Ταυτοποίηση και Αυθεντικοποίηση

Ντίνα Καμπουράκη

Τμήμα Μηχανικών
Πληροφοριακών και Επικοινωνιακών Συστημάτων
Πανεπιστήμιο Αιγαίου

Πανεπιστήμιο Αιγαίου

Αντικείμενο μελέτης

- Ορισμός της ταυτοποίησης και αυθεντικοποίησης και θεμελιώδεις αρχές.
- Παρουσίαση τεχνικών εφαρμογής της ταυτοποίησης και αυθεντικοποίησης
  - Διαχείριση συνθηματικών
  - Ψηφιακά πιστοποιητικά
  - Έξυπνες κάρτες
  - Βιομετρικά Συστήματα

Ταυτοποίηση και αυθεντικοποίηση

Πανεπιστήμιο Αιγαίου

- Ταυτοποίηση (identification) ενός λογικού υποκειμένου καλείται η διαδικασία εκείνη, κατά την οποία το λογικό υποκείμενο παρέχει σε ένα ΠΣ τις πληροφορίες που απαιτούνται προκειμένου να συσχετιστεί με ένα από τα αντικείμενα που δικαιούνται προσπέλασης στους πόρους (resources) του.
- Αυθεντικοποίηση (authentication) ενός λογικού υποκειμένου, καλείται η διαδικασία εκείνη, κατά την οποία ένα λογικό υποκείμενο παρέχει σε ένα ΠΣ τις πληροφορίες που απαιτούνται προκειμένου να ελεγχθεί η βασιμότητα της συσχέτισης που επιτεύχθηκε κατά τη διαδικασία της ταυτοποίησης.

3

Τεχνικές εφαρμογής ελέγχων αυθεντικοποίησης

Πανεπιστήμιο Αιγαίου

- Τύπος I: Κάτι που το λογικό υποκείμενο γνωρίζει *(πχ. ένα συνθηματικό ή ένα PIN)*
- Τύπος II: Κάτι που το λογικό υποκείμενο κατέχει *(μαγνητική συσκευή αναγνώρισης πχ έξυπνη κάρτα ή ψηφιακό πιστοποιητικό)*
- Τύπος III: Κάτι που χαρακτηρίζει το λογικό υποκείμενο με βάση μονοσήμαντα βιομετρικά χαρακτηριστικά του *(συστήματα βιομετρικής τεχνολογίας, πχ. εφαρμογές δακτυλικών αποτυπωμάτων, αναγνώριση φωνής και ίριδας ματιού)*
- Τύπος IV: Κάτι που προσδιορίζει την τοποθεσία που βρίσκεται το λογικό υποκείμενο *(πχ διεύθυνση IP)*.

4

Παράδειγμα

Πανεπιστήμιο Αιγαίου

Σχήματα αυθεντικοποίησης προστατευόμενων πόρων

Προστατευόμενος πόρος	**Κάτι που γνωρίζεις**	**Κάτι που έχεις**	**Κάτι που είσαι**	**Γεωγραφική θέση**
Πλατφόρμα, Host	Όνομα χρήστη/ συνθηματικό	Ιδιωτικό κλειδί - Έξυπνη κάρτα	Βιομετρικό σύστημα (δακτυλικό αποτύπωμα, γεωμετρία χεριού, αναγνώριση προσώπου0	Αναγνωριστικό υπολογιστή ή IP διεύθυνση
Σύστημα Διαχείρισης Δικτύου (σύστημα αρχείων και εκτυπώσεων)	Όνομα χρήστη/ συνθηματικό	Ιδιωτικό κλειδί - Έξυπνη κάρτα - Ψηφιακό πιστοποιητικό	Βιομετρικό σύστημα (δακτυλικό αποτύπωμα, γεωμετρία χεριού, αναγνώριση προσώπου0	Έλεγχος χρονικής στιγμής ή θέση του Η/Υ από τον οποίο γίνεται η πρόσβαση
Υπηρεσία Δικτύου (Web, FTP, Telnet)	Όνομα χρήστη/ συνθηματικό	Ιδιωτικό κλειδί - Έξυπνη κάρτα		Διεύθυνση IP
Σύστημα Διαχείρισης Βάσεων Δεδομένων	Όνομα χρήστη/ συνθηματικό			Διεύθυνση IP

