

Πληροφοριακή Ιδιωτικότητα: Εισαγωγή

Μάθημα Πολιτικές Ασφάλειας & Ιδιωτικότητας στο
Διαδίκτυο

ΠΜΣ «Ψηφιακές Εφαρμογές & Καινοτομία»

Τσώχου Αγγελική atsohou@ionio.gr

Περιεχόμενα Διάλεξης

2

- ❑ Η έννοια της πληροφοριακής ιδιωτικότητας στη σημερινή ψηφιακή κοινωνία
- ❑ Η πληροφοριακή ιδιωτικότητα σήμερα και οι ανησυχίες των χρηστών
- ❑ Προκλήσεις για την προστασία της πληροφοριακής ιδιωτικότητας

Η έννοια της πληροφοριακής ιδιωτικότητας στη σημερινή ψηφιακή κοινωνία

Βασισμένο στο Λαμπρινουδάκης Κ., Μήτρου Λ., Γκρίτζαλης Σ. και Κάτσικας Σ. (2009), Προστασία της Ιδιωτικότητας και Τεχνολογίες Πληροφορικής και Επικοινωνιών: Τεχνικά και Νομικά Θέματα, Μήτρου Λ. Κεφάλαιο 21 (Η προστασία της Ιδιωτικότητας στην Πληροφορική και στις Επικοινωνίες. Η νομική διάσταση)

Η έννοια της ιδιωτικότητας ιστορικά

4

- ❑ Διάκριση μεταξύ ιδιωτικού και δημόσιου χώρου
- ❑ Διάκριση μεταξύ ιδιωτικού «οίκου» και «δημόσιου» εξωτερικού χώρου από την αρχαιότητα
- ❑ Ο τρόπος που νοείται η ιδιωτικότητα εξαρτάται από τη φύση των σχέσεων του ατόμου με την κοινωνία και το Κράτος
- ❑ Αφορά το άτομο και τη σχέση του με τον κοινωνικό περίγυρο

Η έννοια της ιδιωτικότητας ιστορικά

5

- ❑ Τα όρια της ιδιωτικότητας μεταβάλλονται και είναι συχνά δυσδιάκριτα
- ❑ Όρια δημόσιου και ιδιωτικού βίου, δημόσιου και ιδιωτικού χώρου
- ❑ «Ιδιωτικός χώρος»: μπορεί να νοείται και ένας δημόσια προσιτός χώρος, στον οποίο ωστόσο κανείς αναζητά την απόσυρση, ή και ο τερματικός τηλεπικοινωνιακός εξοπλισμός

Παράγοντες που επηρεάζουν την εμβέλεια της ιδιωτικότητας

6

- ☐ Αντιλήψεις, ήθη και έθιμα
- ☐ Μέγεθος, δομής και φύση της οικογένειας
- ☐ Η φύση των κοινωνικών χώρων
- ☐ Η φύση των κοινωνικών πεδίων δραστηριότητας
- ☐ Ο αστικός χώρος και το οικιστικό περιβάλλον
- ☐ Η διάκριση του χώρου εργασίας και χώρου κατοικίας
- ☐ Οι τεχνολογίες

Ανάγκη ή δικαίωμα;

7

Φυσική ανάγκη ή δικαίωμα;

Η ιδιωτικότητα αποτελεί φυσική ανάγκη
όλων των ανθρώπων;

Η ιδιωτικότητα ως δικαίωμα

8

- ❑ Καταγράφεται ως κατάκτηση προνομίου από μία κοινωνική ομάδα:
 - ❑ Επαναστάσεις του 18^{ου} και 19^{ου} αιώνα
 - ❑ Κατοχύρωση ατομικών δικαιωμάτων
 - ❑ Διατύπωση ατομικού δικαιώματος στην ιδιωτικότητα
 - ❑ Δικαίωμα συνδεδεμένο με το δικαίωμα της προσωπικότητας
 - ❑ Προστασία του ατόμου έναντι προσβολών από τη δημόσια-κρατική εξουσία

S. Rodota, Privacy and Data Surveillance: Growing Public Concern. Paris, France: OECD, Information Studies (Vol. 10), 1976, σελ. 133.

Η έννοια της ιδιωτικότητας στην κοινωνία

9

- ❑ Παραπομπή στην συνηγορία των δικαστών Warren και Brandeis (1896) υπέρ του δικαιώματος του ατόμου σε μία ανενόχλητη ιδιωτική ζωή (the right to be let alone)
- ❑ Επαρκεί αυτός ο ορισμός σήμερα;

Η έννοια της ιδιωτικότητας στην κοινωνία

10

- ❑ Εμπλουτισμός της «κλασικής» αντίληψης της ιδιωτικότητας με επιμέρους δικαιώματα:
 - ❑ το δικαίωμα σε ιδιωτική ζωή
 - ❑ ο περιορισμός της προσβασιμότητας
 - ❑ ο αποκλειστικός έλεγχος της πρόσβασης στον ιδιωτικό χώρο (ή άσυλο της κατοικίας)
 - ❑ η ελαχιστοποίηση των “παρεμβάσεων”
 - ❑ η προσδοκία της εχεμύθειας
 - ❑ το δικαίωμα στο απόρρητο
 - ❑ το δικαίωμα στην απόλαυση της μοναξιάς, της
 - ❑ της ανωνυμίας
 - ❑ της απόσυρσης

Η έννοια της ιδιωτικότητας στην κοινωνία

11

- ❑ Στον «κλασικό» ορισμό του Westin η ιδιωτικότητα προσδιορίζεται ως αξίωση των ατόμων, ομάδων ή θεσμών να προσδιορίζουν οι ίδιοι:
 - ❑ Πότε
 - ❑ Πώς
 - ❑ Σε ποια έκτασηοι πληροφορίες που τους αφορούν θα γίνονται γνωστές στους τρίτους.

Η έννοια της ιδιωτικότητας στην κοινωνία

12

- ❑ Κατοχύρωση της προστασίας του ιδιωτικού βίου από το Ευρωπαϊκό Δικαστήριο των Δικαιωμάτων του Ανθρώπου, το άρθρο 8 της Ευρωπαϊκής Σύμβασης Δικαιωμάτων του Ανθρώπου
 - ❑ εξασφάλιση της ανάπτυξης, χωρίς εξωτερική παρέμβαση, της προσωπικότητας κάθε ατόμου στη σχέση του με άλλους ανθρώπους
- ❑ Διαφορά μεταξύ της κυρίαρχης αμερικανικής και της αντίστοιχης ευρωπαϊκής προσέγγισης αναφορικά με το περιεχόμενο της ιδιωτικότητας σε σχέση με τον κοινωνικό περίγυρο

Η έννοια της ιδιωτικότητας στην κοινωνία

13

- ❑ Το Ευρωπαϊκό Δικαστήριο των Δικαιωμάτων του Ανθρώπου αναγνωρίζει:
 - ❑ την υποχρέωση του κράτους να λαμβάνει μέτρα για την προστασία των δικαιωμάτων των προσώπων στην ιδιωτικότητα
 - ❑ την πιθανή ευθύνη του κράτους για παραβιάσεις της ιδιωτικότητας εκ μέρους ιδιωτών, εφόσον δεν έχει λάβει μέτρα για την αποτροπή ή την κύρωσή τους
- ❑ Βασική διαφορά της ευρωπαϊκής συνταγματικής προσέγγισης σε σχέση με την αντίστοιχη των ΗΠΑ όπου το Κράτος δεν υποχρεούται σε παρέμβαση έναντι των ιδιωτών

Η έννοια της ιδιωτικότητας στην κοινωνία

14

- ❑ Η πληροφοριακή ιδιωτικότητα αποσκοπεί στο να καταστήσει δυνατή στο άτομο μία συγκεκριμένη συμμετοχή στις διαδικασίες της κοινωνίας
- ❑ Καθιστά ταυτόχρονα δυνατή την άσκηση άλλων ελευθεριών και την απόλαυση άλλων ατομικών δικαιωμάτων, όπως η ελευθερία της έκφρασης, η συμμετοχή σε πολιτικές ή συνδικαλιστικές ενώσεις, η θρησκευτική ελευθερία

Ιδιωτικότητα vs. Ελευθερία

15

- ❑ Αλληλοεξαρτώμενες έννοιες
- ❑ Εκφράζουν τον «σεβασμό», με τον οποίο μία φιλελεύθερη, δημοκρατική κοινωνία αντιμετωπίζει τα άτομα
- ❑ Στην ευρωπαϊκή προσέγγιση, η ιδιωτικότητα συνδέεται με την αξία/αξιοπρέπεια του ανθρώπου
 - ❑ Αξίωση να μην καθίσταται το άτομο ένα πληροφοριακό αντικείμενο, ένα σύνολο δεδομένων προς επεξεργασία ή προς συναλλαγή

Η Πληροφοριακή Ιδιωτικότητα

16

- ❑ Ανεπαρκής η έννοια της ιδιωτικότητας ως αξίωση σεβασμού της απόσυρσης ή του απόρρητου
- ❑ Διεύρυνση του αγαθού υπό προστασία
- ❑ Αρχές του '70: αναφορά τους κινδύνους ενός νέου «Πανοπτικον», το οποίο, σε αντίθεση με το Panopticon του Bentham, δεν περιοριζόταν σε κλειστές επιτηρούμενες κοινότητες αλλά αφορούσε προοπτικά το σύνολο των ατόμων και των δραστηριοτήτων τους

Κίνητρα για τη διεύρυνση του αγαθού υπό προστασία

17

- ❑ Μεταβολή των δυνατοτήτων συλλογής, επεξεργασίας, διάχυσης, συσχετισμού των πληροφοριών που δημιουργήσαν τα πληροφοριακά και επικοινωνιακά συστήματα
- ❑ Μεταβολή των δυνατοτήτων χρήσης, ανταλλαγής και συσχετισμού των δεδομένων που έχουν συλλεχθεί για πολλαπλούς και διαφορετικούς από τους αρχικούς σκοπούς

Κίνητρα για τη διεύρυνση του αγαθού υπό προστασία

18

- ❑ Αναφορά στη «διαφανή κοινωνία» ή τον «διαφανή πολίτη» σε κείμενα του '70 ή του '80, ως αποτέλεσμα συγκεντρωτικής κρατικής εξουσίας
- ❑ Διάχυση της επεξεργασίας της πληροφορίας στο κράτος, την οικονομία και την κοινωνία
- ❑ Το αγαθό υπό προστασία δεν εντοπίζεται στην αξίωση για ανενόχλητη ιδιωτική σφαίρα, αλλά αφορά την **απώλεια άσκησης ελέγχου επί των ιδίων, προσωπικών πληροφοριών**

