

ΑΝΑΛΥΣΗ ΑΠΕΙΛΩΝ ΙΔΙΩΤΙΚΟΤΗΤΑΣ

## ΒΑΣΙΣΜΕΝΗ ΣΤΑ ΑΝΤΙΣΤΟΙΧΑ ΒΗΜΑΤΑ της ΜΕΘΟΔΟΛΟΓΙΑΣ LINDDUN

### ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΗΣ: **ΑΥΤΟΝΟΜΗ ΟΔΗΓΗΣΗ**

Λαμβάνοντας υπόψη τη μεθοδολογία LINDDUN, την περιγραφή της μελέτης περίπτωσης και το συνημμένο ενδεικτικό διάγραμμα ροής δεδομένων, επισημαίνονται τα παρακάτω:

1. Οτιδήποτε δεν αναφέρεται ρητά στην περιγραφή της μελέτης περίπτωσης, δεν αποτελεί απαραίτητο στοιχείο για να συμπεριληφθεί, εκτός και αν η ύπαρξή του εξάγεται εύκολα από τα συμφραζόμενα.
2. Σε περιπτώσεις περιγραφής μελέτης περίπτωσης, η εφαρμογή της μεθοδολογίας LINDDUN δεν αποφέρει ένα μοναδικό συνδυασμό (μοναδική «λύση»), καθώς όλα εξαρτώνται από την ερμηνεία της περιγραφής. Συνεπώς, στο διάγραμμα και την καταγραφή του σε πίνακα, υφιστάμενα μέρη του συστήματος μπορούν να επεκταθούν, η/και να προστεθούν νέα, ώστε να υπάρχει λεπτομερέστερη αποτύπωση της σκέψης. Ωστόσο, αυτό δεν σημαίνει ότι μπορούμε να παραλείψουμε ή να παραβλέψουμε όσα μέρη αναφέρονται ρητά και συνδέονται με ανάλογες απειλές.
3. Η συμπερίληψη της Βάσης Δεδομένων ΣΔΚ, που αναγράφεται στους πίνακες και το διάγραμμα, εμπίπτει στην παραπάνω επισήμανση. Δεν αναγράφεται στην περιγραφή της μελέτης περίπτωσης, όμως μπορεί να συμπεριληφθεί καθώς ένα σύστημα που διαχειρίζεται την κυκλοφορία, θα πρέπει να έχει κάποιο αποθηκευτικό χώρο ώστε να εξάγει συμπεράσματα για το φόρτο κίνησης, με βάση παλιότερα δεδομένα.
4. Στην περιγραφή της μελέτης περίπτωσης αναφέρεται ρητά ότι το Σύστημα Προειδοποίησης Οχήματος επικοινωνεί με τα άλλα οχήματα που χρησιμοποιούν το ίδιο σύστημα, τους Ευάλωτους Χρήστες του δρόμου αλλά οι δύο τελευταίοι μεταξύ τους. Για λόγους πληρέστερης ενημέρωσης και προειδοποίησης επικοινωνούν όλοι με όλους και όχι μόνο με το ΣΠΟ του οχήματος έκτακτης ανάγκης.
5. Η απειλή ανιχνευσιμότητας σχετίζεται με το γεγονός ότι στην κυκλοφορία των δεδομένων υπάρχει ένα σήμα που διαφέρει από τα υπόλοιπα (έκτακτη ανάγκη).
6. Στη στήλη Άγνοιας του χρήστη (Unawareness), θα μπορούσε να προστεθεί μια απειλή στην οντότητα «Ευάλωτος Χρήστης του δρόμου». Η wearable συσκευή συνήθως επικοινωνεί τα δεδομένα μέσω Bluetooth προς το gateway, το οποίο σημαίνει ότι ο χρήστης θα πρέπει να γνωρίζει ότι χρειάζεται να μεγιστοποιήσει την ασφάλεια με ένα ισχυρό κωδικό. Η απειλή δεν συμπεριλαμβάνεται στον πίνακα επειδή δεν αναφέρονται στην περιγραφή ρητά οι λεπτομέρειες λειτουργίας αυτού του μέρους του συστήματος.
7. Οι απειλές συνδεσιμότητας και αναγνωρισιμότητας δεν εξαρτώνται αποκλειστικά από τον τρόπο σύνδεσης των μερών του συστήματος (HTTPS, V2X κτλ) αλλά και από το περιεχόμενο των δεδομένων που κυκλοφορούν στο σύστημα.

