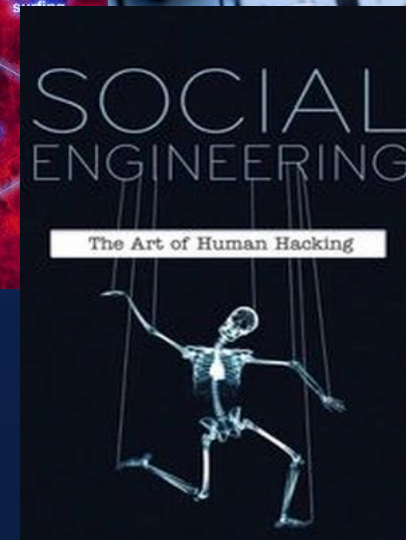




Ιόνιο Πανεπιστήμιο
Τμήμα Πληροφορικής
- Πτυχιακή Εργασία -
Κέρκυρα, 21 Σεπτεμβρίου 2021

- Πτυχιακή Εργασία -

Υλοποίηση και σχεδιασμός Software στην κυβερνοεπίθεση Sim Swap



Λάζαρος Παπανικολάου
ΑΜ Π2017085



Ιόνιο Πανεπιστήμιο
Τμήμα Πληροφορικής
- Πτυχική Εργασία -
Κέρκυρα, 21 Σεπτεμβρίου 2021

Πίνακας Περιεχομένων



01 Ορισμός Κοινωνικής Μηχανικής

02 Στατιστικά επιθέσεων

03 SIM SWAP

04 Ανάπτυξη εφαρμογής

05 Συμπεράσματα



Ιόνιο Πανεπιστήμιο
Τμήμα Πληροφορικής
- Πτυχιακή Εργασία -
Κέρκυρα, 21 Σεπτεμβρίου 2021

Πίνακας Περιεχομένων



Ορισμός Κοινωνικής Μηχανικής

02

Στατιστικά επιθέσεων

03

SIM SWAP

04

Ανάπτυξη εφαρμογής

05

Συμπεράσματα



Ιόνιο Πανεπιστήμιο
Τμήμα Πληροφορικής
- Πτυχιακή Εργασία -
Κέρκυρα, 21 Σεπτεμβρίου 2021

Ορισμός Κοινωνικής Μηχανικής

1. Η κακόβουλη πράξη ως μια ενέργεια χειραγώγησης του χρήστη με στόχο την αποκάλυψη και υποκλοπή των προσωπικών του στοιχείων.

Cambridge, 2021

2. Η θέση και ο ρόλος που πρέπει να έχει ο άνθρωπος στην καθημερινή κοινωνία προσφέροντας τις υπηρεσίες του για ευεργετικούς σκοπούς.

Merriam-Webster, 2021

3.

Η σημασία της πειθούς.

Christopher Hadnagy, 2010



Ιόνιο Πανεπιστήμιο
Τμήμα Πληροφορικής
- Πτυχιακή Εργασία -
Κέρκυρα, 21 Σεπτεμβρίου 2021

Πίνακας Περιεχομένων



01

Ορισμός Κοινωνικής Μηχανικής

Στατιστικά επιθέσεων

03

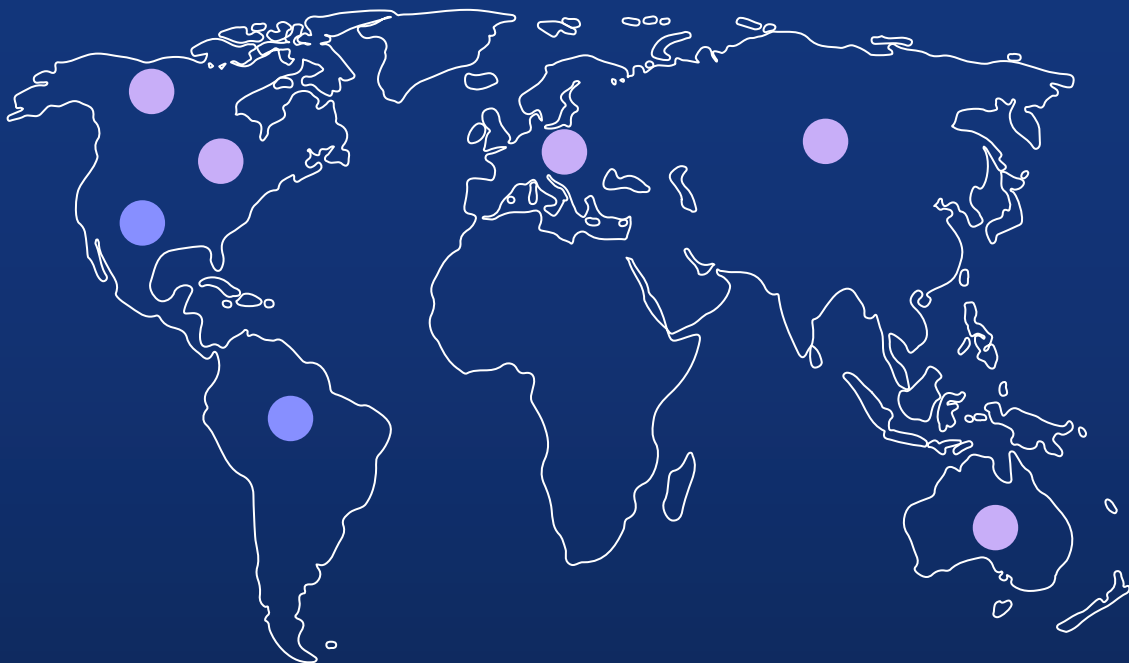
SIM SWAP

04

Ανάπτυξη εφαρμογής

05

Συμπεράσματα



Εμφάνιση συχνότερων επιθέσεων παγκοσμίως, (Federal Bureau of Investigation, 2020).

Έξαρση των επιθέσεων τύπου Phishing

Τύπος εγκλήματος	Θύματα
<u>Phishing/Vishing/Smishing/Pharming</u>	<u>241.342</u>
Non-Payment/Non-Delivery	108.869
Extortion	76.741
Personal Data Breach	45.330
Identity Theft	43.330
Spoofing	28.218
Misrepresentation	24.276
Confidence Fraud/Romance	23.751
Harassment/Threats of Violence	20.604
BEC/EAC	19.369
Credit Card Fraud	17.614
Employment	16.879
Tech Support	15.421
Real Estate/Rental	13.638
Advanced Fee	13.020
Government Impersonation	12.827
Overpayment	10.988

Στατιστικά αριθμητικής υπεροχής σε τύπους ηλεκτρονικού εγκλήματος παγκοσμίως, (Federal Bureau of Investigation, 2020).

4.2 INCREASE IN SIM SWAPPING AND SMISHING

SIM swapping is one of the new key trends in this year's IOCTA. This modus operandi garnered considerable attention over the past twelve months, as law enforcement agencies noticed a significant increase with a growing number of cases in Europe.

SIM swapping is a type of account takeover and refers to the circumvention of SMS-based 2FA to access sensitive user accounts. Criminals fraudulently swap or port the victim's SIM to one in the criminal's possession in order to intercept the one time password (OTP) step of the authentication process. Since this typically requires detailed information on the victim, SIM swapping attacks are highly targeted. This also means that the overall volume of cases differs from Member State to Member State, leading to SIM swapping cases causing significantly higher losses in some jurisdictions while it is barely present in others.

Overall, SIM swapping poses a significant concern and huge potential danger and risk. A successful SIM swapping attack can lead to criminals gaining complete control over a victim's bank, email or social media account, and as a result, enable a number of serious follow-up crimes.



Operation Quinientos Dúsm⁴⁷

In January 2020, investigators from the Spanish National Police together with the Civil Guard and Europol targeted suspects across Spain believed to be part of a hacking ring which stole over €3 million in a series of SIM swapping attacks. Law enforcement arrested 12 individuals in Benidorm (5), Granada (6) and Valladolid (1).

Composed of nationals between the ages of 22 and 52 years old from Italy, Romania, Colombia and Spain, this criminal gang struck over 100 times, stealing between €6 000 and €137 000 from bank accounts of unsuspecting victims per attack.

