Υπηρεσίες Πληροφόρησης στην Ψηφιακή Εποχή: Ζητήματα Ασφάλειας και Προστασίας Ιδιωτικότητας

Βασίλης Ζορκάδης
Ηλ. Μηχ., Δρ. Επιστήμης Υπολογιστών Παν. Καρλσρούης
Αρχή Προστασίας Προσωπικών Δεδομένων
zorkadis@dpa.gr

Παρουσίαση στο Συνέδριο
«Αρχεία, Βιβλιοθήκες και Δίκαιο στην Κοινωνία της Πληροφορίας»
Αθήνα, 2-3 Φεβρουαρίου 2006

Περιεχόμενα Παρουσίασης

- Αρχεία και Βιβλιοθήκες στην Ψηφιακή Εποχή
- Θέματα ασφαλείας (απειλές και μέτρα προστασίας)
- Θέματα προστασίας ιδιωτικότητας (απειλές, μέτρα προστασίας)
- Διαχείριση ταυτότητας
- Εξελίξεις: Διάχυτος υπολογισμός και επικοινωνίες
- Συμπεράσματα

Αρχεία και Βιβλιοθήκες στην Ψηφιακή Εποχή

- Βάσεις δεδομένων, πρωτόκολα εφαρμογών διαδικτύου, εφαρμογές λογισμικού, μέσα αποθήκευσης, τεχνολογίες RFID
- Διαδικασίες (πρόσβασης στην πληροφορία, λειτουργίας, συντήρησης κ.ά.)
- Επιβλαβές λογισμικό (spyware, viruses, trojan horses, logic bombs)
- Απειλές σχετικές με ασφάλεια, πνευματικά δικαιώματα και την ιδιωτικότητα

Ζητήματα Ασφαλείας

- Απειλές (ταξινομημένες σύμφωνα με τις δυνατές επιπτώσεις)
  - Αποκάλυψη περιεχομένου επικοινωνιών, αιτημάτων και αναζητήσεων, καθώς και της ύπαρξής τους
  - Παραποίηση δεδομένων, διαγραφή, αντιγραφή κ.ά.
  - Άρνηση υπηρεσίας (διακοπή), ποιοτική υποβάθμιση
  - Άρνηση αποστολής, λήψης αιτημάτων, παραγγελιών
  - Πειρατεία
  - Ανάλυση δεδομένων κίνησης και ενεργειών

- Μέτρα προστασίας
  - Οργανωτικά
    - Πολιτικές και σχέδια ασφαλείας
    - Σχέδια έκτακτης ανάγκης και ανάκαμψης
    - Αξιολόγηση επικινδυνότητας και έλεγχος συμμόρφωσης
  - Τεχνικά
    - Αυθεντικοποίηση
    - Εμπιστευτικότητα και προστασία απορρήτου
    - Ακεραιότητα
    - Διαθεσιμότητα και διασφάλιση ποιότητας υπηρεσιών
    - Έλεγχος Πρόσβασης
    - Ψηφιακές Υπογραφές
    - Προστασία πνευματικής ιδιοκτησίας

- Τεχνικά μέσα πραγματοποίησης
  - Κρυπτογραφικές τεχνικές και πρωτόκολλα, PKI, firewalls, VPNs, monitoring and security analysis tools, κ.ά.
  - Information hiding techniques

Ζητήματα Προστασίας Ιδιωτικότητας

- Απειλές
  - Υποκλοπή περιεχομένου και δεδομένων κίνησης και θέσης ηλεκτρονικών επικοινωνιών
  - Επιτήρηση/παρακολούθηση με τη βοήθεια ψηφιακών μέσων (monitoring or surveillance systems)
  - Κλοπή στοιχείων και δεδομένων επαλήθευσης ταυτότητας χρηστών ή μελών
  - Απώλεια ελέγχου χρήσης και διανομής στοιχείων ταυτότητας
  - Αθέμιτη χρήση δεδομένων επικοινωνίας (spam)
  - Δημιουργία μορφοτύπων χρηστών/μελών
  - Δημιουργία πληροφοριακού πέπλου
  - Υπολείμματα προσωπικών δεδομένων
- Απειλές κατά τη χρήση τεχνολογιών RFID
  - Αποκάλυψη ενεργειών χρηστών/μελών
  - Αποκάλυψη θέσης
  - Προτιμήσεων, ενδιαφερόντων
  - Συσχετίσεις μελών/χρηστών και συγκεκριμένων αντικειμένων
  - Δημιουργία πληροφοριακού πέπλου
  - Αθέμιτη εκμετάλλευση υπολειμμάτων προσωπικών πληροφοριών