Κίνητρα για τη διεύρυνση του αγαθού υπό προστασία

19

Γεωμετρική αύξηση των δυνατοτήτων επεξεργασίας της προσωπικής πληροφορίας **vs.** ικανότητα του προσώπου να έχει εποπτεία της χρήσης των πληροφοριών που το αφορούν

Η πληροφοριακή ιδιωτικότητα ως ιδιοκτησία;

20

- ❑ Δικαίωμα (αυτό)διάθεσης των πληροφοριών, εξισούμενο κατ' αποτέλεσμα με ένα δικαίωμα κυριότητας;
- ❑ Ευχέρεια παραίτησης από την ιδιωτικότητα και απαλλοτρίωσης των ιδίων δεδομένων;
- ❑ Μήπως αυτή η αντίληψη μειώνει την ιδιωτικότητα σε ένα «ιδιοκτησιακό δικαίωμα» που επιτρέπει στον φορέα του να διαπραγματεύεται την ιδιωτικότητά του αλλά και την τιμή της;

Η πληροφοριακή ιδιωτικότητα ως ιδιοκτησία;

21

- ❑ Η «αγορά της ιδιωτικότητας», διάδραση ανάμεσα στο άτομο και σε αυτόν που επεξεργάζεται πληροφορία
- ❑ Έκφραση του δικαιώματος παραίτησης από την ιδιωτικότητα μέσα από τη συγκατάθεση ενός προσώπου για την επεξεργασία των προσωπικών πληροφοριών του
- ❑ Οι όροι της συναλλαγής – επεξεργασίας στην ευρωπαϊκή προσέγγιση ρυθμίζει η νομοθεσία

Επιχειρήματα κατά της ιδιωτικότητας ως ιδιοκτησία

22

- ❑ Το πληροφοριακό χάσμα/πληροφοριακή ασυμμετρία
 - ❑ Αδυναμία των προσώπων να προσδιορίσουν τις πιθανές μελλοντικές χρήσεις άρα και την οικονομική αξία κτήσης και χρήσης των πληροφοριών τους
 - ❑ Άγνοια των όρων της προστασίας προσωπικών πληροφοριών που οδηγεί σε ανισότητα των διαπραγματευόμενων μερών
- ❑ Η ψευδαίσθηση της συγκατάθεσης
 - ❑ Λόγω της ανισότητας πληροφοριών είναι αμφίβολο εάν μιλάμε για πληροφορημένη συγκατάθεση και κατά συνέπεια και για ενσυνείδητη συγκατάθεση

Επιχειρήματα κατά της ιδιωτικότητας ως ιδιοκτησία

23

- ❑ Σύνδεση της ιδιωτικότητας με την ανθρώπινη αξία και την ισότητα
 - ❑ *Η αξία του ανθρώπου και η προστασία της υλικής και ηθικής του υπόστασης είναι υπέρτατη δημόσιας τάξης αρχή από την οποία δεν είναι δυνατή η παραίτηση (Σύνταγμα, άρθρο 2 § 1)*
- ❑ Η **πληροφοριακή ασυμμετρία** αντιστοιχεί συχνά σε – συχνά εγγενή- **ανισότητα**
- ❑ Η αξίωση της ιδιωτικότητας στον εργασιακό χώρο
- ❑ Η περίπτωση του **Microsoft Biometrics**: Διασύνδεση των εργαζομένων με τους υπολογιστές τους μέσω ασύρματων αισθητήρων, επιτρέποντας στους εργοδότες να παρακολουθούν διαρκώς το μεταβολισμό τους

Ιδιωτικότητα vs. Απόρρητο

24

- ❑ Όροι σχετικοί αλλά όχι ισοδύναμοι
- ❑ Απόρρητο:
 - ❑ Άμεση σύνδεση με την εμπιστευτικότητα
 - ❑ Μη προσπελασιμότητα ορισμένων πληροφοριών που εμπίπτουν στη σφαίρα επιρροής ενός ατόμου
 - ❑ Καθήκον ή την υποχρέωση διαφύλαξης πληροφοριών που είτε ένα άτομο έχει εμπιστευτεί στο φορέα (π.χ. ιατρικό απόρρητο) είτε ένας φορέας της κατέχει λόγω θέσης/αρμοδιότητάς (π.χ. υπηρεσιακό απόρρητο).
 - ❑ Αποκλείει τρίτους από τη γνώση, τη χρήση και αξιοποίηση των πληροφοριών, εφόσον δεν συντρέχει κάποιος νόμιμος λόγος και η αντίστοιχη διαδικασία που επιτρέπουν την άρση του απορρήτου

Προστασία Προσωπικών Δεδομένων

25

- ❑ Η προστασία της πληροφοριακής ιδιωτικότητας συνδέεται άμεσα με τον τρόπο που τεχνολογίες πληροφορικής και επικοινωνιών έχουν αλλάξει ριζικά το περιβάλλον χρήσης της προσωπικής πληροφορίας
- ❑ Σε αντίθεση με την ιδιωτικότητα, η προστασία προσωπικών δεδομένων εγείρεται ως αίτημα αναπόσπαστα συνδεδεμένο με την τεχνολογική εξέλιξη

Προστασία Προσωπικών Δεδομένων

26

- ❑ Δεν περιορίζεται στη ρύθμιση και προστασία της πληροφορίας που το άτομο θεωρεί ιδιωτική και ευαίσθητη
- ❑ Αφορά κάθε πληροφορία που αναφέρεται σε ένα φυσικό πρόσωπο
- ❑ Η προστασία των προσωπικών δεδομένων υπερβαίνει τη διάκριση μεταξύ ιδιωτικής και δημόσιας σφαίρας, καθώς καταρχήν δεν διακρίνει ανάμεσα σε «απλές» και «ιδιωτικές/απόρρητες» πληροφορίες

Προστασία Προσωπικών Δεδομένων

27

- ❑ Δύο κατηγορίες κανονιστικών προσεγγίσεων:
 - ❑ Προαγωγή μίας ολιστικής ρύθμισης όλων των τομέων κρατικής και ιδιωτικής δραστηριότητας
 - ❑ Ρύθμιση ορισμένων τομέων και πεδίων κρατικής και ιδιωτικής δραστηριότητας επενδύοντας στη λύση της αυτορρύθμισης (μη κρατική παρέμβαση –συμμετοχή)

Η πληροφοριακή Ιδιωτικότητα σήμερα και οι ανησυχίες των χρηστών

- ✓ **Πελάτης:** Καλησπέρα! Πιτσαρία Gordon's;
- ✓ **Υπάλληλος:** Όχι κύριε, εδώ είναι πιτσαρία Google's
- ✓ **Πελάτης:** Λάθος νούμερο, συγνώμη
- ✓ **Υπάλληλος:** Όχι κύριε, η επιχείρηση αγοράστηκε από την Google
- ✓ **Πελάτης:** Α, εντάξει. Μπορώ να παραγγείλω;
- ✓ **Υπάλληλος:** Βεβαίως. Θέλετε τα συνηθισμένα;
- ✓ **Πελάτης:** Τι εννοείται τα συνηθισμένα, με ξέρετε;
- ✓ **Υπάλληλος:** Σύμφωνα με τον αριθμό τηλεφώνου σας, τις τελευταίες 12 φορές που παραγγείλατε ζητήσατε πίτσα σπέσιαλ. Θα μπορούσα να σας προτείνω να δοκιμάσετε εναλλακτικά πίτσα με ρόκα, ντοματίνια και πιπεριές;
- ✓ **Πελάτης:** Τι; Μα απεχθάνομαι τα λαχανικά!
- ✓ **Υπάλληλος:** Η χοληστερίνη σας δεν είναι σε καλά επίπεδα κύριε.
- ✓ **Πελάτης:** Μα πώς το ξέρετε εσείς;
- ✓ **Υπάλληλος:** Διασταυρώσαμε τον αριθμό τηλεφώνου σας με το όνομά σας και έχουμε τα αποτελέσματα των ιατρικών σας εξετάσεων από τους ιατρικούς μας συνεργάτες τα τελευταία 7 χρόνια.
- ✓ **Πελάτης:** Τέλος πάντων, εγώ θέλω να παραγγείλω την πίτσα σπέσιαλ. Παίρνω έτσι κι αλλιώς φάρμακα για τη χοληστερίνη.

- ✓ **Υπάλληλος:** Συγνώμη, αλλά τελευταία δεν έχετε πάρει τα φάρμακά σας τακτικά. Σύμφωνα με την εμπορική βάση δεδομένων μας, έχετε αγοράσει μόνο ένα πακέτο ταμπλέτες από το Φάρμακα.gr τους τελευταίους 4 μήνες.
- ✓ **Πελάτης:** Αγόρασα από άλλο κατάστημα...
- ✓ **Υπάλληλος:** Όχι σύμφωνα με τα στοιχεία των πιστωτικών καρτών σας.
- ✓ **Πελάτης:** Πλήρωσα με μετρητά!
- ✓ **Υπάλληλος:** Όχι σύμφωνα τα στοιχεία της τελευταίας σας φορολογικής δήλωσης, εκτός αν τα αγοράσατε με χρήματα από μη δηλωμένο εισόδημα.
- ✓ **Πελάτης:** Τι στο καλό!
- ✓ **Υπάλληλος:** Συγχωρείστε με κύριε, χρησιμοποιούμε αυτές τις πληροφορίες με την πρόθεση αν σας εξυπηρετήσουμε καλύτερα.
- ✓ **Πελάτης:** Αρκετά! Βαρέθηκα την Google, το Facebook, το Twitter, το WhatsApp. Θα πάω σε ένα απομονωμένο νησί, χωρίς Ίντερνετ, κινητό τηλέφωνο και κανείς δε θα μπορεί να με κατασκοπεύει!
- ✓ **Υπάλληλος:** Καταλαβαίνω κύριε, αλλά σας ενημερώνω ότι πρέπει να ανανεώσετε το διαβατήριό σας γιατί έληξε πριν 5 εβδομάδες
- ✓ **Πελάτης:**

Η ιδιωτικότητα σήμερα

31

Αυξανόμενος αριθμός χρηστών Διαδικτύου εκφράζουν ανησυχία αναφορικά με το πλήθος των προσωπικών δεδομένων τους που βρίσκονται διαθέσιμα στο Διαδίκτυο:

- 50% των συνολικών ερωτηθέντων σε σχετική έρευνα που ολοκληρώθηκε [1] το 2013, συγκριτικά με 33% στην αντίστοιχη έρευνα του 2009
- 92% των ερωτηθέντων σε έρευνα του Ινστιτούτου TRUSTe [2] το 2014, συγκριτικά με 89% στην αντίστοιχη έρευνα του 2013

Οι ανησυχίες των χρηστών

32

- Κύριες ανησυχίες των χρηστών [3]:
 - Μη εξουσιοδοτημένη χρήση και γνωστοποίηση των προσωπικών πληροφοριών σε επιχειρήσεις (58%)
 - Παρακολούθηση δραστηριοτήτων στο Διαδίκτυο με σκοπό τη μελλοντική προσωποποιημένη διαφήμιση και διαμόρφωση περιεχομένου ιστοσελίδων (47%)

Οι απόψεις διχάζονται...