The modus operandi was simple, yet effective. The criminals managed to obtain the online banking credentials from the victims of the different banks by through the use of banking Trojans or other types of malware. Once they had these credentials, the suspects would apply for a duplicate of the SIM cards of the victims, providing fake documents.

European Union, Agency for Law Enforcement. 2020. "Internet Organized Crime Threat Assessment." *Iocta 1*

IOCTA EUROPALL



Τον Ιανουάριο του 2020, Spanish National Police, Civil Guard και Europol.

Στοχοποίησαν οργανώσεις με απώλεια περίπου 3 εκατομμύρια ευρώ στην Ισπανία.



Ιόνιο Πανεπιστήμιο
Τμήμα Πληροφορικής
- Πτυχιακή Εργασία -
Κέρκυρα, 21 Σεπτεμβρίου 2021

Πίνακας Περιεχομένων



01 Ορισμός Κοινωνικής Μηχανικής

02 Στατιστικά επιθέσεων

SIM SWAP

04 Ανάπτυξη εφαρμογής

05 Συμπεράσματα



SIM SWAP



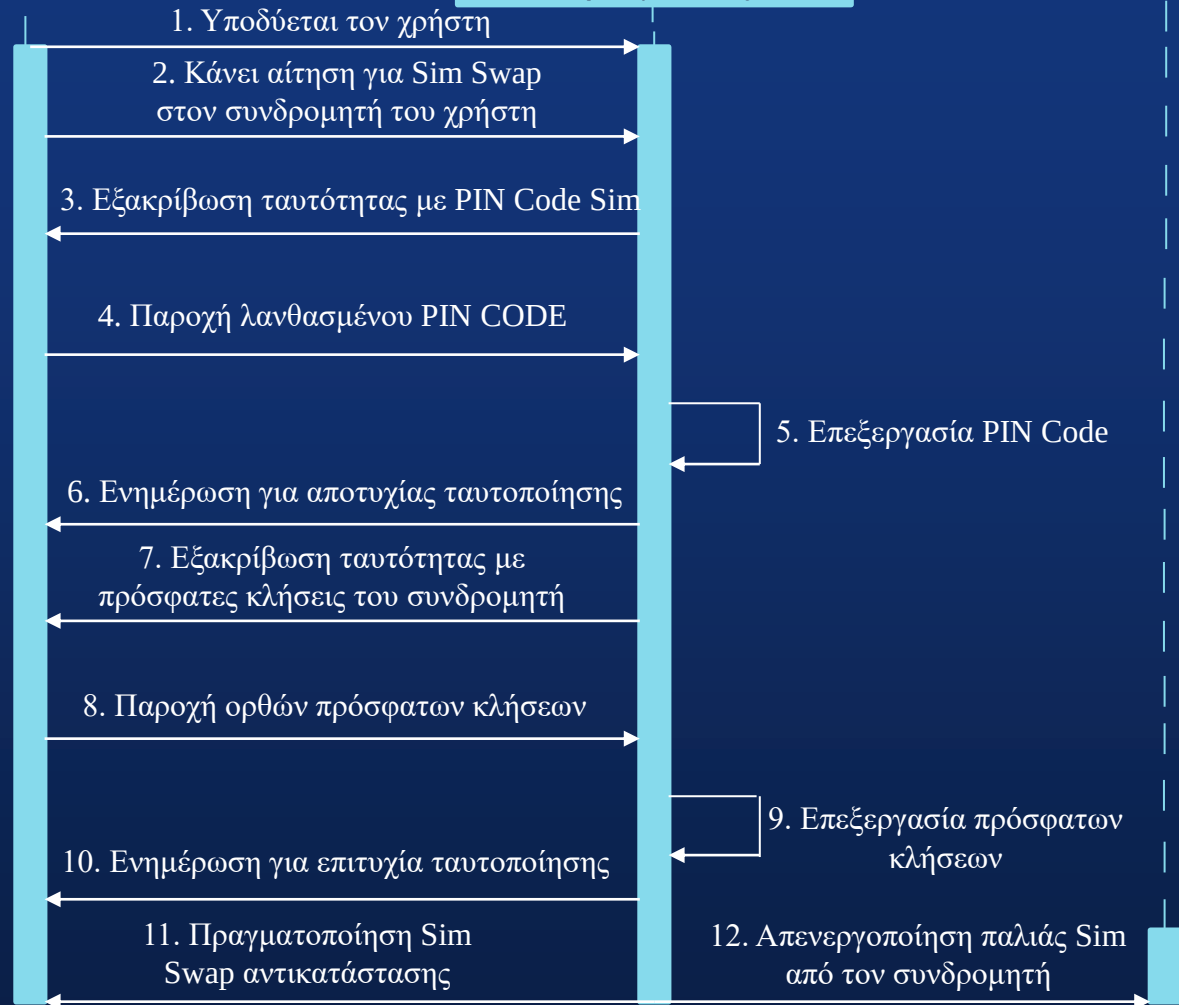
- Αντικατάσταση κάρτας SIM.
- Προσπάθεια εξαγοράς του ηλεκτρονικού λογαριασμού.
- **Port-out scam, SIM splitting, Smishing και SIM jacking**

(Awale & Gupta, 2019b)

