Ευρωπαϊκή Ένωση
Ευρωπαϊκό Ταμείο Περιφερειακής Ανάπτυξης
ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ ΥΠΟΥΡΓΕΙΟ ΟΙΚΟΝΟΜΙΑΣ & ΑΝΑΠΤΥΞΗΣ ΕΙΔΙΚΗ ΓΡΑΜΜΑΤΕΙΑ ΕΤΠΑ & ΤΣ
ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ, ΕΡΕΥΝΑΣ & ΘΡΗΣΚΕΥΜΑΤΩΝ
ΕΥΔΕ ΕΤΕΚ
ΕΠΑνΕΚ 2014-2020 ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΑΝΤΑΓΩΝΙΣΤΙΚΟΤΗΤΑ ΕΠΙΧΕΙΡΗΜΑΤΙΚΟΤΗΤΑ ΚΑΙΝΟΤΟΜΙΑ
ΕΣΠΑ 2014-2020 ανάπτυξη - εργασία - αλληλεγγύη
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Ανάπτυξη Μεθοδολογιών και Ενσωματωμένων Λύσεων Ασφάλειας για Τεχνολογίες Internet of Things σε ηλεκτρονικές Υπηρεσίες Υγείας – ΜΕΛΙΤΥ (Τ1ΕΔΚ-01958)

Ολοκλήρωση των προτεινόμενων λύσεων ασφάλειας σε IoMT συσκευές - Επίδειξη των αποτελεσμάτων του έργου. (Τελική έκθεση)

ΕΝΟΤΗΤΑ ΕΡΓΑΣΙΑΣ ΕΡΓΟΥ:	**ΕΕ5**
ΚΩΔΙΚΟΣ ΠΑΡΑΔΟΤΕΟΥ:	**Π5.1**
ΕΚΔΟΣΗ:	**Τελική**
ΚΑΤΑΣΤΑΣΗ:	***Υποβληθείσα***
ΗΜΕΡΟΜΗΝΙΑ ΟΛΟΚΛΗΡΩΣΗΣ:	**31/01/2022**
ΥΠΕΥΘΥΝΟΣ ΦΟΡΕΑΣ:	**Πανεπιστήμιο Πειραιά**
ΣΥΜΜΕΤΕΧΟΝΤΕΣ ΦΟΡΕΙΣ	**Census, Micrel, ΟΛΥΜΠΙΟΝ, Πανεπιστήμιο Ιωαννίνων**

Πίνακας Περιεχόμενων

1. Εισαγωγή 4
   1.1. Σκοπός και στόχοι του παραδοτέου 4
   1.2. Δομή του παραδοτέου 4
   1.3. Επίδειξη αποτελεσμάτων δοκιμών 5
2. Εργαλείο Χαρτογράφησης «melicc» 6
   2.1. Δυνατότητες του εργαλείου 6
   2.2. Αρχιτεκτονική του εργαλείου 6
      2.2.1. Επικοινωνία μέσω HTTP 6
      2.2.2. HTTP/2 7
      2.2.3. gRPC 7
      2.2.4. Επικοινωνία μέσω WebSockets 7
   2.3. Σενάριο χρήσης εργαλείου 8
      2.3.1. Εκτέλεση εντολών λειτουργικού συστήματος 9
      2.3.2. Έλεγχος πολλαπλών εμφυτευμάτων 9
      2.3.3. Συλλογή πληροφοριών και έλεγχος συστήματος 10
3. Εργαλείο Υπολογισμού Κινδύνων «Attack Path Risk Finder» 12
   3.1. Περιγραφή λειτουργίας του εργαλείου (σενάρια χρήσης) 12
   3.1.1. Βήματα μεθοδολογίας σε βασικό σενάριο χρήσης 13
   3.2. Τεχνολογίες υλοποίησης 18
4. Κατανεμημένη υποδομή για τον έλεγχο πρόσβασης σε ιατρικά δεδομένα «Hierarchical Multi Blockchain» 19
   4.1. Λειτουργίες συστήματος 19
      4.1.1. Ανάπτυξη Παραδείγματος Σεναρίου 20
   4.2. Αρχιτεκτονική συστήματος 22
      4.2.1. Διαγράμματα Ροής Δεδομένων (Data Flow Charts) 22
      4.2.2. Διαγράμματα Όψης Εγκατάστασης (Physical View Diagrams) 24
      4.2.3. Διαγράμματα Όψης Συνιστωσών (Component View Diagrams) 25
   4.3. Λειτουργικές Απαιτήσεις - Σενάρια χρήσης 29
5. Σύνοψη αποτελεσμάτων του έργου 33
   5.1. Κύρια αποτελέσματα του έργου 33
      5.1.1. Ανάπτυξη μεθοδολογίας και εργαλείου ανάλυσης κυβερνο-φυσικών επιθέσεων για κρίσιμες συσκευές IoMT 33
      5.1.2. Ανάπτυξη κατανεμημένης υποδομής (Hierarchical Multi Blockchain) για τον έλεγχο πρόσβασης σε δεδομένα παραγόμενα στο ιατρικό οικοσύστημα 33
      5.1.3. Ανάπτυξη πλαισίου σχεδίασης προσανατολισμένο στην ασφάλεια υλικού συσκευών IoMT 34
      5.1.4. Κατηγοριοποίηση τεχνολογιών και πρωτοκόλλων που χρησιμοποιούνται για την επικοινωνία σε περιβάλλοντα που περιέχουν κρίσιμες συσκευές IoMT 34
   5.2. Σύνοψη ερευνητικών δημοσιεύσεων 35
   5.3. Μελλοντικές επεκτάσεις 36
6. Οπισθόφυλλο 37

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο
ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ ΥΠΟΥΡΓΕΙΟ ΟΙΚΟΝΟΜΙΑΣ & ΑΝΑΠΤΥΞΗΣ ΕΙΔΙΚΗ ΓΡΑΜΜΑΤΕΙΑ ΕΤΠΑ & ΤΣ ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ ΕΠΑνΕΚ
ΕΠΑνΕΚ 2014-2020 ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΑΝΤΑΓΩΝΙΣΤΙΚΟΤΗΤΑ ΕΠΙΧΕΙΡΗΜΑΤΙΚΟΤΗΤΑ ΚΑΙΝΟΤΟΜΙΑ
ΕΣΠΑ 2014-2020 ανάπτυξη - εργασία - αλληλεγγύη
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο
ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ
ΟΙΚΟΝΟΜΙΑΣ & ΑΝΑΠΤΥΞΗΣ
ΕΙΔΙΚΗ ΓΡΑΜΜΑΤΕΙΑ ΕΤΠΑ & ΤΣ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ ΕΠΑνΕΚ
ΕΠΑνΕΚ 2014-2020
ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΑΝΤΑΓΩΝΙΣΤΙΚΟΤΗΤΑ
ΕΠΙΧΕΙΡΗΜΑΤΙΚΟΤΗΤΑ
ΚΑΙΝΟΤΟΜΙΑ
ΕΣΠΑ 2014-2020
ανάπτυξη - εργασία - αλληλεγγύη
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

1. Εισαγωγή

1.1. Σκοπός και στόχοι του παραδοτέου

Σκοπός του παραδοτέου είναι να παρουσιαστούν τα αποτελέσματα της ολοκλήρωσης των προτεινόμενων λύσεων ασφάλειας για συσκευές IoMT, η επικύρωση των εργαλείων ασφάλειας που αναπτύχθηκαν στο πλαίσιο του έργου, καθώς και η επίδειξη των αποτελεσμάτων εφαρμογής τους. Τα εργαλεία έχουν δημιουργηθεί μέσα από την ερευνητική (Π4.1-Π4.5) και την αναπτυξιακή (Π4.6) διαδικασία που έχει πραγματοποιηθεί στα προηγούμενα παραδοτέα του έργου και στις αντίστοιχες ερευνητικές δημοσιεύσεις και έχουν σκοπό να καλύψουν τα βασικά κενά ασφαλείας που προκύπτουν από τις προηγούμενες φάσεις της μελέτης (Π3.1, Π3.2, Π3.4). Εν κατακλείδι βοηθούν στην μελέτη ασφαλείας διασυνδεδεμένων ιατρικών συσκευών που διεκπεραιώνονται σε πληροφοριακά δίκτυα υγειονομικού περιβάλλοντος. Πιο συγκεκριμένα παρουσιάζονται τα αποτελέσματα της εφαρμογής των εργαλείων ασφάλειας που αναπτύχθηκαν, μέσω της εφαρμογής σεναρίων μελέτης που περιλαμβάνουν μεταξύ άλλων σύστημα αντλίας έγχυσης και σύστημα μελέτης ύπνου.

Οι στόχοι του παραδοτέου περιλαμβάνουν:

- Να επικυρωθεί και να επιδειχθεί η δυνατότητα υπολογισμού του κινδύνου που οφείλεται σε κυβερνο-φυσικά μονοπάτια επίθεσης (cyber-physical attack paths), μέσω του εργαλείου ανάλυσης επικινδυνότητας Attack Path Risk Finder – APRF, το οποίο σχεδιάστηκε (Π3.3, Π3.4) και αναπτύχθηκε (Π4.6) στο πλαίσιο του έργου. Με τον τρόπο αυτό ανιχνεύονται κενά ασφαλείας που δημιουργούνται κατά την συνύπαρξη διαφορετικών τεχνολογιών μέσα στο ίδιο δίκτυο.
- Να επικυρωθεί και να επιδειχθεί η δυνατότητα απομακρυσμένης βοήθειας στους διαχειριστές συστημάτων, με σκοπό την συνεχή υποστήριξη των ιατρικών συσκευών αλλά και των χειριστών των μηχανημάτων. Ενέργεια που έχει ως στόχο την μείωση του κινδύνου που αφορά λάθος από ανθρώπινο παράγοντα, κάτι που είναι υψίστης σημασία σε υγειονομικά περιβάλλοντα. Επιπλέον να συλλέγονται ευκολότερα και με μεγαλύτερη ασφάλεια πληροφορίες και τα δεδομένα (τόσο δεδομένα ιατρικής φύσεως, όσο και λοιπά δεδομένα). Η ασφαλής πρόσβαση στα δεδομένα μπορεί να πραγματοποιηθεί μέσω της πλατφόρμας Hierarchical Multi-Blockchain που αναπτύχθηκε (Π4.1, Π4.4, Π4.5) και υλοποιήθηκε (Π4.6) στο πλαίσιο του έργου.
- Να επιλυθούν ζητήματα ασφάλειας κατά την πρόσβαση στα συστήματα-συσκευές που αναγνωρίστηκαν στα παραδοτέα Π3.1, Π3.2 και Π3.4 .Συγκεκριμένα, ο σκοπός είναι να δίνεται η δυνατότητα, σε πληροφοριακά συστήματα όπου συμμετέχουν πολλοί εμπλεκόμενοι, να ανταλλάσσουν ευαίσθητη πληροφορία προστατεύοντας την εμπιστευτικότητα, ακεραιότητα καθώς και την αυθεντικότητα αυτής, ενώ ταυτόχρονα να αξιοποιείται η τεχνολογία Blockchain ώστε όλοι οι εμπλεκόμενοι να έχουν εικόνα των ενεργειών που συνέβησαν στην ευαίσθητη πληροφορία ή στις ευαίσθητες λειτουργίες των συστημάτων που βρίσκονται στο υγειονομικό περιβάλλον.

1.2. Δομή του παραδοτέου

Στο κεφάλαιο 2 θα γίνει μια σύντομη επισκόπηση στις δυνατότητες και στις λειτουργίες του εργαλείου απομακρυσμένου ελέγχου melicc που αναπτύχθηκε (βλέπε Π4.6) με σκοπό την αυτοματοποιημένη χαρτογράφηση του προς μελέτη δικτύου και την κατά το δυνατό αυτοματοποίηση της συλλογής δεδομένων για το εργαλείο ανάλυσης επικινδυνότητας APRF. Θα παρουσιαστεί η αρχιτεκτονική του εργαλείου melicc και θα αναλυθούν τεχνικές λεπτομέρειες που αφορούν τις τεχνολογίες που χρησιμοποιήθηκαν κατά τη δημιουργία του. Επιπλέον παρουσιάζεται το αποτέλεσμα και τα βήματα από την εκτέλεση του εργαλείου πάνω σε πραγματικό σενάριο χρήσης.

Στο κεφάλαιο 3 θα παρουσιαστεί ο σχεδιασμός του εργαλείου ανάλυσης επικινδυνότητας Attack Path Risk Finder (APRF). Θα προσδιοριστούν οι τεχνολογίες που είναι απαραίτητες για την λειτουργία του, μαζί με την τον τρόπο που αλληλεπιδρά με γνωστές βιβλιοθήκες που δίνουν πληροφορίες για την διαδικασία της ανάλυσης επικινδυνότητας, όπως είναι η βιβλιοθήκη του NIST. Σημειώνεται ότι τα αποτελέσματα από την εφαρμογή του εργαλείου APRF σε ένα ρεαλιστικό σενάριο χρήσης ιατρικού περιβάλλοντος, στο οποίο περιλαμβάνονται συσκευές έγχυσης φαρμάκων και συσκευές

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο
ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ ΟΙΚΟΝΟΜΙΑΣ & ΑΝΑΠΤΥΞΗΣ
ΕΙΔΙΚΗ ΓΡΑΜΜΑΤΕΙΑ ΕΤΠΑ & ΤΣ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ ΕΠΑνΕΚ
ΕΠΑνΕΚ 2014-2020
ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΑΝΤΑΓΩΝΙΣΤΙΚΟΤΗΤΑ ΕΠΙΧΕΙΡΗΜΑΤΙΚΟΤΗΤΑ ΚΑΙΝΟΤΟΜΙΑ
ΕΣΠΑ 2014-2020
ανάπτυξη - εργασία - αλληλεγγύη
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

παρακολούθησης ασθενών όπως οι συσκευές μελέτης ύπνου, περιγράφονται αναλυτικά στο παραδοτέο Π3.4.

Στο κεφάλαιο 4 θα παρουσιαστεί μία υποδομή υλοποιημένη με τεχνολογία blockchain με σκοπό τον έλεγχο πρόσβασης σε ιατρικά δεδομένα. Το κεφάλαιο περιέχει αναλυτικά τις λειτουργίες του συστήματος μαζί με τεχνικές λεπτομέρειες που αφορούν την αρχιτεκτονική του, δίνοντας βάση εξίσου στον τρόπο δημιουργίας του αλλά και στον τρόπο εφαρμογής και διασύνδεσης του χρήστη. Επίσης, παρουσιάζονται σενάρια χρήσης αυτού του συστήματος πάνω σε διαφορετικές περιπτώσεις και συνθήκες.

Τέλος, στο κεφάλαιο 5 παρουσιάζονται συνοπτικά τα κύρια αποτελέσματα του έργου, ενώ περιγράφονται και οι πιθανές μελλοντικές επεκτάσεις των αποτελεσμάτων αυτών.

1.3. Επίδειξη αποτελεσμάτων δοκιμών

Για την πληρέστερη επίδειξη των αποτελεσμάτων του έργου, το παρόν παραδοτέο συνοδεύεται από βίντεο επίδειξης (demo videos) των αποτελεσμάτων εφαρμογής των εργαλείων ασφάλειας που αναπτύχθηκαν στο πλαίσιο του έργου. Τα βίντεο επίδειξης βρίσκονται στον φάκελο «ΠΑΡΑΔΟΤΕΑ/ΕΕ5/Demo Videos» και περιλαμβάνουν τα εξής:

(1) Attack Path Risk Finder (APRF) RA tool demo video: Στο φάκελο αυτό περιλαμβάνεται βίντεο επίδειξης της εφαρμογής του εργαλείου APRF (βλέπε Π3.3, Π3.4 και Π4.6), σε συνδυασμό με το εργαλείο meliccc, σε ένα ρεαλιστικό σενάριο εφαρμογής, για την ανάλυση των σύνθετων κυβερνο-φυσικών μονοπατιών επίθεσης, τα οποία στοχεύουν κρίσιμες ιατρικές συσκευές, περιλαμβανομένων αντλιών έγχυσης φαρμάκων και συστημάτων παρακολούθησης ασθενών. Το σενάριο δοκιμής λαμβάνει υπόψη τη χρήση τέτοιων συσκευών τόσο εντός του νοσοκομειακού περιβάλλοντος, όσο και εντός οικιακού περιβάλλοντος.

(2) Hierarchical Multi Blockchain Infrastructure demo video: Στο φάκελο αυτό περιλαμβάνεται βίντεο επίδειξης της υποδομής ελέγχου πρόσβασης σε ιατρικά δεδομένα Hierarchical Multi Blockchain Infrastructure (βλέπε Π4.1, Π4.4, Π4.5), τα οποία παράγονται από διάφορες πηγές όπως είναι ιατρικές συσκευές παρακολούθησης και παροχής υπηρεσιών υγείας. Γίνεται επίδειξη της χρήσης της πλατφόρμας σε διάφορα ρεαλιστικά ερωτήματα, τα οποία περιλαμβάνουν ασφαλή αναζήτηση ιατρικών δεδομένων και ασφαλή αναβάθμιση υλικολογισμικού ιατρικής συσκευής.

(3) Side Channel attacks demo video: Στο φάκελο αυτό περιλαμβάνεται βίντεο επίδειξης της διάταξης και του λογισμικού που αναπτύχθηκε για τη δοκιμή επιθέσεων πλευρικού καναλιού (βλέπε Π4.1), πάνω στα εργαστηριακά πρωτότυπα. Τα αποτελέσματα των επιθέσεων πλευρικού καναλιού αξιοποιήθηκαν κατά την ανάπτυξη του εργαλείου APRF όσο και στη τελική αξιολόγηση επικινδυνότητας των εργαστηριακών πρωτοτύπων.

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο
ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ ΟΙΚΟΝΟΜΙΑΣ & ΑΝΑΠΤΥΞΗΣ
ΕΙΔΙΚΗ ΓΡΑΜΜΑΤΕΙΑ ΕΤΠΑ & ΤΣ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ ΕΠΑνΕΚ
ΕΠΑνΕΚ 2014-2020
ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΑΝΤΑΓΩΝΙΣΤΙΚΟΤΗΤΑ ΕΠΙΧΕΙΡΗΜΑΤΙΚΟΤΗΤΑ ΚΑΙΝΟΤΟΜΙΑ
ΕΣΠΑ 2014-2020
ανάπτυξη - εργασία - αλληλεγγύη
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

2. Εργαλείο Χαρτογράφησης «melicc»

Το εν λόγω εργαλείο έχει δημιουργηθεί στο πλαίσιο του έργου ΜΕΛΙΤΥ. Έχει πάρει το όνομά του από το έργο ΜΕΛΙΤΥ και την λειτουργία του διακομιστή (server) ως σύστημα εντολών και ελέγχου (Command and Control). Το melicc καλύπτει την ανάγκη για συλλογή δεδομένων και πληροφοριών με σκοπό τη διασφάλιση των προτύπων ασφάλειας, στην επικοινωνία και την λειτουργία διασυνδεδεμένων συσκευών που εξυπηρετούν ιατρικούς σκοπούς και όχι μόνο, σε περιβάλλον ιατρικής περίθαλψης. Στόχος του εργαλείου melicc είναι να χρησιμοποιείται από τους διαχειριστές συστημάτων και ιατρικών συσκευών για τη μερική αυτοματοποίηση της καταγραφής των συστημάτων και των μεταξύ τους διασυνδέσεων. Τα δεδομένα αυτά μπορούν στη συνέχεια να εισαχθούν στο εργαλείο ανάλυσης επικινδυνότητας APRF. Συνεπώς το melic λειτουργεί προπαρασκευαστικά για την συλλογή δεδομένων για την ανάλυση επικινδυνότητας. Επιπλέον, το εργαλείο melic μπορεί να συλλέγει πληροφορίες όπως δείκτες συμβιβασμού (Indicators of Compromise – IoC) από συνδεδεμένες συσκευές και να διασφαλίζει συνολικές πρακτικές ασφάλειας.

Για την επίτευξη των παραπάνω στόχων το εργαλείο προσφέρει:

- τη δυνατότητα εντοπισμού κενών ασφαλείας,
- τη συλλογή πληροφοριών για την αποτίμηση των κινδύνων που ελλοχεύουν στα συστήματα υπό εξέταση,
- τη δυνατότητα εφαρμογής κανόνων ασφαλείας,
- τη δυνατότητα αναβάθμισης λογισμικού και εφαρμογής ενημερώσεων ασφαλείας.

Με βάση τα παραπάνω δημιουργήθηκε ένα ευέλικτο εργαλείο το οποίο μπορεί να χρησιμοποιηθεί για την αλληλεπίδραση μεταξύ συστημάτων κάθε είδους, την εκτέλεση εντολών και τη συλλογή των αποτελεσμάτων τους. Η γλώσσα υλοποίησης είναι η Python, καθώς είναι ευανάγνωστη, υποστηρίζει γρήγορη πρωτοτυποποίηση και μπορεί να εκτελεστεί σε κάθε σύστημα που παρέχει έναν διερμηνευτή της γλώσσας.

2.1. Δυνατότητες του εργαλείου

Το melicc, παρέχει τις ακόλουθες δυνατότητες:

- Εκτέλεση εντολών λειτουργικού συστήματος
- Έλεγχος πολλαπλών εμφυτευμάτων ταυτόχρονα
- Συλλογή πληροφοριών με χρήση εντολών φλοιού και ερωτημάτων osquery

2.2. Αρχιτεκτονική του εργαλείου

Το εργαλείο υποστηρίζει επικοινωνία μέσω πρωτοκόλλου HTTP και HTTP/2, gRPC και Web Sockets, όπως περιγράφεται στη συνέχεια.

