Ionian University
Department of Informatics

Ανάλυση απειλών Ιδιωτικότητας

Μεταπτυχιακό Πρόγραμμα Σπουδών: «Ψηφιακές Εφαρμογές και Καινοτομία»
Β’ τρίμηνο 2018-2019

Μάθημα: *Πολιτικές Ασφάλειας και Ιδιωτικότητας στο Διαδίκτυο*

Τρίτη, 7 Μαΐου 2019

Αγγελική Τσώχου – Επίκουρη Καθηγήτρια
Θάνος Παπαϊωάννου – Υποψήφιος Διδάκτορας

Διάρθρωση

- Θεωρητικό πλαίσιο - Εισαγωγή
- Διάγραμμα Ροής Δεδομένων – Microsoft Threat Modelling Tool
- Μεθοδολογία LINDDUN
- Μελέτη Περίπτωσης

1.
Θεωρητικό πλαίσιο

Η Ιδιωτικότητα ως προϋπόθεση

Η σημασία της προστασίας της Ιδιωτικότητας

Οι ανησυχίες για την Ιδιωτικότητα αυξάνονται

Μέχρι σήμερα

- Η προστασία της Ιδιωτικότητας αντιμετωπιζόταν ως ζήτημα, **αφού** προέκυπτε κάποιο πρόβλημα

Σήμερα

- **Privacy by Design**
  - Διαφορετική προσέγγιση: η Ιδιωτικότητα ως εγγενές συστατικό στη διαδικασία ανάπτυξης ενός λογισμικού

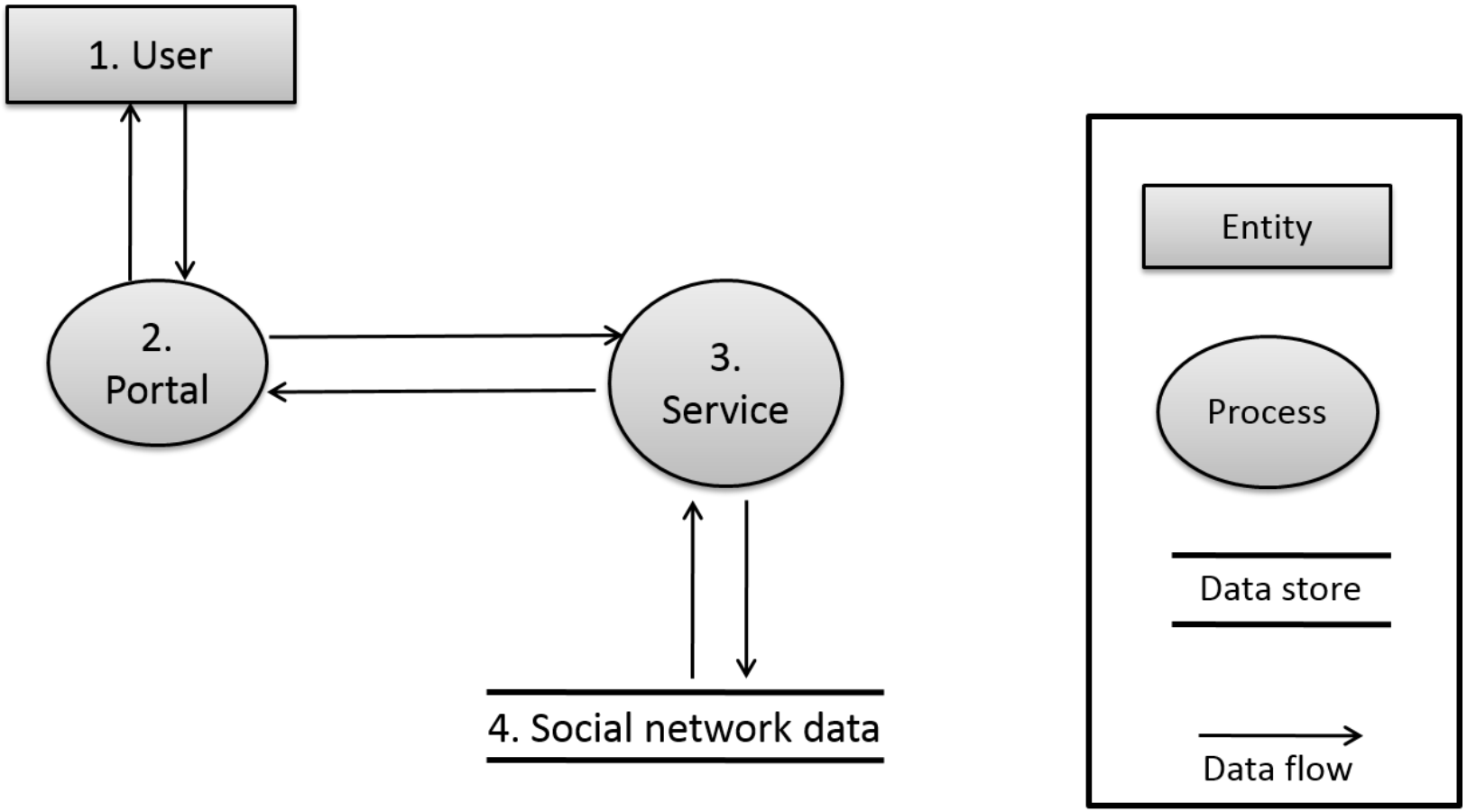
Μεθοδολογίες ανάλυσης απειλών Ιδιωτικότητας

- KAOS
- STRIDE
- PRIAM
- **LINDDUN**

Το Διάγραμμα Ροής Δεδομένων – Data Flow Diagram (DFD)