Επιτιθέμενος

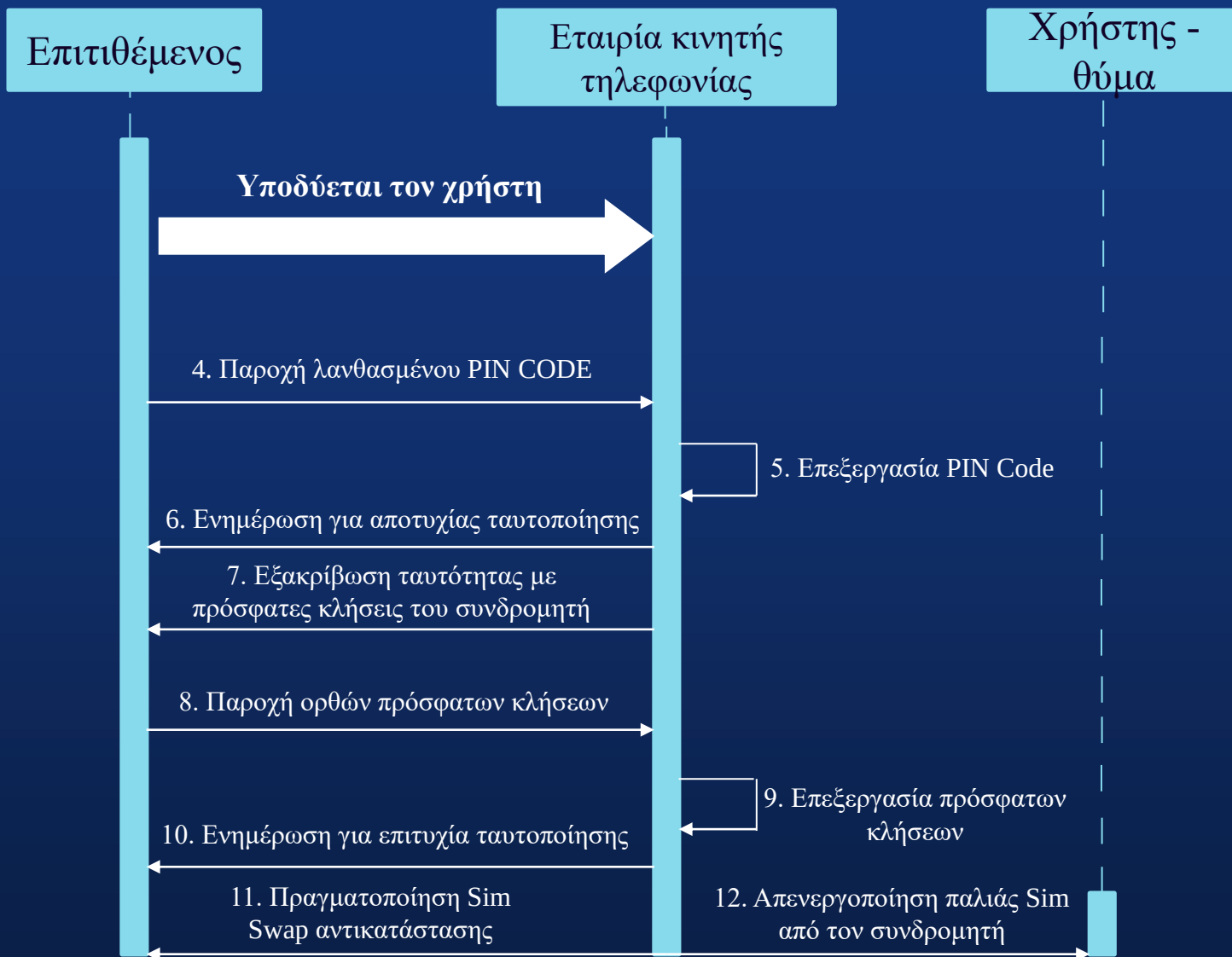
Εταιρία κινητής
τηλεφωνίας

Χρήστης -
θύμα



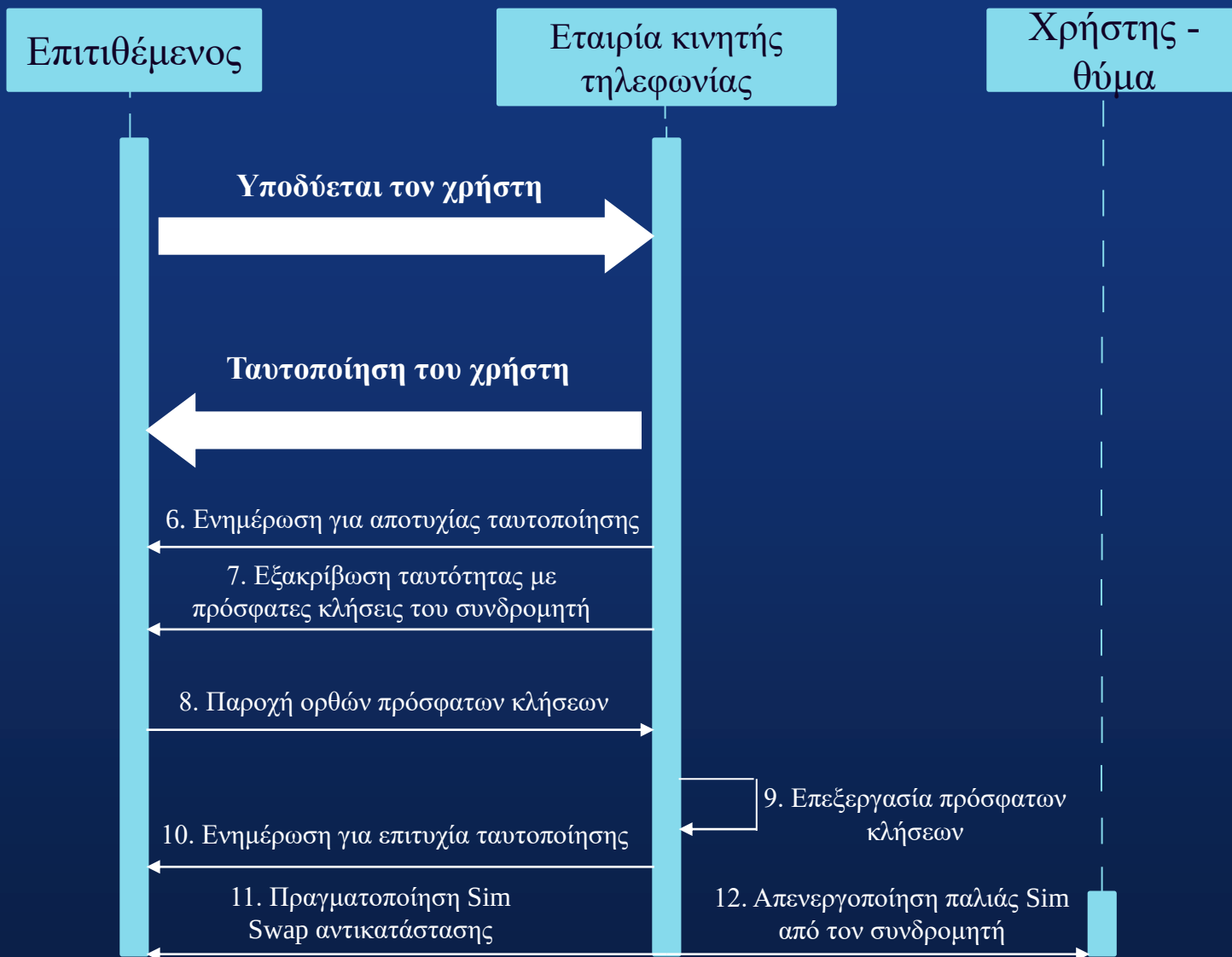
Σχεδιάγραμμα μεθοδολογίας sim swap βάση διαγράμματος ακολουθίας.





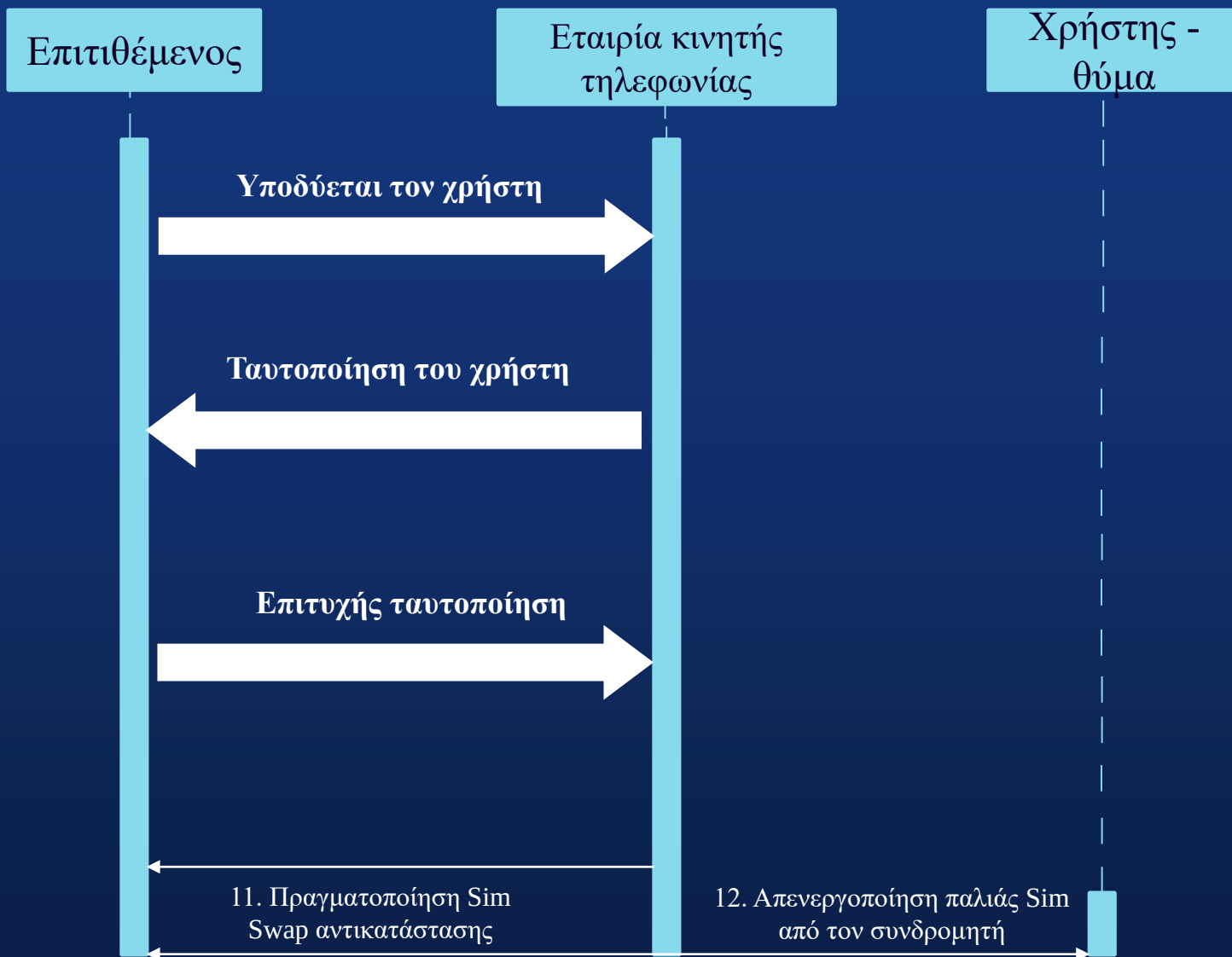
Σχεδιάγραμμα μεθοδολογίας sim swap βάση διαγράμματος ακολουθίας.