Πάτρας

5

Σύστημα Αυθεντικοποίησης

Πανεπιστήμιο Αιγαίου

Αποτελείται από :

- *Το σύνολο A που περιέχει τις πληροφορίες με βάση τις οποίες κάθε λογικό υποκείμενο αποδεικνύει την ταυτότητά του.*
- *Το σύνολο C που περιέχει τις συμπληρωματικές πληροφορίες που αποθηκεύει και χρησιμοποιεί το σύστημα ώστε να επικυρώνει πληροφορίες αυθεντικοποίησης.*
- *Το σύνολο F των συμπληρωματικών συναρτήσεων που δημιουργούν τις συμπληρωματικές πληροφορίες για την αυθεντικοποίηση. Δηλαδή, για $f \in F$, τότε $f: A \rightarrow C$.*
- *Το σύνολο L των συναρτήσεων αυθεντικοποίησης που αναγνωρίζουν ένα λογικό υποκείμενο. Δηλαδή, για $l \in L$, $l: A \times C \rightarrow \{true, false\}$.*
- *Το σύνολο S λοιπών συναρτήσεων επιλογής που δίνουν τη δυνατότητα σε ένα λογικό υποκείμενο να δημιουργήσει ή να τροποποιήσει τις πληροφορίες της αυθεντικοποίησης ή τις συμπληρωματικές πληροφορίες.*

6

Πλεονεκτήματα και μειονεκτήματα 1(2)

Πανεπιστήμιο Αιγαίου

- *Τύπος Ι: Κάτι που γνωρίζει*
- *Μειονεκτήματα:*

1. *Τα τεκμήρια αυθεντικοποίησης εύκολα μπορούν να αντιγραφούν*
2. *Συνήθως είναι εύκολο να τα μαντέψει κανείς, χωρίς ιδιαίτερες τεχνικές γνώσεις*
3. *Συνήθως μπορούν να αποκαλυφθούν με αυτοματοποιημένες μεθόδους (http://www.whatsmypass.com/the-top-500-worst-passwords-of-all-time)*

- *Πλεονεκτήματα:*

1. *Εύκολη υλοποίηση και εφαρμογή*
2. *Τροποποιούνται εύκολα*
3. *Δε χάνονται ή κλέβονται*
4. *Αν και είναι απλά στη χρήση τους, στην περίπτωση που είναι ένας μοναδικός συνδυασμός αριθμών και γραμμάτων, δεν αποκαλύπτονται εύκολα*

7

Πλεονεκτήματα και μειονεκτήματα 2(2)

Πανεπιστήμιο Αιγαίου

- *Τύπος ΙΙ: Κάτι που κατέχει*
- *Μειονεκτήματα:*

1. *Υψηλό κόστος*
2. *Μπορούν να χαθούν ή να κλαπούν*

Πλεονεκτήματα:

1. *Δεν αντιγράφονται εύκολα καθώς κατασκευάζονται από ειδικά υλικά τα οποία δεν είναι ευρέως διαθέσιμα*

- *Τύπος ΙΙΙ: Κάτι που το χαρακτηρίζει*
- *Μειονεκτήματα:*

1. *Δυσκολίες στην κατασκευή αξιόπιστων συσκευών αναγνώρισης με χαμηλό κόστος*
2. *Δεν είναι αλάνθαστα*

- *Πλεονεκτήματα:*

1. *Παρέχουν μεγαλύτερη ασφάλεια από τον Τύπο Ι και Τύπο ΙΙ.*

8

Πανεπιστήμιο Αιγαίου

Συνθηματικά

- Τύπος Ι.
- Συνθηματικό είναι η πληροφορία η οποία σχετίζεται με ένα λογικό υποκείμενο και η οποία επιβεβαιώνει την ταυτότητα του λογικού υποκειμένου

Πανεπιστήμιο Αιγαίου

Συνθηματικά Πλεονεκτήματα

- Απλή λειτουργία, περιορισμένη σχεδιαστική πολυπλοκότητα
- Χαμηλό κόστος (δεν απαιτεί πρόσθετο εξοπλισμό υλοποίησης ή εξειδικευμένες γνώσεις ή επιπλέον εκπαίδευση των χρηστών του ΠΣ)
- Παροχή ικανοποιητικού βαθμού προστασίας.