- ❑ 82% των συμμετεχόντων σε έρευνα που πραγματοποιήθηκε το 2016 [3] δήλωσαν ότι δε νιώθουν άνετα με την πώληση των προσωπικών τους δεδομένων σε τρίτα μέρη, σε αντάλλαγμα με ταχύτητα, άνεση, ποικιλία προϊόντων, καλύτερη τιμή και άλλα εμπορικά οφέλη που παρέχουν οι Διαδικτυακές αγορές.
- ❑ Παραπάνω από το 50% των συμμετεχόντων δήλωσαν ότι θα ήταν διατεθειμένοι να διαμοιράσουν το γένος, την εκπαίδευση ή την εθνικότητά τους στο Διαδίκτυο
- ❑ 16% των συμμετεχόντων νιώθουν άνετα να διαμοιράσουν την τοποθεσία τους
- ❑ 14% τη διεύθυνση μόνιμης κατοικίας τους
- ❑ 13% τα ιατρικά τους δεδομένα

Οι απόψεις διχάζονται...

34

- ❑ Θα συμφωνούσατε με την τήρηση ιστορικού αγορών σας με αντάλλαγμα την παροχή εκπτώσεων από έναν πάροχο; 47% των συμμετεχόντων σε έρευνα που πραγματοποιήθηκε το 2016 από το Pew Research Center το βρίσκει αποδεκτό [4]
- ❑ Θα συμφωνούσατε με την εγκατάσταση «έξυπνου» θερμοστάτη στο σπίτι, ο οποίος μειώνει την κατανάλωση ενέργειας, μέσα από την παρακολούθηση και καταγραφή των κινήσεών σας στο σπίτι; 27% των συμμετεχόντων το βρίσκει αποδεκτό [4]

Οι απόψεις διχάζονται...

35

- ❑ Θα συμφωνούσατε με την καταγραφή των συμπεριφορών οδήγησης σας (π.χ. ταχύτητα, τοποθεσία, διαδρομές) μέσω GPS trackers με αντάλλαγμα την παροχή εκπτώσεων ασφάλισης αυτοκινήτου (λόγω καλής συμπεριφοράς οδήγησης); 37% των συμμετεχόντων το βρίσκει αποδεκτό [4]
- ❑ Θα συμφωνούσατε να κάνει το τοπικό σας ιατρείο τα ιατρικά σας δεδομένα προσβάσιμα μέσω Διαδικτύου (σε ασφαλή τοποθεσία), προκειμένου να υπάρχει ευκολότερη διαχείριση ραντεβού και διαγνώσεων από τους γιατρούς; 52% των συμμετεχόντων το βρίσκει αποδεκτό [4]

Η ιδιωτικότητα σήμερα

36

- Οι επιπτώσεις για τους χρήστες Διαδικτύου από την απώλεια ιδιωτικότητας είναι σημαντικές [1], [5]:
 - 19% των ερωτηθέντων έχουν επίγνωση περιπτώσεων στις οποίες τα προσωπικά τους δεδομένα αξιοποιήθηκαν με διαφορετικό τρόπο από τον αναμενόμενο
 - 13% των ερωτηθέντων αντιμετώπισαν προβλήματα διαπροσωπικών σχέσεων εξ' αιτίας στοιχείων που δημοσίευσαν στο Διαδίκτυο
 - 12% των ερωτηθέντων έχουν υποστεί παρενοχληθεί στο Διαδίκτυο
 - 11% των ερωτηθέντων αναφέρουν υποκλοπή προσωπικών δεδομένων (για παράδειγμα στοιχεία τραπεζικών λογαριασμών)

Η ιδιωτικότητα σήμερα

37

- Οι επιπτώσεις για τους χρήστες Διαδικτύου από την απώλεια ιδιωτικότητας είναι σημαντικές [1], [5]:
 - 6% των ερωτηθέντων έχουν εξαπατηθεί από επιθέσεις διαδικτυακής απάτης (scam) με χρηματικές απώλειες
 - 6% των ερωτηθέντων έχουν υποστεί δυσφήμιση εξ 'αιτίας διαδικτυακών δραστηριοτήτων τους
 - 1% των ερωτηθέντων αποκλείστηκαν από επαγγελματικές ή εκπαιδευτικές ευκαιρίες εξ 'αιτίας στοιχείων που δημοσίευσαν στο Διαδίκτυο

Η ιδιωτικότητα σήμερα

- Η αίσθηση των χρηστών Διαδικτύου είναι ότι [1], [5]:
 - Δεν είναι εφικτό να παραμείνουν ανώνυμοι στο Διαδίκτυο (59%)
 - Η σύγχρονη νομοθεσία είναι ανεπαρκής για την προστασία της Ιδιωτικότητας των χρηστών στο Διαδίκτυο (68%), ενώ μικρό ποσοστό (24%) θεωρεί ότι παρέχεται εύλογη προστασία
 - Θα έπρεπε να έχουν το δικαίωμα να χρησιμοποιήσουν το Διαδίκτυο προστατεύοντας την ανωνυμία τους (59%)
 - Οι πολιτικές Ιδιωτικότητας και χρήσης προσωπικών δεδομένων είναι δυσνόητες (37%)

Η ιδιωτικότητα σήμερα

39

- Οι χρήστες χρησιμοποιούν πλέον διάφορες στρατηγικές για να είναι λιγότερο “ορατοί” στο Διαδίκτυο [1]:
 - Αφαιρούν cookies και διαγράφουν το ιστορικό του λογισμικού πλοήγησης (64%)
 - Διαγράφουν/επεξεργάζονται παρελθούσες δημοσιεύσεις (41%)
 - Απενεργοποιούν τη δυνατότητα εγκατάστασης cookies (41%)
 - Αποφεύγουν τη χρήση ιστοτόπων που απαιτούν πραγματικό όνομα (36%)
 - Άλλες πρακτικές (1%-18%), όπως μεταμφίηση ταυτότητας, κρυπτογραφία επικοινωνιών, δημοσίευση ανακριβών στοιχείων, κ.ά.

Μπορεί να προστατευτεί η ιδιωτικότητα σήμερα;

40

- ❑ Οι επαγγελματίες πληροφορικής τονίζουν ότι η ιδιωτικότητα δεν προστατεύεται από τις επιχειρήσεις κυρίως λόγω:
 - ❑ έλλειψης θέλησης από την ανώτερη διοίκηση,
 - ❑ έλλειψης ελέγχου των συνεργατών για τις πρακτικές τους με τα προσωπικά δεδομένα που έχουν πρόσβαση
 - ❑ έλλειψη τεχνικών αντιμέτρων και στήριξη σε κώδικες δεοντολογίας,
 - ❑ έλλειψη γνώσης των προσωπικών πληροφοριών που βρίσκονται αποθηκευμένα σε βάσεις δεδομένων [6]

Μπορεί να προστατευτεί η ιδιωτικότητα σήμερα;

41

- ❑ Η ενίσχυση της λογοδοσίας των επιχειρήσεων είναι κλειδί για την προστασία της ιδιωτικότητας των ατόμων, μέσω:
 - ❑ ανάπτυξης μετρικών παρακολούθησης (KPIs) της προστασίας της ιδιωτικότητας
 - ❑ Πραγματοποίηση αναλύσεων επιπτώσεων παραβίασης της ιδιωτικότητας
 - ❑ Υλοποίηση προγράμματος αντιμετώπισης περιστατικών παραβίασης προσωπικών δεδομένων
 - ❑ Υλοποίηση συστημάτων διαχείρισης ταυτότητας
 - ❑ Παρακολούθηση της απειλής εκ των έσω
 - ❑ Διαχείριση συγκατάθεσης μέσω right-on-time ειδοποιήσεων έναντι παραδοσιακών πολιτικών ιδιωτικότητας

Προκλήσεις προστασίας της ιδιωτικότητας

Προκλήσεις για την προστασία της ιδιωτικότητας

43

- ❑ Τεχνολογικοί παράγοντες
- ❑ Παγκοσμιοποίηση της επεξεργασίας και της επικοινωνίας
- ❑ Αλλαγές των αντιλήψεων τόσο των ατόμων
- ❑ Αλλαγές των προσεγγίσεων των κρατικών και κοινωνικών οργανώσεων ως προς το περιεχόμενο της ιδιωτικότητας

Τεχνολογικές προκλήσεις

44

- ❑ Οι τεχνολογικές εξελίξεις θέτουν σε δοκιμασία τη ρυθμιστική ικανότητα των νομικών κανόνων
- ❑ Το τεχνολογικό υπόβαθρο της επεξεργασίας προσωπικών πληροφοριών εξελίσσεται ραγδαία:
 - ❑ Από «αρχεία» και μεγάλα υπολογιστικά συστήματα
 - ❑ Στη διάδοση των προσωπικών υπολογιστών
 - ❑ Στην αλματώδη ανάπτυξη των δικτύων και του Διαδικτύου
 - ❑ Στην εξόρυξη δεδομένων
 - ❑ Στο Web 2.0
 - ❑ Στις νανοτεχνολογίες, βιομετρικές τεχνολογίες και RFIDs
 - ❑ Στην καταγραφή τοποθεσίας

Προκλήσεις εμπορευματοποίησης της πληροφορίας

45

- ❑ Παροχή προσωπικών πληροφοριών από τους χρήστες, είτε επειδή προαπαιτούνται για τη δημιουργία ενός λογαριασμού είτε ως «αντάλλαγμα» για την πρόσβαση σε μία υπηρεσία ή πληροφορία
- ❑ Συστήματα που είναι σχεδιασμένα να παρακολουθούν τα άτομα κατά την πλοήγησή τους (π.χ. μέσω IP διευθύνσεων ή cookies)
- ❑ Συλλογή μεγάλου όγκου δεδομένων αδιαφανώς προς τον χρήστη

Προκλήσεις εμπορευματοποίησης της πληροφορίας

46

- ❑ Έρευνες αγοράς και διαφήμιση: χρήση τεχνολογιών εξόρυξης δεδομένων για την παραγωγή νέας πληροφορίας
- ❑ Στοχευμένη διαφήμιση: εξατομικευμένες υπηρεσίες, δημιουργία προφίλ συμπεριφοράς χρήστη
- ❑ Επιχειρηματικές αλλαγές, π.χ. εξαγορά της Double Click από την Google
- ❑ Εξωτερική ανάθεση, και υπηρεσίες νεφοϋπολογιστικής