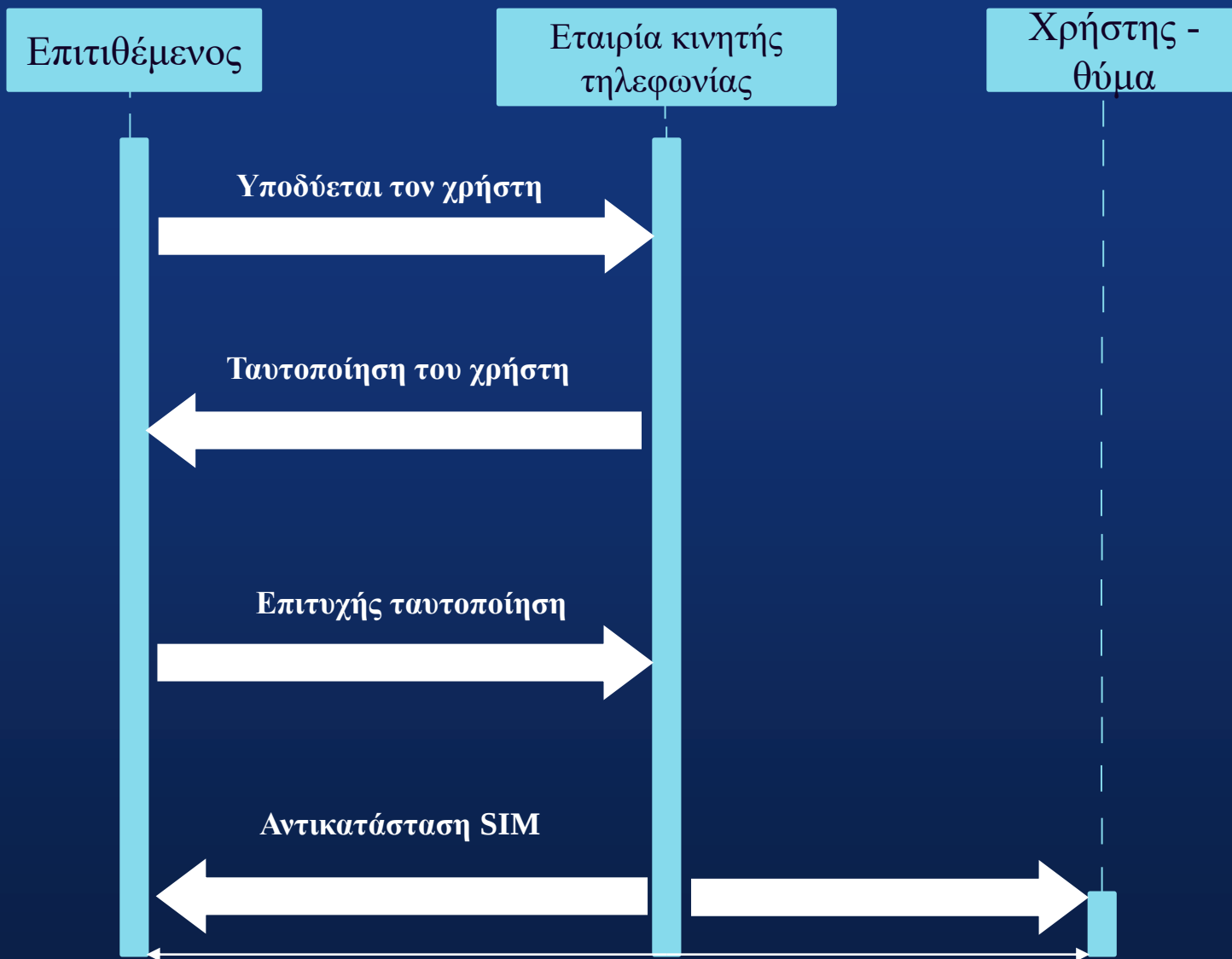
Σχεδιάγραμμα μεθοδολογίας sim swap βάση διαγράμματος ακολουθίας.





Σχεδιάγραμμα μεθοδολογίας sim swar βάση διαγράμματος ακολουθίας.





Σχεδιάγραμμα μεθοδολογίας sim swap βάση διαγράμματος ακολουθίας.



Τελικός στόχος αποτελεί η επιτυχής αντικατάσταση της κάρτας Sim.



Ιόνιο Πανεπιστήμιο
Τμήμα Πληροφορικής
- Πτυχική Εργασία -
Κέρκυρα, 21 Σεπτεμβρίου 2021

Πίνακας Περιεχομένων



01 Ορισμός Κοινωνικής Μηχανικής

02 Στατιστικά επιθέσεων

03 SIM SWAP

Ανάπτυξη εφαρμογής

05 Συμπεράσματα



- ❑ Laravel framework – RESTful API
PUT, GET, POST, DELETE, PATCH

- ❑ MariaDB βάση δεδομένων.

- ❑ PHP γλώσσα προγραμματισμού.