Συνθηματικά Μειονεκτήματα

Πανεπιστήμιο Αιγαίου

- Πιθανότητα τυχαίας αποκάλυψης του συνθηματικού
- Πιθανότητα αποκάλυψης συνθηματικού με συστηματικό τρόπο
- Πιθανότητα αποκάλυψης του συνθηματικού κατά τη διάρκεια της μετάδοσής του (*ειδικά σε κατανεμημένα περιβάλλοντα)*

Πανεπιστήμιο Αιγαίου

Κριτήρια Επιλογής Συνθηματικών

- Μήκος Συνθηματικού: *ορίζεται ελάχιστο μήκος για τα συνθηματικά*
- Μορφότυπο Συνθηματικού: *συνδυασμός γραμμάτων, αριθμών και ειδικών χαρακτήρων.*
- Αποφυγή εύκολων συνθηματικών: εκπαίδευση των χρηστών
- Οδηγίες φύλαξης: να φυλάσσονται σε ασφαλές μέρος.
- Αλλαγή συνθηματικών: να εφαρμόζεται αυτόματος έλεγχος αλλαγής των συνθηματικών από τους χρήστες

Πανεπιστήμιο Αιγαίου

Ψηφιακά Πιστοποιητικά

Τύπος ΙΙ.

- Τα ψηφιακά πιστοποιητικά έχουν τη μορφή δυαδικών αρχείων και η λειτουργία τους στηρίζεται στην Κρυπτογραφία Δημόσιου Κλειδιού.
- Μπορούν να χρησιμοποιηθούν για τον περιορισμό της αποκάλυψης της ταυτότητας του χρήστη, ενσωματώνοντας ψευδώνυμα αντί της πραγματικής ταυτότητάς τους.

13

Πανεπιστήμιο Αιγαίου

Πρότυπα Ψηφιακών Πιστοποιητικών 1(2)

- PKIX (Internet PKI based on X.509)
- SPKI (Simple Public Key Infrastructure)
- PGP (Pretty Good Privacy)

14

Πανεπιστήμιο Αιγαίου

Πρότυπα Ψηφιακών Πιστοποιητικών 2(2)

Τύπος πιστοποιητικού	Χαρακτηριστικά εμπιστοσύνης και πιστοποίησης	Πεδίο αναγνώρισης πιστοποιητικού
PKIX (X.509)	Ιεραρχική εμπιστοσύνη, Ονοματοδοσία οικουμενικής εμβέλειας,Δια-πιστοποίηση, Πολιτικές και δηλώσεις πρακτικών	*Οικουμενικά μοναδικό (X.500):* Διακριτικό όνομα επιλεγμένο από τον πάροχο
SPKI	Αυτόνομη αρχή πιστοποίησης, Ονόματα τοπικής εμβέλειας, Δεν απαιτούνται δηλώσεις πρακτικών	*Τοπικό και αυθαίρετο:* Δημόσιο κλειδί
PGP	Πλέγμα εμπιστοσύνης, Πολλαπλές εναλλακτικές διαδρομές πιστοποίησης, Υπογραφή πιστοποιητικού από οποιονδήποτε, Δεν επιβάλλεται πολιτική	*Οικουμενικά μοναδικό αλλά μη σταθερό:* Διεύθυνση e-mail

15

Πανεπιστήμιο Αιγαίου

Έξυπνες Κάρτες

- Τύπος ΙΙ.
- Διαθέτουν Μικροεπεξεργαστή
- Υψηλό επίπεδο ασφάλειας για τα δεδομένα που αποθηκεύουν και επεξεργάζονται
- Εφαρμογές: Ηλεκτρονικό πορτοφόλι, Κάρτα Ασθενούς, Κινητά τηλέφωνα, Έλεγχος λογικής πρόσβασης σε δίκτυα, Έλεγχος φυσικής πρόσβασης σε εγκαταστάσεις κλπ.

