ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΔΙΑΤΜΗΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

ΠΛΗΡΟΦΟΡΙΚΗ ΚΑΙ ΥΠΟΛΟΓΙΣΤΙΚΗ ΒΙΟΙΑΤΡΙΚΗ

«Ενίσχυση ασφάλειας συστημάτων για την προφύλαξη οθόνης σε κινητά»

Γκογκίδης Ανάργυρος

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Επιβλέπων

Αθανάσιος Κακαρούντας

Λαμία, 2021

UNIVERSITY OF THESSALY

SCHOOL OF SCIENCE

INFORMATICS AND COMPUTATIONAL BIOMEDICINE

«Security enhanced systems for mobile lock screen»

Gkogkidis Anargyros

Master thesis

Athanasios Kakarountas

Lamia, 2021

ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΔΙΑΤΜΗΜΑΤΙΚΟ ΜΕΤΑΠΤΥΧΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΠΛΗΡΟΦΟΡΙΚΗ ΚΑΙ ΥΠΟΛΟΓΙΣΤΙΚΗ ΒΙΟΙΑΤΡΙΚΗ

ΚΑΤΕΥΘΥΝΣΗ ΠΛΗΡΟΦΟΡΙΚΗ ΜΕ ΕΦΑΡΜΟΓΕΣ ΣΤΗΝ ΑΣΦΑΛΕΙΑ, ΔΙΑΧΕΙΡΙΣΗ ΜΕΓΑΛΟΥ ΟΓΚΟΥ ΔΕΔΟΜΕΝΩΝ ΚΑΙ ΠΡΟΣΟΜΟΙΩΣΗ

Ενίσχυση ασφάλειας συστημάτων για την προφύλαξη οθόνης σε κινητά

Γκογκίδης Ανάργυρος

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Επιβλέπων

Αθανάσιος Κακαρούντας

Λαμία, 2021

«Υπεύθυνη Δήλωση μη λογοκλοπής και ανάληψης προσωπικής ευθύνης»

Με πλήρη επίγνωση των συνεπειών του νόμου περί πνευματικών δικαιωμάτων, και γνωρίζοντας τις συνέπειες της λογοκλοπής, δηλώνω υπεύθυνα και ενυπογράφως ότι η παρούσα εργασία με τίτλο [«τίτλος εργασίας»] αποτελεί προϊόν αυστηρά προσωπικής εργασίας και όλες οι πηγές από τις οποίες χρησιμοποίησα δεδομένα, ιδέες, φράσεις, προτάσεις ή λέξεις, είτε επακριβώς (όπως υπάρχουν στο πρωτότυπο ή μεταφρασμένες) είτε με παράφραση, έχουν δηλωθεί κατάλληλα και ευδιάκριτα στο κείμενο με την κατάλληλη παραπομπή και η σχετική αναφορά περιλαμβάνεται στο τμήμα των βιβλιογραφικών αναφορών με πλήρη περιγραφή. Αναλαμβάνω πλήρως, ατομικά και προσωπικά, όλες τις νομικές και διοικητικές συνέπειες που δύναται να προκύψουν στην περίπτωση κατά την οποία αποδειχθεί, διαχρονικά, ότι η εργασία αυτή ή τμήμα της δεν μου ανήκει διότι είναι προϊόν λογοκλοπής.

Ο ΔΗΛΩΝ

Γκογκίδης Ανάργυρος

10 Ιουνίου 2021

Ενίσχυση ασφάλειας συστημάτων για την προφύλαξη οθόνης σε κινητά

Γκογκίδης Ανάργυρος

Τριμελής Επιτροπή:

Αθανάσιος Κακαρούντας, Αναπληρωτής Καθηγητής (Επιβλέπων)

Μαρία Κοζύρη, Επίκουρη Καθηγήτρια

Αθανάσιος Λουκόπουλος, Επίκουρος Καθηγητής

Περίληψη

Η ραγδαία ανάπτυξη της τεχνολογίας των κινητών τηλεφώνων οδήγησε στην εξέλιξη των συσκευών και την μετατροπή τους από μια απλή συσκευή επικοινωνίας σε ένα περίπλοκο ισχυρό υπολογιστικό σύστημα, το οποίο προσφέρει πληθώρα δυνατοτήτων και υπηρεσιών. Το άμεσο αποτέλεσμα είναι η αποθήκευση ευαίσθητων δεδομένων σε συσκευές που μπορούν εύκολα να χαθούν ή ακόμα και να κλαπούν. Στην παρούσα διπλωματική πραγματοποιήθηκε έρευνα σε χρήστες κινητών τηλεφώνων προκειμένου να εξάγουμε συμπεράσματα, όπως το πώς και αν αντιλαμβάνονται τα ευαίσθητα δεδομένα, ποιους τρόπους επιλέγουν για να ασφαλίσουν τη συσκευή τους και αν θα έδειχναν προθυμία στο να δοκιμάσουν νέες μεθόδους αυθεντικοποίησης, οι οποίες προσφέρουν περισσότερη ασφάλεια. Η έρευνα διεξήχθη σε 81 χρήστες κινητών τηλεφώνων και τα αποτελέσματα αποκαλύπτουν πως οι μέθοδοι αυθεντικοποίησης που βασίζονται σε κείμενο, είναι η κύρια προτίμηση των χρηστών, με τη δημοφιλέστερη μάλιστα να είναι χρήση κωδικού PIN. Οι χρήστες που έχουν επιλέξει βιομετρικές μεθόδους φαίνεται να έχουν μία καλύτερη αντίληψη για τη σημασία των ευαίσθητων δεδομένων, και τέλος η ανάλυση έδειξε πως ανεξαρτήτως τρόπου ασφάλειας και αυθεντικοποίησης, η πλειοψηφία των ερωτηθέντων είναι θετική στο να δοκιμάσει νέους μηχανισμούς αυθεντικοποίησης προκειμένου να προστατεύσουν τα προσωπικά τους δεδομένα. Προσπαθήσαμε να καταλάβουμε ποια είναι η κύρια εστίαση του τελικού χρήστη και προτείνουμε ένα σύστημα που προσπαθεί να καλύψει τις περισσότερες ανάγκες του. Το σύστημα υιοθετεί ισχυρά χαρακτηριστικά γνωστών μεθόδων και εισάγει μια τυχαιότητα των δεδομένων των χρηστών σε προκαθορισμένες κατηγορίες έτσι ώστε να είναι σε θέση να αντιμετωπίσει ήδη γνωστές επιθέσεις και τρωτά σημεία άλλων μηχανισμών ασφαλείας.

Abstract

The rapid evolution of mobile phone devices resulted in transforming a communication device into a powerful compact computer that can offer multiple much-needed features and services. The devices, as mentioned earlier, can now store sensitive data that can be easily lost or stolen. As a part of this thesis, a mobile user survey was conducted in order to get a better understanding of which authentication method is mostly, if the users understand the meaning of "sensitive data," the authentication methods they use, and their willingness to try a new more secure authentication method. Eighty-one users took place in the survey, and the results reveal that text-based authentication methods are still the number one preference, with the most commonly used being the Pin-Code. The biometric authentication adapters seem to have a better understanding of sensitive data, and the majority of users, regardless of their preferred authentication method, are willing to try new authentication methods. We tried to understand what is the main focus of the end user and proposed a system which complies with his needs. The system adopts strong characteristics of known methods and intro-duces a randomness of social user data in pre-defined categories. Moreover, the proposed system manages to cope with known vulnerabilities, e.g. over-the-shoulder attack.

Ευχαριστίες

Με την ολοκλήρωση της παρούσας πτυχιακής εργασίας θα ήθελα να ευχαριστήσω όλους τους ανθρώπους που με στήριξαν όλα αυτά τα χρόνια. Αρχικά ευχαριστώ πολύ τον καθηγητή μου κ. Αθανάσιο Κακαρούντα για την εμπιστοσύνη, την καθοδήγηση και τη βοήθειά του, ώστε να ολοκληρωθεί αυτή η εργασία. Ένα μεγάλο ευχαριστώ θέλω να πω στους φίλους μου και υποψήφιους Διδάκτορες, Λένα Μπούμπα και Βασίλη Τσούκα για την πολύτιμη στήριξη και βοήθειά τους για την διεκπεραίωση της παρούσας εργασίας.

Επιπλέον, θα ήθελα να ευχαριστήσω την οικογένειά μου για την στήριξή τους όλα αυτά τα χρόνια και για τα εφόδια που μου έδωσαν, ώστε να καταφέρω να ολοκληρώσω αυτό τον κύκλο σπουδών μου και να γίνω ένας σωστός Άνθρωπος.

Τέλος, θα ήθελα να αφιερώσω την παρούσα εργασία στον Ηλία και τον Κωνσταντίνο που πιστεύουν σε εμένα και μου δίνουν συνεχώς δύναμη για να κυνηγήσω τα όνειρά μου.

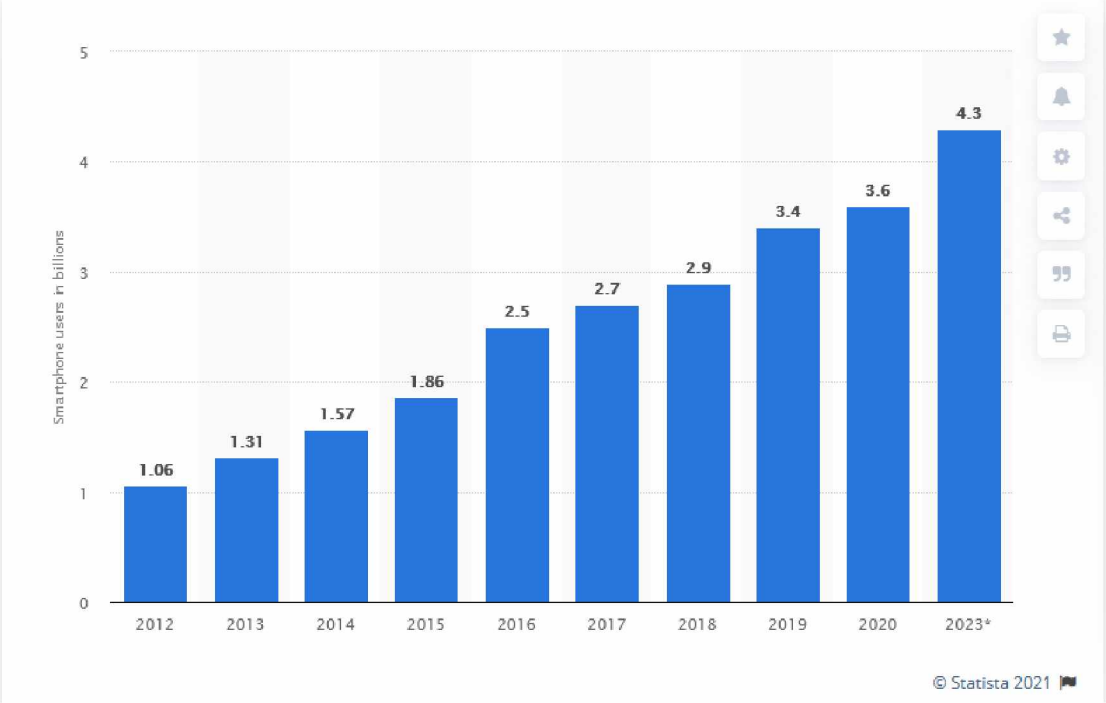
Περιεχόμενα

Ευρετήριο Εικόνων

1. Εισαγωγή

Η ραγδαία ανάπτυξη των κινητών συσκευών, του Διαδικτύου και της υπολογιστικής ισχύς σε φορητές συσκευές, πρόσφερε την ευκαιρία στον τελικό χρήστη να σταματήσει να χρησιμοποιεί συσκευές όπως το MP3 player, ebook reader, tablet ακόμα και τον φορητό υπολογιστή του και να έχει ανάγκη μίας μόνο συσκευή που του προσφέρει όλες τις παραπάνω υπηρεσίες, το κινητό τηλέφωνο.

Σύμφωνα με τη Statista [1] τα τελευταία πέντε χρόνια περίπου 1,4 δισεκατομμύρια smartphones πωλούνται ετησίως, ο συνολικός αριθμός smartphone χρηστών σήμερα ξεπερνά τα τρία δισεκατομμύρια και σύμφωνα με την εταιρεία είναι πολύ πιθανό να αυξηθεί κατά μερικές εκατοντάδες εκατομμύρια μέσα στα επόμενα χρόνια. Η αύξηση στην παγκόσμια χρήση αυτών των συσκευών συνεπάγεται με την αύξηση των ευαίσθητων δεδομένων π.χ. email, τραπεζικοί λογαριασμοί, φωτογραφίες αποθηκευμένες σε συσκευές που μπορούν εύκολα να παραβιαστούν, να χαθούν ή να κλαπούν.



Εικόνα 1 Αριθμός χρηστών smartphones παγκοσμίως από το 2016 εως το 2023

Αμέσως μπορούμε να φτάσουμε στο συμπέρασμα πως η ασφάλεια σε κινητές συσκευές είναι ζωτικής σημασίας και πρέπει να είναι επαρκής για την προστασία του

χρήστη και των ευαίσθητων και εμπιστευτικών δεδομένων του. Η αγαπημένη μέθοδος αυθεντικοποίησης των χρηστών παραμένει το PIN, ο προσωπικός αριθμός αναγνώρισης, και ακολουθούν άλλες δύο παρόμοιες μέθοδοι, το password και το pass-code. Οι μηχανισμοί που προαναφέρθηκαν είναι στην κατηγορία μεθόδων που βασίζονται σε κείμενο και τα δύο βασικότερα αρνητικά τους στοιχεία είναι το ότι ο χρήστης είναι υποχρεωμένος να θυμάται αρκετούς διαφορετικούς κωδικούς για διαφορετικές συσκευές, αλλά και το ότι οι τρόποι αυθεντικοποίησης που βασίζονται σε κείμενο έχουν ευπάθεια σε ένα μεγάλο εύρος γνωστών επιθέσεων [2].

Μία πιθανή λύση που θα μπορούσε να διευκολύνει το χρήστη στο να μην θυμάται ένα μεγάλο πλήθος κωδικών αλλά και μια λύση η οποία εγγυάται υψηλότερο ποσοστό ασφάλειας είναι η υιοθέτηση των Βιομετρικών μεθόδων αυθεντικοποίησης. Σήμερα υπάρχουν αρκετοί μηχανισμοί που χρησιμοποιούν βιομετρικά χαρακτηριστικά, όπως για παράδειγμα ο σαρωτής δαχτυλικού αποτυπώματος, αλλά παρόλη την ασφάλεια που προσφέρουν, χαρακτηρίζονται αρνητικά από έναν μεγάλο αριθμό μειονεκτημάτων, με τα πιο συχνά εμφανιζόμενα να είναι τα ακόλουθα:

1) Η ταχύτητα και ο χρόνος απόκρισης εξαρτάται τόσο από την ποιότητα όσο και από την τοποθέτηση αλλά και το είδος του σαρωτή, πχ απλός σαρωτής δακτυλικού αποτυπώματος ή ultrasonic σαρωτής δακτυλικού αποτυπώματος.
2) Η αστοχία του μηχανισμού στο να αναγνωρίσει τον χρήστη στην περίπτωση που αυτός φοράει γάντια ή έχει ιδρωμένα χέρια.

Έρευνες έχουν δείξει πως οι χρήστες επιθυμούν να έχουν ως μηχανισμό ασφαλείας κάτι αρκετά εύχρηστο και ότι επίσης οι χρήστες δεν γνωρίζουν πως μπορούν να επιλέξουν διαφορετικούς τρόπους αυθεντικοποίησης πέρα από τη χρήση του κωδικού PIN. [3,4] Αυτό οφείλεται στην ελλιπή ενημέρωση των κατασκευαστών αλλά και στην απροθυμία του χρήστη να ενημερωθεί για τις νέες τεχνολογίες, κυρίως γιατί δεν αντιλαμβάνεται σωστά πόσο σημαντικά είναι τα ευαίσθητα δεδομένα του.