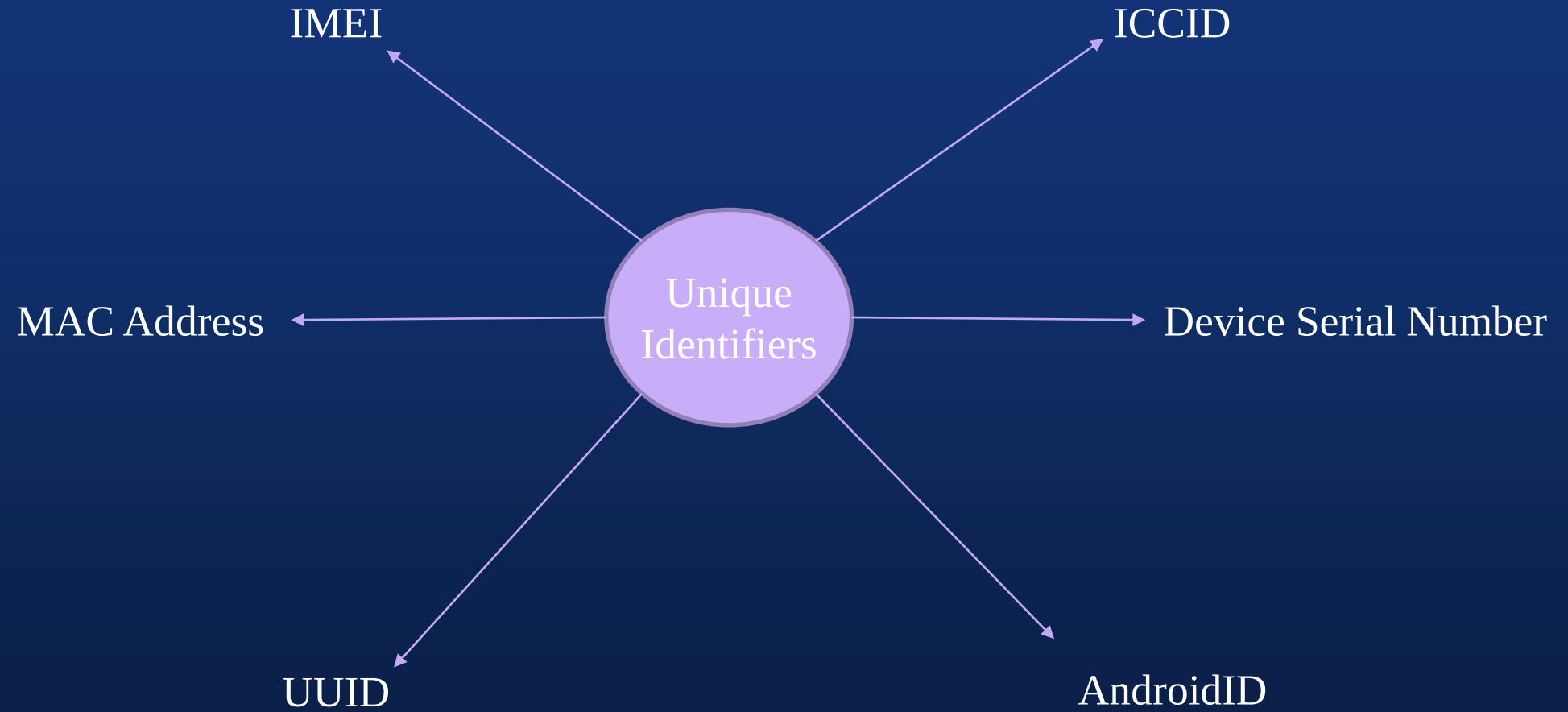


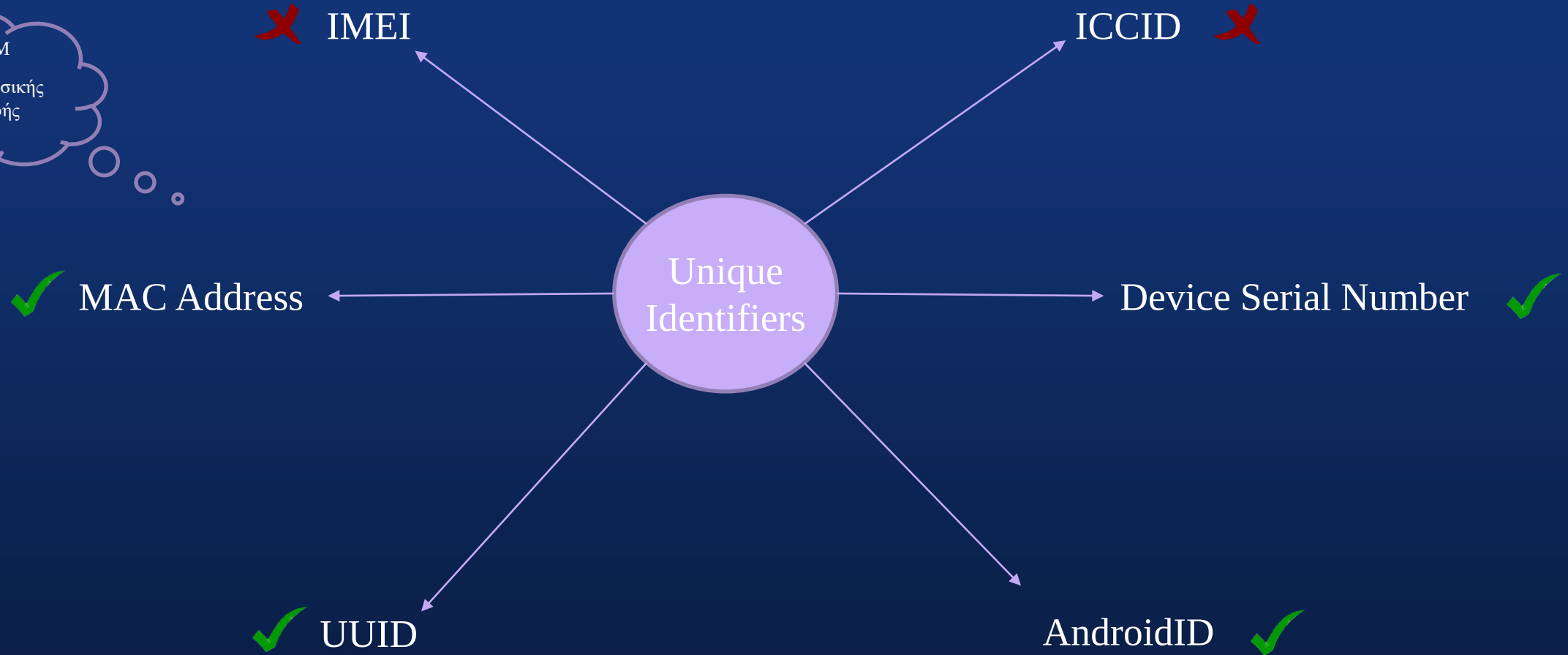
- ❑ Android Studio – User Interface.

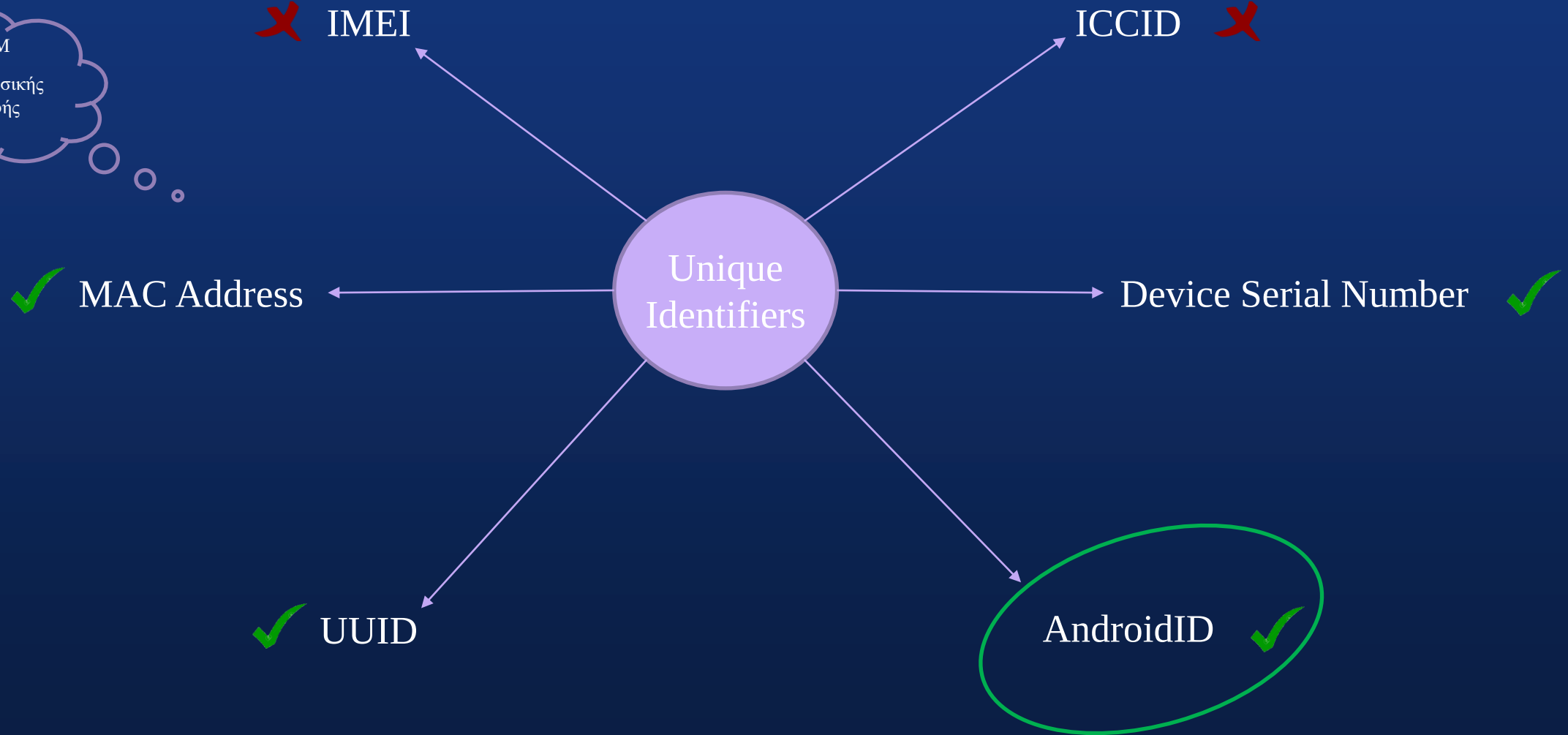
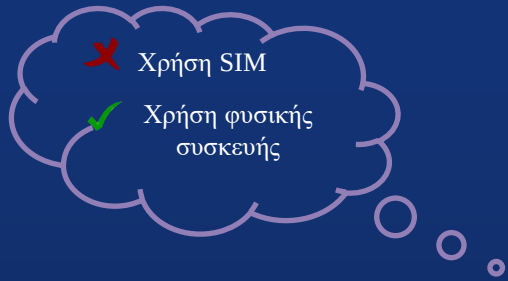
- ❑ JAVA γλώσσα προγραμματισμού.