Προκλήσεις γεωγραφικής οριοθέτησης

47

- ❑ Αποσύνδεση της επεξεργασίας από συγκεκριμένο γεωγραφικό τόπο
- ❑ Η κυκλοφορία της πληροφορίας και η προσπελασιμότητά της υπερβαίνει τα εδαφικά σύνορα
- ❑ Δυσχέρεια προσδιορισμού και εφαρμογής του δικαίου ή/και των δικαστικών αποφάσεων

Η επεξεργασία ως καθημερινότητα

48

- ❑ Τεχνολογίες οικονομικά προσιτές από όλους
- ❑ Ολοένα αυξανόμενες δραστηριότητες που λαμβάνουν χώρα στο τεχνολογικό περιβάλλον
- ❑ Εθισμός των ατόμων να παρέχουν πληροφορίες και να αλληλεπιδρούν μέσω τεχνολογίας
- ❑ Απώλεια της ανωνυμίας ως αντίτιμο της δυνατότητας online διεκπεραίωσης συναλλαγών
- ❑ Αυτοέκθεση των ατόμων μέσω ιστολογίων και κοινωνικών δικτύων
- ❑ Συστήματα επιβράβευσης πελατών

Η ανθρωπινή ασφάλεια ως αντίποδας

49

- ❑ Αποδοχή ή ανοχή της εκτεταμένης επεξεργασίας ως απάντηση στο αίτημα ή την προσδοκία της ασφάλειας
- ❑ «Παραδοσιακό» μοντέλο: αντιμετώπιση συγκεκριμένων κινδύνων προερχόμενων από συγκεκριμένα άτομα ή κύκλους ατόμων
- ❑ Σήμερα παρατηρείται απροσδιοριστία της απειλής και των στόχων αυτής (αόριστοι κίνδυνοι): κάθε άτομο λογίζεται ως δυνάμει ύποπτος:
 - ❑ Βιντεοεπιτήρηση στους δημόσιους χώρους
 - ❑ Υποχρεωτική προληπτική τήρηση δεδομένων από τηλεπικοινωνιακούς παρόχους

Πλαίσιο πληροφοριακής ιδιωτικότητας κατά ISO 29100 (2008)

- Πλαίσιο πληροφοριακής ιδιωτικότητας κατά ISO 29100 (2008)
- Κύριες ιδιότητες και έννοιες
 - i. Ανωνυμία
 - ii. Μη συνδεσιμότητα
 - iii. Μη ανιχνευσιμότητα
 - iv. Μη παρατηρησιμότητα

Το πρότυπο ISO/IEC 29100 (2011)

52

- ❑ Το πρότυπο ISO/IEC 29100 (2011) θέτει ένα πλαίσιο για την προστασία της ιδιωτικότητας κατά την επεξεργασία προσωπικών δεδομένων μέσω πληροφοριακών συστημάτων
- ❑ Προσωπική πληροφορία (personally identifiable information ή PII): Οποιαδήποτε πληροφορία που α) μπορεί να χρησιμοποιηθεί για να αναγνωριστεί το υποκείμενο των δεδομένων, β) συνδέεται ή μπορεί να συνδεθεί άμεσα ή έμμεσα με ένα υποκείμενο των δεδομένων

Πρόσθετοι όροι

53

- ❑ Υποκείμενο των δεδομένων (PII principal): φυσικό πρόσωπο με το οποίο συνδέονται οι προσωπικές πληροφορίες
- ❑ Διαχειριστής προσωπικών πληροφοριών (PII controller): εμπλεκόμενος της ιδιωτικότητας που καθορίζει τους σκοπούς και τα μέσα επεξεργασίας προσωπικών πληροφοριών, εξαιρουμένων τυχόν φυσικών προσώπων που επεξεργάζονται δεδομένα για προσωπικούς σκοπούς

Πρόσθετοι όροι

54

- ❑ Επεξεργαστής προσωπικών πληροφοριών (PII processor): εμπλεκόμενος της ιδιωτικότητας που επεξεργάζεται προσωπικές πληροφορίες εκ μέρους του, και σύμφωνα με τις οδηγίες του διαχειριστή προσωπικών πληροφοριών
- ❑ Τρίτα μέρη (third parties): Οντότητες που λαμβάνουν προσωπικές πληροφορίες από έναν διαχειριστή ή επεξεργαστή προσωπικών πληροφοριών. Τα τρίτα μέρη δεν επεξεργάζονται προσωπικές πληροφορίες εκ μέρους του διαχειριστή. Γενικά, τα τρίτα μέρη γίνονται διακριτοί διαχειριστές των εν λόγω προσωπικών πληροφοριών από τη στιγμή που τα λαμβάνουν

Ενδεχόμενες Αλληλεπιδράσεις Συμμετεχόντων Οντοτήτων

55

- ☐ Το υποκείμενο των δεδομένων παρέχει PII στον διαχειριστή PII
- ☐ Ο διαχειριστής PII παρέχει PII στον επεξεργαστή PII
- ☐ Το υποκείμενο των δεδομένων παρέχει PII σε έναν επεξεργαστή PII που έχει εξουσιοδοτηθεί από τον διαχειριστή PII
- ☐ Ο διαχειριστής PII ή ο επεξεργαστής PII παρέχουν PII στο υποκείμενο των δεδομένων

Ποια δεδομένα

είναι PIIs;

- Περιλαμβάνει αναγνωριστικά μοναδικά στο υποκείμενο των δεδομένων (π.χ. αριθμός ταυτότητας)
- Περιλαμβάνει αναγνωριστικά που συσχετίζονται με το υποκείμενο των δεδομένων (π.χ. αριθμοί λογαριασμών)
- Περιλαμβάνει ή σχετίζεται με αναγνωριστικά που επαρκούν για να γίνει επικοινωνία με ένα υποκείμενο (π.χ. γεωγραφική θέση ή τηλεφωνικός αριθμός)
- Περιλαμβάνει αναφορές που συνδέονται με κάποιο από τα παραπάνω

Examples

Age or special needs of vulnerable natural persons
 Allegations of criminal conduct
 Any information collected during health services
 Bank account or credit card number
 Biometric identifier
 Credit card statements
 Criminal convictions or committed offences
 Criminal investigation reports
 Customer number
 Date of birth
 Diagnostic health information
 Disabilities
 Doctor bills
 Employees' salaries and human resources files
 Financial profile
 Gender
 GPS position
 GPS trajectories
 Home address
 IP address
 Location derived from telecommunications systems
 Medical history
 Name
 National identifiers (e.g., passport number)
 Personal e-mail address
 Personal identification numbers (PIN) or passwords
 Personal interests derived from tracking use of internet web sites
 Personal or behavioural profile
 Personal telephone number
 Photograph or video identifiable to a natural person
 Product and service preferences
 Racial or ethnic origin
 Religious or philosophical beliefs
 Sexual orientation
 Trade-union membership
 Utility bills

Ποια δεδομένα είναι PIIs;

57

❑ Εκτός από άμεσα αναγνωριστικά...

...και δεδομένα που περιλαμβάνουν χαρακτηριστικά που διαχωρίζουν ένα φυσικό πρόσωπο από άλλα φυσικά πρόσωπα (π.χ. βιομετρικά χαρακτηριστικά)

... και οποιοδήποτε χαρακτηριστικό γνώρισμα που μπορεί να αναγνωρίζει μοναδικά ένα φυσικό πρόσωπο

Σημειώνεται ότι η μοναδική αναγνώριση μπορεί να εξαρτάται από το πλαίσιο των δεδομένων

π.χ. ένα επώνυμο σε διεθνές επίπεδο vs. σε εταιρικό επίπεδο

Ευαίσθητες προσωπικές πληροφορίες

58

- ❑ Ευαίσθητες προσωπικές πληροφορίες (Sensitive PII): κατηγορία προσωπικών πληροφοριών των οποίων η φύση είναι ευαίσθητη (π.χ. συνδέονται με το ενδόμυχο πλαίσιο του ατόμου) ή μπορεί να έχουν σημαντική επίδραση για το υποκείμενο των δεδομένων
- ❑ Η ευαισθησία σε ένα σύνολο δεδομένων εξαρτάται από το βαθμό στον οποίο μπορούν να εξαχθούν ευαίσθητες PII. Για παράδειγμα από μία συνταγή γιατρού μπορούν να εξαχθούν πληροφορίες για την υγεία ενός ατόμου

Ευαίσθητες προσωπικές πληροφορίες

59

- ❑ Ανάλογα με τη γεωγραφική θέση και το κράτος, μπορεί να ορίζεται ξεκάθαρα από το νομικό πλαίσιο ποιες πληροφορίες είναι ευαίσθητες
- ❑ Για παράδειγμα στην Ευρωπαϊκή Ένωση είναι τα δεδομένα που αφορούν φυλετική ή εθνική προέλευση, πολιτικά φρονήματα, θρησκευτικές ή φιλοσοφικές πεποιθήσεις, συμμετοχή σε συνδικαλιστική οργάνωση, στην υγεία, στην κοινωνική πρόνοια και στην ερωτική ζωή, στα σχετικά με ποινικές διώξεις ή καταδίκες, καθώς και στη συμμετοχή σε συναφείς με τα ανωτέρω ενώσεις προσώπων

Μέτρα προστασίας της ιδιωτικότητας

60

- ❑ Κίνητρα οργανισμών: προστασία των πελατών, συμμόρφωση με νομικό ή κανονιστικό πλαίσιο, εταιρική ευθύνη, ενίσχυση εμπιστοσύνης των πελατών
- ❑ Οι απαιτήσεις προστασίας εξαρτώνται από πολλούς παράγοντες, όπως ο τρόπος συλλογής και επεξεργασίας PII, η μετάδοση PII σε τρίτα μέρη, οι συμβατικές σχέσεις και όροι μεταξύ διαχειριστών και επεξεργαστών PII, η μετάδοση PII σε άλλα έθνη, κ.ά.