# ΣΤΟΙΧΕΙΑ ΔΙΑΓΡΑΜΜΑΤΟΣ ΡΟΗΣ ΔΕΔΟΜΕΝΩΝ

**Πίνακας 1**

|  |  |
| --- | --- |
| Οντότητα | Οδηγός Οχήματος Έκτακτης Ανάγκης |
|  | Οδηγοί άλλων οχημάτων |
|  | Ευάλωτοι χρήστες του δρόμου |
|  | Διαχειριστής υπηρεσίας Παρακολούθησης Οδικής Κυκλοφορίας (ΠΟΚ - ΕΦΚ) |
| Διεργασία | Παρακολούθηση Οδικής Κυκλοφορίας (**ΠΟΚ**) |
|  | Ελεγκτές Φαναριών Κυκλοφορίας (**ΕΦΚ**) |
|  | Σύστημα Διαχείρισης Κυκλοφορίας (**ΣΔΚ**) |
|  | Υπηρεσία Εξυπηρέτησης Έκτακτης Ανάγκης (**ΥΕΕΑ**) |
|  | Σύστημα Προειδοποίησης Οχήματος (**ΣΠΟ**) (Όχημα Έκτακτης Ανάγκης) |
|  | Σύστημα Προειδοποίησης Οχήματος (**ΣΠΟ**) (άλλα οχήματα) |
|  | Συσκευή **Wearable** (gateway) |
| Αποθήκευση Δεδομένων | Βάση Δεδομένων Συστήματος Διαχείρισης Κυκλοφορίας |
| Ροή Δεδομένων | Παρακολούθηση Οδικής Κυκλοφορίας – Ελεγκτές Φαναριών Κυκλοφορίας |
|  | Παρακολούθηση Οδικής Κυκλοφορίας – Σύστημα Διαχείρισης Κυκλοφορίας |
|  | Ελεγκτές Φαναριών Κυκλοφορίας - Σύστημα Διαχείρισης Κυκλοφορίας |
|  | Σύστημα Διαχείρισης Κυκλοφορίας – Ελεγκτές Φαναριών Κυκλοφορίας |
|  | Σύστημα Διαχείρισης Κυκλοφορίας – Υπηρεσία Εξυπηρέτησης Έκτακτης Ανάγκης |
|  | Υπηρεσία Εξυπηρέτησης Έκτακτης Ανάγκης - Σύστημα Διαχείρισης Κυκλοφορίας |
|  | Υπηρεσία Εξυπηρέτησης Έκτακτης Ανάγκης – Σύστημα Προειδοποίησης Οχήματος |
|  | Σύστημα Προειδοποίησης Οχήματος (έκτακτης ανάγκης) – Σύστημα Προειδοποίησης Οχήματος |
|  | Σύστημα Προειδοποίησης Οχήματος (έκτακτης ανάγκης) – Συσκευή Wearable |
|  | Σύστημα Προειδοποίησης Οχήματος (άλλα οχήματα) – Συσκευή Wearable |

# Determining Privacy Threats for DFD elements within the Use SubCase 1.4

**Πίνακας 2.** (από αριστερά προς τα δεξιά: L-Linkability, I-Identifiability, N-Non Repudiation, D-Detectability, D-Information Disclosure, U-Content Unawareness, N-Consent/policy Noncompliance)

