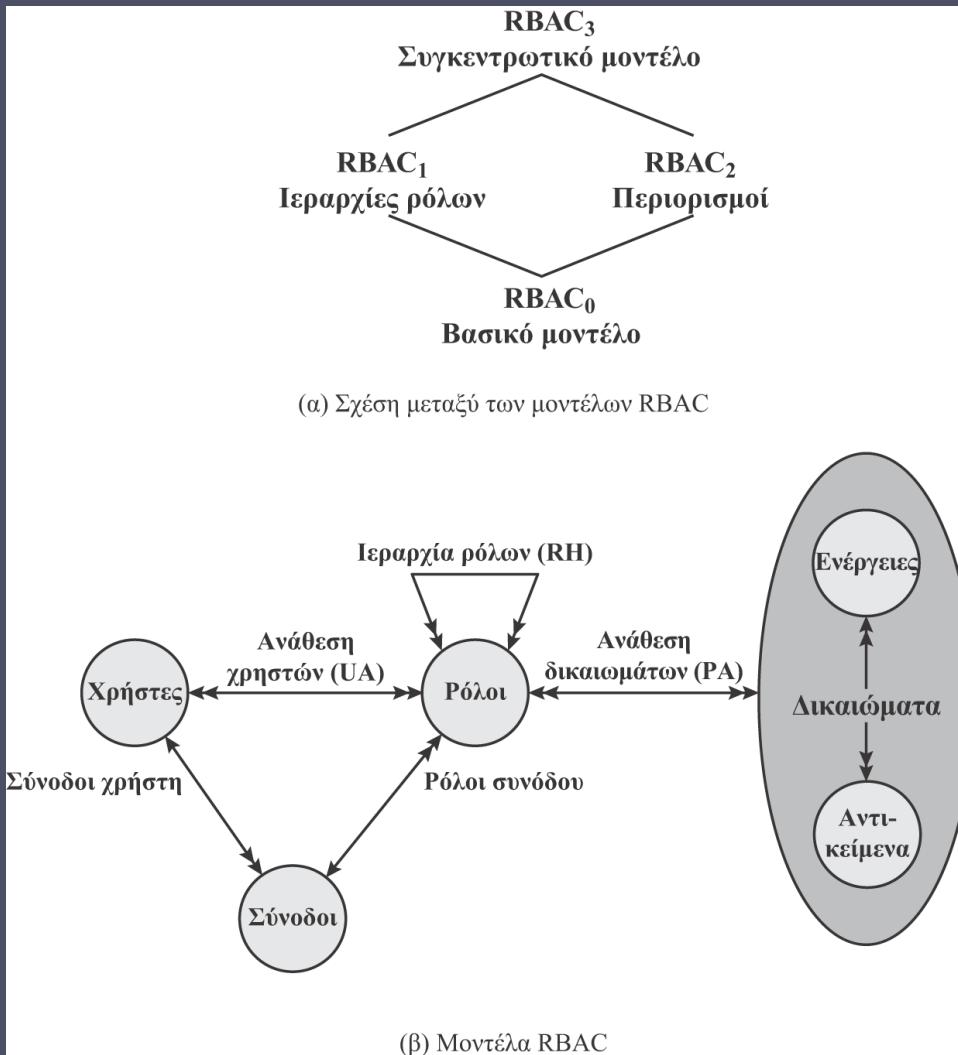


Εικόνα 4.6 Χρήστες, ρόλοι και πόροι

	R ₁	R ₂	• • •	R _n
U ₁	✗			
U ₂	✗			
U ₃		✗		✗
U ₄				✗
U ₅				✗
U ₆				✗
•				
•				
•				
U _m	✗			

	ANTIKEIMENA								
	R ₁	R ₂	R _n	F ₁	F ₂	P ₁	P ₂	D ₁	D ₂
ΡΟΛΟΙ	έλεγχος	κάτοχος	κάτοχος έλεγχος	ανάγνωση *	ανάγνωση κάτοχος	αφύπνιση	αφύπνιση	αναζήτηση	κάτοχος
R ₂		έλεγχος		εγγραφή *	εκτέλεση			κάτοχος	αναζήτηση *
•									
•									
•									
R _n			έλεγχος		εγγραφή	διακοπή			