Μέτρα προστασίας της ιδιωτικότητας

61

- ❑ Η αναγνώριση των απαιτήσεων και μέτρων προστασίας της ιδιωτικότητας πρέπει να προηγείται του σχεδιασμού ενός πληροφοριακού συστήματος
- ❑ Η διαδικασία αυτή συνήθως πραγματοποιείται μέσω της ανάλυσης επικινδυνότητας για την ιδιωτικότητα

Πολιτικές Ιδιωτικότητας

62

- ❑ Ένας οργανισμός που επεξεργάζεται προσωπικές πληροφορίες πρέπει να καθιερώσει μία εγκεκριμένη από την ανώτερη διοίκηση πολιτική ιδιωτικότητας που:
 - ❑ να είναι κατάλληλη για το σκοπό του οργανισμού
 - ❑ να παρέχει ένα πλαίσιο για την θέσπιση στόχων ιδιωτικότητας
 - ❑ να δείχνει τη δέσμευση υλοποίησης των μέτρων προστασίας της ιδιωτικότητας
 - ❑ να δείχνει τη δέσμευση για διαρκή βελτίωση
 - ❑ να διανέμεται στον οργανισμό και να είναι διαθέσιμη σε ενδιαφερόμενα μέρη

Πολιτικές Ιδιωτικότητας

63

- ❑ Εσωτερικές και εξωτερικές πολιτικές ιδιωτικότητας
 - ❑ Εσωτερική πολιτική ιδιωτικότητας: στόχοι, κανόνες, υποχρεώσεις, περιορισμοί και μέτρα προστασίας που θεσπίζει ο οργανισμός για την ικανοποίηση των απαιτήσεων προστασίας της ιδιωτικότητας
 - ❑ Εξωτερική πολιτική ιδιωτικότητας: ενημέρωση εξωτερικών ενδιαφερόμενων μερών για τις πρακτικές προστασίας της ιδιωτικότητας του οργανισμού, πληροφορίες για την ταυτότητα, τη διεύθυνση και στοιχεία επικοινωνίας του διαχειριστή ΡΙΙ, και άλλες πληροφορίες

Αρχές προστασίας της ιδιωτικότητας

64

1. Συναίνεση και επιλογή (Consent and Choice)
2. Νομιμότητα και καθορισμός σκοπού (Purpose legitimacy and specification)
3. Περιορισμός συλλογής (Collection limitation)
4. Ελαχιστοποίηση δεδομένων (Data minimization)
5. Περιορισμός χρήσης, τήρησης και αποκάλυψης (Use, retention and disclosure limitation)
6. Ορθότητα και Ποιότητα (Accuracy and quality)

Αρχές προστασίας της ιδιωτικότητας

65

7. Ειλικρίνεια, διαφάνεια και ενημέρωση (Openness, transparency and notice)
8. Συμμετοχή και Πρόσβαση (Individual participation and access)
9. Λογοδοσία (Accountability)
10. Ασφάλεια πληροφοριών (Information security)
11. Συμμόρφωση με απαιτήσεις προστασίας της ιδιωτικότητας (Privacy compliance)

Το Πλαίσιο

67

- Οι ορισμοί βασίζονται στη θεώρηση ότι υπάρχει:
 - ▣ ένα **πλαίσιο** (setting),
 - ▣ όπου κάποιος **αποστολέας** (sender) ή **δρων αποστολέας** (actor)
 - ▣ αποστέλλει **μηνύματα** (messages)
 - ▣ σε κάποιον **παραλήπτη** (recipient) ή **δρων παραλήπτης** (actee)
 - ▣ μέσω ενός **δικτύου επικοινωνίας** (communication network)
- Στα εκάστοτε περιβάλλοντα, όπως πραγματοποίηση ερωτημάτων σε βάσεις δεδομένων, ηλεκτρονικές αγορές κ.λπ., η ίδια ορολογία μπορεί να χρησιμοποιηθεί αντικαθιστώντας, όπως απαιτείται, τις λέξεις μήνυμα, αποστολέας, παραλήπτης

Ιστορικά στοιχεία

68

- Οι όροι:
 - ▣ ανωνυμία (anonymity)
 - ▣ ψευδωνυμία (pseudonymity)
 - ▣ μη-συνδεσιμότητα (unlinkability)
 - ▣ διαχείριση ταυτότητας (identity management)
- αναφέρθηκαν για πρώτη φορά στη δεκαετία του '80
- Κάθε ερευνητής χρησιμοποιούσε διαφορετικό λεξιλόγιο για τους όρους αυτούς
- Ανάγκη ακριβέστερης ορολογίας

Το Πλαίσιο



- Συνολικά θεωρείται ότι:
 - μία **ενεργή οντότητα** (subject) αποτελεί μία εν δυνάμει δρώσα οντότητα, π.χ., φυσικό πρόσωπο, νομικό πρόσωπο, υπολογιστή, διεργασία
 - ένα **σύνολο ενεργών οντοτήτων** (set of subjects) αποτελεί, π.χ., έναν οργανισμό που δε δρα ως νομικό πρόσωπο, ούτε παρουσιάζεται ως αυτόνομη οντότητα, αλλά ως δομημένο σύνολο από ενεργές οντότητες

Το Πλαίσιο

70

- Η έννοια του πλαισίου (setting) μπορεί να γίνει πιο σαφής με χρήση του όρου **σύστημα** (system), το οποίο έχει τις ακόλουθες ιδιότητες:
 - ▣ Το σύστημα έχει ένα **εξωτερικό περιβάλλον** (surrounding), δηλαδή τμήμα του κόσμου που βρίσκεται εκτός του συστήματος

Σύστημα (system) + Περιβάλλον (surrounding) = Κόσμος (universe)
- Η κατάσταση του συστήματος μπορεί να αλλάξει ανάλογα με τις ενέργειες εντός του συστήματος

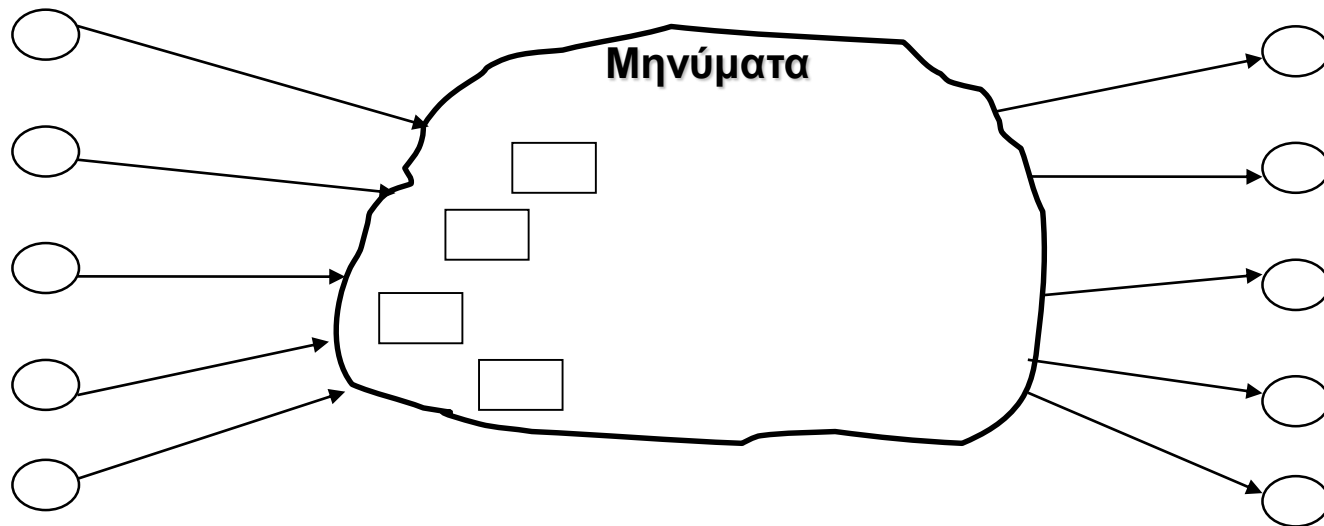
Το Πλαίσιο

71

Αποστολείς

Παραλήπτες

Δίκτυο Επικοινωνίας



Η οπτική του επιτιθέμενου

72

- Ως επιτιθέμενος νοείται κάθε οντότητα που αποσκοπεί ενάντια στους στόχους προστασίας, π.χ. την ανωνυμία
- Ο επιτιθέμενος (attacker) ενδιαφέρεται για:
 - Παρακολούθηση των επικοινωνιών
 - Καταγραφή των προτύπων επικοινωνίας που παρατηρούνται
 - Χειραγώγηση της επικοινωνίας

Η οπτική του επιτιθέμενου

73

- Υποθέτουμε ότι ο επιτιθέμενος:
 - Ενδέχεται να είναι εκτός συστήματος και να παρακολουθεί τις γραμμές επικοινωνίας (outsider)
 - Ενδέχεται να είναι εντός συστήματος, λαμβάνοντας μέρος σε επικοινωνίες ελέγχοντας σταθμούς εργασίας (insider)
 - Αξιοποιεί όλες τις πληροφορίες ώστε να καταλήξει στα στοιχεία που ενδιαφέρουν (Items of Interest - IOIs), π.χ. ποιος έστειλε, ποιος παρέλαβε, ποια μηνύματα

Η οπτική του επιτιθέμενου

74

- Επιπλέον των IOIs, χρήσιμες είναι οι **ιδιότητες** (attributes):
 - Οι ιδιότητες ενδέχεται να είναι και οι ίδιες αντικείμενα που ενδιαφέρουν, ή η παρατήρησή τους μπορεί να οδηγήσει σε IOIs
 - Μια ιδιότητα αποτελεί χαρακτηριστικό μιας οντότητας ή μιας ενέργειας
 - Ιδιότητες οντοτήτων μπορεί να αποτελούν: Αποστολή μηνύματος ή Παραλαβή μηνύματος

