

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 3

Πιστοποίηση ταυτότητας χρηστών

RFC 4949

Η πιστοποίηση ταυτότητας χρηστών ορίζεται στο έγγραφο RFC 4949 ως εξής:

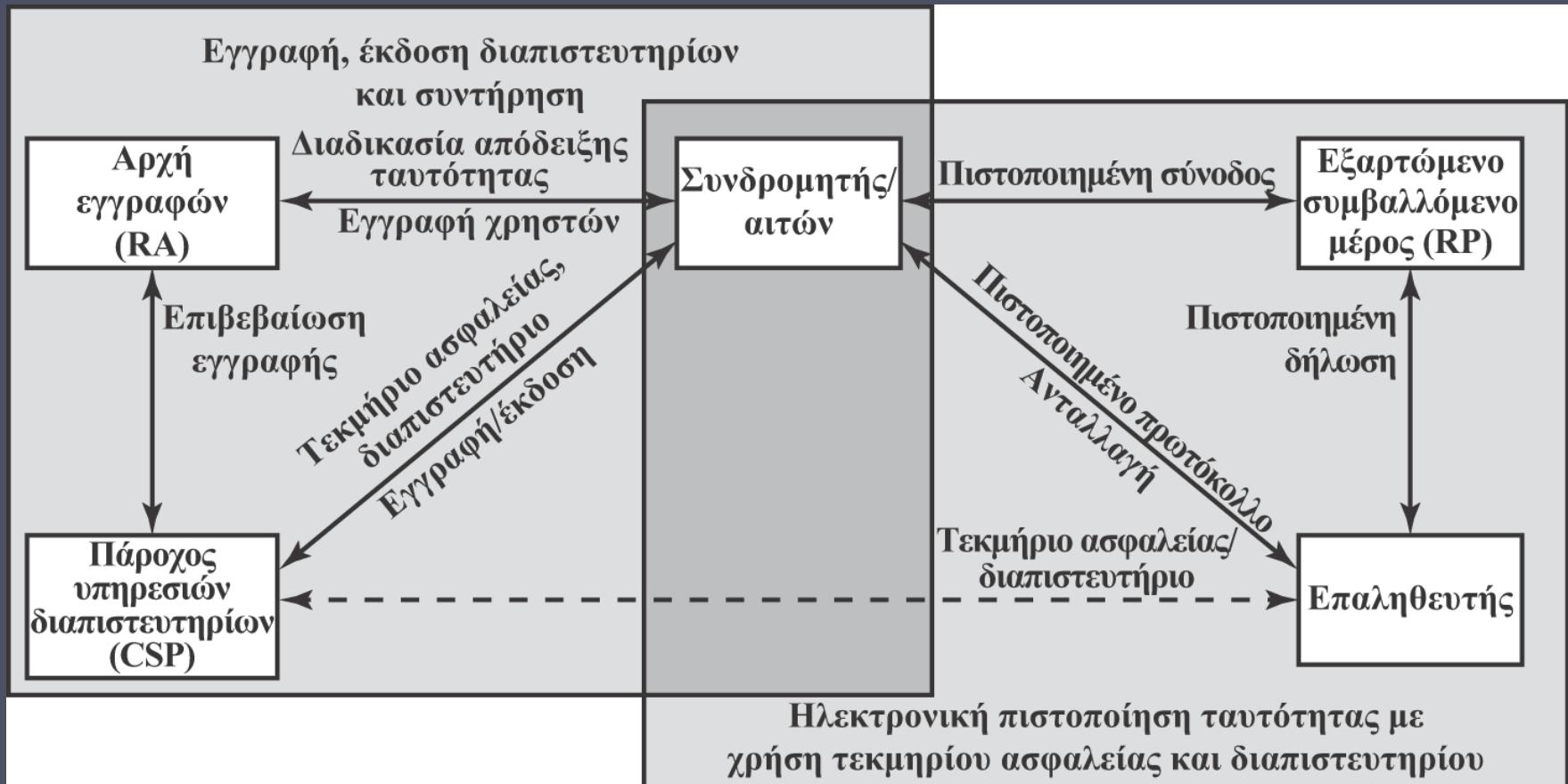
«Η διαδικασία επαλήθευσης της ταυτότητας για μια οντότητα του συστήματος ή εκ μέρους αυτής.»



Διαδικασία πιστοποίησης ταυτότητας

- Βασικό δομικό στοιχείο και κύρια γραμμή άμυνας
- Βάση για τον έλεγχο πρόσβασης και την απόδοση ευθυνών στους χρήστες
- Βήμα ταυτοποίησης
 - Υποβολή ενός αναγνωριστικού προς το σύστημα ασφαλείας
- Βήμα επαλήθευσης
 - Υποβολή ή δημιουργία πληροφοριών πιστοποίησης ταυτότητας οι οποίες επιβεβαιώνουν τη συσχέτιση μεταξύ οντότητας και αναγνωριστικού





Εικόνα 3.1 Το αρχιτεκτονικό μοντέλο ηλεκτρονικής πιστοποίησης ταυτότητας που ορίζεται στο έγγραφο SP 800-63-2 του NIST

Οι τέσσερις τρόποι πιστοποίησης της ταυτότητας ενός χρήστη βασίζονται στα εξής:

Πληροφορία που γνωρίζει το άτομο

- Κωδικός πρόσβασης, PIN, απαντήσεις σε προκαθορισμένες ερωτήσεις

Αντικείμενο
που βρίσκεται
στην κατοχή
του ατόμου
(τεκμήριο
ασφαλείας)

- «Έξυπνη κάρτα»,
ηλεκτρονική κάρτα-
κλειδί, κανονικό
κλειδί

Παθητικό
χαρακτηριστικό
του ατόμου
(στατικό
βιομετρικό
χαρακτηριστικό)

- Δακτυλικά
αποτυπώματα,
αμφιβληστροειδής
χιτώνας, πρόσωπο

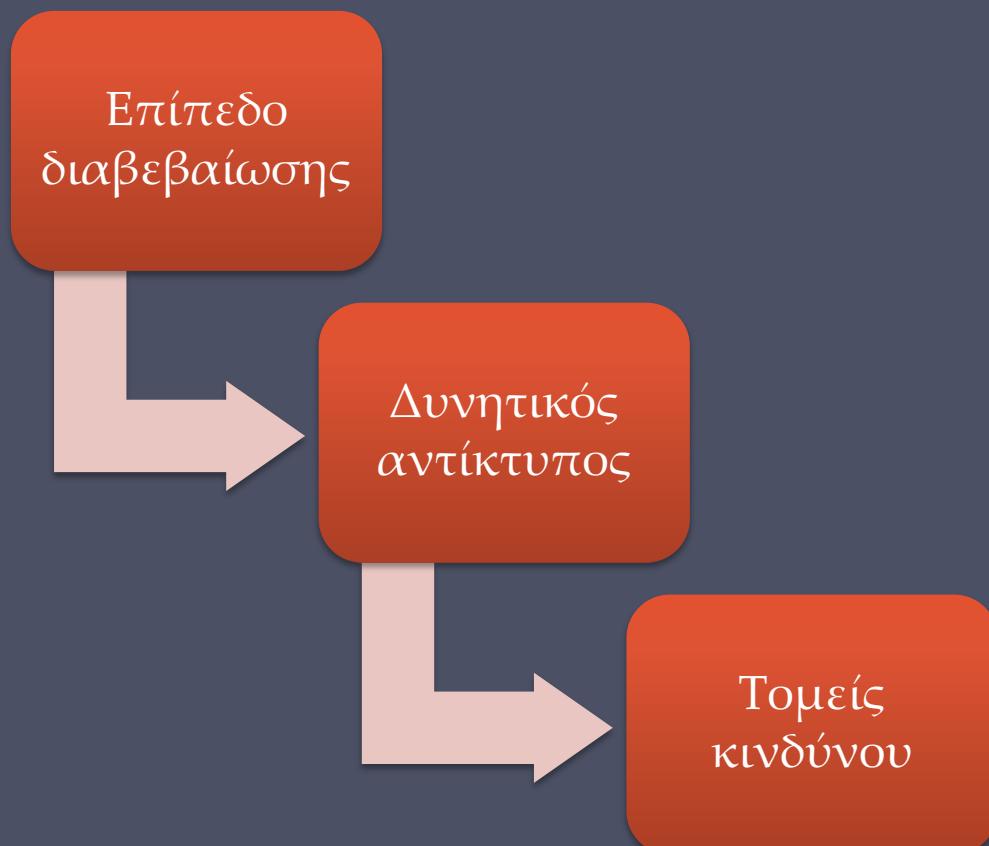
Ενεργητικό
χαρακτηριστικό
του ατόμου
(δυναμικό
βιομετρικό
χαρακτηριστικό)

- Φωνή, γραφικός
χαρακτήρας,
ρυθμός
πληκτρολόγησης

Εκτίμηση κινδύνου

για την πιστοποίηση ταυτότητας χρηστών

- Υπάρχουν τρεις ξεχωριστές έννοιες:



Επίπεδο διαβεβαίωσης

Περιγράφει τον βαθμό βεβαιότητας ενός οργανισμού ότι κάποιος χρήστης έχει υποβάλει διαπιστευτήριο το οποίο αναφέρεται όντως στη δική του ταυτότητα

Πιο συγκεκριμένα, ορίζεται ως εξής:

Ο βαθμός εμπιστοσύνης προς τη διαδικασία αξιολόγησης που χρησιμοποιείται για την τεκμηρίωση της ταυτότητας του ατόμου στο οποίο εκδόθηκε το διαπιστευτήριο

Ο βαθμός εμπιστοσύνης ότι το άτομο που κάνει χρήση του διαπιστευτηρίου είναι όντως το άτομο στο οποίο εκδόθηκε το διαπιστευτήριο

Τέσσερα επίπεδα διαβεβαίωσης

Επίπεδο 1

- Ελάχιστη ή καθόλου εμπιστοσύνη στην εγκυρότητα της επιβεβαιωμένης ταυτότητας

Επίπεδο 2

- Μέτρια εμπιστοσύνη στην εγκυρότητα της επιβεβαιωμένης ταυτότητας

Επίπεδο 3

- Υψηλή εμπιστοσύνη στην εγκυρότητα της επιβεβαιωμένης ταυτότητας

Επίπεδο 4

- Πολύ υψηλή εμπιστοσύνη στην εγκυρότητα της επιβεβαιωμένης ταυτότητας

Δυνητικός αντίκτυπος

- Στο πρότυπο FIPS 199 ορίζονται τρία επίπεδα δυνητικού αντίκτυπου σε οργανισμούς ή φυσικά πρόσωπα στην περίπτωση παραβίασης της ασφάλειας:
 - Χαμηλό
 - 'Ενα σφάλμα πιστοποίησης ταυτότητας αναμένεται να έχει περιορισμένο αντίκτυπο στις λειτουργίες και τους πόρους του οργανισμού, ή στους μεμονωμένους χρήστες
 - Μεσαίο
 - 'Ενα σφάλμα πιστοποίησης ταυτότητας αναμένεται να έχει σοβαρό αντίκτυπο
 - Υψηλό
 - 'Ενα σφάλμα πιστοποίησης ταυτότητας αναμένεται να έχει οδυνηρό ή καταστροφικό αντίκτυπο