Ζητήματα Προστασίας Ιδιωτικότητας

- Πρακτικές – αρχές προστασίας δεδομένων
  - Σύννομη, θεμιτή και ακριβής επεξεργασία
  - Σαφείς και νόμιμοι σκοποί, χρόνος τήρησης
  - Ρητή συγκατάθεση των προσώπων
  - Δικαιώματα ενημέρωσης, πρόσβασης, αντίρρησης
  - Διασφάλιση του απορρήτου και της επεξεργασίας
- Απαιτήσεις (λειτουργιών και δυνατοτήτων) για την ενίσχυση της ιδιωτικότητας
  - Πολιτικές προστασίας ιδιωτικότητας
  - Πιστοποίηση οντοτήτων που εμπλέκονται στην επεξεργασία
  - Καταγραφή και τήρηση στοιχείων ενεργειών
  - Έλεγχος πρόσβασης
  - Διαχείριση σε περιπτώσεις παραβιάσεων
  - Διεπαφές υπευθύνων επεξεργασίας και υποκειμένων
  - Διαπραγμάτευση
  - Έλεγχος ποιότητας δεδομένων
- Τεχνικά μέσα πραγματοποίησης και στόχοι
  - Κρυπτογραφικές τεχνικές και πρωτόκολλα
  - Ανωνυμία, ψευδώνυμα
  - Αδυναμία σύνδεσης (unlinkability),
  - Αδυναμία παρατήρησης (unobservable)

Διαχείριση ταυτότητας

- On-line ταυτότητες (usernames, pseudonyms, e-mail addresses, cookies, etc.
- Off-line ταυτότητες (αριθμός ταυτότητας, αριθμός άδειας οδήγησης, αριθμός τηλεφώνου, αριθμός πιστωτικής κάρτας κ.ά.)
- Απαιτήσεις
  - Dependability (προστασία χρηστών από απάτη, αλλά και διασφάλιση υποχρεώσεων συναλλαγών)
  - Ελεγχόμενη αποκάλυψη πληροφορίας
  - Υποστήριξη πολλαπλών ταυτοτήτων και φορητότητας
- Άλλα θέματα
  - Διαχείριση κύκλου ζωής
  - Formats
  - Cross-domain communication
  - Ανωνυμία
  - Διαχείριση εμπιστοσύνης
  - Ελεγχόμενη διάδοση

Εξελίξεις

- Τεχνολογίες Περιρρέουσας Νοημοσύνης (Ambient Intelligence Technologies)
  - συστήματα διάχυτου υπολογισμού (ubiquitous computing)
  - Ubiquitous communications
  - διεπαφές φιλικές στο χρήση (user-friendly interfaces)
  - ενσωματωμένη νοημοσύνη (embedded intelligence)
  - Sensors, and actuators
- Επιπτώσεις
  - οικία, εργασία, εκπαίδευση, πληροφόρηση, υγεία, αγορά, κινητικότητα
- Απειλές σε ένα Κόσμο Περιρρέουσας Νοημοσύνης
  - Privacy, identity, security, trust
  - Επιτήρηση, spamming, identity theft, επιθέσεις, ψηφιακό χάσμα

Συμπεράσματα

- Απειλές ασφάλειας, παραβίασης πνευματικών δικαιωμάτων και ιδιωτικότητας
- Ασφαλή και φιλικά προς την ιδιωτικότητα συστήματα αρχείων και βιβλιοθηκών
- Επιτακτική ανάγκη διασφάλισης ενόψει νέων τεχνολογιών και γεφύρωσης του φυσικού με το ψηφιακό.