2. Σημαντικότερες απειλές για την ασφάλεια των κινητών τηλεφώνων

Η ασφάλεια των κινητών συσκευών βρίσκεται στην κορυφή της λίστας ανησυχίας κάθε εταιρείας αυτές τις μέρες. Η CSO, εταιρεία που πραγματοποιεί ανάλυση και έρευνα στα θέματα ασφάλειας έχει διεξαγάγει μία πλήρη έρευνα που αφορά τις απειλές σε κινητά τηλέφωνα [24]. Σχεδόν όλοι οι εργαζόμενοι έχουν πλέον συνεχή πρόσβαση σε εταιρικά δεδομένα από smartphone, μια τάση που αναπτύσσεται ακόμη πιο έντονη χάρη στη συνεχιζόμενη παγκόσμια πανδημία. Η συντριπτική πλειονότητα των συσκευών που αλληλεπιδρούν με εταιρικά δεδομένα είναι πλέον φορητές, περίπου το 60% [20], και αυτός ο αριθμός είναι βέβαιο ότι θα συνεχίσει να αυξάνεται καθώς ο κόσμος προσαρμόζεται στη νέα πραγματικότητα της απομακρυσμένης εργασίας.

Η σημασία της διατήρησης ευαίσθητων πληροφοριών από λάθος χέρια είναι ένα όλο και πιο περίπλοκο παζλ. Το μέσο κόστος μιας παραβίασης εταιρικών δεδομένων είναι περίπου 3,86 εκατομμύρια δολάρια, σύμφωνα με έκθεση του Ινστιτούτου Ponemon το 2020 [21]. Αυτό είναι 6,4% περισσότερο από το εκτιμώμενο κόστος μόλις τρία χρόνια νωρίτερα, και η φύση της πανδημίας αναμένεται να αυξήσει ακόμη περισσότερο το κόστος, λαμβάνοντας υπόψη τις πρόσθετες προκλήσεις που παρουσιάζονται λόγω της εργασίας από το σπίτι.

Ενώ το μυαλό όλων μπορεί να πάει στο κακόβουλο λογισμικό, η αλήθεια είναι ότι οι μολύνσεις από κακόβουλα προγράμματα κινητής τηλεφωνίας είναι ασυνήθιστες στον πραγματικό κόσμο. Το κακόβουλο λογισμικό κατατάσσεται ως μία από τις λιγότερο κοινές αρχικές ενέργειες σε περιστατικά παραβίασης δεδομένων, όπως σημειώνεται από την έκθεση έρευνας παραβίασης δεδομένων της Verizon το 2020 [22]. Αυτό οφείλεται τόσο στη φύση του κακόβουλου λογισμικού για κινητά όσο και στις εγγενείς προστασίες που ενσωματώνονται στα σύγχρονα λειτουργικά συστήματα για κινητά.

Οι πιο ρεαλιστικοί κίνδυνοι για την ασφάλεια των κινητών συσκευών βρίσκονται σε ορισμένες περιοχές που συχνά δεν δίνεται η απαιτούμενη προσοχή. Ακολουθεί μία σύντομη περιγραφή ορισμένων τομέων για την ασφάλεια κινητών συσκευών.

2.1 Απάτες Χρηστών

Οι επιθέσεις ηλεκτρονικού ψαρέματος (phising) έχουν αυξηθεί από την έναρξη του COVID, και οι κινητές συσκευές είναι τώρα ο κύριος στόχος. Το phising πλέον σχετίζεται με θέματα που ενδιαφέρουν άμεσα τους χρήστες και έχουν συσχέτιση με τον COVID, όπως για παράδειγμα τρόποι προφύλαξης ή επιδόματα. Ένα περίπου

91% του εγκλήματος στον κυβερνοχώρο ξεκινά με email, σύμφωνα με έκθεση της εταιρείας ασφαλείας FireEye [23]. Αναφέρεται σε τέτοια περιστατικά όπως "επιθέσεις χωρίς κακόβουλο λογισμικό", καθώς βασίζονται σε τακτικές όπως η πλαστοπροσωπία για να εξαπατήσουν τους ανθρώπους να κάνουν κλικ σε επικίνδυνους συνδέσμους ή να παρέχουν ευαίσθητες πληροφορίες. Το ηλεκτρονικό ψάρεμα (phishing) έχει αναπτυχθεί ραγδαία τα τελευταία χρόνια και οι χρήστες κινητών τηλεφώνων διατρέχουν τον μεγαλύτερο κίνδυνο, λόγω του τρόπου με τον οποίο πολλοί πελάτες ηλεκτρονικού ταχυδρομείου για κινητά εμφανίζουν μόνο το όνομα ενός αποστολέα, καθιστώντας το ιδιαίτερα εύκολο να γίνει πλαστογράφηση μηνυμάτων και να εξαπατηθεί ένα άτομο που σκέφτεται ότι ένα email προέρχεται από κάποιον που γνωρίζουν.

Οι χρήστες είναι τρεις φορές πιο πιθανό να ανταποκριθούν σε μια επίθεση ηλεκτρονικού ψαρέματος σε μια φορητή συσκευή από έναν επιτραπέζιο υπολογιστή, σύμφωνα με μελέτη της IBM [25], εν μέρει επειδή το τηλέφωνο είναι η συσκευή όπου ο χρήστης είναι πιθανότερο να δει πρώτα ένα μήνυμα. Η έρευνα της Verizon υποστηρίζει αυτό το συμπέρασμα και προσθέτει ότι τα μικρότερα μεγέθη οθόνης και η αντίστοιχη περιορισμένη εμφάνιση λεπτομερών πληροφοριών σε smartphone (ιδιαίτερα στις ειδοποιήσεις, οι οποίες συχνά περιλαμβάνουν επιλογές με ένα πάτημα για άνοιγμα συνδέσμων ή απόκριση σε μηνύματα) μπορούν επίσης να αυξήσουν την πιθανότητα επιτυχίας του ηλεκτρονικού ψαρέματος.

Ενώ μόνο περίπου το 3,4% των χρηστών κάνουν πραγματικά κλικ σε συνδέσμους που σχετίζονται με το ηλεκτρονικό ψάρεμα (phishing), οι χρήστες αυτοί τείνουν να είναι επαναλαμβανόμενοι παραβάτες. Μάλιστα, έχει αποδειχθεί ότι όσες περισσότερες φορές κάποιος έχει κάνει κλικ σε έναν σύνδεσμο καμπάνιας ηλεκτρονικού ψαρέματος (phishing), τόσο πιθανότερο είναι να το κάνει ξανά στο μέλλον. Η Verizon είχε αναφέρει στο παρελθόν ότι το 15% των χρηστών που έχουν υποβληθεί σε ηλεκτρονικό ψάρεμα θα υποβληθούν σε ηλεκτρονικό ψάρεμα (phishing) τουλάχιστον μία ακόμη φορά εντός του ίδιου έτους.

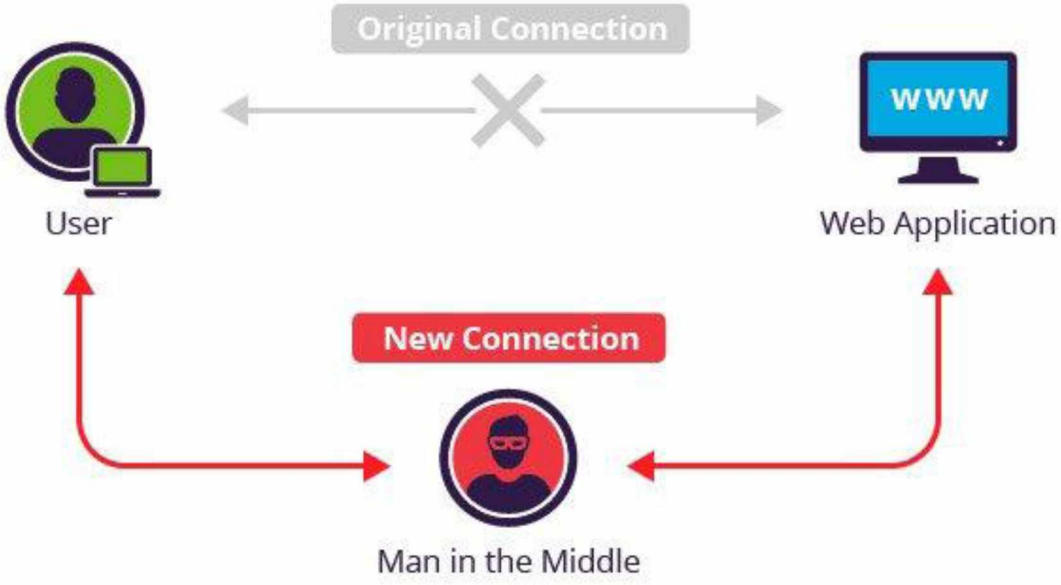
Οι κακόβουλοι χρήστες χρησιμοποιούν ακόμη και phishing για να προσπαθήσουν να εξαπατήσουν τους απλούς χρήστες να τους δώσουν ακόμα και τους κωδικούς ελέγχου ταυτότητας δύο παραγόντων, που έχουν σχεδιαστεί για να προστατεύουν τους λογαριασμούς από μη εξουσιοδοτημένη πρόσβαση.

Η μετάβαση σε μηχανισμούς αυθεντικοποίησης που βασίζεται σε hardware, είναι ο νούμερο ένα τρόπος αποφυγής του phising. Σύμφωνα με μια μελέτη που διεξήχθη από την Google [26], το Πανεπιστήμιο της Νέας Υόρκης και το UC San Diego, ο έλεγχος ταυτότητας στη συσκευή μπορεί να αποτρέψει το 99% των μαζικών επιθέσεων ηλεκτρονικού ψαρέματος και το 90% των στοχευμένων επιθέσεων, σε σύγκριση με το ποσοστό αποτελεσματικότητας 96% και 76% για τους ίδιους τύπους επιθέσεων με τους πιο ευαίσθητους σε phising παραδοσιακούς κωδικούς 2FA.

2.2 Δίκτυα

Ένα κινητό τηλέφωνο είναι εξίσου ασφαλές με το δίκτυο μέσω του οποίου μεταδίδει δεδομένα. Σήμερα όλοι συνδέονται συνεχώς με δίκτυα που ενδέχεται να μην είναι ασφαλή, είτε είναι εσφαλμένα διαμορφωμένα οικιακά δίκτυα, ή και δημόσια δίκτυα WiFi όπου ο καθένας έχει πρόσβαση και οι πληροφορίες και τα δεδομένα δεν είναι επαρκώς προστατευμένα.

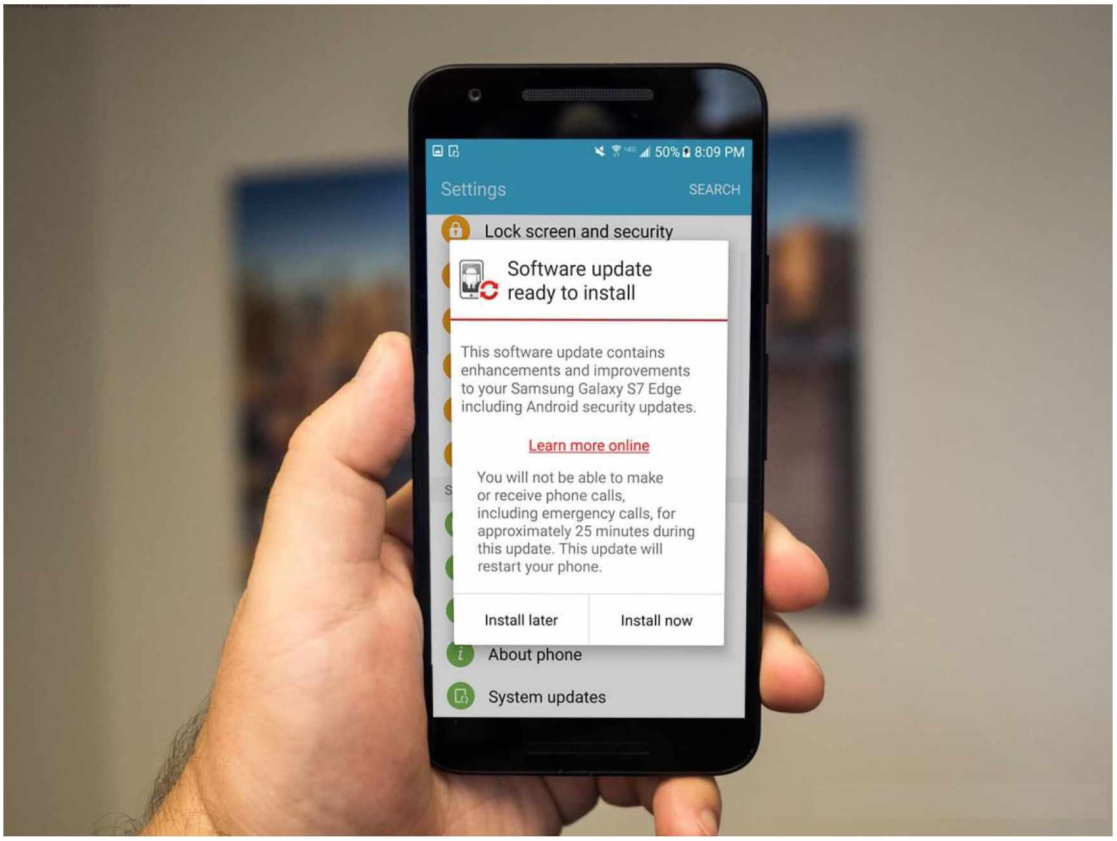
Σχεδόν το ένα τέταρτο των συσκευών σήμερα συνδέονται σε ανοικτά και ανασφαλή δίκτυα WiFi και περίπου το 4% των συσκευών έχουν δεχτεί μια επίθεση man-in-the-middle. Κατά τη διάρκεια αυτού του τύπου της επίθεσης ο επιτιθέμενος παρεμποδίζει την επικοινωνία μεταξύ δύο μερών, τα οποία είναι γνωστά μεταξύ τους. Ο κακόβουλος χρήστης ελέγχει την επικοινωνία και μπορεί να αποσπάσει ή να τροποποιήσει τις πληροφορίες που στέλνονται μεταξύ των δύο μερών. Αυτές οι επιθέσεις σαφώς και έχουν μειωθεί τον τελευταίο χρόνο λόγω των μειωμένων ταξιδιών και λιγότερων φυσικών επιχειρήσεων που ανοίγουν κατά τη διάρκεια του COVID, αλλά αυτό δεν σημαίνει ότι η απειλή έχει εξαλειφθεί.



Εικόνα 2 Επίθεση Man in the Middle

2.3 Μη ενημερωμένες Συσκευές

Τα smartphone αποτελούν σημαντικό κίνδυνο για την ασφάλεια των χρηστών και των επιχειρήσεων, σε αντίθεση με τις παραδοσιακές συσκευές εργασίας, λόγω του ότι δεν συνοδεύονται από εγγυήσεις για έγκαιρες και συνεχείς ενημερώσεις λογισμικού άλλα και ότι ο χρήστης μπορεί να επιλέξει για το αν και πότε θα κάνει την απαραίτητη ενημέρωση. Αυτό είναι ιδιαίτερα εμφανές στις συσκευές με λειτουργικό σύστημα Android, όπου η συντριπτική πλειονότητα των κατασκευαστών είναι δυστυχώς αναποτελεσματικοί στο να διατηρούν τα προϊόντα τους ενημερωμένα - τόσο με ενημερώσεις λειτουργικού συστήματος όσο και με τις μικρότερες μηνιαίες ενημερώσεις κώδικα ασφαλείας. Μάλιστα μεγάλες εταιρείες προσφέρουν πολλές φορές μόνο ένα ή δύο χρόνια υποστήριξη σε ενημερώσεις συσκευών, ενώ ο χρόνος που ο μέσος χρήστης έχει στην κατοχή του την ίδια συσκευή πριν προβεί στην αγορά μίας νέας, είναι σαφώς μεγαλύτερος. Αυτό έχει ως αποτέλεσμα τα ευαίσθητα δεδομένα του χρήστη να μην έχουν το επιθυμητό επίπεδο ασφάλειας ή σε ορισμένες περιπτώσεις να είναι και εντελώς απροστάτευτα.