Πίνακας 3.1

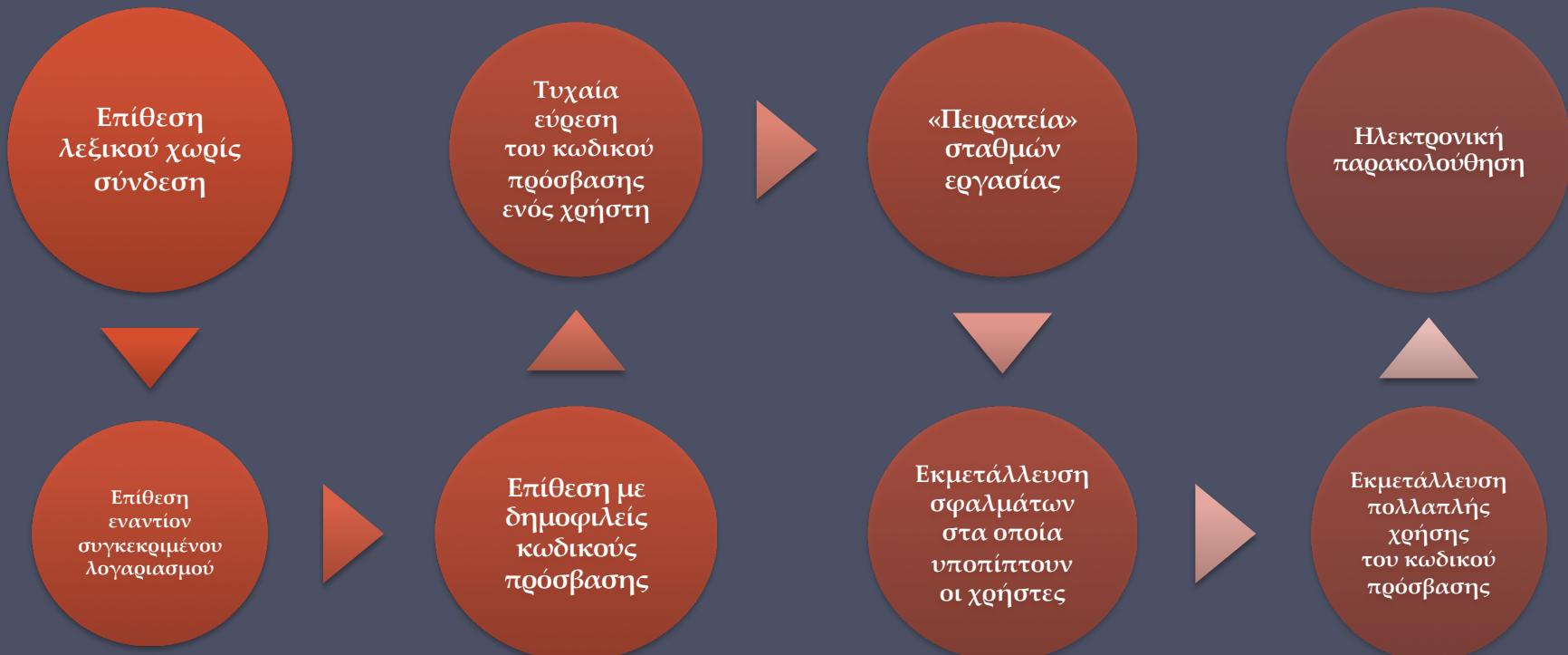
Μέγιστος δυνητικός αντίκτυπος για κάθε επίπεδο διαβεβαίωσης

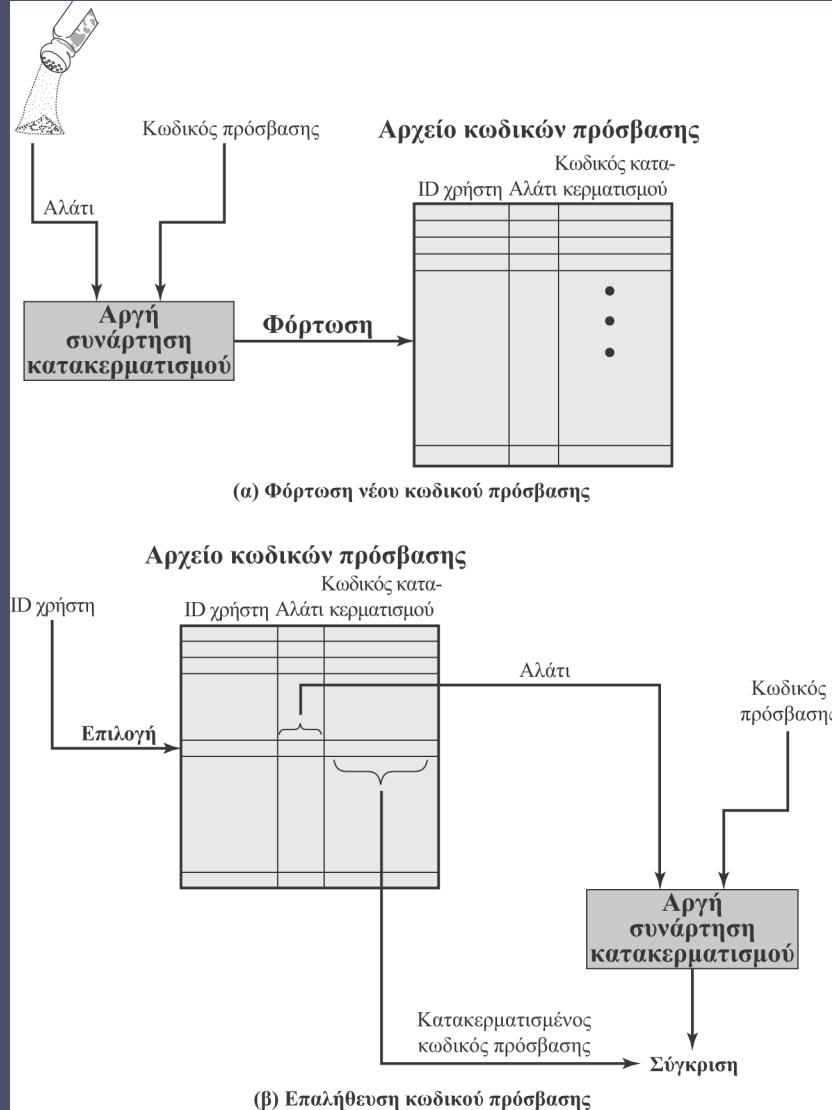
Κατηγορίες δυνητικού αντίκτυπου για σφάλματα πιστοποίησης ταυτότητας	Προφίλ αντίκτυπου επιπέδων διαβεβαίωσης			
	1	2	3	4
Ενόχληση, ανησυχία, ή προσβολή υπόληψης ή φήμης	Χαμηλό	Μεσαίο	Μεσαίο	Υψηλό
Οικονομικές απώλειες ή υπαιτιότητα του οργανισμού	Χαμηλό	Μεσαίο	Μεσαίο	Υψηλό
Ζημιές σε προγράμματα ή συμφέροντα του οργανισμού	Μηδενικό	Χαμηλό	Μεσαίο	Υψηλό
Μη εξουσιοδοτημένη γνωστοποίηση ευαίσθητων πληροφοριών	Μηδενικό	Χαμηλό	Μεσαίο	Υψηλό
Προσωπική ασφάλεια	Μηδενικό	Μηδενικό	Χαμηλό	Μεσαίο/Υψηλό
Παραβάσεις του αστικού ή ποινικού κώδικα	Μηδενικό	Χαμηλό	Μέτριο	Υψηλό

Πιστοποίηση ταυτότητας με κωδικούς πρόσβασης

- Ευρέως χρησιμοποιούμενη γραμμή άμυνας κατά των εισβολέων
 - Ο χρήστης παρέχει όνομα/αναγνωριστικό (ID) και κωδικό πρόσβασης
 - Το σύστημα συγκρίνει τον κωδικό πρόσβασης με έναν ήδη αποθηκευμένο κωδικό για το συγκεκριμένο αναγνωριστικό χρήστη
- Το αναγνωριστικό χρήστη:
 - Προσδιορίζει αν ο χρήστης είναι εξουσιοδοτημένος να έχει πρόσβαση στο σύστημα
 - Καθορίζει τα προνόμια (privileges), ή δικαιώματα, του χρήστη
 - Χρησιμοποιείται στον διακριτικό έλεγχο πρόσβασης (discretionary access control)

Ευπάθειες κωδικών πρόσβασης





Εικόνα 3.2 Μέθοδος κωδικών πρόσβασης του UNIX

Υλοποιήσεις UNIX

Αρχική μέθοδος

- Μήκος έως και οκτώ εκτυπώσιμους χαρακτήρες
- Χρησιμοποιείται τιμή αλατιού των 12 bit για την τροποποίηση της κρυπτογράφησης DES και τη μετατροπή της σε μονόδρομη συνάρτηση κατακρηματισμού
- Η κρυπτογράφηση του τμήματος εισόδου (που έχει μόνο μηδενικά bit) επαναλαμβάνεται 25 φορές
- Η έξοδος «μεταφράζεται» σε ακολουθία 11 χαρακτήρων

Πλέον θεωρείται ανεπαρκής

- Εξακολουθεί να είναι απαραίτητη είτε για λόγους συμβατότητας με υπάρχον λογισμικό διαχείρισης λογαριασμών είτε για χρήση σε περιβάλλοντα με συστήματα που προέρχονται από πολλούς κατασκευαστές

Βελτιωμένες υλοποιήσεις

Υπάρχουν διαθέσιμες άλλες,
πιο ισχυρές, μέθοδοι
κατακρηματισμού/αλατιού
για το UNIX

Το OpenBSD χρησιμοποιεί
συνάρτηση κατακρηματισμού
βασισμένη στο συμμετρικό
κρυπτογράφημα τμημάτων
Blowfish, την Bcrypt

- Η πιο ασφαλής παραλλαγή
της μεθόδου κατακρηματισμού/αλατιού
του UNIX
- Χρησιμοποιεί τιμή αλατιού των 128 bit
για να παράγει τιμή κατακρηματισμού
των 192 bit

Η προτεινόμενη συνάρτηση
κατακρηματισμού βασίζεται
στον αλγόριθμο MD5

- Τιμή αλατιού έως και 48 bit
- Απεριόριστο μήκος
κωδικών πρόσβασης
- Παράγει τιμή κατακρηματισμού
των 128 bit
- Χρησιμοποιεί εσωτερικό βρόχο
με 1000 επαναλήψεις για να επιτύχει
την επιβράδυνση

«Σπάσιμο» κωδικών πρόσβασης

Επιθέσεις λεξικού

- Ανάπτυξη ενός μεγάλου λεξικού με πιθανούς κωδικούς πρόσβασης και σύγκρισή τους με τους κωδικούς πρόσβασης που περιέχονται στο σχετικό αρχείο του συστήματος
- Κάθε κωδικός πρόσβασης πρέπει να κατακερματιστεί με χρήση κάθε διαθέσιμης τιμής αλατιού και μετά να συγκριθεί με αποθηκευμένες τιμές κατακερματισμού

Επιθέσεις με πίνακα «ουράνιου τόξου»

- Εκ των προτέρων υπολογισμός πινάκων με τιμές κατακερματισμού για όλες τις τιμές αλατιού
- Προκύπτει ένας τεράστιος πίνακας τιμών κατακερματισμού
- Μπορεί να αντιμετωπιστεί με χρήση μεγάλης τιμής αλατιού και τιμής κατακερματισμού με μεγάλο μήκος

Οι «σπάστες» κωδικών πρόσβασης εκμεταλλεύονται το γεγονός ότι μερικοί άνθρωποι επιλέγουν κωδικούς πρόσβασης τους οποίους μπορεί κανείς να μαντέψει εύκολα