Αρχή Ασφαλείας

- Απόρρητο Επεξεργασίας
  - Η επεξεργασία δεδομένων μόνο από πρόσωπα που τελούν υπό τον έλεγχο του υπεύθυνου επεξεργασίας ή του εκτελούντος την επεξεργασία είναι απόρρητη. Διεξάγεται αποκλειστικά και μόνον κατ' εντολή του.
- Ασφάλεια Επεξεργασίας
  - Οργανωτικά και τεχνικά μέτρα ασφαλείας. Ο υπεύθυνος επεξεργασίας οφείλει να λαμβάνει τα κατάλληλα οργανωτικά και τεχνικά μέτρα για την ασφάλεια των δεδομένων και την προστασία τους από τυχαία ή αθέμιτη καταστροφή, τυχαία απώλεια, αλλοίωση, απαγορευμένη διάδοση ή πρόσβαση και κάθε άλλη μορφή αθέμιτης επεξεργασίας, ιδίως εάν η επεξεργασία συμπεριλαμβάνει και διαβίβαση των δεδομένων μέσων δικτύου. Αυτά τα μέτρα πρέπει να εξασφαλίζουν επίπεδο ασφαλείας ανάλογο προς τους κινδύνους που συνεπάγεται η επεξεργασία και η φύση των δεδομένων που είναι αντικείμενο της επεξεργασίας. Η Αρχή παρέχει εκάστοτε οδηγίες για το βαθμό ασφαλείας των δεδομένων καθώς και για τα μέτρα προστασίας που είναι αναγκαίο να λαμβάνονται για κάθε κατηγορία δεδομένων, εν' όψει και των τεχνολογικών εξελίξεων.
  - Ασφάλεια Outsourcing Υπηρεσιών. Αν η επεξεργασία διεξάγεται για λογαριασμό του υπεύθυνου από πρόσωπο μη εξαρτώμενο από αυτόν, η σχετική ανάθεση γίνεται υποχρεωτικά εγγράφως. Η ανάθεση προβλέπει υποχρεωτικά ότι ο ενεργών την επεξεργασία την διεξάγει μόνο κατ' εντολή του υπεύθυνου και ότι οι λοιπές υποχρεώσεις του παρόντος άρθρου βαρύνουν αναλόγως και αυτόν.
  - Επιλογή κατάλληλων προσώπων. Για τη διεξαγωγή της επεξεργασίας ο υπεύθυνος επεξεργασίας οφείλει να επιλέγει πρόσωπα με αντίστοιχα επαγγελματικά προσόντα που παρέχουν επαρκείς εγγυήσεις από πλευράς τεχνικών γνώσεων και προσωπικής ακεραιότητας για την τήρηση του απορρήτου.

Κίνδυνοι Ασφαλείας και Παραβίασης της Ιδιωτικότητας στην Ηλεκτρονική Δημοκρατία

- Κίνδυνοι Ασφαλείας: Διακοπή, Υποκλοπή, Παραποίηση, Πειρατεία, Αμφισβήτηση, Πλαστοπροσωπεία

- Κίνδυνοι παραβίασης ιδιωτικότητας:
  - Δημιουργία μορφοτύπων (profiling),
  - tracking,
  - identity theft,
  - loss of control,
  - spam,
  - privacy invasion

Μέτρα Ασφαλείας και Ενίσχυσης της Ιδιωτικότητας

- Μέτρα ασφαλείας: αυθεντικοποίηση, εμπιστευτικότητα περιεχομένου και δεδομένων κίνησης, μηχανισμοί ακεραιότητας, ελέγχου πρόσβασης κλπ.

- Μέτρα ενίσχυσης ιδιωτικότητας:
  - User Empowerment
    - ανωνυμία, ψευδώνυμα
    - privacy preference managers,
    - cookie managers
  - Intermediaries (Εμπιστες τρίτες οντότητες)
  - Τεχνολογίες ενίσχυσης ιδιωτικότητας
    - Notice and awareness, consent, access
    - Information quality, update and correction