- Απαραίτητο στοιχείο στις μεθοδολογίες ανάλυσης απειλών **Ασφάλειας** και **Ιδιωτικότητας**, που βασίζονται σε μοντέλα
- Βάση για την ανάλυση:
  - Κάθε στοιχείο του διαγράμματος εξετάζεται συστηματικά και σε βάθος ως προς την ύπαρξη απειλών Ιδιωτικότητας

Ένα απλό Διάγραμμα Ροής Δεδομένων



2.
Microsoft Threat Modelling Tool 2016

Λειτουργία και χρήση

Microsoft Threat Modelling Tool

Λειτουργίες:

- Δημιουργία Διαγράμματος Ροής Δεδομένων
- Ανάλυση διαγράμματος σε πιθανές απειλές
- Πρόταση αντιμέτρων για να μειωθούν οι ευπάθειες από το σχεδιασμό
- Παραγωγή αναφορών σχετικά με τις απειλές που έχουν εντοπιστεί και αντιμετωπιστεί
- Δημιουργία προσαρμοσμένων υποδειγμάτων για τη μοντελοποίηση απειλών

Microsoft Threat Modelling Tool

Ένα μοντέλο για τις απειλές είναι:

1. Η αναπαράσταση του λογισμικού ή των συσκευών που περιλαμβάνει ένα σύστημα

2. Η ροή των δεδομένων ανάμεσα στα μέρη του συστήματος

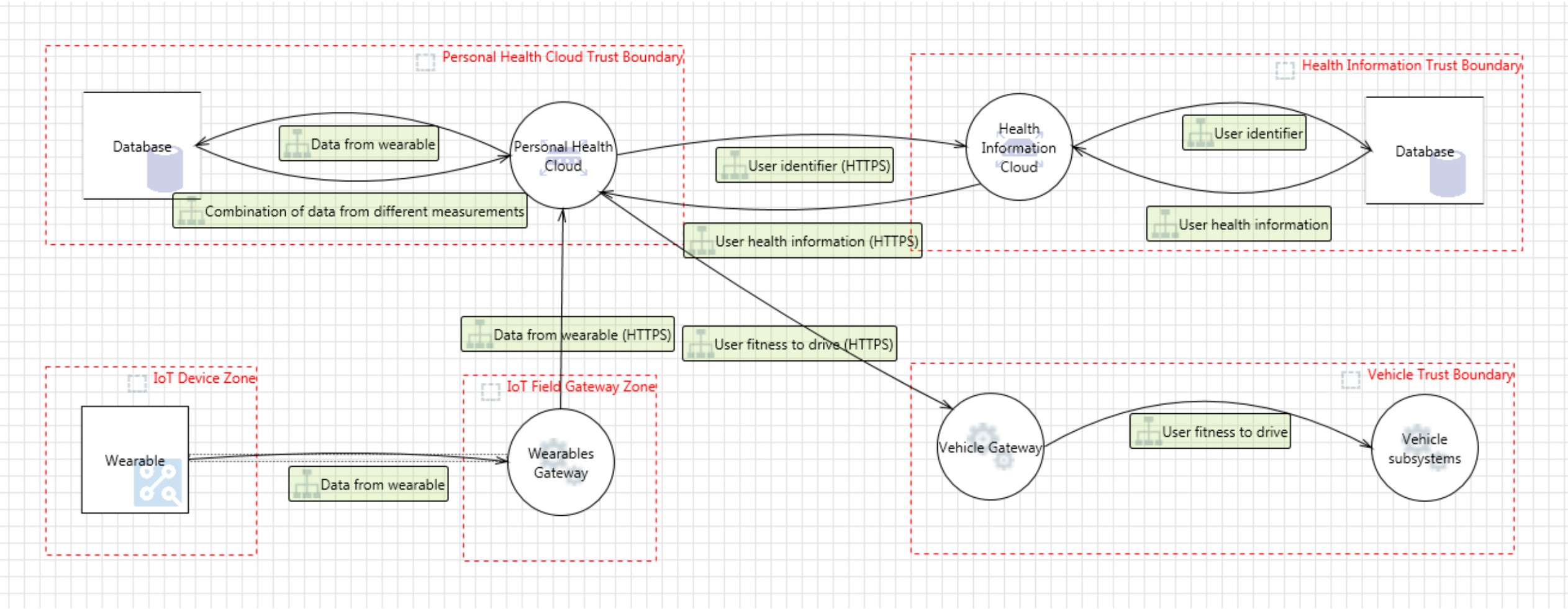
3. Τα «όρια εμπιστοσύνης» μέσα στο σύστημα (trust boundaries)