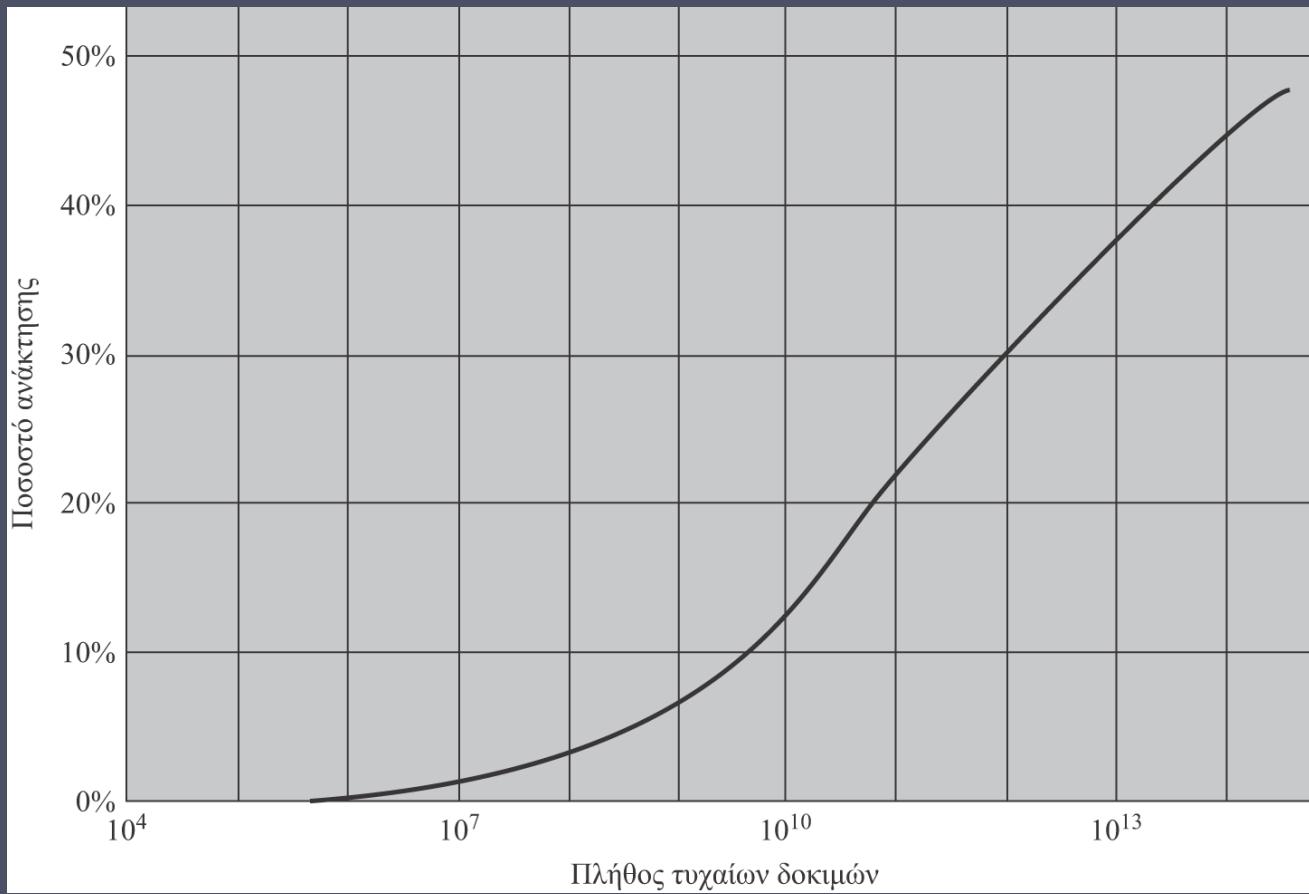
- Αντίστοιχα εύκολο είναι και το «σπάσιμο» κωδικών πρόσβασης με μικρό μήκος

John the Ripper

- «Σπάστης» κωδικών πρόσβασης ανοικτού πιργαίου κώδικα που αναπτύχθηκε αρχικά το 1996
- Χρησιμοποιεί έναν συνδυασμό τεχνικών αρμής βίας και τεχνικών λεξικού

Σύγχρονες προσεγγίσεις

- Πολιτική πολύπλοκων κωδικών πρόσβασης
 - Αναγκάζει τους χρήστες να επιλέγουν πιο ισχυρούς κωδικούς πρόσβασης
- Ωστόσο, και οι τεχνικές «σπασίματος» κωδικών πρόσβασης έχουν βελτιωθεί
 - Έχει αυξηθεί εντυπωσιακά η επεξεργαστική ισχύς που είναι διαθέσιμη για το «σπάσιμο» κωδικών πρόσβασης
 - Χρήση πολύπλοκων αλγορίθμων για την παραγωγή πιθανών κωδικών πρόσβασης
 - Μελέτη παραδειγμάτων και δομών που αφορούν πραγματικούς κωδικούς πρόσβασης οι οποίοι βρίσκονται σε χρήση



Εικόνα 3.3 Το ποσοστό των ανακτηθέντων κωδικών πρόσβασης μετά από δεδομένο αριθμό τυχαίων δοκιμών

Έλεγχος πρόσβασης στο αρχείο των κωδικών πρόσβασης

Η άρνηση πρόσβασης στους κρυπτογραφημένους κωδικούς μπορεί να εμποδίσει επιθέσεις εκτός σύνδεσης που αποσκοπούν στην τυχαία εύρεση



Ευπάθειες

Προσπελάσιμοι
μόνο από
προνομιακούς
χρήστες

Σκιώδες
αρχείο
κωδικών
πρόσβασης

Αδυναμίες
του λειτουργικού
συστήματος
που επιτρέπουν
την πρόσβαση
στο αρχείο

Ένα «ατύχημα»
κατά τον ορισμό
δικαιωμάτων
πρόσβασης
μπορεί
να επιτρέψει
την ανάγνωση
του αρχείου

Χρήστες
με τον ίδιο
κωδικό
πρόσβασης
και σε άλλα
συστήματα

Πρόσβαση
από μέσα
αποθήκευσης
αντιγράφων
ασφαλείας

Ανίχνευση
κωδικών
πρόσβασης
στην κυκλοφορία
δεδομένων
του δικτύου

Στρατηγικές επιλογής κωδικών πρόσβασης

Επιμόρφωση χρηστών

Μπορεί να καταστεί σαφής στους χρήστες η σπουδαιότητα της χρήσης «δύσκολων» κωδικών πρόσβασης και να δοθούν σε αυτούς κατευθυντήριες γραμμές για την επιλογή ισχυρών κωδικών πρόσβασης



Κωδικοί πρόσβασης που παράγονται από υπολογιστή

Οι χρήστες δεν μπορούν να τους απομνημονεύσουν εύκολα



Αντιδραστικός έλεγχος κωδικών πρόσβασης

Το σύστημα εκτελεί περιοδικά το δικό του πρόγραμμα-«σπάστη» για να εντοπίσει εύκολους κωδικούς πρόσβασης

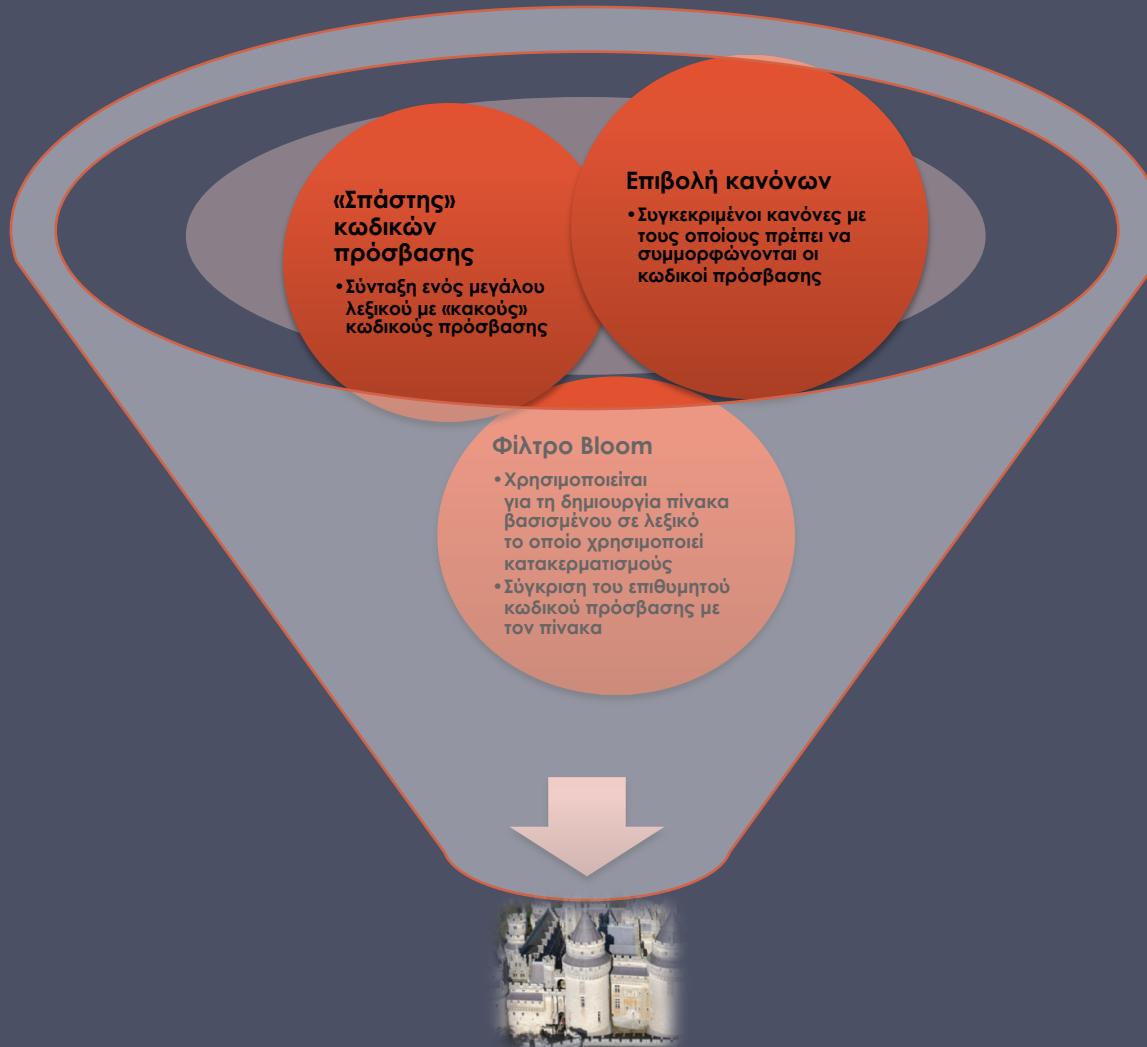


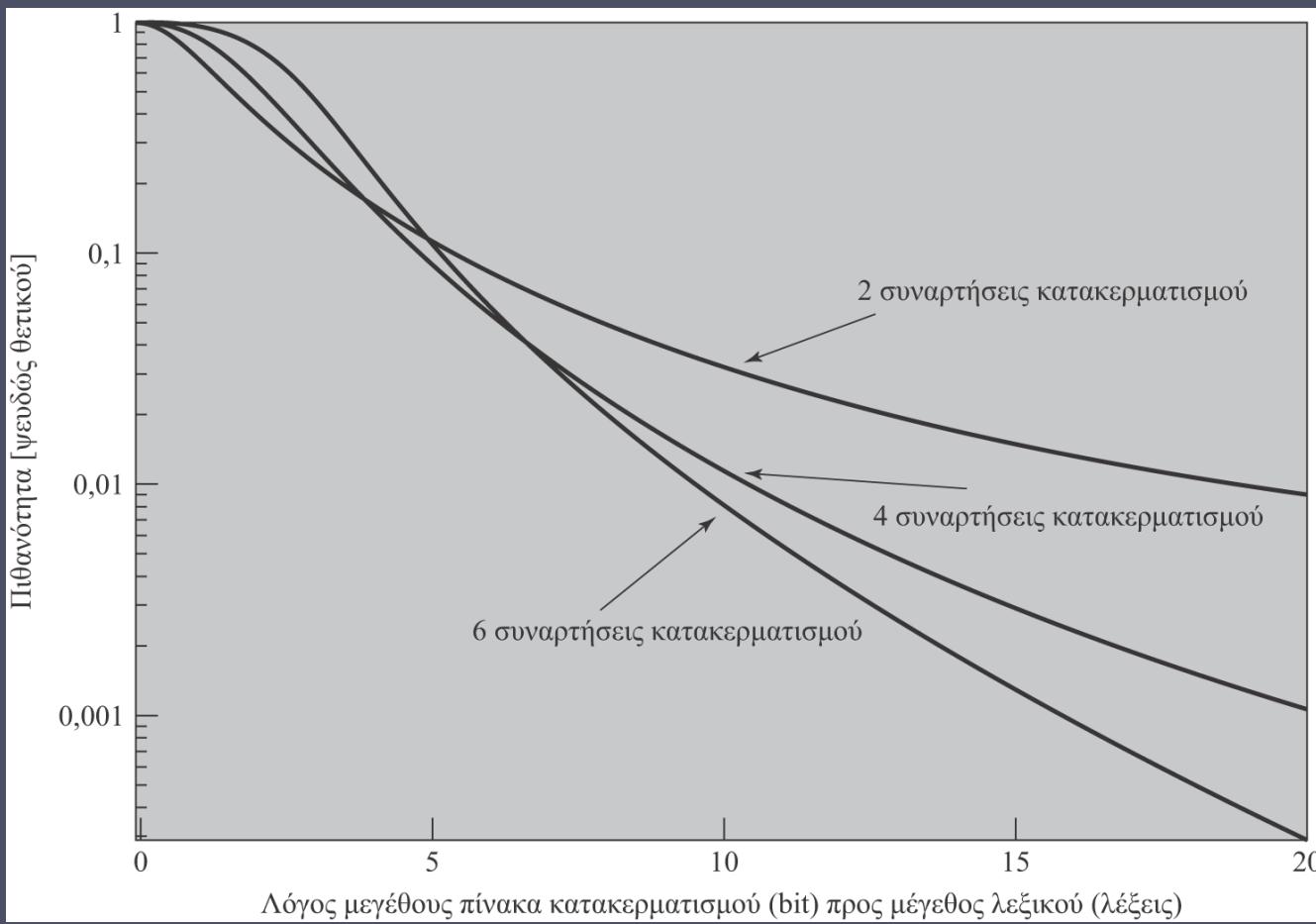
Πολιτική πολύπλοκων κωδικών πρόσβασης

Επιτρέπεται στον χρήστη να επιλέξει εκείνος τον κωδικό πρόσβασής του, όμως το σύστημα ελέγχει για να δει αν ο κωδικός πρόσβασης είναι αποδεκτός αν δεν είναι, τον απορρίπτει

