Πανεπιστήμιο Πελοποννήσου
Τμήμα Επιστήμης και Τεχνολογίας Τηλεπικοινωνιών

Διαχείριση και Ασφάλεια Δικτύων

Ιδιωτικότητα

Ο μύθος…

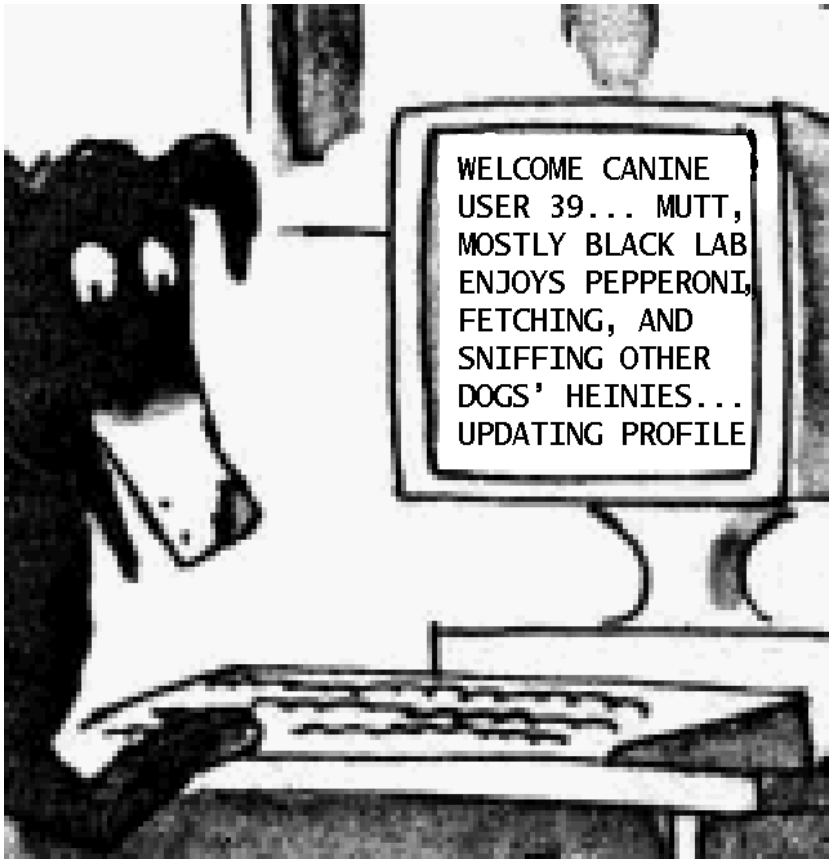
"On the Internet, nobody knows you're a dog."

"On the Internet, nobody knows you are a dog"

Pat Steiner

The New Yorker, Ιούλιος 1993

Η πραγματικότητα!



"You have zero privacy anyway, get over it"

Scott McNealy

Ιανουάριος 1999

Ιδιωτικότητα

«Η αξίωση των ατόμων, ομάδων και οργανισμών να καθορίζουν το χρόνο, τον τρόπο και την έκταση αναφορικά με τη συλλογή και επεξεργασία των προσωπικών τους δεδομένων»

Alan Westin, 1967

(Columbia University)

Ο σύγχρονος κόσμος

- Διαδικτυακές υπηρεσίες
  - Διαδραστικές, προσωποποιημένες υπηρεσίες
  - Web 2.0
  - Υπηρεσίες ηλεκτρονικού εμπορίου, ηλεκτρονικής διακυβέρνησης, …. ….
  - Υπηρεσίες κοινωνικής δικτύωσης
- Κινητές υπηρεσίες
  - Βασισμένες στη θέση του χρήστη
  - Υπηρεσίες με επίγνωση του πλαισίου χρήσης τους
  - m-payment, m-banking, m-commerce, …
- «Πανταχού παρούσα υπολογιστική» – «περιβάλλουσα ευφυΐα»
  - Αισθητήρες
  - Έξυπνες κάμερες
  - RFIDs