- ❑ Volley Library.











Ιόνιο Πανεπιστήμιο
Τμήμα Πληροφορικής
- Πτυχιακή Εργασία -
Κέρκυρα, 21 Σεπτεμβρίου 2021



Create Your Profile



Username



Password



PhoneNumber

Device Id

REGISTER

You already have an account?
Login [HERE](#)



Ιόνιο Πανεπιστήμιο
Τμήμα Πληροφορικής
- Πτυχική Εργασία -
Κέρκυρα, 21 Σεπτεμβρίου 2021

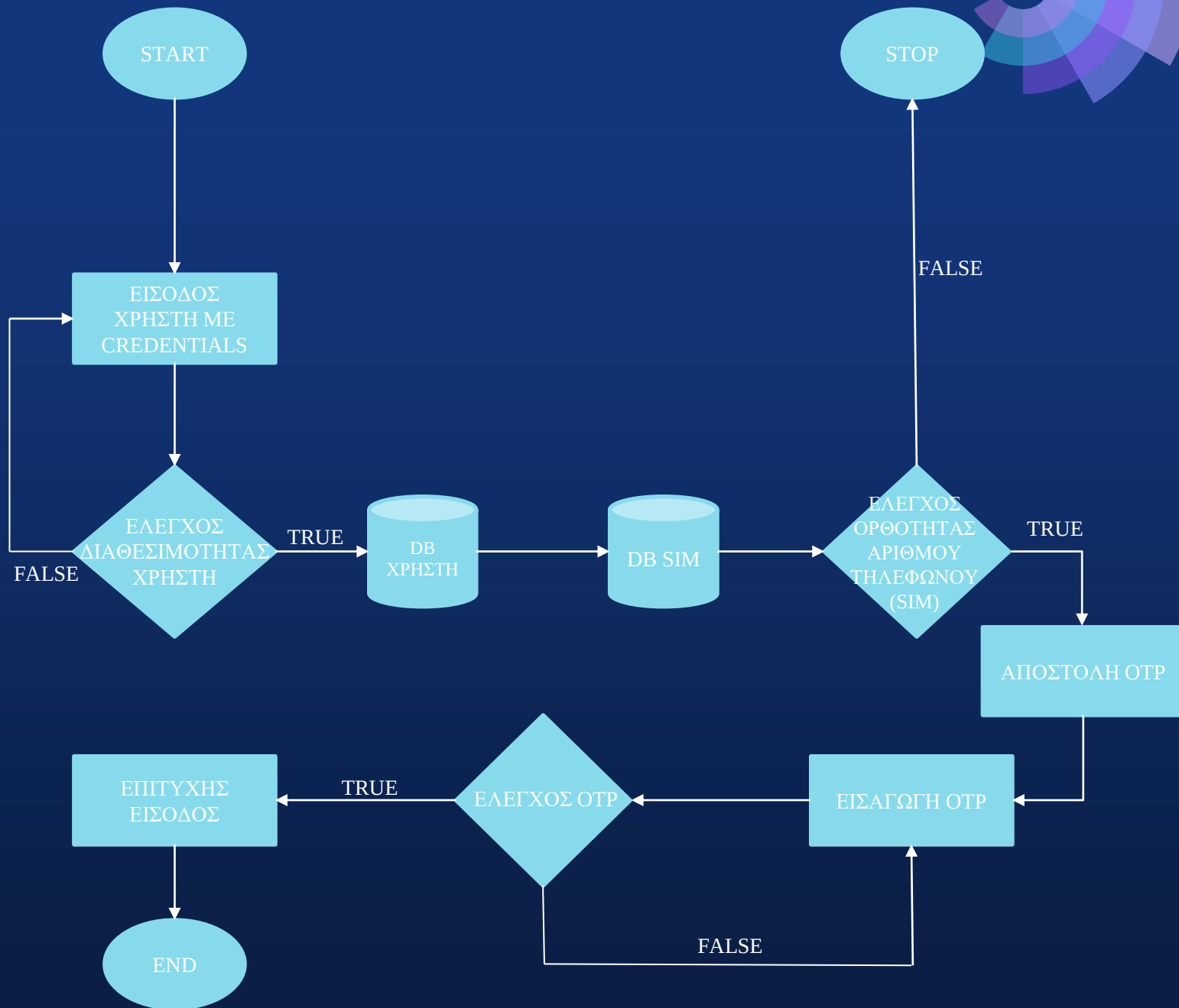
ΠΑΡΟΥΣΙΑΣΗ ΕΦΑΡΜΟΓΗΣ



Ιόνιο Πανεπιστήμιο
Τμήμα Πληροφορικής
- Πτυχική Εργασία -
Κέρκυρα, 21 Σεπτεμβρίου 2021



Η διαδικασία λαμβάνει χώρα για τον επιτιθέμενο.



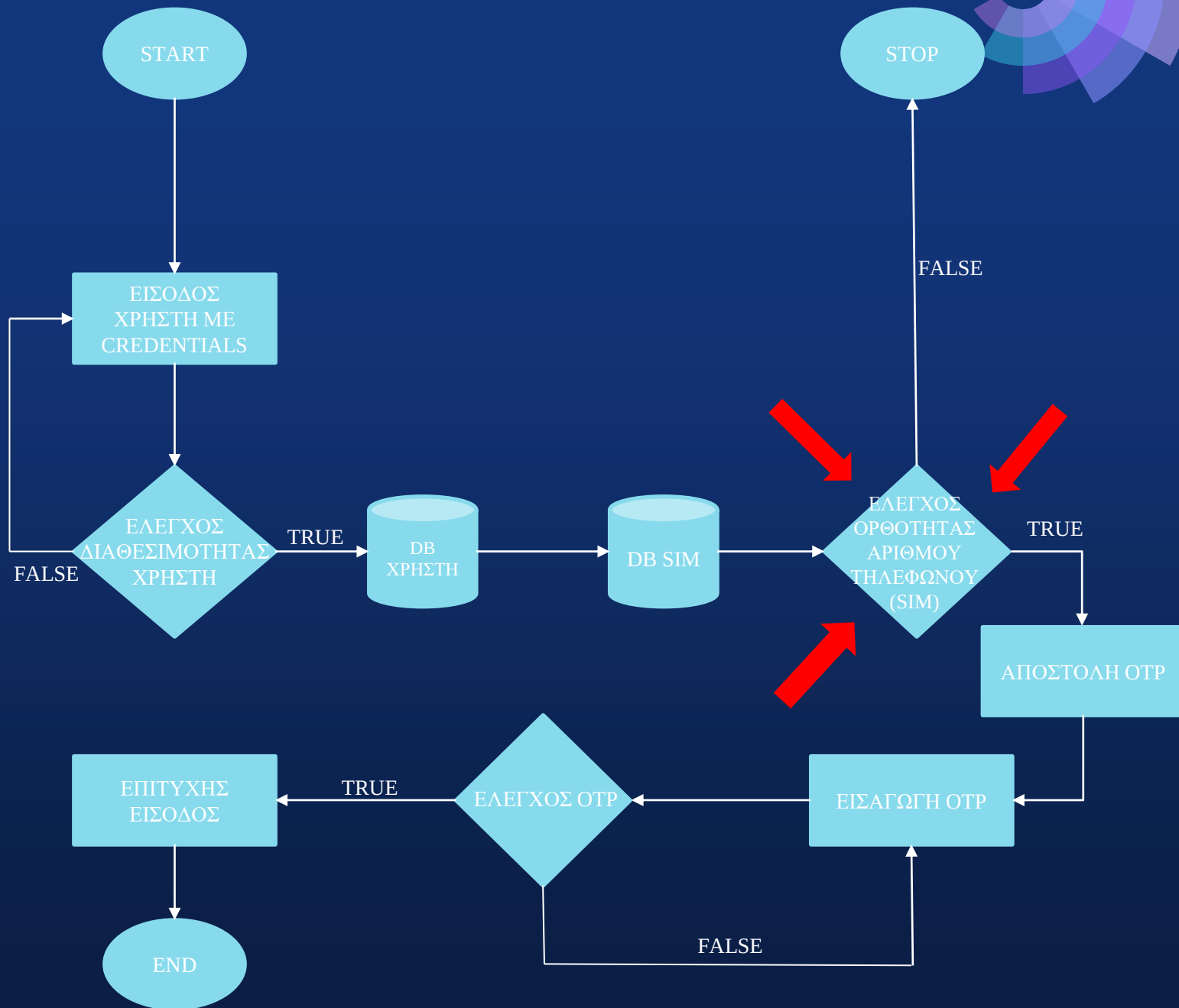
Διάγραμμα τεχνικής διαδικασίας εξέλιξης της ασφάλειας εφαρμογής που βασίζεται στην εγκυρότητα της κάρτας sim.