Ο στόχος είναι να εξαλείψουμε επιλογές κωδικών πρόσβασης τους οποίους θα μπορούσε να μαντέψει κανείς, επιτρέποντας ταυτόχρονα στους χρήστες να επιλέξουν έναν κωδικό πρόσβασης που θα μπορούν να θυμούνται

Προληπτικός έλεγχος κωδικών πρόσβασης





Εικόνα 3.4 Απόδοση του φίλτρου Bloom

Πίνακας 3.2

Τύποι καρτών που χρησιμοποιούνται
ως τεκμήρια ασφαλείας

Τύπος κάρτας	Βασικό χαρακτηριστικό	Παράδειγμα
Ανάγλυφη	Ανάγλυφοι χαρακτήρες στην μπροστινή όψη	Παλιές πιστωτικές κάρτες
Μαγνητικής λωρίδας	Μαγνητική λωρίδα στην οπίσθια όψη, χαρακτήρες στην μπροστινή όψη	Τραπεζικές κάρτες
Μνήμης	Ηλεκτρονική μνήμη στο εσωτερικό	Προπληρωμένες τηλεκάρτες
«Εξυπνη» Επαφική Ανεπαφική	Ηλεκτρονική μνήμη και επεξεργαστής στο εσωτερικό Ηλεκτρικές επαφές εκτεθειμένες στην επιφάνεια Κεραία ραδιοκυμάτων ενσωματωμένη εσωτερικά	Βιομετρικά δελτία ταυτότητας

Κάρτες μνήμης

- Μπορούν να χρησιμοποιηθούν για αποθήκευση, αλλά όχι για επεξεργασία δεδομένων
- Πιο διαδεδομένες είναι οι κάρτες που φέρουν μια μαγνητική λωρίδα στην οπίσθια όψη τους
- Κάποιες διαθέτουν εσωτερική ηλεκτρονική μνήμη
- Χρησιμοποιούνται μόνο για σκοπούς φυσικής πρόσβασης
 - Δωμάτια ξενοδοχείων
 - Μηχανήματα ATM
- Παρέχουν σημαντικά μεγαλύτερη ασφάλεια όταν συνδυάζονται με κωδικό πρόσβασης ή PIN
- Πιθανά μειονεκτήματα:
 - Απαιτείται ειδική συσκευή ανάγνωσης
 - Απώλεια τεκμηρίων ασφαλείας
 - Δυσαρέσκεια χρηστών



«Έξυπνα τεκμήρια ασφαλείας»

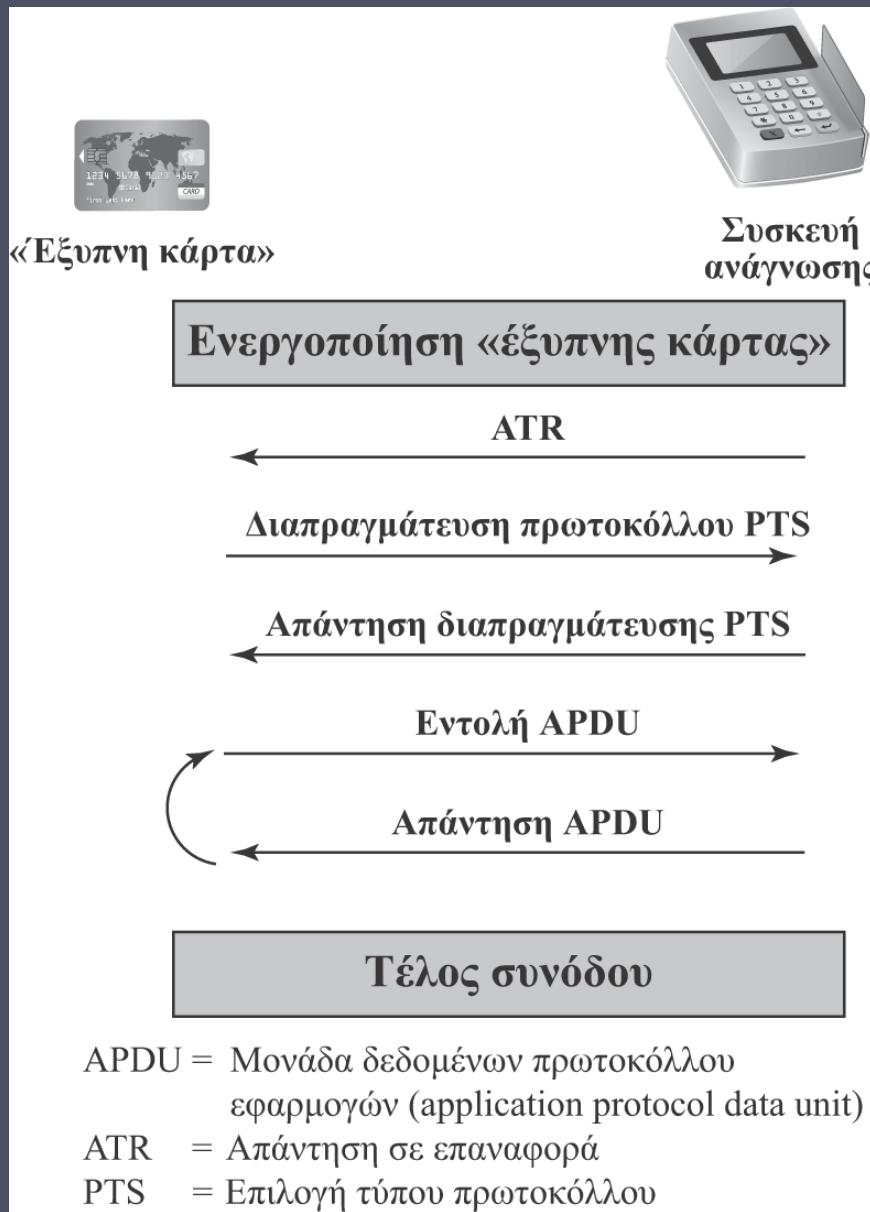
- Φυσικά χαρακτηριστικά:
 - Περιλαμβάνουν ενσωματωμένο μικροεπεξεργαστή
 - «Έξυπνο τεκμήριο ασφαλείας» το οποίο μοιάζει με τραπεζική κάρτα
 - Επίσης, μπορούν να μοιάζουν με αριθμομηχανές, κλειδιά, ή άλλα μικρά και φορητά αντικείμενα
- Διασύνδεση:
 - Οι μη αυτόματες διασυνδέσεις περιλαμβάνουν πληκτρολόγιο και οθόνη για αλληλεπίδραση
 - Οι ηλεκτρονικές διασυνδέσεις επικοινωνούν με μια συμβατή συσκευή ανάγνωσης/εγγραφής
- Πρωτόκολλο πιστοποίησης ταυτότητας:
 - Ταξινομούνται σε τρεις κατηγορίες:
 - Στατικό
 - Δυναμική γεννήτρια κωδικών πρόσβασης
 - Πρόκλησης-απάντησης



«Έξυπνες κάρτες»

- Η πιο σημαντική κατηγορία «έξυπνων τεκμηρίων ασφαλείας»
 - Μοιάζουν με πιστωτικές κάρτες
 - Διαθέτουν ηλεκτρονική διασύνδεση
 - Μπορούν να χρησιμοποιούν οποιοδήποτε από τα παραπάνω πρωτόκολλα
- Περιέχουν:
 - Ολόκληρο μικροεπεξεργαστή ο οποίος διαθέτει
 - Επεξεργαστή
 - Μνήμη
 - Θύρες εισόδου εξόδου (Input/Output, I/O)
- Συνήθως περιλαμβάνουν τρεις τύπους μνήμης:
 - Μνήμη μόνο για ανάγνωση (read-only memory, ROM)
 - Αποθηκεύονται δεδομένα τα οποία δεν αλλάζουν κατά τη διάρκεια ζωής της κάρτας
 - Ηλεκτρικά απαλείψιμη προγραμματίσιμη μνήμη μόνο για ανάγνωση (electrically erasable programmable ROM, EEPROM)
 - Περιέχει δεδομένα εφαρμογών και προγράμματα
 - Μνήμη τυχαίας προσπέλασης (random access memory, RAM)
 - Περιέχει προσωρινά δεδομένα που παράγονται κατά την εκτέλεση εφαρμογών





Εικόνα 3.5 Ανταλλαγή μεταξύ «έξυπνης κάρτας» και συσκευής ανάγνωσης

Ηλεκτρονικά δελτία ταυτότητας (eID)

Χρήση «έξυπνων καρτών» ως δελτίων ταυτότητας των πολιτών

Μπορεί να χρησιμοποιηθεί ακριβώς όπως οποιοδήποτε άλλο εθνικό δελτίο ταυτότητας, ή παρόμοια έγγραφα όπως το δίπλωμα οδήγησης, με σκοπό την πρόσβαση σε κρατικές και εμπορικές υπηρεσίες

Παρέχει πιο ισχυρή απόδειξη της ταυτότητας και μπορεί να αξιοποιηθεί σε μια ευρεία γκάμα εφαρμογών

Ουσιαστικά, η κάρτα eID είναι μια «έξυπνη κάρτα» της οποίας η εγκυρότητα και αυθεντικότητα έχουν επαληθευθεί από το κράτος

Η πιο προχωρημένη μορφή eID είναι το γερμανικό ηλεκτρονικό δελτίο ταυτότητας *neuer Personalausweis*

Διαθέτει τυπωμένα στην επιφάνειά της δεδομένα αναγνώσιμα από ανθρώπους

- Προσωπικά δεδομένα
- Αριθμός εγγράφου
- Αριθμός προσπέλασης κάρτας (card access number, CAN)
- Μηχανικώς αναγνώσιμη ζώνη (machine readable zone, MRZ)



Λειτουργία	Σκοπός	Κωδικός πρόσβασης PACE	Δεδομένα	Χρήσεις
ePass (υποχρεωτική)	Εξουσιοδοτημένα συστήματα επιθεώρησης χωρίς σύνδεση διαβάζουν τα δεδομένα	CAN ή MRZ	Εικόνα προσώπου· δύο εικόνες δακτυλικών αποτυπωμάτων (προαιρετικά)· δεδομένα MRZ	Η βιομετρική επαλήθευση ταυτότητας χωρίς σύνδεση έχει δεσμευθεί για κρατική πρόσβαση
eID (ενεργοποίηση προαιρετική)	Δικτυακές εφαρμογές διαβάζουν τα δεδομένα ή προσπελάζουν τις λειτουργίες ανάλογα με τις εξουσιοδοτήσεις	eID PIN	Ονοματεπώνυμο· ψευδώνυμο και επίπεδο σπουδών· ημερομηνία και τόπος γέννησης· διεύθυνση και αναγνωριστικό κοινότητας· ημερομηνία λήξης ισχύος	Ταυτοποίηση· επαλήθευση ηλικίας· επαλήθευση αναγνωριστικού κοινότητας· περιορισμένη ταυτοποίηση (ψευδώνυμο)· ερώτημα ανάκλησης
	Εξουσιοδοτημένα συστήματα επιθεώρησης χωρίς σύνδεση διαβάζουν τα δεδομένα και ενημερώνουν τη διεύθυνση και το αναγνωριστικό κοινότητας (community ID)	CAN ή MRZ		
eSign (πιστοποιητικό προαιρετικό)	Μια αρχή πιστοποίησης εγκαθιστά το πιστοποιητικό υπογραφής δικτυακά	eID PIN	Kλειδί υπογραφής· πιστοποιητικό X.509	Δημιουργία ηλεκτρονικής υπογραφής
	Οι πολίτες βάζουν ψηφιακή υπογραφή με το eSign PIN	CAN		