2.2.1. Επικοινωνία μέσω HTTP

Στην πρώτη εφαρμογή του εργαλείου, η επικοινωνία μεταξύ του διακομιστή ελέγχου και των εμφυτευμάτων πραγματοποιείται χρησιμοποιώντας απλά αιτήματα και απαντήσεις HTTP/1.1. Χρησιμοποιώντας sockets HTTP/1.1, παρατηρήθηκαν οι ακόλουθοι περιορισμοί:

- Η επικοινωνία είναι ημι-αμφίδρομη και γίνεται με μοτίβο αιτήματος - απόκρισης (σύγχρονη).
- Τα εμφυτεύματα πρέπει να κάνουν νέα αιτήματα εντολών στον διακομιστή ελέγχου, οδηγώντας σε υψηλή επισκεψιμότητα.
- Το timeout κλείνει το socket.
- Αυξημένη επιβάρυνση για την προετοιμασία της σύνδεσης.
- Δύσκολο να εντοπιστεί εάν κάποιο από τα δύο άκρα έχει κλείσει τη σύνδεση, είτε λόγω προβλημάτων δικτύου, σφάλματος συστήματος είτε λόγω επιλογής.

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο
ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ ΟΙΚΟΝΟΜΙΑΣ & ΑΝΑΠΤΥΞΗΣ
ΕΙΔΙΚΗ ΓΡΑΜΜΑΤΕΙΑ ΕΤΠΑ & ΤΣ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ ΕΠΑνΕΚ
ΕΠΑνΕΚ 2014-2020
ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΑΝΤΑΓΩΝΙΣΤΙΚΟΤΗΤΑ ΕΠΙΧΕΙΡΗΜΑΤΙΚΟΤΗΤΑ ΚΑΙΝΟΤΟΜΙΑ
ΕΣΠΑ 2014-2020
ανάπτυξη - εργασία - αλληλεγγύη
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Στην πρώιμη φάση των δοκιμών προκύπτουν διάφορα ζητήματα όπως τα μακροχρόνια αιτήματα, η περίπτωση όπου το ένα κανάλι είναι κλειστό και η σύγχρονη επικοινωνία. Παρακάτω παρουσιάζονται τρεις τεχνολογίες για την επίλυση κάποιων από αυτών των ζητημάτων.

Οι διαθέσιμες επιλογές περιλαμβάνουν τα ακόλουθα πρωτόκολλα:

- HTTP/2
- gRPC
- WebSockets

2.2.2.HTTP/2

Το HTTP/2 είχε ορισμένα πλεονεκτήματα απόδοσης:

- Επίπεδο δυαδικού πλαισίου (Binary framing layer): Σε αντίθεση με το πρωτόκολλο απλού κειμένου HTTP/1.x , όλη η επικοινωνία HTTP/2 χωρίζεται σε μικρότερα μηνύματα και πλαίσια, καθένα από τα οποία κωδικοποιείται σε δυαδική μορφή.
- Αμφίδρομη ροή δεδομένων: Full-duplex επικοινωνία.
- Μονά TCP sockets που μεταφέρουν οποιονδήποτε αριθμό αμφίδρομων ροών..
- Πολυπλεξία αιτήματος και απόκρισης: Τα μηνύματα HTTP χωρίζονται σε ανεξάρτητα πλαίσια τα οποία μπορούν να συναρμολογηθούν εκ νέου στο άλλο άκρο
- Προτεραιότητα ροής: Σε κάθε ροή μπορεί να εκχωρηθεί ένα βάρος μεταξύ 1 και 256. Οι ροές μπορεί επίσης να έχουν σχέσεις εξάρτησης με άλλες ροές
- Push διακομιστή: Ο διακομιστής έχει τη δυνατότητα να αποστείλει (push) πρόσθετους πόρους στον πελάτη, χωρίς ο πελάτης να τους ζητήσει ρητά.
- Συμπίεση κεφαλίδας: Τα πεδία κωδικοποιούνται χρησιμοποιώντας κωδικοποίηση Huffman για μείωση του μεγέθους.

2.2.3.gRPC

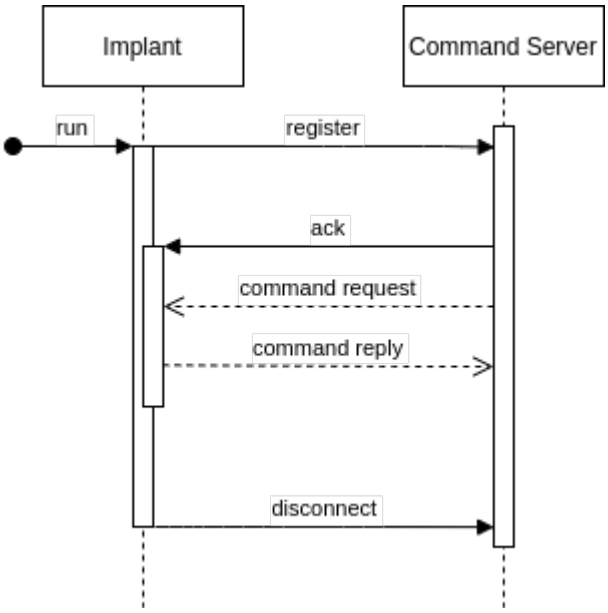
Το gRPC φαίνεται να είναι το πιο αποτελεσματικό πρωτόκολλο και παρέχει αρκετές επεκτάσεις σε σύγκριση με το HTTP/1.1. Χρησιμοποιεί το HTTP/2 ως πρωτόκολλο μεταφοράς και υλοποιεί με μεγάλη ταχύτητα την ανάλυση των μηνυμάτων. Ωστόσο, με τη μεγάλη δύναμη έρχεται μεγάλη ευθύνη και το gRPC δεν αποτελεί εξαίρεση. Είναι ένα πιο προηγμένο πρωτόκολλο και επομένως έχει μια πιο απότομη καμπύλη εκμάθησης. Για αυτόν τον λόγο, το gRPC είναι προς το παρόν λιγότερο δημοφιλές σε σύγκριση με τα WebSockets και το HTTP/2.

2.2.4.Επικοινωνία μέσω WebSockets

Τα WebSockets έχουν επιλεγεί για την επικοινωνία μεταξύ των εμφυτευμάτων και του διακομιστή, λόγω της υψηλής απόδοσης σε σύγκριση με το μοντέλο αιτήματος - απόκρισης HTTP. Ειδικότερα τα WebSockes:

- Είναι ένα πλήρως αμφίδρομο πρωτόκολλο που επιτρέπει στα δύο άκρα να επικοινωνούν ασύγχρονα.
- Απαιτεί τη δημιουργία μόνο μιας υποδοχής για όλη την επικοινωνία μεταξύ των δύο τελικών σημείων.
- Είναι ένα πρωτόκολλο που υποστηρίζεται ευρέως.
- Εύκολο στη χρήση και κατανόηση.
- Και τα δύο άκρα γνωρίζουν πότε το socket είναι κλειστό είτε λόγω προβλημάτων δικτύου, κατάρρευσης συστήματος ή λόγω επιλογής.

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο
ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ ΟΙΚΟΝΟΜΙΑΣ & ΑΝΑΠΤΥΞΗΣ
ΕΙΔΙΚΗ ΓΡΑΜΜΑΤΕΙΑ ΕΤΠΑ & ΤΣ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ ΕΠΑνΕΚ
ΕΠΑνΕΚ 2014-2020
ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΑΝΤΑΓΩΝΙΣΤΙΚΟΤΗΤΑ ΕΠΙΧΕΙΡΗΜΑΤΙΚΟΤΗΤΑ ΚΑΙΝΟΤΟΜΙΑ
ΕΣΠΑ 2014-2020
ανάπτυξη - εργασία - αλληλεγγύη
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης



ΕΙΚΟΝΑ 1 :ΕΠΙΚΟΙΝΩΝΙΑ ΕΜΦΥΤΕΥΜΑΤΩΝ (IMPLANTS) ΜΕ ΕΞΥΠΗΡΕΤΗΤΗ ΙΣΤΟΥ (COMMAND SERVER)

Για την υλοποίηση του συστήματος χρησιμοποιήθηκαν οι ακόλουθες βιβλιοθήκες:

- Argparse: Αναλυτής για ορίσματα γραμμής εντολών.
- Tornado: Μια βιβλιοθήκη ασύγχρονης δικτύωσης, που χρησιμοποιείται για την υλοποίηση του διακομιστή Websocket.
- Osquery: Εργαλεία λειτουργικού συστήματος, που διευκολύνουν την ανάκτηση πληροφοριών σχετικά με την πληροφοριακή υποδομή.
- Cmd: Παρέχει υποστήριξη για τη σύνταξη διερμηνέων εντολών προσανατολισμένων στη γραμμή εντολών. Χρησιμοποιείται για τη δημιουργία της διεπαφής γραμμής εντολών για το Melicc.
- Tinydb: Μια ελαφριά βάση δεδομένων προσανατολισμένη στα έγγραφα, που χρησιμοποιείται ως μηχανισμός καταγραφής για την επικοινωνία μεταξύ διακομιστή ελέγχου και εμφυτευμάτων
- Tkinter: Είναι η τυπική διεπαφή Python για το Tk GUI. Επί του παρόντος χρησιμοποιείται ως ένας τρόπος για την ανάκτηση των περιεχομένων του buffer του προχείρου ενός εμφυτεύματος

2.3.Σενάριο χρήσης εργαλείου

Για τη δοκιμή της λειτουργίας του εργαλείου χρησιμοποιήθηκαν συνολικά τρία Raspberry Pi με Raspbian λειτουργικό χρησιμοποιήθηκαν για σκοπούς δοκιμής: Επιλέχθηκε ένα Raspberry Pi για τον ρόλο του κύριου διακομιστή που λειτουργεί ως διακομιστής ελέγχου του δικτύου και τα άλλα δύο λειτουργούν ως εμφυτεύματα στους δύο εξυπηρετητές. Όταν δημιουργείται ο διακομιστής ελέγχου, εμφανίζει την IP διεπαφής και τη θύρα που ακούει, όπως φαίνεται στην παρακάτω εικόνα:

ΕΙΚΟΝΑ 2 :ΔΙΑΚΟΜΙΣΤΗΣ ΕΛΕΓΧΟΥ

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο
ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ ΟΙΚΟΝΟΜΙΑΣ & ΑΝΑΠΤΥΞΗΣ
ΕΙΔΙΚΗ ΓΡΑΜΜΑΤΕΙΑ ΕΠΑ & ΤΣ
ΕΠΑνΕΚ 2014-2020
ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΑΝΤΑΓΩΝΙΣΤΙΚΟΤΗΤΑ ΕΠΙΧΕΙΡΗΜΑΤΙΚΟΤΗΤΑ ΚΑΙΝΟΤΟΜΙΑ
ΕΣΠΑ 2014-2020
ανάπτυξη - εργασία - αλληλεγγύη
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

```
(venv) achilles@troy ~/t/melicc> ./client/implant.py -t 172.16.13.1 -p 8081
172.16.13.1 8081
[on_message] Received message from server: {"msg": "Welcome}"}
[on_message] Attempting to parse...
[on_message] Unknown exception: 'type'
[on_message] Received message from server: [on_message] Registered
[on_message] Attempting to parse...
[on_message] Received something which is not JSON
```

ΕΙΚΟΝΑ 3: ΣΥΝΔΕΣΗ ΣΕ ΔΙΑΚΟΜΙΣΤΗ ΕΛΕΓΧΟΥ

2.3.1.Εκτέλεση εντολών λειτουργικού συστήματος

Χρησιμοποιώντας το εργαλείο, είναι δυνατό να δοθεί εντολή σε ένα εμφύτευμα να εκτελέσει αυθαίρετες εντολές λειτουργικού συστήματος και να ανακτήσει τις εξόδους τους. Για την εκτέλεση εντολών Λ.Σ. χρησιμοποιούμε την εντολή ‘shell <command>’ είτε τη συντομότερη έκδοση αυτής ‘! <εντολή>’. Για την εκτέλεση εντολών στα εμφυτεύματα, εκτελούμε ‘out = subprocess.check_output(arg, stderr=subprocess.STDOUT, shell=True)’ Αυτός είναι ένας απλός τρόπος εκτέλεσης εντολών και λήψης της εξόδου τους, αν και δεν παρέχει τη δυνατότητα αλληλεπίδρασης με τη διαδικασία προορισμού χρησιμοποιώντας τυπική ροή αρχείων εισόδου (stdin).

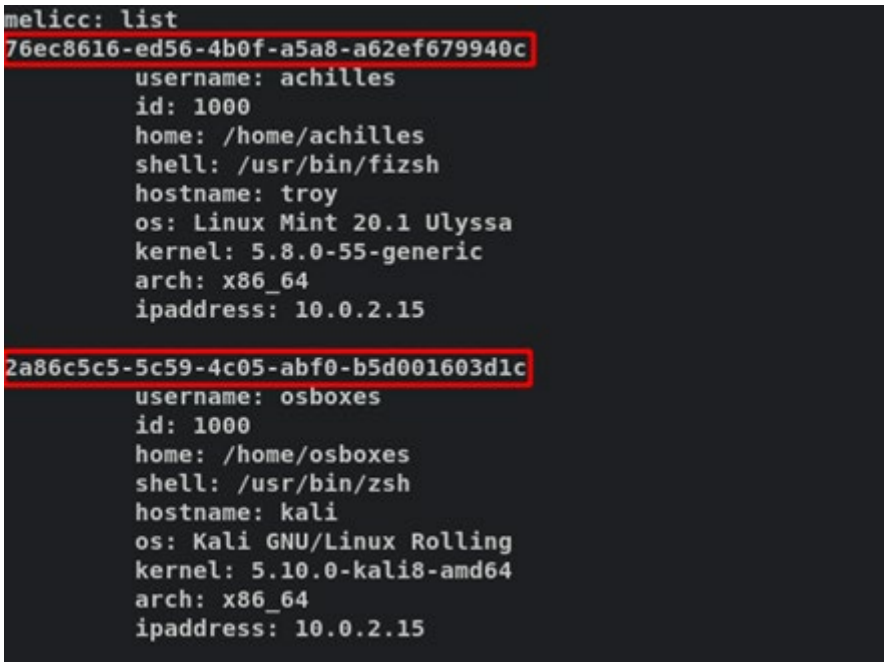
```
[fd64b3c6-7cab-49ca-8802-b2cb1d1384e0]: shell netstat -alvpn
        (Not all processes could be identified, non-owned process info
         will not be shown, you would have to be root to see it all.)
        netstat: no support for `AF INET (sctp)' on this system.
        netstat: no support for `AF INET (sctp)' on this system.
        Active Internet connections (servers and established)
        Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
        tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN      -
        tcp        0      0 0.0.0.0:8888            0.0.0.0:*               LISTEN      -
        tcp        0      0 127.0.0.1:5432          0.0.0.0:*               LISTEN      -
        tcp        0      0 0.0.0.0:12345           0.0.0.0:*               LISTEN      -
        tcp        0      0 127.0.0.1:33060         0.0.0.0:*               LISTEN      -
        tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      -
        tcp        0      0 127.0.0.1:55119         0.0.0.0:*               LISTEN      -
        tcp        0      0 127.0.0.1:37777         0.0.0.0:*               LISTEN      -
        tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      -
        tcp        0      0 10.0.2.15:35170         172.16.13.1:8081        ESTABLISHED 2940/python3
        tcp        0      0 10.0.2.15:12345         10.0.2.2:59682          ESTABLISHED -
        tcp6       0      0 ::1:631                 :::*                    LISTEN      -
        tcp6       0      0 ::1:55119               :::*                    LISTEN      -
        tcp6       0      0 :::80                   :::*                    LISTEN      -
        udp        0      0 0.0.0.0:631             0.0.0.0:*                           -
        udp        0      0 0.0.0.0:5353            0.0.0.0:*                           -
        udp        0      0 0.0.0.0:50696           0.0.0.0:*                           -
        udp        0      0 127.0.0.1:57043         127.0.0.1:57043         ESTABLISHED -
        udp        0      0 127.0.0.53:53           0.0.0.0:*                           -
        udp        0      0 10.0.2.15:68            10.0.2.2:67             ESTABLISHED -
        udp6       0      0 :::5353                 :::*                                -
        udp6       0      0 :::60861                :::*                                -
        raw6       0      0 :::58                   :::*                    7           -
```

ΕΙΚΟΝΑ 4: ΕΚΤΕΛΕΣΗ “NETSTAT -ALVPN”

2.3.2.Έλεγχος πολλαπλών εμφυτευμάτων

Το Melicc δίνει τη δυνατότητα ελέγχου πολλαπλών εμφυτευμάτων ταυτόχρονα. Ουσιαστικά προσομοίωση ενός μηνύματος "πολλαπλής εκπομπής - multicast ". Είναι δυνατή η απαρίθμηση των καταχωρημένων εμφυτευμάτων χρησιμοποιώντας την εντολή "list" και η δημιουργία μιας ομάδας πολλαπλής διανομής χρησιμοποιώντας την εντολή "multicast <όνομα ομάδας>".

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο
ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ ΟΙΚΟΝΟΜΙΑΣ & ΑΝΑΠΤΥΞΗΣ
ΕΙΔΙΚΗ ΓΡΑΜΜΑΤΕΙΑ ΕΤΠΑ & ΤΣ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ ΕΠΑνΕΚ
ΕΠΑνΕΚ 2014-2020
ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΑΝΤΑΓΩΝΙΣΤΙΚΟΤΗΤΑ ΕΠΙΧΕΙΡΗΜΑΤΙΚΟΤΗΤΑ ΚΑΙΝΟΤΟΜΙΑ
ΕΣΠΑ 2014-2020
ανάπτυξη - εργασία - αλληλεγγύη
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης



ΕΙΚΟΝΑ 5: ΚΑΤΑΛΟΓΟΣ ΔΙΑΘΕΣΙΜΩΝ ΕΜΦΥΤΕΥΜΑΤΩΝ

Η προσθήκη εμφυτευμάτων σε έναν τομέα πολλαπλής διανομής, πραγματοποιείται με την εντολή "add <uuid>". Το Melicc παρέχει λειτουργία αυτόματης συμπλήρωσης πατώντας το πλήκτρο "Tab". Οποιαδήποτε εντολή εκδίδεται μέσα στην ομάδα πολλαπλής διανομής θα εκτελείται σε κάθε εμφύτευμα που έχει προστεθεί σε αυτήν την ομάδα.

ΕΙΚΟΝΑ 6: ΕΛΕΓΧΟΣ ΠΟΛΛΑΠΛΩΝ ΕΜΦΥΤΕΥΜΑΤΩΝ ΤΑΥΤΟΧΡΟΝΑ

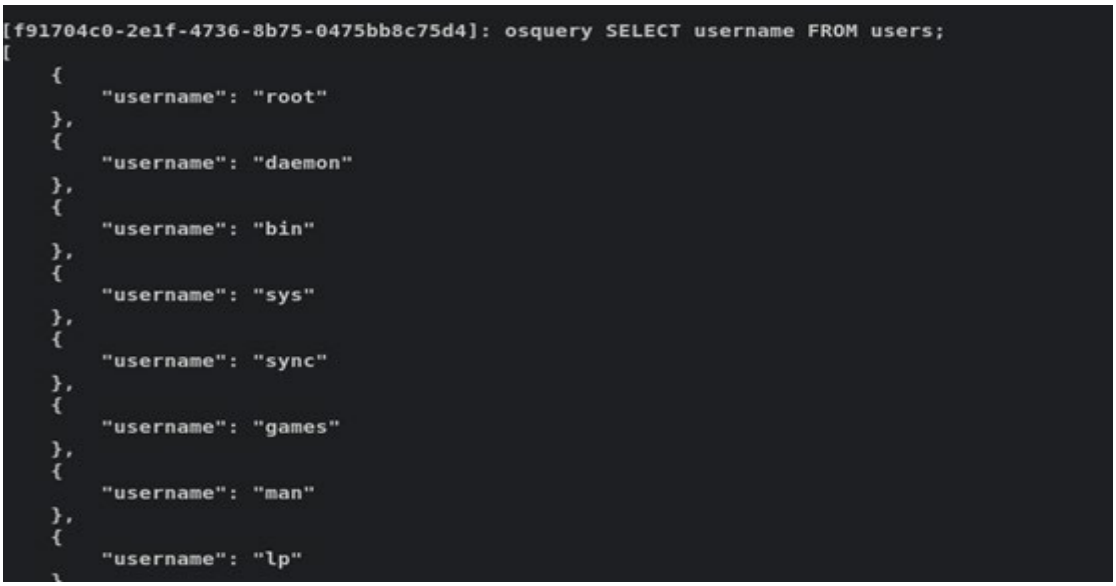
Για να επιτευχθεί η λειτουργία πολλαπλής διανομής, προστίθενται αναγνωριστικά εμφυτευμάτων (uids) σε μια λίστα. Αργότερα, όταν εκδίδεται μια εντολή πολλαπλής διανομής, δημιουργείται μια εργασία για κάθε αναγνωριστικό στη λίστα.

2.3.3.Συλλογή πληροφοριών και έλεγχος συστήματος

Για περαιτέρω απαρίθμηση, το Melicc παρέχει τη δυνατότητα αλληλεπίδρασης με τη σχεσιακή βάση δεδομένων osquery, εκτελώντας ερωτήματα SQL για την ανάκτηση πληροφοριών του λειτουργικού συστήματος, όπως εγκατεστημένα πακέτα, πληροφορίες πυρήνα, θύρες ακρόασης και πολλά άλλα. Το osquery είναι ένα πλαίσιο οργάνων λειτουργικού συστήματος πολλαπλών πλατφορμών και παρέχει χαμηλού επιπέδου ανάλυση και παρακολούθηση του λειτουργικού συστήματος με αποτελεσματικό τρόπο. Με τη δύναμη μιας πλήρους γλώσσας SQL και ενσωματωμένων δεκάδων χρήσιμων πινάκων, το osquery μπορεί να βοηθήσει στην απόκριση περιστατικών, στη διάγνωση ενός προβλήματος λειτουργιών συστήματος, στην αντιμετώπιση προβλημάτων και στη συλλογή πληροφοριών συστήματος και είναι ένα ανεκτίμητο εργαλείο για διαχειριστές συστήματος και αναλυτές ασφαλείας.