16

Έξυπνες Κάρτες - Τμήματα

Πανεπιστήμιο Αιγαίου

- Η μνήμη εργασίας (working memory – Random Access Memory)
- Η μη διαγράψιμη μνήμη ROM (Read Only Memory)
- Η μνήμη εφαρμογών (EEPROM)
  - **Μυστική Περιοχή** (Secret Area)
  - **Περιοχή Ιστορικού Πρόσβασης** (Access Area)
  - **Περιοχή Ελεύθερης Πρόσβασης** (Public Area)
  - **Περιοχή Εργασίας** (Work Area)

17

Έξυπνες Κάρτες

Πανεπιστήμιο Αιγαίου

ΤΑΥΤΟΠΟΙΗΣΗ

- Η ταυτοποίηση του κατόχου της έξυπνης κάρτας γίνεται μέσω του μυστικού προσωπικού κωδικού του (PIN).
- Ο κωδικός συγκρίνεται με τον αντίστοιχο κωδικό που είναι αποθηκευμένος στη μυστική περιοχή της μνήμης της έξυπνης κάρτας.
- Η διαδικασία σύγκρισης εκτελείται εσωτερικά στην έξυπνη κάρτα

18

Πανεπιστήμιο Αιγαίου

Έξυπνες Κάρτες

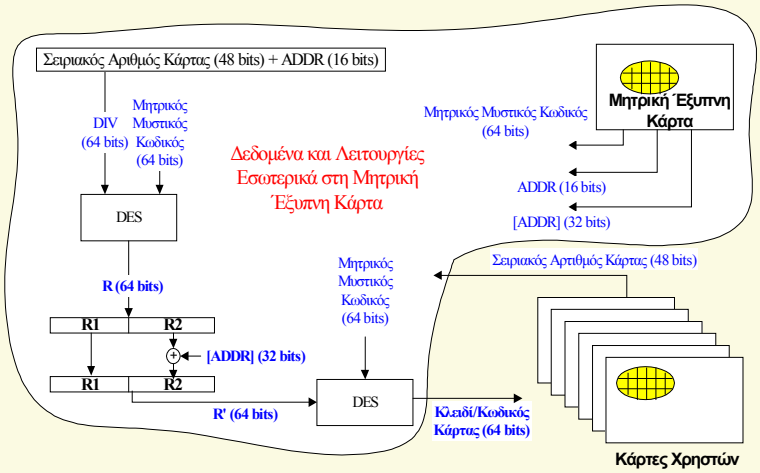
ΑΥΘΕΝΤΙΚΟΠΟΙΗΣΗ

- Στόχος: Διασφάλιση γνησιότητας της έξυπνης κάρτας (*δηλ. έκδοση από εξουσιοδοτημένο φορέα*)
- Η αυθεντικοποίηση μπορεί να γίνει με:
  - χρήση ψηφιακών πιστοποιητικών και ασύμμετρων κρυπτογραφικών αλγορίθμων που προαναφέρθηκαν
  - αξιοποιώντας συμμετρικούς αλγόριθμους κρυπτογράφησης (για παράδειγμα DES).

19

Πανεπιστήμιο Αιγαίου

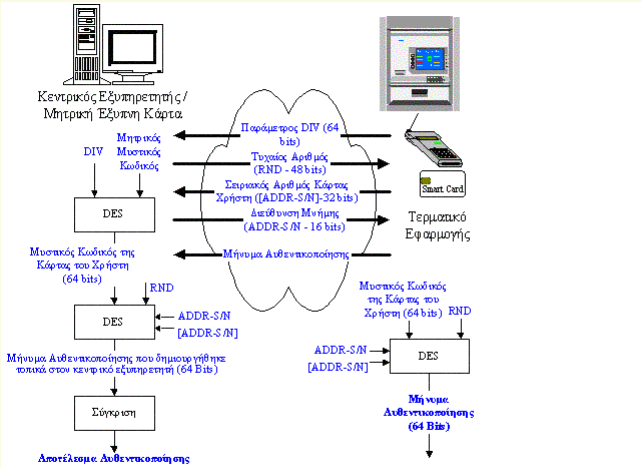
Διαδικασία Πιστοποίησης Έξυπνων Καρτών



20

Πανεπιστήμιο Αιγαίου

Διαδικασία Αυθεντικοποίησης



Πανεπιστήμιο Αιγαίου

Συστήματα Αυθεντικοποίησης

- KERBEROS 1(2)
  - Κατασκευάστηκε στο MIT για να προστατεύσει τις υπηρεσίες δικτύου που αναπτύσσονταν στα πλαίσια του προγράμματος Athena.
  - Οργανωμένο σε πεδία (realms). Σε κάθε πεδίο υπάρχει ένας κεντρικός και φυσικά ασφαλής *εξυπηρέτης αυθεντικοποίησης* (Authentication Server – AS), που έχει κοινό με κάθε συμμετέχοντα P ένα μυστικό κλειδί Kp. Αν ο P είναι χρήστης, τότε το Kp παράγεται από το συνθηματικό του, χρησιμοποιώντας μονόδρομη συνάρτηση σύνοψης.
  - Το σύστημα λειτουργεί παρέχοντας στους συμμετέχοντες εισιτήρια (tickets), τα οποία μπορούν να χρησιμοποιήσουν για να αποδείξουν την ταυτότητά τους και μυστικά κλειδιά για ασφαλείς επικοινωνίες μεταξύ των συμμετεχόντων.