CAN = αριθμός προσπέλασης κάρτας

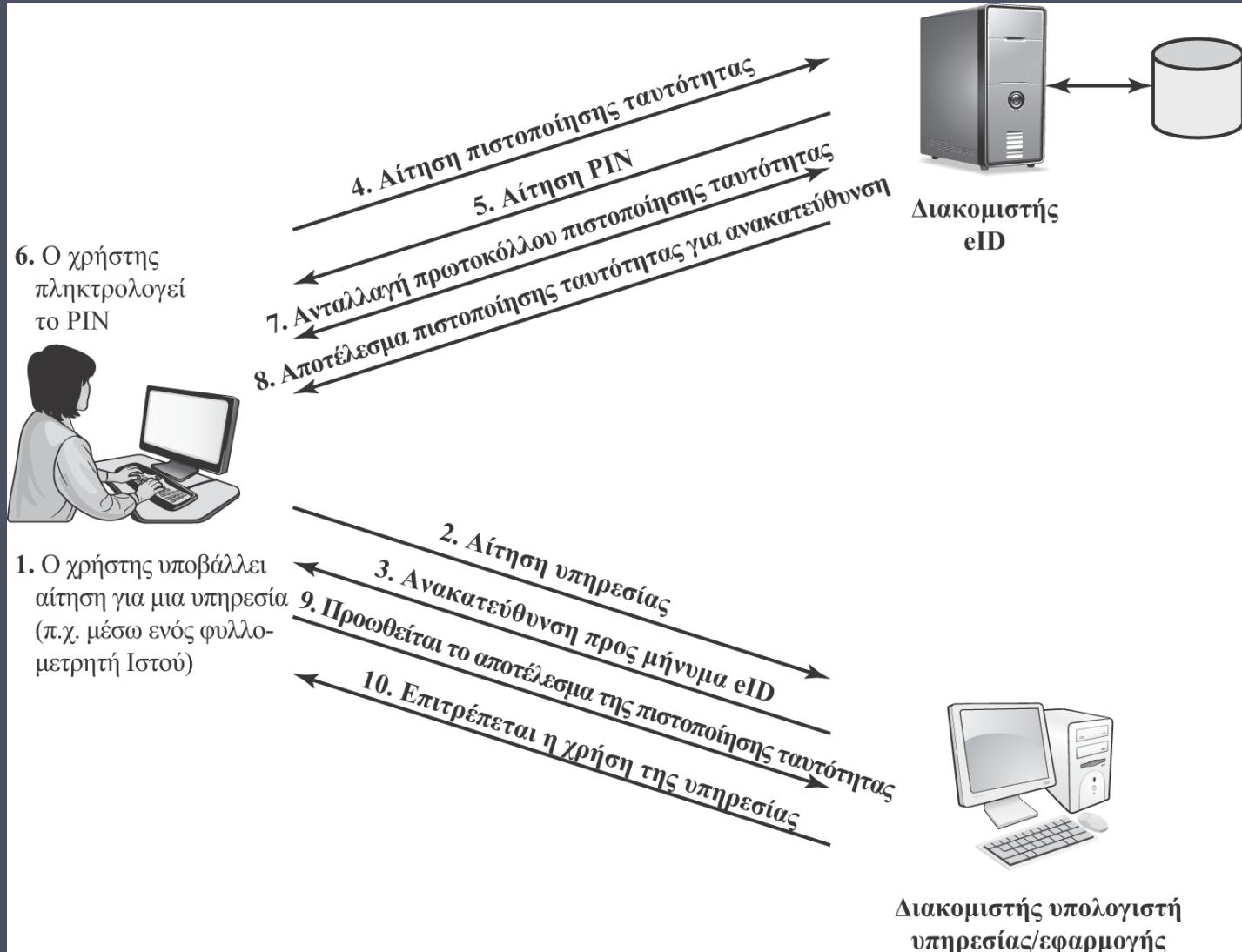
MRZ = μηχανικώς αναγνώσιμη ζώνη

PACE = πραγματοποίηση σύνδεσης με πιστοποίηση ταυτότητας μέσω κωδικού πρόσβασης

PIN = προσωπικός αριθμός αναγνώρισης

Πίνακας 3.3

Ηλεκτρονικές λειτουργίες και δεδομένα για κάρτες eID



Εικόνα 3.6 Πιστοποίηση ταυτότητας χρηστών με eID

Πραγματοποίηση σύνδεσης με πιστοποίηση ταυτότητας μέσω κωδικού πρόσβασης (PACE)

Εξασφαλίζει ότι
το ανεπαφικό τσιπ RF της
κάρτας eID δεν μπορεί να
διαβαστεί χωρίς οητό έλεγχο
πρόσβασης

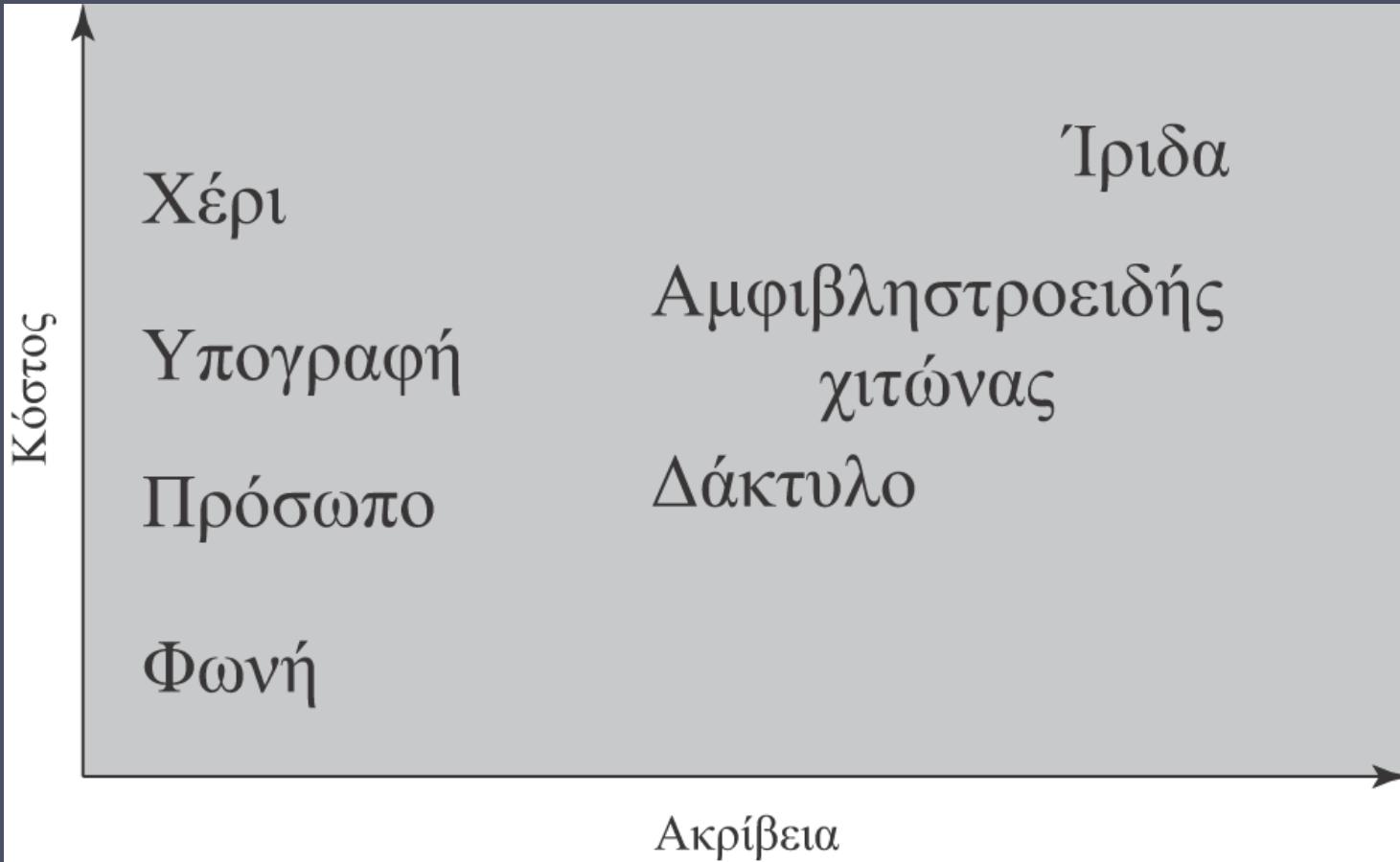
Για δικτυακές εφαρμογές, η
πρόσβαση στην κάρτα
επιτυγχάνεται όταν
ο χρήστης εισαγάγει
τον εξαψήφιο αριθμό PIN,
τον οποίο υποτίθεται ότι
πρέπει να γνωρίζει μόνο
ο κάτοχος της κάρτας

Για εφαρμογές χωρίς
σύνδεση, χρησιμοποιείται
είτε η ζώνη MRZ που είναι
τυπωμένη στην οπίσθια όψη
της κάρτας είτε ο εξαψήφιος
αριθμός προσπέλασης
κάρτας (CAN) που είναι
τυπωμένος στην μπροστινή
όψη