Ιόνιο Πανεπιστήμιο
Τμήμα Πληροφορικής
- Πτυχική Εργασία -
Κέρκυρα, 21 Σεπτεμβρίου 2021



Η διαδικασία λαμβάνει χώρα για τον επιτιθέμενο.



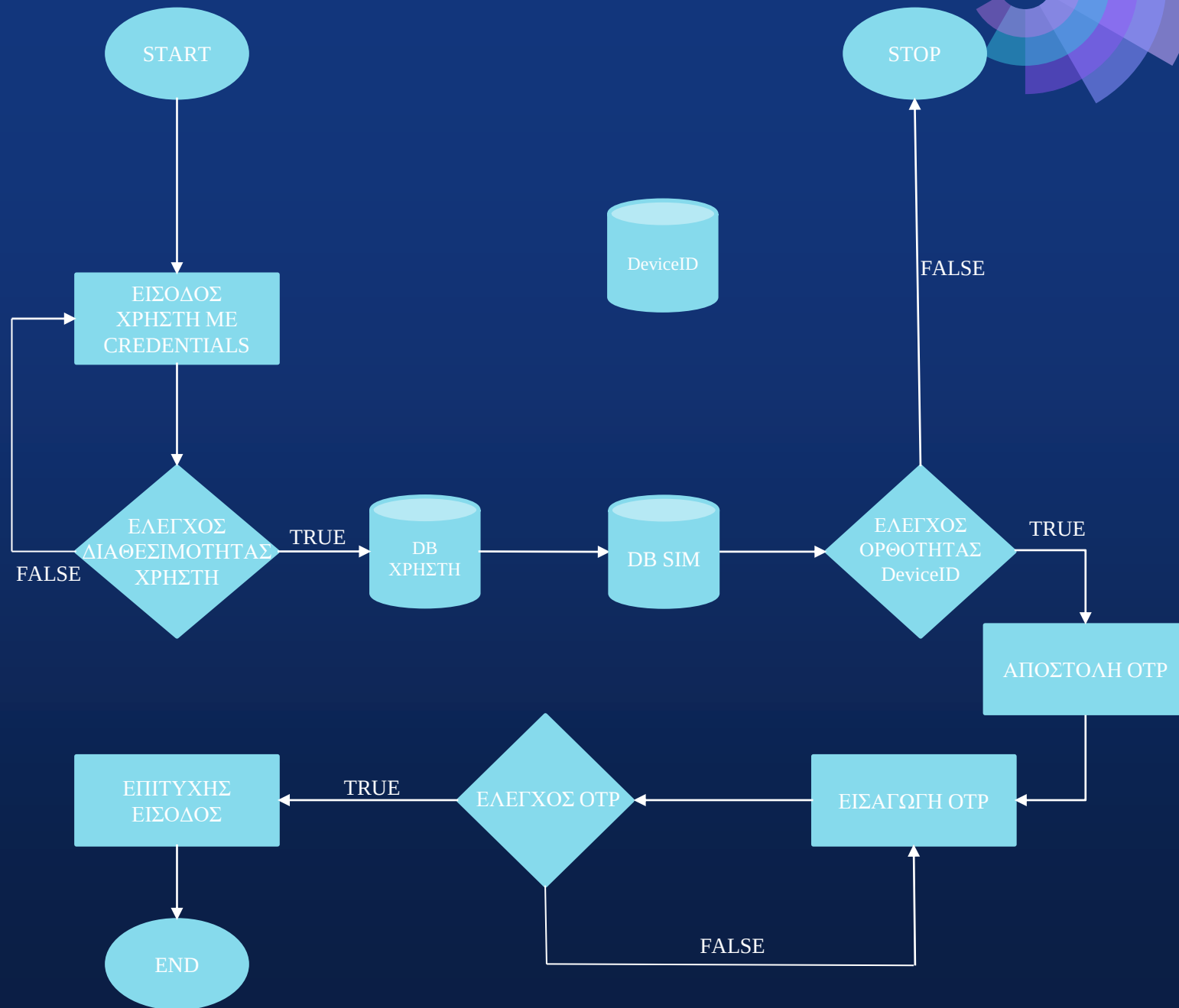
Διάγραμμα τεχνικής διαδικασίας εξέλιξης της ασφάλειας εφαρμογής που βασίζεται στην εγκυρότητα της κάρτας sim.



Ιόνιο Πανεπιστήμιο
Τμήμα Πληροφορικής
- Πτυχιακή Εργασία -
Κέρκυρα, 21 Σεπτεμβρίου 2021



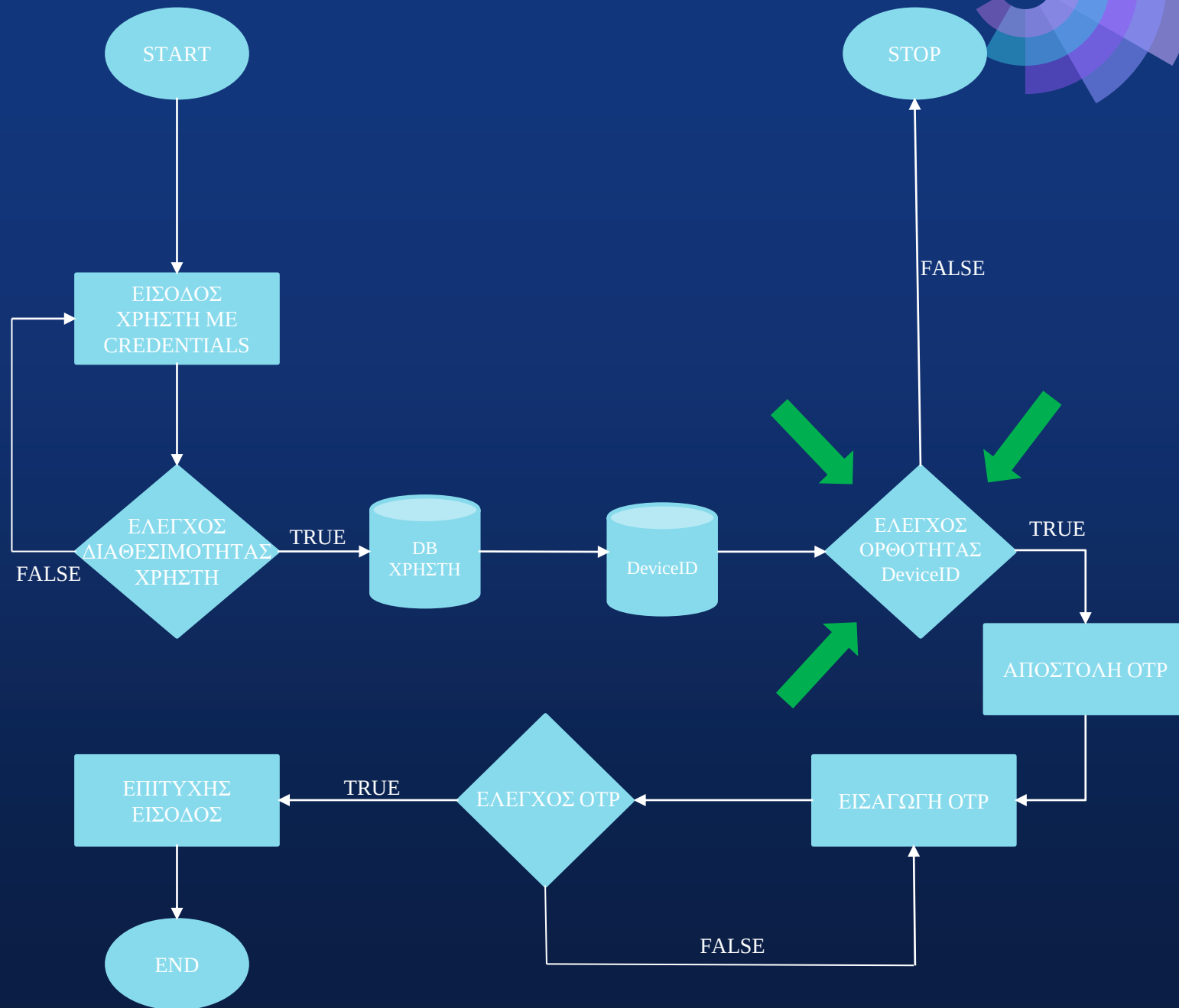
Ο επιτιθέμενος δεν μπορεί να επέμβει
στην διαδικασία αποστολής του OTP.