Εικόνα 4.7 Αναπαράσταση του RBAC με μήτρα ελέγχου πρόσβασης

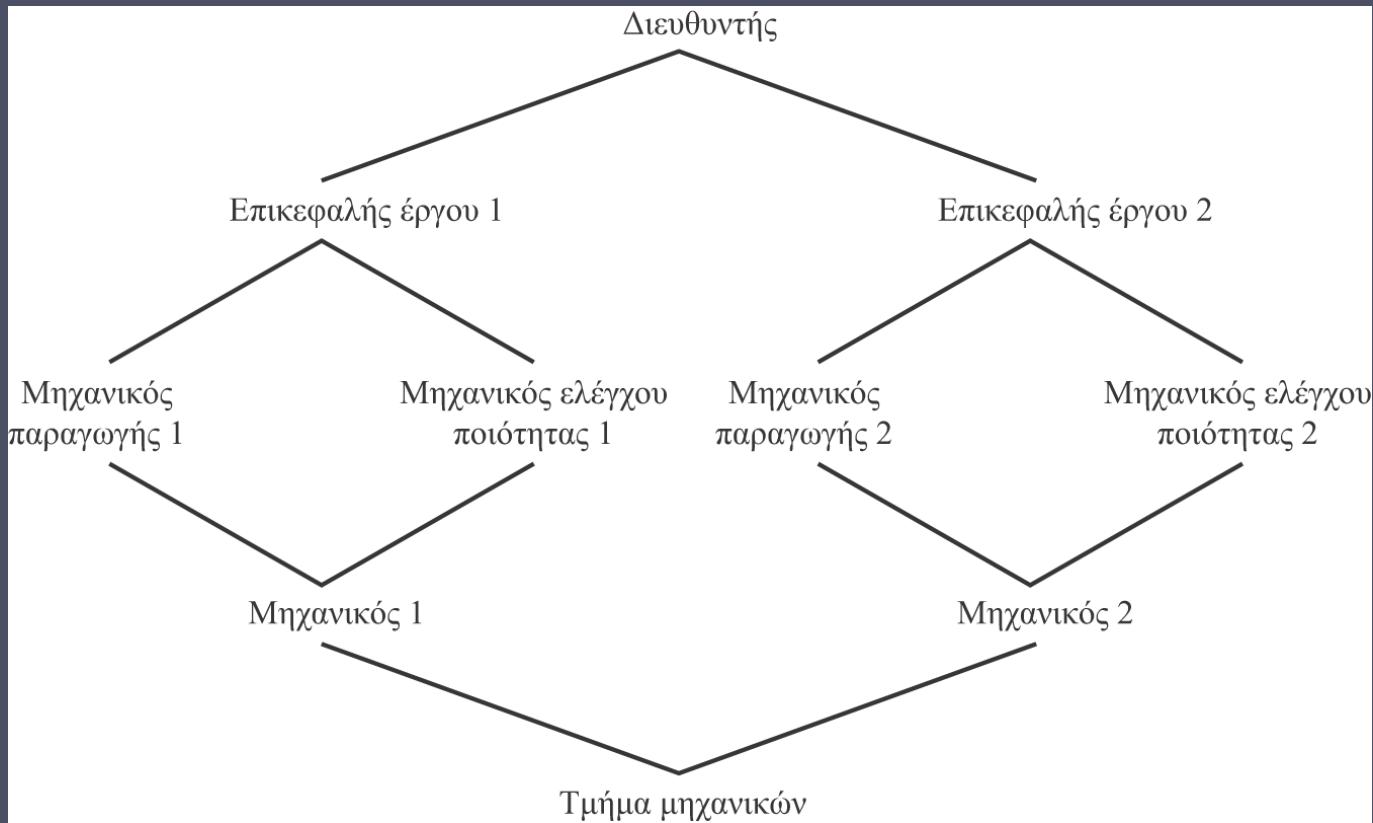


Εικόνα 4.8 Μια οικογένεια μοντέλων ελέγχου πρόσβασης βασισμένου σε ρόλους

Πίνακας 4.3

Εμβέλεια μοντέλων RBAC

Μοντέλα	Ιεραρχίες	Περιορισμοί
RBAC ₀	Όχι	Όχι
RBAC ₁	Ναι	Όχι
RBAC ₂	Όχι	Ναι
RBAC ₃	Ναι	Ναι



Εικόνα 4.9 Παράδειγμα ιεραρχίας ρόλων

Περιορισμοί - RBAC

- Παρέχουν έναν τρόπο προσαρμογής του ελέγχου RBAC στις συγκεκριμένες απαιτήσεις των πολιτικών διαχείρισης και ασφάλειας ενός οργανισμού
- Μια καλώς ορισμένη σχέση μεταξύ ρόλων ή μια συνθήκη που σχετίζεται με ρόλους
- Τύποι:

Αμοιβαία αποκλειόμενοι ρόλοι

- Σε έναν χρήστη μπορεί να ανατεθεί μόνο ένας ρόλος από το σύνολο (είτε κατά τη διάρκεια μίας συνόδου είτε στατικά)
- Κάθε άδεια (δικαίωμα πρόσβασης) μπορεί να χορηγηθεί μόνο σε έναν ρόλο του συνόλου

Πληθικότητα

- Ορισμός ενός μέγιστου πλήθους αναφορικά με τους ρόλους

Προαπαιτούμενοι ρόλοι

- Επιβάλλουν ότι ένας χρήστης δύναται να αναλάβει έναν συγκεκριμένο ρόλο μόνο αν έχει ήδη αναλάβει κάποιον άλλο καθορισμένο ρόλο

Έλεγχος πρόσβασης βασισμένος σε ιδιότητες (ABAC)

Ορίζει εξουσιοδοτήσεις που εκφράζουν συνθήκες για τις ιδιότητες και του πόρου και του υποκειμένου

Το δυνατό σημείο της μεθόδου είναι η ευελιξία και η εκφραστική ισχύς της

Το κύριο εμπόδιο για την υιοθέτησή της σε πραγματικά συστήματα είναι οι ανησυχίες σχετικά με τις επιπτώσεις που θα έχει στην απόδοση ο υπολογισμός κατηγορημάτων (predicates) για κάθε προσπέλαση, τα οποία αφορούν ιδιότητες και του πόρου και των χρηστών

Οι τεχνολογίες των υπηρεσιών Ιστού έχουν πρωτοστατήσει, ιδιαίτερα με την εισαγωγή της Επεκτάσιμης Γλώσσας Σήμανσης Ελέγχου Πρόσβασης (XAMCL)

Υπάρχει σημαντικό ενδιαφέρον για την εφαρμογή του μοντέλου στις υπηρεσίες νέφους

Μοντέλο ABAC: Ιδιότητες

Ιδιότητες υποκειμένου

- Ένα υποκείμενο είναι μια ενεργητική οντότητα που προκαλεί τη ροή πληροφοριών μεταξύ αντικειμένων ή αλλαγές στην κατάσταση του συστήματος
- Οι ιδιότητες ορίζουν την ταυτότητα και τα χαρακτηριστικά του υποκειμένου

Ιδιότητες αντικειμένου

- Ένα αντικείμενο (ή πόρος) είναι μια παθητική οντότητα που σχετίζεται με το πληροφοριακό σύστημα και η οποία περιέχει ή λαμβάνει πληροφορίες
- Τα αντικείμενα έχουν ιδιότητες τις οποίες μπορεί κανείς να εκμεταλλευθεί για τη λήψη αποφάσεων ελέγχου πρόσβασης

Ιδιότητες περιβάλλοντος

- Περιγράφουν το λειτουργικό, το τεχνικό, και ακόμα και το περιστασιακό περιβάλλον ή πλαίσιο στο οποίο λαμβάνει χώρα η προσπέλαση των πληροφοριών
- Μέχρι στιγμής αυτές οι ιδιότητες έχουν κυρίως αγνοηθεί στις περισσότερες πολιτικές ελέγχου πρόσβασης