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Threat target | L | I | N | D | D | U | N |
| Αποθήκευση Δεδομένων | Βάση Δεδομένων ΣΔΚ | X | X | X | 11 | X |  | 16 |
| Ροή  | ΠΟΚ - ΕΦΚ | X | Χ | X | X | X |  | 16 |
| Δεδομένων | ΠΟΚ - ΣΔΚ | X | 5 | X | X | X |  | 16 |
|  | ΕΦΚ - ΣΔΚ | X | X | X | X | X |  | 16 |
|  | ΣΔΚ - ΕΦΚ | X | X | X | 12 | X |  | 16 |
|  | ΣΔΚ – Βάση Δεδομένων ΣΔΚ | Χ | Χ | Χ | Χ | Χ |  | 16 |
|  | ΣΔΚ - ΥΕΕΑ | 1 | Χ | X | X | X |  | 16 |
|  | ΥΕΕΑ - ΣΔΚ | 2 | 6 | X | 13 | X |  | 16 |
|  | ΥΕΕΑ – ΣΠΟ (έκτακτης ανάγκης) | Χ | X | X | X | X |  | 16 |
|  | ΣΠΟ (έκτακτης ανάγκης) – ΣΠΟ | X | X | X | Χ | 14 |  | 16 |
|  | ΣΠΟ (έκτακτης ανάγκης) – Συσκευή Wearable | X | 7 | X | X | 15 |  | 16 |
|  | ΣΠΟ (άλλα οχήματα) – Συσκευή Wearable | Χ | 8 | Χ | Χ | 15 |  | 16 |
| Διεργασία | Παρακολούθηση Οδικής Κυκλοφορίας (**ΠΟΚ**) | X | X | X | X | X |  | 16 |
|  | Ελεγκτές Φαναριών Κυκλοφορίας (**ΕΦΚ**) | X | X | X | X | X |  | 16 |
|  | Σύστημα Διαχείρισης Κυκλοφορίας (**ΣΔΚ**) | X | X | X | X | X |  | 16 |
|  | Υπηρεσία Εξυπηρέτησης Έκτακτης Ανάγκης (**ΥΕΕΑ**) | X | X | X | X | X |  | 16 |
|  | **ΣΠΟ** (έκτακτης ανάγκης) | X | X | X | X | X |  | 16 |
|  | **ΣΠΟ (**άλλα οχήματα) | Χ | Χ | Χ | Χ | Χ |  | 16 |
|  | Συσκευή **Wearable** (gateway) | X | X | X | X | X |  | 16 |
| Entity | Οδηγός Οχήματος Έκτακτης Ανάγκης | X | X |  |  |  | X |  |
|  | Οδηγοί άλλων Οχημάτων | 3 | 9 |  |  |  | X |  |
|  | Ευάλωτοι Χρήστες του δρόμου | 4 | 10 |  |  |  | X |  |
|  | Διαχειριστής υπηρεσίας ΠΟΚ | X | X |  |  |  | X |  |