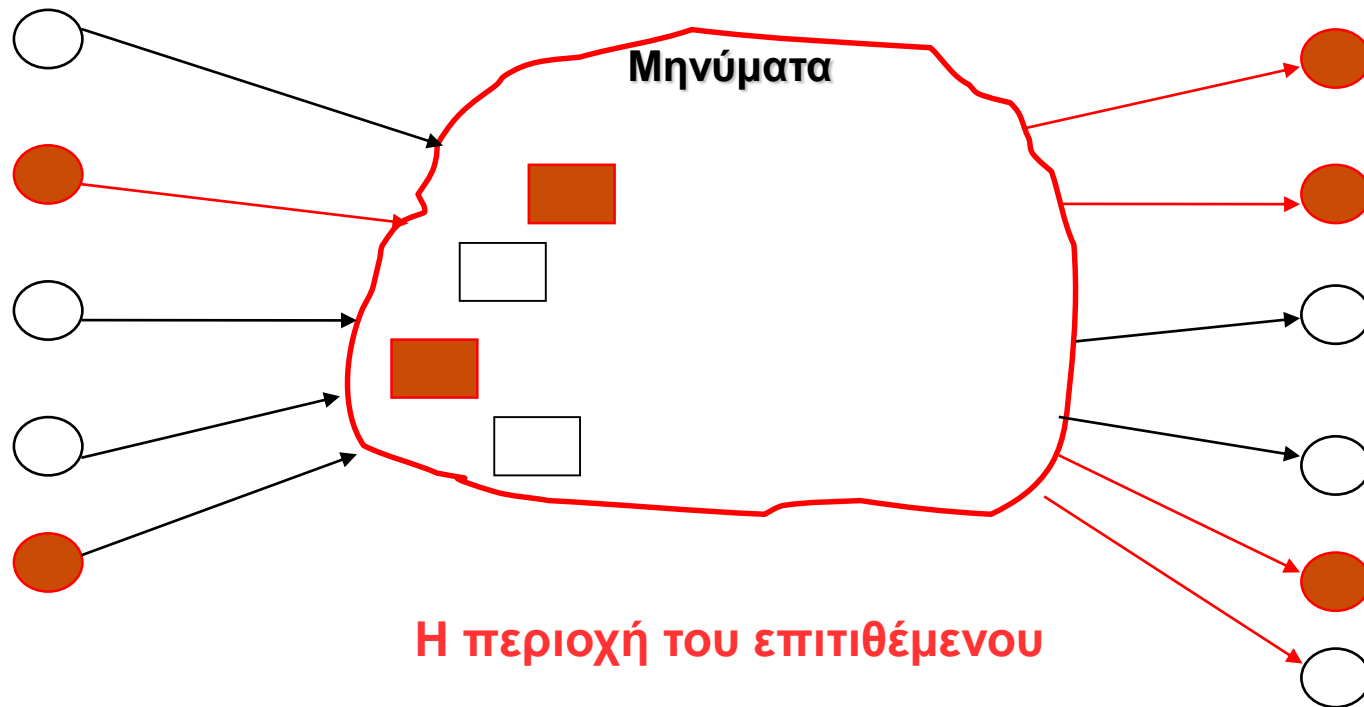
Η περιοχή του επιτιθέμενου

75

Αποστολείς

Παραλήπτες

Δίκτυο επικοινωνίας



Παραδοχές

76

- Ο επιτιθέμενος δεν είναι σε θέση να αποκτήσει γνώση για τον αποστολέα ή τον παραλήπτη από το περιεχόμενο του μηνύματος
- Ο επιτιθέμενος δεν ξεχνά ποτέ κάποια πληροφορία
- Η γνώση (knowledge) του επιτιθέμενου μόνο αυξάνεται
 - Η γνώση αναφέρεται σε πιθανότητες των IOIs: περισσότερη γνώση σημαίνει μεγαλύτερη ακρίβεια στις πιθανότητες
 - Οι πιθανότητες που ο επιτιθέμενος θεωρεί πραγματικές είναι πιο κοντά στις πραγματικές πιθανότητες

Η έννοια της Ανωνυμίας (Anonymity)

77

Ανωνυμία μιας ενεργού οντότητας (anonymity of a subject) σημαίνει ότι η οντότητα **δεν είναι αναγνωρίσιμη** (not identifiable) μέσα σε ένα σύνολο οντοτήτων, δηλαδή στο **σύνολο ανωνύμων οντοτήτων** (anonymity set)

Η έννοια της Ανωνυμίας (Anonymity)

78

- Μη αναγνωρίσιμος (not identifiable): Μη μοναδικά χαρακτηρίσιμος, μη διαχωρίσιμος, με την εκάστοτε γνώση που έχει ο επιτιθέμενος
- Ενεργή οντότητα (subject): Μία εν δυνάμει δρώσα οντότητα (φυσικό πρόσωπο, νομικό πρόσωπο, υπολογιστής, διεργασία)
- Σύνολο ανωνύμων οντοτήτων (anonymity set): Σύνολο με όλες τις πιθανές ενεργές οντότητες, με την εκάστοτε γνώση του επιτιθέμενου
- Η ανωνυμία εξαρτάται από τη γνώση του εκάστοτε επιτιθέμενου, επομένως είναι υποκειμενική αναφορικά με τον επιτιθέμενο

Η έννοια της Ανωνυμίας (Anonymity)

79

- Ο αποστολέας μπορεί να παραμένει ανώνυμος μόνο εντός ενός συνόλου εν δυνάμει αποστολέων που αποτελεί το σύνολο ανωνύμων αποστολέων (sender anonymity set)
- Ο παραλήπτης μπορεί να παραμένει ανώνυμος μόνον εντός ενός συνόλου εν δυνάμει παραληπτών που αποτελεί το σύνολο ανωνύμων παραληπτών (recipient anonymity set)
- Τα δύο σύνολα ενδέχεται να μην περιέχουν κανένα κοινό στοιχείο, να περιέχουν κάποια κοινά στοιχεία, ή να είναι όμοια
- Τα δύο σύνολα ενδέχεται να μην παραμένουν σταθερά στη διάρκεια του χρόνου

Η έννοια της Ανωνυμίας (Anonymity)

- Η ανωνυμία εξασφαλίζει τη μη αποκάλυψη της ταυτότητας του χρήστη κατά την πρόσβαση σε δεδομένα ή υπηρεσίες
- Οι μηχανισμοί προστασίας της ανωνυμίας δεν αποσκοπούν στη γενική προστασία της ταυτότητας μιας ενεργού οντότητας (αν και οι προϋποθέσεις για την επίτευξη ανωνυμίας, παρέχουν την απαιτούμενη προστασία της ταυτότητας του χρήστη):
 - Η ανωνυμία απαιτεί άλλοι χρήστες ή ενεργές οντότητες να μην είναι σε θέση να ανακαλύψουν την ταυτότητα ενός χρήστη μέσω της σύνδεσής του με μία ενεργή οντότητα ή με μία διαδικασία

Η έννοια της Ανωνυμίας (Anonymity)

81

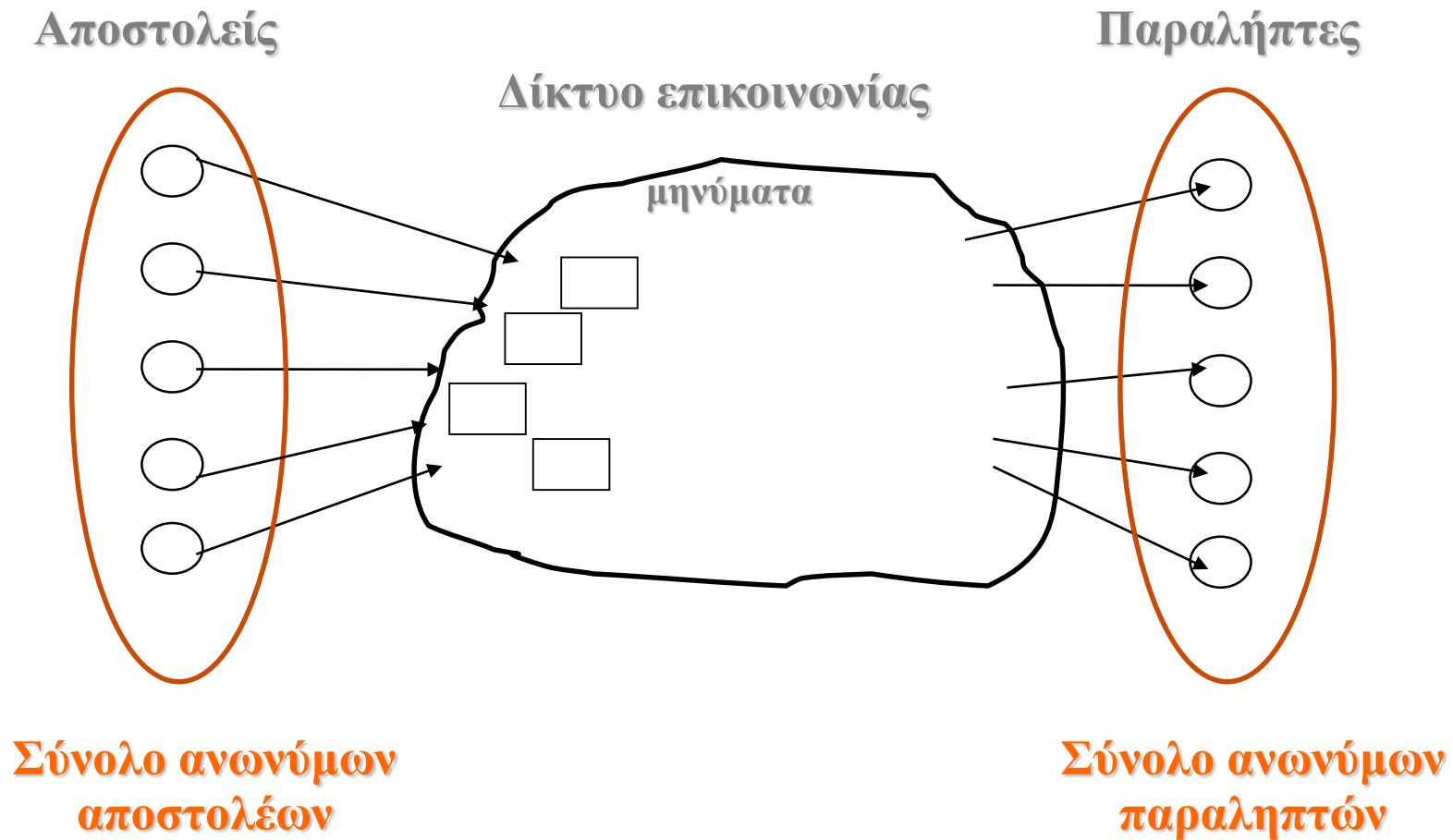
- Εφόσον ο επιτιθέμενος δε ξεχνά καμία πληροφορία, το σύνολο ανωνύμων οντοτήτων δεν μπορεί να μεγαλώσει
- Στην περίπτωση που νέες οντότητες εισέρχονται στο σύστημα μετά από τον επιτιθέμενο, αυτές δε θα ανήκουν στο σύνολο ανωνύμων οντοτήτων του επιτιθέμενου
- Αν ο επιτιθέμενος δεν είναι σε θέση να γνωρίζει το χρόνο εισαγωγής των οντοτήτων στο σύστημα, το σύνολο ανωνύμων οντοτήτων παραμένει σταθερό

Η έννοια της Ανωνυμίας (Anonymity)

- Η ανωνυμία ενός συνόλου ενεργών οντοτήτων (set of subjects), εντός ενός πιθανότατα ευρύτερου συνόλου ανωνύμων οντοτήτων, σημαίνει ότι αυτές οι ενεργές οντότητες δεν είναι αναγνωρίσιμες εντός του συνόλου των ανωνύμων οντοτήτων
- Σύνολο ενεργών οντοτήτων: Χρησιμοποιείται για να περιγράψει ότι όλες οι ενεργές οντότητες που απαρτίζουν το σύνολο διατηρούν την ιδιότητα της ανωνυμίας