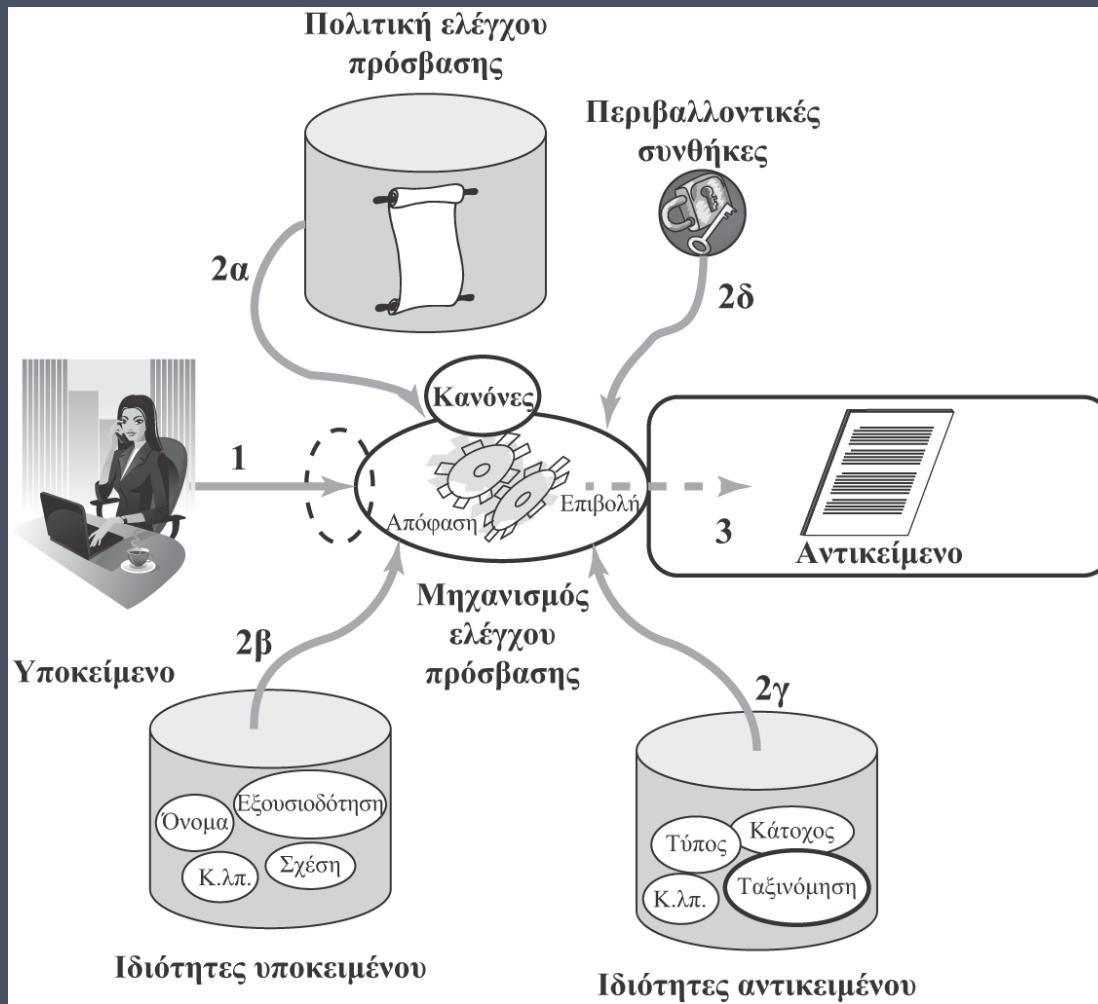
ABAC

Εξωρίζει επειδή ελέγχει την πρόσβαση με βάση κανόνες που αφορούν τις ιδιότητες οντοτήτων, ενέργειες, καθώς και το περιβάλλον που σχετίζεται με την αίτηση

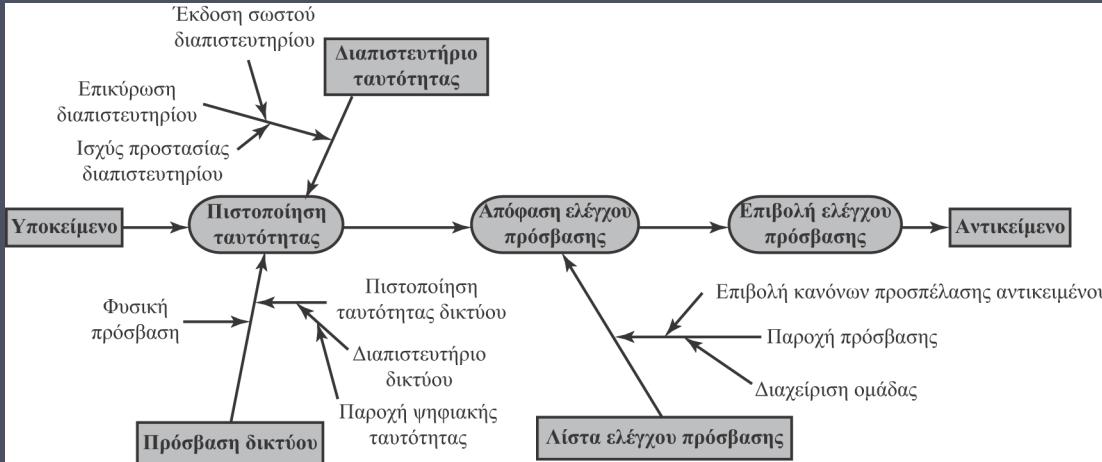
Στηρίζεται στην αξιολόγηση ιδιοτήτων του υποκειμένου, ιδιοτήτων του αντικειμένου, καθώς και σε μια τυπική σχέση ή κανόνα ελέγχου πρόσβασης που ορίζει τις επιτρεπτές ενέργειες για συνδυασμούς ιδιοτήτων υποκειμένου-αντικειμένου σε δεδομένο περιβάλλον

Τα συστήματα ABAC είναι σε θέση να επιβάλλουν ιδέες/ τεχνικές DAC, RBAC και MAC

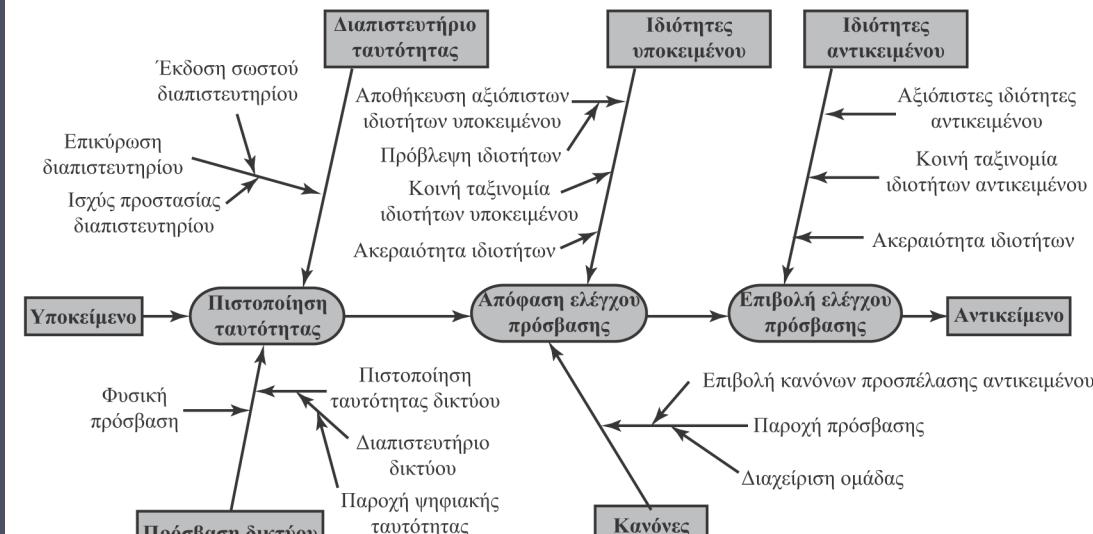
Επιτρέπει τον συνδυασμό απεριόριστων ιδιοτήτων προκειμένου να ικανοποιεί οποιονδήποτε κανόνα ελέγχου πρόσβασης