Ο σύγχρονος κόσμος

- Πολύπλοκες ροές εκτέλεσης υπηρεσιών
  - Πολλοί πάροχοι στην αλυσίδα παροχής
  - Εφαρμογές υλοποιημένες με τη λογική των Υπηρεσιών Ιστού (Web Services)
  - Πολύπλοκα κατανεμημένα συστήματα
  - Υπολογιστική "σύννεφου" (cloud computing)
  - Ομοσπονδιακές ταυτότητες (federated identities), single-sign-on, …
- Ολοκλήρωση συστημάτων υπηρεσιών και παροχή "παραδοσιακών" υπηρεσιών πάνω από δίκτυα IP
  - Triple-play, quad-play
  - IP telephony, IPTV
- Διασύνδεση των πάντων
  - Smart grid
- Μεγάλες εταιρείες των οποίων τα κέρδη πηγάζουν από την εμπορική εκμετάλλευση προσωπικών δεδομένων
  - google
  - facebook

Ιδιωτικότητα και σύγχρονες τεχνολογίες

- 1890: Δύο νομικοί από τη Βοστόνη επισημαίνουν για πρώτη φορά τον κίνδυνο της ιδιωτικής ζωής από την πρόοδο της τεχνολογίας

  Το επίμαχο τεχνολογικό επίτευγμα της εποχής ήταν η φωτογραφία
- Σήμερα, οι οργανισμοί συλλέγουν και επεξεργάζονται τεράστιες ποσότητες προσωπικών δεδομένων και εξάγουν με ευκολία συμπεράσματα:
  - Προσωπικά στοιχεία
  - Καταναλωτικές συνήθειες
  - Ιατρικά δεδομένα
  - Πολιτισμικές και κοινωνικές συνήθειες και απόψεις
  - Δεδομένα θέσης και κίνησης
  - Δεδομένα επικοινωνίας
  - Εικόνες και βίντεο
  - …

- Ραγδαία αύξηση της κλίμακας συλλογής δεδομένων
- Διαφορετικοί τρόποι συλλογής δεδομένων
- Συλλογή νέων τύπων προσωπικών δεδομένων
- Ευκολία πρόσβασης στα δεδομένα
- Ασύλληπτες δυνατότητες επεξεργασίας

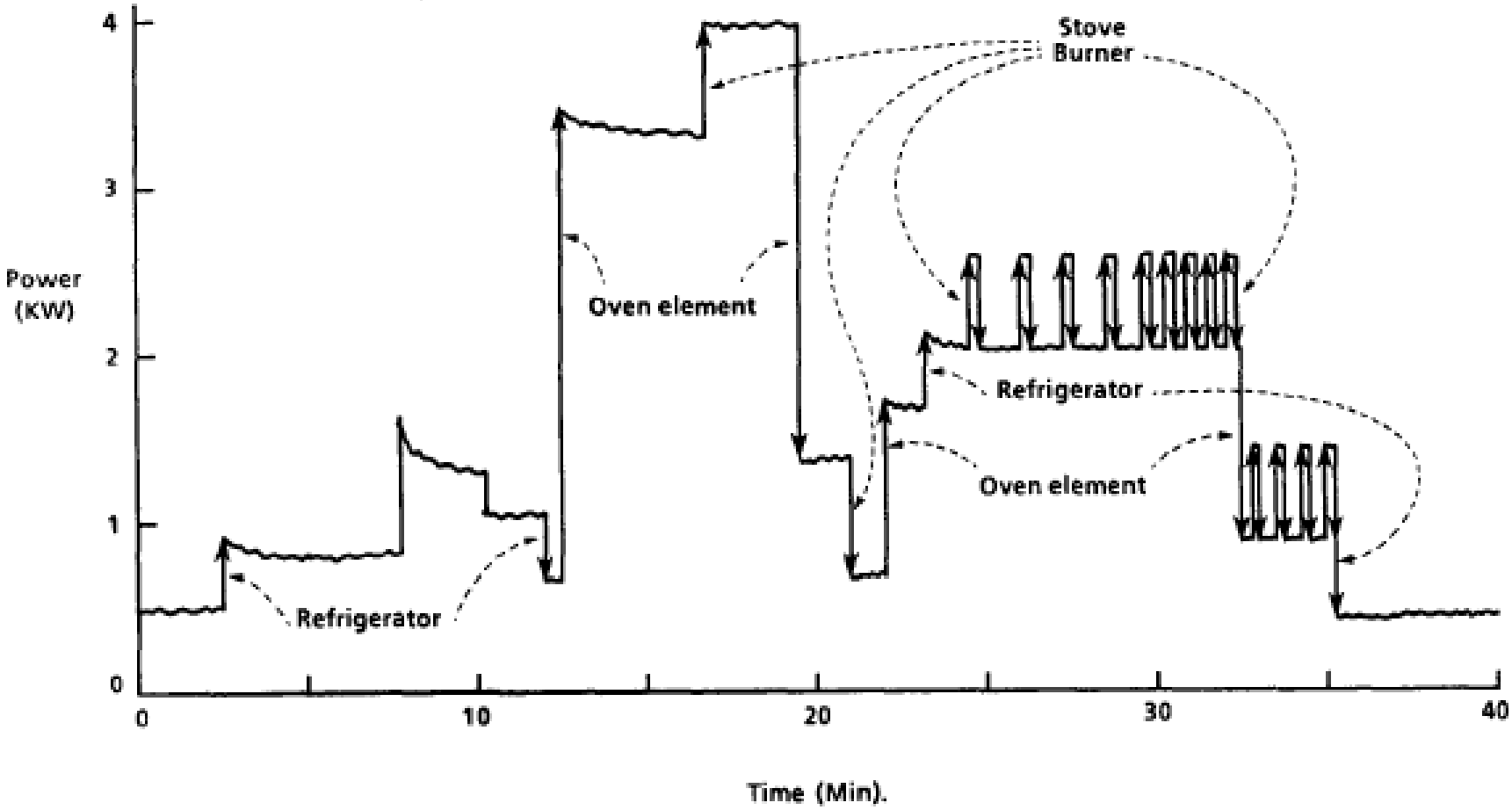
Ο βαθμός συλλογής και επεξεργασίας είναι ανεξέλεγκτος!