Εικόνα 3 Ενημέρωση Ασφάλειας σε σύστημα Android

2.4 Θέματα με κωδικούς πρόσβασης

Μια έρευνα της Google και του Harris Poll [27] διαπίστωσε ότι πάνω από τους μισούς Αμερικανούς επαναχρησιμοποιούν κωδικούς πρόσβασης σε πολλούς λογαριασμούς. Εξίσου ανησυχητικό, σχεδόν το ένα τρίτο δεν χρησιμοποιεί 2FA ή δεν γνωρίζει πως να το χρησιμοποιεί. Μόνο το ένα τέταρτο των ατόμων χρησιμοποιούν ενεργά λογισμικό για την κεντρική διαχείριση κωδικών πρόσβασης, κάτι που υποδηλώνει ότι η συντριπτική πλειοψηφία των ανθρώπων πιθανώς δεν έχουν ισχυρούς κωδικούς πρόσβασης στους περισσότερους λογαριασμούς τους, δεδομένου ότι πιθανώς δημιουργούν κωδικούς από μόνοι τους μη ακολουθώντας σωστές πρακτικές για την σωστή προστασία των συσκευών τους.

Σύμφωνα με μια έρευνα τις εταιρείας LastPass [28], περίπου το 50% των επαγγελματιών έχει παραδεχτεί ότι χρησιμοποιεί τους ίδιους κωδικούς πρόσβασης τόσο για τους εταιρικούς λογαριασμούς όσο και για τους προσωπικούς τους λογαριασμούς. Επίσης παρουσιάζει ότι ένας μέσος υπάλληλος μοιράζεται περίπου έξι κωδικούς πρόσβασης με έναν συνάδελφο κατά τη διάρκεια της απασχόλησής του στην εταιρεία.

Η Verizon σε μία άλλη έρευνα [29] διαπίστωσε ότι οι αδύναμοι ή κλεμμένοι κωδικοί πρόσβασης ευθύνονται για περισσότερο από το 80% των παραβιάσεων που σχετίζονται με παραβιάσεις στις επιχειρήσεις. Ως ένα παράδειγμα μπορούμε να υποθέσουμε ότι οι εργαζόμενοι θέλουν να συνδεθούν γρήγορα σε εφαρμογές, ιστότοπους και υπηρεσίες οπότε πληκτρολογούν έναν μη ασφαλή κωδικό πρόσβασης τον οποίο τον χρησιμοποιούν και σε προσωπικούς λογαριασμούς εκτός εργασίας. Ο ιστότοπος ή η εφαρμογή στην οποία χρησιμοποιήθηκε ο συγκεκριμένος κωδικός είναι αμφιλεγόμενης ποιότητας και πιθανώς κακόβουλος. Σε συνδυασμό τώρα με τον προαναφερθέντα κίνδυνο παρεμβολής WiFi, και πολλαπλασιάζοντας τον με τον συνολικό αριθμό εργαζομένων στο χώρο εργασίας συνυπολογίζοντας και πόσες φορές ανά ημέρα μπορεί να χρειαστεί να πληκτρολογηθεί ο κωδικός πρόσβασης, καταλαβαίνουμε πόσο μεγάλος είναι ο κίνδυνος και η έκθεση των προσωπικών και εταιρικών δεδομένων σε αυτόν.

2.5 Απάτες Διαφημίσεων

Η απάτη διαφημίσεων μπορεί να έχει διάφορες μορφές, αλλά η πιο συνηθισμένη είναι η χρήση κακόβουλου λογισμικού για τη δημιουργία κλικ σε διαφημίσεις που φαίνεται να προέρχονται από πραγματικό χρήστη χρησιμοποιώντας μία γνωστή εφαρμογή ή ιστότοπο. Έτσι, για παράδειγμα, ένας χρήστης μπορεί να κατεβάσει μια εφαρμογή που προσφέρει μια έγκυρη υπηρεσία όπου στο παρασκήνιο όμως η συγκεκριμένη εφαρμογή να δημιουργεί κλικ σε διαφημίσεις που εμφανίζει η εφαρμογή.

Αυτό που μπορούμε να συμπεράνουμε εύκολα είναι πως οι διαφημιζόμενοι είναι τα πιο εμφανή θύματα λόγω του ότι χάνουν τα χρήματα τους καθώς δεν μεταβαίνει ο χρήστης στον διαφημιζόμενο ιστότοπο ή υπηρεσία, ωστόσο, η απάτη διαφημίσεων μπορεί να βλάψει και τους χρήστες κινητών. Το κακόβουλο λογισμικό απάτης διαφημίσεων εκτελείται στο παρασκήνιο και μπορεί να επιβραδύνει την απόδοση ενός smartphone, να εξαντλήσει την μπαταρία του ή ακόμα και να οδηγήσει σε χρεώσεις δεδομένων.

2.6 Επιθέσεις για Cryptomining

Οι συγκεκριμένες επιθέσεις μοιάζουν ιδιαιτέρως με τις απάτες διαφημίσεων που προαναφέρθηκαν. Χρησιμοποιούν δηλαδή την συσκευή του χρήστη προς όφελος κάποιου 3^{ου}. Μπορούμε να δούμε και εδώ πως επιβραδύνει το smartphone, εξαντλεί την μπαταρία του, οδηγεί σε χρεώσεις δεδομένων αλλά και υπερθερμαίνει την συσκευή λόγω του ότι πραγματοποιεί αλόγιστη χρήση των διαθέσιμων πόρων. Για να κατεβάσει ένας χρήστης μία εφαρμογή που θα δημιουργήσει το συγκεκριμένο πρόβλημα θα πρέπει να μπει σε ιστοσελίδες με παράνομο περιεχόμενο, όπως για παράδειγμα ιστοσελίδες για την online προβολή ταινιών ή σειρών, να κατεβάσει κάποια εφαρμογή από ιστοσελίδες τρίτων ή πιο σπάνια εφαρμογή που δεν έχει ελεγχτεί σωστά από το Play Store ή το App Store.

2.7 Παραβιάσεις Συσκευών

Τέλος, μια συσκευή η οποία έχει χαθεί ή κλαπεί διατρέχει μεγάλο κίνδυνο για τα δεδομένα του χρήστη στην περίπτωση που δεν ασφαλίζεται από ισχυρούς μηχανισμούς αυθεντικοποίησης. Μία έρευνα της Ponemon [30] έδειξε ότι το 35% των επαγγελματιών χρηστών κινητών τηλεφώνων δεν έχουν λάβει τα απαραίτητα μέτρα για τις εταιρικές τους συσκευές προκειμένου να εξασφάλισουν τα εταιρικά δεδομένα. Το 50% των ερωτηθέντων δήλωσαν ότι δεν είχαν κωδικό πρόσβασης, PIN ή βιομετρικό μηχανισμό ασφάλειας για την προστασία των συσκευών τους. Περίπου τα δύο τρίτα δήλωσαν ότι δεν χρησιμοποίησαν κρυπτογράφηση και το 68% των ερωτηθέντων δήλωσαν ότι έχουν μοιραστεί κωδικούς πρόσβασης σε προσωπικούς και επαγγελματικούς λογαριασμούς στους οποίους έχουν πρόσβαση οι κινητές συσκευές τους.

3. Μέθοδοι Ασφάλειας

Οι βασικές κατηγορίες αυθεντικοποίησης είναι οι ακόλουθες τρεις [5,19]:

I. *Κάτι που γνωρίζει ο χρήστης*

Ο παράγοντας που γνωρίζει κάτι ο χρήστης είναι ο πιο κοινός παράγοντας που χρησιμοποιείται και μπορεί να είναι ένας κωδικός πρόσβασης ή ένας απλός προσωπικός αριθμός αναγνώρισης (PIN). Ωστόσο, είναι επίσης και ο πιο εύκολος μηχανισμός για να σπάσει. Ένας ισχυρός κωδικός πρόσβασης έχει ένα μείγμα κεφαλαίων, πεζών, αριθμών και ειδικών χαρακτήρων. Στο παρελθόν, οι επαγγελματίες ασφαλείας πρότειναν οι κωδικοί πρόσβασης να έχουν τουλάχιστον οκτώ χαρακτήρες. Ωστόσο, με την αυξανόμενη ισχύ των κωδικών πρόσβασης, είναι σύνηθες να ακούμε επαγγελματίες να προτείνουν μεγαλύτερους κωδικούς πρόσβασης. Για παράδειγμα, πολλοί οργανισμοί απαιτούν οι κωδικοί πρόσβασης διαχειριστή να έχουν τουλάχιστον 15 χαρακτήρες. Οι μεγαλύτεροι κωδικοί πρόσβασης είναι πιο δύσκολο στο να απομνημονευτούν, εκτός εάν έχουν μπει σε συγκεκριμένη σειρά οι χαρακτήρες προκειμένου να σημαίνουν κάτι. Για παράδειγμα, μια φράση όπως "Η ασφάλεια δημιουργεί επιτυχία", μπορεί να γίνει κωδικός πρόσβασης γράφοντάς το "S3curityBr33d $ Succ3 $$". Η λέξη ξεκινά με κεφαλαίο γράμμα, τα πεζά "s" αλλάζουν σε $, κάθε πεζό "e" αλλάζει σε 3 και τα κενά αφαιρούνται. Με αυτόν τον τρόπο έχουμε έναν αρκετά πιο δύσκολο κωδικό τον οποίο όμως μπορούμε να θυμόμαστε πιο εύκολα. Ωστόσο, εάν ένας χρήστης απαιτείται να θυμάται έναν μεγάλο κωδικό πρόσβασης χωρίς κανένα νόημα, όπως για παράδειγμα "1kqd9% lu @ 7cpw #", είναι πολύ πιο πιθανό να σημειώσει σε κάποιο χαρτάκι τον κωδικό πρόσβασης, μειώνοντας με αυτόν τον τρόπο την ασφάλεια του.

II. *Κάτι που είναι ο χρήστης*

Οι βιομετρικές μέθοδοι ανήκουν στην κατηγορία του «κάτι που είναι ο χρήστης». Μερικές από τις βιομετρικές μεθόδους που μπορούν να χρησιμοποιηθούν είναι τα δακτυλικά αποτυπώματα, η γεωμετρία χεριών, η σάρωση αμφιβληστροειδούς ή ίριδας, τα χειρόγραφα και η φωνητική ανάλυση. Τα δακτυλικά αποτυπώματα είναι η πιο διαδεδομένη βιομετρική μέθοδος που χρησιμοποιείται σήμερα. Σχεδόν όλα τα έξυπνα κινητά σήμερα περιλαμβάνουν συσκευές ανάγνωσης δακτυλικών αποτυπωμάτων.

Ενώ οι βιομετρικές μέθοδοι παρέχουν τον ισχυρότερο τρόπο αυθεντικοποίησης, είναι επιρρεπή σε σφάλματα. Ένα σφάλμα λανθασμένης απόρριψης (ονομάζεται επίσης σφάλμα τύπου 1) παρουσιάζεται όταν ένα

σύστημα απορρίπτει λανθασμένα έναν γνωστό χρήστη και υποδεικνύει ότι ο χρήστης δεν είναι γνωστός. Ένα σφάλμα λανθασμένης αποδοχής (ονομάζεται επίσης σφάλμα τύπου 2) παρουσιάζεται όταν ένα σύστημα αναγνωρίζει λανθασμένα έναν άγνωστο χρήστη ως γνωστό χρήστη. Τα βιομετρικά συστήματα μπορούν συνήθως να ρυθμιστούν για ευαισθησία, αλλά η ευαισθησία επηρεάζει άμεσα την ακρίβεια.

III. *Κάτι που έχει ο χρήστης στην κατοχή του*

Το κάτι που μπορεί να κατέχει ο χρήστης αναφέρεται σε στοιχεία, όπως έξυπνες κάρτες ή κάποιο φορητό token. Μια έξυπνη κάρτα είναι μεγέθους πιστωτικής κάρτας, η οποία διαθέτει ενσωματωμένο πιστοποιητικό που χρησιμοποιείται για την αναγνώριση του κατόχου. Ο χρήστης μπορεί να εισαγάγει την κάρτα σε έναν αναγνώστη έξυπνων καρτών για να προχωρήσει σε έλεγχο ταυτότητας του ατόμου και αυθεντικοποίηση του. Οι έξυπνες κάρτες χρησιμοποιούνται συνήθως με ένα PIN που παρέχει έλεγχο ταυτότητας πολλών παραγόντων. Με άλλα λόγια, ο χρήστης πρέπει να έχει κάτι (την έξυπνη κάρτα) και να γνωρίζει κάτι (το PIN).

Το token μπορεί είναι μια φορητή συσκευή με LED που εμφανίζει έναν αριθμό και ο αριθμός συγχρονίζεται με έναν διακομιστή ελέγχου ταυτότητας. Ο αριθμός που εμφανίζεται αλλάζει τακτικά, όπως κάθε 60 δευτερόλεπτα, και ο διακομιστής ελέγχου ταυτότητας γνωρίζει πάντα τον τρέχοντα εμφανιζόμενο αριθμό. Για παράδειγμα, στις 5:01 μ.μ., ο αριθμός που εμφανίζεται στο LED μπορεί να είναι 963147 και ταυτόχρονα, ο διακομιστής γνωρίζει ότι ο αριθμός είναι 963147. Ένα λεπτό αργότερα, ο αριθμός που εμφανίζεται στο LED μπορεί να είναι 246813 και ο έλεγχος ταυτότητας που πραγματοποιείται από το διακομιστή πλέον απαιτεί αυτόν τον νέο αριθμό.

Ένας κοινός σήμερα λόγος για τον οποίο χρησιμοποιούνται τα tokens για έλεγχο ταυτότητας γίνεται στους ιστότοπους. Ο χρήστης πρέπει να πληκτρολογήσει τον αριθμό που εμφανίζεται στο token σε μια ιστοσελίδα. Εάν ο χρήστης πληκτρολογήσει τον ίδιο αριθμό που είναι περασμένος ως σωστός από τον διακομιστή εκείνη τη στιγμή, ο χρήστης μπορεί να πιστοποιηθεί. Είναι αρκετά κοινό σήμερα να χρησιμοποιείται ως μέσο αυθεντικοποίησης το token. Εκτός από την εισαγωγή του αριθμού που εμφανίζεται στο token, ο χρήστης συχνά απαιτείται να εισαγάγει ένα όνομα χρήστη και έναν κωδικό πρόσβασης. Αυτό αποδεικνύει ότι έχουν κάτι (το token) και ξέρουν κάτι (τον κωδικό πρόσβασής τους).

Επιπρόσθετα, υπάρχει ο έλεγχος ταυτότητας πολλαπλών παραγόντων όπου χρησιμοποιεί δύο ή περισσότερους παράγοντες ελέγχου ταυτότητας. Ένα βασικό μέρος αυτού είναι ότι οι παράγοντες ελέγχου ταυτότητας πρέπει να βρίσκονται σε τουλάχιστον δύο από τις κατηγορίες. Για παράδειγμα, η χρήση έξυπνης κάρτας και PIN είναι έλεγχος ταυτότητας πολλαπλών παραγόντων,

καθώς οι δύο παράγοντες είναι κάτι που έχει και κάτι που γνωρίζει ο χρήστης. Ωστόσο, εάν απαιτείται από έναν χρήστη να εισαγάγει έναν κωδικό πρόσβασης και έναν κωδικό PIN, δεν θα ήταν έλεγχος ταυτότητας πολλαπλών παραγόντων, καθώς και οι δύο μέθοδοι προέρχονται από τον ίδιο παράγοντα (κάτι που γνωρίζει δηλαδή).