# περιπτωσεισ καταχρησησ και ενδεικτικα σεναρια

**Πίνακας 3**

|  |  |  |
| --- | --- | --- |
| Αρ. | Περιπτώσεις Κατάχρησης | Ενδεικτικά Σενάρια |
| 1 | Συνδεσιμότητα ροής δεδομένων: Σύστημα Διαχείρισης Κυκλοφορίας – Υπηρεσία Εξυπηρέτησης Έκτακτης Ανάγκης | Η επικοινωνία ανάμεσα στο Όχημα Έκτακτης Ανάγκης και στο σύστημα Διαχείρισης Κυκλοφορίας δεν είναι προστατευμένη και ο επιτιθέμενος αποκαλύπτει πληροφορίες που μπορούν να συσχετιστούν από το περιεχόμενο της επικοινωνίας. |
| Η επικοινωνία ανάμεσα στο Όχημα Έκτακτης Ανάγκης και στο σύστημα Διαχείρισης Κυκλοφορίας δεν είναι ανώνυμη και ο επιτιθέμενος συνδέει ροή δεδομένων βασιζόμενος σε συγκείμενα δεδομένα (δεδομένα σχετικά με τα συμφραζόμενα της επικοινωνίας) προκειμένου να συσχετίσει πληροφορίες για ένα όχημα. |
| Το σύστημα ανωνυμίας που χρησιμοποιείται για την επικοινωνία ανάμεσα στο όχημα και το Σύστημα Διαχείρισης Κυκλοφορίας είναι επισφαλής και ο επιτιθέμενος μπορεί να αναλύσει την κυκλοφορία των δεδομένων για να εξάγει πληροφορίες από μοτίβα ροής δεδομένων (patterns of traffic) προκειμένου να συνδέσει τη δραστηριότητα ενός οχήματος. |
| 2 | Συνδεσιμότητα ροής δεδομένων: Υπηρεσία Εξυπηρέτησης Έκτακτης Ανάγκης - Σύστημα Διαχείρισης Κυκλοφορίας | Η επικοινωνία ανάμεσα στο Σύστημα Διαχείρισης Κυκλοφορίας και το Όχημα Έκτακτης Ανάγκης δεν είναι προστατευμένη και ο επιτιθέμενος αποκαλύπτει πληροφορίες που μπορούν να συσχετιστούν από το περιεχόμενο της επικοινωνίας. |
| Η επικοινωνία ανάμεσα στο Σύστημα Διαχείρισης Κυκλοφορίας και το Όχημα Έκτακτης Ανάγκης δεν είναι ανώνυμη και ο επιτιθέμενος συνδέει ροή δεδομένων βασιζόμενος σε συγκείμενα δεδομένα (δεδομένα σχετικά με τα συμφραζόμενα της επικοινωνίας) προκειμένου να συσχετίσει πληροφορίες για ένα όχημα. |
| Το σύστημα ανωνυμίας που χρησιμοποιείται για την επικοινωνία ανάμεσα στο Σύστημα Διαχείρισης Κυκλοφορίας και το Όχημα Έκτακτης Ανάγκης είναι επισφαλής και ο επιτιθέμενος μπορεί να αναλύσει την κυκλοφορία των δεδομένων για να εξάγει πληροφορίες από μοτίβα ροής δεδομένων (patterns of traffic) προκειμένου να συνδέσει τη δραστηριότητα ενός οχήματος. |
| 3 | Συνδεσιμότητα μιας οντότητας – Οδηγοί άλλων οχημάτων | Ένας επιτιθέμενος μπορεί να συσχετίσει πληροφορίες για τον οδηγό του οχήματος, συνδέοντας στοιχεία ταυτοποίησης (Personally Identifiable Information-PII) βασισμένος σε παράγοντες (π.χ. διεύθυνση IP, session ID, συγκεκριμένα μοτίβα αλληλεπίδρασης κτλ) εκμεταλλευόμενος μια απροστάτευτη ροή δεδομένων ανάμεσα σε δύο οχήματα. |
| 4 | Συνδεσιμότητα μιας οντότητας – Ευάλωτοι Χρήστες του δρόμου | Ένας επιτιθέμενος μπορεί να ταυτοποιήσει έναν ευάλωτο χρήστη του δρόμου (π.χ. πεζό) συνδέοντας στοιχεία ταυτοποίησης βασισμένος σε παράγοντες (π.χ. βιομετρικά στοιχεία, διεύθυνση IP, session ID, συγκεκριμένα μοτίβα αλληλεπίδρασης κτλ) εκμεταλλευόμενος μια απροστάτευτη ροή δεδομένων ανάμεσα στη συσκευή wearable και το Σύστημα Προειδοποίησης ενός άλλου οχήματος. |