Το φαινόμενο google

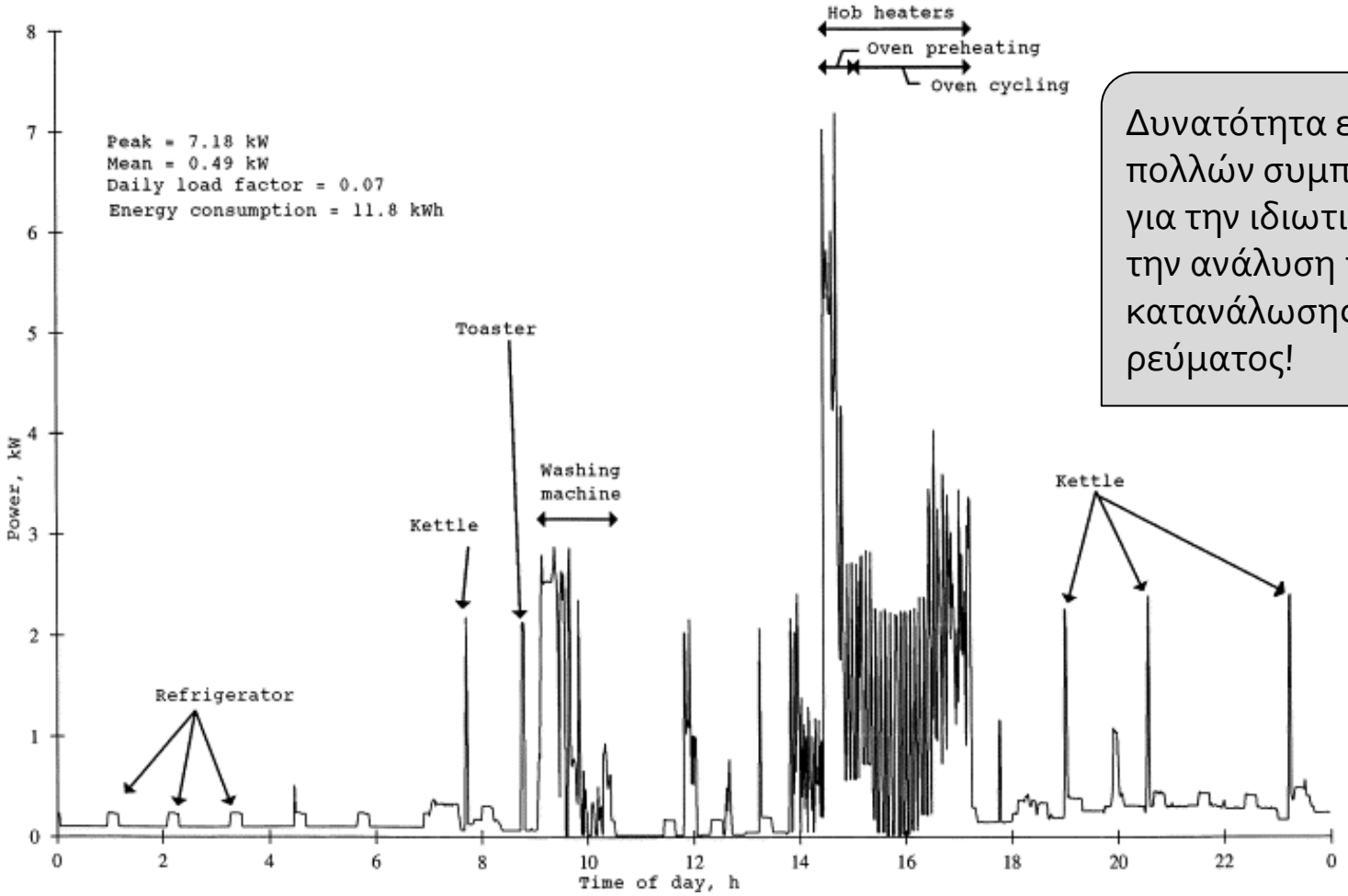
- Η google έχει πρόσβαση σε:
  - Διαδικτυακές αναζητήσεις
  - Επισκεφθείσες ιστοσελίδες (chrome)
  - Ηλεκτρονική αλληλογραφία (gmail)
  - Chat και VoIP (gtalk)
  - Φωτογραφίες (Picasa) και videos (YouTube)
  - Web ημερολόγια (blogspot.com)
  - Αρχεία σε υπολογιστές (g-desktop)
  - Κείμενα και άλλα αρχεία (g-docs)
  - Προσωπικό πρόγραμμα (g-calendar)
  - Εικόνες του πραγματικό κόσμου (streets view)
  - Δεδομένα θέσης και κίνησης (g-latitude, g-maps, …)