Είναι δυνατή η εκτέλεση προσαρμοσμένων ερωτημάτων SQL χρησιμοποιώντας την εντολή "osquey <query>", όπως φαίνεται στην παρακάτω εικόνα:

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο
ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ
ΟΙΚΟΝΟΜΙΑΣ & ΑΝΑΠΤΥΞΗΣ
ΕΙΔΙΚΗ ΓΡΑΜΜΑΤΕΙΑ ΕΠΑ & ΤΣ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ ΕΠΑνΕΚ
ΕΠΑνΕΚ 2014-2020
ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΑΝΤΑΓΩΝΙΣΤΙΚΟΤΗΤΑ
ΕΠΙΧΕΙΡΗΜΑΤΙΚΟΤΗΤΑ
ΚΑΙΝΟΤΟΜΙΑ
ΕΣΠΑ 2014-2020
ανάπτυξη - εργασία - αλληλεγγύη
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

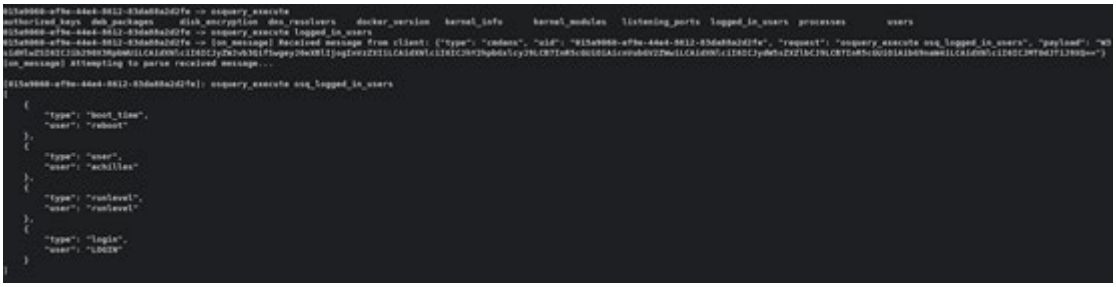


ΕΙΚΟΝΑ 7: ΑΛΛΗΛΕΠΙΔΡΑΣΗ ΜΕ ΤΟ OSQUERRY

Το melicc έχει επίσης ενσωματωμένα ερωτήματα για τις ακόλουθες πληροφορίες:

- SSH authorized_keys του τρέχοντος χρήστη
- Εγκατεστημένα πακέτα deb
- Έλεγχος εάν η κρυπτογράφηση δίσκου έχει ρυθμιστεί
- Αρίθμηση των προγραμμάτων επίλυσης DNS
- Εγκατάσταση έκδοση; Docker
- Πληροφορίες πυρήνα
- Φορτωμένες μονάδες πυρήνα
- Θύρες ακρόασης
- Συνδεδεμένοι χρήστες
- Διαδικασίες συστήματος
- Διαθέσιμοι χρήστες

Περισσότερα ερωτήματα μπορούν να προστεθούν χειροκίνητα στο αρχείο "handlers.py" που βρίσκεται στον κατάλογο "melicc/client/". Τα ήδη καθορισμένα ερωτήματα μπορούν να εκτελεστούν χρησιμοποιώντας την εντολή "osquery_execute <query-name>".



ΕΙΚΟΝΑ 8: ΗΔΗ ΚΑΘΟΡΙΣΜΕΝΑ ΕΡΩΤΗΜΑΤΑ

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο
ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ ΟΙΚΟΝΟΜΙΑΣ & ΑΝΑΠΤΥΞΗΣ
ΕΙΔΙΚΗ ΓΡΑΜΜΑΤΕΙΑ ΕΤΠΑ & ΤΣ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ ΕΠΑνΕΚ
ΕΠΑνΕΚ 2014-2020
ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΑΝΤΑΓΩΝΙΣΤΙΚΟΤΗΤΑ ΕΠΙΧΕΙΡΗΜΑΤΙΚΟΤΗΤΑ ΚΑΙΝΟΤΟΜΙΑ
ΕΣΠΑ 2014-2020
ανάπτυξη - εργασία - αλληλεγγύη
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

3. Εργαλείο Υπολογισμού Κινδύνων «Attack Path Risk Finder»

Στο πλαίσιο του έργου ΜΕΛΙΤΥ, αναπτύχθηκε το πειραματικό εργαλείο ανάλυσης επικινδυνότητας Attack Path Risk Finder (APRF). Το APRF είναι ένα εργαλείο για τον εντοπισμό και την αξιολόγηση κινδύνων από σύνθετα κυβερνο-φυσικά μονοπάτια επίθεσης (cyber-physical attack paths), τα οποία δημιουργούνται μέσω των πληροφοριακών/κυβερνητικών (cyber) και φυσικών (physical) αλληλεπιδράσεων μεταξύ διασυνδεδεμένων συστημάτων. Το εργαλείο υλοποιεί τη μεθοδολογία που παρουσιάστηκε στο παραδοτέο Π3.3 (σχετική δημοσίευση: *Stellios, Ioannis, Panayiotis Kotzanikolaou, and Christos Grigoriadis. "Assessing IoT enabled cyber-physical attack paths against critical systems." Computers & Security 107 (2021): 102316*).

Ο εκάστοτε ερευνητής ασφαλείας καλείται να συμπληρώσει αυτά τα αρχεία με πληροφορίες για το σύστημα που μελετά όπως:

- Το λειτουργικό σύστημα και οι εφαρμογές που είναι εγκατεστημένα σε μια συσκευή.
- Οι διεπαφές της κάθε συσκευής και το δίκτυο με το οποίο επικοινωνούν.
- Η φυσική τοποθεσία και η ανάλογη κατηγορία τύπου πρόσβασης που της αναλογεί, σε συνδυασμό με την εγγύτητα της συσκευής με άλλες συσκευές του συστήματος.
- Τα δικαιώματα εκτέλεσης της συσκευής σε συσκευές που είναι συνδεδεμένη.
- Η τεχνολογία που χρησιμοποιεί και η συχνότητα εκπομπής ενός δικτύου.
- Οι διασυνδέσεις μεταξύ διαφορετικών δικτύων και το επίπεδο ασφαλείας(CIA) που εφαρμόζεται στο πλαίσιο των μεταξύ τους επικοινωνιών.

Όπως αναφέρθηκε στην προηγούμενη ενότητα, το εργαλείο melic μπορεί να προσφέρει μερική αυτοματοποίηση της συλλογής των παραπάνω δεδομένων.

3.1.Περιγραφή λειτουργίας του εργαλείου (σενάρια χρήσης)

Για την λειτουργικότητα του εργαλείου είναι απαραίτητη η αξιοποίηση της βάσης δεδομένων αδυναμιών του NIST[1]. Με αυτόν τον τρόπο ανιχνεύονται όλες οι καταγεγραμμένες αδυναμίες των υφιστάμενων συσκευών και εφαρμογών, οι οποίες συμπληρώνονται ως στοιχεία στα πλαίσια δεδομένων.

Με την εκτέλεση του προγράμματος, το εργαλείο διαβάζει όλες τις εισόδους και παραπέμπει τον χρήστη να διαλέξει ποια από τις υφιστάμενες συσκευές θέλει να θέσει ως στόχο, με την επιλογή της συσκευής τρέχει ένας αλγόριθμος που υπολογίζει όλες τις πιθανές αλληλεπιδράσεις των συσκευών που έχουν καταγραφεί και μπορεί να οδηγήσουν στη συσκευή στόχο. Στη συνέχεια με βάση τη συνδεσιμότητα, τη δυνατότητα εκτέλεσης και τις υφιστάμενες αδυναμίες, συνδυάζονται οι πιθανές αλληλεπιδράσεις και καταγράφονται όλα τα μονοπάτια επιθέσεων που δύναται να αξιοποιηθούν στο πλαίσιο της υφιστάμενης υποδομής. Για κάθε μονοπάτι δημιουργείται ένας πίνακας χαρακτηριστικών που λειτουργεί ως το γενικότερο επίπεδο αδυναμίας του μονοπατιού, το οποίο τελικά συγκρίνεται με ανάλογα δομημένους πίνακες που εκφράζουν προφίλ κακόβουλων χρηστών. Με βάση τα παραπάνω υπολογίζεται το ρίσκο και οι επιπτώσεις από κάθε πιθανό μονοπάτι επίθεσης συνδυαστικά με κάθε πιθανό προφίλ κακόβουλου χρήστη.

Με την διαδοχική καταγραφή σεναρίων που εμπεριέχουν διαφορετικές ρυθμίσεις ασφαλείας ο ερευνητής ασφαλείας μπορεί να εντοπίσει ποια μέτρα πρέπει να λάβει για την μείωση των ενεργών μονοπατιών επιθέσεων και συνεπώς την προστασία των κρίσιμων συστημάτων της υποδομής που μελετά.

GUI Application

Η διαδοχική καταγραφή σεναρίων που εμπεριέχουν διαφορετικές ρυθμίσεις ασφαλείας από τον ερευνητή ασφαλείας αποτελεί ιδιαίτερα χρονοβόρα διαδικασία. Για την επιτάχυνση της καταγραφής των απαραίτητων δεδομένων αναπτύχθηκε ένα γραφικό περιβάλλον στο οποίο οι ερευνητές ασφαλείας έχουν τη δυνατότητα να δημιουργήσουν τα αρχεία devices.csv και networks.csv μέσα από μια σειρά από φόρμες:

[1] https://nvd.nist.gov/

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο
ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ ΟΙΚΟΝΟΜΙΑΣ & ΑΝΑΠΤΥΞΗΣ
ΕΙΔΙΚΗ ΓΡΑΜΜΑΤΕΙΑ ΕΤΠΑ & ΤΣ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ ΕΠΑνΕΚ
ΕΠΑνΕΚ 2014-2020
ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΑΝΤΑΓΩΝΙΣΤΙΚΟΤΗΤΑ ΕΠΙΧΕΙΡΗΜΑΤΙΚΟΤΗΤΑ ΚΑΙΝΟΤΟΜΙΑ
ΕΣΠΑ 2014-2020
ανάπτυξη - εργασία - αλληλεγγύη
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

- Στο πλαίσιο της φόρμας **Physical Locations** ο χρήστης καλείται να καταγράψει μια λίστα απο φυσικές τοποθεσίες στις οποίες μπορεί να είναι εγκατεστημένα τα δίκτυα και οι συσκευές του οργανισμού υπό εξέταση. Οι φυσικές τοποθεσίες έχουν τρείς κατηγορίες: εσωτερική, εξωτερική, προστατευμένη.
- Στο πλαίσιο της φόρμας **Networks** ο χρήστης καλείται να καταγράψει όλα τα διαθέσιμα δίκτυα του οργανισμού υπο εξέταση, την τοποθεσία στην οποία έχουν εγκατασταθεί, μια σειρά χαρακτηριστικών για κάθε δίκτυο (τεχνολογία, συχνότητα, τύπος δικτύου) καθώς και θα μέτρα ασφαλείας που τηρούνται στο πλαίσιο του δικτύου(CIA controls).
- Στο πλαίσιο της φόρμας **Network Interconnections** ο χρήστης καλείται να καταγράψει όλες τις διασυνδέσεις μεταξύ των δικτύων που δηλώθηκαν στην προηγούμενη φόρμα καθώς και τα μέτρα ασφαλείας που τηρούνται στο πλαίσιο της κάθε σύνδεσης(CIA controls).
- Στο πλαίσιο της φόρμας **Devices** ο χρήστης καλείται να καταγράψει όλες τις διαθέσιμες συσκευές της υποδομής υπο εξέταση και να ορίσει μια λίστα από χαρακτηριστικά:

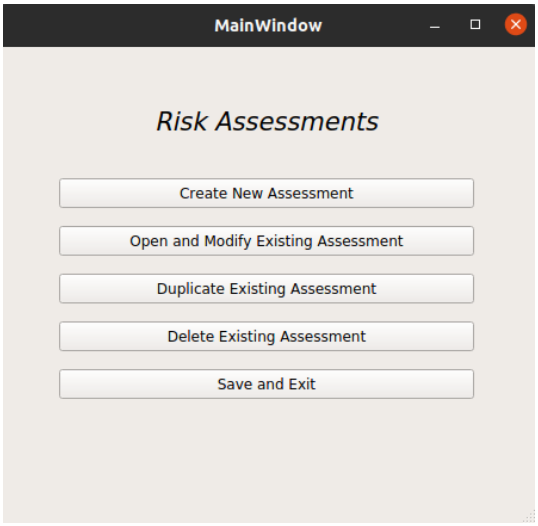
    - Γενικά χαρακτηριστικά όπως όνομα συσκευής είδος συσκευής, τοποθεσία συσκευής.
    - Χαρακτηριστικά συνδεσιμότητας όπως οι διεπαφές της συσκευής, ο τύπος της διεπαφής και το δίκτυο στο οποίο συνδέεται η διεπαφή.
    - Ειδικά χαρακτηριστικά συσκευής όπως τύπος asset(HW,OS,App), όνομα κατασκευαστή, όνομα προϊόντος, έκδοση προϊόντος που παράγουν το Common Platform Enumeration (CPE) URI του asset.

- Στο πλαίσιο της φόρμας **Device Interconnections** ο χρήστης καλείται να καταγράψει όλες τις διασυνδέσεις μεταξύ των καταγεγραμμένων συσκευών καθώς και τα χαρακτηριστικά της σύνδεσης που περιλαμβάνουν τα δικαιώματα εκτέλεσης και την χωρική εγγύτητα.
- Στο πλαίσιο της φόρμας **Conduct Risk Assessment** ο χρήστης καλείται να:

    - Επιλέξει τις ευπάθειες που αναλογούν σε κάθε συσκευή. Βάσει του asset που έχει οριστεί σε κάθε συσκευή το εργαλείο τραβάει δυναμικά και προβάλει στο χρήστη τη λίστα των γνωστών ευπαθειών που του αναλογούν από το Application Programming Interface (API) του εθνικού ινστιτούτου τεχνολογίας (NIST).
    - Αποθηκεύσει τις πληροφορίες που συμπλήρωσε στις φόρμες σε μορφή csv μέσω της επιλογής translate forms.

3.1.1. Βήματα μεθοδολογίας σε βασικό σενάριο χρήσης

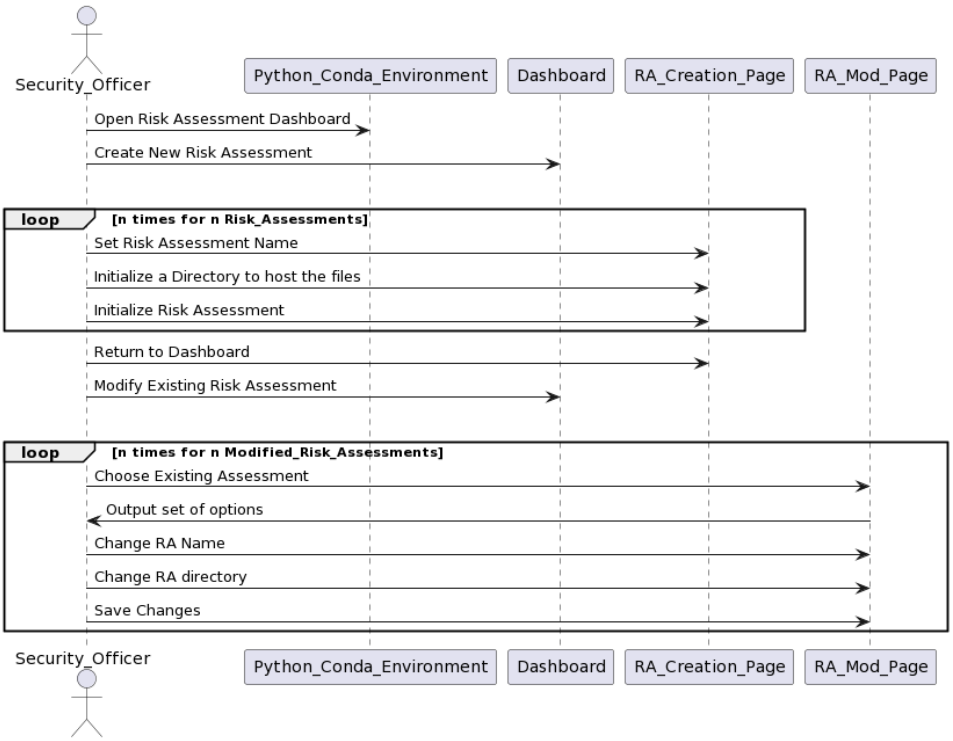
Το πρώτο βήμα για τον αναλυτή επικινδυνότητας που θέλει να κάνει αποτίμηση επικινδυνότητας για τα φυσικά και ψηφιακά συστήματα της υποδομής που μελετά, είναι να εκτελέσει την εφαρμογή σε ένα περιβάλλον python και να ακολουθήσει την επιλογή Create New Risk Assessment της κεντρικής σελίδας της εφαρμογής. Η κεντρική σελίδα παρουσιάζεται στην Εικόνα 9.



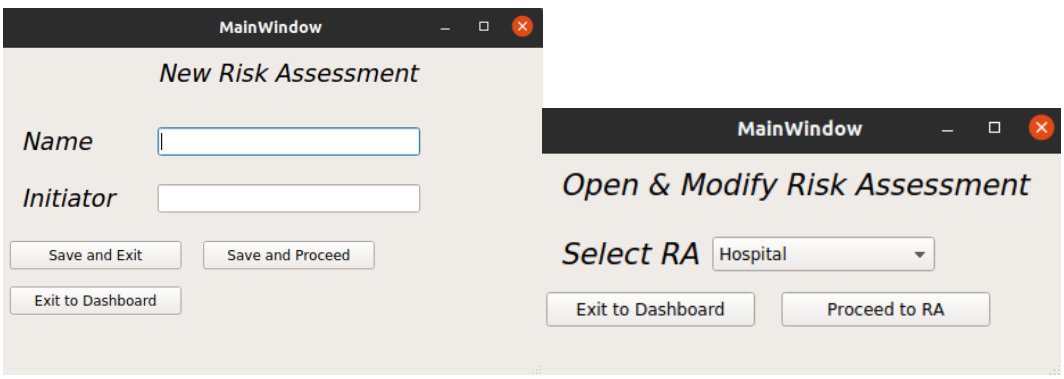
ΕΙΚΟΝΑ 9: RISK ASSESSMENT GUI-GENERAL DASHBOARD

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο
ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ ΟΙΚΟΝΟΜΙΑΣ & ΑΝΑΠΤΥΞΗΣ
ΕΙΔΙΚΗ ΓΡΑΜΜΑΤΕΙΑ ΕΤΠΑ & ΤΣ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ ΕΠΑνΕΚ
ΕΠΑνΕΚ 2014-2020
ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΑΝΤΑΓΩΝΙΣΤΙΚΟΤΗΤΑ ΕΠΙΧΕΙΡΗΜΑΤΙΚΟΤΗΤΑ ΚΑΙΝΟΤΟΜΙΑ
ΕΣΠΑ 2014-2020
ανάπτυξη - εργασία - αλληλεγγύη
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Στο πλαίσιο της φόρμας Create New Risk Assessment πρέπει να οριστεί ένα όνομά για την παρούσα εκτίμηση ρίσκου και να δημιουργήσει ένα καινούργιο directory στο οποίο θα αποθηκευτούν τα παραγόμενα αρχεία. Ο αναλυτής κινδύνου μπορεί στη συνέχεια να προχωρήσει απευθείας στη σελίδα της εκτίμησης κινδύνου και να ξεκινήσει τη διαδικασία αποτίμησης επικινδυνότητας. Μέσω της κεντρικής σελίδας υπάρχει δυνατότητα πρόσβασης, επεξεργασίας και διαγραφής παλαιότερων εκτιμήσεων. Οι διαδικασίες που εκτελούνται στο πλαίσιο της παρούσας φόρμας παρουσιάζονται στο διάγραμμα ροής στην Εικόνα 10, οι φόρμες Create/Modify/Delete Risk Assessment παρουσιάζονται στις Εικόνες 10,11,12 και τέλος η σελίδα εκτίμησης ρίσκου παρουσιάζεται στην Εικόνα 12.