Εικόνα 4.10 Απλό σενάριο ΑΒΑC



(a) Αλυσίδα εμπιστοσύνης λιστών ACL



(b) Αλυσίδα εμπιστοσύνης ελέγχου ABAC

Εικόνα 4.11 Σχέσεις εμπιστοσύνης λιστών ACL και ελέγχου ABAC

Πολιτικές ABAC

Μια πολιτική είναι ένα σύνολο κανόνων και σχέσεων που ορίζουν την επιτρεπτή συμπεριφορά μέσα σε έναν οργανισμό, με βάση τα προνόμια των υποκειμένων και τον τρόπο με τον οποίο πρέπει να προστατεύονται οι πόροι ή τα αντικείμενα υπό συγκεκριμένες περιβαλλοντικές συνθήκες

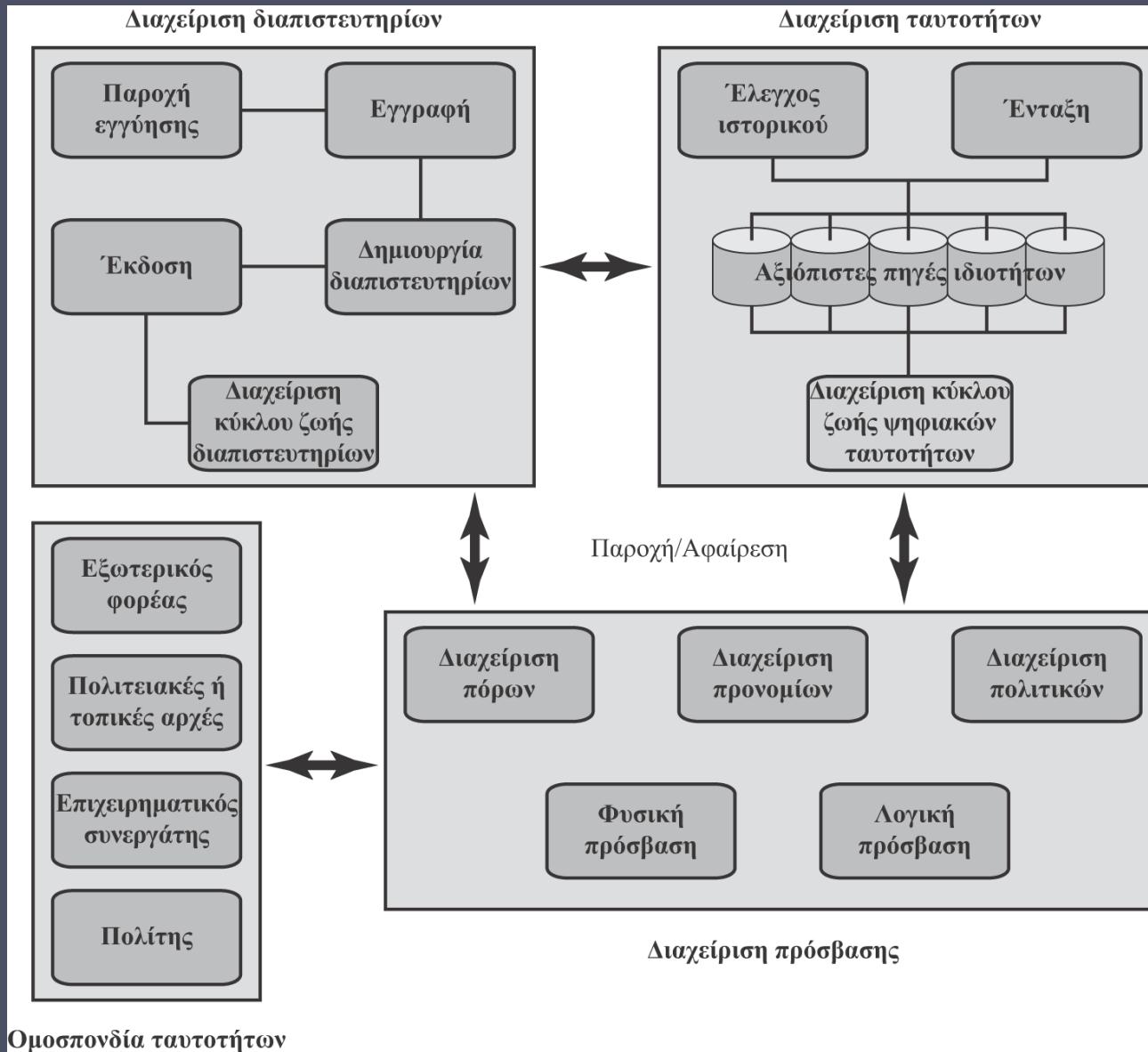
Συνήθως συντάσσεται από τη σκοπιά του αντικειμένου το οποίο χρειάζεται προστασία και των προνομίων που είναι διαθέσιμα για τα υποκείμενα

Τα **προνόμια** αντιπροσωπεύουν την εξουσιοδοτημένη συμπεριφορά ενός υποκειμένου ορίζονται από κάποια αρχή και ενσωματώνονται σε μια πολιτική

Άλλοι όροι που χρησιμοποιούνται ως συνώνυμοι των προνομίων είναι οι όροι δικαιώματα (rights), εξουσιοδοτήσεις (authorizations) και δικαιοδοτήσεις (entitlements)

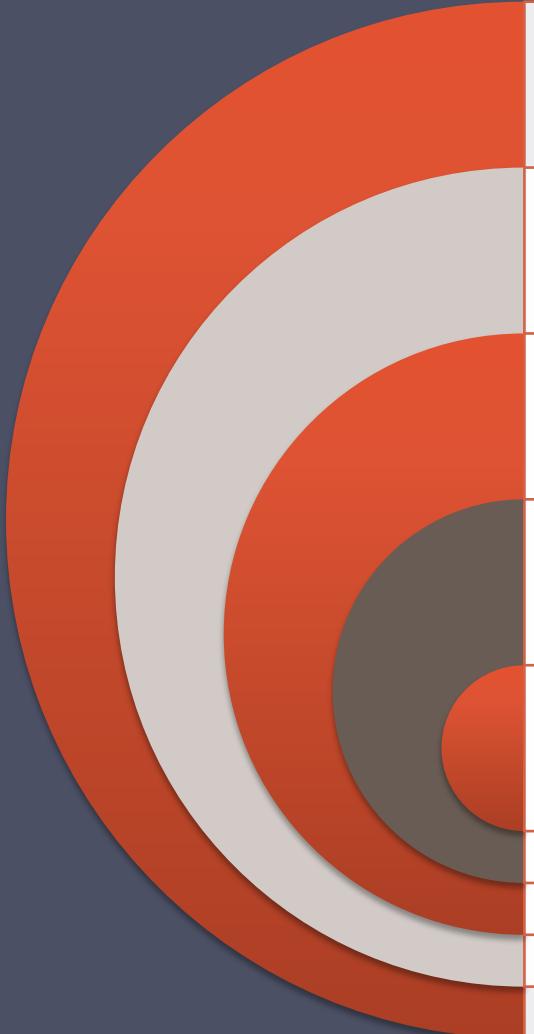
Διαχείριση ταυτότητων, διαπιστευτηρίων και πρόσβασης (ICAM)