Μια ακόμα μέθοδος που δεν θα μπορούσε να τοποθετηθεί σε μοναδική κατηγορία λόγω του ότι δεν χρησιμοποιείται συχνά είναι ο έλεγχος βάσει τοποθεσίας. Ο έλεγχος ταυτότητας βάσει τοποθεσίας μπορεί να χρησιμοποιηθεί για απομακρυσμένη πρόσβαση μέσω τηλεφώνου ως πρόσθετος παράγοντας ελέγχου ταυτότητας. Για παράδειγμα ο Joe είναι εξουσιοδοτημένος να εργάζεται από το σπίτι χρησιμοποιώντας μια σύνδεση απομακρυσμένης πρόσβασης μέσω τηλεφώνου για σύνδεση με πόρους που βασίζονται στην εργασία. Ο διακομιστής απομακρυσμένης πρόσβασης μπορεί να διαμορφωθεί, έτσι ώστε μόλις ο Joe καλέσει και κάνει έλεγχο ταυτότητας, ο διακομιστής αποσυνδέεται από το τηλέφωνο και δίνει πρόσβαση στον υπολογιστή του Joe στο σπίτι.

Όσο ο Joe προσπαθεί να συνδεθεί από τον υπολογιστή του σπιτιού του, η σύνδεση θα λειτουργεί. Ωστόσο, εάν ένας εισβολέας προσπαθούσε να πλαστογραφήσει τον Joe χρησιμοποιώντας το όνομα χρήστη και τον κωδικό πρόσβασης του Joe, ο εισβολέας δεν θα μπορούσε να συνδεθεί. Αντίθετα, όταν ο εισβολέας έκανε έλεγχο ταυτότητας με τα διαπιστευτήρια του Joe, ο διακομιστής απομακρυσμένης πρόσβασης θα προσπαθούσε να καλέσει τον υπολογιστή του Joe και να δώσει πρόσβαση μόνο σε αυτόν.

Ακολουθεί μία σύντομη περιγραφή των μεθόδων αυθεντικοποίησης που προτιμούν και έχουν επιλέξει οι χρήστες που συμμετείχαν στην έρευνα.

3.1 Κωδικός PIN

Ο Προσωπικός Αριθμός Αναγνώρισης (Κωδικός PIN) είναι ένας από τους ευκολότερους και ο πιο συχνά χρησιμοποιούμενος μηχανισμός αυθεντικοποίησης. Οι χρήστες τον προτιμούν γιατί είναι εύκολος στην αρχική του ρύθμιση, εύχρηστος για καθημερινή χρήση και ταχύτατος στο ξεκλείδωμα της συσκευής. Είναι πολλές οι περιπτώσεις όπου χρησιμοποιείται μαζί με άλλους μηχανισμούς, ως ένα επιπλέον σκαλοπάτι ασφάλειας. Ο κωδικός Pin βασίζεται σε κάτι που μόνο ο εξουσιοδοτημένος χρήστης γνωρίζει και η ισχύς ασφαλείας που προσφέρει βασίζεται κυρίως στο μήκος του κώδικα. Μια μελέτη διαπίστωσε ότι οι Pin-Codes είναι ο ασφαλέστερος μηχανισμός για επιθέσεις που ονομάζονται shoulder surfing attacks [6]

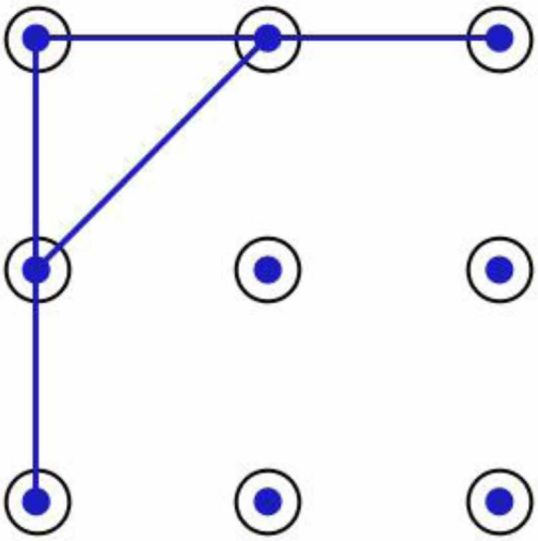
και ότι το μήκος του κώδικα έχει μεγάλη επίδραση με τους κωδικούς που απαρτίζονται από περισσότερα των τεσσάρων ψηφίων να είναι πιο ασφαλή [7]. Μπορεί ο κωδικός Pin να είναι ιδιαίτερα εύχρηστος αλλά αποτελεί έναν από τους πιο αδύναμους μηχανισμούς ασφαλείας με ένα τεράστιο αριθμό μειονεκτημάτων. Ο μηχανισμός είναι άμεσα συνδεδεμένος με το χρήστη και βασίζεται στις επιλογές του. Οι χρήστες επιλέγουν συχνά εύκολους κωδικούς, όπως η ημερομηνία γέννησης ενός μέλους της οικογένειας, ενός κοντινού προσώπου ή ακόμα χειρότερα την ημερομηνία γέννησης των ίδιων. Επιπλέον τείνουν να μοιράζονται τους κωδικούς με άλλα μέλη της οικογένειας ή συναδέλφους τους, αλλά και να γράφουν τον κωδικό τους σε χαρτάκια κολλημένα πάνω στην οθόνη ή το πληκτρολόγιό τους. Τέλος, οι χρήστες χρησιμοποιούν συχνά τον ίδιο κωδικό σε πολλούς λογαριασμούς και συσκευές και διατηρούν τον ίδιο κωδικό για μεγάλο χρονικό διάστημα, ή δεν τον αλλάζουν ποτέ.

Εικόνα 4 Κωδικός PIN

3.2 Μοτίβο

Μία εναλλακτική επιλογή των μηχανισμών που βασίζονται σε κείμενο είναι οι μέθοδοι που βασίζονται σε γραφικά σχήματα. Οι κωδικοί πρόσβασης γραφικών βασίζονται στο ότι ο ανθρώπινος εγκέφαλος μπορεί να απομνημονεύσει πολύ πιο εύκολα μια εικόνα από ένα κείμενο ή μια σειρά ψηφίων. Συγκριτικά με τους κωδικούς που βασίζονται σε κείμενο μπορούν να προσφέρουν μεγαλύτερη ασφάλεια και είναι αρκετά δύσκολο να σπάσουν από αυτοματοποιημένες επιθέσεις. Συμπερασματικά λοιπόν οι κωδικοί που βασίζονται σε γραφικά είναι πιο εύκολοι για

την ανθρώπινη μνήμη και προσφέρουν αρκετά υψηλή ασφάλεια. Σήμερα σχεδόν όλες οι συσκευές προσφέρουν το συγκεκριμένο μηχανισμό ασφαλείας και υπάρχει μεγάλο ενδιαφέρον για την βελτίωση του, λόγω της αυξημένης του χρήσης από τους χρήστες κινητών τηλεφώνων. Το μοτίβο ως μέθοδος αυθεντικοποίησης απαιτεί από τον χρήστη τον σχεδιασμό ενός μοτίβου που συνδέει μια ακολουθία σημείων. Το πιο σύνηθες είναι το μοτίβο που αποτελείται από 9 σημεία και ακολουθούν αυτά με 12 και 16 σημεία αντίστοιχα. Το σημαντικότερο μειονέκτημα τις συγκεκριμένης μεθόδου είναι η αδυναμία, που έχουν όλες οι μέθοδοι που βασίζονται σε γραφικά, να προφυλάξουν από επιθέσεις shoulder surfing.



Εικόνα 5 Μέθοδος Μοτίβου

3.3 Σαρωτής Δακτυλικού Αποτυπώματος

Οι δύο προηγούμενες μέθοδοι ανήκαν στην κατηγορία όπου ο χρήστης γνωρίζει κάτι και για να επιτραπεί η πρόσβαση στην κινητή συσκευή, ο χρήστης θα πρέπει να απομνημονεύσει είτε μια ακολουθία ψηφίων είτε ένα μοτίβο μιας εικόνας. Οι βιομετρικοί μηχανισμοί αυθεντικοποίησης απαιτούν ένα φυσικό χαρακτηριστικό του χρήστη προκειμένου να τον πιστοποιήσουν και να επιτρέψουν την είσοδό του στη συσκευή. Μπορεί επίσης να γίνει ένας συνδυασμός από χαρακτηριστικά κάτι το

οποίο θα συντελέσει στην αύξηση του επιπέδου της ασφάλειας. Η πρώτη βιομετρική μέθοδος που θα εξεταστεί είναι ο σαρωτής δακτυλικού αποτυπώματος. Το βιομετρικό σύστημα λειτουργεί εκτελώντας μια σύγκριση του δακτυλικού αποτυπώματος του χρήστη με ένα αποθηκευμένο δείγμα που έχει προκύψει από την αρχική ρύθμιση του μηχανισμού. Στην περίπτωση που αυτά τα δύο ταιριάζουν τότε ο χρήστης έχει πιστοποιηθεί επιτυχώς και αποκτά πρόσβαση στην συσκευή. Η αρχική ρύθμιση του συστήματος είναι αρκετά εύκολη και γρήγορη. Ο μηχανισμός ζητάει από το χρήστη δείγματα από το αποτύπωμά του και του δίνει τη δυνατότητα να αποθηκεύσει περισσότερα από ένα δάχτυλα για μεγαλύτερη διευκόλυνση. Η συγκεκριμένη μέθοδος αυθεντικοποίησης μπορεί να προσφέρει περισσότερη ασφάλεια από τις μεθόδους που προαναφέρθηκαν, αλλά δεν είναι τέλεια, καθώς συνοδεύεται από αρκετά μειονεκτήματα. Το πρώτο αρνητικό της στοιχείο συνδέεται με το απαιτούμενο hardware. Το hardware μπορεί να είναι ακριβό, να μην είναι τοποθετημένο σε σωστό για το χρήστη σημείο, ώστε να το βρίσκει βολικό στη χρήση ή ακόμα και να αποτελεί υλοποίηση παλιότερης τεχνολογίας που θα το καθιστά αρκετά αργό στο ξεκλείδωμα της συσκευής. Από άποψη ασφάλειας, το κύριο ζήτημα είναι ότι αυτός ο μηχανισμός βασίζεται μόνο σε εικόνες και μπορεί να παραπλανηθεί από μια πλαστή εικόνα που έχει δημιουργήσει ένας κακόβουλος χρήστης ή λογισμικό. Επιπλέον, το σύστημα όπως είναι αναμενόμενο, δεν μπορεί να πραγματοποιήσει αναγνώριση ενός χρήστη που φοράει γάντια ή ακόμα και ενός χρήστη με βρεγμένα χέρια. Η νεότερη προσθήκη στις βιομετρικές μεθόδους και αρκετά παρόμοια με το δακτυλικό αποτύπωμα είναι το υπερηχητικό δακτυλικό αποτύπωμα. Θεωρείται ότι είναι πιο ασφαλές σε σύγκριση με έναν απλό αισθητήρα δακτυλικών αποτυπωμάτων, λόγω του ότι δεν λαμβάνει υπόψη μόνο τις εικόνες του δαχτυλικού αποτυπώματος, αλλά όμως λόγω του ότι είναι παρόμοιες τεχνολογίες, συνοδεύεται με τα περισσότερα μειονεκτήματα του απλού αισθητήρα δακτυλικών αποτυπωμάτων [8,9].

3.4 Αναγνώριση Προσώπου

Η αναγνώριση προσώπου είναι μια βιομετρική μέθοδος για πιστοποίηση ταυτότητας και έχει χρησιμοποιηθεί ευρέως σε πολλούς τομείς, όπως ο στρατός, η οικονομία και η δημόσια ασφάλεια [10]. Σήμερα η αναγνώριση προσώπου είναι μια από τις αγαπημένες και ευρύτερα αποδεκτές μεθόδους από χρήστες κινητών συσκευών για την ασφάλεια των συσκευών τους. Η κύρια ιδέα πίσω από το πώς λειτουργεί αυτός ο μηχανισμός είναι αρκετά παρόμοια με τον έλεγχο δακτυλικών αποτυπωμάτων. Κατά τη διάρκεια της αναγνώρισης προσώπου, η συσκευή προσπαθεί να κάνει μια θετική ταυτοποίηση του προσώπου του χρήστη έναντι ενός προϋπάρχοντος δείγματος που ορίστηκε από τον χρήστη εγγράφηκε κατά την αρχική ρύθμιση της μεθόδου αναγνώρισης προσώπου. Καθώς το ανθρώπινο πρόσωπο αποτελεί ένα δυναμικό αντικείμενο με υψηλό βαθμό μεταβλητότητας στην εμφάνισή του, καθιστά την ανίχνευση προσώπου ένα δύσκολο πρόβλημα με τα δύο βασικότερα ζητήματα να είναι η ακρίβεια και η ταχύτητα αναγνώρισης [11]. Ένα ακόμα μειονέκτημα είναι ότι

η μπροστινή κάμερα της συσκευής παίζει σημαντικό ρόλο στην όλη διαδικασία και όσον αφορά το κύριο ζήτημα ασφάλειας είναι το ίδιο πρόβλημα που αναφέρθηκε και για τον αισθητήρα δακτυλικών αποτυπωμάτων, ότι βασίζεται δηλαδή ο μηχανισμός σε εικόνες και μπορεί να παραπλανηθεί από μια πλαστή εικόνα.

Εικόνα 6 Μέθοδος Αναγνώρισης Προσώπου

4. Έρευνες για τις μεθόδους αυθεντικοποίησης

Τα προσωπικά δεδομένα μπορεί να είναι κάθε πληροφορία που αναφέρεται σε ένα ορισμένο πρόσωπο. Διακρίνονται σε δύο κατηγορίες σε *απλά* και *ευαίσθητα*. Τα ευαίσθητα προσωπικά δεδομένα απαιτούν μεγαλύτερο επίπεδο προστασίας και έχουν αυστηρότερες προϋποθέσεις για την πρόσβαση σε αυτά και τα αρχεία ή τις συσκευές που τα εμπεριέχουν.

Πιο συγκεκριμένα ως ευαίσθητα προσωπικά δεδομένα ορίζονται τα δεδομένα που αφορούν στη φυλετική ή εθνική προέλευση, στα πολιτικά φρονήματα, στις θρησκευτικές ή φιλοσοφικές πεποιθήσεις, στην υγεία, στην κοινωνική πρόνοια και στην ερωτική ζωή κ.α. Παράδειγμα: Το ονοματεπώνυμο, η διεύθυνση ηλεκτρονικού ταχυδρομείου, η διεύθυνση πρωτοκόλλου διαδικτύου (IP address), τα στοιχεία θέασης/ διαβάσματος αρχείων, τα στοιχεία που αφορούν λήψεις / παραγγελίες αρχείων ενός ηλεκτρονικού αποθετηρίου αποτελούν προσωπικά δεδομένα. Η πληροφορία περί συμμετοχής ενός συγγραφέα σε συνδικαλιστική οργάνωση αποτελεί ευαίσθητο προσωπικό δεδομένο [18].

Το 2015, τρεις μελέτες σε χρήστες κινητών τηλεφώνων iPhone διαπίστωσαν ότι οι χρήστες δεν χρησιμοποιούν το βιομετρικό σύστημα αυθεντικοποίησης της Apple, Touch ID και προτιμούν άλλες πιο αδύναμες μεθόδους με την νούμερο ένα προτίμησή τους να είναι ο κωδικός Pin. Ένα άλλο ενδιαφέρον αποτέλεσμα είναι ότι πάνω από το 30% των συμμετεχόντων δεν ήξεραν ότι μπορούσαν να επιλέξουν ανάμεσα σε μια πληθώρα άλλων μηχανισμών ασφάλειας αντί του τυπικού Pin-Code. Σύμφωνα με τους συμμετέχοντες, ο κύριος λόγος για τον οποίο επέλεξαν να χρησιμοποιούν το PIN ήταν η μεγαλύτερη χρηστικότητα του σε σύγκριση με τους κωδικούς πρόσβασης. Οι περισσότεροι από τους συμμετέχοντες συμφώνησαν ότι όντως η βιομετρική μέθοδος της Apple προσφέρει πράγματι ορισμένα οφέλη όπως η ταχύτητα και η ευκολία χρήσης. Τέλος, ένα ενδιαφέρον συμπέρασμα, είναι ότι οι περισσότεροι χρήστες δεν μπορούσαν να εκτιμήσουν σωστά το επίπεδο ασφάλειας που προσφέρουν οι κωδικοί πρόσβασης [12].