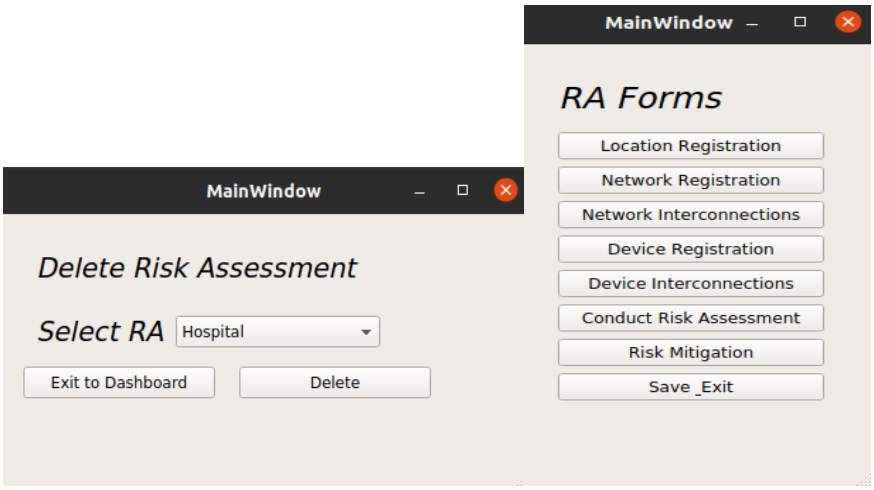


ΕΙΚΟΝΑ 10: ΔΙΑΓΡΑΜΜΑ ΡΟΗΣ ΓΙΑ ΤΙΣ ΦΟΡΜΕΣ CREATE/MODIFY/DELETE RISK ASSESSMENT



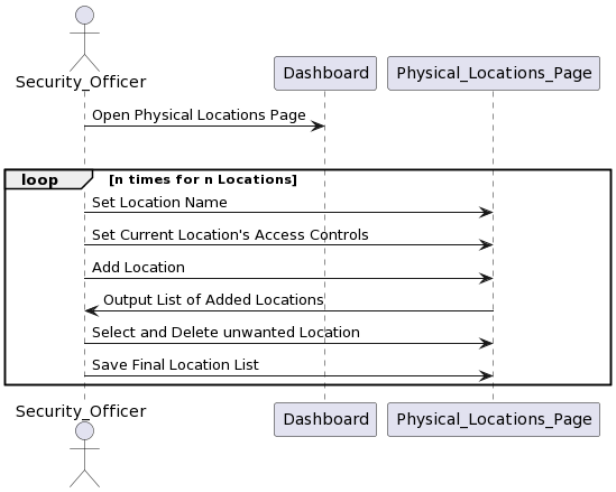
ΕΙΚΟΝΑ 11: RISK ASSESSMENT GUI-OPEN AND MODIFY EXISTING ASSESSMENT-GUI-CREATE NEW ASSESSMENT

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο
ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ ΟΙΚΟΝΟΜΙΑΣ & ΑΝΑΠΤΥΞΗΣ
ΕΙΔΙΚΗ ΓΡΑΜΜΑΤΕΙΑ ΕΤΠΑ & ΤΣ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ ΕΠΑνΕΚ
ΕΠΑνΕΚ 2014-2020
ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΑΝΤΑΓΩΝΙΣΤΙΚΟΤΗΤΑ ΕΠΙΧΕΙΡΗΜΑΤΙΚΟΤΗΤΑ ΚΑΙΝΟΤΟΜΙΑ
ΕΣΠΑ 2014-2020
ανάπτυξη - εργασία - αλληλεγγύη
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης



ΕΙΚΟΝΑ 12: RISK ASSESSMENT GUI-DELETE EXISTING ASSESSMENT AND GUI-RISK ASSESSMENT FORMS

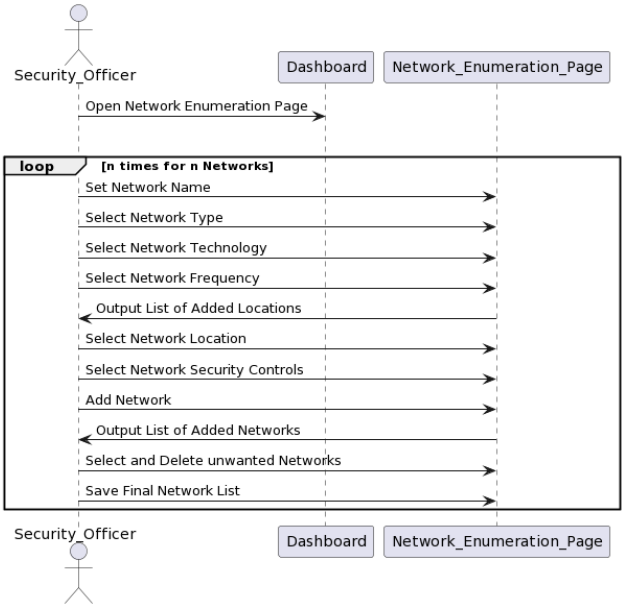
Στο πλαίσιο της φόρμας Location Registration ο χρήστης καλείται να καταγράψει μια λίστα από φυσικές τοποθεσίες στις οποίες μπορεί να είναι εγκατεστημένα τα δίκτυα και οι συσκευές του οργανισμού υπό εξέταση. Οι φυσικές τοποθεσίες έχουν τρεις κατηγορίες: εσωτερική, εξωτερική, προστατευμένη. Οι διαδικασίες που εκτελούνται στο πλαίσιο της παρούσας φόρμας παρουσιάζονται στο διάγραμμα ροής στην Εικόνα 13.



ΕΙΚΟΝΑ 13: ΔΙΑΓΡΑΜΜΑ ΡΟΗΣ ΓΙΑ ΤΗ ΦΟΡΜΑ PHYSICAL LOCATIONS

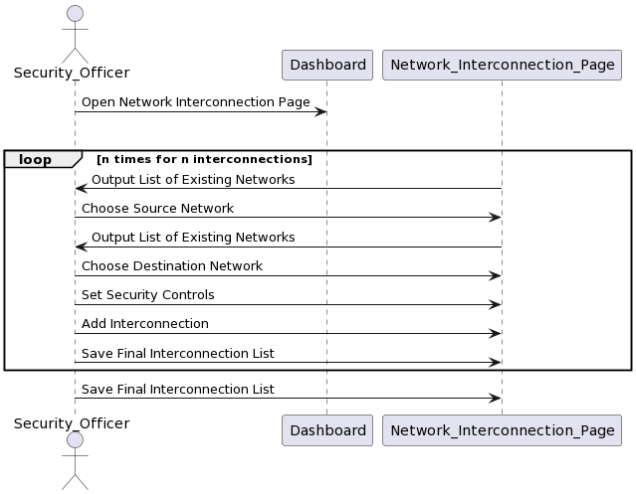
Στο πλαίσιο της φόρμας Network Enumeration ο χρήστης καλείται να καταγράψει όλα τα διαθέσιμα δίκτυα του οργανισμού υπό εξέταση, την τοποθεσία στην οποία έχουν εγκατασταθεί, μια σειρά χαρακτηριστικών για κάθε δίκτυο (τεχνολογία, συχνότητα, τύπος δικτύου) καθώς και θα μέτρα ασφαλείας που τηρούνται στο πλαίσιο του δικτύου(CIA controls). Οι διαδικασίες που εκτελούνται στο πλαίσιο της παρούσας φόρμας παρουσιάζονται στο διάγραμμα ροής στην Εικόνα 14.

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο
ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ ΟΙΚΟΝΟΜΙΑΣ & ΑΝΑΠΤΥΞΗΣ
ΕΙΔΙΚΗ ΓΡΑΜΜΑΤΕΙΑ ΕΤΠΑ & ΤΣ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ ΕΠΑνΕΚ
ΕΠΑνΕΚ 2014-2020
ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΑΝΤΑΓΩΝΙΣΤΙΚΟΤΗΤΑ ΕΠΙΧΕΙΡΗΜΑΤΙΚΟΤΗΤΑ ΚΑΙΝΟΤΟΜΙΑ
ΕΣΠΑ 2014-2020
ανάπτυξη - εργασία - αλληλεγγύη
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης



ΕΙΚΟΝΑ 14: ΔΙΑΓΡΑΜΜΑ ΡΟΗΣ ΓΙΑ ΤΗ ΦΟΡΜΑ NETWORK ENUMERATION

Στο πλαίσιο της φόρμας Network Interconnections ο χρήστης καλείται να καταγράψει όλες τις διασυνδέσεις μεταξύ των δικτύων που δηλώθηκαν στην προηγούμενη φόρμα καθώς και τα μέτρα ασφαλείας που τηρούνται στο πλαίσιο της κάθε σύνδεσης(CIA controls). Οι διαδικασίες που εκτελούνται στο πλαίσιο της παρούσας φόρμας παρουσιάζονται στο διάγραμμα ροής στην Εικόνα 15.



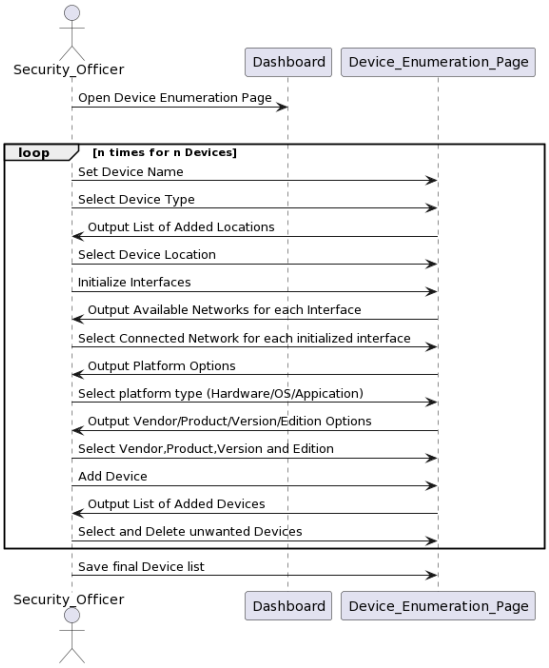
ΕΙΚΟΝΑ 15: ΔΙΑΓΡΑΜΜΑ ΡΟΗΣ ΓΙΑ ΤΗ ΦΟΡΜΑ NETWORK INTERCONNECTIONS

Στο πλαίσιο της φόρμας Devices ο χρήστης καλείται να καταγράψει όλες τις διαθέσιμες συσκευές της υποδομής υπό εξέταση και να ορίσει μια λίστα απο χαρακτηριστικά:

- Γενικά χαρακτηριστικά όπως όνομα συσκευής είδος συσκευής, τοποθεσία συσκευής.
- Χαρακτηριστικά συνδεσιμότητας όπως οι διεπαφές της συσκευής, ο τύπος της διεπαφής και το δίκτυο στο οποίο συνδέεται η διεπαφή.
- Ειδικά χαρακτηριστικά συσκευής όπως τύπος asset(HW,OS,App), όνομα κατασκευαστή, όνομα προϊόντος, έκδοση προϊόντος που παράγουν το Common Platform Enumeration (CPE) URI του asset.

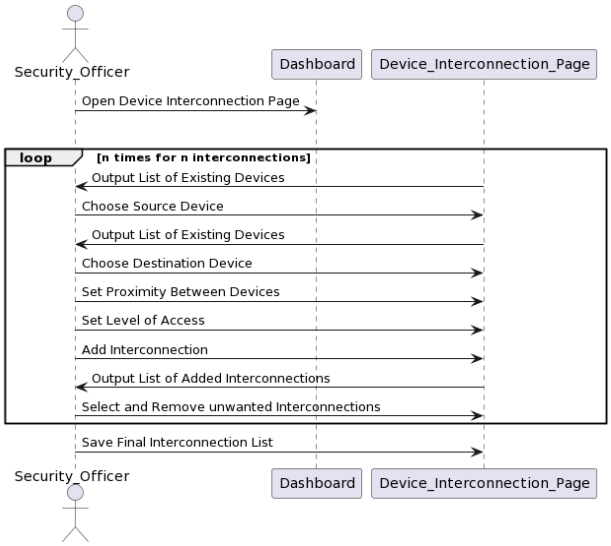
Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο
ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ
ΟΙΚΟΝΟΜΙΑΣ & ΑΝΑΠΤΥΞΗΣ
ΕΙΔΙΚΗ ΓΡΑΜΜΑΤΕΙΑ ΕΠΠΑ & ΤΣ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ ΕΠΑνΕΚ
ΕΠΑνΕΚ 2014-2020
ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΑΝΤΑΓΩΝΙΣΤΙΚΟΤΗΤΑ
ΕΠΙΧΕΙΡΗΜΑΤΙΚΟΤΗΤΑ
ΚΑΙΝΟΤΟΜΙΑ
ΕΣΠΑ 2014-2020
ανάπτυξη - εργασία - αλληλεγγύη
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Οι διαδικασίες που εκτελούνται στο πλαίσιο της παρούσας φόρμας παρουσιάζονται στο διάγραμμα ροής στην Εικόνα 16.



ΕΙΚΟΝΑ 16: ΔΙΑΓΡΑΜΜΑ ΡΟΗΣ ΓΙΑ ΤΗ ΦΟΡΜΑ DEVICE ENUMERATION

Στο πλαίσιο της φόρμας Device Interconnections ο χρήστης καλείται να καταγράψει όλες τις διασυνδέσεις μεταξύ των καταγεγραμμένων συσκευών καθώς και τα χαρακτηριστικά της σύνδεσης που περιλαμβάνουν τα δικαιώματα εκτέλεσης και την χωρική εγγύτητα.



ΕΙΚΟΝΑ 17: ΔΙΑΓΡΑΜΜΑ ΡΟΗΣ ΓΙΑ ΤΗ ΦΟΡΜΑ DEVICE ENUMERATION

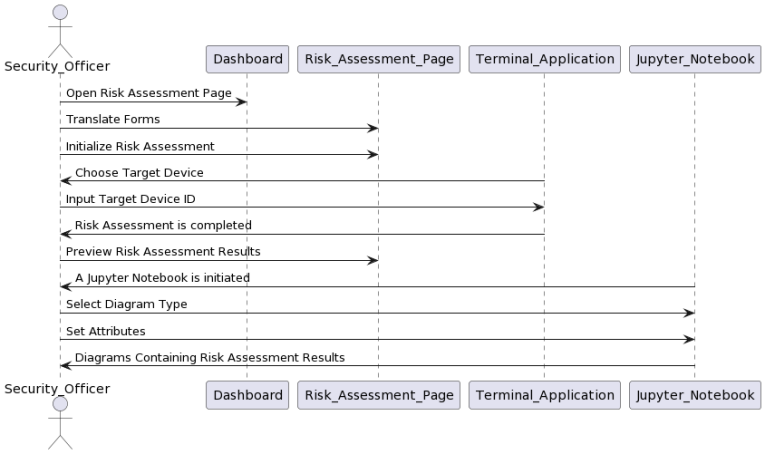
Στο πλαίσιο της φόρμας Conduct Risk Assessment ο χρήστης καλείται να:

- Επιλέξει τις ευπάθειες που αναλογούν σε κάθε συσκευή. Βάσει του asset που έχει οριστεί σε κάθε συσκευή το εργαλείο τραβάει δυναμικά και προβάλλει στο χρήστη τη λίστα των γνωστών ευπαθειών που του αναλογούν από το Application Programming Interface (API) του εθνικού ινστιτούτου τεχνολογίας (NIST).

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο
ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ ΟΙΚΟΝΟΜΙΑΣ & ΑΝΑΠΤΥΞΗΣ
ΕΙΔΙΚΗ ΓΡΑΜΜΑΤΕΙΑ ΕΤΠΑ & ΤΣ
ΕΠΑνΕΚ 2014-2020
ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΑΝΤΑΓΩΝΙΣΤΙΚΟΤΗΤΑ ΕΠΙΧΕΙΡΗΜΑΤΙΚΟΤΗΤΑ ΚΑΙΝΟΤΟΜΙΑ
ΕΣΠΑ 2014-2020
ανάπτυξη - εργασία - αλληλεγγύη
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

- Αποθηκεύσει τις πληροφορίες που συμπλήρωσε στις φόρμες σε μορφή csv μέσω της επιλογής translate forms.
- Να εκκινήσει τη διαδικασία του Risk Assessment και να επιλέξει μια συσκευή ως στόχο.

Οι διαδικασίες που εκτελούνται στο πλαίσιο της παρούσας φόρμας παρουσιάζονται στο διάγραμμα ροής στην Εικόνα 18.



ΕΙΚΟΝΑ 18: ΔΙΑΓΡΑΜΜΑ ΡΟΗΣ ΓΙΑ ΤΗ ΦΟΡΜΑ CONDUCT RISK ASSESSMENT

3.2. Τεχνολογίες υλοποίησης

Η υλοποίηση της εφαρμογής γραφικού περιβάλλοντος πραγματοποιήθηκε μέσω της βιβλιοθήκης Python pyQT5, ενώ οι δομές δεδομένων καταγράφηκαν μέσω της βιβλιοθήκης pandas σε Dataframes. Τέλος η κλήση στο API του NIST που επιστρέφει τις ευπάθειες πραγματοποιείται μέσω των βιβλιοθηκών requests και json.

Το εργαλείο έχει αναπτυχθεί στην προγραμματιστική γλώσσα Python 3.7 και λειτουργεί ως εργαλείο γραμμής εντολών. Περιλαμβάνει υλοποιήσεις των βιβλιοθηκών pandas,cvss, cvsslib,requests, xmltodict και json. Κατά την εκτέλεση, το εργαλείο δέχεται ως είσοδο csv αρχεία που περιλαμβάνουν λεξικά για την επεξεργασία δεδομένων βάσεων αδυναμιών και δυο csv αρχεία που περιλαμβάνουν στοιχεία για το σύστημα υπό διερεύνηση, το devices.csv και το networks.csv όπου καταγράφονται λεπτομέρειες για τις ενεργές συσκευές και δίκτυα, τα οποία αργότερα μετατρέπονται σε πλαίσια δεδομένων (Dataframes) της βιβλιοθήκης pandas.

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο
ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ ΟΙΚΟΝΟΜΙΑΣ & ΑΝΑΠΤΥΞΗΣ
ΕΙΔΙΚΗ ΓΡΑΜΜΑΤΕΙΑ ΕΠΑ & ΤΣ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ ΕΠΑνΕΚ
ΕΠΑνΕΚ 2014-2020
ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΑΝΤΑΓΩΝΙΣΤΙΚΟΤΗΤΑ ΕΠΙΧΕΙΡΗΜΑΤΙΚΟΤΗΤΑ ΚΑΙΝΟΤΟΜΙΑ
ΕΣΠΑ 2014-2020
ανάπτυξη - εργασία - αλληλεγγύη
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

4. Κατανεμημένη υποδομή για τον έλεγχο πρόσβασης σε ιατρικά δεδομένα «Hierarchical Multi Blockchain»

Σε αυτή την ενότητα παρουσιάζει μία υλοποίηση του συστήματος Hierarchical Multi Blockchain (HMBC) που σχεδιάστηκε στο πλαίσιο των παραδοτέων Π4.1, Π4.4 και Π4.5, καθώς και των σχετικών ερευνητικών δημοσιεύσεων που αντιστοιχούν στα παραδοτέα αυτά, και υλοποιήθηκε στο πλαίσιο του παραδοτέου Π4.6. Η υλοποίηση αυτή χρησιμοποιείται για την ολοκλήρωση και την επίδειξη των αποτελεσμάτων του έργου και προτείνει ένα σύστημα το οποίο επιλύει ζητήματα ασφάλειας κατά την πρόσβαση που αναγνωρίστηκαν στα παραδοτέα Π 3.1, Π 3.2 και Π 3.4.

Η συγκεκριμένη πλατφόρμα δίνει τη δυνατότητα σε πληροφοριακά συστήματα όπου συμμετέχουν πολλοί εμπλεκόμενοl να ανταλλάσσουν ευαίσθητη πληροφορία, προστατεύοντας την εμπιστευτικότητα, ακεραιότητα καθώς και την αυθεντικότητα αυτής, ενώ ταυτόχρονα αξιοποιεί την τεχνολογία Blockchain ώστε όλοι οι εμπλεκόμενοι να έχουν εικόνα των ενεργειών που συνέβησαν στην ευαίσθητη πληροφορία ή στις ευαίσθητες λειτουργίες των συστημάτων.

Επίσης, επιτρέπει την αποστολή και την παραλαβή ευαίσθητης πληροφορίας (ή την αποστολή/παραλαβή ευαίσθητων εντολών/αποτελεσμάτων) όπου τόσο η αίτηση όσο και τα αποτελέσματα μπορούν να είναι αναγνώσιμα μόνο από τις οντότητες για τις οποίες ο οργανισμός που είναι κάτοχος των συγκεκριμένων δεδομένων, έχει ορίσει δυναμικά ότι θα είχαν πρόσβαση σε τέτοια πληροφορία. Ως δυναμικό αίτημα πρόσβασης ορίζεται η δυνατότητα του συστήματος να επιτρέπει την άντληση και την πρόσβαση σε πληροφορία μόνο από οντότητες οι οποίες έχουν λάβει την κατάλληλη έγκριση από το εμπλεκόμενο μέρος στο οποίο ανήκουν, μέσω πολιτικών. Οι πολιτικές αυτές μπορούν να ανανεώνονται από το κάθε εμπλεκόμενο μέρος, οποιαδήποτε στιγμή, σύμφωνα με τις εκάστοτε ανάγκες και συνθήκες. Για παράδειγμα, ένας γιατρός ο οποίος ανήκει σε ένα εμπλεκόμενο μέρος (stakeholder) του συστήματος (π.χ. ιατρικό οργανισμό), μπορεί να λάβει το ιατρικό ιστορικό ενός ασθενή ο οποίος χρήζει ιατρικής παρακολούθησης, μόνο εφόσον ικανοποιεί τουλάχιστον μία από τις παρακάτω δύο συνθήκες:

1. Εάν ο γιατρός είναι ο θεράπων ιατρός του ασθενούς
2. Εάν ο γιατρός αυτός είναι *γιατρός εν εφημερία*, για τη χρονική περίοδο (ωράριο εργασίας/εφημερίας) όπου ο ασθενής χρήζει παρακολούθησης

Οι παραπάνω δύο συνθήκες εκτελούνται και ελέγχονται αυτόματα από το σύστημα, μέσω των εξατομικευμένων πολιτικών του κάθε εμπλεκόμενου μέρους. Στο συγκεκριμένο παράδειγμα, αξιοποιούνται οι πολιτικές του ιατρικού οργανισμού στον οποίο ανήκει ο γιατρός αυτός ο οποίος επιθυμεί να λάβει πρόσβαση στα δεδομένα του ασθενούς.