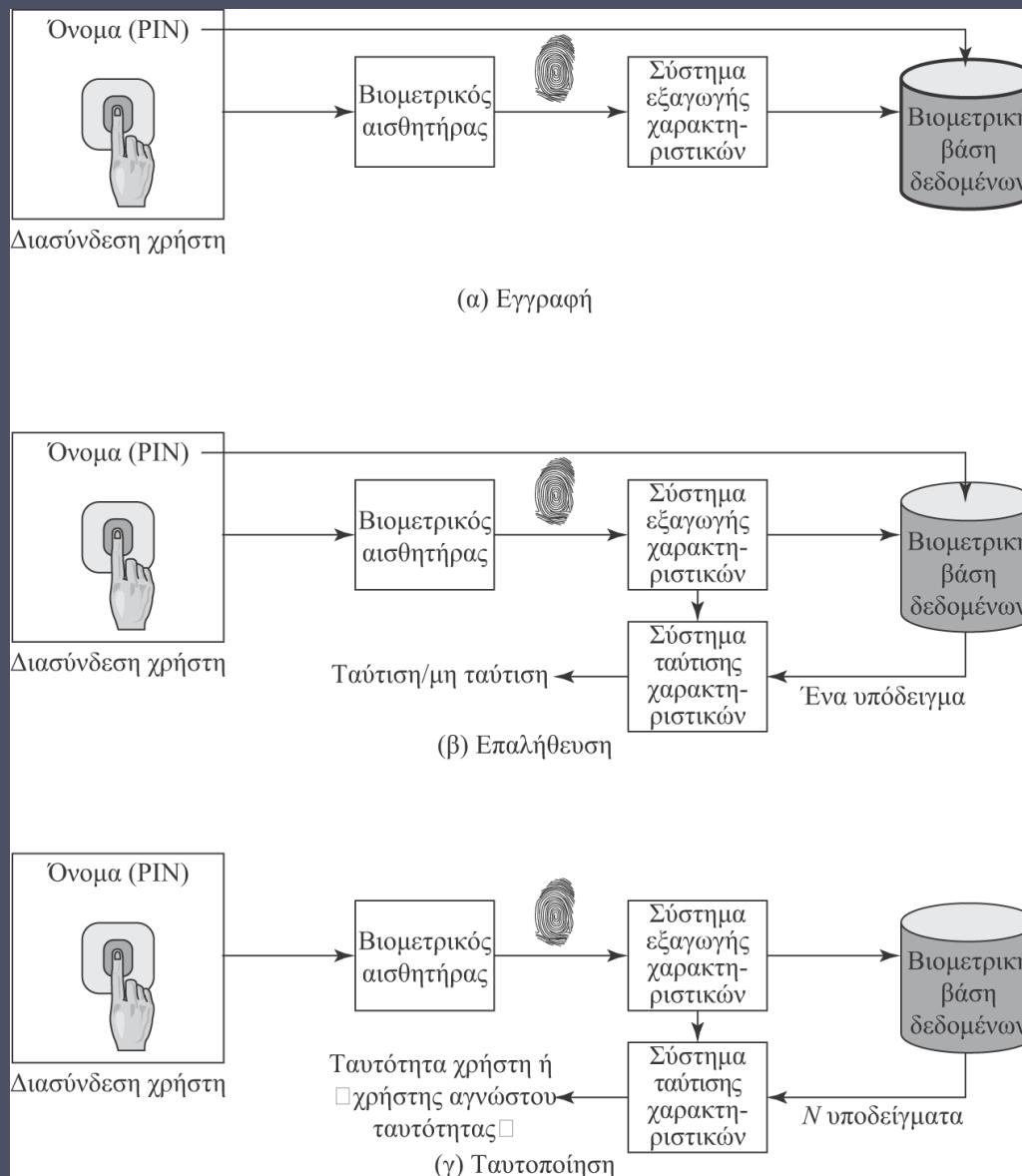
Βιομετρική πιστοποίηση ταυτότητας

- Προσπαθεί να πιστοποιήσει την ταυτότητα ενός ατόμου με βάση τα μοναδικά φυσικά χαρακτηριστικά του
- Βασίζεται στην αναγνώριση μορφών (pattern recognition), ή προτύπων.
- Σε σύγκριση με τους κωδικούς πρόσβασης και τα τεκμήρια ασφαλείας, είναι πιο περίπλοκη και πιο ακριβή από τεχνική άποψη
- Στα φυσικά χαρακτηριστικά περιλαμβάνονται:
 - Χαρακτηριστικά προσώπου
 - Δακτυλικά αποτυπώματα
 - Γεωμετρία χεριού
 - Μορφή αμφιβληστροειδούς χιτώνα
 - Ίριδα
 - Υπογραφή
 - Φωνητικό αποτύπωμα

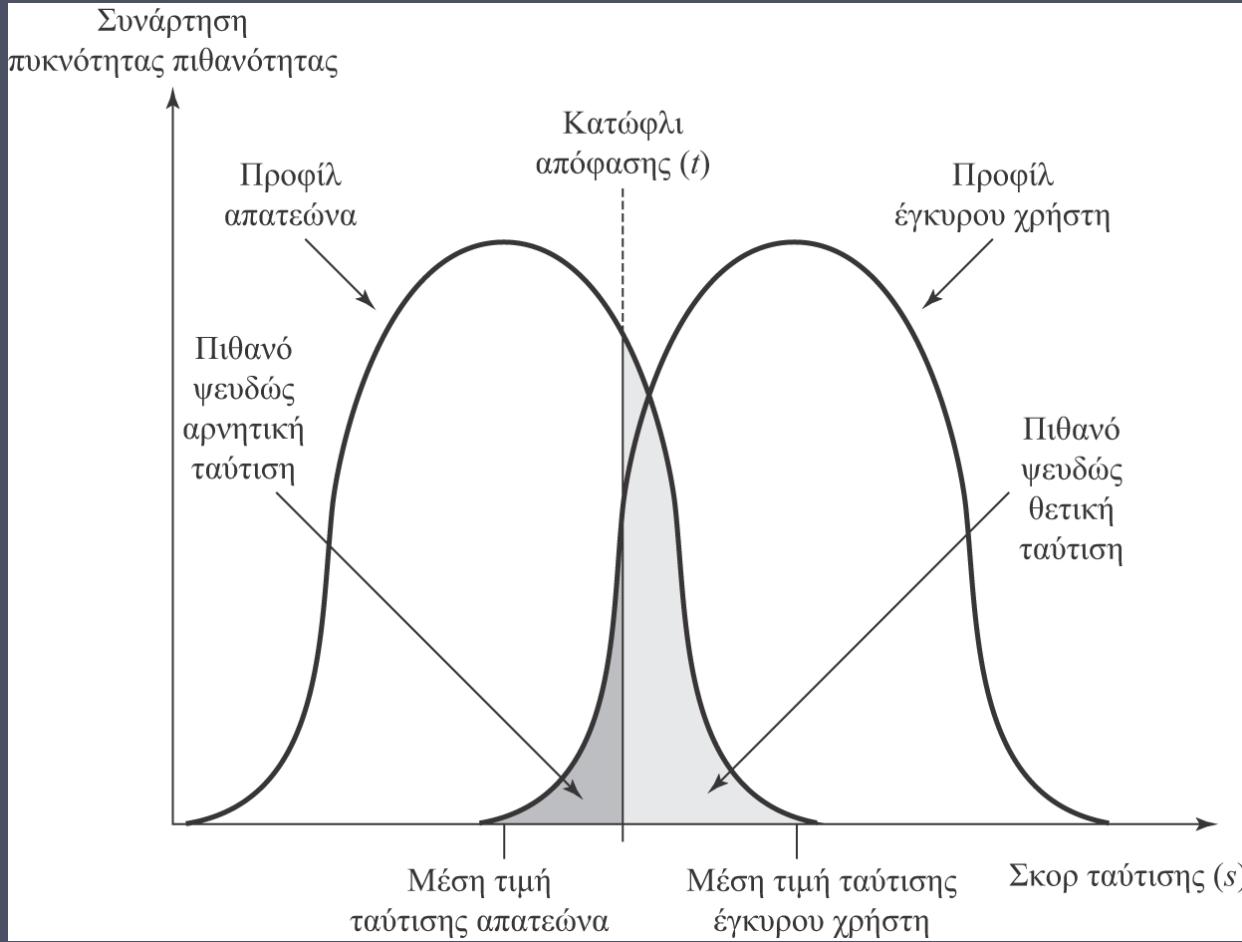




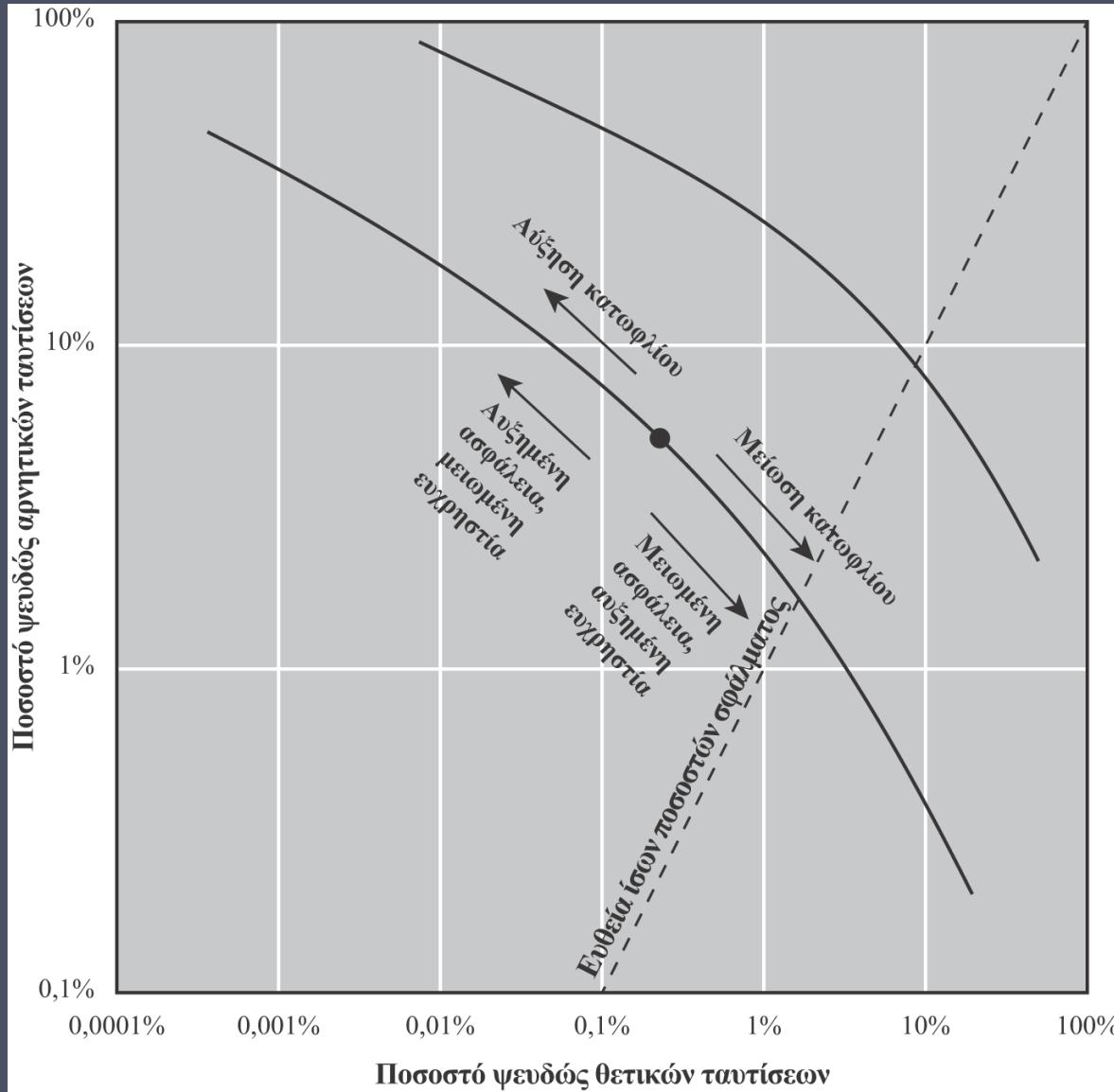
Εικόνα 3.7 Γράφημα κόστους-ακρίβειας διαφόρων βιομετρικών χαρακτηριστικών που χρησιμοποιούνται σε συστήματα πιστοποίησης ταυτότητας χρηστών