Microsoft Threat Modelling Tool

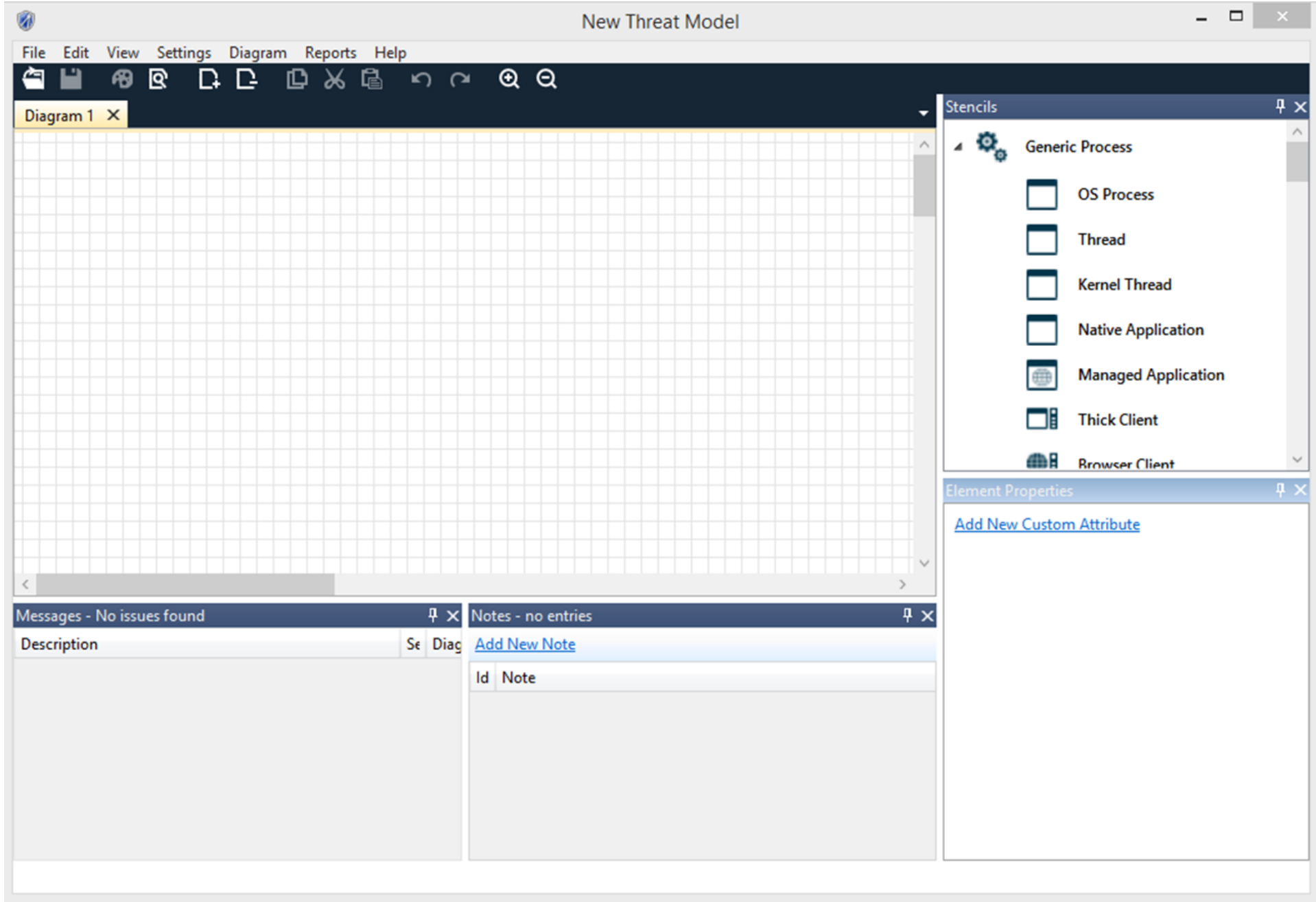
Με τη μοντελοποίηση των απειλών, αναλύονται οι ιδιότητες της ασφάλειας του συστήματος και προκύπτουν οι πιθανές ευπάθειες από το σχεδιασμό του.

Εφαρμόζεται **πριν** από τη δημιουργία και τη χρήση ενός προϊόντος ή μιας υπηρεσίας

Διασφαλίζονται οι προβλέψεις “**Privacy by Design**” και “Security by Design”


Personal Health Cloud Trust Boundary
Database
Data from wearable
Personal Health Cloud
Combination of data from different measurements
User identifier (HTTPS)
Health Information Cloud
Health Information Trust Boundary
User identifier
Database
User health information
User health information (HTTPS)
Data from wearable (HTTPS)
User fitness to drive (HTTPS)
IoT Device Zone
Wearable
Data from wearable
IoT Field Gateway Zone
Wearables Gateway
Vehicle Gateway
Vehicle Trust Boundary
User fitness to drive
Vehicle subsystems

Το περιβάλλον χρήσης και εργασίας



Τα βασικά σύμβολα

Οντότητα

Διεργασία

Αποθηκευτικός χώρος

Ροή Δεδομένων - Σύνδεση

Item	Symbol
Data flow	One way arrow
Data store	Two parallel horizontal lines
Process	Circle
Multi-process	Two concentric circles
Interactions	Rectangle
Trust boundary	Dotted line