Όπως γίνεται αντιληπτό, ένα εξαιρετικά σημαντικό σημείο της προτεινόμενης υλοποίησης είναι πως οι πολιτικές αυτές δεν απαιτούν καμία άλλη ενέργεια από τα εμπλεκόμενα μέρη, πέραν της ανανέωσής τους, αφού αξιοποιούνται αυτόματα από το σύστημα, χωρίς να απαιτούν την ύπαρξη του ανθρώπινου παράγοντα κατά τη λήψη αποφάσεων και γενικότερα κατά την εκτέλεση κρίσιμων ενεργειών.

4.1.Λειτουργίες συστήματος

Στο σύστημα αναπτύσσονται πέντε (5) σενάρια χρήσης, μέσω των οποίων διαφαίνονται μερικές από τις κύριες δυνατότητες του, όπως αυτές είναι:

- Δημιουργία αιτήματος για τη λήψη πληροφοριών από τα εμπλεκόμενα μέρη.
- Αυθεντικοποίηση και Εξουσιοδότηση οντότητας.
- Συγκέντρωση και αξιοποίηση ρόλων οντότητας (μόνιμων και προσωρινών, π.χ. Γιατρός, Ερευνητής (Μόνιμοι ρόλοι) και Ωράριο βάρδιας εργασίας, Θεράπων ιατρός ασθενούς (Προσωρινοί ρόλοι).
- Προώθηση αιτήματος στο αρμόδιο Domain Blockchain.
- Λήψη δεδομένων και πληροφοριών, που αφορούν το αίτημα, από τις Βάσεις Δεδομένων των εμπλεκόμενων μερών του συστήματος.
- Μερική και Πλήρης αποκρυπτογράφηση δεδομένων.
- Προώθηση των ληφθέντων πληροφοριών από τα εμπλεκόμενα μέρη, που αφορούν ένα αίτημα μιας οντότητας, στην οντότητα αυτή.

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο
ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ ΟΙΚΟΝΟΜΙΑΣ & ΑΝΑΠΤΥΞΗΣ
ΕΙΔΙΚΗ ΓΡΑΜΜΑΤΕΙΑ ΕΤΠΑ & ΤΣ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ ΕΠΑνΕΚ
ΕΠΑνΕΚ 2014-2020
ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΑΝΤΑΓΩΝΙΣΤΙΚΟΤΗΤΑ ΕΠΙΧΕΙΡΗΜΑΤΙΚΟΤΗΤΑ ΚΑΙΝΟΤΟΜΙΑ
ΕΣΠΑ 2014-2020
ανάπτυξη - εργασία - αλληλεγγύη
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Τα διαθέσιμα σενάρια που αναπτύσσονται στο παραδοτέο, αναφέρονται και περιγράφονται στον πίνακα που ακολουθεί:

Σενάρια	Ονομασία	Περιγραφή	Ρόλος χρήστη	Αποδέκτης
Data_00	***GET PATIENT HISTORY***	Λήψη του ιατρικού ιστορικού ενός ασθενή	**ΓΙΑΤΡΟΣ** (Νοσοκομείο)	Νοσοκομεία
Data_01	***CHECK DEVICE FIRMWARE***	Έλεγχος υλισμικού σχετικά με το αν διαθέτει το νεότερο διαθέσιμο firmware	**ΤΕΧΝΙΚΟΣ** (Νοσοκομείο)	Κατασκευαστής Ιατρικού Εξοπλισμού
Data_02	***GET FAULT STATS***	Λήψη στατιστικών σχετικά με τα σφάλματα τα οποία έχει εμφανίσει ένα μοντέλο μίας συσκευής	**ΕΡΕΥΝΗΤΗΣ** (Νοσοκομείο)	Κατασκευαστής Ιατρικού Εξοπλισμού
Data_03	***GET DISEASE STATS***	Λήψη στατιστικών που αφορούν μία συγκεκριμένη ασθένεια	**ΕΡΕΥΝΗΤΗΣ** (Νοσοκομείο)	Νοσοκομεία
Data_04	***IS DEVICE OWNED***	Λήψη πληροφοριών που αφορούν την ύπαρξη μιας συσκευής στις διαθέσιμες κλινικές	**ΥΠΑΛΛΗΛΟΣ ΚΑΤΑΣΚΕΥΑΣΤΗ ΙΑΤΡΙΚΟΥ ΕΞΟΠΛΙΣΜΟΥ** (Κατασκευαστής)	Νοσοκομεία

ΠΙΝΑΚΑΣ 1: ΣΕΝΑΡΙΑ ΣΥΣΤΗΜΑΤΟΣ

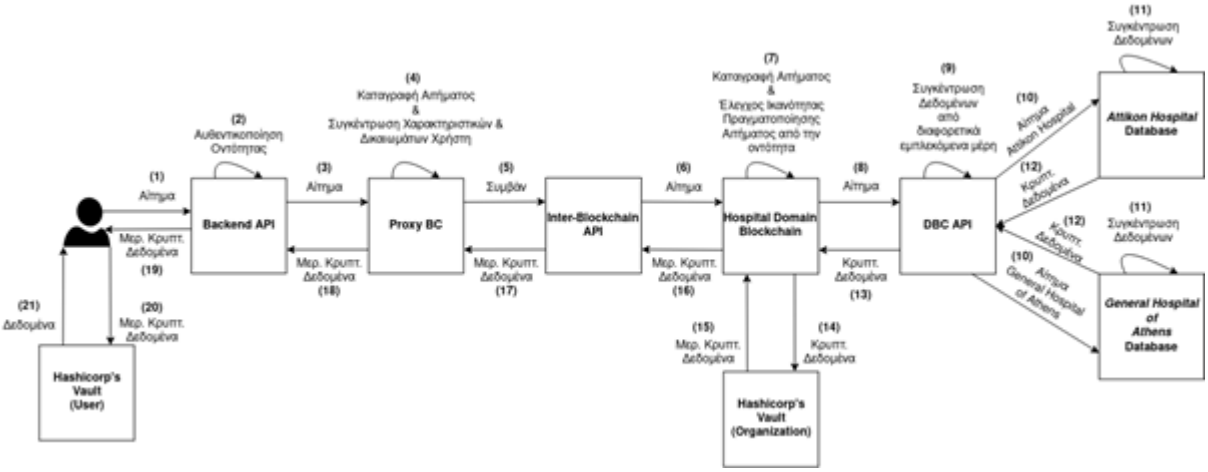
4.1.1.Ανάπτυξη Παραδείγματος Σεναρίου

Στο παρόν σημείο, θα αναπτυχθεί και θα παρουσιαστεί το σενάριο που αναπτύσσεται στο σύστημα, *GET PATIENT HISTORY* (***Data_00***), κατά το οποίο ένας γιατρός ζητάει από το σύστημα να του αποστείλει το ιατρικό ιστορικό ενός ασθενή.

Σημαντικό σημείο αυτού του αιτήματος είναι πως τα δεδομένα που λαμβάνονται από το σύστημα, από τα εμπλεκόμενα μέρη, είναι σε κρυπτογραφημένη μορφή ενώ για την αξίωση πρόσβασης στα δεδομένα και τη λήψη τους από τα εμπλεκόμενα μέρη, ο χρήστης που συνθέτει και αποστέλλει το αίτημα (Γιατρός), πρέπει να ικανοποιεί συγκεκριμένες προϋποθέσεις οι οποίες ορίζονται τόσο από τις κοινές πολιτικές που υφίστανται στο σύστημα, όσο και από τις εξατομικευμένες πολιτικές του εμπλεκόμενου μέρους στο οποίο ο γιατρός αυτός ανήκει (π.χ. Θεράπων ιατρός, ιατρός σε εφημερία). Συνεπώς, το σύστημα αξιοποιείται πλήρως, αφού όλα του τα μέρη ενεργοποιούνται για την ολοκλήρωση του συγκεκριμένου αιτήματος. Το παράδειγμα θα αναπτυχθεί με βάση τα εμπλεκόμενα μέρη του παραδοτέου, τα οποία αποτελούνται από δύο (2) υποθετικούς οργανισμούς που ανήκουν στον τομέα της υγείας (*Attikon Hospital, General Hospital of Athens)*[2].

[2] Τα ονόματα όλων των εμπλεκόμενων μερών που χρησιμοποιούνται για τους σκοπούς του σεναρίου είναι υποθετικά και χρησιμοποιούνται για να διευκολύνουν την περιγραφή του σεναρίου.

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο
ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ ΟΙΚΟΝΟΜΙΑΣ & ΑΝΑΠΤΥΞΗΣ
ΕΙΔΙΚΗ ΓΡΑΜΜΑΤΕΙΑ ΕΤΠΑ & ΤΣ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ ΕΠΑνΕΚ
ΕΠΑνΕΚ 2014-2020
ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΑΝΤΑΓΩΝΙΣΤΙΚΟΤΗΤΑ ΕΠΙΧΕΙΡΗΜΑΤΙΚΟΤΗΤΑ ΚΑΙΝΟΤΟΜΙΑ
ΕΣΠΑ 2014-2020
ανάπτυξη - εργασία - αλληλεγγύη
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης



ΕΙΚΟΝΑ 19: ΠΑΡΑΔΕΙΓΜΑ ΣΕΝΑΡΙΟΥ ΧΡΗΣΗΣ

Αρχικά, ο Γιατρός (χρήστης εμπλεκόμενου μέρους Attikon Hospital), κατασκευάζει, μέσω της Εφαρμογής Χρήστη (Client Application), ένα αίτημα το οποίο θα αποσταλεί στο Proxy Blockchain για την εκτέλεση του. Το αίτημα αυτό ζητάει τη λήψη του ιατρικού ιστορικού ενός ασθενούς από τις βάσεις δεδομένων όλων των εμπλεκόμενων μερών που διαθέτουν κλινικές δομές.

Στο αίτημα αυτό, ο χρήστης (Γιατρός) συμπεριλαμβάνει το μοναδικό αναγνωριστικό (*UUID*) του ασθενούς, καθώς και τον τύπο του αιτήματος (*Data_00*). Το αίτημα, αφού αποσταλεί από την Εφαρμογή Χρήστη στο Backend API, προωθείται στο Proxy Blockchain. Σε αυτήν τη φάση, το Proxy BC συγκεντρώνει όλα τα ιδιαίτερα γνωρίσματα (Μόνιμους και Προσωρινούς ρόλους) του χρήστη που δημιούργησε το αίτημα (Τύπος Χρήστη (Γιατρός), Ωράριο εφημερίας κ.λπ.) μέσω των εξατομικευμένων πολιτικών, ελέγχει ότι ο οργανισμός στον οποίο ο γιατρός, αυτός, ανήκει, είναι ενεργός και ότι δεν έχει ανακληθεί από τα υπόλοιπα εμπλεκόμενα μέρη, καθώς και ότι το πιστοποιητικό του (X.509 Certificate) είναι αποδεκτό και έγκυρο και εισάγει τα δεδομένα αυτά στο υπάρχον αίτημα. Με την ολοκλήρωση των ανωτέρω, το Proxy BC αποθηκεύει τα στοιχεία του αιτήματος στις καταγραφές του και προωθεί το επεξεργασμένο αίτημα στο Inter-Blockchain API το οποίο το αναλύει και αποφασίζει το Domain Blockchain το οποίο θα πρέπει να το παραλάβει. Στην παρούσα περίπτωση, το αίτημα παραλαμβάνεται από το Hospital Domain Blockchain (HDBC).

Με την παραλαβή του αιτήματος από το κατάλληλο Domain Blockchain, γίνεται έλεγχος των χαρακτηριστικών του χρήστη, προκειμένου το σύστημα να αποφανθεί εάν αυτός έχει τη δυνατότητα λήψης των πληροφοριών που ζήτησε. Στη συγκεκριμένη περίπτωση, ελέγχεται:

- εάν ο χρήστης (Γιατρός), είναι ο θεράπων ιατρός του ασθενούς με το υποβληθέν UUID
- εάν ο χρήστης (Γιατρός) είναι γιατρός σε εφημερία

Εάν τουλάχιστον μία από τις παραπάνω συνθήκες ικανοποιείται, τότε η επεξεργασία του αιτήματος συνεχίζεται. Διαφορετικά, το αίτημα απορρίπτεται και ενημερώνεται το Proxy BC σχετικά με αυτό. Στην περίπτωση της απόρριψης ενός αιτήματος, ο χρήστης ενημερώνεται μέσω του Proxy BC.

Αφού πραγματοποιηθεί ο έλεγχος των χαρακτηριστικών και των ρόλων του χρήστη που δημιούργησε το αίτημα, το Domain Blockchain επικοινωνεί με το DBC API το οποίο στέλνει τα απαραίτητα ερωτήματα στις βάσεις δεδομένων των εμπλεκόμενων μερών που το αίτημα αφορά και, παραλαμβάνει από αυτό, τις πληροφορίες και τα δεδομένα που απαντούν στο ερώτημα που έθεσε ο γιατρός (λήψη ιατρικού ιστορικού ασθενούς με συγκεκριμένο *UUID* αναγνωριστικό).

Με τη λήψη των πληροφοριών του αιτήματος από τις βάσεις δεδομένων των εμπλεκόμενων μερών, το Domain Blockchain εκτελεί τη μερική αποκρυπτογράφηση των δεδομένων αυτών, συνδυάζοντας ταυτόχρονα το μοναδικό αναγνωριστικό του χρήστη που δημιούργησε το αίτημα (GID), ώστε μόνον αυτός να μπορεί να αποκρυπτογραφήσει πλήρως τα δεδομένα. Για την εκτέλεση αυτής της ενέργειας, το Domain Blockchain επικοινωνεί με το Hashirocorp Vault και το ABE Plugin που έχει αναπτυχθεί για τις ανάγκες της παρούσας μελέτης, στο οποίο υλοποιούνται όλες οι ABE κρυπτογραφικές ενέργειες που

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο
ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ ΟΙΚΟΝΟΜΙΑΣ & ΑΝΑΠΤΥΞΗΣ
ΕΙΔΙΚΗ ΓΡΑΜΜΑΤΕΙΑ ΕΤΠΑ & ΤΣ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ ΕΠΑνΕΚ
ΕΠΑνΕΚ 2014-2020
ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΑΝΤΑΓΩΝΙΣΤΙΚΟΤΗΤΑ ΕΠΙΧΕΙΡΗΜΑΤΙΚΟΤΗΤΑ ΚΑΙΝΟΤΟΜΙΑ
ΕΣΠΑ 2014-2020
ανάπτυξη - εργασία - αλληλεγγύη
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

συμβαίνουν στο σύστημα. Με το πέρας και της ανωτέρω διαδικασίας, το Domain Blockchain, επαναπροωθεί το αίτημα και τα μερικώς αποκρυπτογραφημένα δεδομένα, δια μέσω του Inter-Blockchain API, στο Proxy BC. Τότε, το Proxy BC ενημερώνει την υπάρχουσα εγγραφή ότι το αίτημα ολοκληρώθηκε επιτυχώς και αποθηκεύει τα μερικώς αποκρυπτογραφημένα δεδομένα στο Blockchain.

Πλέον, ο χρήστης μπορεί να παραλάβει τα δεδομένα αυτά και να τα αποκρυπτογραφήσει πλήρως, χρησιμοποιώντας τα δικά του εξατομικευμένα ABE κλειδιά που διαθέτει και ικανοποιούν την ABE πολιτική (ABE Policy) με την οποία κρυπτογραφήθηκαν τα δεδομένα που ζήτησε μέσω του αιτήματός του.

4.2.Αρχιτεκτονική συστήματος

Η παρούσα υλοποίηση έχει αναπτυχθεί βάσει της αρθρωτής αρχιτεκτονικής (modular architecture). Όπως παρουσιάστηκε κατά την προηγούμενη ενότητα, κάθε επιμέρους στοιχείο του συστήματος επιτελεί συγκεκριμένη λειτουργία. Όλες οι λειτουργίες συνολικά, συντελούν στο σχεδιασμό του τελικού συστήματος. Όλα τα λογισμικά του συστήματος εκτελούνται σε containerized περιβάλλον και η διαχείριση αυτών επιτυγχάνεται με τη χρήση του λογισμικού *Kubernetes.*

4.2.1.Διαγράμματα Ροής Δεδομένων (Data Flow Charts)

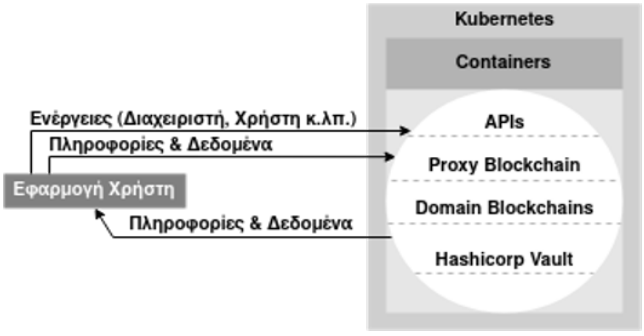
Στην υποενότητα αυτή θα γίνει ανάπτυξη των διαγραμμάτων ροής δεδομένων του συστήματος.

Η ανάπτυξη θα γίνει σε δύο επίπεδα,

- **Επίπεδο 0**: Θα απεικονιστεί το σύστημα ως σύνολο
- **Επίπεδο 1**: Θα παρουσιαστούν συνολικά όλα τα μέρη από τα οποία αποτελείται η υλοποίηση. Επίσης, θα απεικονιστούν οι σχέσεις που έχουν τα διάφορα μέρη του συστήματος αναμεταξύ τους, ενώ ακόμη θα φανούν τα εσωτερικά (internal) κύρια στοιχεία από τα οποία αποτελείται κάθε λογισμικό του συστήματος

Γενικό Διάγραμμα (Context) – Επίπεδο 0

Όπως απεικονίζεται στο διάγραμμα Επιπέδου 0, κάθε λογισμικό το οποίο εκτελείται στο σύστημα, εκτελείται μέσα σε ένα απομονωμένο container, ενώ για τη διαχείριση αυτών των containers (έλεγχος, αποσφαλμάτωση, λειτουργία κ.λπ.), υπεύθυνο είναι το Kubernetes.



ΕΙΚΟΝΑ 20: ΔΙΑΓΡΑΜΜΑ ΕΠΙΠΕΔΟΥ 0

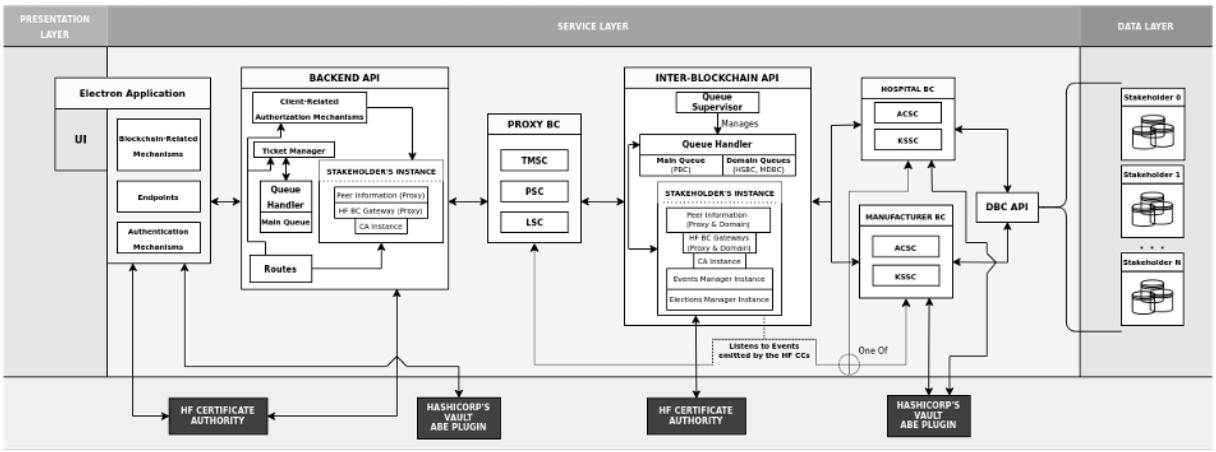
Διάγραμμα– Επίπεδο 1

Στο διάγραμμα *επιπέδου 1*, παρουσιάζονται όλα τα μέρη που συμμετέχουν στη λειτουργία της υλοποίησης καθώς και οι αναμεταξύ τους σχέσεις που δημιουργούνται, ανά στρώμα (Layer) λειτουργικότητας.