- Συγκέντρωση τεράστιας ποσότητας προσωπικών πληροφοριών, πλούσιας σε σημασιολογία και μεταδεδομένα, σε ένα μόνο φορέα!
- …με σκανδαλώδη πολιτική απορρήτου και ιστορία καταχρήσεων…
- Πολλές οι αναφορές παραβίασης της προσωπικής ζωής!!

Smart grid


Power
(KW)
4
3
2
1
0
0
10
20
30
40
Time (Min).
Stove
Burner
Oven element
Refrigerator
Refrigerator
Oven element

Smart grid



Δυνατότητα εξαγωγής πολλών συμπερασμάτων για την ιδιωτική ζωή από την ανάλυση του ρυθμού κατανάλωσης ηλεκτρικού ρεύματος!

Η Ιδιωτικότητα ως Δικαίωμα

- Οικουμενική Διακήρυξη για τα Ανθρώπινα Δικαιώματα:

  Κανείς δεν επιτρέπεται να υποστεί αυθαίρετες επεμβάσεις στην ιδιωτική του ζωή, την οικογένεια, την κατοικία ή την αλληλογραφία του.

- Σύνταγμα της Ελλάδας:

  Καθένας έχει δικαίωμα προστασίας από τη συλλογή, επεξεργασία και χρήση, ιδίως με ηλεκτρονικά μέσα, των προσωπικών του δεδομένων.

  Το απόρρητο των επιστολών και της ελεύθερης ανταπόκρισης ή επικοινωνίας με οποιονδήποτε άλλο τρόπο είναι απόλυτα απαραβίαστο.

Νομοθεσία

- Ευρωπαϊκή Νομοθεσία
  - Οδηγία 95/46/ΕΚ, "*για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη διακίνηση των δεδομένων αυτών*"
  - Οδηγία 2002/58/ΕΚ, "*σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών*"
  - Οδηγία 2006/24/ΕΚ, "*για τη διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημοσίων δικτύων επικοινωνιών*"
- Εθνική Νομοθεσία:
  - Νόμος 2472/1997
  - Νόμος 3471/2006
  - Νόμος 3917/2011
  - Οδηγίες, Προεδρικά Διατάγματα, Συστάσεις, Κανονισμοί (π.χ., οι Κανονισμοί της ΑΔΑΕ)

Βασικές αρχές ιδιωτικότητας

- Αρχή της νομιμότητας

  Η συλλογή και επεξεργασία των προσωπικών δεδομένων θα πρέπει να γίνεται σύμφωνα με τη σχετική νομοθεσία.
- Αρχή του περιορισμού της συλλογής