Πανεπιστήμιο Αιγαίου

Συστήματα Αυθεντικοποίησης

- KERBEROS 2(2)
  - Βασίζεται σε πρωτόκολλα διανομής κλειδιών .
  - Αργότερα τροποποιήθηκαν για να περιλάβουν και χρονοσφραγίδες.

Το πρωτόκολλο μπορεί να συνοψισθεί ως εξής:

1: C	→	AS	: U,TGS
2: AS	→	C	: Tc,tgs, {TGS, K, tstart, texpire}Ku
3: C	→	TGS	: S, Tc,tgs, Ac,tgs
4: TGS	→	C	: Tc,s, {S, K΄, t΄start, t΄expire}K
5: C	→	S	: Tc,s, Ac,s
6: S	→	C	: {t΄}K΄

  - Το πρωτόκολλο περιλαμβάνει τρεις ανταλλαγές: Μια ανταλλαγή μεταξύ του C και του AS στα βήματα 1 και 2, μια ανταλλαγή μεταξύ του C και του TGS στα βήματα 3 και 4 και μια ανταλλαγή μεταξύ του C και ενός S στα βήματα 5 και 6.

23

Πανεπιστήμιο Αιγαίου

Συστήματα Αυθεντικοποίησης

- SESAME
  - Ευρωπαϊκό Σύστημα Ασφάλειας για εφαρμογές που λειτουργούν σε ανομοιογενή υπολογιστικά περιβάλλοντα.
  - Προσφέρει βασικές λειτουργίες ασφάλειας με τις οποίες οι κατασκευαστές υλοποιούν τα τελικά προϊόντα πληροφορικής.
  - Παρουσιάζει ομοιότητες με το σύστημα αυθεντικοποίησης KERBEROS.
  - Αρχιτεκτονική Δομή:
    - *Εξυπηρετητής Αυθεντικοποίησης (Authentication Server - AS)*
    - *Εξυπηρετητής εκχώρησης δικαιωμάτων (Privilege Attribute Server - PAC)*
    - *Εξυπηρετητής διανομής κλειδιών (Key Distribution Server - KDS)*

24

Πανεπιστήμιο Αιγαίου

Βιομετρικά Συστήματα 1(5)

- Τύπος ΙΙΙ.
- Η διαδικασία ταυτοποίησης με εφαρμογή συστημάτων βιομετρικής τεχνολογίας, βασίζεται σε φυσικά χαρακτηριστικά του ανθρώπινου σώματος ως αποδεικτικά στοιχεία για την αναγνωρισιμότητα του λογικού υποκειμένου από ένα ΠΣ.
- Κύρια τεκμήρια συνήθως είναι:
  - Δακτυλικά αποτυπώματα
  - Ίριδα ματιού
  - Χροιά φωνής
  - Γεωμετρία χεριού
  - DNA.
- Δυνατότητα περιορισμού της αποκάλυψης της ταυτότητας του χρήστη με ενσωμάτωση ψευδωνύμων αντί της πραγματικής ταυτότητάς τους.

25

Πανεπιστήμιο Αιγαίου

Βιομετρικά Συστήματα 2(5)

- Κατηγορίες
- τεχνική μέτρησης ανθρώπινων *φυσικών χαρακτηριστικών*
- τεχνική μέτρησης της *συμπεριφοράς*.

- Βασικές Έννοιες
- *ανοχή σε σφάλματα*
- *μέθοδος αποθήκευσης των προτύπων ανάλυσης*.