3.
Η μεθοδολογία ανάλυσης απειλών ιδιωτικότητας LINDDUN

Δομή της μεθοδολογίας

Model-based

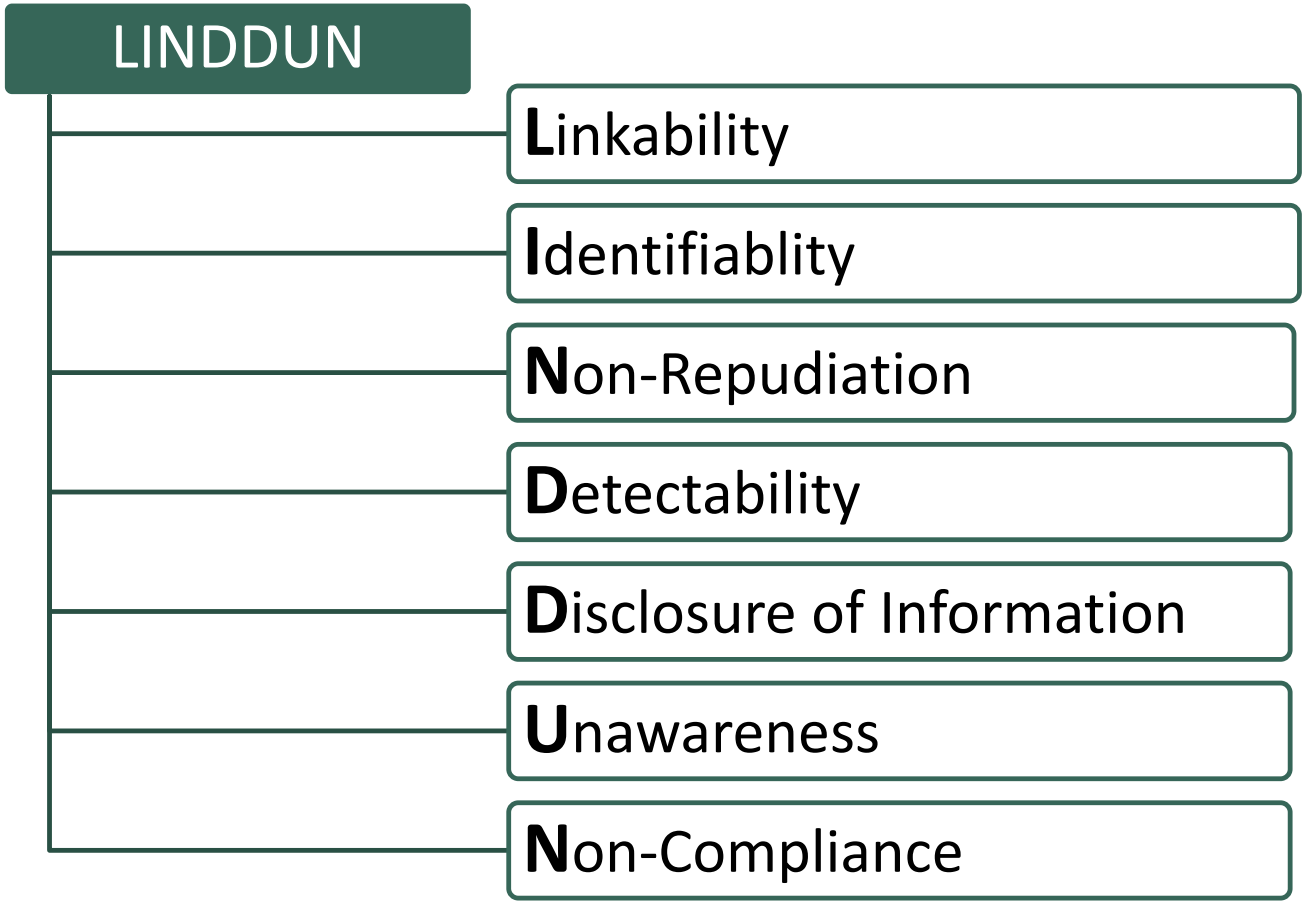
- Αξιοποιεί το διάγραμμα ροής δεδομένων, ως αναπαράσταση του συστήματος που θα αναλυθεί.

Knowledge-based

- Περιλαμβάνει τους πιο συνηθισμένους τύπους επίθεσης που σχετίζονται με το σύνολο των απειλών κατά της ιδιωτικότητας.