Μια άλλη μελέτη [13] έδειξε ότι σχεδόν κάθε συμμετέχων σώζει προσωπικά δεδομένα και 13% από αυτούς αποθηκεύουν ακόμη και κωδικούς πρόσβασης ή PIN στις κινητές συσκευές τους. Οι συμμετέχοντες ρωτήθηκαν εάν χρησιμοποιούν κάποια μέθοδο ασφαλείας κατά τη χρήση του τηλεφώνου όσο αυτό είναι ενεργοποιημένο και σε κατάσταση αναμονής. Μόνο το 13% προστατεύονταν από PIN ή οπτικό κώδικα. Οι συμμετέχοντες ρωτήθηκαν επίσης για πιο λόγο έχουν επιλέξει να έχουν χαμηλό επίπεδο ασφάλειας ή και καθόλου και το 40% απάντησαν ότι το επέλεξαν επειδή είναι πιο γρήγορη η πρόσβαση τους στο τηλέφωνο ενώ το 34% απάντησε πως δεν σκέφτηκε καν ότι θα έπρεπε να ασφαλίσει την συσκευή. Ένα 17% δήλωσε ότι το τηλέφωνό τους δεν υποστηρίζει κάποια μέθοδο αυθεντικοποίησης όσο η συσκευή τους είναι ενεργοποιημένη και σε κατάσταση αναμονής, ενώ ένα 3% δήλωσε ότι είναι πολύ δύσκολο να απομνημονεύσει έναν κωδικό PIN.

Μια έρευνα [14] 297 χρηστών κινητών τηλεφώνων αποκάλυψε ότι η πλειονότητα των ερωτηθέντων οι οποίοι κάνουν σημαντική χρήση των φορητών συσκευών τους και έχουν σαφείς απαιτήσεις για την ασφάλεια και την προστασία των δεδομένων τους. Όσον αφορά τη χρήση, το 83% των συμμετεχόντων δήλωσαν ότι έχουν ενεργοποιημένο και χρησιμοποιούν το κινητό τους για περισσότερες από 10 ώρες την ημέρα. Το 66% των ερωτηθέντων ανέφεραν ότι χρησιμοποιούν PIN κατά την ενεργοποίηση της συσκευής με το 18% να χρησιμοποιεί επίσης το τον κωδικό PIN ως μηχανισμό κλειδώματος της οθόνης όσο η συσκευή βρίσκεται σε κατάσταση αναμονής. Περίπου το ένα τρίτο των χρηστών θεωρούν ότι δεν είναι καθόλου χρηστικό το PIN ως μέθοδος αυθεντικοποίησης και το 25% ανέφερε ότι αισθάνονται σίγουροι και ασφαλείς με το επίπεδο ασφάλειας που παρέχεται από τον κωδικό PIN. Επιπλέον, κάποια άλλα στατιστικά στοιχεία δείχνουν ότι το 45% των ερωτηθέντων δεν έχουν αλλάξει ποτέ τον κωδικό τους, το 42% τον έχει αλλάξει μόνο μία φορά και το υπόλοιπο 13% έχει αλλάξει τον κωδικό PIN περισσότερες από μία φορές. Τέλος, ένα αρκετά ενδιαφέρον στοιχείο είναι πως το 36% των ερωτηθέντων χρησιμοποιούν τον ίδιο κωδικό για πολλές συσκευές και το 26% των συμμετεχόντων έχουν μοιραστεί τον κωδικό τους με κάποιον άλλο.

Το 2017, μια μελέτη [7] διαπίστωσε ότι είναι πολύ πιο εύκολο για τους ανθρώπους να απομνημονεύσουν ένα μοτίβο παρά έναν κωδικό πρόσβασης. Οι ερευνητές χρησιμοποίησαν 1173 εθελοντές για να ενεργήσουν ως επιτιθέμενοι, κάνοντας επιθέσεις ove the shoulder. Χρησιμοποιήθηκαν δύο συσκευές, το Nexus 5 με οθόνη 5 ιντσών και το OnePlus One με οθόνη 6 ιντσών. Αυτά τα δύο τηλέφωνα επιλέχθηκαν αφού σύμφωνα με τους ερευνητές έχουν παρόμοιο μέγεθος και εμφάνιση με τα πιο δημοφιλή σήμερα στην αγορά Android και iPhone. Η μελέτη ανακάλυψε ότι οι κωδικοί Pin είναι ο πιο ασφαλής μηχανισμός για επιθέσεις over the shoulder, το μήκος του κώδικα έχει μεγάλη επίδραση με τους κωδικούς που αποτελούνται από περισσότερα ψηφία να είναι πιο ασφαλείς, και τέλος οι πολλαπλές προβολές του μηχανισμού αυθεντικοποίησης βελτιώνουν την απόδοση του εισβολέα. Τα μοτίβα τεσσάρων σημείων με ορατές γραμμές είναι η ευκολότερη τεχνική για απομνημόνευση και, ως εκ τούτου, ο λιγότερος ασφαλής μηχανισμός για το κλείδωμα της συσκευής. Μια ανακεφαλαίωση των πειραμάτων που πραγματοποίησαν είναι:

- Το 10,8% των εξαψήφιων κωδικών έσπασαν μετά από μια παρατήρηση
- Το 26,5% των εξαψήφιων κωδικών έσπασαν μετά από δύο παρατηρήσεις
- Το 64,2% των μοτίβων έξι σημείων με γραμμές ανίχνευσης έσπασαν μετά από δύο παρατηρήσεις
- Το 79,9% των μοτίβων έξι σημείων με γραμμές ανίχνευσης έσπασαν μετά από δύο παρατηρήσεις

- Το 35,3% των μοτίβων έξι σημείων χωρίς γραμμές ανίχνευσης έσπασαν μετά από δύο παρατηρήσεις
- Το 52,1% των μοτίβων έξι σημείων χωρίς γραμμές ανίχνευσης έσπασαν μετά από δύο παρατηρήσεις

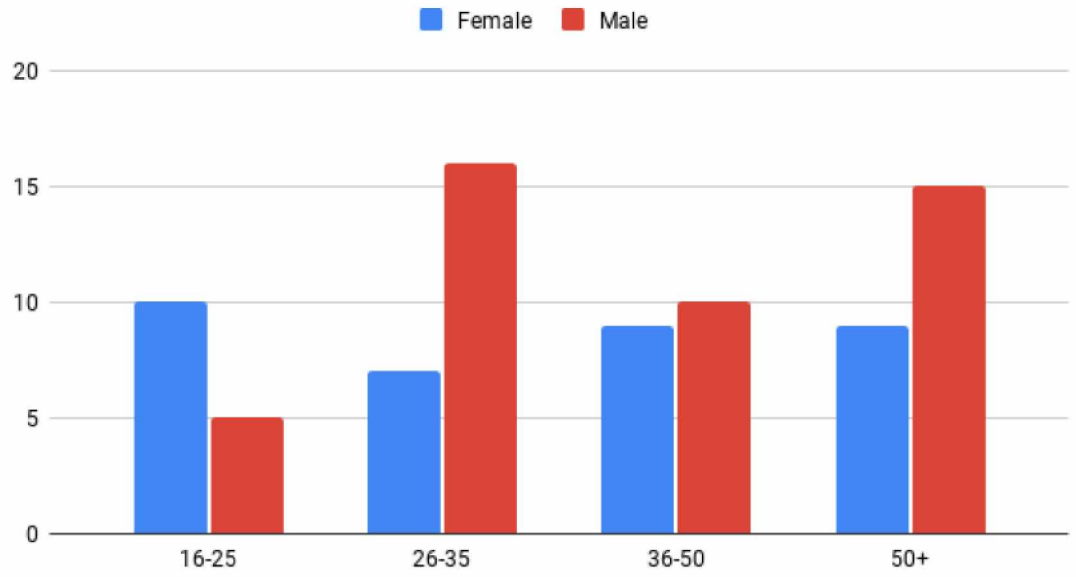
Μια μελέτη από το Πανεπιστήμιο του Λάνκαστερ [33] διαπίστωσε ότι ένας αλγόριθμος οπτικής παρακολούθησης μπορεί να παρακολουθεί τις κινήσεις των δακτυλικών αποτυπωμάτων χρησιμοποιώντας μια βιντεοσκόπηση από κάμερα κινητού τηλεφώνου. Χρησιμοποιώντας γεωμετρία πληροφοριών που εξήχθησαν από τις κινήσεις που παρακολουθούνταν, μπόρεσαν να εντοπίσουν έναν μικρό αριθμό υποψήφιων μοτίβων που θα μπορούσαν να δοκιμαστούν. Συλλέχθηκαν 120 μοναδικά μοτίβα από 215 ανεξάρτητους χρήστες και τα πειράματα αποκάλυψαν ότι με την προσέγγισή τους το 95% των μοτίβων θα μπορούσε να ξεκλειδώσει τη συσκευή σε πέντε προσπάθειες, γιατί η συσκευή κλειδώνεται αυτόματα από το λειτουργικό σύστημα. Επιπλέον, ανακάλυψαν ότι, σε αντίθεση με την πεποίθηση πολλών ανθρώπων, τα περίπλοκα μοτίβα δεν προσφέρουν ισχυρότερη προστασία. Κατάφεραν να σπάσουν όλα, εκτός από ένα αρκετά πολύπλοκο μοτίβο, με ποσοστό επιτυχίας 97,5%, όπως έκαναν και με τα απλά μοτίβα με μόλις μία προσπάθεια.

Μια νέα μελέτη [34] ανέφερε μια ποιοτική έρευνα μεταξύ των χρηστών κινητών συσκευών που είναι ειδικοί σε θέματα ασφάλειας και μη ειδικών σχετικά με την υιοθέτηση βιομετρικών μεθόδων αυθεντικοποίησης. Οι εμπειρογνώμονες ασφαλείας υιοθέτησαν πιο εύκολα βιομετρικά από τους μη ειδικούς. Επιπλέον, οι εμπειρογνώμονες ασφαλείας δεν έδειξαν υψηλή αποδοχή στη χρήση βιομετρικών τεχνικών για ευαίσθητες συναλλαγές, λόγω του φόβου για κλοπή της βιομετρικής υπογραφής τους και επίσης, σε ορισμένες περιπτώσεις έδειξαν να μην εμπιστεύονται τις νεότερες μεθόδους όπως για παράδειγμα το μηχανισμό αναγνώρισης προσώπου. Και οι δύο ομάδες είχαν τις ίδιες πιθανότητες στο να σταματήσουν να χρησιμοποιούν βιομετρικές μεθόδους κυρίως λόγω της χρηστικότητάς τους.

Μια άλλη μελέτη [35] ανέφερε ότι η ανθρώπινη κακή συμπεριφορά σε θέματα ασφάλειας μπορεί να προκαλέσει παραβίαση του. Η μελέτη διερεύνησε την πρόθεση του χρήστη να χρησιμοποιήσει βιομετρικά χαρακτηριστικά ως κύρια μέθοδο αυθεντικοποίησης. Στην έρευνα συμμετείχαν 74 χρήστες κινητών τηλεφώνων. Τα αποτελέσματα αποκάλυψαν ότι η ευκολία στη χρήση είναι από τα βασικότερα στοιχεία που συμβάλουν στη πρόθεση να χρησιμοποιήσει κάποιος βιομετρικές μεθόδους ως μηχανισμό ελέγχου ταυτότητας. Επιπλέον, τα αποτελέσματα δείχνουν ότι από το πόσο εύκολα ως μέθοδο ξεκλειδώματος γίνεται αντιληπτή από τον χρήστη, συμβάλει στο να τη δοκιμάσει για πρώτη φορά και να συνεχίσει να τη χρησιμοποιεί.

5. Αποτελέσματα της Έρευνας

Ογδόντα ένας χρήστες κινητών τηλεφώνων συμμετείχαν στην διαδικτυακή έρευνα. Η έρευνα ήταν στην ελληνική γλώσσα χωρίς γεωγραφικούς περιορισμούς ανά τη χώρα. Στον πίνακα 1 φαίνεται η κατανομή ανά ηλικία και φύλο. Ακολουθεί περιγραφή των κυριότερων αποτελεσμάτων της έρευνας. Η πλειοψηφία των ερωτηθέντων ήταν άνω των 50 ετών και αντιπροσωπεύει το μεγαλύτερο ηλικιακό group των ερωτηθέντων με ποσοστό 29,62%. Υπάρχει μια σημαντική διαφορά μεταξύ του αριθμού ανδρών και γυναικών στο διάστημα ηλικίας 26 και 35 ετών. Όπως μπορεί να παρατηρηθεί, η πλειονότητα των ερωτηθέντων είναι άνδρες, που αντιπροσωπεύουν το 55% και το 35% αυτών ανήκουν στην ηλικιακή ομάδα 26 έως 35 ετών. Ένα από τα πρώτο σημαντικά στοιχεία που παρατηρήθηκε από τις απαντήσεις του ερωτηματολογίου είναι πως πάνω από το 90% των συμμετεχόντων χρησιμοποιεί πλέον smartphone και όχι κινητό τηλέφωνο απλής χρήσης. Αυτό είναι ένα αποτέλεσμα που αναμέναμε εφόσον τα τελευταία πέντε χρόνια πωλούνται πάνω από 1,4 δισεκατομμύρια smartphone κάθε χρόνο [15].



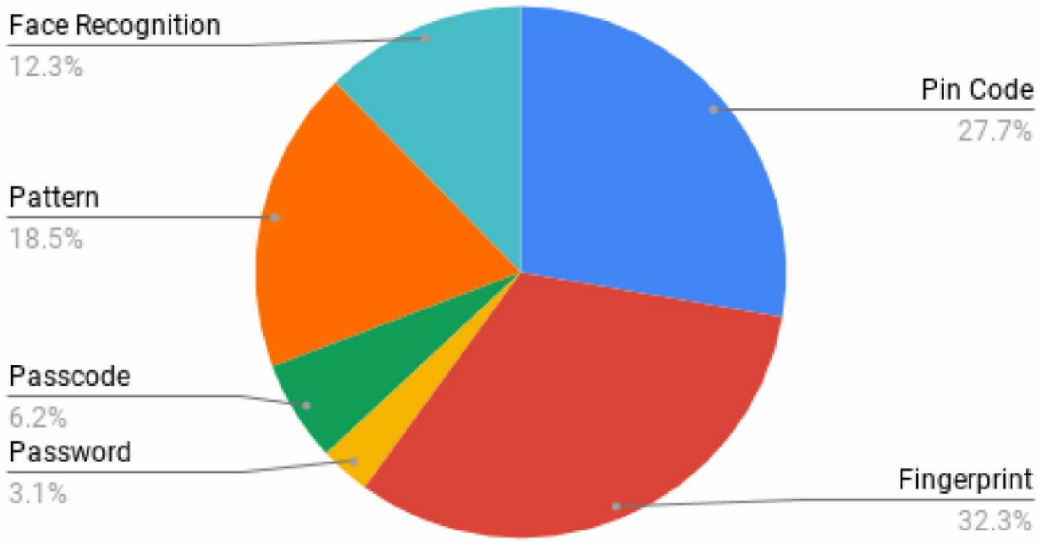
Εικόνα 7 Ηλικιακά Group

Οι συμμετέχοντες ρωτήθηκαν εάν υπάρχουν αποθηκευμένα ευαίσθητα δεδομένα τις κινητές συσκευές τους. Τα αποτελέσματα φαίνονται στον πίνακα 2. Η πλειοψηφία ανδρών συμμετεχόντων (70%) φαίνεται να έχει καλύτερη κατανόηση για το τι είναι τα ευαίσθητα δεδομένα. Επιπλέον, όσον αφορά τις ηλικιακές ομάδες με τον τρόπο που αντιλαμβάνονται τα ευαίσθητα δεδομένα παρατηρούμε ότι η ηλικιακή ομάδα 26

έως 35 έχει την καλύτερη αντίληψη για τα ευαίσθητα δεδομένα. Αντιθέτως, η ηλικιακή ομάδα 36-50 και ειδικά η ομάδα των 50+ φαίνεται να έχει τη λιγότερη κατανόηση για τα ευαίσθητα δεδομένα.