- Διεξοδική προσέγγιση της διαχείρισης και υλοποίησης ψηφιακών ταυτότητων, διαπιστευτηρίων και ελέγχου πρόσβασης
- Έχει αναπτυχθεί από την κυβέρνηση των Η.Π.Α
- Είναι σχεδιασμένη:
 - Να δημιουργεί έμπιστες αναπαραστάσεις ψηφιακών ταυτότητων για φυσικά πρόσωπα και μη φυσικές οντότητες (nonperson entities, NPE)
 - Να συνδέει αυτές τις ταυτότητες με διαπιστευτήρια τα οποία μπορούν να ενεργούν ως πληρεξούσιοι για τα φυσικά πρόσωπα ή τις NPE σε συναλλαγές πρόσβασης
 - Το διαπιστευτήριο είναι ένα αντικείμενο ή μια δομή δεδομένων που συνδέει με αξιόπιστο τρόπο μια ταυτότητα με ένα τεκμήριο ασφαλείας το οποίο βρίσκεται στην κατοχή και υπό τον έλεγχο ενός συνδρομητή
 - Να χρησιμοποιεί τα διαπιστευτήρια για να παρέχει εξουσιοδοτημένη πρόσβαση στους πόρους ενός φορέα ή υπηρεσίας



Εικόνα 4.12 Διαχείριση ταυτοτήτων, διαπιστευτηρίων και πρόσβασης (ICAM)

Διαχείριση ταυτότητων



	<p>Ασχολείται με την ανάθεση ιδιοτήτων σε μια ψηφιακή ταυτότητα και τη σύνδεση της συγκεκριμένης ταυτότητας με ένα φυσικό πρόσωπο ή NPE</p>
	<p>Ο στόχος είναι η δημιουργία φερέγγυας ψηφιακής ταυτότητας η οποία δεν εξαρτάται από συγκεκριμένη εφαρμογή ή πλαίσιο</p>
	<p>Η δημοφιλέστερη μέθοδος, ελέγχου πρόσβασης για εφαρμογές και προγράμματα είναι η δημιουργία ψηφιακής αναπαράστασης μιας ταυτότητας για τη συγκεκριμένη χρήση της εφαρμογής ή του προγράμματος</p>
	<p>Η συντήρηση και προστασία της ίδιας της ταυτότητας θεωρείται δευτερεύουσα σε σχέση με τον σκοπό της εφαρμογής</p>
	<p>Ένα τελευταίο στοιχείο είναι η διαχείριση κύκλου ζωής (lifecycle management), στην οποία περιλαμβάνονται τα εξής:</p> <ul style="list-style-type: none">• Μηχανισμοί, πολιτικές και διαδικασίες για την προστασία των προσωπικών δεδομένων των ταυτοτήτων• Ελέγχος πρόσβασης στα δεδομένα των ταυτοτήτων• Τεχνικές για κοινή χρήση αξιόπιστων δεδομένων από ταυτότητες με εφαρμογές που τα χρειάζονται• Κατάργηση μιας εταιρικής ταυτότητας

Διαχείριση διαπιστευτηρίων

Η διαχείριση του κύκλου ζωής του διαπιστευτηρίου

Παραδείγματα διαπιστευτηρίων είναι οι «έξυπνες κάρτες», τα ιδιωτικά/δημόσια κρυπτογραφικά κλειδιά, και τα ψηφιακά πιστοποιητικά

Εμπεριέχει πέντε λογικά συστατικά μέρη:

Προκειμένου να τεκμηριωθεί η ανάγκη για ένα διαπιστευτήριο, απαιτείται η παροχή εγγύησης από ένα εξουσιοδοτημένο φυσικό πρόσωπο για ένα άλλο φυσικό πρόσωπο ή οντότητα

Το προτεινόμενο φυσικό πρόσωπο ή οντότητα προχωρά σε εγγραφή για το διαπιστευτήριο

- Η διαδικασία συνήθως αποτελείται από την παροχή σχετικών αποδεικτικών εγγράφων για την ταυτότητα του αιτούντος, καθώς και την απόκτηση βιογραφικών και βιομετρικών δεδομένων
- Αυτό το βήμα ενδέχεται να περιλαμβάνει και την ενοιωμάτωση αξιόπιστων δεδομένων που αφορούν ιδιότητες, τα οποία βρίσκονται αποθηκευμένα στην υπομονάδα διαχείρισης ταυτοτήτων

Δημιουργείται ένα διαπιστευτήριο

- Ανάλογα με τον τύπο του, το βήμα αυτό μπορεί να περιλαμβάνει κρυπτογράφηση, χορήγη ψηφιακής υπογραφής, δημιουργία «έξυπνης κάρτας», ή άλλες λειτουργίες

Εκδίδεται το διαπιστευτήριο στο φυσικό πρόσωπο ή την NPE

Ένα διαπιστευτήριο πρέπει να συντηρείται για όσο διάστημα διαρκεί ο κύκλος ζωής του

- Αυτό μπορεί να περιλαμβάνει τυχόν ανάκληση, επανείδοση/αντικατάσταση, επανεγγραφή, λήξη, επαναφορά προσωπικού αριθμού αναγνώρισης (PIN), αναστολή ισχύος, ή επανέναρξη ισχύος

Διαχείριση πρόσβασης

Ασχολείται με τη διαχείριση και τον έλεγχο των τρόπων με τους οποίους επιτρέπεται η πρόσβαση οντοτήτων σε πόρους

Καλύπτει και τη λογική και τη φυσική πρόσβαση

Μπορεί να αποτελεί εσωτερικό ή εξωτερικό στοιχείο του συστήματος

Ο σκοπός της είναι να εξασφαλίσει ότι ακολουθείται η σωστή διαδικασία επαλήθευσης της ταυτότητας όταν ένα άτομο επιχειρεί να εισέλθει σε προστατευόμενες κτιριακές εγκαταστάσεις ή να προσπελάσει προστατευόμενα υπολογιστικά συστήματα, ή δεδομένα