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο
ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ ΟΙΚΟΝΟΜΙΑΣ & ΑΝΑΠΤΥΞΗΣ
ΕΙΔΙΚΗ ΓΡΑΜΜΑΤΕΙΑ ΕΤΠΑ & ΤΣ
ΕΠΑνΕΚ 2014-2020
ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΑΝΤΑΓΩΝΙΣΤΙΚΟΤΗΤΑ ΕΠΙΧΕΙΡΗΜΑΤΙΚΟΤΗΤΑ ΚΑΙΝΟΤΟΜΙΑ
ΕΣΠΑ 2014-2020
ανάπτυξη - εργασία - αλληλεγγύη
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Στρώμα Παρουσίασης (Presentation Layer)
• Λογισμικό Εφαρμογής Χρήστη (Electron Application - UI)
Στρώμα Υπηρεσιών (Service Layer)
• Λογισμικό Εφαρμογής Χρήστη (Electron Application) • Λογισμικό Διασύνδεσης Χρήστη – Σύστημα (Backend API) • Λογισμικό Διασύνδεσης Blockchain Συστημάτων (Inter-Blockchain API) • Blockchain Συστήματα (Proxy BC, Domain BCs) • Λογισμικό Διασύνδεσης Συστήματος – Βάσεων Δεδομένων (DBC API) • Αρχή έκδοσης πιστοποιητικών (CA) εμπλεκόμενου μέρους • Hashicorp's Vault ABE Plugin
Στρώμα Δεδομένων (Data Layer)
• Βάσεις Δεδομένων των εμπλεκόμενων μερών

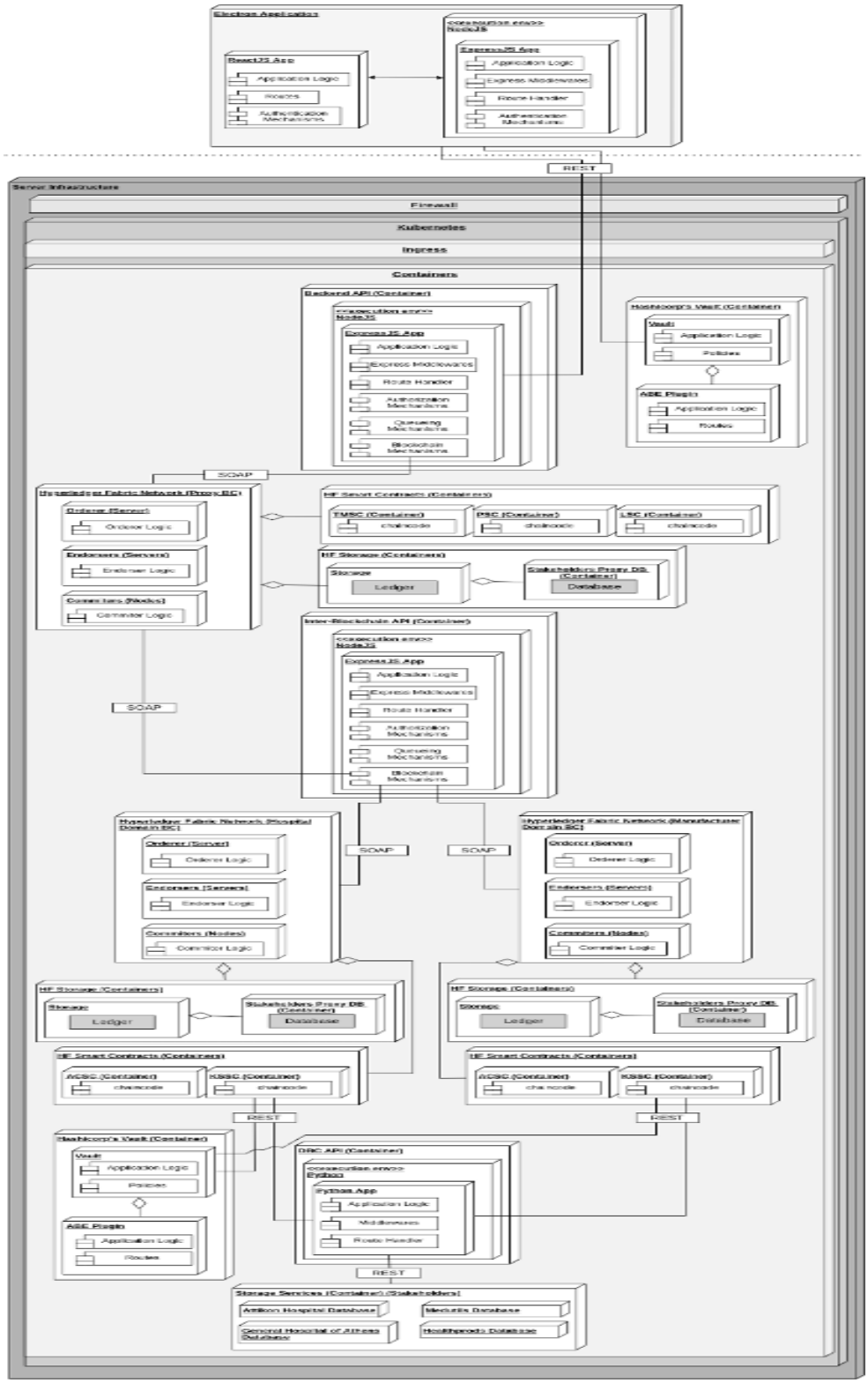
ΠΙΝΑΚΑΣ 2: ΣΤΡΩΜΑΤΑ (LAYERS) ΤΟΥ ΣΥΣΤΗΜΑΤΟΣ



ΕΙΚΟΝΑ 21: ΓΕΝΙΚΗ ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΣΥΣΤΗΜΑΤΟΣ

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο
ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ ΟΙΚΟΝΟΜΙΑΣ & ΑΝΑΠΤΥΞΗΣ
ΕΙΔΙΚΗ ΓΡΑΜΜΑΤΕΙΑ ΕΤΠΑ & ΤΣ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ ΕΠΑνΕΚ
ΕΠΑνΕΚ 2014-2020
ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΑΝΤΑΓΩΝΙΣΤΙΚΟΤΗΤΑ ΕΠΙΧΕΙΡΗΜΑΤΙΚΟΤΗΤΑ ΚΑΙΝΟΤΟΜΙΑ
ΕΣΠΑ 2014-2020
ανάπτυξη - εργασία - αλληλεγγύη
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

4.2.2.Διαγράμματα Όψης Εγκατάστασης (Physical View Diagrams)

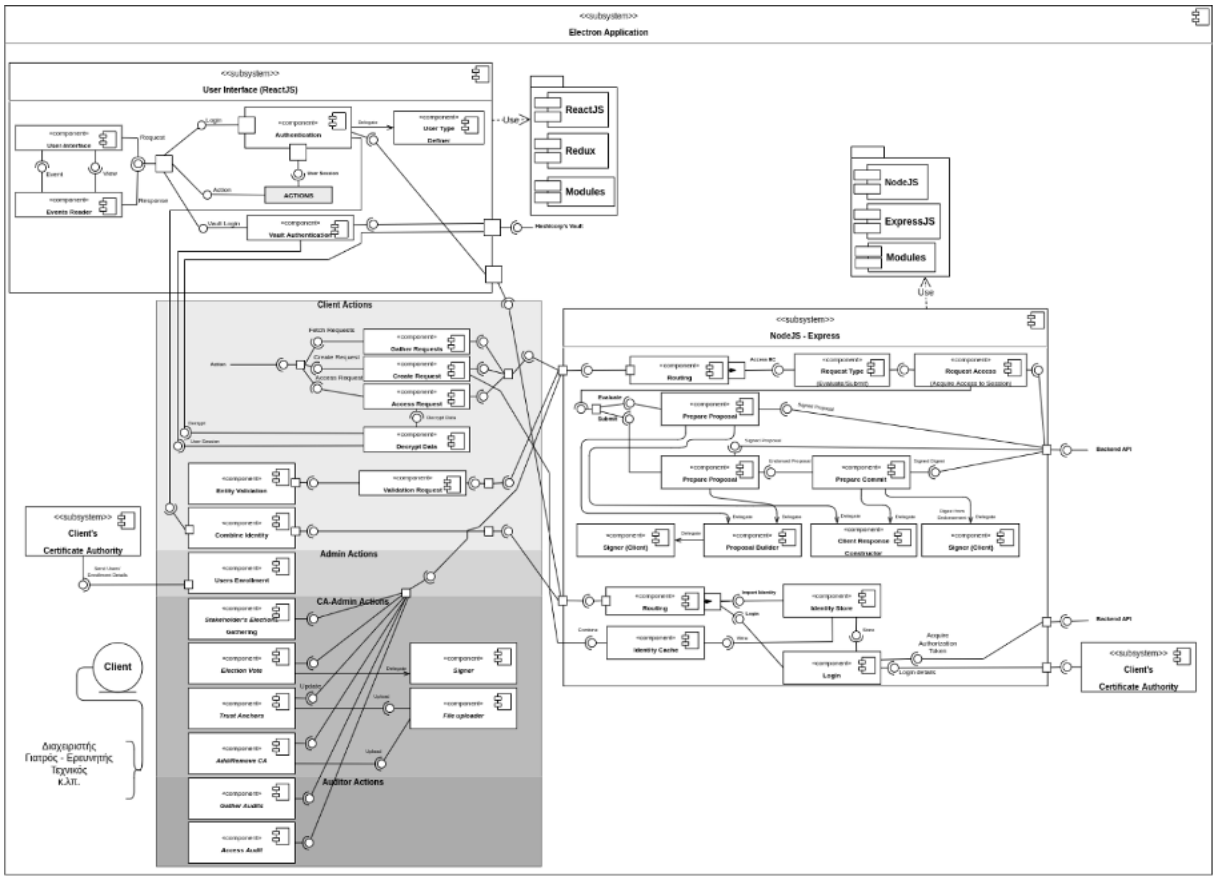


ΕΙΚΟΝΑ 22: ΔΙΑΓΡΑΜΜΑ ΟΨΗΣ

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο
ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ
ΟΙΚΟΝΟΜΙΑΣ & ΑΝΑΠΤΥΞΗΣ
ΕΙΔΙΚΗ ΓΡΑΜΜΑΤΕΙΑ ΕΠΑ & ΤΣ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ ΕΠΑνΕΚ
ΕΠΑνΕΚ 2014-2020
ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΑΝΤΑΓΩΝΙΣΤΙΚΟΤΗΤΑ
ΕΠΙΧΕΙΡΗΜΑΤΙΚΟΤΗΤΑ
ΚΑΙΝΟΤΟΜΙΑ
ΕΣΠΑ 2014-2020
ανάπτυξη - εργασία - αλληλεγγύη
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

4.2.3.Διαγράμματα Όψης Συνιστωσών (Component View Diagrams)

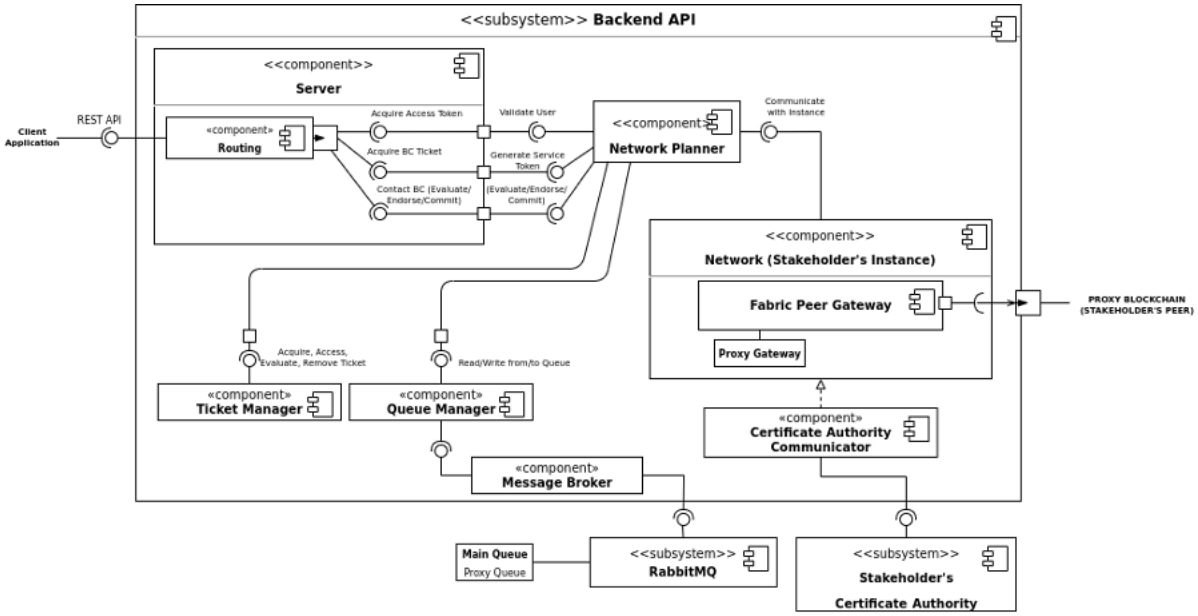
Λογισμικό Εφαρμογής Χρήστη (Electron Application)



ΕΙΚΟΝΑ 23: ELECTRON APPLICATION

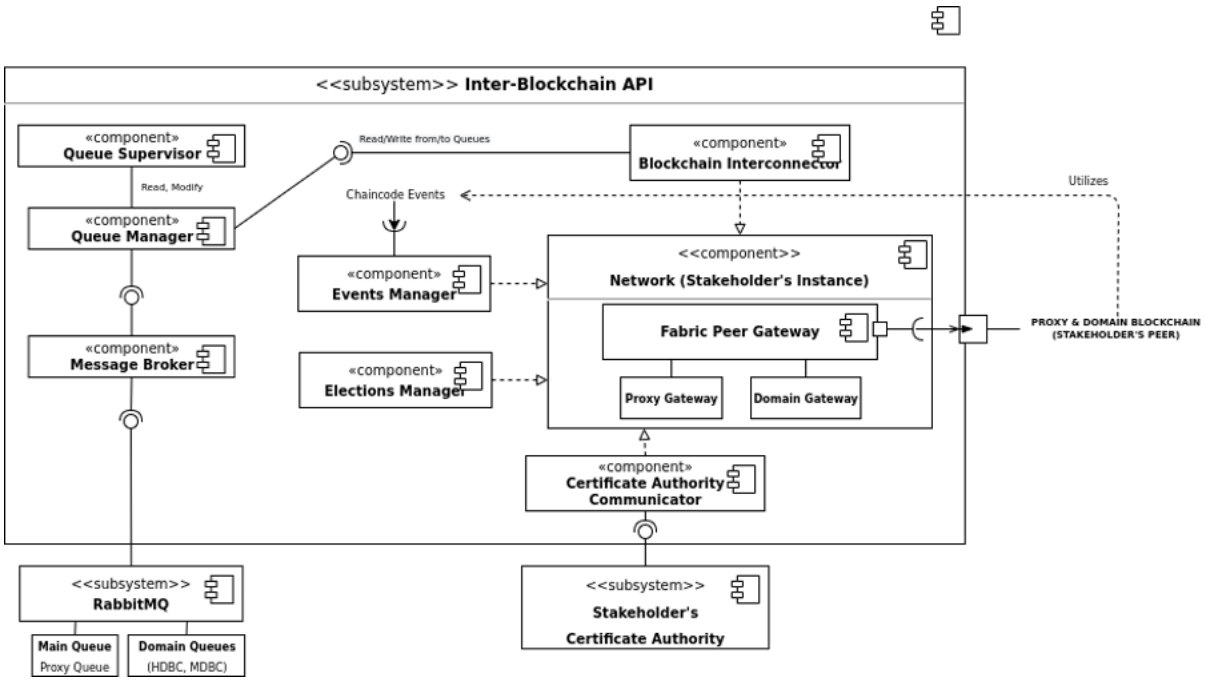
Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο
ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ
ΟΙΚΟΝΟΜΙΑΣ & ΑΝΑΠΤΥΞΗΣ
ΕΙΔΙΚΗ ΓΡΑΜΜΑΤΕΙΑ ΕΤΠΑ & ΤΣ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ ΕΠΑνΕΚ
ΕΠΑνΕΚ 2014-2020
ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΑΝΤΑΓΩΝΙΣΤΙΚΟΤΗΤΑ
ΕΠΙΧΕΙΡΗΜΑΤΙΚΟΤΗΤΑ
ΚΑΙΝΟΤΟΜΙΑ
ΕΣΠΑ 2014-2020
ανάπτυξη - εργασία - αλληλεγγύη
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Λογισμικό Διασύνδεσης Χρήστη-Συστήματος (Backend API)



ΕΙΚΟΝΑ 24: BACKEND API

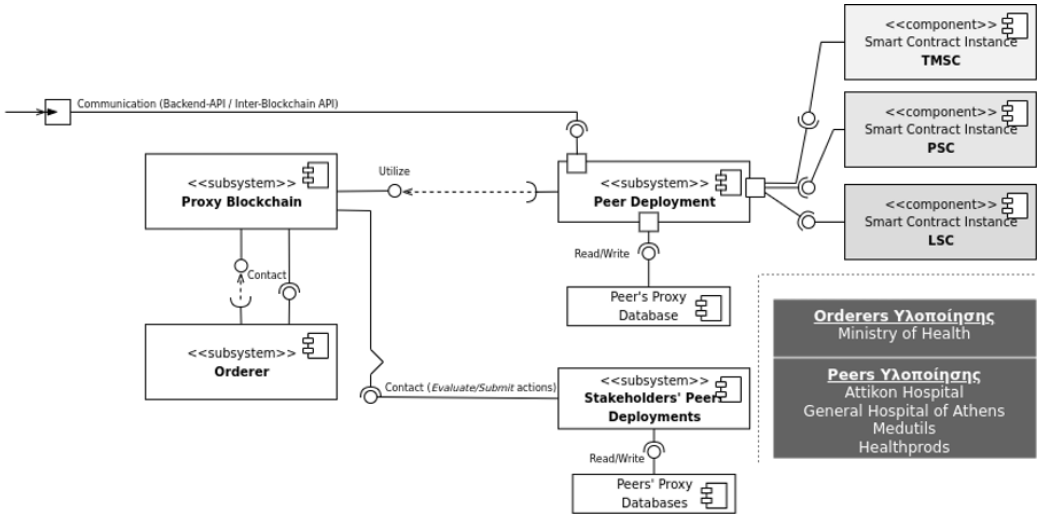
Λογισμικό Διασύνδεσης Blockchain Συστημάτων (Inter-Blockchain API)



ΕΙΚΟΝΑ 25: INTER-BLOCKCHAIN API

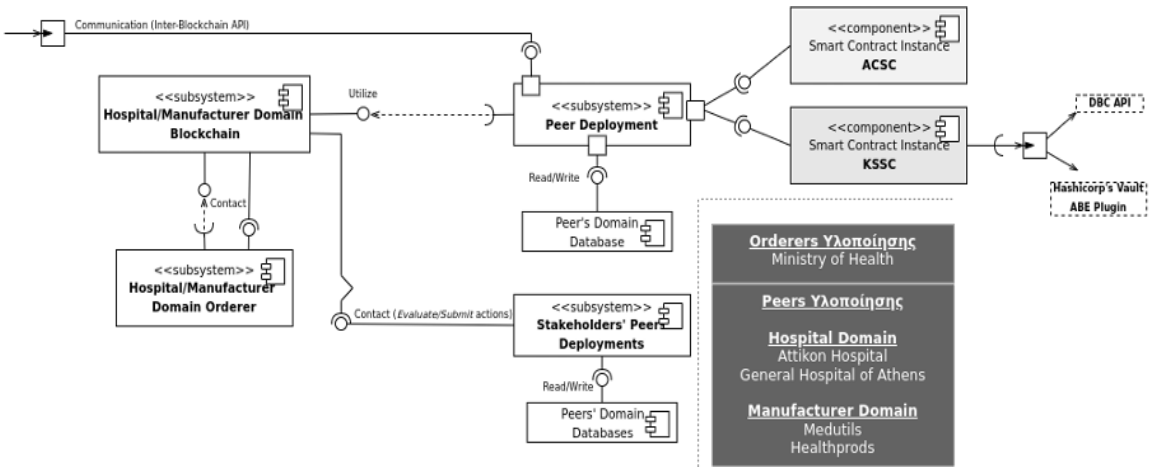
Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο
ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ
ΟΙΚΟΝΟΜΙΑΣ & ΑΝΑΠΤΥΞΗΣ
ΕΙΔΙΚΗ ΓΡΑΜΜΑΤΕΙΑ ΕΤΠΑ & ΤΣ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ ΕΠΑνΕΚ
ΕΠΑνΕΚ 2014-2020
ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΑΝΤΑΓΩΝΙΣΤΙΚΟΤΗΤΑ
ΕΠΙΧΕΙΡΗΜΑΤΙΚΟΤΗΤΑ
ΚΑΙΝΟΤΟΜΙΑ
ΕΣΠΑ 2014-2020
ανάπτυξη - εργασία - αλληλεγγύη
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Proxy Blockchain (PBC)



ΕΙΚΟΝΑ 26: PROXY BLOCKCHAIN

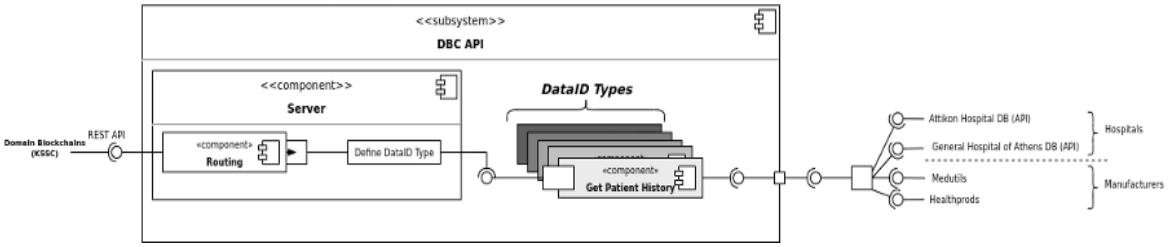
Domain Blockchains (HDBC, MDBC)