Σε μια ερώτηση οι συμμετέχοντες ρωτήθηκαν εάν τα δεδομένα που είναι αποθηκευμένα στα κινητά τους τηλέφωνα είναι ασφαλή και προστατευμένα. Τα αποτελέσματα δείχνουν ότι το 58% όλων των συμμετεχόντων δεν πιστεύουν ότι τα δεδομένα που βρίσκονται αποθηκευμένα στις συσκευές τους είναι επαρκώς προστατευμένα. Ένα ακόμα ενδιαφέρον αποτέλεσμα που εξήχθη από την έρευνα και αφορούσε την προηγούμενη ερώτηση, είναι πως μόνο το 60% των ερωτηθέντων που πιστεύουν πως έχουν ευαίσθητα δεδομένα στα κινητά τους τηλέφωνα, απάντησαν επίσης ότι τα δεδομένα αυτά δεν είναι ασφαλή.

Όπως φαίνεται στην Εικόνα 5, σύμφωνα με την έρευνα, περίπου το 32% των ερωτηθέντων έχει επιλέξει ως κύρια μέθοδο αυθεντικοποίησης το δακτυλικό αποτύπωμα ενώ ακολουθεί στη δεύτερη θέση ο κωδικός Pin (ένας τετραψήφιος κωδικός). Στη συνέχεια εμφανίζεται το μοτίβο με 18% και η αναγνώριση προσώπου με 12%. Συνολικά, σχεδόν το 45% των συμμετεχόντων χρησιμοποιεί βιομετρικές μεθόδους ως μηχανισμούς ελέγχου ταυτότητας και ασφάλειας, κάτι το οποίο είναι ενθαρρυντικό για νέες μελέτες και τη δημιουργία άλλων τρόπων ελέγχου ταυτότητας με βιομετρικά στοιχεία, όπως ο καρδιακός ρυθμός [16].



Εικόνα 8 Προτιμήσεις Μεθόδων Αυθεντικοποίησης

Επιπλέον, περίπου το 71% απάντησε πως θα δοκίμαζε ευχαρίστως νέους τρόπους αυθεντικοποίησης για κινητές συσκευές, με την προϋπόθεση ότι θα μπορούν να

παρέχουν ένα πιο ασφαλές και αξιόπιστο περιβάλλον μειώνοντας την πιθανότητα να παραβιαστούν οι συσκευές από κακόβουλο λογισμικό και επιθέσεις. Υπάρχουν μελέτες που προτείνουν νέα συστήματα, όπως για παράδειγμα το σύστημα ελέγχου ταυτότητας καρδιακού παλμού που αναφέρθηκε πιο πάνω, ή μία άλλη ευρέως γνωστή πλέον μέθοδος που αποτρέπει γνωστές αυτοματοποιημένες επιθέσεις, το ReCaptcha ή και συστήματα τα οποία επιχειρούν συνεχής ελέγχους ταυτότητας [17].

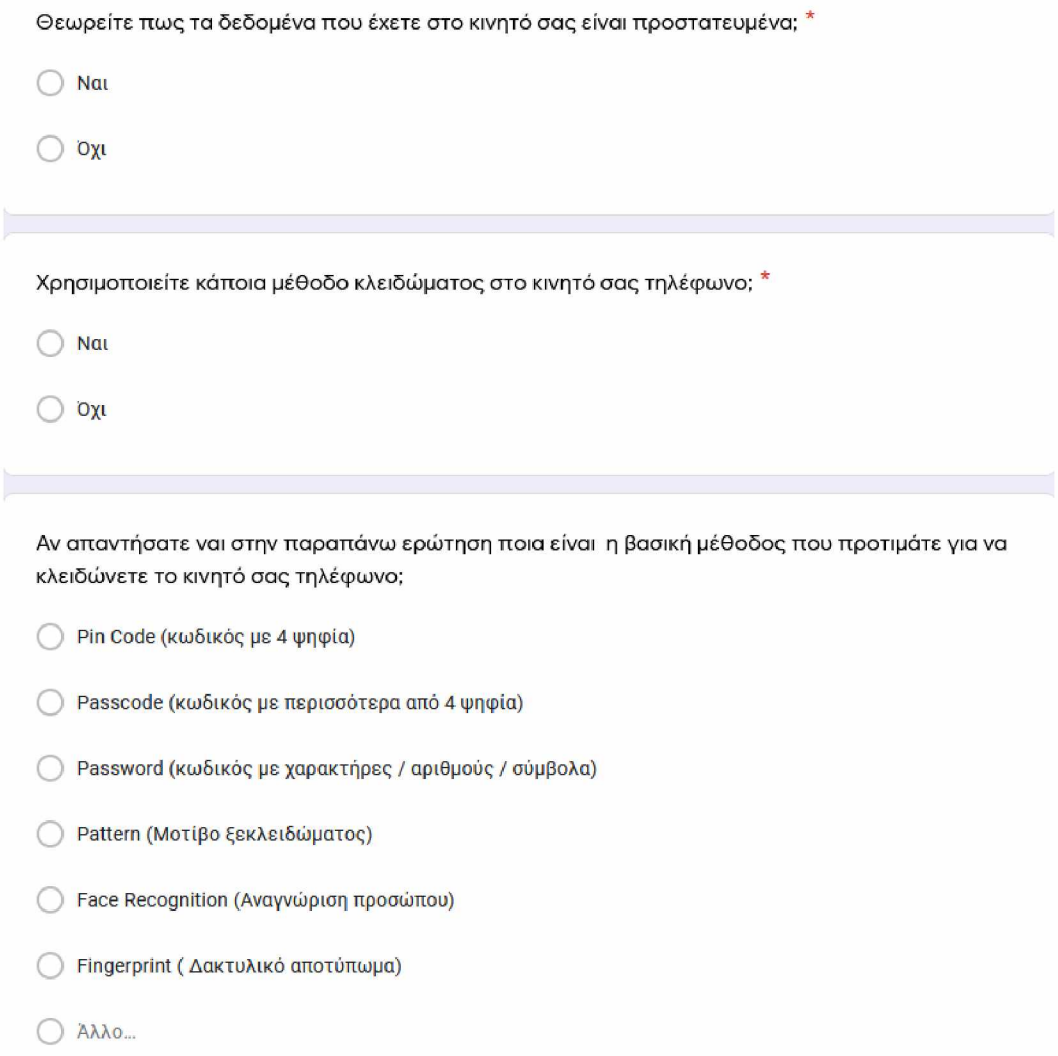
Ο Πίνακας 1 δείχνει ότι το 85% των ερωτηθέντων που χρησιμοποιούν το δακτυλικό αποτύπωμα ως μέθοδο ελέγχου ταυτότητας, πιστεύουν επίσης, ότι έχουν ευαίσθητα δεδομένα αποθηκευμένα στις συσκευές τους. Υπάρχει μια μικρή αύξηση στον αριθμό των συμμετεχόντων που προτιμούν τη μέθοδο αναγνώρισης προσώπου και πιστεύουν ότι έχουν ευαίσθητα δεδομένα με 87%. Ένα άλλο ενδιαφέρον αποτέλεσμα είναι ότι το 66% των χρηστών που χρησιμοποιούν Pin-Code πιστεύουν ότι έχουν ευαίσθητα δεδομένα αποθηκευμένα στα κινητά τους τηλέφωνα, παρόλα αυτά έχουν επιλέξει τη λιγότερο ασφαλή μέθοδο. Τέλος, η πλειοψηφία των ερωτηθέντων, που αντιπροσωπεύουν το 75%, οι οποίοι δεν χρησιμοποιούν καμία μέθοδο ελέγχου ταυτότητας, πιστεύουν επίσης ότι δεν έχουν ευαίσθητα δεδομένα αποθηκευμένα στις συσκευές τους.

Πίνακας 1 Σχέση Μεθόδων Αυθεντικοποίησης και ευαίσθητων δεδομένων

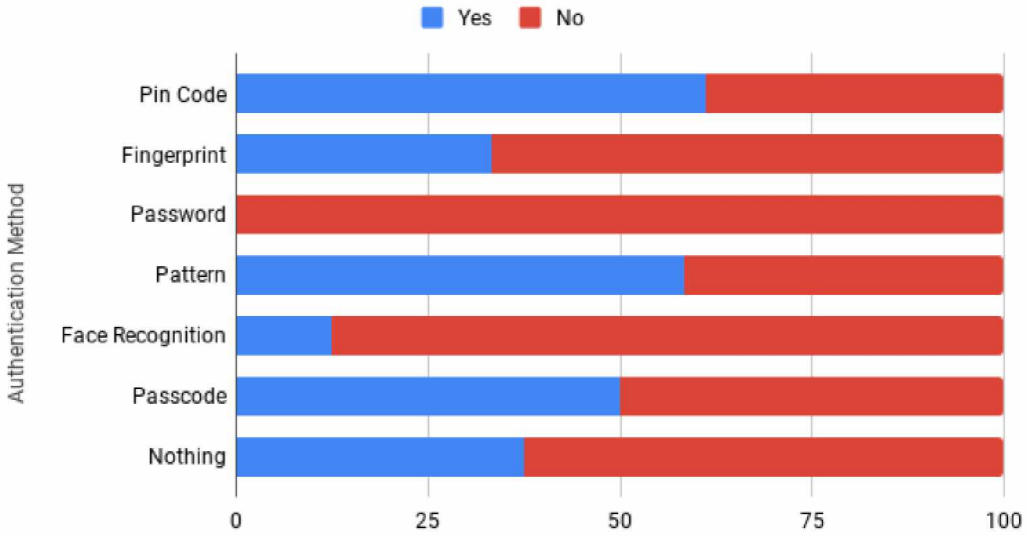
Authentication Method	Sensitive Data	
	Yes	No
Pin-Code	66.70%	33.30%
Fingerprint	85.70%	14.30%
Password	50.00%	50.00%
Pattern	66.70%	33.30%
Face Recognition	87.50%	12.50%
Pass-code	75.00%	25.00%
Nothing	25.00%	75.00%

Ένα ενδιαφέρον εύρημα είναι ότι η πλειοψηφία των συμμετεχόντων που χρησιμοποιούν τις δύο βιομετρικές μεθόδους, 66% για το δακτυλικό αποτύπωμα και 87% για την αναγνώριση προσώπου, πιστεύουν ότι τα δεδομένα τους δεν είναι καλά προστατευμένα και ασφαλή, ενώ το 61% των ερωτηθέντων που χρησιμοποιούν τον κωδικό PIN και το 58% των ερωτηθέντων που χρησιμοποιούν το μοτίβο θεωρούν ότι τα δεδομένα τους είναι ασφαλή.

Η πλειοψηφία των χρηστών, ανεξάρτητα από την προτιμώμενη μέθοδο αυθεντικοποίησης, εκτός από εκείνους που χρησιμοποιούν τον κωδικό πρόσβασης δείχνουν την προθυμία να δοκιμάσουν νέες μεθόδους ελέγχου ταυτότητας που εγγυώνται υψηλότερο επίπεδο ασφάλειας και προστασίας.



Εικόνα 9 Απόσπασμα της Online Έρευνας



Εικόνα 10 Μέθοδοι αυθεντικοποίησης και Ασφάλεια Δεδομένων

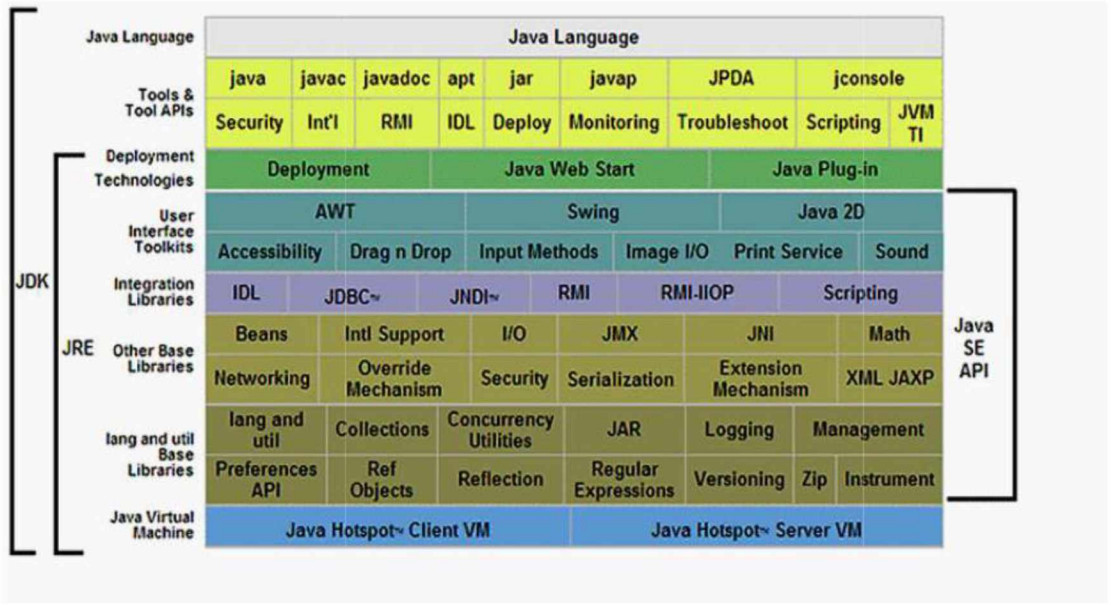
6. Το Σύστημα

6.1 Τεχνολογίες και εργαλεία για την υλοποίηση

Ακολουθεί μία σύντομη περιγραφή της γλώσσας προγραμματισμού, καθώς και του εργαλείου που χρησιμοποιήθηκε για την ανάπτυξη της εφαρμογής.

6.1.1 Java

Η Java είναι μία: απλή, αντικειμενοστραφής, υψηλής απόδοσης γλώσσα προγραμματισμού. Η Sun, ομάδα ανάπτυξης της Java, σχεδιάστηκε έτσι ώστε να είναι μια γλώσσα εύκολη στην χρήση, που δεν απαιτεί πολλή εξάσκηση και εκπαίδευση από τον προγραμματιστή. Σημαντικό πλεονέκτημα της γλώσσας είναι ότι λόγω της απλότητα της και του μικρού μεγέθους των εργαλείων της μπορεί να τρέξει σε μεγάλο πλήθος συσκευών και να χρησιμοποιηθεί και στο διαδίκτυο. Είναι μια αντικειμενοστραφής γλώσσα προγραμματισμού, δηλαδή η τεχνική σχεδιασμού ενός προγράμματος συγκεντρώνεται σε αντικείμενα. Ένα αντικείμενο αποτελεί το στιγμιότυπο μιας κλάσης. Τα αντικείμενα δεν είναι ανεξάρτητα μεταξύ τους, αλλά βρίσκονται σε σχέση αλληλεξάρτησης με τα υπόλοιπα. Υπάρχει επίσης η έννοια της κληρονομικότητας μεταξύ των αντικειμένων, δηλαδή ένα αντικείμενο μπορεί να κληρονομήσει χαρακτηριστικά και ιδιότητες από άλλα αντικείμενα. Η Java είναι γλώσσα υψηλού επιπέδου κατάλληλη για τη δημιουργία μεγάλων εφαρμογών, όπως δηλαδή και του προτεινόμενου συστήματος. Η Java έχει σχεδιαστεί για να υποστηρίζει και δικτυακές εφαρμογές. Ένα δίκτυο, όμως, μπορεί να αποτελείται από μια μεγάλη ποικιλία διαφορετικών συστημάτων, με διαφορετικούς επεξεργαστές και λειτουργικά συστήματα. Για να μπορούν οι Java εφαρμογές να εκτελούνται παντού, το πρόγραμμα Java πρέπει να περάσει από δύο διαδικασίες ώστε να καταλήξει σε εκτελέσιμη μορφή, την μεταγλώττιση και την ερμηνεία. Τα εκτελέσιμα αρχεία χωρίζονται σε δύο είδη προγραμμάτων, τα applets και τις εφαρμογές (applications). Τα applets είναι μικρά κομμάτια εκτελέσιμου κώδικα που απαιτούν έναν φυλλομετρητή για να τρέξουν. Η κύρια δουλειά τους είναι να εμπλουτίζουν τις σελίδες με αλληλεπιδραστικές εφαρμογές. Οι εφαρμογές είναι αυτόνομα προγράμματα, βρίσκονται τοπικά αποθηκευμένες και δεν απαιτούν κάποιον φυλλομετρητή για να τρέξουν. Ένα παράδειγμα εφαρμογής μπορεί να είναι ένας επεξεργαστής κειμένου, μία android εφαρμογή και φυσικά το σύστημα που δημιουργήθηκε στα πλαίσια αυτής της διπλωματικής εργασίας.