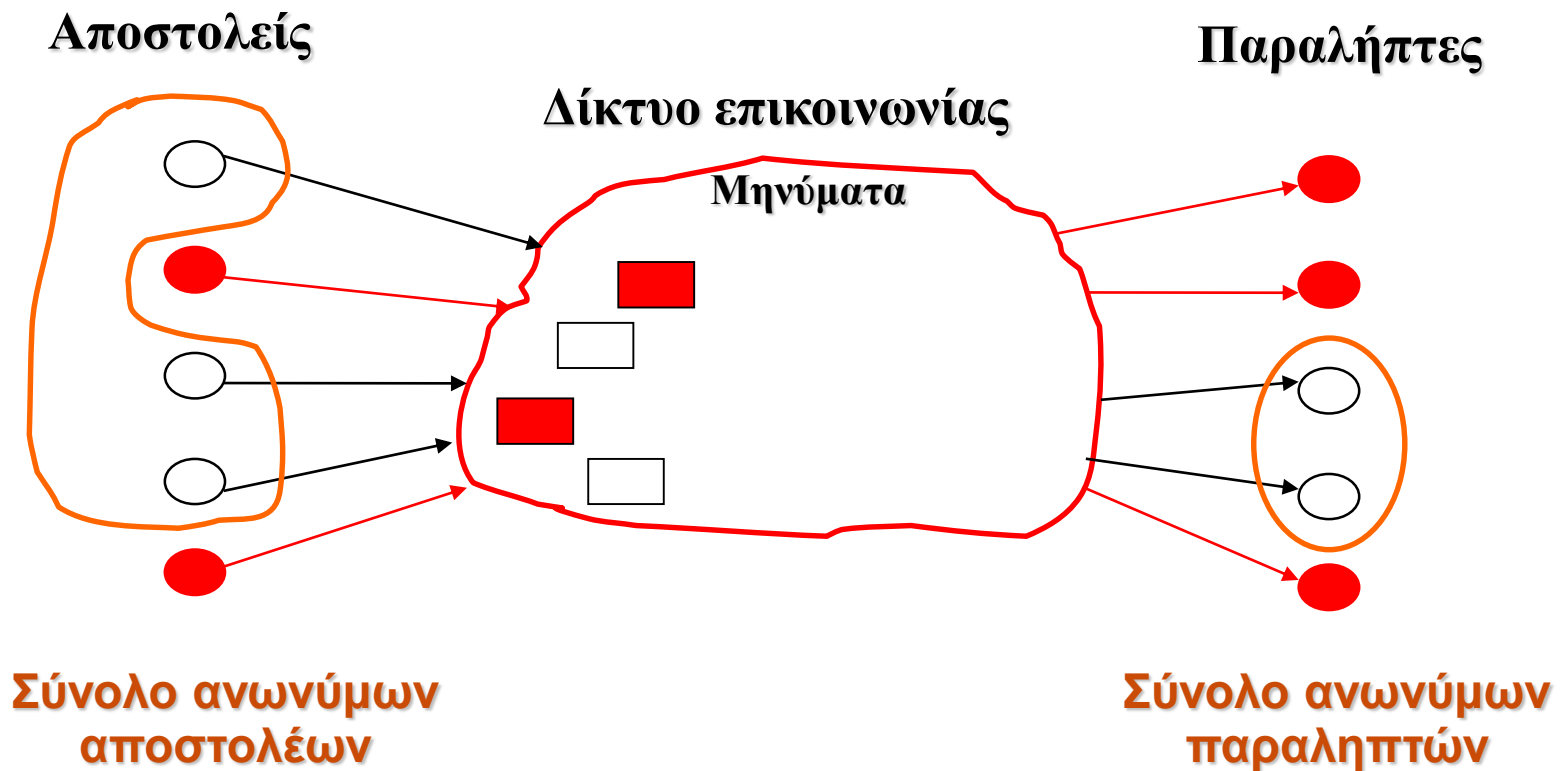
Μέγιστα εν δυνάμει σύνολα ανωνύμων οντοτήτων

83



Μέγιστα εν δυνάμει σύνολα ανωνύμων οντοτήτων σε σχέση με τους επιτιθέμενους

84



Μέγιστα εν δυνάμει σύνολα ανωνύμων
οντοτήτων σε σχέση με τους **επιτιθέμενους**

Η έννοια της μη-συνδεσιμότητας

Μη-συνδεσιμότητα (unlinkability) δύο τουλάχιστον IOIs στοιχείων ενδιαφέροντος (όπως ενεργές οντότητες, μηνύματα, συμβάντα), υπό την οπτική του επιτιθέμενου, σημαίνει ότι, εσωτερικά του συστήματος ο επιτιθέμενος δεν είναι σε θέση να συνάγει αν τα στοιχεία αυτά σχετίζονται μεταξύ τους

Η έννοια της μη-συνδεσιμότητας



(Ορισμός προσανατολισμένος στο χρήστη...) Η μη-συνδεσιμότητα εξασφαλίζει ότι ο χρήστης μπορεί να πραγματοποιήσει πολλαπλές χρήσεις δεδομένων και υπηρεσιών, χωρίς να είναι εφικτή από κάποιον τρίτο η σύνδεση των χρήσεων αυτών μεταξύ τους

Η μη-συνδεσιμότητα σημαίνει ότι χρήστες δεν είναι σε θέση να διαπιστώσουν αν ένας συγκεκριμένος χρήστης έχει λάβει μέρος σε συγκεκριμένες λειτουργίες εντός του συστήματος

Μη-συνδεσιμότητα: Ποσοτικοποίηση

87

- Όπως στην ανωνυμία και για την ποσοτικοποίηση της μη-συνδεσιμότητας μπορεί να γίνει χρήση της εντροπίας
- Για την ποσοτικοποίηση της μη-συνδεσιμότητας μπορεί να χρησιμοποιηθούν πιθανότητες, εντροπίες, ή οποιοδήποτε άλλο μέγεθος

Η έννοια της μη-ανιχνευσιμότητας

88

Μη-ανιχνευσιμότητα (undetectability) ενός στοιχείου ενδιαφέροντος (IOI), όπως ενεργή οντότητα, μήνυμα, συμβάν, υπό την οπτική του επιτιθέμενου, σημαίνει ότι ο επιτιθέμενος δεν είναι σε θέση να προσδιορίσει επακριβώς αν το στοιχείο υφίσταται ή όχι

Η έννοια της μη-ανιχνευσιμότητας

89

- Τέλεια μη-ανιχνευσιμότητα (perfect undetectability) ή Μέγιστη μη-ανιχνευσιμότητα (maximum undetectability) καταγράφεται όταν η ύπαρξη, ή μη, ενός ΙΟΙ στοιχείου που ενδιαφέρει είναι μη αναγνωρίσιμη, δηλαδή είναι απόλυτα δυσδιάκριτη

Η έννοια της Μη- παρατηρησιμότητας

90

Μη-παρατηρησιμότητα (unobservability) ενός ΙΟΙ στοιχείου που ενδιαφέρει, σημαίνει:

- και μη-ανιχνευσιμότητα του ΙΟΙ στοιχείου ενδιαφέροντος, σε σχέση με όλες τις οντότητες που δε σχετίζονται με αυτό
- και ανωνυμία των οντοτήτων που σχετίζονται με το ΙΟΙ στοιχείο ενδιαφέροντος, ακόμη και ενάντια σε άλλες οντότητες που σχετίζονται με το ίδιο στοιχείο

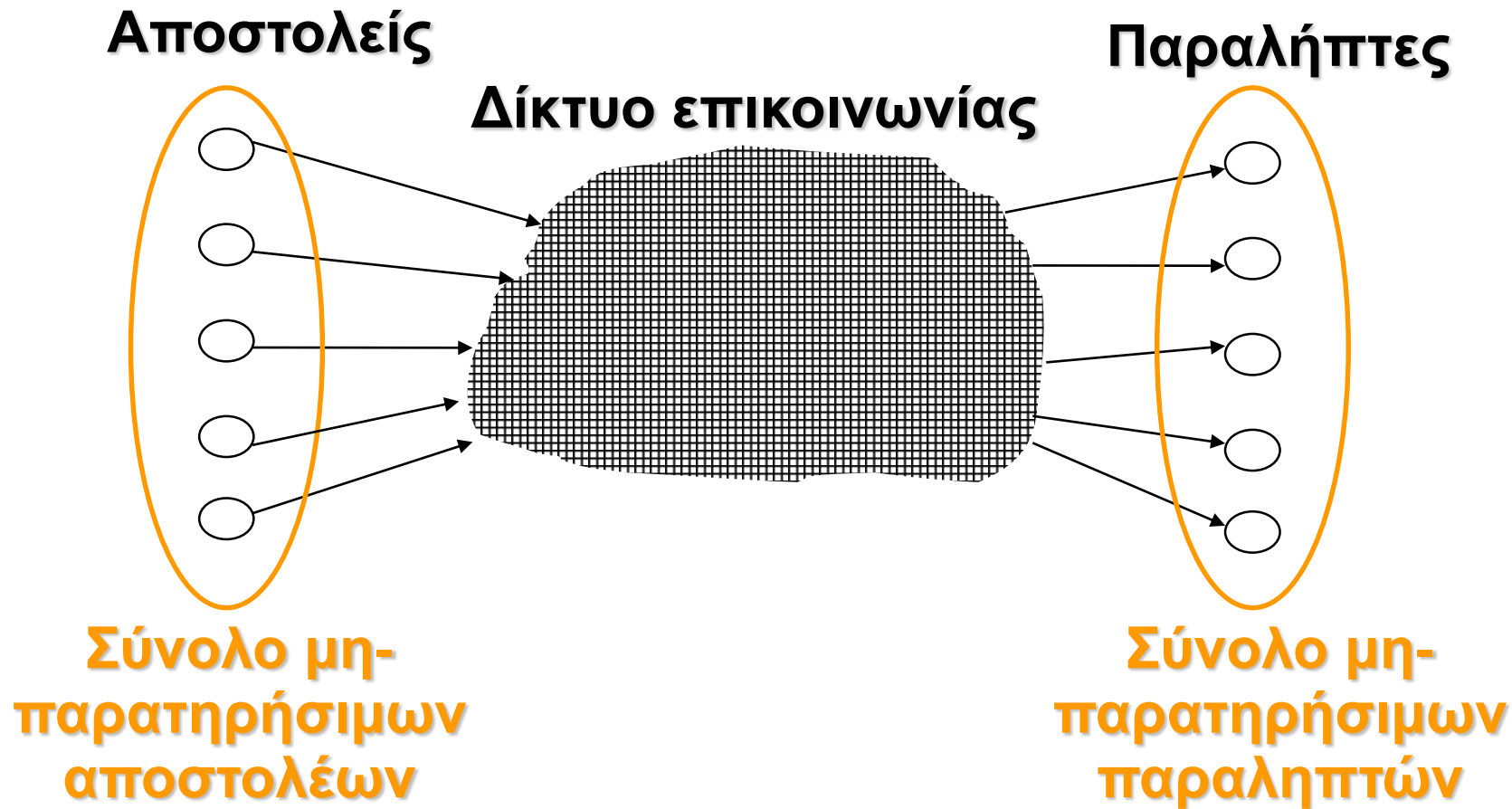
Η έννοια της Μη- παρατηρησιμότητας

91

- Η μη-παρατηρησιμότητα σημαίνει ότι καμία οντότητα δεν μπορεί να αντιληφθεί την πραγματοποίηση μιας διαδικασίας
- Η μη-παρατηρησιμότητα, πρακτικά, εξασφαλίζει ότι μία οντότητα μπορεί να έχει πρόσβαση σε δεδομένα ή υπηρεσίες χωρίς οποιασδήποτε άλλη οντότητα να μπορεί να αντιληφθεί ότι υπάρχει πρόσβαση από κάποιον στα δεδομένα ή στις υπηρεσίες αυτές
- Ο ορισμός αυτός είναι γενικός, καθώς αναφέρεται σε οποιοδήποτε IOI στοιχείο που ενδιαφέρει και περιγράφει τις συνθήκες επίτευξης μη παρατηρησιμότητας μέσω αποτροπής της αποκάλυψης IOIs