Το ακρωνύμιο LINDDUN

Οι κατηγορίες των απειλών κατά της Ιδιωτικότητας

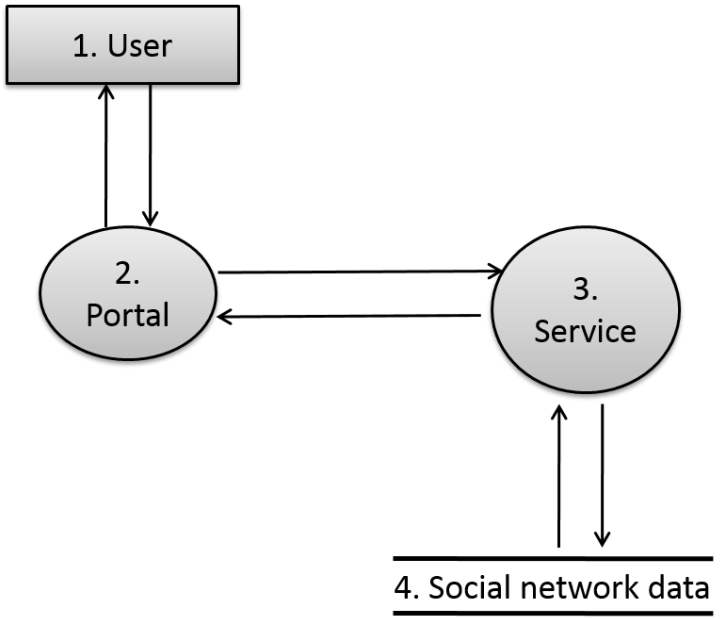


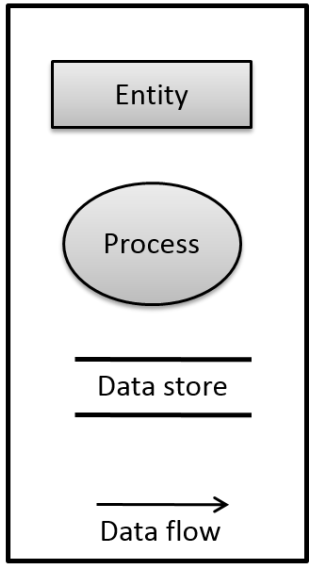
Linkability **Συνδεσιμότητα**	Ο επιτιθέμενος μπορεί να διακρίνει επαρκώς αν δύο αντικείμενα ενδιαφέροντος σχετίζονται ή όχι
Identifiability **Αναγνωρισιμότητα**	Ο επιτιθέμενος μπορεί να προσδιορίσει επαρκώς το υποκείμενο μέσα σε ένα σύνολο υποκειμένων
Non-Repudiation **Μη αποποίηση (ευθύνης)**	Ο επιτιθέμενος λαμβάνει αποδεικτικά στοιχεία σχετικά με την εμφάνιση (ή μη) ενός συμβάντος ή μιας ενέργειας
Detectability **Ανιχνευσιμότητα**	Ο επιτιθέμενος μπορεί να διακρίνει επαρκώς αν ένα αντικείμενο ενδιαφέροντος υπάρχει ή όχι
Disclosure of Information **Εμπιστευτικότητα** (Confidentiality)	Περιορισμοί στην πρόσβαση και αποκάλυψη πληροφοριών - Μέσα για την προστασία της ιδιωτικότητας
Unawareness **Άγνοια**	Ο χρήστης δεν γνωρίζει τις συνέπειες όταν διαμοιράζεται πληροφορίες και προσωπικά δεδομένα
Non-Compliance **Μη Συμμόρφωση**	Παρόλο που το σύστημα εμφανίζει τις πολιτικές απορρήτου στους χρήστες, δεν υπάρχει καμία εγγύηση ότι το σύστημα συμμορφώνεται πραγματικά με τις πολιτικές αυτές

Τα βήματα της μεθοδολογίας

Μετά το διάγραμμα: Καταγραφή των μερών του συστήματος

Entity	User
Process	Portal
	Social Network service
Data Store	Social Network Database
Data Flow	User Data stream (user-portal)
	Service data stream (portal-service)
	Database data stream (service-database)





2ο Βήμα: Αντιστοίχιση απειλών ιδιωτικότητας με τα στοιχεία του διαγράμματος ροής δεδομένων

Step 2: Map threats to DFD elements

MAPPING TEMPLATE	LINDDUN PRIVACY BY DESIGN	Linkability	Identifiability	Non-repudiation	Detectability	Information Disclosure	Content Unawareness	Policy & Consent Non-compliance
	Data store	X	X	X	X	X		X
	Data flow	X	X	X	X	X		X
	Process	X	X	X	X	X		X
	Entity	X	X				X	

3ο βήμα: Αναγνώριση σεναρίων απειλών

- Το αποτέλεσμα της παραπάνω διαδικασίας θα πρέπει να είναι μια συλλογή από σενάρια απειλών που πρέπει να καταγραφούν.
- Συνήθως χρησιμοποιούνται ενδεικτικές περιπτώσεις κατάχρησης από έναν επιτιθέμενο
- Ως επιτιθέμενος, θεωρείται αυτός που προκαλεί την περίπτωση κατάχρησης, είτε σκόπιμα, είτε ακούσια

5ο βήμα: Ορισμός στρατηγικών αντιμετώπισης
6ο βήμα: Επιλογή αντίστοιχων PETs

- Κάθε περίπτωση κατάχρησης αντιστοιχεί με μια απαίτηση για την προστασία της ιδιωτικότητας
- Κάθε απαίτηση οδηγεί σε μια αντίστοιχη στρατηγική αντιμετώπισης/επίλυσης
- Η λίστα που θα προκύψει καταγράφεται σε πίνακα με την παρακάτω μορφή:

No.	Misuse cases	Privacy requirements	Suggested mitigation strategies and techniques
1	Linkability of social network data store	Unlinkability of data entries within the social network database	Apply data anonymization techniques, such as k-anonymity [67]
		Protection of data store	Enforce data protection by means of relationship-based access control [79]

4.
Μελέτη Περίπτωσης
«Αυτόνομη Οδήγηση: ***Ικανότητα οδηγού»***

Πλαίσιο

- Αξιολόγηση της κατάστασης της υγείας ενός οδηγού
- Με ποιο τρόπο η κατάσταση της υγείας μπορεί να επηρεάσει την ικανότητα οδήγησης ενός (αυτοματοποιημένου) αυτοκινήτου με ασφάλεια;

Σενάριο

- Ένας ιδιοκτήτης και οδηγός ενός (αυτοματοποιημένου) αυτοκινήτου χρησιμοποιεί συσκευές (wearables), οι οποίες παρακολουθούν τις ζωτικές ενδείξεις αλλά και πιο λεπτομερείς παραμέτρους της υγείας σε συνθήκες καθημερινής ζωής (π.χ. περπάτημα, εργασία, οδήγηση, δραστηριότητες κτλ.)
- Οι συσκευές αυτές μπορούν να εκτιμήσουν το κατά πόσο είναι ικανός να οδηγήσει ένα αυτοκίνητο με ασφάλεια (π.χ. σε περίπτωση υπνηλίας ή ιλίγγου)
- Τα δεδομένα που συλλέγουν οι συσκευές αξιοποιούνται με ασφάλεια μέσα σε ειδικά συστήματα του αυτοκινήτου
- Ένας εξελιγμένος «πλοηγός» του αυτοκινήτου θα μπορούσε να χρησιμοποιήσει αυτά τα δεδομένα για να λάβει αποφάσεις για την οδήγηση (π.χ. να προσαρμόσει την απόσταση από το προπορευόμενο αυτοκίνητο, να αυξήσει την εγρήγορση του οδηγού κτλ.)