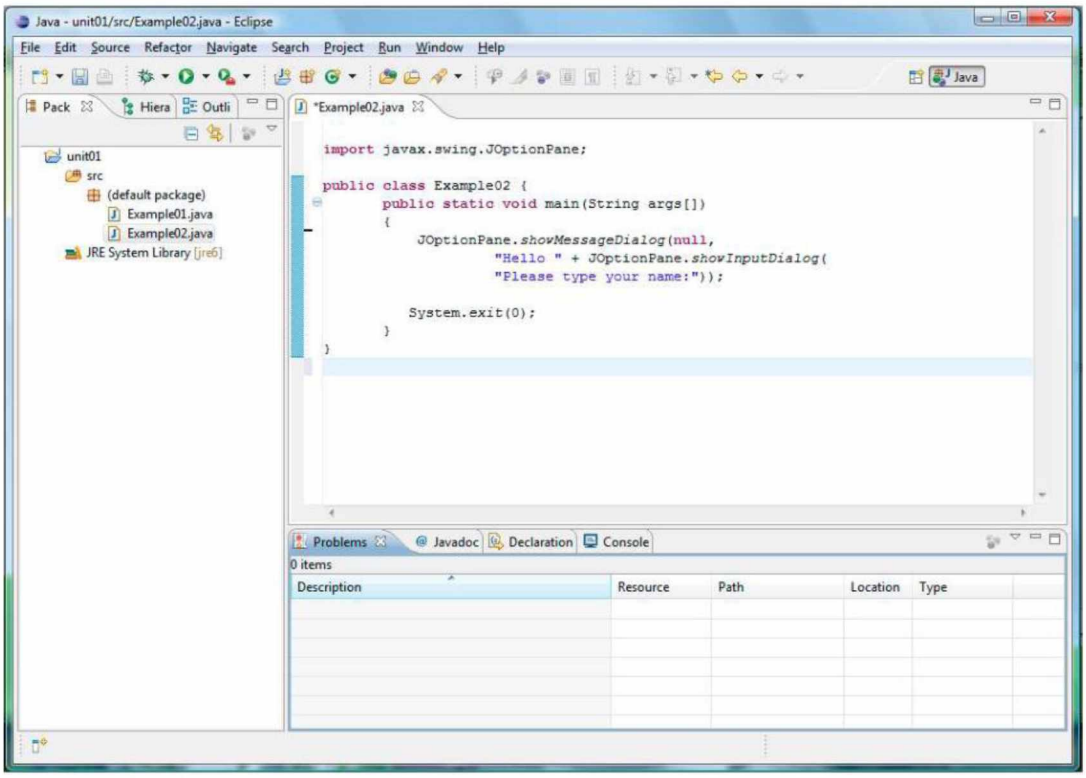
Εικόνα 11 Αρχιτεκτονική της γλώσσας Java

Για την εκτέλεση ενός προγράμματος γραμμένο σε Java σε κάποιον υπολογιστή, είναι απαραίτητη η εγκατάσταση στον υπολογιστή αυτόν και το αντίστοιχο JRE (Java Runtime για τον επεξεργαστή που διαθέτει και το λειτουργικό σύστημα που χρησιμοποιεί. Ως τα βασικότερα μέρη της αρχιτεκτονικής της γλώσσας θα μπορούσαν να οριστούν τα ακόλουθα:

- Η εικονική μηχανή (virtual machine) είναι ίσως από τα πιο σημαντικά μέρη της αρχιτεκτονικής καθώς είναι υπεύθυνη για την εκτέλεση και την μετατροπή του κώδικα σε μορφή που αντιλαμβάνεται, τόσο το λειτουργικό σύστημα όσο και ο επεξεργαστής του μηχανήματος
- Το Java SE API αποτελείται από ένα σετ κλάσεις και interfaces απαραίτητα για.να παρέχουν τη λειτουργικότητα στη γλώσσα.
- Οι Deployment Technologies είναι οι εχνολογίες που διευκολύνουν την εγκατάσταση και εκτέλεση εφαρμογών Java
- Τα Tools είναι ένα σετ από εργαλεία με τα σημαντικότερα από αυτά να είναι: Ο compiler της Java, ο διερμηνέας της Java και ο Disassembler αρχείων τύπου .class [31]

Η ανάπτυξη εφαρμογών γίνεται με τη βοήθεια εξειδικευμένων εφαρμογών που ονομάζονται Integrated Development Environments ή απλά IDEs. Ένα IDE προσφέρει έναν editor που διαχωρίζει τις λέξεις που έχουν ειδική σημασία για τη γλώσσα, προβάλλοντάς τες ξεχωριστό χρώμα και επισημαίνει τις γραμμές που του υποδεικνύει ο compiler πως υπάρχουν σφάλματα. Επίσης, αναλαμβάνουν τη διαχείριση των αρχείων όπου υπάρχει η δυνατότητα να χρησιμοποιηθούν εκτός από

τη γλώσσα και άλλα αρχεία όπως εικόνες, γραφικά και ήχος και τέλος επιτρέπουν την εργασία πάνω σε διαφορετικά projects ταυτόχρονα [32].



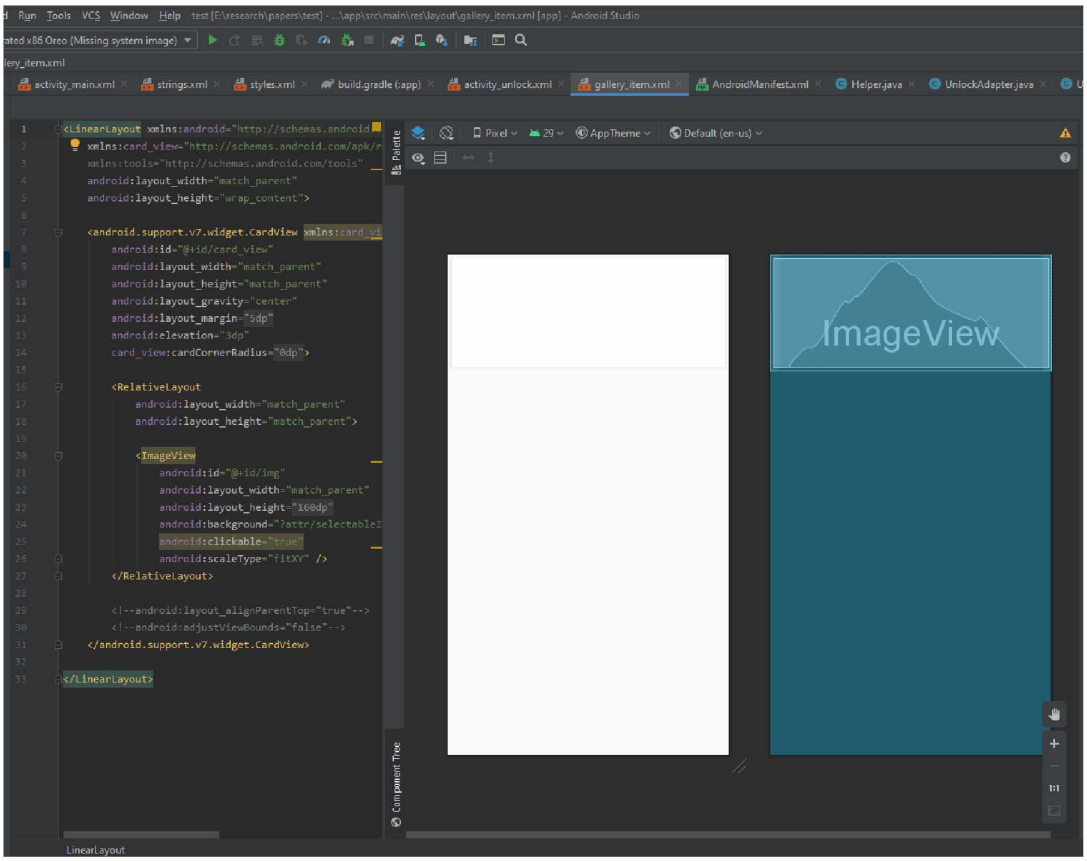
Εικόνα 12 Παράδειγμα ενός IDE

6.1.2 Android Studio

Το Android Studio είναι ένα ολοκληρωμένο προγραμματιστικό περιβάλλον (IDE) για ανάπτυξη εφαρμογών στην πλατφόρμα Android και το IDE που χρησιμοποιήθηκε στα πλαίσια της διπλωματικής. Πρώτη φορά παρουσιάστηκε στις 16 Μαΐου 2013 και από τότε είναι διαθέσιμο ελεύθερα με την άδεια Apache License 2.0.

Βασίζεται στο λογισμικό της JetBrains' IntelliJ IDEA, και έχει δημιουργηθεί αποκλειστικά για προγραμματισμό Android εφαρμογών. Είναι διαθέσιμο για όλα τα κύρια διαθέσιμα λειτουργικά συστήματα Windows, Mac OS X και Linux Κάποια από τα βασικά του συστατικά είναι τα ακόλουθα:

- Επεξεργαστής πλοήγησης για τη δημιουργία προορισμών και τη μετάβαση μεταξύ τους
- Profiler tracking για τη βελτίωση της απόδοσης της εφαρμογής
- Instant apps
- Πληροφορίες για απομάκρυνση σφαλμάτων κατά τη χρήση παρωχημένων APIs



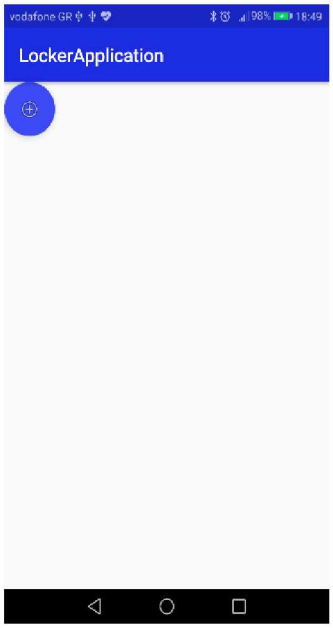
Εικόνα 13 Το περιβάλλον του Android Studio

6.1.3 Το σύστημα

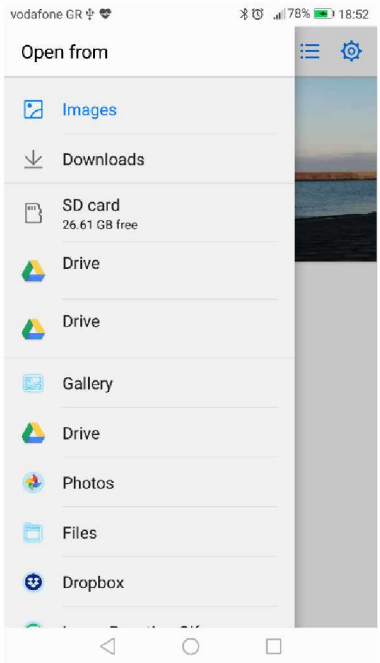
Το προτεινόμενο σύστημα είναι ένα σύστημα αναγνώρισης που βασίζεται στον χρήστη και χρησιμοποιεί μια μέθοδο παρόμοια με τα CAPTCHAs (Πλήρως αυτοματοποιημένη δοκιμή διαχωρισμού μηχανών και ανθρώπων) [37,38]. Ο χρήστης στην αρχική εγκατάσταση, πρέπει να δημιουργήσει τις επιθυμητές κατηγορίες και να τις συσχετίσει με τις εικόνες που υπάρχουν ήδη αποθηκευμένες στο κινητό του τηλέφωνο και επιθυμεί να χρησιμοποιηθούν στη διαδικασία ελέγχου ταυτότητας. Στη συνέχεια, για κάθε κατηγορία, ορισμένες εικόνες θα πρέπει να επισημαίνονται με κάποιο ειδικό tag, ώστε το σύστημα να τις αναγνωρίζει και να ξεκλειδώνει επιτυχώς την κινητή συσκευή. Έτσι, το πρώτο βασικό σημείο εδώ, είναι ότι το όριο των κατηγοριών καθορίζεται από τον χρήστη και μπορεί να αλλάξει ανά πάσα στιγμή. Ο ίδιος κανόνας ισχύει για τις εικόνες που θα χρησιμοποιηθούν στον έλεγχο ταυτότητας και σε εκείνες που έχουν τη δυνατότητα να ξεκλειδώσουν το τηλέφωνο.

Μια αρχική περίπτωση δοκιμής είναι η ακόλουθη. Ο χρήστης έχει καθορίσει μια κατηγορία με την ένδειξη "Αγαπημένα μέρη". Σε αυτήν την κατηγορία υπάρχουν

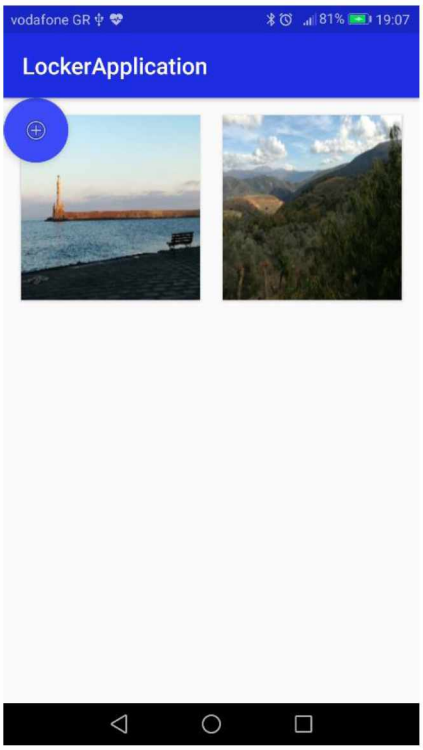
συσχετισμένες N εικόνες και P από αυτές επισημάνθηκαν ως εκείνες που μπορούν να ξεκλειδώσουν επιτυχώς την κινητή συσκευή. Αυτή η διαδικασία απεικονίζεται στις Εικόνες (11,12,13).



Εικόνα 14 Άδειος κατάλογος μίας κατηγορίας



Εικόνα 15 Επιλογή φακέλου για προσθήκη εικόνων



Εικόνα 16 Κατηγορία "Αγαπημένα μέρη" με δύο εικόνες ικανές να ξεκλειδώσουν τη συσκευή

Όπως κάθε σύστημα reCAPTCHA (για παράδειγμα Google reCAPTCHA) κάθε φορά το σύστημα θα ζητά από τον χρήστη να επιλέξει μία από τις εικόνες P μεταξύ των εικόνων N της τυχαίας επιλεγμένης κατηγορίας. Για παράδειγμα, την πρώτη φορά το σύστημα, θα μπορούσε να ζητήσει από τον χρήστη να επιλέξει μια εικόνα από την κατηγορία "Αγαπημένα μέρη", η οποία είναι μία από τις κατηγορίες X που δημιουργήθηκαν. Στη συνέχεια, ένα σχήμα πλέγματος 3x2 (17), συμπληρώνεται με τυχαίες εικόνες και ο χρήστης πρέπει να επιλέξει μόνο μία από την σωστή κατηγορία για να ξεκλειδώσει την κινητή συσκευή.