| 5 | Αναγνωρισιμότητα ροής δεδομένων: Παρακολούθηση Οδικής Κυκλοφορίας – Σύστημα Διαχείρισης Κυκλοφορίας | Η επικοινωνία ανάμεσα στην Παρακολούθηση Οδικής Κυκλοφορίας και το Σύστημα Διαχείρισης Κυκλοφορίας δεν είναι προστατευμένη και ένας επιτιθέμενος αποκαλύπτει στοιχεία ταυτοποίησης του αυτοκινήτου από το περιεχόμενο της επικοινωνίας (π.χ. εικόνα από κάμερα στην οποία φαίνονται πινακίδες). |
| 6 | Αναγνωρισιμότητα ροής δεδομένων: Υπηρεσία Εξυπηρέτησης Έκτακτης Ανάγκης - Σύστημα Διαχείρισης Κυκλοφορίας | Η επικοινωνία ανάμεσα στο Όχημα Έκτακτης Ανάγκης και το Σύστημα Διαχείρισης Κυκλοφορίας δεν είναι προστατευμένη και ένας επιτιθέμενος αποκαλύπτει πληροφορίες ταυτοποίησης του αυτοκινήτου από το περιεχόμενο της επικοινωνίας. |
| Η επικοινωνία ανάμεσα στο Όχημα Έκτακτης Ανάγκης και το Σύστημα Διαχείρισης Κυκλοφορίας δεν είναι ανωνυμοποιημένη και ο επιτιθέμενος συνδέει ροή δεδομένων βασιζόμενος σε συγκείμενα δεδομένα (δεδομένα σχετικά με τα συμφραζόμενα της επικοινωνίας) προκειμένου να ταυτοποίησει τον οδηγό μέσω των πληροφοριών του αυτοκινήτου (π.χ. πινακίδες ή άδεια κυκλοφορίας). |
| Το σύστημα ανωνυμίας που χρησιμοποιείται για την επικοινωνία ανάμεσα στο Όχημα Έκτακτης Ανάγκης και το Σύστημα Διαχείρισης Κυκλοφορίας είναι επισφαλής και ο επιτιθέμενος μπορεί να αναλύσει τη ροή δεδομένων για να εξάγει πληροφορίες από μοτίβα ροής δεδομένων (patterns of traffic) προκειμένου να ταυτοποιήσει τον οδηγό μέσω πληροφοριών του αυτοκινήτου (π.χ. πινακίδες ή άδεια κυκλοφορίας). |
| 7 | Αναγνωρισιμότητα ροής δεδομένων: Σύστημα Προειδοποίησης Οχήματος (έκτακτης ανάγκης) – Συσκευή Wearable (gateway) | Η επικοινωνία ανάμεσα στο Όχημα Έκτακτης Ανάγκης και τη Συσκευή Wearable (gateway) δεν είναι προστατευμένη και ένας επιτιθέμενος αποκαλύπτει πληροφορίες ταυτοποίησης ενός πεζού από το περιεχόμενο της επικοινωνίας. |
| Η επικοινωνία ανάμεσα στο Όχημα Έκτακτης Ανάγκης και τη Συσκευή Wearable (gateway) δεν είναι ανωνυμοποιημένη και ο επιτιθέμενος συνδέει ροή δεδομένων βασιζόμενος σε συγκείμενα δεδομένα (δεδομένα σχετικά με τα συμφραζόμενα της επικοινωνίας, όπως βιομετρικά στοιχεία από τη wearable συσκευή) προκειμένου να ταυτοποίησει έναν πεζό. |
| Το σύστημα ανωνυμίας που χρησιμοποιείται για την επικοινωνία ανάμεσα στο Όχημα Έκτακτης Ανάγκης και τη Συσκευή Wearable (gateway) είναι επισφαλής και ο επιτιθέμενος μπορεί να αναλύσει τη ροή δεδομένων για να εξάγει πληροφορίες από μοτίβα ροής δεδομένων (patterns of traffic) προκειμένου να ταυτοποιήσει έναν πεζό. |
| 8 | Αναγνωρισιμότητα ροής δεδομένων: Σύστημα Προειδοποίησης Οχήματος (άλλα οχήματα) – Συσκευή Wearable (gateway) | Η επικοινωνία ανάμεσα σε ένα όχημα και τη Συσκευή Wearable (gateway) δεν είναι προστατευμένη και ένας επιτιθέμενος αποκαλύπτει πληροφορίες ταυτοποίησης ενός πεζού από το περιεχόμενο της επικοινωνίας. |