  Θα πρέπει να υπάρχουν όρια στη συλλογή προσωπικών δεδομένων, η συλλογή τους θα πρέπει να πραγματοποιείται με χρήση θεμιτών και σύννομων μέσων και –όπου είναι δυνατό– με τη συναίνεση ή την ενημέρωση του χρήστη.
- Αρχή της ποιότητας των δεδομένων

  Τα προσωπικά δεδομένα θα πρέπει να είναι σχετικά με το σκοπό για τον οποίο πρόκειται να χρησιμοποιηθούν ενώ –στο βαθμό που είναι απαραίτητο για το σκοπό αυτό– θα πρέπει να είναι πλήρη, ακριβή και ενημερωμένα.
- Αρχή προσδιορισμού του σκοπού

  Ο σκοπός για τον οποίο συλλέγονται προσωπικά δεδομένα θα πρέπει να προσδιορίζεται το αργότερο κατά τη χρονική στιγμή της συλλογής τους.

  Η συνακόλουθη χρήση τους θα πρέπει να περιορίζεται στην εκπλήρωση του σκοπού αυτού ή κάποιου πλήρως συμβατού σκοπού.

Βασικές αρχές ιδιωτικότητας

- Αρχή περιορισμού της χρήσης

  Τα προσωπικά δεδομένα δε θα πρέπει να κοινοποιούνται σε τρίτες οντότητες ή να χρησιμοποιούνται για άλλο σκοπό εκτός από τον προσδιορισμένο σύμφωνα με την αρχή προσδιορισμού του σκοπού, εκτός εάν υπάρχει η σχετική συναίνεση του χρήστη ή η εξουσιοδότηση από το νόμο.
- Αρχή της ασφάλειας και της εμπιστευτικότητας

  Τα προσωπικά δεδομένα θα πρέπει να προστατεύονται με χρήση των κατάλληλων μηχανισμών απέναντι σε κινδύνους όπως η μη εξουσιοδοτημένη πρόσβαση, καταστροφή, χρήση, τροποποίηση ή κοινοποίηση σε τρίτες οντότητες. Θα πρέπει να διασφαλίζονται η εμπιστευτικότητα και ακεραιότητα των δεδομένων.
- Αρχή της διαφάνειας

  Θα πρέπει να υπάρχει γενική διαφάνεια αναφορικά με τις πολιτικές και πρακτικές που σχετίζονται με τη συλλογή και επεξεργασία των προσωπικών δεδομένων καθώς και με την ταυτότητα του φορέα που διενεργεί τη συλλογή και επεξεργασία.

Βασικές αρχές ιδιωτικότητας

- Αρχή της ευθύνης

  Κάθε φορέας που διενεργεί συλλογή και επεξεργασία δεδομένων προσωπικού χαρακτήρα θα πρέπει να είναι υπόλογος αναφορικά με την εφαρμογή των μέτρων εκείνων που προάγουν τις αρχές οι οποίες πρέπει να διέπουν την προστασία των προσωπικών δεδομένων.
- Αρχή της συμμετοχής του ατόμου

  Το κάθε άτομο, θα πρέπει να έχει το δικαίωμα:
  - Να αποκτά είτε απ' ευθείας από τον υπεύθυνο της επεξεργασίας είτε μέσω κάποιου άλλου τρόπου επιβεβαίωση αναφορικά με το αν ο υπεύθυνος της επεξεργασίας διαθέτει δεδομένα που σχετίζονται με το εν λόγω άτομο.
  - Να του ανακοινώνονται δεδομένα που σχετίζονται με αυτό, μέσα σε εύλογο χρονικό διάστημα, με εύλογο τρόπο, σε μορφή εύκολα κατανοητή.
  - Να του παρέχονται οι λόγοι για τους οποίους απορρίπτονται αιτήσεις του που αναφέρονται στις δύο παραπάνω παραγράφους και να διατηρεί στην περίπτωση αυτή τη δυνατότητα της αμφισβήτησης της απόρριψης και της περαιτέρω διεκδίκησης.
  - Να αμφισβητεί προσωπικά δεδομένα που σχετίζονται με αυτό και σε περίπτωση επιτυχημένης αμφισβήτησης να μπορεί να προχωρεί σε εξάλειψη ή διόρθωση των δεδομένων αυτών.