Εικόνα 17 Πλέγμα 3x2 που περιέχει φωτογραφίες από τα αγαπημένα μέρη του χρήστη

Όπως μπορεί να παρατηρηθεί, δεδομένου ότι υπάρχουν συνολικά 6 εικόνες στο πλέγμα και μία από αυτές είναι η σωστή, η πιθανότητα εύρεσης της σωστής είναι 1/6. Όμως, υπάρχει και η πιθανότητα η απάντηση να είναι λάθος στην πρώτη ερώτηση. Σε αυτήν την περίπτωση, το σύστημα θα ζητήσει πάλι από τον χρήστη να επιλέξει μια εικόνα από άλλη κατηγορία ή θα μπορούσε να ζητήσει από το χρήστη να επιλέγει συνεχώς την εικόνα που πληροί τα απαιτούμενα κριτήρια. Για παράδειγμα, θα μπορούσε να ζητήσει από τους χρήστες να επιλέγουν συνεχώς οποιαδήποτε από τις Εικόνες που σχετίζονται με τα "Αγαπημένα μέρη". Σε αυτήν την περίπτωση, το πλέγμα μετά από μια επιτυχημένη επιλογή θα πρέπει να επαναπροσδιοριστεί με νέες τυχαίες εικόνες. Από την άλλη πλευρά, εάν το αρχικό αίτημα δεν απαντήθηκε σωστά, το σύστημα μπορεί επίσης να ζητήσει από το χρήστη να επιλέξει μια εικόνα από άλλη κατηγορία.

Σε αντίθεση με τα ήδη προτεινόμενα συστήματα, όπως ο σαρωτής δακτυλικών αποτυπωμάτων, αυτό το προτεινόμενο σύστημα μπορεί να αποφύγει brute force attacks που είναι πολύ κοινά σε συστήματα αυθεντικοποίησης όπως στον κωδικό pin, καθώς μπορεί να αλλάζει συνεχώς τα αιτήματα και το εμφανιζόμενο πλέγμα.

7. Συμπεράσματα

Η ραγδαία ανάπτυξη της τεχνολογίας είχε ως αποτέλεσμα την αύξηση στην χρήση έξυπνων κινητών τηλεφώνων και ως εκ τούτου επίσης την αύξηση των αποθηκευμένων δεδομένων σε αυτές τις συσκευές. Οι πληροφορίες που αποθηκεύονται σε αυτές τις συσκευές δεν είναι πλέον μόνο η λίστα επαφών, οι φωτογραφίες κ.λπ. Πλέον αποθηκεύονται, επεξεργάζονται και αποστέλλονται μεγάλου όγκου προσωπικά και εμπορικά ευαίσθητα δεδομένα. Αυτή η έρευνα πραγματοποιήθηκε για την καλύτερη κατανόηση του τρόπου που αντιλαμβάνονται οι χρήστες τα ευαίσθητα δεδομένα και τις μεθόδους που χρησιμοποιούν για να τα προστατεύσουν.

Από την έρευνα εξήχθησαν τα ακόλουθα συμπεράσματα. Υπάρχει μια σαφής διαφορά μεταξύ του φύλου, όσον αφορά την κατανόηση ευαίσθητων δεδομένων και την ασφάλειά τους. Αυτό θα μπορούσε να είναι η βάση για νέες μελέτες και τη δημιουργία εκπαιδευτικών μαθημάτων για όλους, έτσι ώστε περισσότεροι χρήστες κινητών τηλεφώνων να μπορέσουν να κατανοήσουν τη σημαντικότητα των ευαίσθητων δεδομένων. Εκτός από το φύλο, φαίνεται πως σημαντικό ρόλο κατέχει και η ηλικιακή ομάδα, κάτι που δείχνει την αναγκαιότητα δημιουργίας εκπαιδευτικών προγραμμάτων για να βοηθήσουν άτομα μεγαλύτερης ηλικίας στη μετάβαση των εξελίξεων στην τεχνολογία.

Τέλος, οι χρήστες που έχουν επιλέξει τις βιομετρικές μεθόδους ελέγχου ταυτότητας έχουν καλύτερη κατανόηση της σημασίας των ευαίσθητων δεδομένων, δεν το πιστεύουν ότι προστατεύονται πλήρως και δείχνουν προθυμία να δοκιμάσουν νέες μεθόδους αυθεντικοποίησης.

Προσπαθήσαμε να καταλάβουμε ποια είναι η κύρια εστίαση του τελικού χρήστη και προτείνουμε ένα σύστημα που θα ανταποκρίνεται στις ανάγκες του. Το προτεινόμενο σύστημα υιοθετεί ισχυρά χαρακτηριστικά γνωστών μεθόδων και εισάγει μια τυχαιότητα των δεδομένων των χρηστών σε προκαθορισμένες κατηγορίες. Επίσης, καθώς αυτή η μέθοδος έχει τη δυνατότητα να χρησιμοποιηθεί ως ο κύριος τρόπος ξεκλειδώματος της κινητής συσκευής, οι ίδιες αρχές που ισχύουν και για το PIN ισχύουν και εδώ. Αυτό σημαίνει, ότι σε περίπτωση που ο χρήστης ξεχάσει τις εικόνες που μπορούν να ξεκλειδώσουν τη συσκευή, ο μόνος τρόπος για να επανακτήσει την πρόσβαση είναι να πραγματοποιήσετε επαναφορά εργοστασιακών ρυθμίσεων.

Επιπλέον, το σύστημα είναι σε θέση να αντιμετωπίσει επιθέσεις και γνωστά τρωτά σημεία άλλων μηχανισμών ασφαλείας, π.χ. over-the-shoulder attack. Δηλαδή, η ίδια φωτογραφία-εικόνα μπορεί να είναι επιλέξιμη σε μία κατηγορία και εσφαλμένη σε μια άλλη. Με βάση τα ευρήματα που προέκυψαν από τη δοκιμή του συστήματός μας, θα θέλαμε να βελτιώσουμε το σύστημα κάνοντάς το πιο ασφαλές χρησιμοποιώντας την τεχνολογία της Deep Learning. Ο χρήστης θα είναι σε θέση να εκπαιδεύσει τα

δικά του μοντέλα με τη συλλογή εικόνων του από ένα εύχρηστο περιβάλλον με όλα τα δεδομένα του να είναι ασφαλή στο cloud. Επιπλέον, βρίσκεται σε εξέλιξη μια αξιολόγηση της ικανοποίησης και της χρηστικότητας του από χρήστες που θέλησαν να δοκιμάσουν το σύστημα.

Βιβλιογραφία

[1] S. O'Dea. 2020. Smartphone users worldwide 2016-2021. Statista. Retrieved September 10, 2020 from https://www.statista.com/statistics/330695/number-ofsmartphone-users-worldwide/

[2] Nur Haryani Zakaria, David Griffiths, Sacha Brostoff, and Jeff Yan. 2011. Shoulder Surfing Defence for Recall-Based Graphical Passwords. In Proceedings of the Seventh Symposium on Usable Privacy and Security (Pittsburgh, Pennsylvania) (SOUPS '11). Association for Computing Machinery, New York, NY, USA, Article 6, 12 pages. https://doi.org/10.1145/2078827.2078835

[3] Ivan Cherapau, Ildar Muslukhov, Nalin Asanka, and Konstantin Beznosov. 2015. On the Impact of Touch ID on IPhone Passcodes. In Proceedings of the Eleventh USENIX Conference on Usable Privacy and Security (Ottawa, Canada) (SOUPS '15). USENIX Association, USA, 257–276.

[4] Abdullah Rashed and Nancy Alajarmeh. 2015. Towards understanding user perceptions of biometrics authentication technologies. International Journal of Computer Science and Information Security 13, 6 (2015), 25.

[5] Thamer Alhussain, Rayed AlGhamdi, Salem Alkhalaf, and Osama Alfarraj. 2013. Users" Perceptions of Mobile Phone Security: A Survey Study in the Kingdom of Saudi Arabia. international journal of computer theory and engineering 5, 5 (2013), 793.

[6] Ojaswi Kasat, Umesh Bhadade, and Ms Naimisha Trivedi. 2015. Study and analysis of shoulder-surfing methods. International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), ISSN 1 (2015), 256–261.

[7] Adam J. Aviv, John T. Davin, FlynnWolf, and Ravi Kuber. 2017. Towards Baselines for Shoulder Surfing on Mobile Authentication. In Proceedings of the 33rd Annual Computer Security Applications Conference (Orlando, FL, USA) (ACSAC 2017). Association for Computing Machinery, New York, NY, USA, 486–498. https: //doi.org/10.1145/3134600.3134609

[8] Derrick Rountree. 2013. Chapter 2 - What Is Federated Identity? In Federated Identity Primer, Derrick Rountree (Ed.). Syngress, Boston, 13 – 36. https://doi. org/10.1016/B978-0-12-407189-6.00002-9

[9] Vasileios Tsoukas, Athanasios Kakarountas, Anargyros Gkogkidis, and Georgios Giannakas. 2019. Multi-screen lock: visual passwords from user's social data. In Proceedings of the 23rd Pan-Hellenic Conference on Informatics. ACM, New York, NY, USA, 90–95.

[10] I. Masi, Y. Wu, T. Hassner, and P. Natarajan. 2018. Deep Face Recognition: A Survey. In 2018 31st SIBGRAPI Conference on Graphics, Patterns and Images (SIBGRAPI). IEEE, New York, NY, USA, 471–478.

[11] Faizan Ahmad, Aaima Najam, and Zeeshan Ahmed. 2013. Image-based Face

Detection and Recognition: "State of the Art". arXiv:1302.6379 [cs.CV]

[12] Ivan Cherapau, Ildar Muslukhov, Nalin Asanka, and Konstantin Beznosov. 2015. On the Impact of Touch ID on IPhone Passcodes. In Proceedings of the Eleventh USENIX Conference on Usable Privacy and Security (Ottawa, Canada) (SOUPS '15). USENIX Association, USA, 257–276.

[13] Frank Breitinger and Claudia Nickel. 2010. User survey on phone security and usage. In BIOSIG 2010: Biometrics and Electronic Signatures. Proceedings of the Special Interest Group on Biometrics and Electronic Signatures, Arslan Brömme and Christoph Busch (Eds.). Gesellschaft für Informatik e.V., Bonn, 139–144.

[14] Nathan L Clarke and Steven M Furnell. 2005. Authentication of users on mobile telephones–A survey of attitudes and practices. Computers & Security 24, 7 (2005), 519–527.

[15] S. O'Dea. 2020. Smartphone users worldwide 2016-2021. Statista. Retrieved September 20, 2020 from https://www.statista.com/statistics/263437/global-smartphonesales-to-end-users-since-2007/

[16] Lei Wang, Kang Huang, Ke Sun, Wei Wang, Chen Tian, Lei Xie, and Qing Gu. 2018. Unlock with Your Heart: Heartbeat-Based Authentication on Commercial Mobile Phones. Proc. ACM Interact. Mob.Wearable Ubiquitous Technol. 2, 3, Article 140 (Sept. 2018), 22 pages. https://doi.org/10.1145/3264950

[17] V. M. Patel, R. Chellappa, D. Chandra, and B. Barbello. 2016. Continuous User Authentication on Mobile Devices: Recent progress and remaining challenges. IEEE Signal Processing Magazine 33, 4 (2016), 49–61.

[18] Τι είναι προσωπικά δεδομένα και τι ευαίσθητα προσωπικά δεδομένα;. Heal-link. Retrieved March 20, 2021. https://legal.heal-link.gr/index.php/sensitive-personal-data

[19] James Michael Stewart. The Three Types of Multi-Factor Authentication(MFA) . Global Knowledge. Retrieved March 20, 2021. https://www.globalknowledge.com/us-en/resources/resource-library/articles/the-three-types-of-multi-factor-authentication-mfa/

[20] Enterprise Mobile Security. Zimperium. Retrieved March 20, 2021. https://www.zimperium.com/enterprise-mobile-security

[21] How much would a data breach cost your business? Retrieved March 20, 2021. https://www.ibm.com/security/data-breach

[22] 2020 Data Breach Investigations Report. Verizon. Retrieved March 20, 2021.

https://enterprise.verizon.com/resources/reports/dbir/

[23] Email Threat Report. FireEye. Retrieved March 20, 2021.

https://www.fireeye.com/offers/rpt-email-threat-report.html

[24] JR Raphael. 8 mobile security threats you should take seriously. Retrieved March 20, 2021. https://www.csoonline.com/article/3241727/8-mobile-security-threats-you-should-take-seriously.html

[25] Mickey Boodaei. Mobile Users 3 Times More Vulnerable to Phishing Attacks. Security Intelligence. Retrieved March 20, 2021. https://securityintelligence.com/mobile-users-3-times-more-vulnerable-to-phishing-attacks/

[26] New research: How effective is basic account hygiene at preventing hijacking. Google. Retrieved March 20, 2021. https://security.googleblog.com/2019/05/new-research-how-effective-is-basic.html

[27] Online Security Survey. Google / Harris Poll. Retrieved March 20, 2021. https://services.google.com/fh/files/blogs/google_security_infographic.pdf

[28] The 2018 Global Password Security Report. Lastpass. Retrieved March 20, 2021. https://lp-cdn.lastpass.com/lporcamedia/document-library/lastpass/pdf/en/IAM_LastPass_SOTP_ebook.pdf

[29] 2017 Verizon Data Breach Investigations Report (DBIR) from the Perspective of Exterior Security Perimeter. Verizon. Retrieved March 20, 2021. https://www.verizondigitalmedia.com/blog/2017-verizon-data-breach-investigations-report/

[30] How Much Is the Data on Your Mobile Device Worth?. Ponemon. Retrieved March 20, 2021. https://www.ponemon.org/local/upload/file/How%20much%20is%20the%20data%20on%20your%20mobile%20device%20worth%20Final%2010.pdf

[31] Java. Retrieved March 20, 2021. http://www.islab.demokritos.gr/gr/html/ptixiakes/kostas-aris_ptyxiakh/Phtml/java.htm

[32] Εισαγωγή στη Γλώσσα Προγραμματισμού Java. Retrieved March 20, 2021. https://people.iee.ihu.gr/~sfetsos/java_book_EMP.pdf

[33] Guixin Ye, Zhanyong Tang, Dingyi Fang, Xiaojiang Chen, Kwang In Kim, BenTaylor, and Zheng Wang. 2017. Cracking Android pattern lock in five attempts.(2017).

[34] Flynn Wolf, Ravi Kuber, and Adam J Aviv. 2019. Pretty Close to a Must-Have:Balancing Usability Desire and Security Concern in Biometric Adoption. InProceedings of the 2019 CHI Conference on Human Factors in Computing Systems.

[35] Abdullah Rashed and Nancy Alajarmeh. 2015. Towards understanding userperceptions of biometrics authentication technologies. International Journal ofComputer Science and Information Security13, 6 (2015), 25

[37] Liming Wang, Xiuling Chang, Zhongjie Ren, Haichang Gao, Xiyang Liu, and UweAickelin. 2010. Against spyware using CAPTCHA in graphical password scheme.In2010 24th IEEE International Conference on Advanced Information Networkingand Applications. IEEE, 760–767.

[38] Bin B Zhu, Jeff Yan, Guanbo Bao, Maowei Yang, and Ning Xu. 2014. CAPTCHAas graphical passwords—a new security primitive based on hard AI problems.IEEE transactions on information forensics and security9, 6 (2014), 891–904.

Πηγές Εικόνων

Εικόνα 18 Αριθμός χρηστών smartphones παγκοσμίως από το 2016 εως το 2023

https://www.statista.com/statistics/330695/number-ofsmartphone-users-worldwide/

Εικόνα 19 Επίθεση Man in the Middle

https://nowmag.gr/wpcontent/uploads/2019/09/mn.jpg

Εικόνα 20 Ενημέρωση Ασφάλειας σε σύστημα Android

https://futuredrafted.com/android-update-becomes-very-beautiful-inside-540122be5c63

Εικόνα 4 Κωδικός PIN

https://www.freeimages.com/photo/security-1238201

Εικόνα 5 Μέθοδος Μοτίβου

https://hashtagsandkeywords.com/5-most-difficult-pattern-lock-ideas-for-android/

Εικόνα 6 Μέθοδος Αναγνώρισης Προσώπου

https://medium.com/advancing-justice-aajc/facial-recognition-technology-the-need-for-robust-civil-rights-protections-790f26d5a1b9

Εικόνα 11 Αρχιτεκτονική της γλώσσας Java

http://www.islab.demokritos.gr/gr/html/ptixiakes/kostas-aris_ptyxiakh/Phtml/java.htm

Εικόνα 12 Παράδειγμα ενός IDE

https://people.iee.ihu.gr/~sfetsos/java_book_EMP.pdf

Εργαλεία που χρησιμοποιήθηκαν

Android Studio