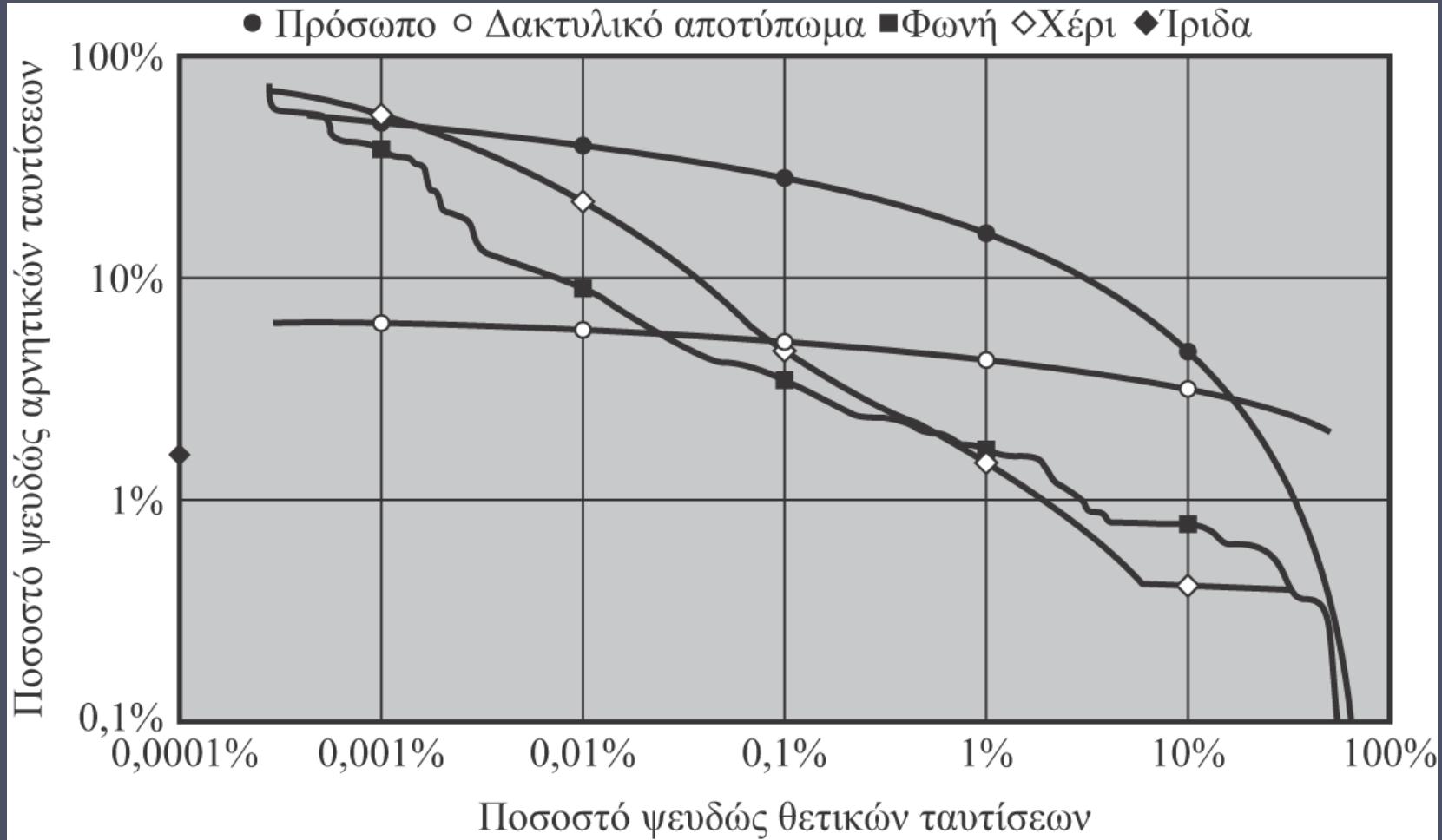
Εικόνα 3.8 Γενικό βιομετρικό σύστημα Η εγγραφή δημιουργεί μια συσχέτιση μεταξύ ενός χρήστη και των βιομετρικών χαρακτηριστικών του. Ανάλογα με την εφαρμογή, η πιστοποίηση ταυτότητας χρηστών περιλαμβάνει είτε την επαλήθευση ότι ο χρήστης είναι όντως αυτός που ισχυρίζεται ότι είναι είτε την ταυτοποίηση ενός άγνωστου χρήστη



Εικόνα 3.9 Προφίλ βιομετρικού χαρακτηριστικού ενός απατεώνα και ενός εξουσιοδοτημένου χρήστη Σε αυτή την εικόνα, η σύγκριση μεταξύ του υποβαλλόμενου χαρακτηριστικού και ενός χαρακτηριστικού αναφοράς ανάγεται σε μία μόνο αριθμητική τιμή. Αν η τιμή εισόδου (s) είναι μεγαλύτερη από ένα προκαθορισμένο κατώφλι (t), προκύπτει ταίριασμα



Εικόνα 3.10 Ιδανικές χαρακτηριστικές καμπύλες λειτουργίας βιομετρικών μετρήσεων (λογαριθμική κλίμακα και στους δύο άξονες)

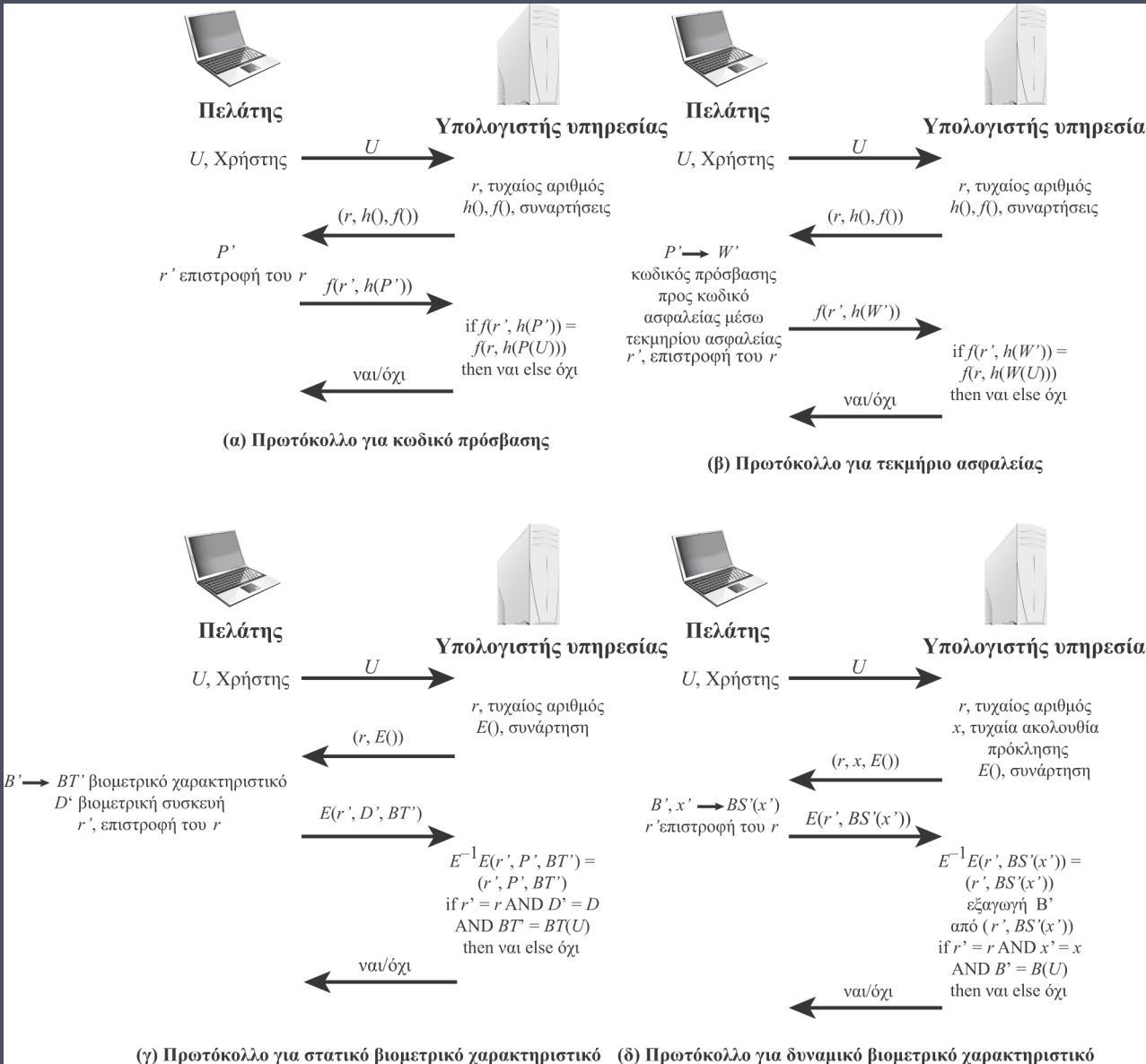


Εικόνα 3.11 Πραγματικές χαρακτηριστικές καμπύλες λειτουργίας βιομετρικών μετρήσεων από το [MANSO1] Προκειμένου να διακρίνονται οι διαφορές μεταξύ των συστημάτων, χρησιμοποιείται λογαριθμική κλίμακα και στους δύο άξονες

Απομακρυσμένη πιστοποίηση ταυτότητας χρηστών

- Η πιστοποίηση ταυτότητας μέσω ενός δικτύου, του Διαδικτύου, ή ενός συνδέσμου επικοινωνίας είναι πιο περίπλοκη
- Πρόσθετες απειλές για την ασφάλεια όπως:
 - Όταν ο αντίπαλος είναι σε θέση να υποκλέψει έναν κωδικό πρόσβασης ή να αναπαραγάγει μια ακολουθία (μηνυμάτων) πιστοποίησης ταυτότητας την οποία έχει παρατηρήσει
- Στηρίζεται γενικά σε κάποια μορφή πρωτοκόλλου πρόκλησης-απάντησης





Εικόνα 3.12 Βασικά πρωτόκολλα πρόκλησης-απάντησης για απομακρυσμένη πιστοποίηση ταυτότητας χρηστών

Υποκλοπή

Ο αντίπαλος προσπαθεί να μάθει τον κωδικό πρόσβασης με κάποια μορφή επίθεσης που χαρακτηρίζεται από τη φυσική εγγύτητα χρήστη και αντιπάλου

Άρνηση εξυπηρέτησης

Επιχειρεί να μπλοκάρει κάποια υπηρεσία πιστοποίησης ταυτότητας χρηστών κατακλύζοντάς την με πολυάριθμες αιτήσεις πιστοποίησης

Δούρειος ίππος

Μια εφαρμογή ή φυσική συσκευή «μεταμφιέζεται» σε γνήσια για να υποκλέψει τον κωδικό πρόσβασης, τον κωδικό ασφαλείας, ή τη βιομετρική παράμετρο ενός χρήστη

Επιθέσεις εναντίον υπολογιστών υπηρεσίας

Έχουν ως στόχο το αρχείο χρηστών στον υπολογιστή υπηρεσίας όπου βρίσκονται αποθηκευμένοι κωδικοί πρόσβασης, κωδικοί ασφαλείας τεκμηρίων, ή βιομετρικά υποδείγματα

Αναπαραγωγή

Ο αντίπαλος αναπαράγει μια απάντηση του χρήστη την οποία έχει υποκλέψει νωρίτερα

Επιθέσεις εναντίον πελατών

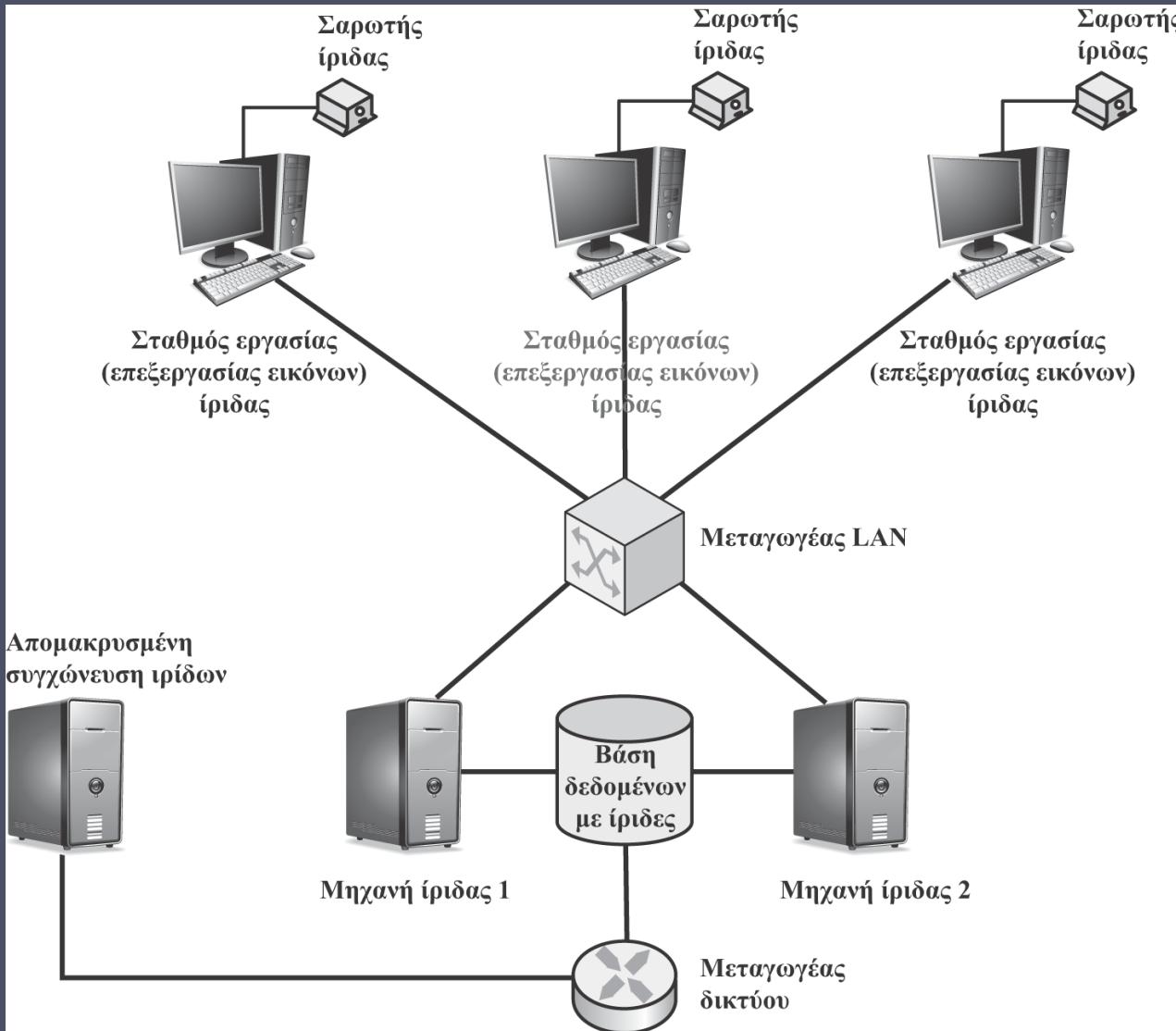
Ο αντίπαλος προσπαθεί να πιστοποιήσει την ταυτότητά του χωρίς πρόσβαση στον απομακρυσμένο υπολογιστή υπηρεσίας ή στην ενδιάμεση διαδρομή της επικοινωνίας