Μηχανισμοί προστασίας

- Τυπικός διαχωρισμός:
  - "Προστασία" της ιδιωτικότητας:

    Μέθοδοι που εφαρμόζονται κυρίως από το χρήστη προκειμένου να προστατεύσει ενεργά ή να αποκρύψει προσωπικά δεδομένα, κυρίως κατά το στάδιο της μετάδοσής τους.
  - "Διαχείριση" της ιδιωτικότητας:

    Εφαρμογή μηχανισμών για τον έλεγχο της πρόσβασης σε προσωπικά δεδομένα και τη χρήση τεχνικών μέσων και ιδιαιτέρως συστημάτων που βασίζονται σε πολιτικές και κανόνες για την εφαρμογή των απαιτήσεων της σχετικής Νομοθεσίας και των ίδιων των χρηστών, κυρίως σε επιχειρησιακά περιβάλλοντα.

Προστασία της ιδιωτικότητας

- Κρυπτογραφία
  - Διασφάλιση συνδέσεων
  - Προστασία βάσεων δεδομένων
  - Ψηφιακές υπογραφές
- Ανωνυμία
  - Απόκρυψη IP διεύθυνσης (π.χ., δίκτυα Mix)
  - *k*-Anonymity
- Ψευδωνυμία
  - Διαχείριση ταυτοτήτων με τη μεσολάβηση τρίτης οντότητας
- Μηχανισμοί ασφάλειας
  - Firewalls, IDS, … : προστασία από «εξωτερικές» απειλές
  - Έλεγχος πρόσβασης: προστασία από «εσωτερικές» απειλές
  - …

Διαχείριση της ιδιωτικότητας

- Πολιτικές ιδιωτικότητας
  - Σε φυσική γλώσσα
  - Σε κάποια γλώσσα προδιαγραφής, π.χ. P3P – APPEL
- Πολιτικές ιδιωτικότητας σε βάσεις δεδομένων
  - Φιλτράρισμα των SQL queries με βάση την πολιτική
  - Χαρακτηριστικό παράδειγμα: Hippocratic Databases
- Επιχειρησιακές πολιτικές
  - Στοχεύουν στη διασφάλιση της εφαρμογής, ακολουθώντας το μοντέλο PDP – PEP
  - Μεταφράζονται σε κανόνες ελέγχου πρόσβασης
  - Χαρακτηριστικά παραδείγματα: OASIS XACML, IBM EPAL

Βασικά Προβλήματα

- Μηχανισμοί προστασίας της ιδιωτικότητας :
  - Καλύπτουν μόνο ένα μέρος του προβλήματος
    - Δεν μπορούν να προστατεύσουν από παρόχους – καταχραστές προσωπικών δεδομένων
    - Ο χρήστης χάνει κάθε έλεγχο μετά την παροχή των δεδομένων
    - Δεν προσφέρουν διαφάνεια και συσχέτιση με το σκοπό συλλογής
  - Έχουν μικρό εύρος εφαρμογής
  - Η απόκρυψη αναγκαίων δεδομένων καθιστά την παροχή υπηρεσιών ανέφικτη (π.χ. δεδομένα πιστωτικής κάρτας σε συναλλαγές)
  - Δεν μπορούν να εφαρμοστούν σε υπηρεσίες που ο χρήστης παρέχει ακούσια τα δεδομένα του (π.χ. βίντεο από κάμερες ασφάλειας)
  - ➔ Αναγκαία η εφαρμογή τους αλλά ανεπαρκής!
- Μηχανισμοί διαχείρισης της ιδιωτικότητας:
  - Εφόσον κάποιος πάροχος αποκτήσει πρόσβαση σε δεδομένα, δεν υπάρχει μέσο διασφάλισης της θεμιτής περαιτέρω επεξεργασίας / χρήσης τους
  - Ο χρήστης δε διαθέτει εγγυήσεις για την εφαρμογή της πολιτικής ιδιωτικότητας που δηλώνει ο πάροχος

Εν κατακλείδι

- Ron Rivest:

  The "reversal of defaults"

  What was once private is now public;

  what once was hard to copy is now trivial to duplicate;

  what was once easily forgotten is now stored forever.

  (*Διάλεξη στο CMU, Μάρτιος 2001*)

- Bob Dylan:

  After a while you learn that privacy is something you

  can sell, but you can't buy it back.

  (*Chronicles Vol. I, pp. 117-18, Simon & Schuster, New York, 2004*)