Για ένα σύστημα ελέγχου πρόσβασης που καλύπτει μια ολόκληρη επιχείρηση, απαιτούνται τρία υποστηρικτικά στοιχεία:

- Διαχείριση πόρων
- Διαχείριση προνομίων
- Διαχείριση πολιτικών

Για ένα σύστημα ελέγχου πρόσβασης που καλύπτει μια ολόκληρη επιχείρηση, απαιτούνται τρία υποστηρικτικά στοιχεία:

Διαχείριση πόρων

- Ασχολείται με τον ορισμό κανόνων που αφορούν έναν πόρο για τον οποίο απαιτείται έλεγχος πρόσβασης
- Οι κανόνες μπορεί να περιλαμβάνουν απαιτήσεις διαπιστευτηρίων και τυχόν ιδιότητες χρηστών, ιδιότητες πόρων, και περιβαλλοντικές συνθήκες οι οποίες απαιτούνται για την προσπέλαση μιας δεδομένης λειτουργίας ενός δεδομένου πόρου

Διαχείριση προνομίων

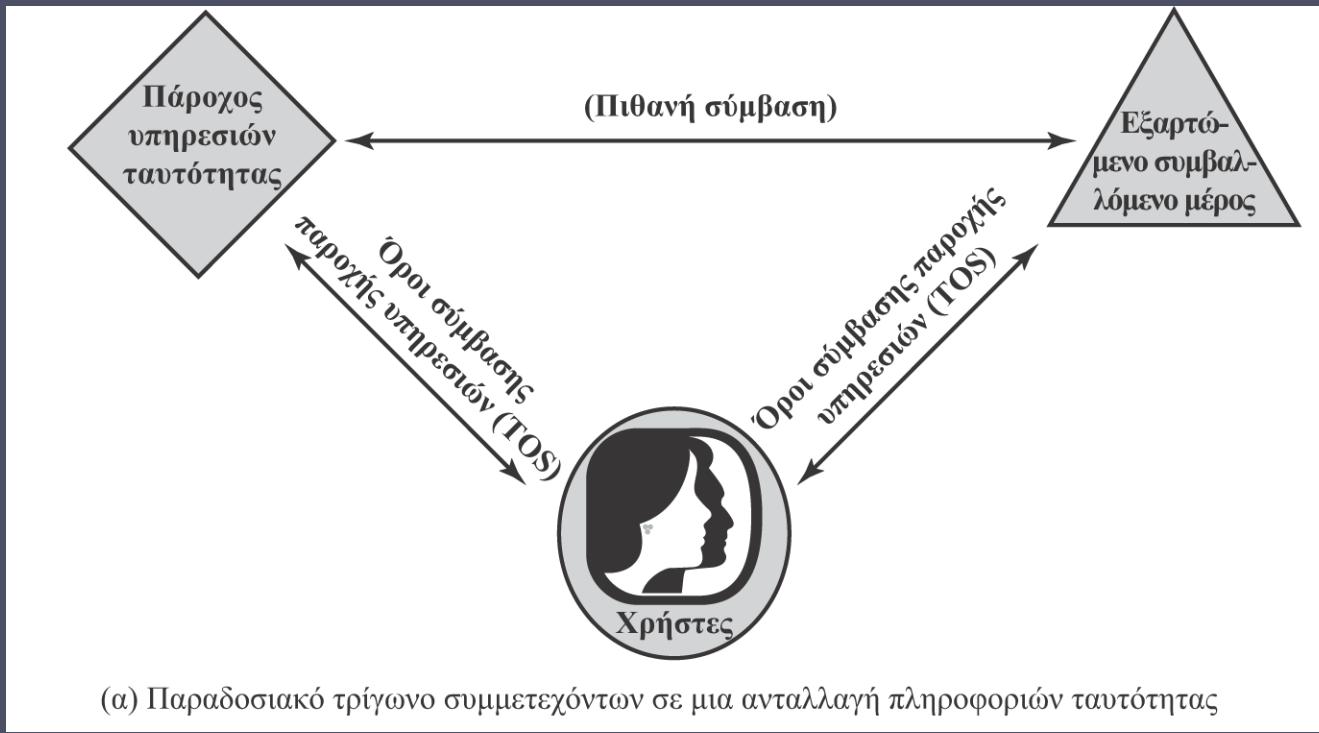
- Ασχολείται με τον προσδιορισμό και τη διατήρηση των ιδιοτήτων δικαιοδότησης ή προνομίων οι οποίες συνιστούν το προφίλ πρόσβασης ενός ατόμου
- Αυτές οι ιδιότητες αναπαριστούν χαρακτηριστικά του ατόμου και μπορούν να χρησιμοποιηθούν ως βάση για τη λήψη αποφάσεων που σχετίζονται με την πρόσβαση τόσο σε φυσικούς όσο και σε λογικούς πόρους
- Τα προνόμια θεωρούνται ιδιότητες οι οποίες μπορούν να συνδεθούν με μια ψηφιακή ταυτότητα

Διαχείριση πολιτικών

- Καθορίζει τι επιτρέπεται και τι δεν επιτρέπεται σε μια συναλλαγή πρόσβασης

Ομοσπονδία ταυτότητων

- Όρος που χρησιμοποιείται για να περιγράψει την τεχνολογία, τα πρότυπα, τις πολιτικές και τις διαδικασίες που επιτρέπουν σε έναν οργανισμό να εμπιστεύεται ψηφιακές ταυτότητες, ιδιότητες ταυτότητων και διαπιστευτήρια που έχουν δημιουργηθεί και εκδοθεί από κάποιον άλλο οργανισμό
- Απαντά σε δύο ερωτήματα:
 - Με ποιον τρόπο εμπιστεύεστε τις ταυτότητες ατόμων από εξωτερικούς οργανισμούς τα οποία χρειάζονται πρόσβαση στα συστήματά σας;
 - Με ποιον τρόπο παρέχετε εγγυήσεις για τις ταυτότητες ατόμων του οργανισμού σας όταν τα άτομα αυτά πρέπει να συνεργαστούν με εξωτερικούς οργανισμούς;



Εικόνα 4.13 Τεχνικές ανταλλαγής πληροφοριών ταυτότητας

Ανοικτό Πλαίσιο Εμπιστοσύνης Ταυτοτήτων

OpenID

- Ανοικτό πρότυπο το οποίο επιτρέπει την πιστοποίηση της ταυτότητας των χρηστών από ορισμένους συνεργαζόμενους ιστότοπους με χρήση ανεξάρτητης υπηρεσίας