| Η επικοινωνία ανάμεσα σε ένα όχημα και τη Συσκευή Wearable (gateway) δεν είναι ανωνυμοποιημένη και ο επιτιθέμενος συνδέει ροή δεδομένων βασιζόμενος σε συγκείμενα δεδομένα (δεδομένα σχετικά με τα συμφραζόμενα της επικοινωνίας, όπως βιομετρικά στοιχεία από τη wearable συσκευή) προκειμένου να ταυτοποίησει έναν πεζό. |
| Το σύστημα ανωνυμίας που χρησιμοποιείται για την επικοινωνία ανάμεσα σε ένα όχημα και τη Συσκευή Wearable (gateway) είναι επισφαλής και ο επιτιθέμενος μπορεί να αναλύσει τη ροή δεδομένων για να εξάγει πληροφορίες από μοτίβα ροής δεδομένων (patterns of traffic) προκειμένου να ταυτοποιήσει έναν πεζό. |
| 9 | Αναγνωρισιμότητα οντοτήτων: Οδηγοί άλλων οχημάτων | Ο οδηγός μπορεί να ταυτοποιηθεί από τη ροή δεδομένων μέσω V2X (ΣΠΟ σε άλλα οχήματα – ΣΠΟ σε όχημα έκτακτης ανάγκης). |
| 10 | Αναγνωρισιμότητα οντοτήτων: Ευάλωτοι Χρήστες του δρόμου  | Ένας πεζός (VRU) μπορεί να ταυτοποιηθεί από τη ροή δεδομένων μέσω V2X (Συσκευή Wearable – ΣΠΟ οχήματος) |
| 11 | Ανιχνευσιμότητα στη Βάση Δεδομένων του Συστήματος Διαχείρισης Κυκλοφορίας | Η απόκρυψη των καταχωρίσεων στη Βάση Δεδομένων του Συστήματος είναι αδύναμη και ένας επιτιθέμενος εκμεταλλεύεται ελλιπή έλεγχο πρόσβασης για να ανιχνεύσει ένα σήμα οχήματος για επείγον περιστατικό.  |
| 12 | Ανιχνευσιμότητα ροής δεδομένων: Σύστημα Διαχείρισης Κυκλοφορίας – Έλεγχος Φαναριών Κυκλοφορίας | Η ροή δεδομένων ανάμεσα στο Σύστημα Διαχείρισης Κυκλοφορίας και τον Έλεγχο Φαναριών Κυκλοφορίας μπορεί να αποκαλύψει ότι μια κλήση για επείγον περιστατικό διαφέρει από την υπόλοιπη κίνηση του δικτύου (network traffic). |
| 13 | Ανιχνευσιμότητα ροής δεδομένων: Υπηρεσία Εξυπηρέτησης Έκτακτης Ανάγκης – Σύστημα Διαχείρισης Κυκλοφορίας | Η ροή δεδομένων ανάμεσα στην Όχημα Έκτακτης Ανάγκης (ΥΕΕΑ) και το Σύστημα Διαχείρισης Κυκλοφορίας μπορεί να αποκαλύψει ότι η κλήση για ένα επείγον περιστατικό διαφέρει από την υπόλοιπη κίνηση του δικτύου (network traffic). |
| 14 | Δημοσιοποίηση πληροφοριών από την επικοινωνία ανάμεσα στα Οχήματα | Η επικοινωνία ανάμεσα στα οχήματα δεν είναι προστατευμένη και ένας επιτιθέμενος ανακτά πληροφορίες για ένα όχημα ή/και τον οδηγό του από το περιεχόμενο της επικοινωνίας. |
| 15 | Δημοσιοποίηση πληροφοριών από την επικοινωνία ανάμεσα σε Ευάλωτους Χρήστες του δρόμου και στα Οχήματα | Η επικοινωνία ανάμεσα στα οχήματα και τους Ευάλωτους Χρήστες του δρόμου δεν είναι προστατευμένη και ένας επιτιθέμενος ανακτά πληροφορίες για πεζό (VRU) από το περιεχόμενο της επικοινωνίας. |
| 15 | Μη συμμόρφωση στην πολιτική και τη συγκατάθεση του ατόμου στο σύνολο του συστήματος | Ένας επιτιθέμενος αποκτά πρόσβαση στη Βάση Δεδομένων του Συστήματος Διαχείρισης Κυκλοφορίας και δημοσιοποιεί τα δεδομένα σε έναν τρίτο. |
| Ένας επιτιθέμενος ταυτοποιεί έναν Ευάλωτο Χρήστη του δρόμου (π.χ. πεζό) μέσω βιομετρικών δεδομένων από τη συσκευή wearable και δημοσιοποιεί τις πληροφορίες σε έναν τρίτο. |