Διάγραμμα τεχνικής διαδικασίας εξέλιξης της ασφάλειας εφαρμογής που βασίζεται
στην εγκυρότητα του DeviceID.



Ο επιτιθέμενος δεν μπορεί να επέμβει
στην διαδικασία αποστολής του OTP.



Διάγραμμα τεχνικής διαδικασίας εξέλιξης της ασφάλειας εφαρμογής που βασίζεται στην εγκυρότητα του DeviceID.



Ιόνιο Πανεπιστήμιο
Τμήμα Πληροφορικής
- Πτυχιακή Εργασία -
Κέρκυρα, 21 Σεπτεμβρίου 2021

Πίνακας Περιεχομένων



01

Ορισμός Κοινωνικής Μηχανικής

02

Στατιστικά επιθέσεων

03

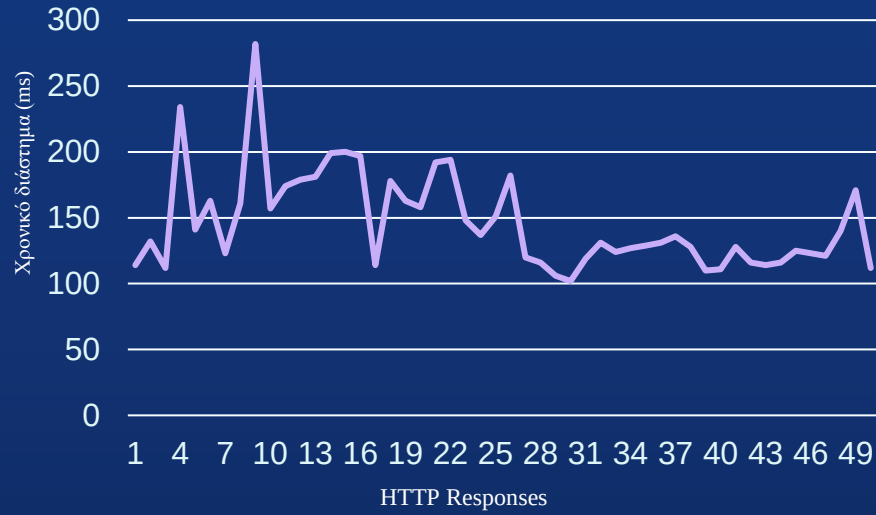
SIM SWAP

04

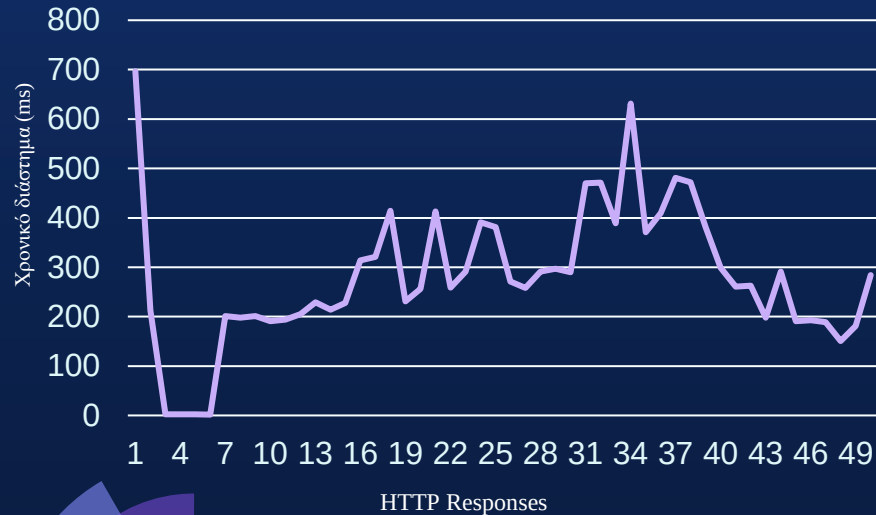
Ανάπτυξη εφαρμογής

Συμπεράσματα

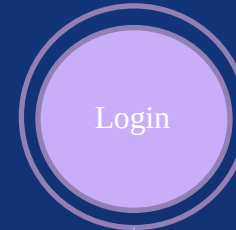
Συμπεράσματα- Αξιολόγηση



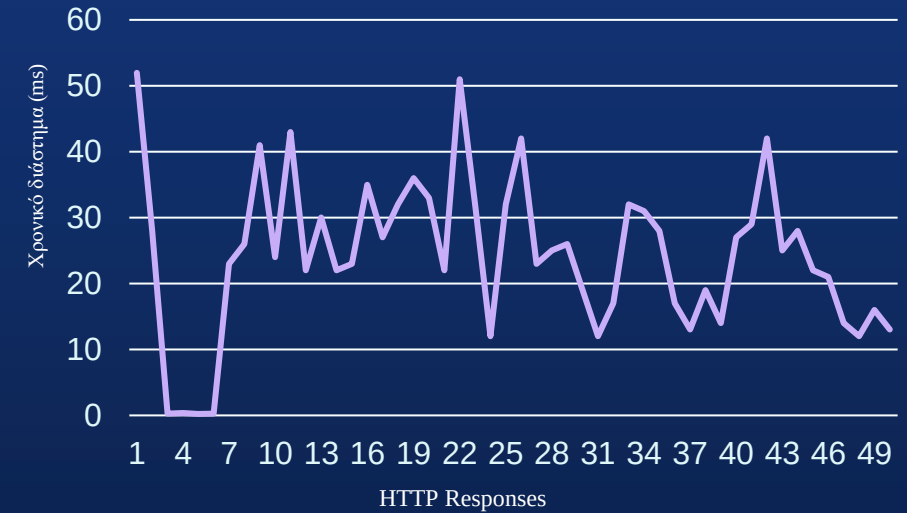
Αποτελέσματα POSTMAN για Login.



Αποτελέσματα POSTMAN για Register.



Efficiency



Αποτελέσματα POSTMAN για ConfirmOtp.



Effectiveness

- ❑ Απαραίτητη η διεξαγωγή αρκετών πειραμάτων για τον έλεγχο της λειτουργικότητας της εφαρμογής.
- ❑ ΤΦΑ αποτελεί έναν από τους πιο ασφαλείς τρόπους εξασφάλισης της ιδιωτικότητας και διαφύλαξης των προσωπικών στοιχείων κατά την πραγματοποίηση διαδικτυακών συναλλαγών.

Impact on the environment of user

- ❑ Απαραίτητη είναι η χρήση της εφαρμογής για την διεξαγωγή του πορίσματος σχετικά με την ασφάλεια της.





Μελλοντικές Προεκτάσεις

- ✓ Πίνακας στο RESTful API που θα αποθηκεύει όλους τους OTP έχουν δημιουργηθεί μέσα σε ένα μικρό χρονικό διάστημα. Η αλλαγή αυτήν θα εξασφαλίζει την ανωνυμία του επομένου αριθμού OTP καθώς θα αποτελείται από διαφορετικούς μη χρησιμοποιήσιμους συνδυασμούς ψηφίων.
- ✓ Δημιουργία μιας χρονικής μπάρας στο frontend η οποία θα χρησιμοποιείται για την λήξη του αριθμού OTP, έχοντας ως βασικό χαρακτηριστικό την λήψη του χρόνου λήξης του αριθμού από το API οπού και δημιουργείται.