OIDF

- Το Ίδρυμα OpenID είναι ένας διεθνής μη κερδοσκοπικός οργανισμός φυσικών προσώπων και εταιριών που συμφώνησαν να χρησιμοποιούν, να προωθούν και να προστατεύουν τις τεχνολογίες OpenID

ICF

- Το Ίδρυμα Πληροφοριακών Καρτών είναι μη κερδοσκοπική κοινότητα εταιρειών και φυσικών προσώπων που συνεργάζονται με στόχο την εξέλιξη των οικοσύστηματος των Πληροφοριακών Καρτών

OITF

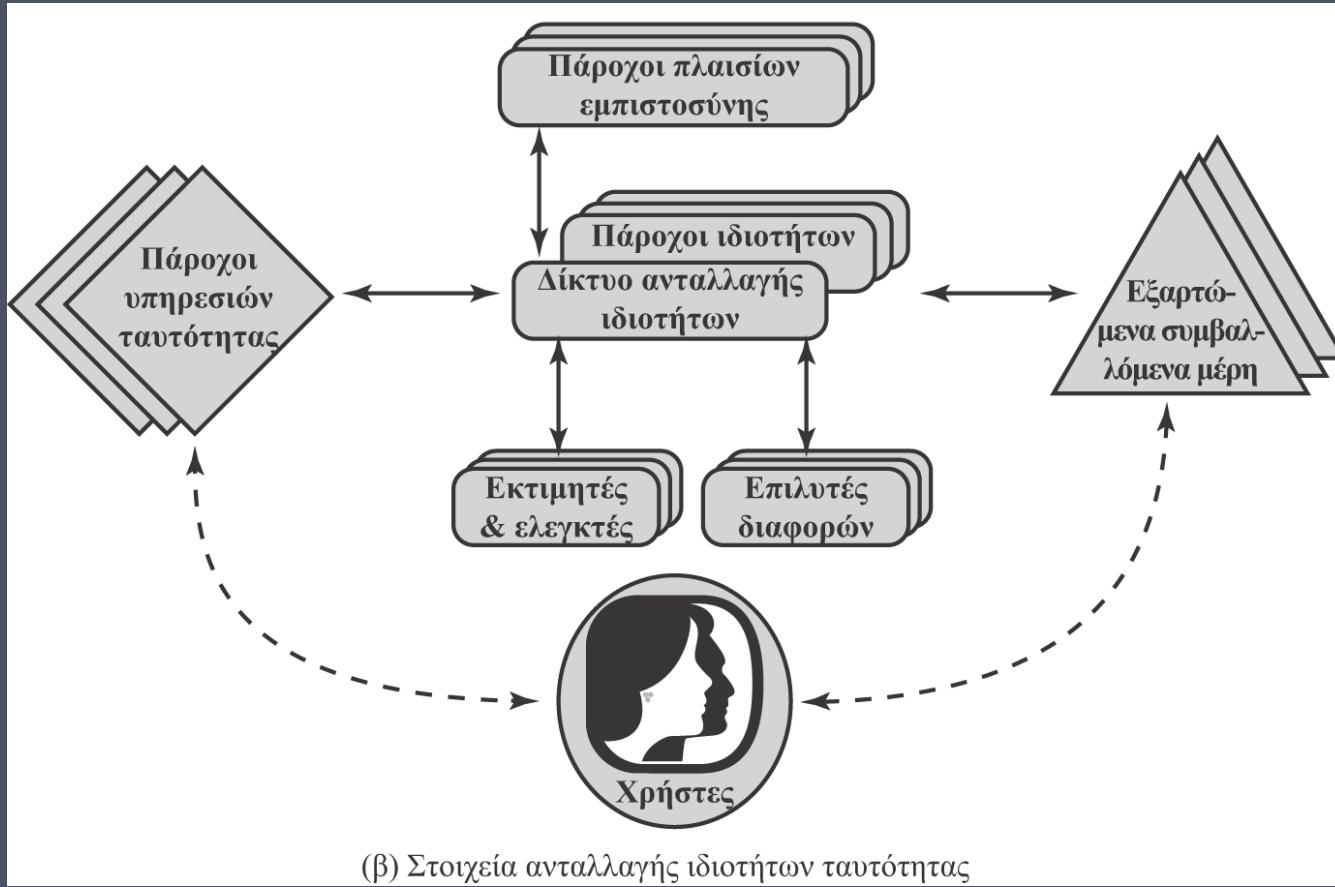
- Το Ανοικτό Πλαίσιο Εμπιστοσύνης Ταυτοτήτων είναι μια προτυποποιημένη, ανοικτή προδιαγραφή ενός πλαισίου εμπιστοσύνης για ανταλλαγή ταυτοτήτων και ιδιοτήτων, το οποίο έχουν αναπτύξει από κοινού τα ίδρυματα OIDF και ICF

OIX

- Ο Ανοικτός Οργανισμός Ανταλλαγής Ταυτοτήτων είναι ένας ανεξάρτητος, ουδέτερος, διεθνής πάροχος πιστοποίησης πλαισίων εμπιστοσύνης ο οποίος έχει υιοθετήσει το μοντέλο OITF

AXN

- Το Δίκτυο Ανταλλαγής Ιδιοτήτων είναι μια ηλεκτρονική πύλη κλίμακας Διαδικτύου που επιτρέπει σε παρόχους υπηρεσιών ταυτότητας και εξαρτώμενα συμβαλλόμενα μέρη να προσπελάζουν μαζικά, αποδοτικά και με προσιτό κόστος, ιδιότητες ηλεκτρονικών ταυτοτήτων που έχουν βεβαιωθεί, αδειοδοτηθεί και επαληθευθεί από τους χρήστες



Εικόνα 4.13 Τεχνικές ανταλλαγής πληροφοριών ταυτότητας

Πίνακας 4.4

Καθήκοντα και ρόλοι για το παράδειγμα της τράπεζας

α) Καθήκοντα και τίτλοι θέσεων

Ρόλος	Καθήκοντα	Τίτλος θέσης
A	οικονομικός αναλυτής	Υπάλληλος
B	οικονομικός αναλυτής	Υπεύθυνος Ομάδας
C	οικονομικός αναλυτής	Προϊστάμενος Τμήματος
D	οικονομικός αναλυτής	Κατώτερος
E	οικονομικός αναλυτής	Ανώτερος
F	οικονομικός αναλυτής	Ειδικός
G	οικονομικός αναλυτής	Βοηθός
...	...	
X	τεχνικός αναλυτής μετοχών	Υπάλληλος
Y	υποστήριξη ηλεκτρονικού εμπορίου	Κατώτερος
Z	επιχειρηματική τραπεζική	Προϊστάμενος Τμήματος