Εμπλεκόμενα μέρη

1. Οδηγός/ιδιοκτήτης του αυτοκινήτου
2. Αυτοκίνητο
3. Φορητές συσκευές παρακολούθησης της κατάστασης της υγείας (wearables)
4. Σύννεφο (επεξεργασία και αποθήκευση δεδομένων του οδηγού)
5. Υποδομές επικοινωνίας

Υποδομές – στοιχεία και συνδέσεις του συστήματος

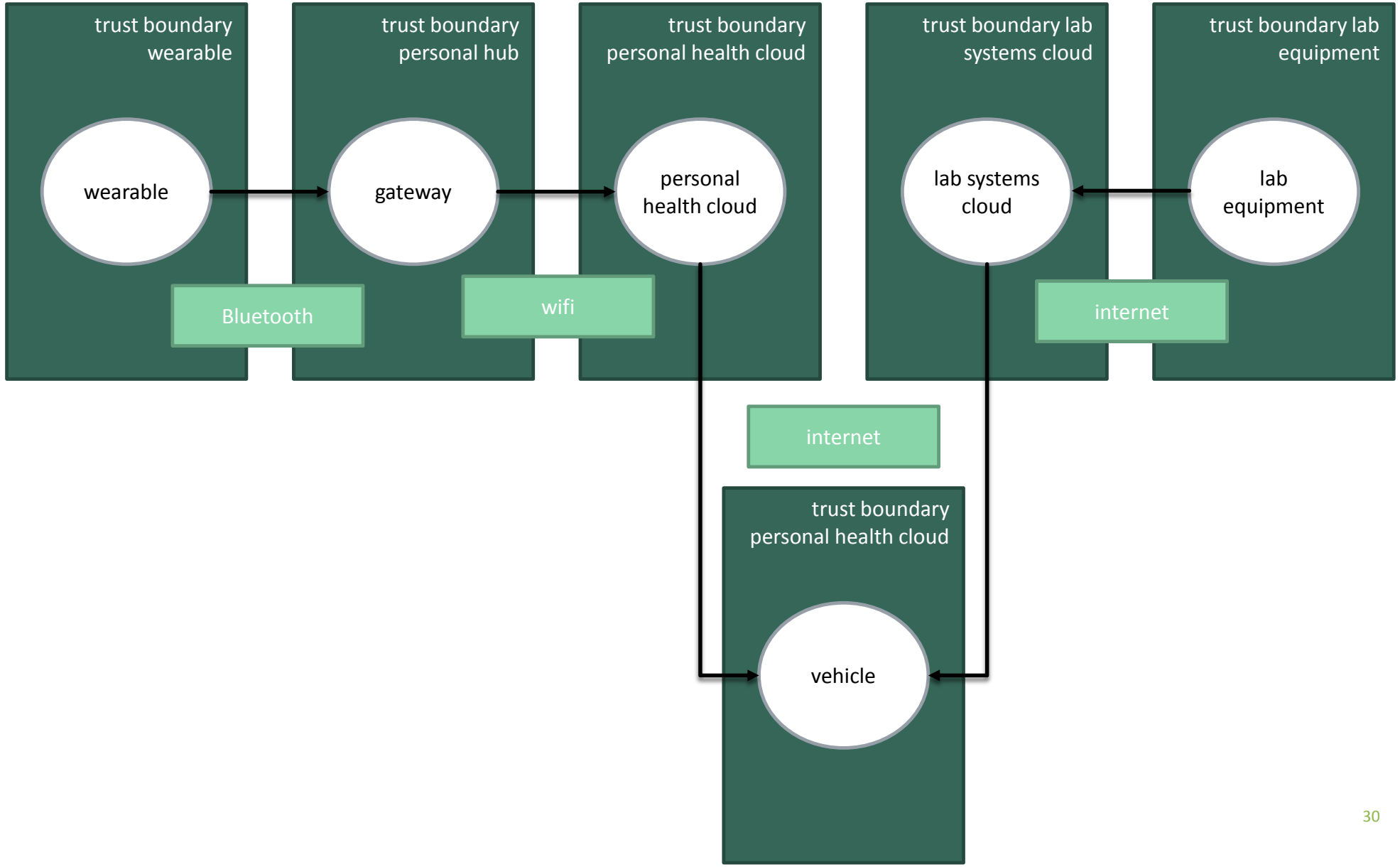
1. Ο οδηγός φοράει τις φορητές συσκευές
2. Οι φορητές συσκευές επικοινωνούν με την Υπηρεσία Υγείας («σύννεφο»)
3. Τα αυτοκίνητα επικοινωνούν με την Υπηρεσία Υγείας («σύννεφο»)
4. Τα δεδομένα που αφορούν στην ικανότητα του οδηγού είναι διαθέσιμα στα συστήματα του αυτοκινήτου