26

Πανεπιστήμιο Αιγαίου

Βιομετρικά Συστήματα 3(5)

- Χαρακτηριστικά
  - Ακρίβεια
  - Ταχύτητα
  - Αξιοπιστία
  - Αποθήκευση δεδομένων και Απαιτήσεις επεξεργασίας
  - Διαδικασία Καταχώρισης
  - Μοναδικότητα
  - Παραποίηση στοιχείων
  - Αποδοχή του χρήστη

Πανεπιστήμιο Αιγαίου

Βιομετρικά Συστήματα 4(5)

- **Πλεονεκτήματα**
- Δεν απαιτούν χρήση κλειδιού, κάρτας ή άλλης συσκευής από το χρήστη
- Δεν απαιτούν την απομνημόνευση Συνθηματικού πρόσβασης
- Δεν απαιτούν τη διαχείριση σχετικά με την τροποποίηση στοιχείων συνθηματικών για την πρόσβαση κλπ
- Η πιθανότητα ορθής αναγνώρισης βασίζεται σε μοναδικά χαρακτηριστικά
- Τα κριτήρια είναι μόνιμα και δεν απαιτούν ανανέωση (εξαίρεση αποτελεί η αναγνώριση φωνής, η σύγκριση υπογραφής και η αναγνώριση πληκτρολόγησης, που απαιτούν ανανέωση με το γήρας του χρήστη)
- **Μειονεκτήματα Παλαιότερων Βιομετρικών Συστημάτων**
- Υψηλό κόστος
- Αργοί χρόνοι απόκρισης
- Απαιτήσεις για μεγάλες βάσεις δεδομένων
- Υψηλό ποσοστό απόρριψης, απαίτηση για εφαρμογή τεχνικών λήψης αντιγράφων ασφαλείας για την αυθεντικοποίηση με έμμεσο αποτέλεσμα τη δυσαρέσκεια του χρήστη
- Υψηλές απαιτήσεις συντήρησης
- Μακροσκελείς διαδικασίες καταχώρισης
- Η κοινωνική αντίληψη ότι η λήψη δακτυλικών αποτυπωμάτων συνδυάζεται με εγκληματική δραστηριότητα
- Η κοινωνική αντίληψη ότι η χρήση ακτινοβολίας βλάπτει την υγεία
- Η αντίσταση των χρηστών

Πανεπιστήμιο Αιγαίου

Βιομετρικά Συστήματα 5(5)

- **Εφαρμογές**
- Έλεγχος πρόσβασης σε κρίσιμες εγκαταστάσεις
- Ευρεία διείσδυση σε τομείς όπως κυβερνητικές υπηρεσίες, αστυνομικές υπηρεσίες, εμπορικούς οργανισμούς κλπ.
- Ισπανία: εθνικό σύστημα δακτυλοσκόπησης για τα προνόμια των ανέργων και το σύστημα υγείας
- Ρωσία: μελλοντικά σχέδια για την εγκατάσταση ενός παρόμοιου εθνικού συστήματος στις τράπεζες.
- Τζαμάικα: Οι πολίτες είναι υποχρεωμένοι να ακουμπούν τον αντίχειρά τους σε οθόνες όποτε συμμετέχουν ως ψηφοφόροι στις εκλογές.
- Γαλλία και Γερμανία: ελέγχεται σε πειραματική φάση ειδικός εξοπλισμός ο οποίος θα εισάγει την ψηφιακή απεικόνιση του δακτυλικού αποτυπώματος στην πιστωτική κάρτα.
- Η πιο αμφιλεγόμενη μορφή εφαρμογής των βιομετρικών συστημάτων, είναι η αναγνώριση του DNA. Αστυνομικές υπηρεσίες σε διάφορες χώρες όπως στον Καναδά, τη Γερμανία και τις ΗΠΑ, έχουν δημιουργήσει τεράστιες βάσεις δεδομένων με δείγματα DNA από ανθρώπους που έχουν διαπράξει αξιόποινες πράξεις.

29

Πανεπιστήμιο Αιγαίου

Συμπεράσματα

- Η διαδικασία της ταυτοποίησης και αυθεντικοποίησης αποτελούν μέρος της ασφάλειας των υπολογιστικών και πληροφοριακών συστημάτων.
- Η αναγνώριση και η επαλήθευση της ταυτότητας ενός λογικού υποκειμένου που αιτείται προσπέλασης σε ένα αυτοματοποιημένο Πληροφοριακό Σύστημα αποτελεί το βασικό στοιχείο της διαδικασίας ελέγχου της προσπέλασης.

30