Πίνακας 4.4

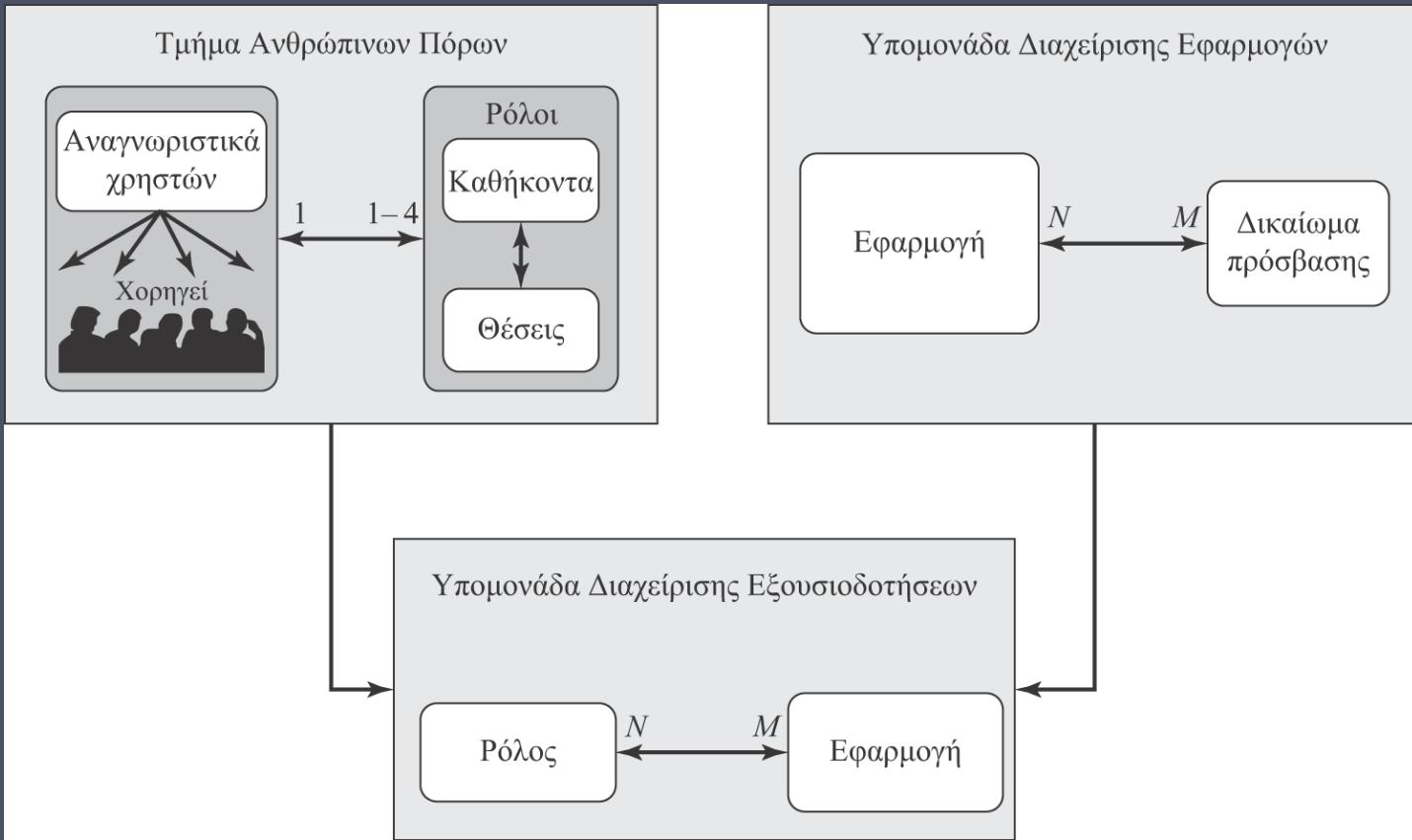
Καθήκοντα και ρόλοι για το παράδειγμα της τράπεζας

β) Αναθέσεις αδειών
(δικαιωμάτων πρόσβασης)

Ρόλος	Εφαρμογή	Δικαίωμα πρόσβασης
A	μέσα αγοράς χρήματος	1, 2, 3, 4
	διαπραγμάτευση παραγώγων	1, 2, 3, 7, 10, 12
	έντοκα μέσα	1, 4, 8, 12, 14, 16
B	μέσα αγοράς χρήματος	1, 2, 3, 4, 7
	διαπραγμάτευση παραγώγων	1, 2, 3, 7, 10, 12, 14
	έντοκα μέσα	1, 4, 8, 12, 14, 16
	καταναλωτικά μέσα για ιδιώτες	1, 2, 4, 7
...

γ) Αναθέσεις αδειών
με κληρονομικότητα

Ρόλος	Εφαρμογή	Δικαίωμα πρόσβασης
A	μέσα αγοράς χρήματος	1, 2, 3, 4
	διαπραγμάτευση παραγώγων	1, 2, 3, 7, 10, 12
	έντοκα μέσα	1, 4, 8, 12, 14, 16
B	μέσα αγοράς χρήματος	7
	διαπραγμάτευση παραγώγων	14
	καταναλωτικά μέσα για ιδιώτες	1, 2, 4, 7
...



Εικόνα 4.14 Παράδειγμα διαχείρισης ελέγχου πρόσβασης

Σύνοψη

- Αρχές ελέγχου πρόσβασης
 - Γενικό πλαίσιο ελέγχου πρόσβασης
 - Πολιτικές ελέγχου πρόσβασης
- Υποκείμενα, αντικείμενα και δικαιώματα πρόσβασης
- Διακριτικός έλεγχος πρόσβασης
 - Ένα μοντέλο ελέγχου πρόσβασης
 - Περιοχές προστασίας
- Παράδειγμα: Έλεγχος πρόσβασης σε αρχεία του UNIX
 - Παραδοσιακός έλεγχος πρόσβασης σε αρχεία του UNIX
 - Λίστες ελέγχου πρόσβασης στο UNIX
- Έλεγχος πρόσβασης βασισμένος σε ρόλους
 - Μοντέλα αναφοράς RBAC
- Έλεγχος πρόσβασης βασισμένος σε ιδιότητες
 - Ιδιότητες
 - Λογική αρχιτεκτονική ελέγχου ABAC
 - Πολιτικές ελέγχου ABAC

Διαχείριση ταυτότητων, διαπιστευτηρίων και πρόσβασης

 - Διαχείριση ταυτότητων
 - Διαχείριση διαπιστευτηρίων
 - Διαχείριση πρόσβασης
 - Ομοσπονδία ταυτότητων
- Πλαίσια εμπιστοσύνης
 - Παραδοσιακή μέθοδος ανταλλαγής ταυτότητων
 - Ανοικτό πλαίσιο εμπιστοσύνης ταυτότητων
- Σύστημα RBAC για μια τράπεζα