Εκτέλεση σεναρίου

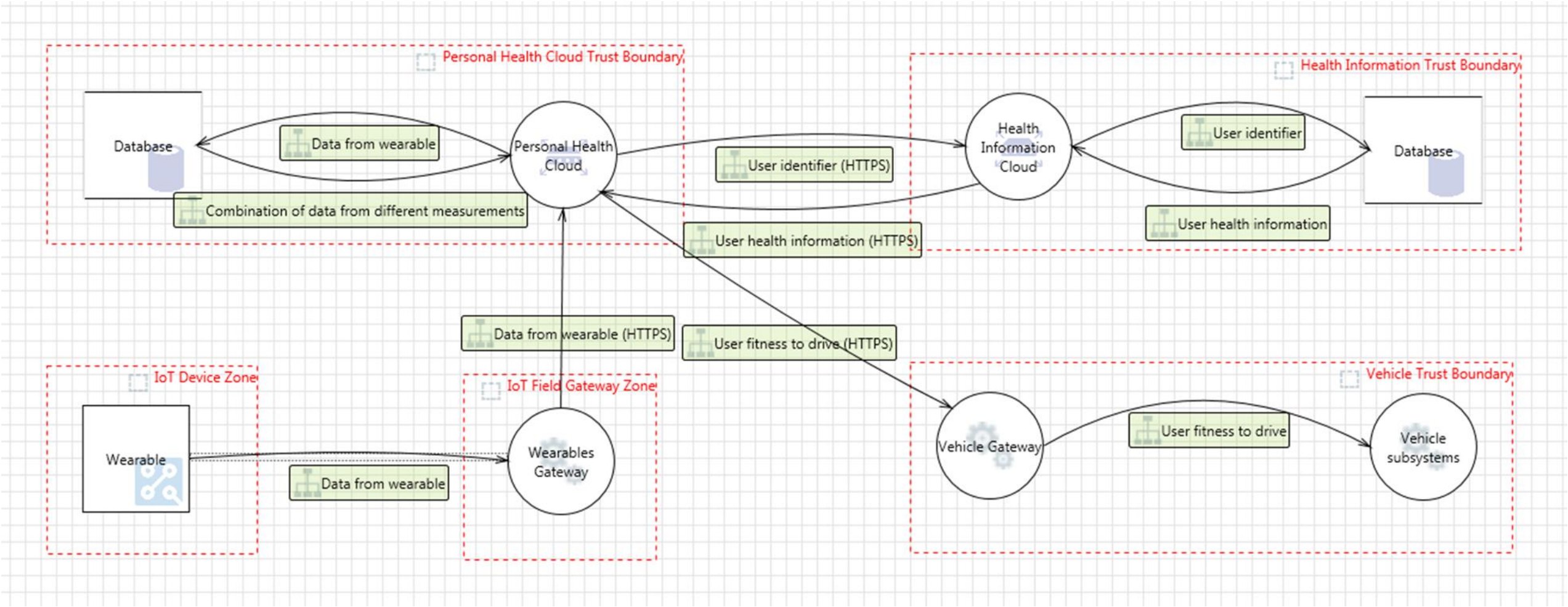
1. Ο οδηγός φοράει καθημερινά τις φορητές συσκευές μέτρησης δεδομένων υγείας
2. Τα δεδομένα της υγείας του «ανεβαίνουν» και αποθηκεύονται στο σύννεφο σε τακτική βάση
3. Η κατάσταση της υγείας του οδηγού αξιολογείται με βάση τα παραπάνω δεδομένα
4. Η υπηρεσία στο «σύννεφο» εκτιμά την ικανότητα του ατόμου να οδηγεί το αυτοκίνητο
5. Η υπηρεσία στο «σύννεφο» διαβιβάζει τα δεδομένα στο αυτοκίνητο
6. Το αυτοκίνητο λαμβάνει τα δεδομένα για την ικανότητα του οδηγού, τα διαμοιράζει στα υποσυστήματά του και λαμβάνονται πιθανές αποφάσεις.

Εκτέλεση σεναρίου

Σχήμα



Διάγραμμα Ροής Δεδομένων – Data Flow Diagram



Καταγραφή των μερών του συστήματος

Entity	Driver / Car's owner
Process	Wearables Gateway
	Personal Health Cloud (PHC)
	Health Information Cloud (HIC)
	Vehicle Gateway
	Vehicle Subsystems
Data Store	Personal Health Cloud database
	Health Information Cloud database
Data flow	Wearable – Wearable Gateway
	Wearable - Personal Health Cloud
	Personal Health Cloud - Personal Health Cloud database
	Personal Health Cloud - Health Information Cloud
	Health Information Cloud – Health Information Cloud database
	Personal Health Cloud - Vehicle Gateway
	Vehicle Gateway- Vehicle Subsystems

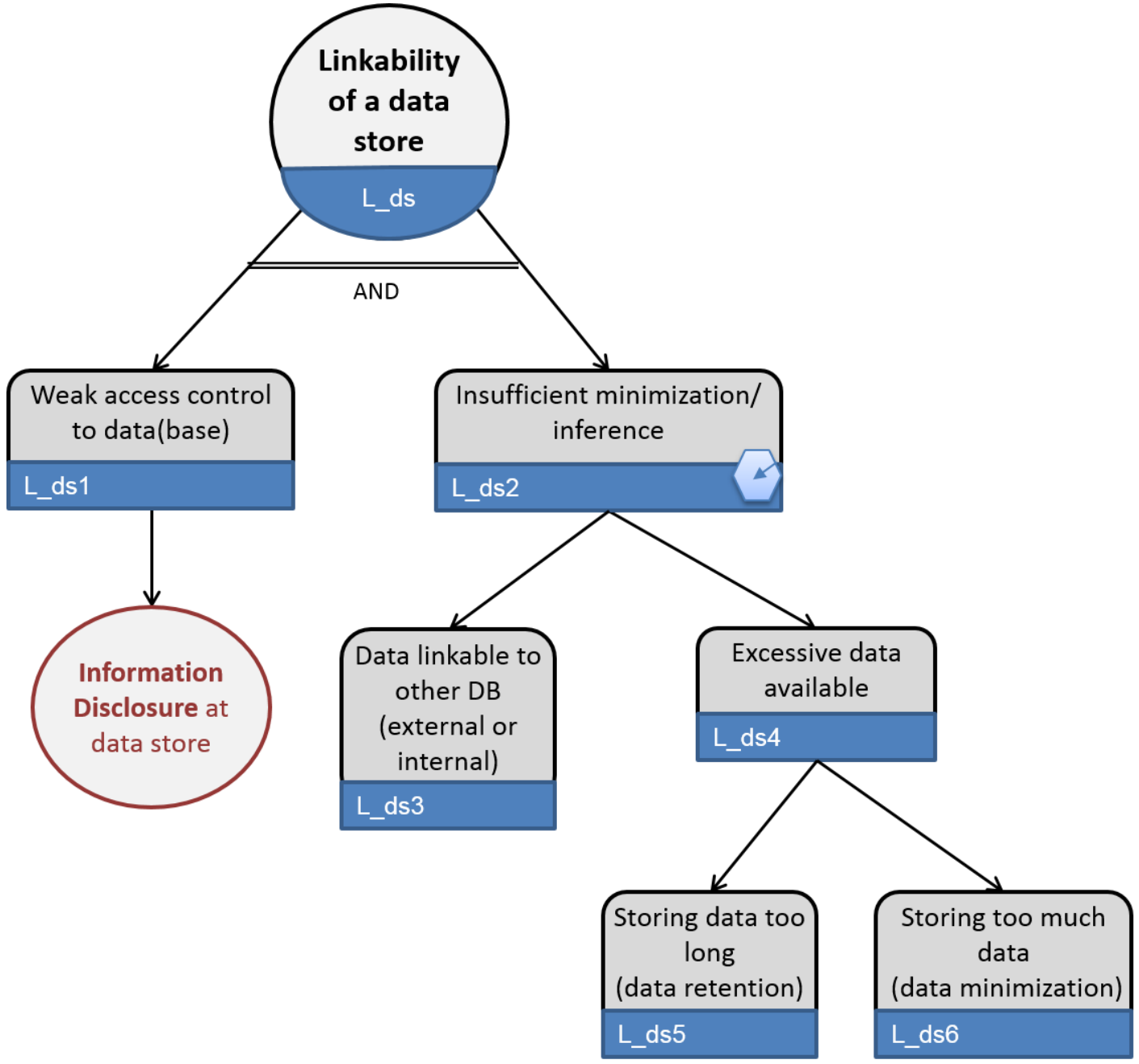
Αντιστοίχιση απειλών ιδιωτικότητας με τα στοιχεία του διαγράμματος ροής δεδομένων