ΠΙΣΤΟΠΟΙΗΣΗ ΤΑΥΤΟΤΗΤΑΣ: ΖΗΤΗΜΑΤΑ ΑΣΦΑΛΕΙΑΣ

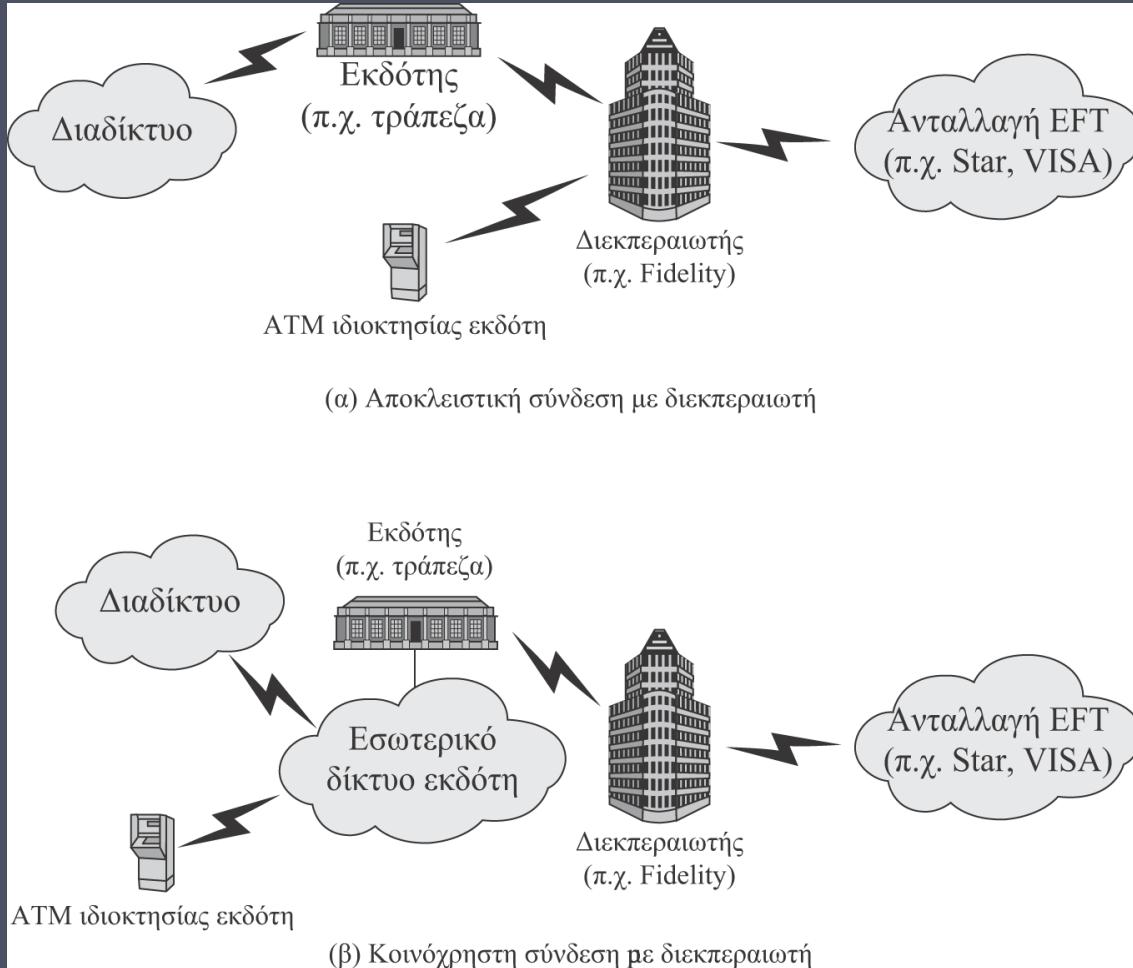
Πίνακας 3.4

Πιθανές επιθέσεις,
ευάλωτοι
πιστοποιητές,
και τυπικές άμυνες

Επιθέσεις	Πιστοποιητές	Παραδείγματα	Τυπικές άμυνες
Επίθεση εναντίον πελάτη	Κωδικός πρόσβασης	Τυχαία εύρεση, εξαντλητική αναζήτηση	Μεγάλη εντροπία· περιορισμένες απόπειρες
	Τεκμήριο ασφαλείας	Εξαντλητική αναζήτηση	Μεγάλη εντροπία· περιορισμένες απόπειρες· η κλοπή του αντικειμένου απαιτεί φυσική παρουσία
	Βιομετρικό χαρακτηριστικό	Ψευδώς θετική ταυτιση	Μεγάλη εντροπία· περιορισμένες απόπειρες
Επίθεση εναντίον υπολογιστή υπηρεσίας	Κωδικός πρόσβασης	Κλοπή απλού κειμένου, αναζήτηση με λεξικό/εξαντλητική αναζήτηση	Κατακερματισμός· μεγάλη εντροπία· προστασία της βάσης δεδομένων που περιέχει τους κωδικούς πρόσβασης
	Τεκμήριο ασφαλείας	Κλοπή κωδικού ασφαλείας	Τιδες όπως στην περίπτωση του κωδικού πρόσβασης· κωδικός ασφαλείας μίας χρήστης
	Βιομετρικό χαρακτηριστικό	Κλοπή υποδείγματος	Πιστοποίηση ταυτότητας συσκευής σύλληψης· πρόκληση-απάντηση
Υποκλοπή, κλοπή και αντιγραφή	Κωδικός πρόσβασης	«Παρακολούθηση πάνω από τον ώμο»	Μέριμνα από μέρους του χρήστη ώστε να παραμείνει μυστικός· μέριμνα από μέρους του διαχειριστή για την έγκαιρη κατάργηση παραβιασμένων κωδικών πρόσβασης· πολυπαραγοντική πιστοποίηση ταυτότητας
	Τεκμήριο ασφαλείας	Κλοπή, υλικό πλαστογράφησης	Πολυπαραγοντική πιστοποίηση ταυτότητας· τεκμήριο ασφαλείας ανθεκτικό σε παραβιάσεις ή στο οποίο γίνεται εμφανής οποιαδήποτε απόπειρα παραβίασης
	Βιομετρικό χαρακτηριστικό	Αντιγραφή (παραπλάνηση) βιομετρικού χαρακτηριστικού	Ανίχνευση αντιγραφής στη συσκευή σύλληψης και πιστοποίηση ταυτότητας συσκευής σύλληψης
Αναπαραγωγή	Κωδικός πρόσβασης	Αναπαραγωγή κλειμένης απάντησης με τον κωδικό πρόσβασης	Πρωτόκολλο πρόκλησης-απάντησης
	Τεκμήριο ασφαλείας	Αναπαραγωγή κλειμένης απάντησης με τον κωδικό ασφαλείας	Πρωτόκολλο πρόκλησης-απάντησης· κωδικός ασφαλείας μίας χρήστης
	Βιομετρικό χαρακτηριστικό	Αναπαραγωγή κλειμένης απάντησης με το βιομετρικό υπόδειγμα	Ανίχνευση αντιγραφής στη συσκευή καταγραφής και πιστοποίηση ταυτότητας συσκευής καταγραφής μέσω πρωτοκόλλου πρόκλησης-απάντησης
Δούρειος ίππος	Κωδικός πρόσβασης, τεκμήριο ασφαλείας, βιομετρικό χαρακτηριστικό	Εγκατάσταση «παράνομου» πελάτη ή συσκευής καταγραφής	Πιστοποίηση ταυτότητας πελάτη ή συσκευής καταγραφής εντός της έμπιστης περιμέτρου ασφαλείας
Άρνηση εξυπηρέτησης	Κωδικός πρόσβασης, τεκμήριο ασφαλείας, βιομετρικό χαρακτηριστικό	Κλείδωμα εξαιτίας πολλών αποτυχημένων προσπαθειών πιστοποίησης ταυτότητας	Πολυπαραγοντική με τεκμήριο ασφαλείας



Εικόνα 3.13 Γενική αρχιτεκτονική των τοποθεσιών σάρωσης ίριδας για το σύστημα των Ηνωμένων Αραβικών Εμιράτων



Εικόνα 3.14 Αρχιτεκτονικές ATM Οι περισσότεροι μικρομεσαίοι εκδότες χρεωστικών καρτών συνάπτουν συμβάσεις με διεκπεραιωτές οι οποίοι παρέχουν υπηρεσίες βασικής επεξεργασίας δεδομένων και ηλεκτρονικής μεταφοράς κεφαλαίων (EFT). Το μηχάνημα ATM της τράπεζας ενδέχεται να συνδέεται απευθείας με τον διεκπεραιωτή ή την τράπεζα

Περιπτωσιολογική
μελέτη:
Προβλήματα
ασφαλείας
των συστημάτων
ATM

Σύνοψη

- Αρχές ηλεκτρονικής πιστοποίησης ταυτότητας χρηστών
 - Ένα μοντέλο για την ηλεκτρονική πιστοποίηση ταυτότητας χρηστών
 - Τρόποι πιστοποίησης ταυτότητας
 - Εκτίμηση κινδύνου για την πιστοποίηση ταυτότητας χρηστών
- Πιστοποίηση ταυτότητας βασισμένη σε κωδικούς πρόσβασης
 - Ευπάθειες κωδικών πρόσβασης
 - Χρήση κατακερματισμένων κωδικών πρόσβασης
 - «Σπάσιμο» κωδικών πρόσβασης επιλεγμένων από τους χρήστες
 - Έλεγχος πρόσβασης στο αρχείο των κωδικών πρόσβασης
 - Στρατηγικές επιλογής κωδικών πρόσβασης
- Πιστοποίηση ταυτότητας βασισμένη σε τεκμήρια ασφαλείας
 - Κάρτες μνήμης
 - «Έξυπνες κάρτες»
 - Ηλεκτρονικά δελτία ταυτότητας
- Βιομετρική πιστοποίηση ταυτότητας
 - Φυσικά χαρακτηριστικά που χρησιμοποιούνται σε βιομετρικές εφαρμογές
 - Λειτουργία ενός βιομετρικού συστήματος πιστοποίησης ταυτότητας
 - Ακρίβεια βιομετρικών συστημάτων
- Απομακρυσμένη πιστοποίηση ταυτότητας χρηστών
 - Πρωτόκολλο κωδικών πρόσβασης
 - Πρωτόκολλο τεκμηρίων ασφαλείας
 - Στατικό βιομετρικό πρωτόκολλο
 - Δυναμικό βιομετρικό πρωτόκολλο
- Ζητήματα ασφαλείας της πιστοποίησης ταυτότητας χρηστών