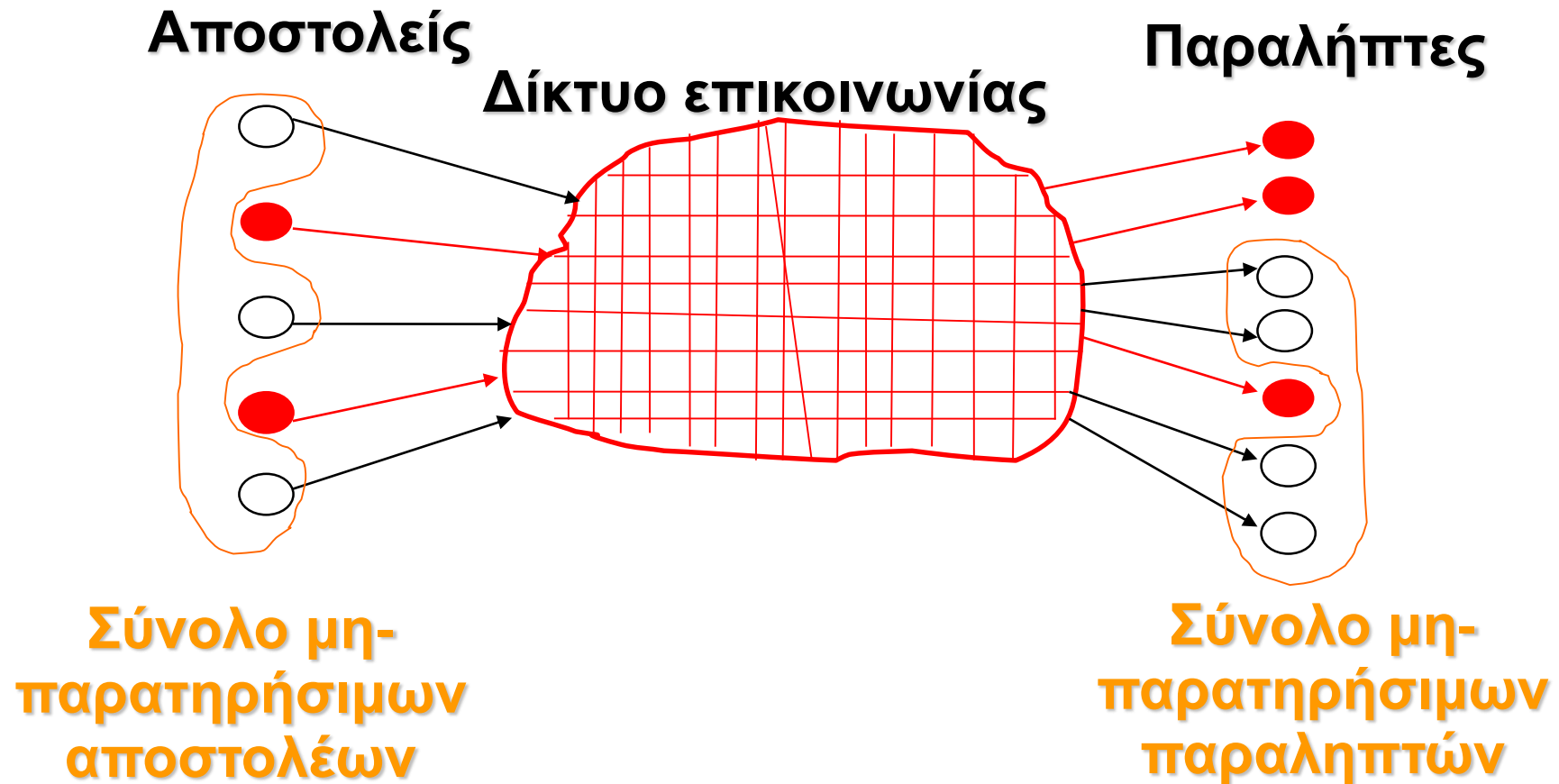
Μη-παρατηρησιμότητα: Μέγιστα εν δυνάμει σύνολα μη παρατηρήσιμων οντοτήτων

92



Μη-παρατηρησιμότητα: Μέγιστα εν δυνάμει σύνολα μη παρατηρήσιμων οντοτήτων

93



Μέγιστα εν-δυνάμει σύνολα μη-παρατηρησιμότητας σε
σχέση με τον **επιτιθέμενο**

Επισκόπηση βασικών ορισμών

94

Ανωνυμία μίας οντότητας (anonymity of a subject), υπό την οπτική του επιτιθέμενου, σημαίνει ότι ο επιτιθέμενος δεν μπορεί να προσδιορίσει επακριβώς την οντότητα μέσα σε ένα σύνολο οντοτήτων, το σύνολο των ενεργών οντοτήτων

Αναγνωρισιμότητα μίας οντότητας (identifiability of a subject), υπό την οπτική του επιτιθέμενου, αναφέρεται στην ικανότητά του να αναγνωρίσει την οντότητα ανάμεσα σε ένα σύνολο οντοτήτων, το σύνολο των αναγνωρίσιμων οντοτήτων

Μη-συνδεσιμότητα (unlinkability) δύο ή περισσότερων IOIs στοιχείων που ενδιαφέρουν (όπως ενεργές οντότητες, μηνύματα, συμβάντα), υπό την οπτική του επιτιθέμενου, σημαίνει ότι, εσωτερικά του συστήματος ο επιτιθέμενος δεν είναι σε θέση να συνάγει αν τα στοιχεία αυτά σχετίζονται μεταξύ τους

Συνδεσιμότητα (linkability) δύο ή περισσότερων IOIs στοιχείων που ενδιαφέρουν (όπως ενεργές οντότητες, μηνύματα, συμβάντα), υπό την οπτική του επιτιθέμενου, σημαίνει ότι εσωτερικά του συστήματος, ο επιτιθέμενος είναι σε θέση να συνάγει αν τα στοιχεία αυτά σχετίζονται μεταξύ τους

Επισκόπηση βασικών ορισμών

Μη-ανιχνευσιμότητα (undetectability) ενός ΙΟΙ στοιχείου που ενδιαφέρει (όπως ενεργή οντότητα, μήνυμα, συμβάν), υπό την οπτική του επιτιθέμενου, σημαίνει ότι ο επιτιθέμενος δεν είναι σε θέση να προσδιορίσει επακριβώς αν το στοιχείο υφίσταται ή όχι

Ανιχνευσιμότητα (detectability) ενός ΙΟΙ στοιχείου που ενδιαφέρει (όπως ενεργή οντότητα, μήνυμα, συμβάν), υπό την οπτική του επιτιθέμενου, σημαίνει ότι ο επιτιθέμενος είναι σε θέση να προσδιορίσει επακριβώς αν το στοιχείο υφίσταται ή όχι

Μη-παρατηρησιμότητα (unobservability) ενός ΙΟΙ στοιχείου που ενδιαφέρει, σημαίνει και μη-ανιχνευσιμότητα του ΙΟΙ στοιχείου που ενδιαφέρει, σε σχέση με όλες τις οντότητες που σχετίζονται με αυτό, και ανωνυμία των οντοτήτων που σχετίζονται με το ΙΟΙ στοιχείο που ενδιαφέρει, ακόμη και ενάντια σε άλλες οντότητες που σχετίζονται με το ίδιο στοιχείο

Σύνοψη

96

- ❑ Διαφοροποίηση των εννοιών ιδιωτικότητα, πληροφοριακή ιδιωτικότητα, απόρρητο, προστασία προσωπικών δεδομένων
- ❑ Τα όρια της ιδιωτικότητας μεταβάλλονται και εξελίσσονται σύμφωνα με ένα σύνολο παραγόντων
- ❑ Οι κανονιστικές ρυθμίσεις για την προστασίας προσωπικών δεδομένων ορίζουν τους κανόνες της επεξεργασίας/συναλλαγής
- ❑ Οι χρήστες εκφράζουν αυξανόμενες ανησυχίες για την προστασία της ιδιωτικότητάς τους

Βιβλιογραφία

97

- [1] Pew Research Center's Internet Project (2016), Privacy and Information Sharing, <http://www.pewinternet.org/2016/01/14/privacy-and-information-sharing/>
- [2] TRUSTe 2014 US Consumer Confidence Privacy Report (2014), TRUSTe <http://www.truste.com/us-consumer-confidence-index-2014/>
- [3] KPMG (2016), Crossing the line: Staying on the right side of consumer privacy, <https://home.kpmg.com/sg/en/home/insights/2016/11/crossing-the-line.html>
- [4] Pew Research Center's Internet Project (2016), Privacy and Information Sharing, <http://www.pewinternet.org/2016/01/14/privacy-and-information-sharing/>
- [5] Global Internet User Survey (2012), Internet Society <http://www.internetsociety.org/survey>
- [6] Ernst & Young (2016) Can privacy really be protected anymore? [http://www.ey.com/Publication/vwLUAssets/ey-can-privacy-really-be-protected-anymore/\\$FILE/ey-can-privacy-really-be-protected-anymore.pdf](http://www.ey.com/Publication/vwLUAssets/ey-can-privacy-really-be-protected-anymore/$FILE/ey-can-privacy-really-be-protected-anymore.pdf)