	Threat target	L	I	N	D	D	U	N
Data Store	Personal Health Cloud (PHC)	1	5	X	X	10		15
	Health Information Cloud (HIC)	2	6	X	X	11		15
Data Flow	Wearable-wearable gateway	3	X	X	X	X		15
	Wearable - Personal Health Cloud	X	X	X	X	X		15
	Personal Health Cloud - Personal Health Cloud database	X	X	X	X	X		15
	Personal Health Cloud - Health Information Cloud	X	7	X	X	12		15
	Health Information Cloud – Health Information Cloud database	X	8	X	X	13		15
	Personal Health Cloud - Vehicle Gateway	X	X	X	X	X		15
	Vehicle Gateway- Vehicle Subsystems	X	X	X	X	X		15
Process	Wearables Gateway	X	X	X	X	X		15
	Personal Health Cloud (PHC)	X	X	X	X	X		15
	Health Information Cloud (HIC)	X	X	X	X	X		15
	Vehicle Gateway	X	X	X	X	X		15
	Vehicle Subsystems	X	X	X	X	X		15
Entity	Driver / Car’s owner	4	9				14	

Αναγνώριση σεναρίων απειλών

No.	Misuse cases	Indicative Misuse Scenarios
1	Linkability of Personal Health Cloud database	The database entries of the cloud provider are weakly anonymized, and an attacker exploits weak access control to associate driver's health data with his/her identity.
3	Linkability of data flow of Wearable - Wearable gateway	The communication between wearable and its gateway is unprotected and an attacker reveals linkable information from the content of the communication.
		The communication between wearable and its gateway is non-anonymous and the attacker links data flow based on contextual data (e.g. session ID, identifier and biometrics) in order to associate information about the driver.
		The anonymity system that is being used for the communication between wearable and its gateway is insecure and the attacker can analyze the traffic to extract information out of patterns of traffic in order to link the driver's activity.
5	Linkability of entities – Driver / Car's owner	An attacker can associate the driver's identity and his/her car by linking PII based on factors (e.g. IP address, session ID, biometrics, location, time, frequency or any combination of these factors) exploiting access to his/her Personal Health Cloud storage
		An attacker can associate a car's registration number with its owner's identity by linking PII based on factors (e.g. IP address, session ID, biometrics, location, time, frequency or any combination of these factors) exploiting access to his/her Personal Health Cloud storage.

«Δέντρα» απειλών ιδιωτικότητας



Βιβλιογραφία

1. Deng, M., Wuyts, K., Scandariato, R., Preneel, B., & Joosen, W. (2011). A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements. *Requirements Engineering*, *16*(1), 3-32.
2. Microsoft, "Improving web application security: Threats and countermeasures," [Online]. Available: https://msdn.microsoft.com/en-us/library/aa302419.aspx#c03618429_011.
3. A. Pfitzmann and M. Hansen, "A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management, v0.34," 2010.
4. Danezis G (2008) Talk: an introduction to u-prove privacy protection technology, and its role in the identity metasystem—what future for privacy technology.
5. NIST, "Risk management guide for information technology systems, special publication 800-30," [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf.
6. K. Wuyts, R. Scandariato and W. Joosen, "Empirical evaluation of a privacy-focussed threat modeling methodology," The Journal of Systems and Software, vol. 96, pp. 122-138, 2014.
7. G. Sindre and A. L. Opdahl, "Eliciting security requirements with misuse cases," *Requirements Engineering,* vol. 10, no. 1, pp. 34-44, 2005.
8. S. Patil and A. Kobsa, "Privacy Considerations in Awareness Systems: Designing with Privacy in Mind," in Human-Computer Interaction Series, Springer, 2009, pp. 187-206.

Ionian University
Department of Informatics

Σας ευχαριστούμε πολύ