ΕΙΚΟΝΑ 27: DOMAIN BLOCKCHAINS

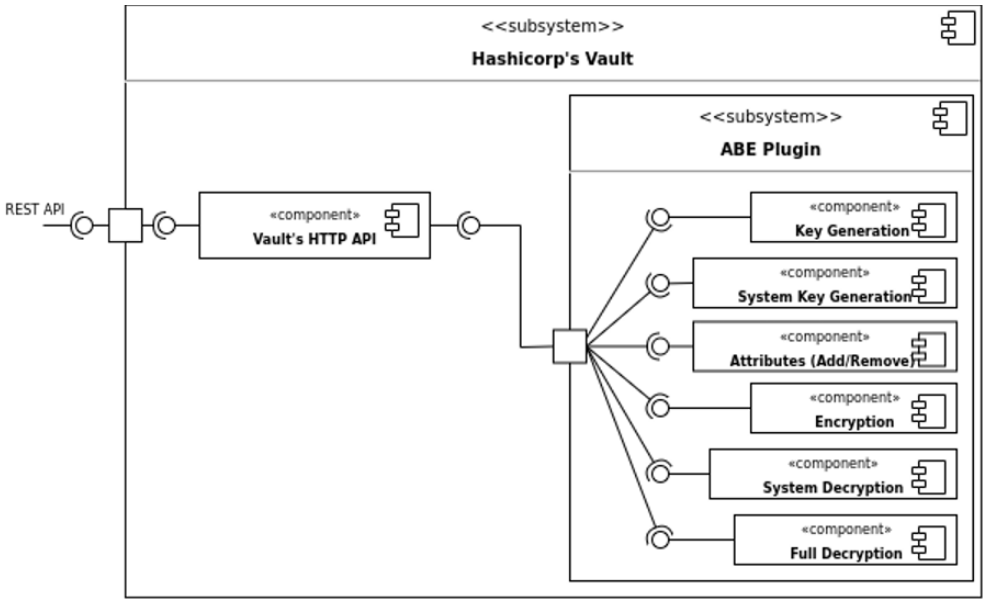
Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο
ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ ΟΙΚΟΝΟΜΙΑΣ & ΑΝΑΠΤΥΞΗΣ
ΕΙΔΙΚΗ ΓΡΑΜΜΑΤΕΙΑ ΕΤΠΑ & ΤΣ
ΕΠΑνΕΚ 2014-2020
ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΑΝΤΑΓΩΝΙΣΤΙΚΟΤΗΤΑ ΕΠΙΧΕΙΡΗΜΑΤΙΚΟΤΗΤΑ ΚΑΙΝΟΤΟΜΙΑ
ΕΣΠΑ 2014-2020
ανάπτυξη - εργασία - αλληλεγγύη
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Λογισμικό Διασύνδεσης Συστήματος – Βάσεων Δεδομένων (DBC API)



ΕΙΚΟΝΑ 28: DATABASE API

Λογισμικό Κρυπτογράφησης – Αποκρυπτογράφησης (Hashicorp's Vault ABE plugin)



ΕΙΚΟΝΑ 29: HASHICORP VAULT ABE PLUGIN

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο
ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ ΟΙΚΟΝΟΜΙΑΣ & ΑΝΑΠΤΥΞΗΣ
ΕΙΔΙΚΗ ΓΡΑΜΜΑΤΕΙΑ ΕΠΠΑ & ΤΣ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ ΕΠΑνΕΚ
ΕΠΑνΕΚ 2014-2020
ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΑΝΤΑΓΩΝΙΣΤΙΚΟΤΗΤΑ ΕΠΙΧΕΙΡΗΜΑΤΙΚΟΤΗΤΑ ΚΑΙΝΟΤΟΜΙΑ
ΕΣΠΑ 2014-2020
ανάπτυξη - εργασία - αλληλεγγύη
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

4.3.Λειτουργικές Απαιτήσεις - Σενάρια χρήσης

Προτού γίνει αποτύπωση των διαφόρων σεναρίων χρήσης που μπορούν να αναπτυχθούν στο σύστημα, θα αναλυθούν οι λειτουργικές απαιτήσεις που υπάρχουν. Στον παρακάτω πίνακα αναπτύσσονται οι Λειτουργικές απαιτήσεις του Συστήματος. Οι απαιτήσεις αυτές θα αναπτυχθούν σαν ολοκληρωμένες λειτουργίες και θα αναφέρονται ως *OpReqXX*. Για κάθε απαίτηση, θα αναφέρεται ο ρόλος του συστήματος (Backend API, Inter-Blockchain API κ.ο.κ.) ή ο Ανθρώπινος Ρόλος (Admin, CA-Admin, Auditor, Client) που θα μπορεί να εκτελέσει τη λειτουργία.

	Απαίτηση	Σχέση	Απαίτηση	Προϋπόθεση
ADMIN	**OpReq00**	Certificate Authority	Να υπάρχει η δυνατότητα δημιουργίας λογαριασμών (CA-Admin, Auditor, Client) για κάθε εμπλεκόμενο	
	OpReq01	Hashicorp's Vautl	Να μπορεί να παρέχει προσωπικά γνωρίσματα (Attributes) στους χρήστες (Clients) του συστήματος και στο Hashicorp Vault ABE Plugin, προκειμένου οι χρήστες να μπορούν να αποκρυπτογραφούν την ήδη κρυπτογραφημένη, από τον κάθε εμπλεκόμενο, πληροφορία	Ο οργανισμός να διαθέτει το αντίστοιχο ABE Key το οποίο συσχετίζεται με το attribute
CA-ADMIN	**OpReq02**	Backend API - Proxy BC	Να είναι δυνατή η ανανέωση των στοιχείων ενός εμπλεκόμενου (Certificate, CRL, ACL)	Ο οργανισμός να μην έχει ανακληθεί Τα Certificate, CRL να είναι μεταγενέστερα των υπαρχόντων
	OpReq03	Backend API - Proxy BC	Να μπορεί να λαμβάνει μέρος σε ψηφοφορίες (για την εισαγωγή/αφαίρεση εμπλεκόμενου, για την έγκριση άδειας σε έναν Ελεγκτή ώστε να λάβει είσοδο (access) στις καταγραφές (Logs) του συστήματος)	Ο οργανισμός να μην έχει ανακληθεί
	OpReq04	Backend API - Proxy BC	Να μπορεί να δημιουργεί ψηφοφορίες για την εισαγωγή ενός νέου εμπλεκόμενου, στο σύστημα	Ο οργανισμός να μην έχει ανακληθεί
	OpReq05	Backend API - Proxy BC	Να μπορεί να δημιουργεί ψηφοφορίες για την αφαίρεση ενός εμπλεκόμενου από το σύστημα	Ο οργανισμός να μην έχει ανακληθεί

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο
ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ ΟΙΚΟΝΟΜΙΑΣ & ΑΝΑΠΤΥΞΗΣ
ΕΙΔΙΚΗ ΓΡΑΜΜΑΤΕΙΑ ΕΤΠΑ & ΤΣ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ ΕΠΑνΕΚ
ΕΠΑνΕΚ 2014-2020
ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΑΝΤΑΓΩΝΙΣΤΙΚΟΤΗΤΑ ΕΠΙΧΕΙΡΗΜΑΤΙΚΟΤΗΤΑ ΚΑΙΝΟΤΟΜΙΑ
ΕΣΠΑ 2014-2020
ανάπτυξη - εργασία - αλληλεγγύη
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

AUDITOR	**OpReq06**	Backend API - Proxy BC	Να μπορεί να λάβει πρόσβαση καθώς και να ελέγξει τις αιτήσεις του για είσοδο στις καταγραφές (Logs) του συστήματος	Ο οργανισμός να μην έχει ανακληθεί
	OpReq07	Backend API - Proxy BC	Να μπορεί να βλέπει τις καταγραφές με την πρόσβαση που του έχει δοθεί από μία αίτηση για Έλεγχο (Audit)	Ο οργανισμός να μην έχει ανακληθεί Η πρόσβαση να μην έχει ανακληθεί
	OpReq08	Backend API - Proxy BC	Να μπορεί να ζητάει πρόσβαση, είτε συνολικά στο σύστημα (Proxy BC), από όλα τα εμπλεκόμενα μέρη, είτε ανά επιχειρηματικό τομέα (Domain BC), στις καταγραφές (Logs) του συστήματος	Ο οργανισμός να μην έχει ανακληθεί
CLIENT	**OpReq09**	Backend API - Inter-Blockchain API - Proxy BC	Να μπορεί να δημιουργεί μία αίτηση (Request) για τη λήψη πληροφοριών από τη Βάση Δεδομένων ενός ή περισσότερων εμπλεκόμενων που ανήκουν στον ίδιο ή διαφορετικό επιχειρηματικό τομέα με αυτόν	Ο οργανισμός, ή ο χρήστης να μην έχει ανακληθεί
	OpReq10	Hashicorp's Vault	Να μπορεί να αποκρυπτογραφεί (decrypt) τα δεδομένα που ελήφθησαν από τη βάση δεδομένων (ή τις βάσεις δεδομένων) των εμπλεκόμενων και τα οποία αντιστοιχούν στην αίτησή του	Ο χρήστης να διαθέτει τα απαραίτητα ABE attributes με τα οποία έχει κρυπτογραφηθεί η πληροφορία
	OpReq11	Backend API - Proxy BC	Να μπορεί να διαχειρίζεται τις αιτήσεις του (Requests), καθώς και να μπορεί να ελέγξει την πορεία ολοκλήρωσης τους (Ολοκληρωμένες, Επιτυχημένες)	Ο οργανισμός, ή ο χρήστης να μην έχει ανακληθεί
	OpReq12	Certificate Authority	Να έχει τη δυνατότητα, σε περίπτωση που αυτό απαιτείται από μία αίτηση, να συνδυάζει Ρόλους που έχει λάβει μέσω ταυτοποίησης στους διάφορους εμπλεκόμενους φορείς	Ο οργανισμός, ή ο χρήστης να μην έχει ανακληθεί Το GID να είναι κοινό για όλες τις οντότητες του χρήστη

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο
ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ ΟΙΚΟΝΟΜΙΑΣ & ΑΝΑΠΤΥΞΗΣ
ΕΙΔΙΚΗ ΓΡΑΜΜΑΤΕΙΑ ΕΤΠΑ & ΤΣ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ ΕΠΑνΕΚ
ΕΠΑνΕΚ 2014-2020
ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΑΝΤΑΓΩΝΙΣΤΙΚΟΤΗΤΑ ΕΠΙΧΕΙΡΗΜΑΤΙΚΟΤΗΤΑ ΚΑΙΝΟΤΟΜΙΑ
ΕΣΠΑ 2014-2020
ανάπτυξη - εργασία - αλληλεγγύη
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

	OpReq13	Backend API - Proxy BC	Να μπορεί να έχει επισκόπηση επί των ενεργών του ρόλων	Ο οργανισμός, ή ο χρήστης να μην έχει ανακληθεί
INTER-BLOCKCHAIN API	**OpReq14**	Proxy BC	Να ελέγχει σε τακτά χρονικά διαστήματα, ή έπειτα από τη λήψη ενός συμβάντος (event) από το Blockchain, την πορεία των ψηφοφοριών	
	OpReq15	Proxy BC	Να ενημερώνει το Blockchain για τη λήξη μίας ψηφοφορίας	
	OpReq16	Proxy BC	Να εισάγει αυτόματα νέες ψηφοφορίες στη λίστα με τις ψηφοφορίες που πρέπει να ελέγχει	
	OpReq17	Proxy BC – Domain BC	Να μεταβιβάζει συμβάντα (events) που έλαβε από το Proxy Blockchain στο κατάλληλο Domain Blockchain και αντίστροφα	Ο οργανισμός να συμμετέχει στο Inter-Blockchain API
BACKEND API	**OpReq18**	Client Application – Proxy BC	Να μεταβιβάζει τις αιτήσεις από τους χρήστες (CA-Admins, Auditors, Clients) του συστήματος, στο Proxy Blockchain και αντίστροφα	
	OpReq19	Client Application	Να δημιουργεί τεκμήριο μέσω του οποίου ένας Client θα μπορεί να χρησιμοποιήσει το Backend-API για τη μεταφορά πληροφορίας προς το Proxy Blockchain	Ο οργανισμός να συμμετέχει στο Backend API
PROXYBLOCKCHA	**OpReq20**	Client Application – Backend API – Inter-Blockchain API	Να δέχεται αιτήματα από χρήστη του συστήματος, μέσω του Backend API, να επικυρώνει τον χρήστη, να συγκεντρώνει τα χαρακτηριστικά και στοιχεία (Ρόλοι και Προσωρινοί ρόλοι) που τον αφορούν και αναφέρονται στις πολιτικές των εμπλεκόμενων, να αποθηκεύει το αίτημα στις εγγραφές του συστήματος και να προωθεί το αίτημα, μαζί με τα χαρακτηριστικά του που συγκεντρώθηκαν από τις πολιτικές, στο Inter-Blockchain API	Ο οργανισμός να συμμετέχει στα Backend / Inter-Blockchain APIs Ο οργανισμός, ή ο χρήστης να μην έχει ανακληθεί

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο
ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ ΟΙΚΟΝΟΜΙΑΣ & ΑΝΑΠΤΥΞΗΣ
ΕΙΔΙΚΗ ΓΡΑΜΜΑΤΕΙΑ ΕΤΠΑ & ΤΣ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ ΕΠΑνΕΚ
ΕΠΑνΕΚ 2014-2020
ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΑΝΤΑΓΩΝΙΣΤΙΚΟΤΗΤΑ ΕΠΙΧΕΙΡΗΜΑΤΙΚΟΤΗΤΑ ΚΑΙΝΟΤΟΜΙΑ
ΕΣΠΑ 2014-2020
ανάπτυξη - εργασία - αλληλεγγύη
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

IN	**OpReq21**	Inter-Blockchain API	Να καταχωρεί στις καταγραφές του συστήματος, τα αιτήματα που έχουν δημιουργηθεί από τους χρήστες. Όταν η διαδικασία του αιτήματος ολοκληρώνεται, να λαμβάνει από το Inter-Blockchain API τις πληροφορίες και δεδομένα που αφορούν το αίτημα και να ενημερώνει τις καταγραφές για την ολοκλήρωσή του.	
	OpReq22		Να λαμβάνει αίτημα για τη δημιουργία ψηφοφορίας, να ελέγχει εάν υπάρχει (ίδια) υφιστάμενη ψηφοφορία που εκτελείται, να δημιουργεί τα ψηφοδέλτια για κάθε εμπλεκόμενο που η ψηφοφορία αφορά	Ο οργανισμός, ή ο χρήστης να μην έχει ανακληθεί
	OpReq23	Client Application – Backend API	Να επιτρέπει την ανανέωση των εξατομικευμένων πολιτικών	Ο οργανισμός, ή ο χρήστης να μην έχει ανακληθεί
DOMAINBLOCKCHAIN	**OpReq24**	Hashicorp's Vault	Να μπορεί να εκτελεί τη μερική αποκρυπτογράφηση των δεδομένων τα οποία ελήφθησαν από την επικοινωνία του Συστήματος με τις βάσεις δεδομένων των εμπλεκόμενων μερών	Ο οργανισμός να μπορεί να κάνει χρήση του *SA* ABE Attribute
	OpReq25	Proxy BC-Inter-Blockchain API – DBC API	Να λαμβάνει αιτήματα (Requests) από το Proxy BC, διαμέσω του Inter-Blockchain API, και να αξιώνει πρόσβαση στη λήψη πληροφοριών και δεδομένων από τα εμπλεκόμενα μέρη, σύμφωνα με τις πολιτικές που έχουν θεσπισθεί από αυτά. Να επιστρέφει τα αποτελέσματα στο Proxy BC, διαμέσω του Inter-Blockchain API	

ΠΙΝΑΚΑΣ 3: ΛΕΙΤΟΥΡΓΙΚΕΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΣΕΝΑΡΙΑ ΧΡΗΣΗΣ

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο
ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ ΟΙΚΟΝΟΜΙΑΣ & ΑΝΑΠΤΥΞΗΣ
ΕΙΔΙΚΗ ΓΡΑΜΜΑΤΕΙΑ ΕΤΠΑ & ΤΣ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ ΕΠΑνΕΚ
ΕΠΑνΕΚ 2014-2020
ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΑΝΤΑΓΩΝΙΣΤΙΚΟΤΗΤΑ ΕΠΙΧΕΙΡΗΜΑΤΙΚΟΤΗΤΑ ΚΑΙΝΟΤΟΜΙΑ
ΕΣΠΑ 2014-2020
ανάπτυξη - εργασία - αλληλεγγύη
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

5. Σύνοψη αποτελεσμάτων του έργου

Με βάση την ολοκλήρωση των αποτελεσμάτων του έργου ΜΕΛΙΤΥ, τη δοκιμή και επικύρωση των μεθοδολογιών ασφάλειας και των εργαλείων λογισμικού που αναπτύχθηκαν σε ένα ρεαλιστικό περιβάλλον δοκιμών το οποίο κατέστη δυνατό μέσω της συμμετοχής των τελικών χρηστών, προκύπτουν τα ακόλουθα συμπεράσματα.

5.1.Κύρια αποτελέσματα του έργου

Τα κύρια αποτελέσματα του έργου συνοψίζονται ως ακολούθως:

5.1.1.Ανάπτυξη μεθοδολογίας και εργαλείου ανάλυσης κυβερνο-φυσικών επιθέσεων για κρίσιμες συσκευές IoMT

Στο πλαίσιο του έργου προτάθηκε μια μεθοδολογία βασισμένη στον κίνδυνο για τον εντοπισμό και την αξιολόγηση διαδρομών/μονοπατιών επίθεσης (attack paths) εναντίον κρίσιμων κυβερνο-φυσικών συστημάτων (cyber-physical systems). Ενώ η πλειονότητα των υπαρχουσών προσεγγίσεων επικεντρώνεται μόνο στη συνδεσιμότητα του συστήματος στον κυβερνοχώρο, η προτεινόμενη μεθοδολογία μοντελοποιεί και τις φυσικές αλληλεπιδράσεις. Επιπλέον, σε σύγκριση με τις υπάρχουσες λύσεις, η εν λόγω προσέγγισή είναι σημαντικά πιο αποτελεσματική, χρησιμοποιώντας μια τοπολογία δέντρου επίθεσης (attack tree). Η μεθοδολογία χρησιμοποιεί ως δομικά στοιχεία γνωστά συστήματα αξιολόγησης αδυναμιών, όπως το Common Vulnerabilities and Exposures (CVE), το Common Vulnerability Scoring System (CVSS), καθώς και μοντελοποίηση απειλών. Επιπλέον, μειώνει σημαντικά τα ψευδώς θετικά αποτελέσματα χρησιμοποιώντας μετρικές κινδύνου, ώστε να μπορεί ο υπεύθυνος λήψης αποφάσεων να εντοπίσει συγκεκριμένα μέτρα ασφάλειας, τα οποία αντιμετωπίζουν ταυτόχρονα περισσότερες διαδρομές επίθεσης. Για την επικύρωση της μεθοδολογίας, η ερευνητική ομάδα ανέπτυξε μια εφαρμογή την οποία εφάρμοσε σε ένα ρεαλιστικό σενάριο από τον τομέα της υγείας. Τα αποτελέσματά δείχνουν ότι η προτεινόμενη μεθοδολογία μπορεί να προσδιορίσει και να αξιολογήσει αποτελεσματικά κρυφές ή/και υποτιμημένες διαδρομές κυβερνο-φυσικών επιθέσεων. Στο πλαίσιο του έργου αναπτύχθηκε το εργαλείο ανάλυσης επικινδυνότητας Attack Path Risk Finder (APRF) για την επικύρωση (proof-of-concept) της μεθοδολογίας. Το εργαλείο δοκιμάστηκε σε ρεαλιστικά σενάρια εφαρμογής, τα οποία περιλαμβάνουν ιατρικές συσκευές IoMT τόσο σε περιβάλλον νοσοκομείου όσο και εκτός. Επιπλέον χρησιμοποιήθηκαν αδυναμίες (CVEs) πραγματικών συστημάτων.

5.1.2.Ανάπτυξη κατανεμημένης υποδομής (Hierarchical Multi Blockchain) για τον έλεγχο πρόσβασης σε δεδομένα παραγόμενα στο ιατρικό οικοσύστημα

Στο πλαίσιο του έργου αναπτύχθηκε μια υποδομή βασισμένη στην τεχνολογία κατανεμημένου καθολικού (blockchain) η οποία δίνει την δυνατότητα σε πολύπλοκα πληροφοριακά συστήματα με πολλούς συμμετέχοντες, να ανταλλάσσουν ευαίσθητες πληροφορίες μέσα από ένα δυναμικό και ευέλικτο μηχανισμό ελέγχου πρόσβασης, σύμφωνα με πολιτικές πρόσβασης που ορίζουν οι οργανισμοί. Συγκριτικά με άλλες λύσεις που έχουν προταθεί στην βιβλιογραφία, η συγκεκριμένη υποδομή προσφέρει στους εμπλεκόμενους: α) διαφάνεια, εμπιστευτικότητα και αυθεντικότητα για τα δεδομένα και τις κρίσιμες ενέργειες που εκτελούνται στο σύστημα, β) αυτοματισμό των λειτουργιών, γ) δυναμική διαχείριση των κρυπτογραφικών στοιχείων που επιτρέπουν την ασφαλή και διαβαθμισμένη πρόσβαση σε μεμονωμένους χρήστες ή σε δυναμικές ομάδες. Η υποδομή αναπτύχθηκε στην πλατφόρμα κατανεμημένου καθολικού Hyperledger Fabric ενώ για την υλοποίηση του κρυπτογραφικού μέρους αναπτύχθηκε νέα βιβλιοθήκη για το λογισμικό Hashicorp Vault που ενσωματώνει το κρυπτογραφικό σχήμα MA-CP-ABE με αποκρυπτογράφηση δύο βημάτων. Η ερευνητική ομάδα αξιολόγησε την απόδοση του προτεινόμενου συστήματος εφαρμόζοντας την σε δύο ρεαλιστικά σενάρια από τον τομέα της υγείας χρησιμοποιώντας υπολογιστικά συστήματα διαφορετικών επεξεργαστικών δυνατοτήτων. Τα ευρήματα έδειξαν ότι η προτεινόμενη υποδομή μπορεί να αποτελέσει μια αποδοτική λύση για το οικοσύστημα της υγείας παίρνοντας υπόψη ότι η ταχύτητα απόκρισης του συστήματος εξαρτάται σε σημαντικό βαθμό από τους διατιθέμενους πόρους.

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο
ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ ΟΙΚΟΝΟΜΙΑΣ & ΑΝΑΠΤΥΞΗΣ
ΕΙΔΙΚΗ ΓΡΑΜΜΑΤΕΙΑ ΕΤΠΑ & ΤΣ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ ΕΠΑνΕΚ
ΕΠΑνΕΚ 2014-2020
ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΑΝΤΑΓΩΝΙΣΤΙΚΟΤΗΤΑ ΕΠΙΧΕΙΡΗΜΑΤΙΚΟΤΗΤΑ ΚΑΙΝΟΤΟΜΙΑ
ΕΣΠΑ 2014-2020
ανάπτυξη - εργασία - αλληλεγγύη
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

5.1.3.Ανάπτυξη πλαισίου σχεδίασης προσανατολισμένο στην ασφάλεια υλικού συσκευών IoMT

Στόχος αυτού του πλαισίου σχεδίασης είναι η εκτενής αξιολόγηση της ασφάλειας υλικού από τα πρώτα στάδια μέχρι την τελική ανάπτυξη μίας συσκευής IoMT. Η αξιοποίηση αυτής της προσέγγισης μπορεί να μειώσει το επιπλέον κόστος για έναν ασφαλή σχεδιασμό καθώς αναγνωρίζει και αναδεικνύει όλους τους τομείς ασφαλείας που χρειάζονται να ληφθούν υπόψη για να αντιμετωπιστούν επιθέσεις που έχουν ως αφετηρία τους το υλικό μια συσκευής. Μέσω του πλαισίου αυτού πραγματοποιείται η κατηγοριοποίηση μιας συσκευής σε επιμέρους στοιχεία υλικού που περιλαμβάνουν: τον πυρήνα (μικροελεγκτή), το επίπεδο επικοινωνίας, τους ενεργοποιητές και τους αισθητήρες. Επιπροσθέτως, ενσωματώσαμε στο προτεινόμενο πλαίσιο ένα υπαρκτό μοντέλο αντλίας έγχυσης ινσουλίνης μέσω του MATLAB. Με αυτό τον τρόπο έχουμε την πλήρη προσομοίωση μιας συσκευής IoMT. Για να αναδείξουμε την χρησιμότητα του προτεινόμενου πλαισίου πραγματοποιήσαμε μια επίθεση ανάλυσης πλευρικού καναλιού (ΑΠΚ) σε ένα κρυπτογραφικό αλγόριθμο ο οποίος είναι ενσωματωμένος στο σύστημα το οποίο προσομοιώσαμε. Σκοπός της επίθεσης αυτής είναι να εντοπίσουμε ποια από τα στοιχεία υλικού επηρεάζονται άμεσα ή έμμεσα. Με αυτό τον τρόπο μπορεί να αξιολογηθεί η ασφάλεια της συσκευής σε πρώιμα στάδια σχεδίασης και να ληφθούν υπόψη οι αδυναμίες που παρουσιάζονται με σκοπό να δοθεί η δυνατότητα αντιμετώπισής τους και σε επίπεδο υλικού.

Για να μπορέσουμε να αποκτήσουμε μια πιο συνολική εικόνα της ασφάλειας υλικού της συσκευής IoMT που προσομοιώσαμε, είναι αναγκαίο να μελετηθούν επιπλέον σχετικά αντίμετρα ενάντιας σε επιθέσεις υλικού. Στα πλαίσια της προσπάθειας αυτής αναπτύχθηκε μια πλατφόρμα αξιολόγησης που μπορεί να πραγματοποιήσει εισαγωγή σφαλμάτων κατά των σύγχρονων μονάδων μικροελεγκτών και ταυτόχρονα να καταγράφει πειραματικές ηλεκτρομαγνητικές εκπομπές και ίχνη ισχύος. Η δυνατότητα αυτή αξιοποιείται από μεθοδολογίες επιθέσεων ΑΠΚ. Για τις ανάγκες του έργου αξιολογήθηκαν δυο διαφορετικού τύπου αντίμετρα ασφάλειας υλικού σε δύο διαφορετικούς αλγόριθμους κρυπτογράφησης. Η εκτεταμένη πειραματική αξιολόγηση μέσω της πλατφόρμας αξιολόγησης οδήγησε σε ένα κοινό συμπέρασμα για το σύνολο των περιπτώσεων που εξετάσαμε. Η εισαγωγή σφαλμάτων βελτιώνει την αποτελεσματικότητα των επιθέσεων πλευρικού καναλιού και μειώνουν σημαντικά τον χρόνο που απαιτείται για την ανάκτηση του μυστικού κλειδιού των κρυπτογραφικών αλγόριθμων.

Ακολουθώντας την ροή των τεχνολογικών εξελίξεων οι επιθέσεις πλευρικού καναλιού ισχυροποιήθηκαν με τη χρήση Μηχανικής Μάθησης. Το γεγονός αυτό δημιούργησε την ανάγκη να μελετηθούν επιθέσεις μηχανικής μάθησης καθώς και προτεινόμενα αντίμετρα. Οι επιθέσεις αυτές απλοποιήθηκαν ακόμα περισσότερο με την χρήση προ εκπαιδευμένων δικτύων γεγονός το οποίο διευκολύνει έναν επιτιθέμενο να πραγματοποιήσει μια επιτυχημένη επίθεση χωρίς να απαιτείται να έχει γνώση μεθόδων Μηχανικής Μάθησης. Στο πλαίσιο του έργου, αξιολογήσαμε δυο διαφορετικά αντίμετρα τα οποία στοχεύουν να μπερδέψουν ένα δίκτυο μηχανικής μάθησης και να το οδηγήσουν σε εσφαλμένη εκτίμηση προστατεύοντας με αυτό τον τρόπο έναν κρυπτογραφικό αλγόριθμο. Τα αποτελέσματα της πειραματικής αξιολόγησης έδειξαν ότι η συνδυαστική χρήση των δύο προτεινόμενων αντιμέτρων είναι ικανή να προστατέψει έως ένα επίπεδο τον κρυπτογραφικό αλγόριθμο.

5.1.4.Κατηγοριοποίηση τεχνολογιών και πρωτοκόλλων που χρησιμοποιούνται για την επικοινωνία σε περιβάλλοντα που περιέχουν κρίσιμες συσκευές IoMT

Στο πλαίσιο του έργου μελετήθηκαν και παρουσιάστηκαν όλες οι διαθέσιμες τεχνολογίες – πρωτόκολλα επικοινωνίας που είτε έχουν χρησιμοποιηθεί, είτε έχουν τη δυνατότητα να χρησιμοποιηθούν σε περιβάλλοντα ιατρικής περίθαλψης. Τα πρωτόκολλα και οι τεχνολογίες αυτές έχουν φιλτραριστεί με βάση την λειτουργικότητά τους ανάμεσα σε έξυπνες συσκευές ιατροφαρμακευτικής περίθαλψης. Η μελέτη γίνεται με βάση τα χαρακτηριστικά ασφάλειας που έχει κάθε πρωτόκολλο – τεχνολογία κατά τη λειτουργία του. Αρχικά αναφέρονται τα λειτουργικά χαρακτηριστικά του κάθε πρωτοκόλλου όπως, επίπεδο λειτουργίας, κατανάλωση ενέργειας, εύρος σήματος, ισχύς σήματος και βασικά στοιχεία αρχιτεκτονικής. Έπειτα όλες οι λεπτομέρειες που αφορούν τα χαρακτηριστικά ασφάλειας όπως, ευπάθειες και επιθέσεις που μπορούν να υλοποιηθούν και να αξιοποιήσουν τις ευπάθειες , μέτρα για την προστασία από τις επιθέσεις και γενικότερα χαρακτηριστικά ασφαλείας όπως αν και τι είδους κρυπτογράφηση χρησιμοποιείται.

Έπειτα παρουσιάστηκαν τοπολογίες, μεταξύ αυτών και οι τοπολογίες που αφορούσαν την αντλία έγχυσης φαρμάκου και το σύστημα μελέτης ύπνου. Σε αυτές τις τοπολογίες προτάθηκαν τεχνολογίες και πρωτόκολλα από τα παραπάνω που μελετήθηκαν. Σκοπός η επίτευξη όσο το δυνατόν λειτουργικότερης και κυρίως ασφαλέστερης διάδρασης – επικοινωνίας των IoMT συσκευών. Μέσα από

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο
ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ
ΟΙΚΟΝΟΜΙΑΣ & ΑΝΑΠΤΥΞΗΣ
ΕΙΔΙΚΗ ΓΡΑΜΜΑΤΕΙΑ ΕΤΠΑ & ΤΣ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ ΕΠΑνΕΚ
ΕΠΑνΕΚ 2014-2020
ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΑΝΤΑΓΩΝΙΣΤΙΚΟΤΗΤΑ
ΕΠΙΧΕΙΡΗΜΑΤΙΚΟΤΗΤΑ
ΚΑΙΝΟΤΟΜΙΑ
ΕΣΠΑ 2014-2020
ανάπτυξη - εργασία - αλληλεγγύη
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

την παραπάνω διαδικασία τέθηκαν τα δεδομένα και δημιουργήθηκαν ιδέες για την μετέπειτα πειραματική υλοποίηση των δύο βασικών συστημάτων. Πάνω σε αυτές τις υλοποιήσεις δημιουργήθηκαν και εξετάστηκαν τα διάφορα εργαλεία που δημιουργήθηκαν στα πλαίσια αυτού του έργου.

5.2. Σύνοψη ερευνητικών δημοσιεύσεων

Στο πλαίσιο του έργου ΜΕΛΙΤΥ προέκυψε σημαντικός αριθμός ερευνητικών δημοσιεύσεων σε επιστημονικά περιοδικά και συνέδρια, τόσο στο πλαίσιο παραδοτέων του έργου, όσο και γενικότερα στο πλαίσιο της διάχυσης των αποτελεσμάτων. Στον παρακάτω πίνακα παρουσιάζεται συνοπτικά το σύνολο των ερευνητικών δημοσιεύσεων που παρήχθησαν από το έργο ΜΕΛΙΤΥ. Σε περίπτωση που μία ερευνητική δημοσίευση σχετίζεται με κάποιο παραδοτέο του έργου, αναφέρεται το σχετιζόμενο παραδοτέο. Το σύνολο των δημοσιεύσεων αποτελούν μέρος της διάχυσης των ερευνητικών αποτελεσμάτων του έργου.

α.α.	Στοιχεία Δημοσίευσης	Σχετιζόμενο Παραδοτέο
1.	F. Casino, K. R. Choo and C. Patsakis, "HEDGE: Efficient Traffic Classification of Encrypted and Compressed Packets," in *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 11, pp. 2916-2926, Nov. 2019.	
2.	Tsipouras, M.G. Spectral information of EEG signals with respect to epilepsy classification. EURASIP J. Adv. Signal Process. 2019, 10 (2019). https://doi.org/10.1186/s13634-019-0606-8	
3.	Geogre Chatzisophroniou and Panayiotis Kotzanikolaou, “Association Attacks in IEEE 802.11: Exploiting WiFi Usability Features”. In Proc. of the 9th International Workshop on Socio-Technical Aspects in SecuriTy – STAST2019 (*ESORICS 2019 Workshops*), Luxembourg, September 2019.	
4.	Malamas, V., Chantzis, F., Dasaklis, T. K., Stergiopoulos, G., Kotzanikolaou, P., & Douligeris, C. (2021). Risk assessment methodologies for the internet of medical things: A survey and comparative appraisal. *IEEE Access*, *9*, 40049-40075.	Π1.5
5.	K. Nomikos, A. Papadimitriou, G. Stergiopoulos, D. Koutras, M. Psarakis and P. Kotzanikolaou, "On a Security-oriented Design Framework for Medical IoT Devices: The Hardware Security Perspective," 2020 23rd Euromicro Conference on Digital System Design (DSD), 2020, pp. 301-308, doi: 10.1109/DSD51259.2020.00056.	Π2.3
6.	Ioannis Stellios, Panayiotis Kotzanikolaou, Christos Grigoriadis, Assessing IoT enabled cyber-physical attack paths against critical systems. Computers & Security, Volume 107, 2021, 102316, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2021.102316	Π3.3
7.	V. Malamas, T. Dasaklis, P. Kotzanikolaou, M. Burmester and S. Katsikas, "A Forensics-by-Design Management Framework for Medical Devices Based on Blockchain," *2019 IEEE World Congress on Services (SERVICES)*, Milan, Italy, 2019, pp. 35-40.	Π4.1
8.	V. Malamas, P. Kotzanikolaou, T. K. Dasaklis and M. Burmester, "A Hierarchical Multi Blockchain for Fine Grained Access to Medical Data," in IEEE Access, vol. 8, pp. 134393-134412, 2020, doi: 10.1109/ACCESS.2020.3011201.	Π4.1
9.	Papadimitriou, K. Nomikos, M. Psarakis, E. Aerabi and D. Hely, "You can detect but you cannot hide: Fault Assisted Side Channel Analysis on Protected Software-based Block Ciphers," 2020 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT), 2020, pp. 1-6, doi: 10.1109/DFT50435.2020.9250870	Π4.1
10.	K. Nomikos, A. Papadimitriou, M. Psarakis, A. Pikrakis and V. Beroulle, "Evaluation of Hiding-based Countermeasures against Deep Learning Side Channel Attacks with Pre-trained Networks", submitted to IEEE Computer Society Annual Symposium on VLSI 2022.	Π4.1
11.	Koutras, D.; Stergiopoulos, G.; Dasaklis, T.; Kotzanikolaou, P.; Glynos, D.; Douligeris, C. Security in IoMT Communications: A Survey. Sensors 2020, 20, 4828. https://doi.org/10.3390/s20174828	Π4.2

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο
ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ ΟΙΚΟΝΟΜΙΑΣ & ΑΝΑΠΤΥΞΗΣ
ΕΙΔΙΚΗ ΓΡΑΜΜΑΤΕΙΑ ΕΤΠΑ & ΤΣ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ ΕΠΑνΕΚ
ΕΠΑνΕΚ 2014-2020
ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΑΝΤΑΓΩΝΙΣΤΙΚΟΤΗΤΑ ΕΠΙΧΕΙΡΗΜΑΤΙΚΟΤΗΤΑ ΚΑΙΝΟΤΟΜΙΑ
ΕΣΠΑ 2014-2020
ανάπτυξη - εργασία - αλληλεγγύη
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

12.	Anagnostakis, A. G., Giannakeas, N., Tsipouras, M. G., Glavas, E., & Tzallas, A. T. (2021). IoT Micro-Blockchain Fundamentals. *Sensors*, *21*(8), 2784.	Π4.3
13.	F. Fotopoulos, V. Malamas, T. K. Dasaklis, P. Kotzanikolaou and C. Douligeris, "A Blockchain-enabled Architecture for IoMT Device Authentication," 2020 IEEE Eurasia Conference on IOT, Communication and Engineering (ECICE), 2020, pp. 89-92, doi: 10.1109/ECICE50847.2020.9301913.	Π4.4
14.	Vangelis Malamas, George Palaiologos, Panayiotis Kotzanikolaou, Mike Burmester and Dimitris Glynos. Janus: Efficient Multi-Authority & Multi-Domain Attribute Based Access Control in Practice, submitted in the 31st USENIX Security Symposium, August 10–12, 2022, Boston, MA, USA	Π4.5
15.	Chatzisofroniou, George and Kotzanikolaou, Panayiotis. 'Exploiting WiFi Usability Features for Association Attacks in IEEE 802.11: Attack Analysis and Mitigation Controls'. 1 Jan. 2022: 1 – 24. DOI: 10.3233/JCS-210036	
16.	George Stergiopoulos, Panayiotis Kotzanikolaou, Charalambos Konstantinou, and Achilleas Tsoukalis, *"Process-Aware Attacks on Medication Control of Type-I Diabetics using Infusion Pumps"*, submitted at IEEE Systems journal (under review)	

ΠΙΝΑΚΑΣ 4: ΣΥΝΟΨΗ ΕΡΕΥΝΗΤΙΚΩΝ ΔΗΜΟΣΙΕΥΣΕΩΝ ΤΟΥ ΕΡΓΟΥ

5.3.Μελλοντικές επεκτάσεις

Πέραν της δοκιμής καινοτόμων τεχνολογιών ασφάλειας για τεχνολογίες και υπηρεσίες υγείας σε ρεαλιστικό περιβάλλον εφαρμογής, στόχος των φορέων υλοποίησης του έργου είναι η περαιτέρω ωρίμανση των τεχνολογιών που αναπτύχθηκαν σε υψηλότερο επίπεδο τεχνολογικής ετοιμότητας (technology readiness), ώστε να είναι δυνατή η δοκιμαστική εφαρμογή τέτοιων τεχνολογιών ασφάλειας σε πραγματικό περιβάλλον.

Επιπλέον, για κάθε μία από τις τεχνολογίες και μεθοδολογίες που αναπτύχθηκαν, στόχος των φορέων είναι η ερευνητική και αναπτυξιακή εξέλιξή τους. Ειδικότερα:

- **Επέκταση της υλοποίησης του εργαλείου APRF και της σχετικής μεθοδολογίας αποτίμησης επικινδυνότητας.** Στόχος είναι η επέκταση της μεθοδολογίας αποτίμησης επικινδυνότητας ώστε να αυτοματοποιηθεί η συλλογή και επεξεργασία δεδομένων σχετικά με την αποτίμηση των απειλών και των κινδύνων, χρησιμοποιώντας τεχνικές μηχανικής μάθησης. Επιπλέον στόχος είναι η περαιτέρω επέκταση και ορίμανση της υλοποίησης του εργαλείου λογισμικού APRF.
- **Επέκταση της υλοποίησης της κατανεμημένης υποδομής ελέγχου πρόσβασης Hierarchical Multi Blockchain.** Στόχος είναι η επέκταση της υποδομής ώστε να αυτοματοποιεί την διαδικασία μετατροπής πιστοποιητικών χρηστών και συσκευών σε πιστοποιητικά αποδεκτά από το σύστημα, καθώς και η επέκταση του μηχανισμού αυθεντικοποίησης με χρήση σχημάτων ZNP (Zero-Knowledge Proof) και SSI (Self-Sovereign Identity).
- **Ενίσχυση του πλαισίου σχεδίασης ασφαλούς υλικού για συστήματα IoMT.** Στόχος είναι η επέκταση του προτεινόμενου πλαισίου με την ενσωμάτωση σε αυτό επιθέσεων διαφορετικού τύπου, όπως για παράδειγμα επιθέσεων σε επίπεδο λογισμικού, δικτύου και διαδικασίας (process-based), και την εκτέλεση συνδυαστικών επιθέσεων καθώς και την προσθήκη διαφορετικών μοντέλων σφαλμάτων. Επιπλέον, όσον αφορά τις επιθέσεις ΑΠΚ με χρήση Μηχανικής Μάθησης, στόχος είναι η επέκταση της μεθοδολογίας με την ανάπτυξη ισχυρότερων αντιμέτρων, τα οποία θα μεταλλάσσονται δυναμικά ώστε να αντιμετωπίζουν αποτελεσματικά αυτές τις επιθέσεις και να οδηγούν σε ασφαλέστερες συσκευές IoMT.
- **Αυτοματοποίηση ανίχνευσης ευπαθειών σε πρωτόκολλα επικοινωνίας για συστήματα IoMT.** Στόχος είναι η επέκταση των σχετικών αποτελεσμάτων του έργου, όπως είναι το εργαλείο melic, και η δημιουργία εργαλείου αυτοματοποιημένης ανάλυσης αδυναμιών ασφάλειας που σχετίζονται με τα χρησιμοποιούμενα πρωτόκολλα επικοινωνίας σε πραγματικά περιβάλλοντα εφαρμογής.

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο
ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ ΟΙΚΟΝΟΜΙΑΣ & ΑΝΑΠΤΥΞΗΣ
ΕΙΔΙΚΗ ΓΡΑΜΜΑΤΕΙΑ ΕΤΠΑ & ΤΣ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ ΕΠΑνΕΚ
ΕΠΑνΕΚ 2014-2020
ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΑΝΤΑΓΩΝΙΣΤΙΚΟΤΗΤΑ ΕΠΙΧΕΙΡΗΜΑΤΙΚΟΤΗΤΑ ΚΑΙΝΟΤΟΜΙΑ
ΕΣΠΑ 2014-2020
ανάπτυξη - εργασία - αλληλεγγύη
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

6. Οπισθόφυλλο

«Η εργασία υλοποιήθηκε στο πλαίσιο της Δράσης ΕΡΕΥΝΩ – ΔΗΜΙΟΥΡΓΩ - ΚΑΙΝΟΤΟΜΩ και συγχρηματοδοτήθηκε από την Ευρωπαϊκή Ένωση και εθνικούς πόρους μέσω του Ε.Π. Ανταγωνιστικότητα, Επιχειρηματικότητα & Καινοτομία (ΕΠΑνΕΚ) (κωδικός έργου:Τ1ΕΔΚ-01958)»

This research has been co-financed by the European Union and Greek national funds through the Operational Program Competitiveness, Entrepreneurship and Innovation, under the call RESEARCH – CREATE – INNOVATE (project code:T1EDK-01958)

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο
ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ ΟΙΚΟΝΟΜΙΑΣ & ΑΝΑΠΤΥΞΗΣ
ΕΙΔΙΚΗ ΓΡΑΜΜΑΤΕΙΑ ΕΤΠΑ & ΤΣ
ΕΠΑνΕΚ 2014-2020
ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΑΝΤΑΓΩΝΙΣΤΙΚΟΤΗΤΑ ΕΠΙΧΕΙΡΗΜΑΤΙΚΟΤΗΤΑ ΚΑΙΝΟΤΟΜΙΑ
ΕΣΠΑ 2014-2020
ανάπτυξη - εργασία - αλληλεγγύη
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης