ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΜΑΚΕΔΟΝΙΑΣ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Μελέτη του πλαισίου VAPT (Vulnerability Assessment and Penetration Testing) για την ενίσχυση της ασφάλειας των κινητών πλατφορμών και εφαρμογών Android και iOS

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

του

ΜΙΧΑΗΛ ΤΣΙΑΜΟΥΡΗ

(ΑΕΜ: 2978)

Επιβλέπων : **Νικολάου Σπυρίδων**

Λέκτορας

Καστοριά , Ιούνιος 2024

Η παρούσα σελίδα σκοπίμως παραμένει λευκή

ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΜΑΚΕΔΟΝΙΑΣ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Μελέτη του πλαισίου VAPT (Vulnerability Assessment and Penetration Testing) για την ενίσχυση της ασφάλειας των κινητών πλατφορμών και εφαρμογών Android και iOS

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

του

ΜΙΧΑΗΛ ΤΣΙΑΜΟΥΡΗ

(ΑΕΜ: 2978)

Επιβλέπων : **Νικολάου Σπυρίδων**

Λέκτορας

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την ημερομηνία εξέτασης

.....	.....	.....
Ον/μο Μέλους	Ον/μο Μέλους	Ον/μο Μέλους
Ιδίοτητα Μέλους	Ιδίοτητα Μέλους	Ιδίοτητα Μέλους

Καστοριά, Ιούνιος 2024

Ευχαριστίες

Ευχαριστώ ιδιαιτέρως τον καθηγητή μου, κύριο Σπυρίδων Νικολάου, για την καθοδήγηση και την άψογη συνεργασία καθ' όλη την διάρκεια της εκπόνησης της πτυχιακής μου εργασίας.

Επίσης, ευχαριστώ θερμά όλους όσους με στήριξαν στο κοντινό μου περιβάλλον.

Περίληψη

Η παρούσα πτυχιακή εργασία εστιάζει στην αξιολόγηση ευπαθειών (Vulnerability Assessment) και στις δοκιμές διείσδυσης (Penetration Testing) σε κινητές πλατφόρμες Android και iOS, καθώς και στις εφαρμογές τους. Οι κύριοι στόχοι είναι η αναγνώριση, η ανάλυση και ο περιορισμός των πιθανών απειλών που αντιμετωπίζουν οι χρήστες αυτών των εφαρμογών. Η εργασία ξεκινά με την παρουσίαση των βασικών εννοιών και διαφορών μεταξύ της αξιολόγησης ευπαθειών και των δοκιμών διείσδυσης, ενώ ακολουθεί μια λεπτομερής εξέταση των πιο διαδεδομένων μεθοδολογιών στον τομέα αυτό. Μεθοδολογίες όπως η NIST-SP 800-115, το Penetration Testing Execution Standard (PTES) και το OWASP Mobile Security Testing Guide (MSTG) αναλύονται διεξοδικά, παρέχοντας κατευθύνσεις για την εφαρμογή τους στις κινητές πλατφόρμες. Επίσης, γίνεται εκτενής αναφορά στα εργαλεία που χρησιμοποιούνται για την αξιολόγηση των ευπαθειών και την εκμετάλλευση αυτών, όπως τα εργαλεία συλλογής πληροφοριών, ανάλυσης ευπαθειών και εκμετάλλευσης (exploitation tools).

Μέσα από συγκεκριμένα παραδείγματα και περιπτωσιολογικές μελέτες, αναλύονται οι συνήθεις ευπάθειες των εφαρμογών κινητής τραπεζικής (Mobile Banking Applications - MBAs), έναν τομέα που αποκτά ολοένα και μεγαλύτερη σημασία λόγω της εκτεταμένης χρήσης των κινητών συσκευών για τραπεζικές συναλλαγές. Η ασφάλεια αυτών των εφαρμογών είναι κρίσιμη, καθώς οι ευπάθειες όπως η μη ασφαλής αποθήκευση δεδομένων, οι ανεπαρκείς έλεγχοι ταυτότητας και εξουσιοδότησης, και οι ευπάθειες στα δίκτυα επικοινωνίας, μπορούν να οδηγήσουν σε σοβαρές παραβιάσεις δεδομένων και οικονομικές απώλειες. Προτείνονται πρακτικές λύσεις και μέτρα πρόληψης, όπως η κρυπτογράφηση δεδομένων, η εφαρμογή ασφαλών πολιτικών διαχείρισης κωδικών και η εκπαίδευση των χρηστών για την αναγνώριση και αποφυγή των κινδύνων.

Η ανάλυση της συγκεκριμένης μελέτης περίπτωσης καταλήγει με συμπεράσματα που υπογραμμίζουν τη σημασία της συνεχούς βελτίωσης των μέτρων ασφαλείας στις εφαρμογές κινητής τραπεζικής και προτείνει κατευθύνσεις για μελλοντική έρευνα, όπως η διερεύνηση των νέων τεχνολογιών ασφαλείας και η ενσωμάτωση τεχνικών μηχανικής μάθησης για την ανίχνευση και πρόληψη των επιθέσεων.

Λέξεις Κλειδιά : **Αξιολόγηση Ευπαθειών, Δοκιμές Διείσδυσης, Android, iOS Ασφάλεια κινητών εφαρμογών, Mobile Banking Applications, NIST-SP 800-115, PTES, OWASP MSTG, εργαλεία εκμετάλλευσης, κρυπτογράφηση δεδομένων, διαχείριση κωδικών, Kali Linux.**

Abstract

This thesis focuses on Vulnerability Assessment and Penetration Testing on Android and IOS mobile platforms and their applications. The main objectives are to identify, analyze and mitigate the potential threats faced by the users of these applications. Methodologies such as NIST-SP 800-115, the Penetration Testing Execution Standard (PTES), and the OWASP Mobile Security Testing Guide (MSTG) are thoroughly analyzed, providing guidelines for their application on mobile platforms. There is also an extensive reference to the tools used for vulnerability assessment and exploitation, including information gathering tools, vulnerability analysis tools, and exploitation tools.

Through specific examples and case studies, common vulnerabilities of Mobile Banking Applications (MBAs), a field that is gaining increasing importance due to the widespread use of mobile devices for banking transactions. The security of these applications is critical, as vulnerabilities such as insecure data storage, inadequate authentication and authorization controls, and vulnerabilities in communication networks, can lead to severe data breaches and financial losses. Practical solutions and preventive measures are proposed, such as data encryption, the implementation of secure password management policies, and user education to recognize and avoid risks.

The thesis concludes with findings that emphasize the importance of continuously improving security measures in mobile banking applications and suggests directions for future research, such as the exploration of new security technologies and the integration of machine learning techniques for the detection and prevention of attacks.

Keywords: **Vulnerability Assessment, Penetration Testing, Mobile application security, Mobile Banking Applications, NIST-SP 800-115, PTES, OWASP MSTG, exploitation tools, data encryption, password management, Kali Linux.**

Πίνακας Περιεχομένων

Λίστα Εικόνων

ΕΙΣΑΓΩΓΗ

Η τεχνολογία έχει αλλάξει ριζικά τον τρόπο με τον οποίο πραγματοποιούμε τις καθημερινές μας συναλλαγές, με τις εφαρμογές κινητής τραπεζικής (Mobile Banking Applications - MBAs) να αποτελούν πλέον ένα αναπόσπαστο κομμάτι της ζωής μας. Οι εφαρμογές αυτές προσφέρουν ευκολία και αμεσότητα στις τραπεζικές συναλλαγές, όμως η αυξανόμενη χρήση τους έχει φέρει στο προσκήνιο σοβαρά ζητήματα ασφαλείας. Η προστασία των δεδομένων των χρηστών και η εξασφάλιση της ακεραιότητας των χρηματικών συναλλαγών αποτελούν κεντρικά θέματα που απαιτούν συστηματική έρευνα και προσεκτική ανάλυση.

Σκοπός της παρούσας πτυχιακής εργασίας είναι η διερεύνηση και αξιολόγηση των ευπαθειών που ενδέχεται να εμφανίζουν οι εφαρμογές κινητής τραπεζικής, καθώς και η ανάπτυξη πρακτικών μεθόδων και εργαλείων για την ενίσχυση της ασφάλειάς τους. Με την εφαρμογή δοκιμών διείσδυσης (Penetration Testing) και αξιολόγησης ευπαθειών (Vulnerability Assessment), επιδιώκεται η αναγνώριση των τρωτών σημείων και η παροχή λύσεων για τη θωράκιση των εφαρμογών αυτών απέναντι σε πιθανές απειλές.

Η εργασία αυτή είναι δομημένη σε πέντε κύρια κεφάλαια, τα οποία καλύπτουν όλες τις πτυχές του θέματος:

Στο πρώτο κεφάλαιο παρουσιάζονται οι βασικές έννοιες της αξιολόγησης ευπαθειών και των δοκιμών διείσδυσης, ενώ αναλύονται οι διαφορές και οι ομοιότητες μεταξύ αυτών των δύο διαδικασιών. Επίσης, γίνεται μια επισκόπηση των κυριότερων μεθοδολογιών και προτύπων που χρησιμοποιούνται στον τομέα αυτό, όπως η NIST-SP 800-115, το Penetration Testing Execution Standard (PTES) και το OWASP Mobile Security Testing Guide (MSTG).

Το δεύτερο κεφάλαιο εστιάζει στα εργαλεία και τις τεχνικές που χρησιμοποιούνται για την αξιολόγηση των ευπαθειών και την εκτέλεση δοκιμών διείσδυσης. Παρουσιάζονται τα βασικά εργαλεία συλλογής πληροφοριών, ανάλυσης ευπαθειών, και εκμετάλλευσης, καθώς και τα εργαλεία αντίστροφης μηχανικής που είναι κρίσιμα για την ανάλυση των κινητών εφαρμογών.

Το τρίτο κεφάλαιο εξετάζει τις προκλήσεις ασφαλείας που σχετίζονται με τις πιο δημοφιλείς πλατφόρμες κινητών συσκευών, το Android και το iOS. Αναλύονται οι ιδιαιτερότητες κάθε πλατφόρμας και οι μέθοδοι ενίσχυσης της ασφάλειάς τους, περιλαμβάνοντας τη σωστή διαχείριση κρυπτογράφησης δεδομένων και την εφαρμογή ασφαλών πρακτικών προγραμματισμού.

Το τέταρτο κεφάλαιο περιλαμβάνει πρακτικά παραδείγματα και περιπτώσεις μελέτης, στις οποίες εφαρμόζονται οι θεωρητικές γνώσεις και τα εργαλεία που αναφέρθηκαν στα προηγούμενα κεφάλαια. Αναλύονται πραγματικές περιπτώσεις ευπαθειών που εντοπίστηκαν σε εφαρμογές κινητής τραπεζικής και προτείνονται λύσεις για την αντιμετώπισή τους.

Το τελευταίο κεφάλαιο συνοψίζει τα ευρήματα της έρευνας, υπογραμμίζοντας τη σημασία της συνεχούς βελτίωσης των μέτρων ασφαλείας στις εφαρμογές κινητής τραπεζικής. Παράλληλα, προτείνονται κατευθύνσεις για μελλοντική έρευνα, όπως η ενσωμάτωση νέων τεχνολογιών και τεχνικών μηχανικής μάθησης για την καλύτερη ανίχνευση και πρόληψη των απειλών.

Η παρούσα εργασία επιδιώκει να συμβάλει ουσιαστικά στην κατανόηση των απειλών που αντιμετωπίζουν οι εφαρμογές κινητής τραπεζικής και να προσφέρει πρακτικές λύσεις για την ενίσχυση της ασφάλειας των χρηστών.

1. ΑΞΙΟΛΟΓΗΣΗ ΕΥΠΑΘΕΙΩΝ (VULNERABILITY ASSESSMENT) & ΔΟΚΙΜΕΣ ΔΙΕΙΣΔΥΣΗΣ (PENETRATION TESTING)

Η σύγχυση μεταξύ των όρων «**αξιολόγηση ευπαθειών**» ή «**vulnerability assessment**» και «**δοκιμές διείσδυσης**» ή «**penetration testing**» συχνά ξεκινάει στο επίπεδο της γλώσσας. Όσοι δεν είναι επαγγελματίες στον τομέα της κυβερνοασφάλειας ή όσοι είναι… νέοι στον χώρο, συχνά συγχέουν τις έννοιες πολλές φορές αναφερόμενοι σε κάποια σημαντική ιστορία που επηρεάζει τους καταναλωτές, χρησιμοποιούν τους όρους εναλλακτικά, σαν να αναφέρονται στην ίδια διαδικασία. Οι έμπειροι επαγγελματίες του κλάδου γνωρίζουν τη διαφορά,. Αυτό συμβαίνει διότι ακόμη και οι επαγγελματίες τυγχάνει πολλές φορές να χρησιμοποιούν όρους και έννοιες με ασαφείς ή ανακριβείς τρόπους, όταν θα έπρεπε να είναι σε θέση να διακρίνουν πράγματα που διαφέρουν. Ας δούμε όμως τη σαφή διαφορά μεταξύ τους.

1.1 Τι είναι η αξιολόγηση ευπάθειας (vulnerability assessment);

Μία αξιολόγηση ευπάθειας [1] περιλαμβάνει τη διεξαγωγή μιας σειράς πολλαπλών δοκιμών ενάντια σε ορισμένες ιστοσελίδες, σε εφαρμογές ιστού, σε διευθύνσεις IP και σε εύρη IP, χρησιμοποιώντας μια γνωστή λίστα ευπαθειών και τρωτών σημείων, σαν αυτά που περιλαμβάνονται στη λίστα Top 10 του OWASP. Όσοι πραγματοποιούν αξιολογήσεις, μπορούν επίσης να πραγματοποιήσουν δοκιμές σε συστήματα που γνωρίζουν ότι έχουν εσφαλμένα διαμορφωθεί ή στα οποία δεν έχουν εφαρμοστεί ενημερώσεις ασφαλείας και patches.

Συχνά, χρησιμοποιούνται αυτοματοποιημένα εργαλεία σάρωσης ασφαλείας. Τα συνδρομητικά εργαλεία με άδεια εμπορικής χρήστης θεωρούνται περισσότερο ασφαλή – έρχονται με τακτικές ενημερώσεις, υπάρχουν λιγότερες πιθανότητες να συμπεριλαμβάνουν κακόβουλο κώδικα (τα αντίστοιχα εργαλεία ανοιχτού κώδικα, πάντως, έχουν το σημαντικό πλεονέκτημα να είναι ακριβώς τα ίδια εργαλεία που προτιμούν να χρησιμοποιούν κακόβουλοι χάκερς).

Οι εκτιμήσεις ευπάθειας τείνουν να περιλαμβάνουν τα ακόλουθα στάδια:

- Προσδιορισμός όλων των πόρων, και των συνδεδεμένων πόρων, των συστημάτων πληροφορικής στο εσωτερικό ενός οργανισμού
- Αντιστοίχιση κάποιας τιμής ή προτεραιότητας σε κάθε έναν (από αυτούς)
- Διεξαγωγή αξιολόγησης μίας λίστας γνωστών τρωτών σημείων κατά μήκος ενός μεγάλου αριθμού επιφανειών επίθεσης (από login screens έως παραμέτρους διευθύνσεων URL και μέχρι διακομιστές ηλεκτρονικής αλληλογραφίας)
- Καθορισμός των πιο κρίσιμων τρωτών σημείων και λήψη αποφάσεων σχετικά με τον τρόπο αντιμετώπισης των υπολοίπων

1.2 Τι είναι η δοκιμή διείσδυσης (penetration testing);

Η δοκιμή διείσδυσης (pen testing) [2] από την άλλη – μολονότι ότι μπορεί να θεωρηθεί ως ένας τύπος αξιολόγησης ευπάθειας – περιλαμβάνει την αναπαραγωγή ενός συγκεκριμένου τύπου επίθεσης που μπορεί να εκτελεστεί από κάποιον χάκερ. Κάποιος που πραγματοποιεί δοκιμές διείσδυσης θα εξερευνήσει διεξοδικά τα συστήματα μέχρι να εντοπίσει κάποια ευπάθεια. Ενδεχομένως να χρησιμοποιήσει ακόμα και κάποιο εργαλείο αξιολόγησης ευπάθειας για να αποκαλυφθεί κάποια μια ευπάθεια. Μόλις εντοπιστεί κάτι, τότε θα γίνει προσπάθεια εκμετάλλευσης, για να καθοριστεί αν είναι δυνατό για έναν χάκερ να επιτύχει ένα συγκεκριμένο στόχο (πρόσβαση, αλλαγή ή διαγραφή δεδομένων, για παράδειγμα).

Συχνά, ενώ πραγματοποιείται η δοκιμή διείσδυσης, μπορεί να συναντήσει –εκείνος που κάνει τη δοκιμή- τυχαία άλλες αδυναμίες και να τις ακολουθήσει εκεί που οδηγούν. Όποιος κάνει επίσης τη δοκιμή μπορεί να χρησιμοποιήσει κάποιο αυτοματοποιημένο εργαλείο σε αυτό το σημείο για να εκτελέσει μια σειρά από exploits ενάντια στην ευπάθεια.

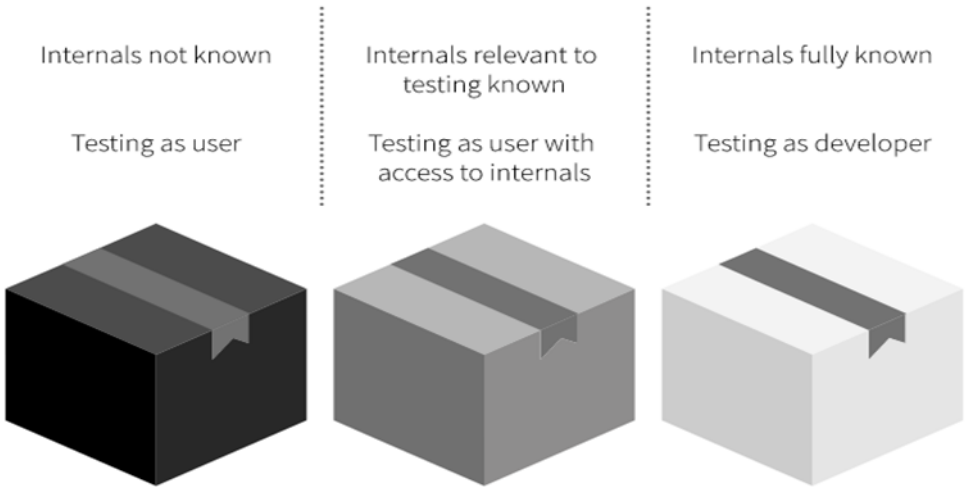
Ορισμένες δοκιμές διείσδυσης αναφέρονται ως «white box». Είναι μια μέθοδος ελέγχου διείσδυσης που διαθέτει πλήρη πρόσβαση στον κώδικα και στη δομή του συστήματος ή της εφαρμογής που ελέγχει. Κατά τη διάρκεια αυτού του είδους του τεστ, ο ελεγκτής έχει πρόσβαση σε όλες τις λειτουργίες και τις εσωτερικές διαδικασίες του συστήματος και μπορεί να ελέγξει τον κώδικα για πιθανές ευπάθειες. Ένα από τα βασικά πλεονεκτήματα του WhiteBox Testing είναι ότι επιτρέπει στον ελεγκτή να ανακαλύψει προβλήματα ασφαλείας που είναι δύσκολα ή αδύνατο να ανιχνευθούν με άλλες μεθόδους ελέγχου. Επίσης, η πλήρης πρόσβαση στον κώδικα επιτρέπει στον ελεγκτή να εκτελέσει εξειδικευμένες αναλύσεις και επιθέσεις που απαιτούν γνώση του εσωτερικού μηχανισμού του συστήματος. Ωστόσο, ένα από τα μειονεκτήματα του WhiteBox Testing είναι ότι απαιτεί πρόσβαση στον κώδικα του συστήματος ή της εφαρμογής, το οποίο μπορεί να είναι περιοριστικό ή αδύνατο σε ορισμένες περιπτώσεις. Επιπλέον, η ανάλυση του κώδικα μπορεί να είναι χρονοβόρα και απαιτητική από άποψη πόρων, ενώ η πλούσια πληροφορία που προσφέρει μπορεί να καθιστά την αξιολόγηση πιο περίπλοκη ο δοκιμαστής διείσδυσης έχει δώσει λεπτομερείς πληροφορίες για το περιβάλλον, όπως έναν κατάλογο περιουσιακών στοιχείων που ανήκουν στον οργανισμό, πηγαίο κώδικα, ονόματα υπαλλήλων και διευθύνσεις ηλεκτρονικού ταχυδρομείου κ.λπ.

Όταν –οι δοκιμές- αναφέρονται ως «black box» [1], σημαίνει ότι ο ελεγκτής δεν έχει προηγούμενη πρόσβαση ή γνώση για το σύστημα ή την εφαρμογή που ελέγχει. Αυτό σημαίνει ότι ο ελεγκτής προσεγγίζει το σύστημα από την άποψη ενός εξωτερικού επιτιθέμενου, χωρίς να έχει εσωτερική γνώση ή προνομιακή πρόσβαση. Κατά τη διάρκεια του BlackBox Testing, ο ελεγκτής εκτελεί διάφορες επιθέσεις που ένας εξωτερικός επιτιθέμενος θα μπορούσε να χρησιμοποιήσει για να εισβάλει στο σύστημα. Ένα από τα πλεονεκτήματα του BlackBox Testing είναι ότι αντιπροσωπεύει μια πραγματική επίθεση από έναν εξωτερικό επιτιθέμενο, χωρίς προηγούμενη γνώση

ή πρόσβαση στο σύστημα. Αυτό βοηθάει στην ανίχνευση ευπαθειών που θα μπορούσαν να εκμεταλλευτούν κακόβουλοι επιτιθέμενοι. Ωστόσο, ένα μειονέκτημα είναι ότι ο ελεγκτής είναι περιορισμένος στο να ανακαλύψει εσωτερικές αδυναμίες που δεν είναι ορατές από έξω.

Ακόμα υπάρχει και το GreyBox Penetration Testing το οποίο αποτελεί μια προσέγγιση στον έλεγχο διείσδυσης που συνδυάζει στοιχεία από τόσο το BlackBox όσο και το WhiteBox Testing. Κατά τη διάρκεια αυτού του είδους του τεστ, ο ελεγκτής διαθέτει μερική πρόσβαση στο σύστημα ή στην εφαρμογή που ελέγχει, καθώς έχει προηγούμενη γνώση για τον τρόπο λειτουργίας του συστήματος αλλά όχι πλήρη πρόσβαση στον κώδικα ή στη δομή του. Τα πλεονεκτήματα του GreyBox Testing περιλαμβάνουν τη δυνατότητα για πιο στοχευμένες επιθέσεις σε σχέση με το BlackBox Testing, καθώς και την ικανότητα να ανακαλυφθούν ευπάθειες που απαιτούν προηγούμενη γνώση.

Επίσης, η πρόσβαση σε μερικές πληροφορίες για το σύστημα μπορεί να βοηθήσει τον ελεγκτή να επιλέξει αποτελεσματικότερες μεθόδους επίθεσης. Ωστόσο, το GreyBox Testing μπορεί να παραβλέψει ευπάθειες που είναι ορατές μόνο από εξωτερικούς επιτιθέμενους ή να αποτύχει να ανακαλύψει εσωτερικές αδυναμίες που δεν είναι προσβάσιμες με την περιορισμένη πρόσβαση του ελεγκτή. Επιπλέον, η ποιότητα των αποτελεσμάτων εξαρτάται σε μεγάλο βαθμό από την επίπεδο γνώσης και εμπειρίας του ελεγκτή σχετικά με τον τρόπο λειτουργίας του συστήματος.



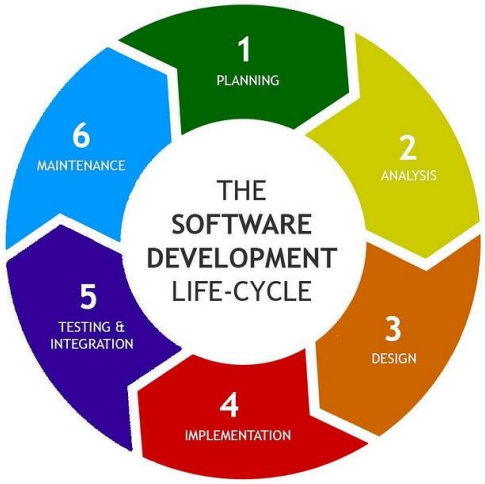
Εικόνα 1. Black-Grey-White Box Penetration-Testing

Πηγή : https://whitehacklabs.com/blog/penetration-testing-types-black-box-vs-white-box/

Τα αποτελέσματα συγκεντρώνονται σε μια αυτοματοποιημένη, μακροσκελή αναφορά, που περιλαμβάνει μία εκτεταμένη λίστα τρωτών σημείων που έχουν ανιχνευθεί και ταξινομηθεί κατά προτεραιότητα, από το πόσο σοβαρά και κρίσιμα είναι

για την επιχείρησή. Με το πέρασμα του χρόνου, αυτή η λίστα μπορεί να αποκαλύψει αλλαγές από την τελευταία αναφορά. Ορισμένοι πάντως θα επικρίνουν τα επιτευχθέντα αποτελέσματα επειδή, σε αντίθεση με τις δοκιμές διείσδυσης, μπορεί να περιέχουν ψευδώς θετικά ή ψευδώς αρνητικά. Φυσικά, κάτι τέτοιο δεν πρόκειται να συμβεί αν χρησιμοποιείτε τον σαρωτή ευπάθειας εφαρμογών ιστού Netsparker (web application vulnerability scanner) για να διεξάγετε τις δοκιμές διείσδυσης. Και αυτό είναι ένα από τα βασικά χαρακτηριστικά που διαφοροποιούν την Netsparker – η αυτόματη επαλήθευση εντοπισμένων τρωτών σημείων με το Proof-Based Scanning.

Οι αναφορές οφείλουν να περιλαμβάνουν έναν οδηγό που θα υποδεικνύει τρόπους αποκατάστασης των τρωτών σημείων και ευπαθειών που εντοπίστηκαν. Κάποιες φορές τα ίδια τα εργαλεία συνοδεύονται από τα κατάλληλα patches που μπορούν να τρέξουν και να εφαρμόσουν οι διάφοροι συνδρομητές. Στις περισσότερες περιπτώσεις, τα αποτελέσματα μπορούν να διανεμηθούν στη συνέχεια σε εξειδικευμένες ομάδες ανάπτυξης για να εφαρμόσουν διορθώσεις, να απομακρύνουν τις πιο σοβαρές ευπάθειες αλλά και να αντιμετωπίσουν με το κατάλληλο τρόπο τις λιγότερο σοβαρές στη συνέχεια. Σε έναν ιδανικό κόσμο, αυτή η δραστηριότητα είναι συνεχιζόμενη, αφού προγραμματίζεται τακτικά, και είναι ενσωματωμένη στο SDLC (Software Development Life Cycle) κάθε οργανισμού.



Εικόνα 2. Software development life-cycle (SDLC)

Πηγή : https://medium.com/@artjoms/software-development-life-cycle-sdlc-6155dbfe3cbc

Με τη δοκιμή διείσδυσης, δεν υπάρχει κάποια μακροσκελή δημόσια αναφορά, αν και κάποιοι καταγράφουν και δημοσιεύουν τις ενέργειές τους και τα ανώνυμα ευρήματα τους, αναρτούν σε blogs τα πειράματά τους ή επιχειρούν χάκινγκ σε συνέδρια. Αν ωστόσο προσλάβετε κάποιον για να πραγματοποιήσει δοκιμές διείσδυσης, οφείλει να σας ετοιμάσει και να σας παρουσιάσει μια αναφορά, αν και στις περισσότερες περιπτώσεις τέτοιες αναφορές επικεντρώνονται στη μέθοδο της επίθεσης ή στα exploits αλλά και ακριβώς ποια δεδομένα βρίσκονται σε κίνδυνο. Γενικά, επίσης,

θα συνοδεύεται και από προτάσεις σχετικά με το τι μπορεί να κάνει κάποιος χάκερ σε αυτά ή με αυτά. Τα παραπάνω, θα βοηθήσουν τους αναλυτές επιχειρήσεων και τους μη τεχνικούς επαγγελματίες, που μπορεί να μην καταλαβαίνουν ή αντιλαμβάνονται όλη αυτή τη τεχνολογία που υπάρχει πίσω από τις δοκιμές τους είδους, να αντιληφθούν γρήγορα τον αντίκτυπο των επιχειρηματικών διαδικασιών.

Κάποιες φορές οι εκθέσεις περιλαμβάνουν επίσης συμβουλές αποκατάστασης. Ωστόσο, δεν ενσωματώνουν όλες οι δοκιμές διείσδυσης το λεγόμενο «exploitation των τρωτών σημείων» με τον τρόπο που το κάνει η λύση Netsparker. Μπορεί απλώς να αρκεί η επίδειξη ότι μία επίθεση μπορεί να είναι δυνατή. Σε ορισμένες περιπτώσεις, η αναφορά δοκιμής διείσδυσης μπορεί απλώς να αναφέρει θεωρητικές ευπάθειες επειδή οποιαδήποτε προσπάθεια «εκμετάλλευσης» θα μπορούσε να οδηγήσει σε μία καταστροφική άρνηση υπηρεσίας (DoS). Και τέλος, δεν υπάρχει αξιολόγηση των τρωτών σημείων ή των ευπαθειών, δεδομένου ότι ο στόχος είναι απλώς να γίνει ένα

Οι εκτιμήσεις ή αξιολογήσεις ευπάθειας αποτελούν έναν ιδιαίτερα συστηματοποιημένο τρόπο για να αποκτήσουν καθιερωμένες εταιρείες και οργανισμοί μια ολοκληρωμένη εικόνα για τη στάση τους στην ασφάλεια και κατόπιν να την διατηρήσουν και να την βελτιώνουν διαρκώς.

Όταν προστίθενται νέες συσκευές, θύρες, ιστότοποι, εφαρμογές ιστού ή υπηρεσίες, συμπεριλαμβάνονται στις συνήθεις σαρώσεις. Μια αξιολόγηση ευπάθειας είναι ένας πολύ καλός τρόπος για να εντοπίσετε και τελικά να διορθώσετε κοινές ευπάθειες στις εφαρμογές και στους διακομιστές σας. Οι περισσότεροι επαγγελματίες στον χώρο της ασφάλειας συστήνουν στις εταιρείες να προχωρούν σε αξιολογήσεις ευπάθειας

Από την ώρα που οι δοκιμές διείσδυσης είναι τόσο συγκεκριμένες, είναι ιδανικές για περιβάλλοντα όπου η ασφάλεια Ιστού καθώς και του δικτύου ενός οργανισμού θεωρείται ότι είναι ήδη αρκετά ισχυρή. Οι οργανισμοί μπορούν να ζητήσουν από έναν ελεγκτή να επιχειρήσει να κάνει κάτι συγκεκριμένο, όπως να επιχειρήσει να αποκτήσει πρόσβαση σε μια βάση δεδομένων τραπεζικών συναλλαγών ή τραπεζικών στοιχείων ή προσπαθήσει να τροποποιήσει ή να διαγράψει τον φάκελο κάποιου χρήστη (δεδομένα κ.λπ). Σκοπός είναι να μειωθεί η έκθεση σε συγκεκριμένους κινδύνους.

Οι δοκιμαστές διείσδυσης ελέγχουν για αδύναμα σημεία στην αρχιτεκτονική. Ενώ οι αξιολογήσεις ευπαθειών ή τρωτών σημείων αντιμετωπίζουν ως επί το πλείστων τα κενά ασφαλείας στο λογισμικό, οι δοκιμαστές διείσδυσης συχνά χρησιμοποιούν τεχνικές phishing ή κοινωνικής μηχανικής αλλά και άλλες τεχνικές για να επιτύχουν το στόχο τους. Ως εκ τούτου, μπορούν να παρέχουν μια σαφέστερη και ακριβέστερη απεικόνιση ή εκτίμηση του επιπέδου ασφαλείας μίας εταιρείας. Λειτουργούν ακριβώς όπως οι κακόβουλοι χάκερ, αλλά χωρίς να προκαλούν καταστροφικές απώλειες ή αλλοίωση δεδομένων, φυσικά. Για παράδειγμα, ένας δοκιμαστής διείσδυσης μπορεί να προσπαθήσει να δημιουργήσει μια σύνδεση με έναν απομακρυσμένο διακομιστή χωρίς να εντοπιστεί, προκειμένου να απομακρύνει ευαίσθητα δεδομένα από ένα σύστημα. Είναι ένας χρήσιμος τρόπος για να αποδειχτεί ότι υπάρχουν πιθανότητες για κάποιους επιτιθέμενους να επιτύχουν τους κακόβουλους σκοπούς τους. Φαινομενικά, όμως, ένας

δοκιμαστής διείσδυσης θα προχωρούσε στη διεξαγωγή μίας ατελείωτης σειράς από απόπειρες χάκινγκ.

Τόσο οι αξιολογήσεις ευπάθειας όσο και οι δοκιμές διείσδυσης πρέπει να πραγματοποιούνται ενάντια σε συσκευές δικτύου και ενάντια σε εσωτερικούς και εξωτερικούς διακομιστές. Είναι σημαντικό να καθοριστεί αν μια επίθεση μπορεί να γίνει από το εξωτερικό (για παράδειγμα, από έναν κακόβουλο εισβολέα που στοχεύει σε διαθέσιμες στο κοινό επιφάνειες στόχων στο διαδίκτυο) ή από το εσωτερικό (για παράδειγμα, από έναν δυσαρεστημένο υπάλληλο ή παλιό συνεργάτη, κάποιον χρήστη με δικαιώματα που δεν θα έπρεπε να έχει ή από κάποιον υπολογιστή που έχει μολυνθεί στο εσωτερικό δίκτυο).

Μερικές φορές οι εταιρείες και οργανισμοί πρέπει να εργάζονται εντός συγκεκριμένων παραμέτρων: έχουν PCI DSS ή άλλες μορφές συμμόρφωσης που οφείλουν να τηρούν και θέλουν να ελέγξουν αν η υφιστάμενη αρχιτεκτονική τους, και τα συστήματα και οι συσκευές τους είναι σε θέση να περάσουν τη δοκιμή. Μπορεί να θέλουν να εκτελέσουν μια σάρωση θυρών ή να ελέγξουν τα πάντα στη λίστα Top 10 του OWASP. Σε τέτοια σενάρια, μια αξιολόγηση ευπάθειας θα δώσει μια πιο ρεαλιστική και συστηματική προσέγγιση. Ακόμα και μια πολύ μεγάλη ομάδα προγραμματιστών δεν θα μπορούσε να φέρει εις πέρας τέτοιες δοκιμές.

Οι δοκιμές διείσδυσης βοηθούν επίσης στην ασφάλεια αλλά υπό διαφορετική γωνία. Οι δοκιμαστές (εκείνοι που θα πραγματοποιήσουν τις δοκιμές διείσδυσης) θα αποκαλύψουν τους κινδύνους ασφαλείας με τον ίδιο τρόπο που το κάνουν οι χάκερ – πραγματοποιώντας επιθέσεις έχοντας στο νου τους μόνο ένα σκοπό, να αποκτήσουν πρόσβαση σε συγκεκριμένα δεδομένα ή να αλλάξουν κάτι στον ιστότοπο ενός οργανισμού, για παράδειγμα. Οι δοκιμαστές διείσδυσης είναι καλύτερο να «προσλαμβάνονται» με ανοιχτό μυαλό, αφήνοντάς τους ελεύθερους να διεξάγουν τόσο τις επιδιωκόμενες επιθέσεις όσο και οτιδήποτε άλλο που πέσει στην αντίληψη τους, αναλόγως βεβαίως και της επαγγελματικής τους πείρας.

Ένα από τα πιο σημαντικά ερωτήματα που πρέπει να θέσουμε, για να αποφύγουμε τη σύγχυση μεταξύ της αξιολόγησης ευπάθειας και της δοκιμής διείσδυσης είναι: Ποιος διεξάγει τη δοκιμή; Σε αντίθεση με ορισμένα άρθρα σχετικά με το θέμα, οι δοκιμές ευπάθειας δεν είναι μια πλήρως αυτοματοποιημένη διαδικασία, με την έννοια ότι το μόνο που θα χρειαστεί είναι να πατήσετε ένα κουμπί. Το άτομο που διαχειρίζεται συχνές, αυτοματοποιημένες αξιολογήσεις ευπάθειας θα πρέπει να εξειδικεύεται εξίσου και να έχει εμπειρία και στις διαδικασίες ασφάλειας πληροφοριών. Οφείλει να γνωρίζει ποια περιβάλλοντα και ποιες επιφάνειες επίθεσης πρέπει να αξιολογήσει καθώς και πάνω σε τι να τα αξιολογήσει, καθώς ακόμα και οι αυτοματοποιημένοι σαρωτές ασφαλείας απαιτούν εξίσου κάποια διαμόρφωση ή ρύθμιση. Επιπλέον, πρέπει να είναι σε θέση να ερμηνεύει τις όποιες αναφορές προκύπτουν αλλά και να διατυπώνει συστάσεις σχετικά με το τι πρέπει να γίνει στη συνέχεια.

Οι εσωτερικοί επαγγελματίες ασφαλείας που είναι υπεύθυνοι για την αξιολόγηση ευπαθειών αποτελούν πρόσθετη αξία για την στάση ασφαλείας που κρατούν εταιρείες και οργανισμοί. Κατά πρώτο λόγο είναι σε θέση να ορίσουν τις βασικές γραμμές.

Επιπλέον, το πιθανότερο είναι να θελήσουν να καθιερώσουν κάποια συστήματα, όπως κάποιο χρονοδιάγραμμα αξιολόγησης και αναφορών.

Συμβάλουν στην ευαισθητοποίηση των εργαζομένων εντός της εταιρείας, και παράλληλα ευνοούν την διαρκή μείωση των κινδύνων ασφαλείας. Εν τω μεταξύ, είναι σχεδόν σίγουρο πως θα επεκτείνουν τις δικές τους γνώσεις και δεξιότητες. Και αναμφισβήτητα είναι πολύ πιο πιθανό να αισθάνονται πιστοί στην εταιρεία που εργάζονται ήδη.

Όσοι επιχειρούν δοκιμές διεισδύσεις θα πρέπει επίσης να είναι έμπειροι επαγγελματίες και να έχουν αυτοπεποίθηση για τις ικανότητές και τις δεξιότητές τους.

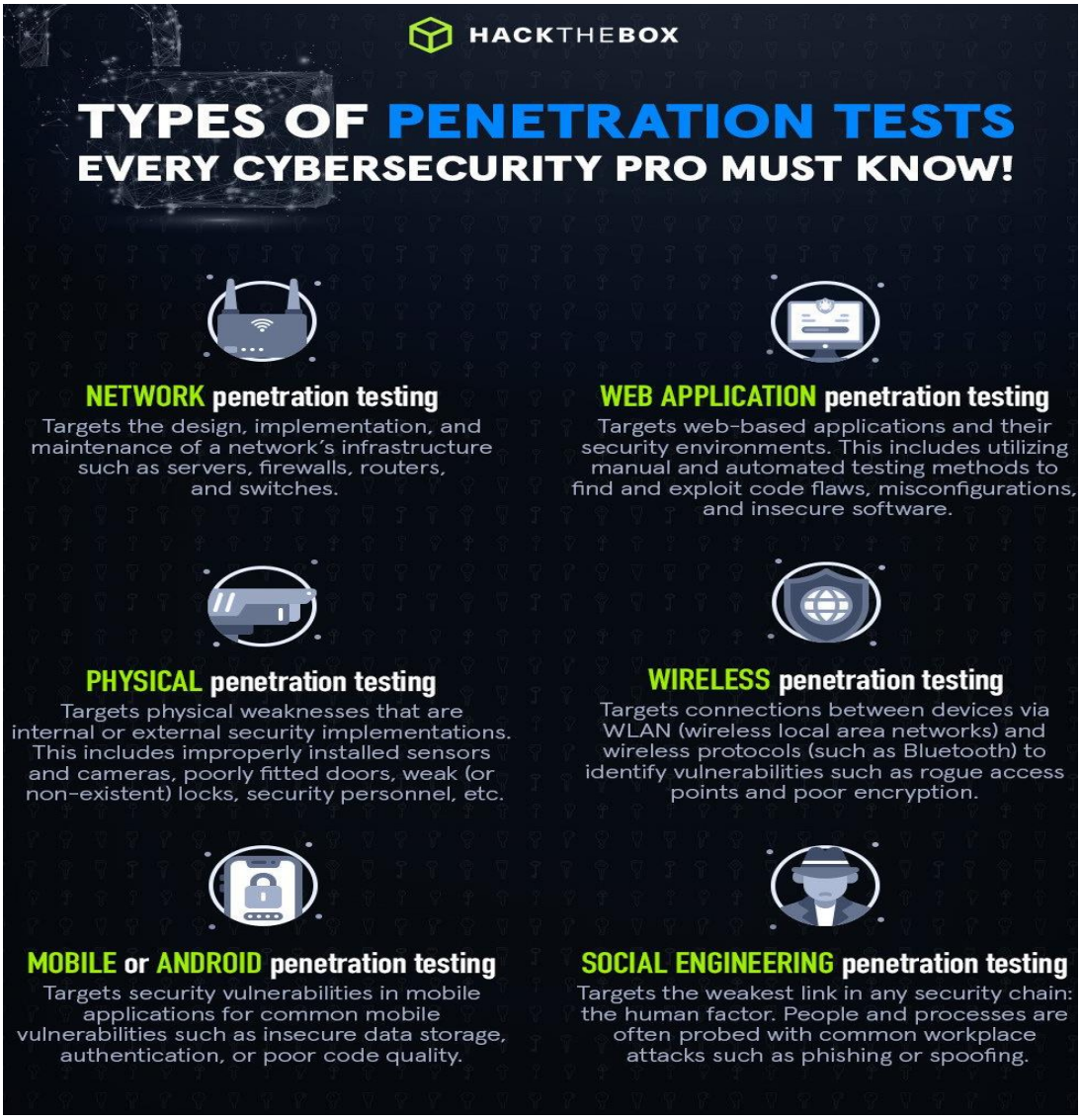
Οι περισσότεροι επαγγελματίες στον τομέα, συστήνουν οι δοκιμαστές διείσδυσης να είναι ανεξάρτητοι, εξωτερικοί επαγγελματίες. Πρέπει να διατηρούν αρκετή απόσταση από την εταιρεία ή τα συστήματα σας, ώστε να μην παρεμποδίζονται ή επηρεάζονται από ανησυχίες σχετικά με την προσωπική τους οικονομική ασφάλεια, την πίστη τους ή την πολιτική της εταιρείας. Και αυτό τους δίνει τη δυνατότητα έχοντας το ελεύθερο να πουν την γνώμη τους ανεπηρέαστα, και να στην ουσία να πουν τα πράγματα με το όνομα τους σχετικά με την κατάστασή της εταιρείας σας στον τομέα της ασφάλειας, όσο και αν αυτό πονάει.

Το κόστος των αξιολογήσεων ευπάθειας και των δοκιμών διείσδυσης εξαρτάται στην ουσία από το μέγεθος της επιχείρησης (από την επιφάνεια επίθεσης επομένως κλπ). Για τις μικρές εταιρείες, η τιμή θα είναι σημαντικά χαμηλότερη από ό, τι είναι για μια μεγάλη εταιρία με χιλιάδες δυνητικά ευάλωτες συσκευές και υπολογιστές, IPs και παρόχους Internet.

Ανεξάρτητα από το κόστος, οι εκτιμήσεις ευπαθειών ή τρωτότητας συνεισφέρουν στην καλύτερη απόδοση της επένδυσής σας. Ενώ μια δοκιμή διείσδυσης μπορεί να προσφέρει μία αρκετά καλή και βαθιά εικόνα για το πόσο ασφαλή είναι τα συστήματά σας, στην πραγματικότητα αποκαλύπτει μόνο ένα πράγμα και προς μία κατεύθυνση. Από την άλλη, με τις αξιολογήσεις ευπαθειών και επενδύοντας σε χρόνο και πόρους στην ανάπτυξη συστημάτων και διαδικασιών θα έχετε ένα σταθερό επίπεδο ασφάλειας πάνω στο οποίο θα αναπτυχθούν περαιτέρω τα συστήματά σας και θα ενσωματωθούν νέα εξαρτήματα.

1.3 Δοκιμές Ευπαθειών και Αδυναμιών

Ο τύπος των δοκιμών διείσδυσης και ελέγχου ευπαθειών [1] που διεξάγουμε θα καθοριστεί από τις ανάγκες ενός οργανισμού και θα προσδιοριστεί νωρίς με ένα λεπτομερές πεδίο εργασίας που αποσαφηνίζει τις παραμέτρους δοκιμών, τη σύμβαση και τους κανόνες εμπλοκής. Ένας οργανισμός μπορεί να θέλει μια εκτεταμένη δοκιμή (Amazon Web Services) AWS pentest της υποδομής που φιλοξενείται στο cloud, ένας άλλος μπορεί να θέλει μια φυσική δοκιμή της ασφάλειας του κτιρίου τους.



Εικόνα 3. Τύποι Penetration Testing

Πηγή: https://www.hackthebox.com/blog/what-is-penetration-testing

Οι πιο συνηθισμένοι τύποι δοκιμών διείσδυσης είναι:

- **Δοκιμή διείσδυσης δικτύου (Network Penetration Test) :** Στοχεύει στο σχεδιασμό, την υλοποίηση και τη συντήρηση της υποδομής ενός δικτύου, όπως διακομιστές, τείχη προστασίας, δρομολογητές και μεταγωγείς.
- **Δοκιμές διείσδυσης εφαρμογών Web (Web Application Penetration Test) :** Στοχεύει εφαρμογές που βασίζονται στο web και τα περιβάλλοντα ασφαλείας τους. Αυτό περιλαμβάνει τη χρήση μη αυτόματων και αυτοματοποιημένων μεθόδων δοκιμών για την εύρεση και εκμετάλλευση ελαττωμάτων κώδικα, εσφαλμένων διαμορφώσεων και μη ασφαλούς λογισμικού.
- **Δοκιμές διείσδυσης για κινητά ή Android (Mobile or Android penetration testing):** Στοχεύει αδυναμίες ασφαλείας σε εφαρμογές για κινητές συσκευές για

κοινές ευπάθειες για κινητές συσκευές, όπως μη ασφαλή αποθήκευση δεδομένων, έλεγχος ταυτότητας ή κακή ποιότητα κώδικα.

- **Δοκιμές διείσδυσης ασύρματης σύνδεσης (Wireless penetration testing):** Στοχεύει συνδέσεις μεταξύ συσκευών μέσω WLAN (ασύρματα τοπικά δίκτυα) και ασύρματων πρωτοκόλλων (όπως Bluetooth) για τον εντοπισμό τρωτών σημείων, όπως παραπλανητικά σημεία πρόσβασης και κακή κρυπτογράφηση.
- **Δοκιμή φυσικής διείσδυσης (Physical penetration testing):** Στοχεύει φυσικές αδυναμίες που είναι εσωτερικές ή εξωτερικές εφαρμογές ασφάλειας. Αυτό περιλαμβάνει ακατάλληλα εγκατεστημένους αισθητήρες και κάμερες, κακώς τοποθετημένες πόρτες, αδύναμες (ή ανύπαρκτες) κλειδαριές, προσωπικό ασφαλείας κλπ.
- **Δοκιμές διείσδυσης κοινωνικής μηχανικής (Social engineering penetration testing**): Στοχεύει τον πιο αδύναμο κρίκο σε οποιαδήποτε αλυσίδα ασφάλειας: τον ανθρώπινο παράγοντα. Οι άνθρωποι και οι διαδικασίες συχνά διερευνώνται με κοινές επιθέσεις στο χώρο εργασίας, όπως το ηλεκτρονικό ψάρεμα (phishing) ή η πλαστογράφηση (spoofing).

1.4 Μεθοδολογίες Penetration Testing

Οι μεθοδολογίες penetration testing αναπαριστούν μια σειρά συστηματικών προσεγγίσεων που χρησιμοποιούνται για τον έλεγχο και την αξιολόγηση της ασφάλειας ενός συστήματος ή μιας εφαρμογής. Η βασική τους ιδέα είναι να εντοπίσουν πιθανές αδυναμίες και ευπάθειες, καθώς και πιθανά σημεία εισόδου για επιθέσεις, προκειμένου να ληφθούν μέτρα για την ενίσχυση της ασφάλειας. Υπάρχουν πολλές διαφορετικές μεθοδολογίες που χρησιμοποιούνται στον τομέα αυτό, αλλά οι πιο γνωστές είναι οι εξής:

- NIST-SP 800-115
- Penetration Testing Execution Standard (PTES)
- OWASP Mobile Security Testing Guide (MSTG)
- MITRE ATT&CK Framework
- OSSTMM (Open-Source Security Testing Methodology Manual)
- ISSAF

Κάθε μεθοδολογία έχει τις δικές της τεχνικές και προσεγγίσεις, αλλά ο στόχος τους είναι ο ίδιος: η εντοπισμός αδυναμιών και η βελτίωση της ασφάλειας. Ανάλογα με τις ανάγκες και τα χαρακτηριστικά του συστήματος που ελέγχεται, επιλέγεται η κατάλληλη μεθοδολογία. Συνήθως, κατά τη διάρκεια ενός penetration test, χρησιμοποιούνται εργαλεία και τεχνικές όπως η εκτέλεση ελεγχόμενων επιθέσεων, η ανάλυση αδυναμιών και η καταγραφή αποτελεσμάτων. Το αποτέλεσμα είναι η αναφορά των ευρημάτων και η πρόταση βελτιώσεων για την ασφάλεια του συστήματος.

1.4.1 Μεθοδολογία NIST-SP 800-115

Η μεθοδολογία NIST-SP 800-115 [3] παρέχει κατευθυντήριες γραμμές για τον σχεδιασμό και τη διεξαγωγή δοκιμών και αξιολογήσεων ασφάλειας τεχνικών πληροφοριών. Στοχεύει στην ανάπτυξη στρατηγικών αντιμετώπισης προβλημάτων και παρέχει πρακτικές συστάσεις για την εφαρμογή, τη διατήρηση και την αξιολόγηση των τεχνικών πληροφοριών σε σχέση με την ασφάλεια. Δεν προορίζεται ως ένα ολοκληρωμένο πρόγραμμα δοκιμών ή αξιολόγησης της ασφάλειας των πληροφοριών, αλλά ως μια επισκόπηση των βασικών στοιχείων της τεχνικής δοκιμής και αξιολόγησης ασφαλείας, με έμφαση σε συγκεκριμένες τεχνικές, οφέλη, περιορισμούς και συστάσεις για τη χρήση τους. Συνολικά, απευθύνεται κυρίως σε μεγάλους οργανισμούς που επιθυμούν να βελτιώσουν την ασφάλεια των πληροφοριών τους και να εφαρμόσουν αποτελεσματικές πρακτικές δοκιμών και αξιολογήσεων ασφάλειας. Αρχικά, η μεθοδολογία ορίζει τέσσερις βασικούς πυλώνες. Αυτοί είναι:

- Δημιουργία πολιτικής (Policy establishment)
- Επαναληπτικότητα και τεκμηρίωση (Implementation of a repeatable
- and documented methodology)
- Καθορισμός των στόχων (Determination of the objectives)
- Ανάλυση των ευρημάτων (Analysis of findings)

Η διαμόρφωση αυτών των πυλώνων αποτελεί βασικό βήμα για οποιαδήποτε υλοποίηση της μεθόδου. Μετά τη διαμόρφωση αυτών των πυλώνων, η μεθοδολογία ορίζει τις φάσεις της. Αυτές είναι οι:

1. Σχεδιασμός (Planning)
2. Ανεύρεση (Discovery)
3. Επίθεση (Attack)
4. Δημιουργία Αναφοράς (Reporting)

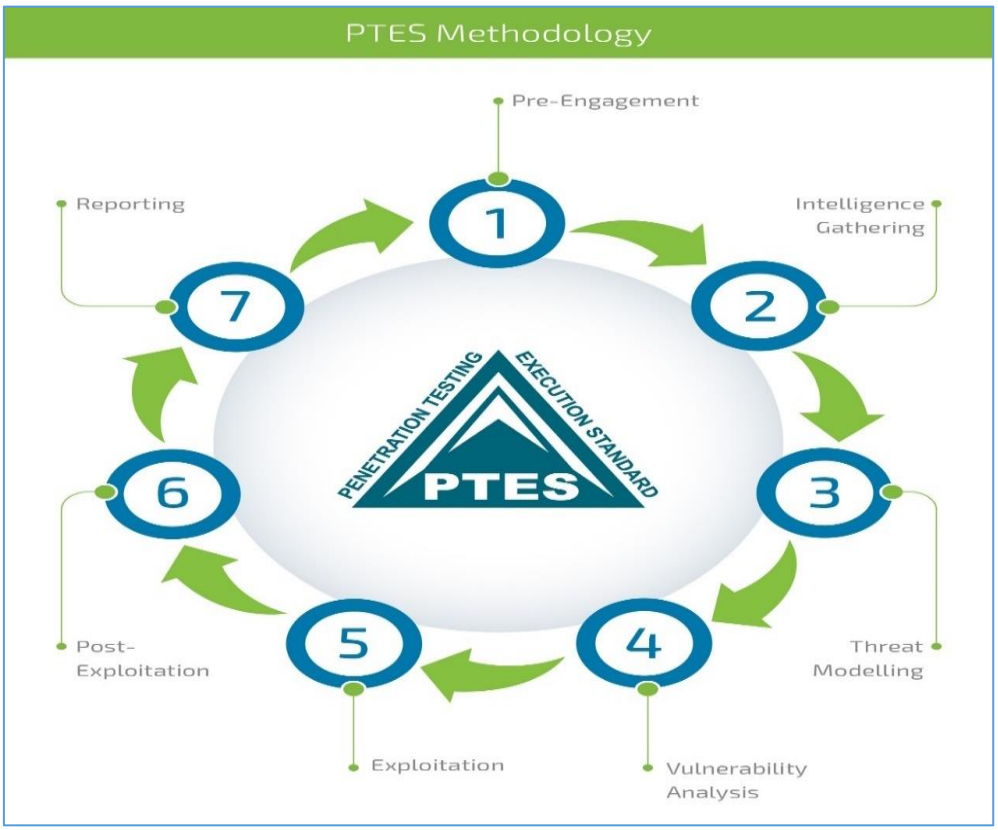
Από τον ορισμό των φάσεων και τον αριθμό τους διαφαίνεται ο αφαιρετικός χαρακτήρας της μεθοδολογίας NIST-SP 800-115 αλλά και η ενσωμάτωση φάσεων σε μία.

Εικόνα 4. Φάσεις NIST-SP 800-115

Πηγή: https://thecyphere.com/blog/nist-penetration-testing/

1.4.2 Penetration Testing Execution Standard (PTES)

Το Πρότυπο Εκτέλεσης Δοκιμών Διείσδυσης (PTES) [4] αντιπροσωπεύει μια πολύτιμη πηγή καθοδήγησης για εκτελεστές δοκιμών διείσδυσης, προσφέροντας μια στρατηγική και δομημένη προσέγγιση για τη διεξαγωγή τους. Τα κύρια στάδια του PTES παρέχουν μια ολοκληρωμένη εικόνα του διαδικαστικού πλαισίου ενός penetration test.



Εικόνα 5. Φάσεις PTES

Πηγή: https://www.infopulse.com/blog/guide-to-modern-penetration-testing-part-2-fifty-shades-of-grey-box

1) **Φάση Προετοιμασίας (Pre-engagement Interactions)**: Η οριοθέτηση του στόχου αποτελεί αναμφίβολα ένα από τα κρίσιμα στάδια σε κάθε διαδικασία ελέγχου διείσδυσης, αλλά συχνά παραμελείται. Παρόλο που υπάρχουν αμέτρητοι τόμοι που ασχολούνται με τα εργαλεία και τις τεχνικές για την απόκτηση πρόσβασης σε ένα δίκτυο, λίγοι επικεντρώνονται στην προηγούμενη διαδικασία. Αν η φάση προετοιμασίας δεν διεξάγεται σωστά με την εταιρεία, μπορεί να προκύψουν πολλαπλά προβλήματα, όπως η δυσαρέσκεια των πελατών και νομικά ζητήματα. Ο καθορισμός του πεδίου του στόχου προσδιορίζει συγκεκριμένα τι θα υποβληθεί σε δοκιμή, ενώ οι κανόνες δέσμευσης καλύπτουν τον τρόπο διεξαγωγής και κάθε λεπτομέρεια του ελέγχου διείσδυσης.
2) **Φάση Συλλογής Πληροφοριών (Intelligence Gathering)**: Κατά τη φάση της συλλογής πληροφοριών, έχει ζωτική σημασία να πραγματοποιηθεί η

αναγνώριση του στόχου. Σε αυτή τη φάση, ο penetration tester συλλέγει όσο το δυνατόν περισσότερες πληροφορίες που θα χρησιμοποιηθούν στις επόμενες φάσεις αναγνώρισης τρωτοτήτων και εκμετάλλευσης ευπαθειών. Η συλλογή αυτών των πληροφοριών αποτελείται συχνά από τη χρήση μεθόδων ανοιχτής πηγής πληροφόρησης (OSINT). Στη μέθοδο OSINT, ο penetration tester αναζητά δεδομένα από διαφορετικές πηγές που είναι διαθέσιμες στο διαδίκτυο και μπορεί να περιλαμβάνουν ευαίσθητες πληροφορίες για έναν οργανισμό. Αυτό μπορεί να βοηθήσει τον penetration tester να αξιολογήσει το επίπεδο ασφαλείας της εταιρείας και να αναπτύξει τις κατάλληλες τεχνικές για τη διείσδυσή τους. Ωστόσο, πρέπει να σημειωθεί ότι η φάση αυτή δεν είναι πάντα αποτελεσματική, καθώς οι πληροφορίες που βρίσκονται στο διαδίκτυο μπορεί να είναι είτε ξεπερασμένες και να μην αντανακλούν την παρούσα κατάσταση της εταιρείας, είτε να έχουν τροποποιηθεί με σκοπό να παραπλανήσουν κακόβουλους χρήστες.

3) **Φάση Μοντελοποίησης Απειλών (Threat Modeling)**: Η φάση της μοντελοποίησης απειλών αποτελεί ένα κρίσιμο στάδιο στην εκτέλεση ενός ελέγχου διείσδυσης. Σε αυτήν τη φάση, ο στόχος είναι η δημιουργία ενός σαφούς μοντέλου που θα αναλύει τις απειλές που μπορεί να αντιμετωπίσει ο ελεγκτής και ο πελάτης. Το μοντέλο απειλών συνήθως προσδιορίζει διάφορα στοιχεία, συμπεριλαμβανομένων:
    - **Επιχειρηματικών Αγαθών (Business Assets):** Αυτά είναι τα κρίσιμα περιουσιακά στοιχεία της εταιρείας, όπως δεδομένα πελατών, εμπιστευτικές πληροφορίες, ή κρίσιμες υποδομές.
    - **Επιχειρηματικές Διαδικασίες (Business Processes):** Αυτές είναι οι λειτουργίες και οι διαδικασίες που είναι κρίσιμες για τη λειτουργία της επιχείρησης, όπως η διαχείριση παραγγελιών ή η διαχείριση πληροφοριών.

    Ο προσδιορισμός των απειλών συνήθως γίνεται με συνεργασία με τον πελάτη. Αν και μπορεί να υπάρχουν προηγούμενες γνώσεις για τους στόχους και τις απειλές, σε μια κατάσταση "μαύρου κουτιού" όπου ο ελεγκτής δεν έχει προηγούμενη πληροφόρηση, είναι απαραίτητο να δημιουργήσει ένα μοντέλο απειλής βασισμένο στην προοπτική ενός επιτιθέμενου, συνδυάζοντας τις πληροφορίες που αντλούνται από την έρευνα OSINT σχετικά με τον πελάτη. Το μοντέλο απειλής παρέχει τη βάση για την αξιολόγηση του κινδύνου και τη δημιουργία στρατηγικών προστασίας. Η καλά τεκμηριωμένη παράδοση αυτού του μοντέλου ως μέρος της τελικής αναφοράς βοηθάει στην αντιμετώπιση των απειλών με πιο συγκεκριμένο και αποτελεσματικό τρόπο.

4) **Φάση Αναγνώρισης Τρωτοτήτων (Vulnerability Analysis)**: Η φάση αυτή επικεντρώνεται στον εντοπισμό των ευπαθειών στον στόχο του ελέγχου διείσδυσης. Αυτή η φάση αποτελεί κρίσιμο βήμα, καθώς οι ευπαθείς πόροι παρέχουν τις δυνατότητες για εκμετάλλευση από επιτιθέμενους. Ο εντοπισμός τρωτοτήτων περιλαμβάνει τόσο αυτόματες όσο και χειροκίνητες μεθόδους.

- ✓ **Αυτόματες Μέθοδοι:** Αυτές περιλαμβάνουν τη χρήση εργαλείων αναγνώρισης ευπαθειών, όπως vulnerability scanners, που ανιχνεύουν αυτόματα ευπαθείς σημεία στον στόχο. Αυτά τα εργαλεία εκτελούν σάρωση του δικτύου ή των εφαρμογών και εντοπίζουν ευπαθείς σημεία όπως ανοικτές θύρες, αδύναμες κωδικοποιήσεις, ή ανενεργές εφαρμογές.
- ✓ **Χειροκίνητες Μέθοδοι:** Αυτή η προσέγγιση περιλαμβάνει μια λεπτομερή εξέταση των ευπαθών περιοχών του στόχου από έναν εξειδικευμένο ελεγκτή διείσδυσης. Κατά τη διάρκεια αυτής της διαδικασίας, ο ελεγκτής ελέγχει χειροκίνητα τον κώδικα, τις ρυθμίσεις δικτύου, και άλλα στοιχεία για να εντοπίσει πιθανές ευπαθείς συνθήκες. Στη συνέχεια, οι ευπαθείς πόροι επικυρώνονται για να διασφαλιστεί η εγκυρότητα των ευρεθέντων τρωτοτήτων. Κάθε ευπάθεια πρέπει να ταξινομηθεί σύμφωνα με τον βαθμό της σοβαρότητάς της και να τεκμηριωθεί προσεκτικά για να ενσωματωθεί στην τελική αναφορά του ελέγχου διείσδυσης.

5) **Φάση Εκμετάλλευσης Ευπαθειών (Exploitation)**: Αποτελεί ένα κρίσιμο στάδιο στον έλεγχο διείσδυσης καθώς επικεντρώνεται στο να αξιοποιηθούν οι ευπάθειες που ανακαλύφθηκαν στην προηγούμενη φάση. Κατά τη διάρκεια αυτής της φάσης, οι penetration testers χρησιμοποιούν επίδειξη ευπάθειας (proof of concept) ή επιτυχημένα εκτελέσιμες κώδικες για να επιβεβαιώσουν ότι μπορούν πράγματι να εκμεταλλευτούν τις ευπάθειες. Στόχος είναι η απόκτηση πρόσβασης ή ο έλεγχος του συστήματος. Η διαδικασία εκμετάλλευσης περιλαμβάνει την επιλογή και την εφαρμογή επιθέσεων κατά των ευπαθειών, όπως εκμετάλλευση ελλείψεων ασφάλειας, εκτελέσιμοι κώδικες, ή κοινωνική μηχανική. Κατά την εκμετάλλευση, οι penetration testers συχνά χρησιμοποιούν εργαλεία εκμετάλλευσης ή αναπτύσσουν προσαρμοσμένους κώδικες για να επιτύχουν τους στόχους τους. Επιπλέον, η φάση αυτή είναι σημαντική για την αξιολόγηση του βαθμού επιτυχίας των επιθέσεων και την καταγραφή των αποτελεσμάτων. Η πληροφορία που συλλέγεται από αυτήν τη φάση χρησιμοποιείται στη συνέχεια για την εκπόνηση της τελικής αναφοράς διείσδυσης, καθώς και για την ανάπτυξη συστάσεων ασφάλειας και την βελτίωση των μέτρων προστασίας του συστήματος.

6) **Φάση μετά την Εκμετάλλευση Ευπαθειών (Post Exploitation)**: Αποτελεί μια σημαντική πτυχή του ελέγχου διείσδυσης κατά την οποία οι penetration testers προσπαθούν να διατηρήσουν τον έλεγχο ή την πρόσβαση στα συστήματα που έχουν εισβάλλει. Κατά τη διάρκεια αυτής της φάσης, οι penetration testers εξετάζουν τα συστήματα που έχουν εισβάλει για πιθανές αξιοποιήσεις, εντοπίζουν ευαίσθητες πληροφορίες και προσπαθούν να διατηρήσουν την πρόσβασή τους για μελλοντική χρήση. Αυτό μπορεί να συμπεριλαμβάνει την εγκατάσταση κρυφών θυρών/κερκόπορτες, τη δημιουργία πίσω προσβάσεων, την εξαγωγή ευαίσθητων δεδομένων, την εγκατάσταση κακόβουλου λογισμικού ή τη δημιουργία πίσω πόρτας για μελλοντική πρόσβαση. Οι

penetration testers μπορούν επίσης να προσπαθήσουν να αποκτήσουν πρόσβαση σε ευαίσθητα συστήματα ή δεδομένα, όπως πιστωτικές κάρτες, προσωπικές πληροφορίες, κρυπτονομίσματα κ.λπ., που μπορεί να χρησιμοποιηθούν για απάτη, εκβιασμό ή άλλους εγκληματικούς σκοπούς. Η σωστή αξιοποίηση της φάσης μετά την εκμετάλλευση των ευπαθειών επιτρέπει στους penetration testers να κατανοήσουν και να επιδιώξουν τους στόχους τους πέρα από απλή πρόσβαση. Τέλος, η συλλογή στοιχείων από αυτήν τη φάση είναι ουσιώδης για την παραγωγή μιας ολοκληρωμένης αναφοράς διείσδυσης που παρέχει αναλυτική πληροφόρηση στον πελάτη σχετικά με τις ευπάθειες του συστήματος και τις συστάσεις για βελτίωση της ασφάλειας.

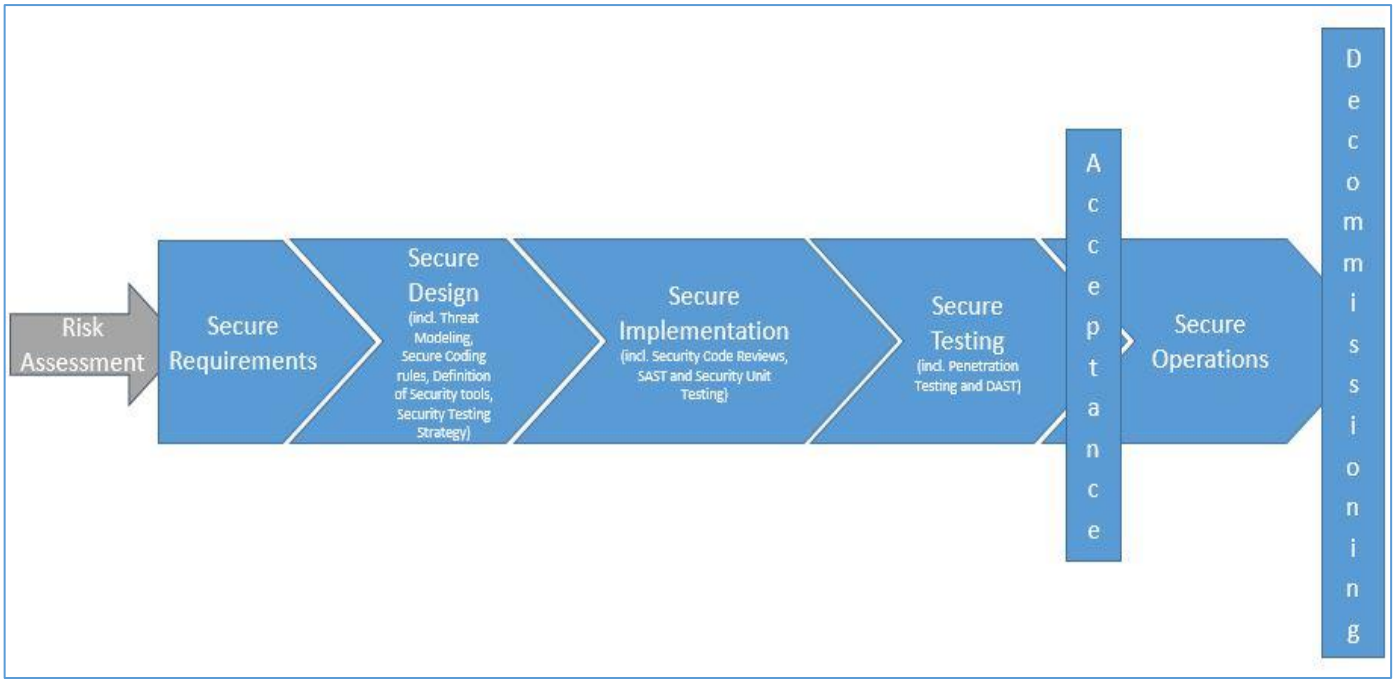
7) **Υποβολή Αναφοράς (Reporting)**: Αποτελεί μια ουσιώδη διαδικασία για την παροχή τεκμηριωμένης ανάλυσης των ευπαθειών και των ευκαιριών βελτίωσης στον πελάτη. Αυτή η φάση είναι κρίσιμη για την επίτευξη των στόχων του ελέγχου διείσδυσης και για τη διασφάλιση της ασφάλειας του συστήματος. Κατά τη φάση αυτή, οι penetration testers συντάσσουν δύο βασικές αναφορές:

   - ✓ **Συνοπτική Αναφορά (Executive Summary):** Παρέχει μια συνοπτική επισκόπηση των ευρημάτων, του επιπέδου κινδύνου και των προτεινόμενων μέτρων για τη βελτίωση της ασφάλειας στον οργανισμό. Απευθύνεται στη διοίκηση (management) και τους ενδιαφερόμενους φορείς λήψης αποφάσεων.
   - ✓ **Τεχνική Αναφορά (Technical Report):** Παρέχει λεπτομερείς πληροφορίες σχετικά με τις ευπάθειες που εντοπίστηκαν, τις εκτιμήσεις κινδύνου και τις συστάσεις για αντιμετώπισή τους. Αυτή η αναφορά απευθύνεται κυρίως στους τεχνικούς και τους ανθρώπους ασφάλειας του οργανισμού και παρέχει τις λεπτομερείς πληροφορίες που απαιτούνται για την αντιμετώπιση των ευπαθειών.

   Και οι δύο αναφορές πρέπει να είναι κατανοητές, σαφείς και ακριβείς, καθώς και να παρέχουν συστάσεις για την αντιμετώπιση των ευπαθειών και τη βελτίωση της ασφάλειας. Η υποβολή αυτών των αναφορών αποτελεί το τελικό στάδιο του ελέγχου διείσδυσης και είναι ουσιώδης για τη διατήρηση της ασφάλειας και της εμπιστοσύνης του πελάτη στον οργανισμό.

1.4.3 OWASP Mobile Security Testing Guide (MSTG)

Το OWASP Mobile Security Testing Guide (MSTG) [5] είναι ένα εκτενές και πολύτιμο εγχειρίδιο που αναπτύχθηκε από τον Οργανισμό Ανοιχτού Κώδικα Ασφάλειας Εφαρμογών Ιστού (OWASP) για την καθοδήγηση επαγγελματιών ασφάλειας σχετικά με τον έλεγχο ασφάλειας σε κινητές εφαρμογές. Το MSTG παρέχει οδηγίες, μεθοδολογίες και εργαλεία για τον έλεγχο και την εξασφάλιση της ασφάλειας σε κινητές εφαρμογές, καλύπτοντας ένα ευρύ φάσμα τεχνικών και απειλών.



Εικόνα 6. Φάσεις OWASP Mobile Security Testing Guide (MSTG)

Πηγή: https://mas.owasp.org/MASTG/General/0x04b-Mobile-App-Security-Testing/

Το εγχειρίδιο αυτό περιλαμβάνει διάφορες ενότητες και κεφάλαια που αναλύουν τις διάφορες πτυχές της ασφάλειας στις κινητές εφαρμογές. Αυτές οι ενότητες περιλαμβάνουν, μεταξύ άλλων:

1) **Εισαγωγή και Ορισμός των Στόχων (Introduction and Objectives):** Σε αυτήν τη φάση θεσμοθετείται ο πλαίσιο για τη διαδικασία δοκιμής, καθορίζοντας τους στόχους, το πεδίο εφαρμογής και τη μεθοδολογία που θα ακολουθηθεί κατά τη διάρκεια των δοκιμών.
2) **Ρύθμιση του Περιβάλλοντος (Environment Setup) :** Πριν από τη διεξαγωγή οποιωνδήποτε δοκιμών, είναι κρίσιμο να διαμορφωθεί σωστά το περιβάλλον δοκιμής. Αυτή η φάση περιλαμβάνει τη ρύθμιση των απαραίτητων εργαλείων, εξομοιωτών, συσκευών και ρυθμίσεων δικτύου για τις δοκιμές.
3) **Βασικές Δοκιμές Ασφάλειας (Basic Security Testing) :** Σε αυτή τη φάση πραγματοποιούνται βασικοί έλεγχοι ασφάλειας στην κινητή εφαρμογή. Αυτό περιλαμβάνει την εξέταση των δικαιωμάτων της εφαρμογής, των πρακτικών αποθήκευσης δεδομένων και των επικοινωνιακών πρακτικών δικτύου.
4) **Δυναμική Ανάλυση (Dynamic Analysis) :** Η δυναμική ανάλυση περιλαμβάνει την εκτέλεση της εφαρμογής σε έναν ελεγχόμενο περιβάλλον για την παρατήρηση της συμπεριφοράς της. Αυτή η φάση περιλαμβάνει δραστηριότητες όπως η διαμόρφωση κατά τη διάρκεια εκτέλεσης, η παρακολούθηση της κίνησης και η αποσφαλμάτωση κατά τη διάρκεια της εκτέλεσης.

5) **Στατική Ανάλυση (Static Analysis) :** Η στατική ανάλυση περιλαμβάνει την εξέταση του πηγαίου κώδικα ή των δυαδικών αρχείων της εφαρμογής χωρίς να τα εκτελέσει. Αυτή η φάση στοχεύει στον εντοπισμό ευπαθειών μέσω της ανάλυσης της δομής του κώδικα της εφαρμογής, των βιβλιοθηκών και των αρχείων διαμόρφωσης της.

6) **Δοκιμές Δικτύου (Network Testing) :** Οι δοκιμές δικτύου επικεντρώνονται στην αξιολόγηση της ασφάλειας της μετάδοσης δεδομένων μεταξύ της κινητής εφαρμογής και των πίσω μελών εξυπηρέτησης. Αυτή η φάση περιλαμβάνει την ανάκτηση και ανάλυση της κίνησης του δικτύου για την εντοπισμό πιθανών θεμάτων ασφαλείας.

7) **Δοκιμές Αποθήκευσης Δεδομένων (Data Storage Testing) :** Αυτή η φάση περιλαμβάνει την εξέταση του τρόπου αποθήκευσης ευαίσθητων δεδομένων τοπικά στη συσκευή. Περιλαμβάνει τον έλεγχο για ανασφαλείς πρακτικές αποθήκευσης δεδομένων, όπως η αποθήκευση ευαίσθητων πληροφοριών σε απλό κείμενο ή σε μη ασφαλή κρυπτογραφημένα μορφή.

8) **Κρυπτογραφία (Cryptography) :** Οι δοκιμές κρυπτογραφίας αξιολογούν την υλοποίηση κρυπτογραφικών αλγορίθμων και τεχνικών εντός της κινητής εφαρμογής. Αυτή η φάση στοχεύει στον εντοπισμό αδυναμιών στην κρυπτογράφηση, την ανάκτηση και τη διαχείριση κλειδιών.

9) **Δοκιμές Ταυτοποίησης (Authentication Testing) :** Οι δοκιμές ταυτοποίησης επικεντρώνονται στην αξιολόγηση της δύναμης και της αποτελεσματικότητας των μηχανισμών ταυτοποίησης της εφαρμογής. Αυτό περιλαμβάνει δοκιμές για κοινές αδυναμίες στην ταυτοποίηση, όπως αδύναμους κωδικούς πρόσβασης, μη ασφαλείς μεθόδους ταυτοποίησης και θέματα διαχείρισης συνεδρίας.

10) **Δοκιμές Εξουσιοδότησης (Authorization Testing) :** Οι δοκιμές εξουσιοδότησης αξιολογούν τους μηχανισμούς ελέγχου πρόσβασης της εφαρμογής. Αυτή η φάση περιλαμβάνει δοκιμές για προνομιακή αύξηση, ανασφαλείς αναφορές αντικειμένων και άλλες εξουσιοδοτικές αδυναμίες.

11) **Ελέγχους Πελάτη (Client-Side Controls Testing) :** Αυτή η φάση επικεντρώνεται στους ελέγχους ασφάλειας πελάτη που υλοποιούνται εντός της κινητής εφαρμογής. Περιλαμβάνει την αξιολόγηση προστασιών εναντίον κοινών επιθέσεων πελάτη, όπως ο έλεγχος εισόδου, οι επιθέσεις εισροής κώδικα και η αντιμετώπιση ευπαθειών δεδομένων.

12) **Ελέγχους Διακομιστή (Server-Side Controls Testing) :** Οι έλεγχοι διακομιστή περιλαμβάνουν την αξιολόγηση της ασφάλειας των πίσω τελών και των API που χρησιμοποιεί η κινητή εφαρμογή. Αυτή η φάση περιλαμβάνει δοκιμές για ευπαθείς εναλλακτικές διεπαφές, μη ασφαλείς σημεία έκθεσης API και ανεπαρκείς ελέγχους διακομιστή.

13) **Δοκιμές Ασφάλειας Επιπέδου Μεταφοράς (Transport Layer Security Testing) :** Οι δοκιμές TLS αξιολογούν την υλοποίηση ασφαλών πρωτοκόλλων επικοινωνίας μεταξύ της κινητής εφαρμογής και των πίσω τελών. Αυτή η φάση

περιλαμβάνει την αξιολόγηση των ρυθμίσεων TLS, τον έλεγχο εγκυρότητας πιστοποιητικών και την ευπάθεια σε επιθέσεις man-in-the-middle.

14) **Αρχιτεκτονική Ασφάλειας (Security Architecture) :** Αυτή η φάση επικεντρώνεται στην αναθεώρηση της συνολικής αρχιτεκτονικής ασφάλειας της κινητής εφαρμογής. Περιλαμβάνει την αξιολόγηση του σχεδιασμού των ελέγχων ασφαλείας, τη μοντελοποίηση των απειλών και τη συμμόρφωση με ασφαλείς πρακτικές κωδικοποίησης.

15) **Δοκιμές Ανθεκτικότητας (Resiliency Testing) :** Οι δοκιμές ανθεκτικότητας αξιολογούν την ανθεκτικότητα της εφαρμογής σε διάφορες απειλές και επιθέσεις ασφάλειας. Αυτή η φάση περιλαμβάνει τη διεξαγωγή δοκιμών διείσδυσης, σάρωση ευπαθειών και δοκιμές φόρτωσης για την αξιολόγηση της ικανότητας της εφαρμογής να αντιστέκεται σε επιθέσεις και να διατηρεί τη λειτουργικότητά της σε δυσμενείς συνθήκες.

16) **Αναφορά και Αντιμετώπιση (Reporting and Remediation) :** Η τελική φάση περιλαμβάνει την τεκμηρίωση των ευρημάτων της διαδικασίας δοκιμής ασφάλειας και την παροχή προτάσεων για την αντιμετώπισή τους. Αυτό περιλαμβάνει την προετοιμασία λεπτομερών αναφορών, την κατάταξη των ευπαθειών με βάση το βαθμό σοβαρότητας και τη συνεργασία με τους ενδιαφερόμενους φορείς για την αντιμετώπιση των θεμάτων ασφαλείας αποτελεσματικά.

1.4.4 MITRE ATT&CK Framework

Το MITRE ATT&CK Framework [6] είναι ένα σύστημα γνώσης που περιέχει τεχνικές και τακτικές που χρησιμοποιούν στις κυβερνοεπιθέσεις. Ο όρος "ATT&CK" αναφέρεται στις "Adversarial Tactics, Techniques, and Common Knowledge". Το πλαίσιο παρέχει έναν οργανωμένο και δομημένο τρόπο για την καταγραφή των τεχνικών που χρησιμοποιούν επιθέσεις από κυβερνοεχθρούς, βασισμένο σε παρατηρήσεις από τον πραγματικό κόσμο. Το MITRE ATT&CK Framework δεν ορίζει αυστηρά φάσεις, αλλά παρέχει μια κατανομή των τακτικών και τεχνικών που χρησιμοποιούν οι επιτιθέμενοι κατά την διάρκεια μιας επίθεσης. Ωστόσο, μπορούμε να ομαδοποιήσουμε τις τεχνικές σε γενικές φάσεις που σχετίζονται με τις ενέργειες που λαμβάνονται από τον επιτιθέμενο κατά τη διάρκεια μιας επίθεσης. Αυτές οι φάσεις μπορεί να είναι:

1) **Αρχική Πρόσβαση (Initial Access):** Ο επιτιθέμενος αρχικά εισέρχεται στο σύστημα ή το δίκτυο του θύματος. Αυτό μπορεί να γίνει μέσω phishing emails, εκμετάλλευσης ευπαθειών στο λογισμικό, εκμετάλλευσης αδυναμιών στο δίκτυο κ.λπ.

2) **Εκτέλεση (Execution):** Ο επιτιθέμενος εκτελεί κώδικα στο σύστημα ή το δίκτυο του θύματος για να επιτύχει τους στόχους του. Αυτό μπορεί να περιλαμβάνει την εκτέλεση κακόβουλου λογισμικού ή εντολών.

3) **Απόκτηση Δικαιωμάτων (Privilege Escalation):** Ο επιτιθέμενος αποκτά επιπλέον δικαιώματα στο σύστημα ή το δίκτυο για να επιτελέσει περαιτέρω επιθέσεις ή να παραμείνει απαρατήρητος.

4) **Επέκταση Δικαιωμάτων (Lateral Movement):** Ο επιτιθέμενος κινείται οριζόντια στο δίκτυο του θύματος, εξερευνώντας και εκμεταλλευόμενος πιθανά ευπαθή σημεία για να κερδίσει πρόσβαση σε άλλα συστήματα ή υπηρεσίες.

5) **Κρυπτογράφηση Δεδομένων (Data Encryption):** Ο επιτιθέμενος κρυπτογραφεί τα δεδομένα για να δυσκολέψει την ανίχνευση ή την ανάκτησή τους από τους υπεύθυνους ασφάλειας.

6) **Κατακερματισμός Ιχνών (Defense Evasion):** Ο επιτιθέμενος προσπαθεί να αποφύγει την ανίχνευση ή τον αποκλεισμό από τα συστήματα ασφαλείας του θύματος.

7) **Ανακάλυψη (Discovery):** Ο επιτιθέμενος ανιχνεύει το περιβάλλον του θύματος για να κατανοήσει τη διαμόρφωση του, τις αδυναμίες του και τις πιθανές ευκαιρίες επίθεσης.

8) **Κλοπή Δεδομένων (Exfiltration):** Ο επιτιθέμενος κλέβει ευαίσθητα δεδομένα από το σύστημα ή το δίκτυο του θύματος για να τα χρησιμοποιήσει ή να τα πωλήσει σε επόμενες φάσεις της επίθεσης.

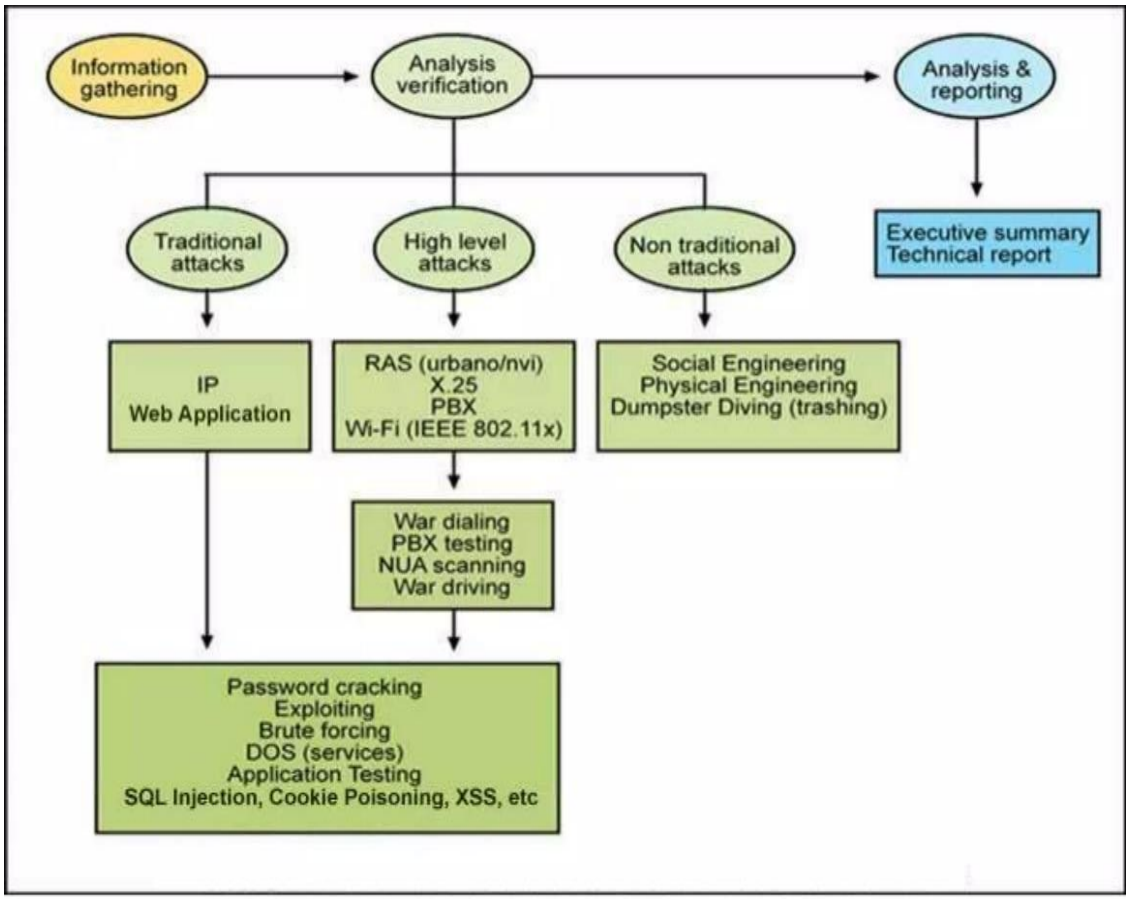
Εικόνα 7. Φάσεις MITRE ATT&CK Framework

Πηγή: https://www.blackberry.com/us/en/solutions/endpoint-security/mitre-attack

1.4.5 Open-Source Security Testing Methodology Manual (OSSTMM)

Το OSSTMM (Open-Source Security Testing Methodology Manual) [7] είναι ένα πρότυπο μεθοδολογίας δοκιμών ασφάλειας που δημιουργήθηκε από το Institute for Security and Open Methodologies (ISECOM). Αποτελεί ένα ανοιχτό πρότυπο, δηλαδή είναι διαθέσιμο για ελεύθερη χρήση και αναδιανομή, προωθώντας την ανοιχτή προσέγγιση στις δοκιμές ασφάλειας.

Το OSSTMM περιλαμβάνει ένα σύνολο μεθόδων και τεχνικών που χρησιμοποιούνται για τη διεξαγωγή δοκιμών ασφαλείας σε διάφορα συστήματα και εφαρμογές. Στόχος του είναι να παρέχει ένα ολοκληρωμένο πλαίσιο για την αξιολόγηση της ασφάλειας συστημάτων, καθορίζοντας προσεκτικά τις διαδικασίες δοκιμών και τις τεχνικές που πρέπει να ακολουθηθούν.



Εικόνα 8. Φάσεις OSSTMM

Πηγή: https://www.slideshare.net/DSS_ITSEC/proactive-security-the-opensource-security-testing-methodology-manual-osstmm-from-isecom

Το OSSTMM (Open Source Security Testing Methodology Manual) περιλαμβάνει τις ακόλουθες φάσεις:

1) **Προετοιμασία (Preparation):** Αυτή η φάση περιλαμβάνει την οριοθέτηση του στόχου του τεστ, του εύρους του, και την ανάπτυξη μιας στρατηγικής για το πώς θα διεξαχθεί το τεστ.

2) **Συλλογή Πληροφοριών (Information Gathering):** Σε αυτή τη φάση, συγκεντρώνονται πληροφορίες για τον στόχο του τεστ, όπως πληροφορίες για το δίκτυο, τα συστήματα, τις εφαρμογές, κλπ.
3) **Ανάλυση (Analysis):** Κατά τη φάση αυτή, οι συλλεγμένες πληροφορίες αναλύονται για να κατανοήσουν καλύτερα οι δοκιμαστές το περιβάλλον και τις πιθανές ευπάθειες.
4) **Επίθεση (Attack):** Σε αυτή τη φάση, οι δοκιμαστές πραγματοποιούν επιθέσεις και εκμεταλλεύονται τις ευπάθειες που ανακαλύφθηκαν κατά τη διάρκεια των προηγούμενων φάσεων.
5) **Ελέγχους (Controls):** Σε αυτή τη φάση, εξετάζονται οι έλεγχοι ασφαλείας που υπάρχουν στο σύστημα για να διαπιστωθεί αν είναι αποτελεσματικοί.
6) **Αναφορά (Reporting):** Σε αυτή τη φάση, παρουσιάζεται μια ολοκληρωμένη αναφορά των ευρημάτων του τεστ, συμπεριλαμβανομένων των ευπαθειών που εντοπίστηκαν και των προτεινόμενων μέτρων ασφαλείας.

1.4.6 Information Systems Security Assessment Framework (ISSAF)

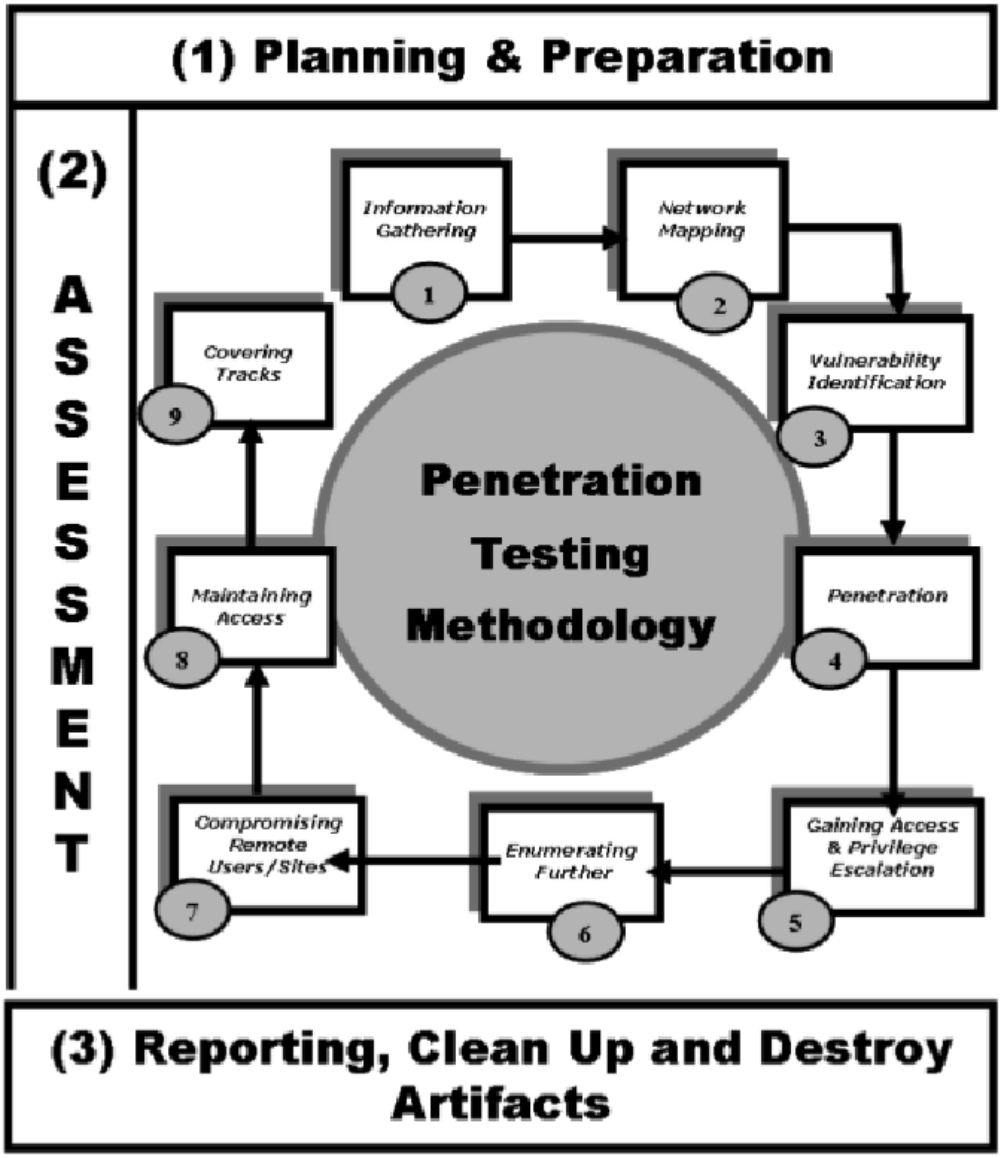
Το Πλαίσιο Αξιολόγησης Ασφάλειας Πληροφοριακών Συστημάτων (ISSAF) [8] είναι ένα ολοκληρωμένο εργαλείο για την αξιολόγηση και ενίσχυση της ασφάλειας πληροφοριακών συστημάτων. Παρέχει μια δομημένη διαδικασία που περιλαμβάνει τις εξής φάσεις αξιολόγησης :

Φάση 1: Σχεδιασμός και Προετοιμασία: Στη φάση του σχεδιασμού και της προετοιμασίας, ορίζονται οι στόχοι και το εύρος της αξιολόγησης ασφαλείας. Περιλαμβάνει την ανάλυση των αναγκών του οργανισμού, την κατανόηση του περιβάλλοντος, τον καθορισμό των προτεραιοτήτων και την εξασφάλιση των απαραίτητων πόρων και εργαλείων για την εκτέλεση της αξιολόγησης. Η προσεκτική προετοιμασία εξασφαλίζει ότι η αξιολόγηση θα είναι αποδοτική και στοχευμένη.

Φάση 2: Αξιολόγηση: Η φάση της αξιολόγησης περιλαμβάνει την εκτέλεση των δοκιμών ασφαλείας, όπως οι σαρώσεις ευπαθειών και οι δοκιμές διείσδυσης. Κατά τη διάρκεια αυτής της φάσης, οι αναλυτές ασφαλείας χρησιμοποιούν διάφορα εργαλεία και τεχνικές για την ταυτοποίηση αδυναμιών και την αξιολόγηση της ανθεκτικότητας των πληροφοριακών συστημάτων απέναντι σε πιθανές απειλές. Τα ευρήματα καταγράφονται λεπτομερώς για περαιτέρω ανάλυση.

Φάση 3: Υποβολή αναφοράς, καθαρισμός ιχνών και καταστροφή ευρημάτων: Στην τελική φάση, οι αναλυτές συντάσσουν αναλυτικές αναφορές με τα αποτελέσματα της αξιολόγησης, τις προτεραιότητες των ευπαθειών και τις προτάσεις για διορθωτικές ενέργειες. Επίσης, περιλαμβάνεται η διαδικασία καθαρισμού ιχνών για να εξασφαλιστεί ότι δεν υπάρχουν υπολείμματα της αξιολόγησης που θα μπορούσαν να εκτεθούν σε μη εξουσιοδοτημένα άτομα. Τέλος, τα ευρήματα και τα δεδομένα της

αξιολόγησης καταστρέφονται με ασφάλεια για την προστασία των ευαίσθητων πληροφοριών του οργανισμού.



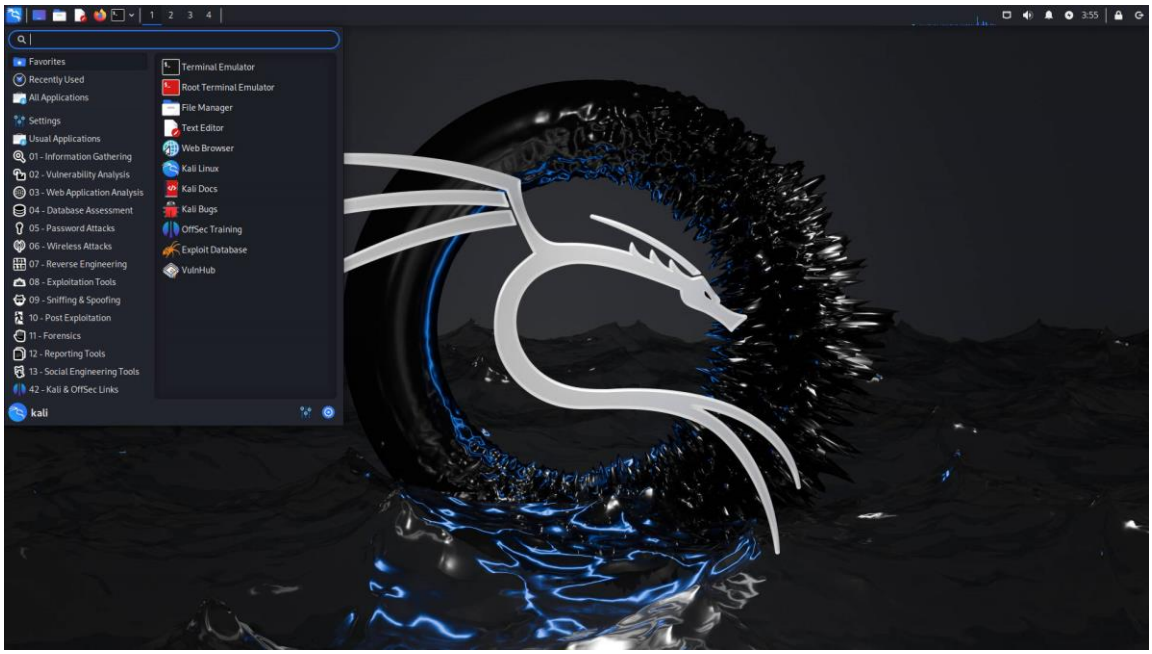
Εικόνα 9. Information Systems Security Assessment Framework (ISSAF)

Πηγή : https://www.semanticscholar.org/paper/Towards-a-practical-and-effective-security-testing-Prandini-Ramilli/cb223c1cfbbcef98a359cc5930e628a7f69476cf/figure/0

2. ΕΡΓΑΛΕΙΑ ΕΛΕΓΧΟΥ ΤΡΩΤΟΤΗΤΑΣ & ΑΞΙΟΛΟΓΗΣΗΣ ΕΥΠΑΘΕΙΩΝ

Η πιο διαδεδομένη διανομή Linux είναι το Kali Linux [10] που σχεδιάστηκε ειδικά για τον χώρο της κυβερνοασφάλειας και των δοκιμών διείσδυσης και πάνω σε αυτή θα αναπτύξουμε στη συνέχεια την μελέτη περίπτωσης. Το Kali Linux βασίζεται στο Debian και αποτελεί την εξέλιξη του προηγούμενου εργαλείου της Offensive Security, του BackTrack. Η πρώτη έκδοση του Kali Linux κυκλοφόρησε τον Μάρτιο του 2013 και από τότε έχει αναπτυχθεί σημαντικά, ενσωματώνοντας χιλιάδες εργαλεία που καλύπτουν ευρύ φάσμα αναγκών ασφάλειας, όπως δοκιμές διείσδυσης, ανάλυση ευπαθειών, ψηφιακή εγκληματολογία και πολλά άλλα.

Η βασική ιδέα πίσω από το Kali Linux είναι να παρέχει ένα περιβάλλον που είναι πλήρως εξοπλισμένο με εργαλεία και εφαρμογές που χρησιμοποιούνται για τεστ ασφάλειας, εκτέλεση επιθέσεων και αξιολόγηση ευπάθειας. Αυτό σημαίνει ότι περιλαμβάνει μια ευρεία γκάμα εργαλείων, όπως σαρωτές ασφαλείας, εργαλεία για κρυπτογραφία, ανάκτηση κωδικών, εργαλεία για την εκμάθηση και την εκτέλεση επιθέσεων, κ.λπ. Η κοινότητα του Kali Linux αποτελείται από επαγγελματίες κυβερνοασφάλειας, ερευνητές ασφάλειας και ερασιτέχνες που ασχολούνται με τον τομέα της ασφάλειας των πληροφοριών.



Εικόνα 10. Kali Linux

Πηγή : https://www.kali.org/

Τα **εργαλεία ελέγχου τρωτότητας και αξιολόγησης ευπαθειών** είναι λογισμικά ή εργαλεία που χρησιμοποιούνται για να εντοπίσουν πιθανές ευπάθειες σε ένα σύστημα ή μια εφαρμογή. Τα εργαλεία αυτά είναι ευρέως χρησιμοποιούμενα από

επαγγελματίες κυβερνοασφάλειας και ερευνητές ασφάλειας προκειμένου να αξιολογήσουν την ασφάλεια ενός συστήματος και να εντοπίσουν πιθανά σημεία εισβολής. Αυτά τα εργαλεία μπορεί να περιλαμβάνουν:

2.1 Information Gathering (Συλλογή Πληροφοριών)

Αφορά τη διαδικασία συλλογής δεδομένων και πληροφοριών σχετικά με έναν στόχο, όπως δίκτυα, συστήματα, εφαρμογές ή οργανισμούς, πριν από την εκτέλεση μιας αξιολόγησης ασφαλείας ή μιας επίθεσης. Αυτή η φάση είναι θεμελιώδης για την κατανόηση της δομής, των υπηρεσιών, των ευπαθειών και των πιθανών σημείων εισόδου ενός στόχου. Η αποτελεσματική συλλογή πληροφοριών επιτρέπει στους αναλυτές ασφαλείας και στους ηθικούς χάκερ να αναπτύξουν μια ολοκληρωμένη στρατηγική για την περαιτέρω αξιολόγηση και την αντιμετώπιση των κινδύνων ασφαλείας.

Το **Nmap** [11] είναι ένα πολύ δημοφιλές εργαλείο ανοικτού κώδικα για σάρωση δικτύων και εντοπισμό ασφαλείας. Ο όρος Nmap προέρχεται από τον όρο "Network Mapper". Χρησιμοποιείται κυρίως από επαγγελματίες ασφαλείας, διαχειριστές συστημάτων και δικτύων για να εξετάζουν και να αναλύουν το δίκτυό τους.

Εικόνα 11. Βασικές εντολές Nmap

Πηγή : https://www.linkedin.com/pulse/essential-nmap-cheat-sheet-quick-reference-natan-morette-kjonf/

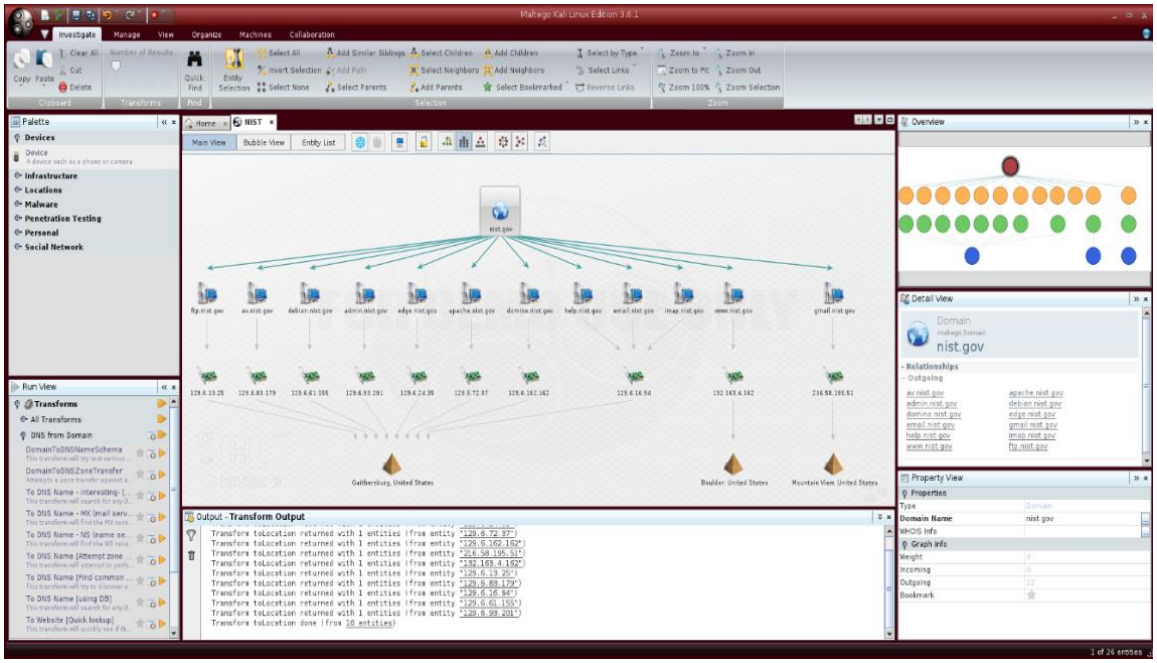
Το Nmap μπορεί να εκτελέσει ποικίλες εργασίες σάρωσης δικτύου, συμπεριλαμβανομένης της εντοπιστικής πληροφορίας για τους υπολογιστές σε ένα δίκτυο, των ανοιχτών θυρών, των υπηρεσιών που εκτελούνται σε αυτές τις θύρες, και άλλων ευπαθειών του συστήματος. Μπορεί επίσης να αναγνωρίσει το λειτουργικό σύστημα που τρέχει σε έναν συγκεκριμένο υπολογιστή στο δίκτυο.

Οι δυνατότητες του Nmap το καθιστούν ιδιαίτερα χρήσιμο εργαλείο για τον εντοπισμό ευπαθειών στο δίκτυο, την εκτίμηση της ασφάλειας των συστημάτων και τον εντοπισμό πιθανών σημείων εισόδου για επιθέσεις.

Το **Maltego** [12] είναι ένα λογισμικό που χρησιμοποιείται για την εκτέλεση αναζητήσεων και αναλύσεων επιθέσεων στον τομέα της κυβερνοασφάλειας και της ερευνητικής εργασίας. Κατασκευάστηκε από την εταιρεία Paterva και επιτρέπει στους χρήστες να διερευνήσουν σχέσεις μεταξύ διαφόρων οντοτήτων σε ένα δίκτυο.

Το Maltego λειτουργεί με τη χρήση δεδομένων που είναι διαθέσιμα δημόσια, όπως πληροφορίες WHOIS, διευθύνσεις IP, ονόματα domain, δεδομένα από κοινωνικά δίκτυα και πολλά άλλα. Οι χρήστες μπορούν να εκτελούν γραφικές αναζητήσεις και να οπτικοποιούν τις σχέσεις μεταξύ διαφόρων οντοτήτων με τη χρήση γραφικών γραφημάτων και διαγραμμάτων.

Ακόμα είναι χρήσιμο για ερευνητές ασφαλείας και επαγγελματίες κυβερνοασφάλειας που χρειάζονται ένα εργαλείο για την ανάλυση των συνδέσεων και των σχέσεων σε ένα δίκτυο, προκειμένου να εντοπίσουν ευπαθείς πόρους ή να προβλέψουν πιθανές επιθέσεις.



Εικόνα 12. Διάγραμμα χρήσης του Maltego

Πηγή : https://spreadsecurity.github.io/2016/09/03/open-source-intelligence-with-maltego.html

2.2 Vulnerability Analysis Tools (Εργαλεία Ανάλυσης Ευπαθειών)

Αποτελούν ένα σημαντικό κομμάτι της εργαλειοθήκης ενός ειδικού ασφάλειας πληροφοριών. Αυτά τα εργαλεία επιτρέπουν την ανίχνευση και την ανάλυση ευπαθειών σε δίκτυα, συστήματα και εφαρμογές, προκειμένου να εντοπιστούν πιθανά σημεία εισβολής και παραβιάσεων ασφάλειας. Αυτά τα εργαλεία εκτελούν αυτόματες σαρώσεις στις υποδομές και τα συστήματα, εντοπίζοντας γνωστές ευπάθειες, εσφαλμένες ρυθμίσεις και αδυναμίες ασφάλειας. Στη συνέχεια, παρέχουν έναν

κατάλογο με πιθανές ευπάθειες, συχνά με περιγραφή και συστάσεις για διορθώσεις. Με τη χρήση αυτών των εργαλείων, οι ειδικοί ασφάλειας μπορούν να αξιολογήσουν και να βελτιώσουν την ασφάλεια των συστημάτων και των εφαρμογών, μειώνοντας έτσι τον κίνδυνο πιθανών επιθέσεων και διαρροών δεδομένων.

Το **SQLMap** [23] είναι ένα δημοφιλές εργαλείο ασφαλείας λογισμικού που χρησιμοποιείται για την ανίχνευση και την εκμετάλλευση ευπαθειών SQL injection σε ιστοσελίδες και εφαρμογές. Το SQL injection είναι μια επίθεση που εκμεταλλεύεται αδυναμίες στην επεξεργασία εισόδων SQL από μια εφαρμογή, επιτρέποντας στον επιτιθέμενο να εκτελέσει κακόβουλες SQL εντολές στη βάση δεδομένων της εφαρμογής.

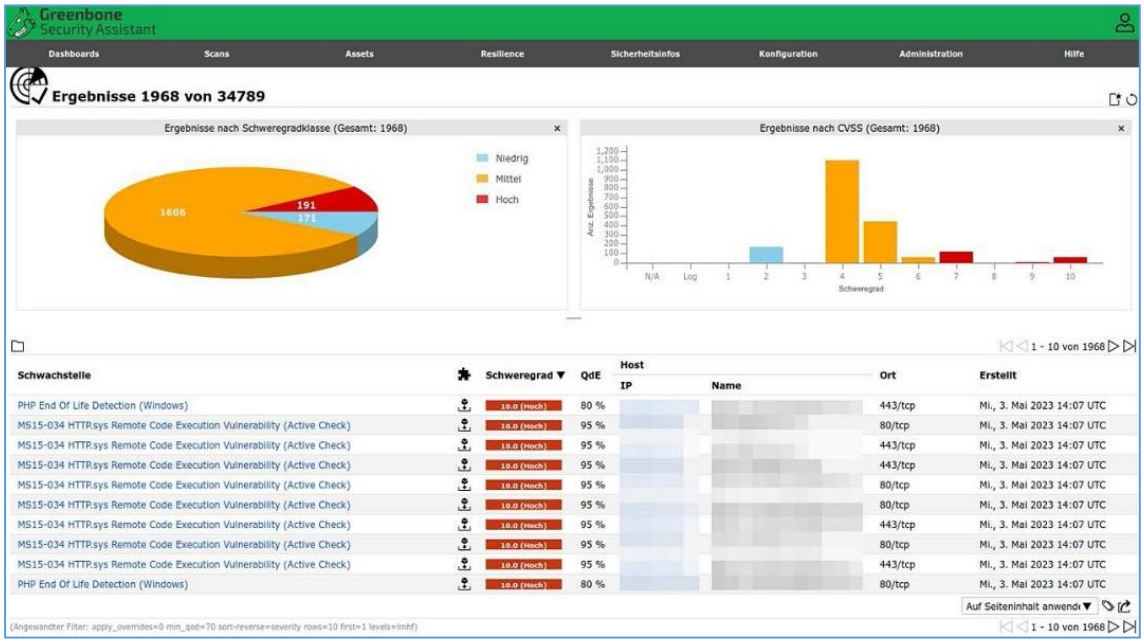
Το SQLMap αναλαμβάνει την αυτοματοποιημένη διερεύνηση μιας ιστοσελίδας για πιθανές ευπάθειες SQL injection, αναλύοντας την δομή της βάσης δεδομένων και εκτελώντας αυτόματα επιθέσεις SQL injection. Το εργαλείο είναι εξαιρετικά ισχυρό και παρέχει πολλές επιλογές για προσαρμογή και εκτέλεση διαφόρων ειδών επιθέσεων SQL injection, συμπεριλαμβανομένων της εξόρυξης δεδομένων, της αναζήτησης και της αξιολόγησης ευπαθειών, καθώς και της αυτοματοποιημένης εκμετάλλευσής τους.

Εικόνα 24. Παράδειγμα χρήσης SQL Map

Πηγή : https://github.com/sqlmapproject/sqlmap/wiki/Screenshots

Το **OpenVAS** [9] (Open Vulnerability Assessment System) είναι ένα εργαλείο ανοικτού κώδικα για την ανίχνευση και αξιολόγηση ευπαθειών σε δικτυακά συστήματα

και εφαρμογές. Χρησιμοποιείται από επαγγελματίες της ασφάλειας πληροφορικής για να εντοπίζουν και να διαχειρίζονται τυχόν ευπάθειες στα δίκτυά τους. Προσφέρει δυνατότητες σάρωσης ευπαθειών, διαχείρισης ευπαθειών και ενημερώσεις ασφαλείας μέσω του feed των NVTs (Network Vulnerability Tests). Χρησιμοποιείται για εσωτερικούς και εξωτερικούς ελέγχους ασφαλείας, συμμόρφωση με κανονισμούς, ανάλυση κινδύνων, και προσφέρει αναλυτικές αναφορές και δυνατότητες παρακολούθησης. Είναι μέρος του Greenbone Vulnerability Management (GVM), προσφέροντας μια ολοκληρωμένη λύση για τη διαχείριση ευπαθειών, και είναι δημοφιλές τόσο σε επαγγελματίες ασφαλείας όσο και σε ερευνητές λόγω της αποτελεσματικότητάς του και της δυνατότητάς του να προσαρμόζεται σε διαφορετικές ανάγκες ασφάλειας.

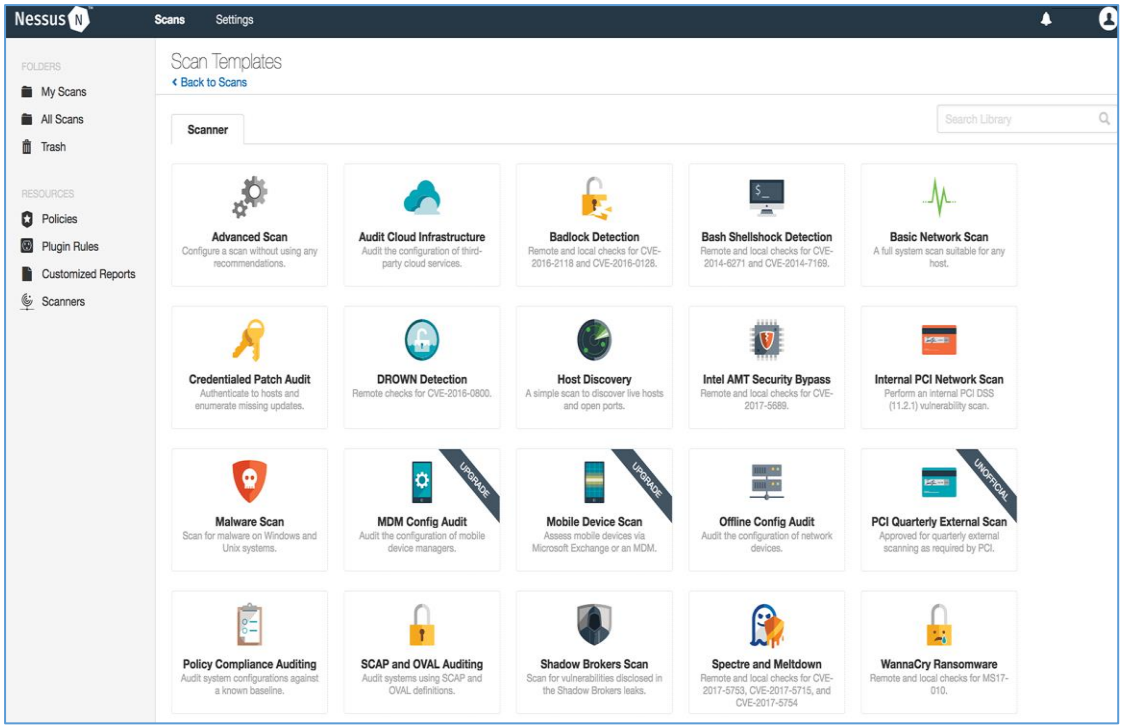


Εικόνα 11. OpenVAS

Πηγή : https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Freie-Software/Tools/OpenVAS/OpenVAS_node.html

Το **Nessus** [14] είναι ένα δημοφιλές εργαλείο αξιολόγησης ευπαθειών (vulnerability assessment tool) που χρησιμοποιείται για τον έλεγχο ασφάλειας συστημάτων και δικτύων. Αναπτύχθηκε από την εταιρεία Tenable και παρέχει μια πληθώρα εργαλείων για τον εντοπισμό, την αξιολόγηση και τη διαχείριση ευπαθειών σε συστήματα και δίκτυα. Οι βασικές λειτουργίες του Nessus περιλαμβάνουν τη σάρωση των συστημάτων για τον εντοπισμό πιθανών ευπαθειών, την ανάλυση αποτελεσμάτων, την παροχή συστάσεων για διορθώσεις και τη δημιουργία αναφορών ασφάλειας. Το Nessus υποστηρίζει τη σάρωση για διάφορες κατηγορίες ευπαθειών, συμπεριλαμβανομένων των ευπαθειών λογισμικού, ευπαθειών λειτουργικού συστήματος, ανεπιθύμητης λογισμικού και πολλών άλλων. Οι εκδόσεις του Nessus ποικίλλουν από δωρεάν έκδοση (Nessus Essentials) με περιορισμένες δυνατότητες έως επαγγελματικές και επιχειρησιακές εκδόσεις με προηγμένες λειτουργίες και

υποστήριξη. Το Nessus είναι ένα από τα πιο δημοφιλή εργαλεία αξιολόγησης ευπαθειών και χρησιμοποιείται ευρέως από επαγγελματίες ασφαλείας πληροφοριών και διαχειριστές συστημάτων για την προστασία των δικτύων και των συστημάτων τους από επιθέσεις και ευπάθειες.



Εικόνα 12. Nessus Scan Templates

Πηγή : https://www.tenable.com/

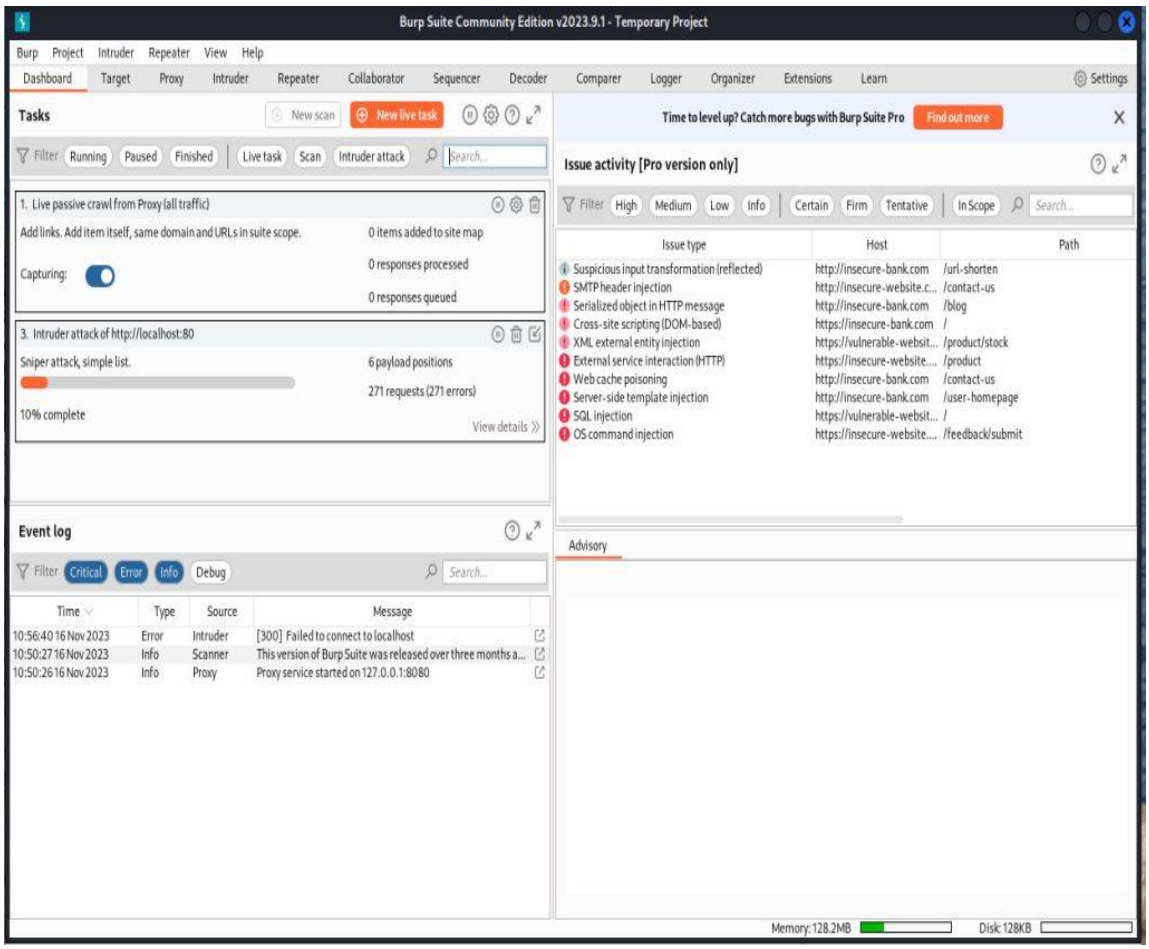
2.3 Web Application Analysis Tools (Εργαλεία Ανάλυσης Εφαρμογών Ιστού)

Τα εργαλεία ανάλυσης εφαρμογών ιστού (Web Application Analysis Tools) αποτελούν ένα σημαντικό κομμάτι της εργαλειοθήκης ασφαλείας για επαγγελματίες ασφάλειας πληροφοριακών συστημάτων και εθελοντές ηθικούς χάκερ. Αυτά τα εργαλεία επιτρέπουν την εκτεταμένη ανάλυση των διαδικτυακών εφαρμογών προκειμένου να εντοπιστούν πιθανές ευπάθειες και αδυναμίες ασφαλείας.

Το **BurpSuite** [15] είναι ένα εργαλείο από την εταιρεία Portswigger το οποίο ειδικεύεται στις δοκιμές ασφάλειας διαδικτυακών εφαρμογών και διατίθεται σε δύο εκδόσεις, την community edition και την pro edition. Το BurpSuite προσφέρει ένα φιλικό γραφικό περιβάλλον και μια μεγάλη γκάμα από αυτοματισμούς που επιτρέπουν τη δοκιμή διαφόρων ευπαθειών σε ιστοσελίδες.

Ένα από τα ισχυρά σημεία του BurpSuite είναι η δυνατότητα να λειτουργεί ως "man in the middle" και να καταγράφει την επικοινωνία μεταξύ του προγράμματος περιήγησης και του διακομιστή. Αυτό επιτρέπει την ανάλυση των δεδομένων που ανταλλάσσονται και τη δοκιμή για ευπάθειες στις εφαρμογές.

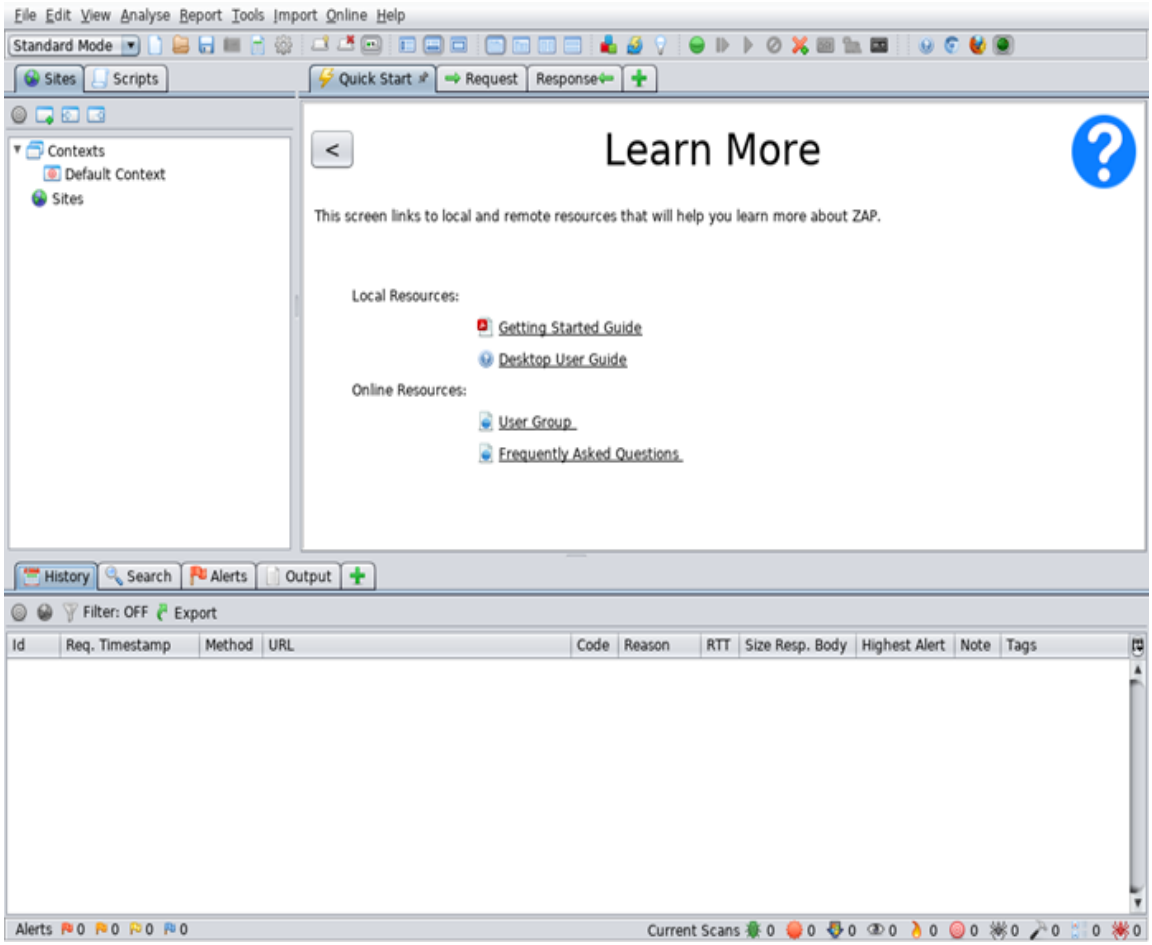
Επιπλέον, το BurpSuite περιλαμβάνει πολλές επιλογές που είναι χρήσιμες για penetration testers και καθιστούν το εργαλείο αυτό ένα από τα καταλληλότερα για δοκιμές διαδικτυακών εφαρμογών.



Εικόνα 13. Περιβάλλον Burp Suite

Πηγή : https://thenewstack.io/pentest-your-web-apps-with-burp-suite-on-kali-linux/

Το **OWASP ZAP** [11] είναι ένα εργαλείο ασφάλειας λογισμικού ανοικτού κώδικα που χρησιμοποιείται για την εντοπισμό ασφαλείας εφαρμογών. Είναι ένα από τα δημοφιλέστερα εργαλεία ασφαλείας εφαρμογών στην κοινότητα ασφάλειας πληροφοριών. Προσφέρει διάφορες λειτουργίες, συμπεριλαμβανομένης της εντοπισμού ευπαθειών ασφαλείας σε ιστοσελίδες και εφαρμογές, όπως επίθεση SQL injection, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), και πολλές άλλες. Επιπλέον, μπορεί να χρησιμοποιηθεί για τον έλεγχο ασφάλειας API. Οι χρήστες μπορούν να χρησιμοποιήσουν το OWASP ZAP είτε μέσω του γραφικού περιβάλλοντος χρήστη (GUI) είτε μέσω της προγραμματιστικής διεπαφής εντολών (API) για αυτοματοποίηση διαδικασιών ελέγχου ασφάλειας.

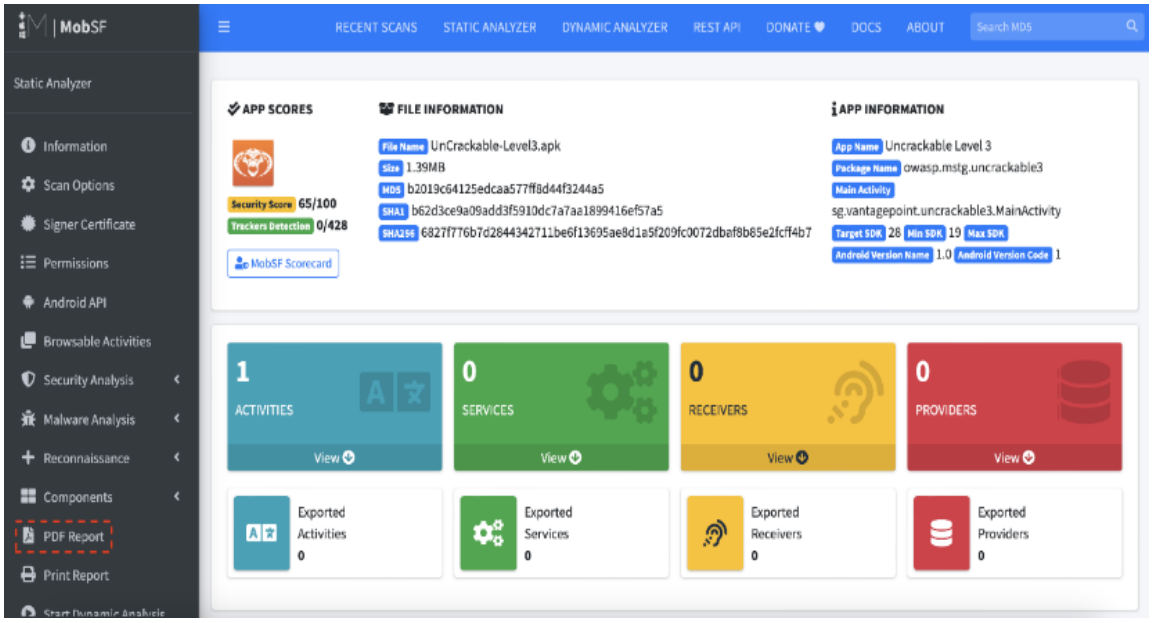


Εικόνα 14. Γραφικό περιβάλλον OWASP ZAP (Zed Attack Proxy)

Πηγή : https://www.zaproxy.org/getting-started/#overview

Το MOSBF [17] (Εργαλείο Ανίχνευσης Πληροφοριών Εφαρμογής είναι ένα εργαλείο λογισμικού ανοικτού κώδικα που χρησιμοποιείται για τη σάρωση και τον έλεγχο ασφαλείας εφαρμογών. Στόχος του είναι να εντοπίζει ευπαθείς πόρους σε εφαρμογές και ιστοσελίδες, όπως ανοιχτές πόρτες, ευπαθείς υπηρεσίες, αδυναμίες αυθεντικοποίησης και άλλες πιθανές ευπάθειες ασφαλείας.

Το MOSBF είναι ειδικά σχεδιασμένο για να επικεντρώνεται σε εφαρμογές που χρησιμοποιούνται σε διάφορα περιβάλλοντα, όπως διακομιστές, βάσεις δεδομένων, και άλλα συστήματα. Χρησιμοποιείται συνήθως από ερευνητές ασφαλείας και επαγγελματίες κυβερνοασφάλειας για την εντοπισμό πιθανών αδυναμιών σε εφαρμογές και δικτυακά συστήματα, προκειμένου να βελτιώσουν την ασφάλεια των πληροφοριών και να προστατεύσουν τα συστήματά τους από πιθανές επιθέσεις.



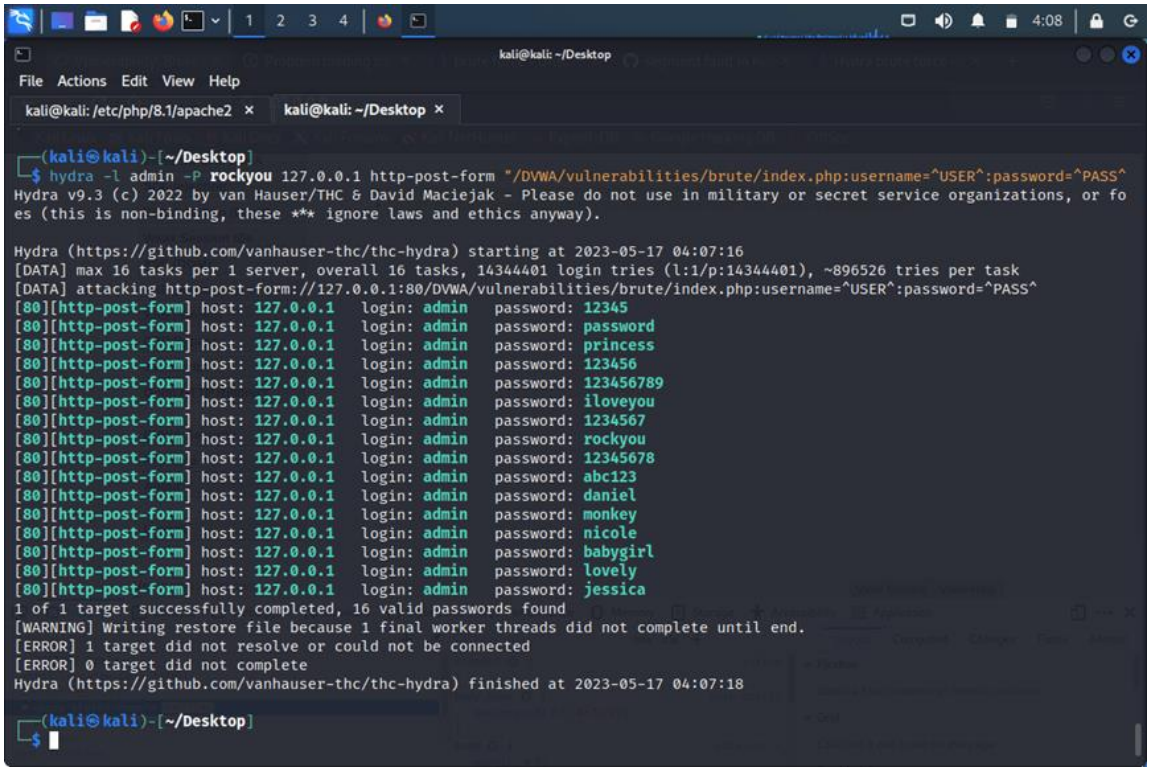
Εικόνα 15. Ανάλυση ασφαλείας με το MOSBF

Πηγή : https://support.corellium.com/integrations/mobsf

2.4 Password Attacks Tools (Εργαλεία Επίθεσης Κωδικών Πρόσβασης)

Τα εργαλεία επιθέσεων κωδικών πρόσβασης (Password Attacks Tools) αποτελούν ένα σημαντικό σύνολο εργαλείων που χρησιμοποιούνται στον χώρο της κυβερνοασφάλειας για τη δοκιμή της ανθεκτικότητας των συστημάτων και των εφαρμογών στις επιθέσεις που στοχεύουν στην παράνομη πρόσβαση σε προστατευμένους λογαριασμούς. Αυτά τα εργαλεία είναι εξειδικευμένα στην ανάλυση και αποκρυπτογράφηση κωδικών πρόσβασης, χρησιμοποιώντας διάφορες τεχνικές όπως η λεξική επίθεση, η επίθεση με βάση τον κανόνα, και η επίθεση μέσω Brute Force. Με τη χρήση των εργαλείων επιθέσεων κωδικών πρόσβασης, οι επαγγελματίες ασφαλείας και ηθικοί χάκερ μπορούν να αξιολογήσουν την ανθεκτικότητα των συστημάτων, να ανιχνεύσουν τυχόν αδυναμίες στην ασφάλεια των κωδικών πρόσβασης και να λάβουν τα απαραίτητα μέτρα για την ενίσχυση της προστασίας των προσβάσεων. Ωστόσο, είναι σημαντικό να σημειωθεί ότι η χρήση αυτών των εργαλείων πρέπει να γίνεται με ηθικούς και νόμιμους τρόπους, με τη συναίνεση και την έγκριση των ενδιαφερομένων για την εκτέλεση των δοκιμών ασφαλείας.

Το **Hydra** [12] είναι ένα εργαλείο ανοιχτού κώδικα για επίθεση Brute Force, που χρησιμοποιείται για την εύρεση κωδικών πρόσβασης μέσω επαναλαμβανόμενων προσπαθειών. Το Hydra είναι ένα από τα πιο δημοφιλή εργαλεία στην κοινότητα της κυβερνοασφάλειας και χρησιμοποιείται ευρέως για δοκιμές ελέγχου ασφαλείας συστημάτων. Με το Hydra, μπορείς να εκτελέσεις επιθέσεις Brute Force σε πρωτόκολλα όπως HTTP, FTP, SMTP, MySQL, SSH και πολλά άλλα. Το εργαλείο υποστηρίζει πολλές μορφές επιθέσεων, συμπεριλαμβανομένης της επίθεσης με λεξικό, της επίθεσης με λίστα πιθανών κωδικών, και άλλες παραλλαγές.



Εικόνα 16. Brute-Force Attack με το Hydra

Πηγή : https://www.stationx.net/how-to-use-hydra/

2.5 Wireless Attacks Tools (Εργαλεία Ασύρματων Επιθέσεων)

Η κατηγορία εργαλείων "Wireless Attacks" αναφέρεται σε μια συλλογή εργαλείων που χρησιμοποιούνται για επιθέσεις κατά ασύρματων δικτύων. Αυτά τα εργαλεία είναι σχεδιασμένα για να επιτρέπουν σε ειδικούς ασφάλειας και ερευνητές να εξετάσουν την ασφάλεια των ασύρματων δικτύων, να εντοπίσουν ευπάθειες και να δοκιμάσουν τις αντίστοιχες επιθέσεις για να βελτιώσουν την ασφάλεια τους.

Αυτά τα εργαλεία μπορούν να περιλαμβάνουν διάφορες λειτουργίες όπως η εντοπισμός και η λεηλασία κλειδιών ασύρματων δικτύων, η παρακολούθηση και η ανάλυση της κίνησης δεδομένων, καθώς και η εκτέλεση επιθέσεων ανακρίβειας και αποσπασμάτων. Οι επιθέσεις που μπορούν να εκτελεστούν μέσω αυτών των εργαλείων περιλαμβάνουν τον έλεγχο αυθεντικοποίησης, την εξαγωγή κλειδιών και την παραβίαση της ασφάλειας του δικτύου.

Το κύριο πλεονέκτημα αυτών των εργαλείων είναι ότι παρέχουν μια πλήρη εικόνα της ασφάλειας του ασύρματου δικτύου, επιτρέποντας στους διαχειριστές και στους ειδικούς ασφάλειας να λάβουν τα αναγκαία μέτρα για την προστασία του. Επίσης, αυτά τα εργαλεία μπορούν να χρησιμοποιηθούν για εκπαιδευτικούς σκοπούς, επιτρέποντας στους ενδιαφερόμενους να κατανοήσουν καλύτερα τις αδυναμίες των ασύρματων δικτύων και τις πιθανές επιθέσεις που μπορεί να αντιμετωπίσουν.

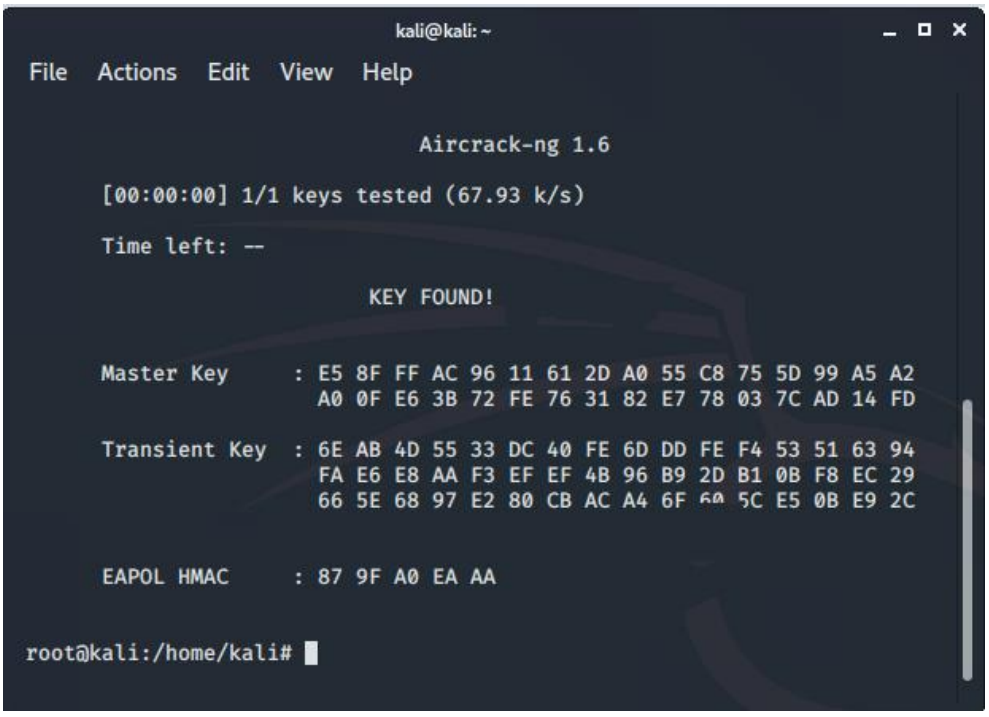
Το **Aircrack-NG** είναι ένα σύνολο εργαλείων ασφαλείας ασύρματου δικτύου (wireless network security tools) που χρησιμοποιούνται κυρίως για την επίθεση και τον έλεγχο ασφάλειας ασύρματων δικτύων Wi-Fi. Το Aircrack-NG προσφέρει διάφορα εργαλεία για τον εντοπισμό και την εκμετάλλευση ευπαθειών στα δίκτυα Wi-Fi. Κάποια από τα βασικά εργαλεία του Aircrack-NG περιλαμβάνουν:

1. **Aircrack-ng:** Ένα εργαλείο ανάκτησης κλειδιών WEP και WPA/WPA2 μέσω επιθέσεων λεξικού και επίθεσης διαρροής κλειδιού (brute force).

2. **Airmon-ng:** Ένα εργαλείο που επιτρέπει την ενεργοποίηση και τη διαχείριση της λειτουργίας monitor mode σε ασύρματες κάρτες δικτύου.

3. **Airodump-ng:** Ένα εργαλείο που χρησιμοποιείται για τον εντοπισμό και την ανάλυση ασύρματων δικτύων Wi-Fi και των σταθμών πρόσβασης.

4. **Aireplay-ng:** Ένα εργαλείο που χρησιμοποιείται για ενεργητικές επιθέσεις εναντίον ασύρματων δικτύων, όπως η αποσύνδεση συσκευών από το δίκτυο (deauthentication attacks) και άλλες επιθέσεις.



Εικόνα 17. Brute-force Attack με το Aircrack-ng

Πηγή : https://www.geeksforgeeks.org/kali-linux-aircrack-ng/

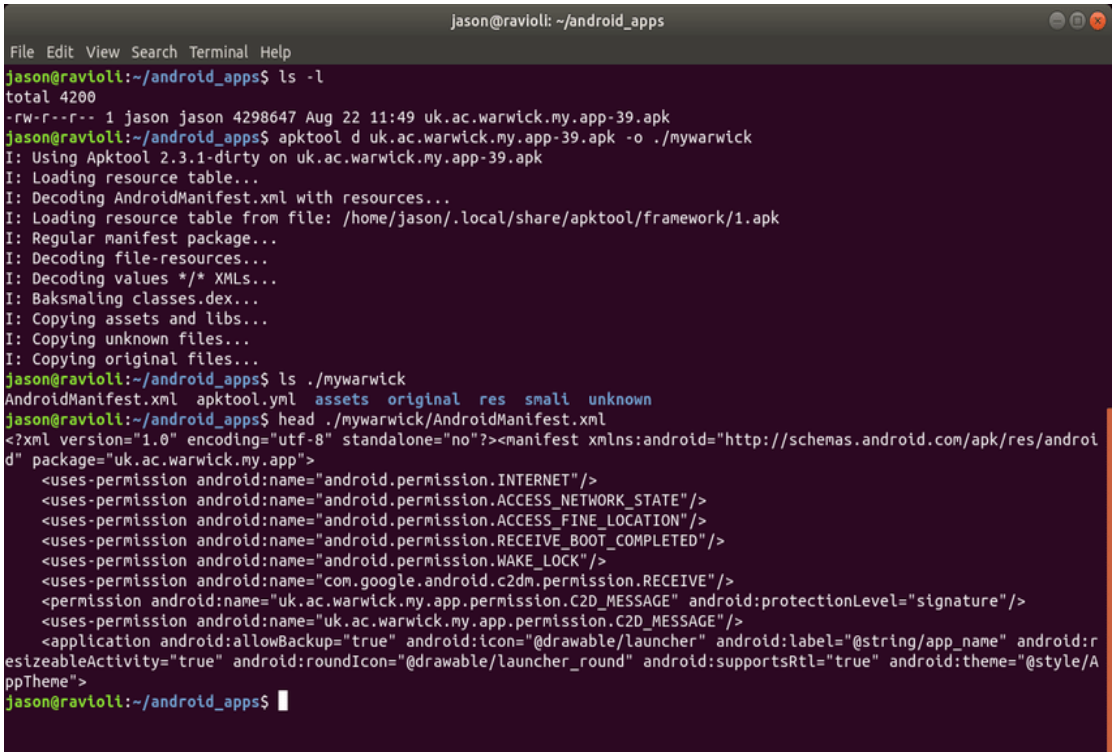
2.6 Reverse Engineering Tools (Εργαλεία Αντίστροφης Μηχανικής)

Τα εργαλεία αντίστροφης μηχανικής (Reverse Engineering Tools) αποτελούν ένα σημαντικό μέρος στον τομέα της κυβερνοασφάλειας. Αυτά τα εργαλεία επιτρέπουν την ανάλυση και την αποσυναρμολόγηση λογισμικού, προκειμένου να κατανοήσουμε τη λειτουργία του, τις ευπάθειές του και τις ενδεχόμενες ευκαιρίες για εκμετάλλευση.

Μερικά από τα βασικά χαρακτηριστικά που προσφέρουν τα εργαλεία αντίστροφης μηχανικής περιλαμβάνουν την αποκρυπτογράφηση του κώδικα, την ανίχνευση και την ανάλυση των αλγορίθμων, την ανασυγκρότηση της δομής του προγράμματος και την εξαγωγή σημαντικών πληροφοριών.

Με τη βοήθεια των εργαλείων αντίστροφης μηχανικής, οι ειδικοί ασφαλείας μπορούν να εντοπίσουν ευπάθειες σε εφαρμογές και να αναπτύξουν αποτελεσματικές αντιμετώπισης. Επιπλέον, αυτά τα εργαλεία επιτρέπουν την αναγνώριση της λειτουργίας του εκάστοτε λογισμικού, καθιστώντας τα απαραίτητα για την αποκρυπτογράφηση και την κατανόηση προγραμμάτων που δεν έχουν πρόσβαση στον πηγαίο κώδικα. Τέλος, η ανάλυση αυτή μπορεί να διευκολύνει την ανάπτυξη αντιμετώπισης για ευάλωτες εφαρμογές ή ακόμη και την προστασία των δικών μας εφαρμογών από πιθανούς επιτιθέμενους.

Το **Apktool** [13] είναι ένα εργαλείο ανοικτού κώδικα που χρησιμοποιείται για το decoding και το rebuilding εφαρμογών Android (APK αρχεία). Αυτό σημαίνει ότι μπορεί να εξάγει τους πόρους και τον κώδικα από ένα APK αρχείο, επιτρέποντας στους χρήστες να τροποποιήσουν το περιεχόμενο της εφαρμογής και να την επανασυναρμολογήσουν. Το Apktool είναι ιδιαίτερα χρήσιμο για την ανάλυση, την τροποποίηση, και την εντοπισμό σφαλμάτων σε εφαρμογές Android, καθώς και για τη μετάφραση εφαρμογών, δηλαδή την προσθήκη ή την τροποποίηση μεταφράσεων γλώσσας.



Εικόνα 18. APKtool

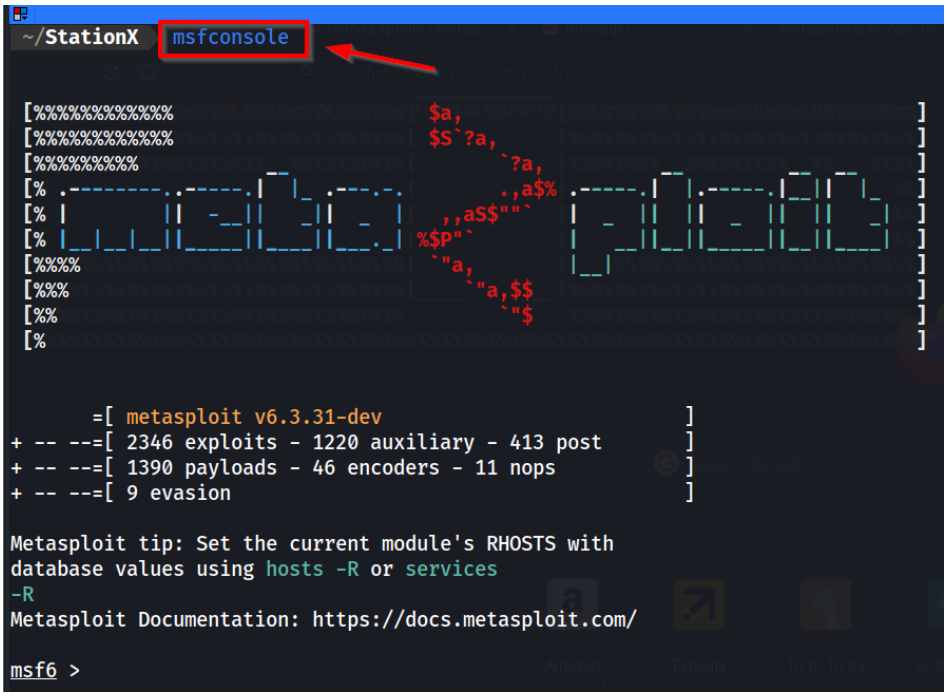
Πηγή : https://www.researchgate.net/figure/Demonstration-I-used-APKTool-to-extract-and-decode-files-an-APK-The-content-of_fig2_329516263

2.7 Exploitation Tools (Εργαλεία Εκμετάλλευσης Ευπαθειών)

Τα εργαλεία εκμετάλλευσης (Exploitation Tools) αποτελούν ένα σημαντικό μέρος του ευρύτερου οικοσυστήματος εργαλείων ασφάλειας πληροφοριών. Αυτά τα εργαλεία σχεδιάζονται και χρησιμοποιούνται με σκοπό την εκμετάλλευση ευπαθειών σε πληροφοριακά συστήματα και εφαρμογές. Συνήθως, αυτές οι ευπαθείς σημειώσεις προέρχονται από αδυναμίες λογισμικού, εσφαλμένες ρυθμίσεις, ή ανεπαρκή αντιμετώπιση από τους διαχειριστές συστημάτων. Με τη χρήση εργαλείων εκμετάλλευσης, οι εισβολείς μπορούν να εκτελέσουν κακόβουλο κώδικα σε ευάλωτες περιοχές του συστήματος ή να αποκτήσουν πρόσβαση σε ευαίσθητα δεδομένα.

Τα εργαλεία εκμετάλλευσης ποικίλουν από απλά σενάρια εκμετάλλευσης έως πιο προηγμένες επιθέσεις με στόχο την πλήρη παράβλεψη των ασφαλείας. Κάποια εργαλεία επικεντρώνονται σε συγκεκριμένες πλατφόρμες ή ευπαθείς εφαρμογές, ενώ άλλα μπορεί να προσφέρουν πολλαπλές δυνατότητες εκμετάλλευσης για διαφορετικούς τύπους συστημάτων.

Τα εργαλεία εκμετάλλευσης πρέπει να χρησιμοποιούνται με προσοχή και με σκοπό την αποτροπή επιθέσεων, καθώς η παράνομη ή κακόβουλη χρήση αυτών των εργαλείων μπορεί να προκαλέσει σοβαρές επιπτώσεις στην ασφάλεια και την ιδιωτικότητα των συστημάτων και των δεδομένων.



Εικόνα 19. Metasploit Framework

Πηγή : https://www.stationx.net/metasploit-tutorial/

Το **Metasploit** είναι ένα πλαίσιο εκμετάλλευσης ασφαλείας και εργαλείο ασφαλείας υπολογιστών που χρησιμοποιείται κυρίως για τη δημιουργία και εκτέλεση επιθέσεων διείσδυσης σε συστήματα υπολογιστών.

Αρχικά αναπτύχθηκε ως ένα ανοικτό πρότυπο από την Rapid7 και πλέον υπάρχει ένα εκτεταμένο οικοσύστημα ανοικτού κώδικα που ονομάζεται Metasploit Framework. Επιπλέον παρέχει ένα εύρος εργαλείων για την εκτέλεση επιθέσεων, συμπεριλαμβανομένων εργαλείων εκμετάλλευσης ευπαθειών, εργαλείων καταγραφής, εργαλείων επιθετικής ερευνητικής ασφάλειας, και πολλά άλλα. Τέλος περιλαμβάνει μια ευέλικτη γραφική διεπαφή χρήστη καθώς και μια πλήρης εντολών γραμμής, προσφέροντας διάφορες επιλογές χρήσης στους χρήστες ανάλογα με τις ανάγκες τους και τις προτιμήσεις τους.

Χρησιμοποιείται ευρέως από ερευνητές ασφαλείας, επαγγελματίες κυβερνοασφάλειας και μηχανικούς ασφάλειας πληροφοριών για να ελέγξουν την ασφάλεια των συστημάτων τους και να αξιολογήσουν τις ευπάθειές τους.

2.8 Sniffing and Spoofing Tools (Εργαλεία παρακολούθησης, καταγραφής και παραποίησης δεδομένων)

Χρησιμοποιούνται για την παρακολούθηση, καταγραφή και την παραποίηση δεδομένων σε δίκτυα. Η λειτουργία τους είναι κρίσιμη για την ανίχνευση αδυναμιών ασφαλείας, τη διάγνωση προβλημάτων δικτύου και την προστασία από κακόβουλες επιθέσεις.

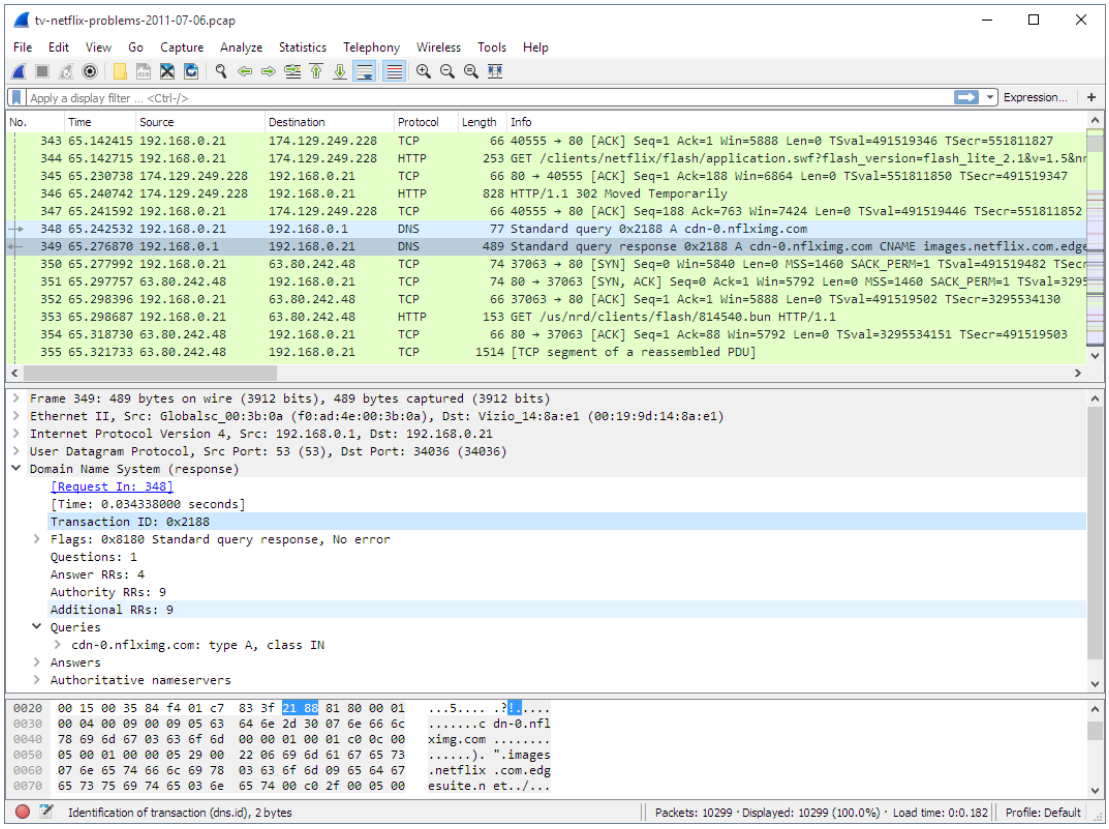
Τα εργαλεία Sniffing χρησιμοποιούνται για την παρακολούθηση της κίνησης δεδομένων σε ένα δίκτυο. Αυτά τα εργαλεία επιτρέπουν στους διαχειριστές να παρακολουθούν την αλληλεπίδραση μεταξύ συσκευών, να ανιχνεύουν ασυνήθιστη κίνηση και να ανακαλύπτουν πιθανές απειλές. Από την άλλη πλευρά, τα εργαλεία Spoofing επιτρέπουν στους χρήστες να παραποιούν δεδομένα, να προσποιούνται ως άλλες συσκευές ή να παραποιούν την πραγματική κίνηση δεδομένων στο δίκτυο.

Η χρήση αυτών των εργαλείων απαιτεί προσοχή και ευαισθησία, καθώς μπορεί να χρησιμοποιηθούν για παράνομες δραστηριότητες όπως η κλοπή δεδομένων ή η κατάχρηση της ταυτότητας. Ωστόσο, σε ένα περιβάλλον ασφαλούς δικτύωσης, αυτά τα εργαλεία μπορούν να είναι ιδιαίτερα χρήσιμα για την ανάπτυξη και τη διαχείριση των ασφαλών δικτύων.

Το **Wireshark** [13] είναι ένα δημοφιλές εργαλείο ανάλυσης πακέτων δικτύου. Χρησιμοποιείται για την εγγραφή και την ανάλυση της κίνησης δεδομένων που κυκλοφορεί μέσα από ένα δίκτυο. Το Wireshark επιτρέπει στους χρήστες να αναλύσουν την επικοινωνία μεταξύ διαφόρων συσκευών σε ένα δίκτυο, να εντοπίσουν προβλήματα δικτύου, να αναγνωρίσουν ανεπιθύμητη κίνηση ή δραστηριότητα, και να παρακολουθήσουν την ασφάλεια του δικτύου. Υποστηρίζει πολλά πρωτόκολλα δικτύου και μπορεί να αναλύσει διάφορα είδη κίνησης δεδομένων, συμπεριλαμβανομένων πρωτοκόλλων όπως το TCP, το UDP, το ICMP και πολλά άλλα.

Το Wireshark παρέχει ένα εύχρηστο γραφικό περιβάλλον χρήστη για την επεξεργασία και την ανάλυση των πακέτων, καθώς και μια ποικιλία εργαλείων και

δυνατοτήτων για τη διεξαγωγή λεπτομερών ελέγχων της κίνησης δεδομένων. Το Wireshark είναι ένα από τα πλέον διαδεδομένα εργαλεία ανάλυσης πακέτων και χρησιμοποιείται ευρέως από επαγγελματίες δικτύου και ασφάλειας, ερευνητές ασφάλειας, καθώς και από φοιτητές και ερασιτέχνες για την εξέταση και την ανάλυση δικτυακής κίνησης.



Εικόνα 20. Καταγραφή πακέτων με το Wireshark

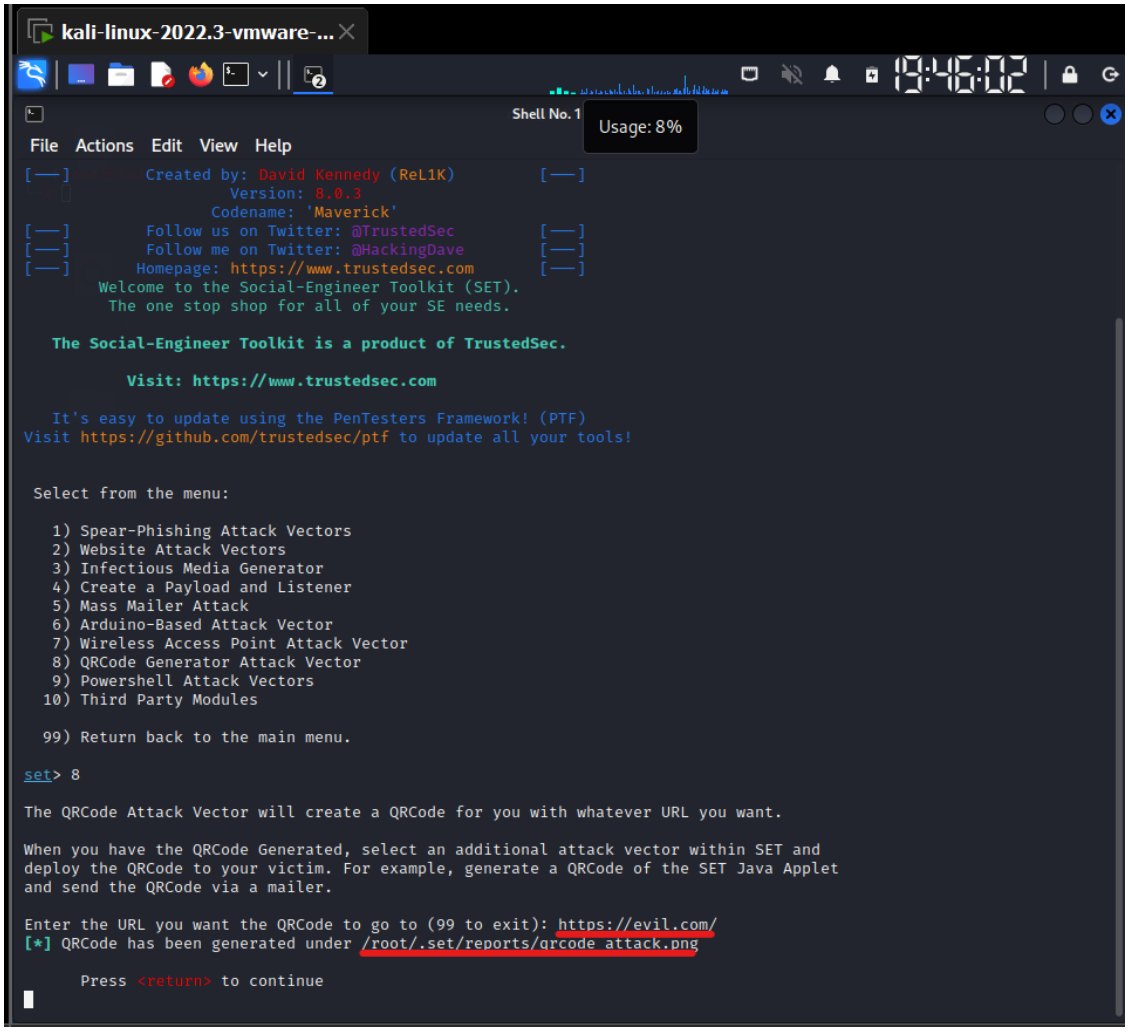
Πηγή: https://www.wireshark.org/docs/wsug_html_chunked/ChapterIntroduction.html

2.9 Social Engineering Tools (Εργαλεία Κοινωνικής Μηχανικής)

Περιλαμβάνει εργαλεία που χρησιμοποιούνται για την εκτέλεση και ανάλυση επιθέσεων κοινωνικής μηχανικής. Αυτές οι επιθέσεις εκμεταλλεύονται την ανθρώπινη αλληλεπίδραση και την ψυχολογία για να παραπλανήσουν τα θύματα και να αποκτήσουν ευαίσθητες πληροφορίες, όπως κωδικούς πρόσβασης ή προσωπικά δεδομένα. Αυτά τα εργαλεία είναι χρήσιμα για τους επαγγελματίες ασφάλειας, καθώς τους επιτρέπουν να αξιολογούν την ανθεκτικότητα των οργανισμών στις επιθέσεις κοινωνικής μηχανικής και να εκπαιδεύουν τους χρήστες στην αναγνώριση και την αποφυγή τέτοιων απειλών.

Το **Social Engineering Toolkit (SET)** [21] είναι ένα εργαλείο ανοικτού κώδικα που χρησιμοποιείται για εκτέλεση επιθέσεων social engineering. Το SET προσφέρει ένα σύνολο εργαλείων και λειτουργιών που επιτρέπουν στους χρήστες να εκτελέσουν ποικίλες μορφές επιθέσεων social engineering, συμπεριλαμβανομένων των (phishing) επιθέσεων, εκμετάλλευσης ανθρώπινων αδυναμιών και άλλων κοινωνικών μεθόδων

για την απόκτηση πληροφοριών ή πρόσβασης σε συστήματα. Οι λειτουργίες του SET περιλαμβάνουν τη δημιουργία παραπλανητικών ιστοσελίδων, τη δημιουργία κακόβουλων ηλεκτρονικών μηνυμάτων, την εκτέλεση επιθέσεων εκμετάλλευσης ευπαθειών σε περιβάλλοντα όπως τον κοινωνικό τεχνολογικό παράγοντα (social engineering attacks), την καταγραφή πληροφοριών από τα θύματα, και άλλα.



Εικόνα 21. Κατηγορίες επιθέσεων του Social Engineering Toolkit

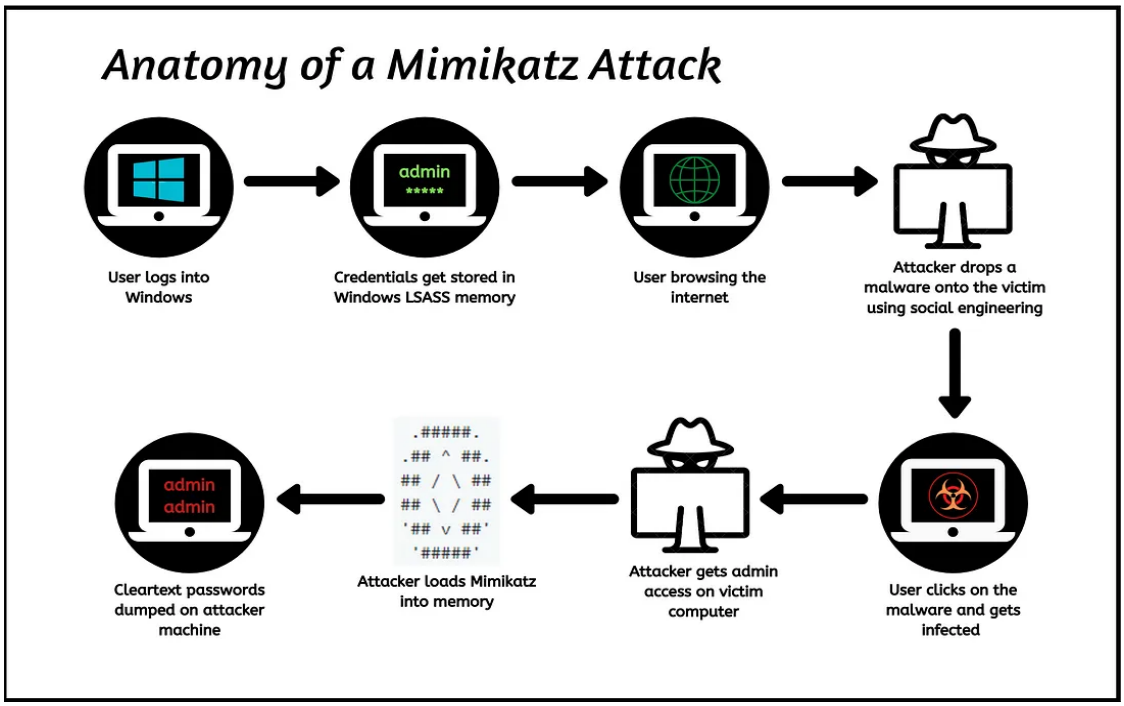
Πηγή : https://kalilinuxtutorials.com/social-engineering-toolkit-tutorial/

2.10 Post Exploitation Tools (Εργαλεία Μετα-εκμετάλλευσης)

Τα εργαλεία Post Exploitation είναι λογισμικά που χρησιμοποιούνται μετά την επιτυχή διείσδυση σε ένα σύστημα για τη διατήρηση της πρόσβασης, τη συλλογή πληροφοριών και τη μεγιστοποίηση του ελέγχου επί του στόχου. Αυτά τα εργαλεία επιτρέπουν στους επαγγελματίες ασφαλείας να εκτελούν ενέργειες όπως η εξαγωγή ευαίσθητων δεδομένων, η ανάλυση του δικτύου, η ανύψωση προνομίων, η εγκατάσταση μόνιμων backdoors και η δημιουργία αναφορών για τα ευρήματα. Οι δραστηριότητες αυτές είναι κρίσιμες για την κατανόηση του εύρους και της

σοβαρότητας των επιπτώσεων μιας παραβίασης και για την ανάπτυξη κατάλληλων στρατηγικών αντιμετώπισης.

Το **Mimikatz** [16] είναι ένα πολύ ισχυρό εργαλείο λογισμικού που χρησιμοποιείται για την εξόρυξη ευαίσθητων πληροφοριών σχετικά με τα διαπιστευτήρια ασφαλείας σε λειτουργικά συστήματα Windows. Δημιουργήθηκε αρχικά από τον Benjamin Delpy και είναι διαθέσιμο ως λογισμικό ανοικτού κώδικα.



Εικόνα 22. Πως δουλεύει το Mimikatz

Πηγή : https://shahrukhiqbal24.medium.com/attacking-windows-10-using-mimikatz-824c73eb9f3d

Το Mimikatz μπορεί να χρησιμοποιηθεί για την ανάκτηση και την εκτύπωση κωδικών πρόσβασης που είναι αποθηκευμένοι στον μνήμη του συστήματος, όπως κωδικοί NTLM, κλειδιά BitLocker, κλειδιά κρυπτογράφησης και άλλα.

Το εργαλείο αυτό είναι ιδιαίτερα δημοφιλές στον χώρο της κυβερνοασφάλειας και συχνά χρησιμοποιείται σε δοκιμές διαπερατότητας και αξιολογήσεις ασφαλείας για την εντοπισμό πιθανών αδυναμιών στην ασφάλεια του συστήματος.

Το **Evilginx** [22] είναι ένα εργαλείο (phishing) που αναπτύχθηκε από τον ερευνητή ασφάλειας Kuba Gretzky. Χρησιμοποιείται για την εκτέλεση εξαιρετικά εξελιγμένων επιθέσεων σε ιστοσελίδες που χρησιμοποιούν το πρωτόκολλο OAuth (Open Authorization).

Η βασική λειτουργία του Evilginx είναι η εκμετάλλευση της επίθεσης "Man-in-the-Middle" (MITM), όπου ο κακόβουλος επιτιθέμενος διακόπτει την επικοινωνία μεταξύ του χρήστη και του αυθεντικού διακομιστή, προσποιούμενος ότι είναι ο αυθεντικός διακομιστής. Έτσι, όταν ο χρήστης προσπαθεί να συνδεθεί στην ιστοσελίδα που υποκρίνεται το Evilginx, όλη η επικοινωνία περνάει από τον κακόβουλο διακομιστή,

επιτρέποντάς του να κλέψει τα διαπιστευτήρια εισόδου (όπως ονόματα χρηστών και κωδικοί πρόσβασης).

Το Evilginx είναι ένα ισχυρό εργαλείο και χρησιμοποιείται κυρίως για την εκτέλεση στοχευμένων phising επιθέσεων εναντίον επιχειρήσεων, οργανισμών ή ατόμων που χρησιμοποιούν το πρωτόκολλο OAuth για την είσοδο σε διάφορες υπηρεσίες ή λογαριασμούς (όπως τα κοινωνικά δίκτυα, το email, κλπ.). Επειδή εκμεταλλεύεται τις ευπάθειες του πρωτοκόλλου OAuth και δεν απαιτεί την παραβίαση κρυπτογράφησης ή τη χρήση κακόβουλου λογισμικού στον υπολογιστή του θύματος, μπορεί να είναι αποτελεσματικό ακόμη και εάν οι χρήστες έχουν ενεργοποιημένα τα μέτρα ασφαλείας τους.

Εικόνα 23. Man-in-the-Middle Attack με το Evilginx

Πηγή : https://github.com/kgretzky/evilginx2?tab=readme-ov-file

3. ΕΝΙΣΧΥΣΗ ΑΣΦΑΛΕΙΑΣ ΣΤΙΣ ΚΙΝΗΤΕΣ ΠΛΑΤΦΟΡΜΕΣ ANDROID & IOS

Η ασφάλεια στις κινητές πλατφόρμες **Android** [8] και **iOS** [9] αποτελεί έναν κρίσιμο παράγοντα για τη διασφάλιση της προστασίας των δεδομένων και την πρόληψη επιθέσεων κατά των κινητών συσκευών και των εφαρμογών που εκτελούνται σε αυτές. Οι δύο αυτές πλατφόρμες έχουν διαφορετικές αρχιτεκτονικές και προσεγγίσεις στην ασφάλεια, αλλά και κοινά στοιχεία που αφορούν την ενίσχυση της ασφάλειας των εφαρμογών και των συσκευών τους.

3.1 Λειτουργικό Σύστημα Android

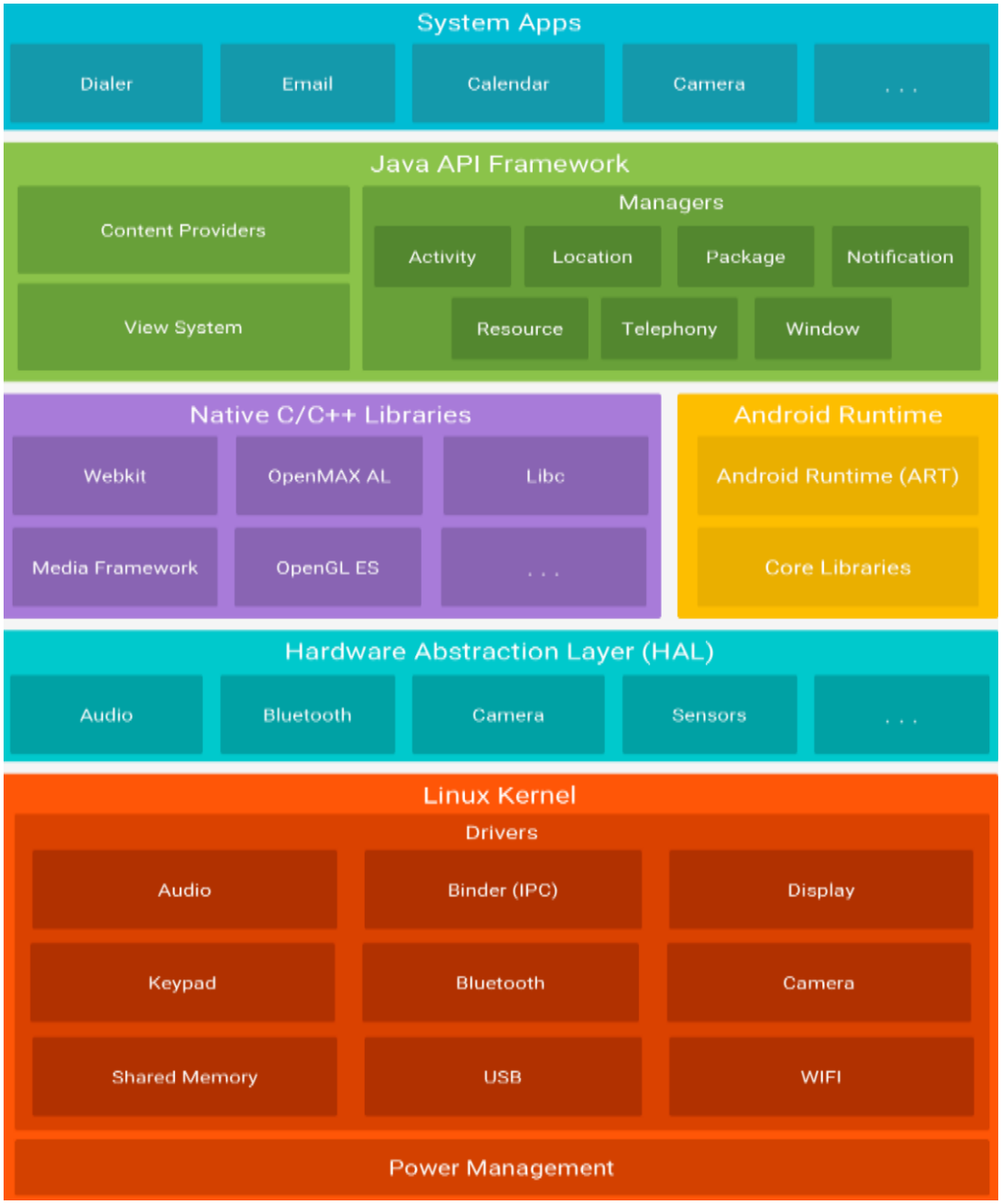
Σε αυτή την ενότητα θα αναλύσουμε το λειτουργικό του Android ώστε να κατανοήσουμε καλύτερα την δομή και την αρχιτεκτονική του και θα μας βοηθήσει στη συνέχεια για την εκτέλεση του penetration testing. Το Android [24] είναι ένα λειτουργικό σύστημα για κινητές συσκευές που βασίζεται σε μια προσαρμοσμένη έκδοση του πυρήνα του Linux και άλλων λογισμικών ανοικτού κώδικα. Αρχικά σχεδιάστηκε για συσκευές με οθόνη αφής, όπως smartphones και tablets, αλλά πλέον χρησιμοποιείται επίσης σε άλλες συσκευές όπως τηλεοράσεις, αυτοκίνητα και ρολόγια χειρός. Η εταιρεία Android Inc. ιδρύθηκε το 2003 και τον Ιούλιο του 2005 εξαγοράστηκε από την Google. Η πρώτη επίσημη παρουσίαση της πλατφόρμας Android έγινε τον Νοέμβριο του 2007, ενώ η πρώτη συσκευή που χρησιμοποίησε το Android κυκλοφόρησε στην αγορά τον Σεπτέμβριο του 2008.

Εικόνα 24. Ιστορικό εκδόσεων Android

Πηγή : https://twitter.com/Android_History/status/1751821503962775836

3.1.1 Αρχιτεκτονική Android

Η αρχιτεκτονική του Android αναφέρεται στη δομή και τον τρόπο λειτουργίας του λειτουργικού συστήματος Android. Η αρχιτεκτονική του Android σχεδιάζεται για να είναι ευέλικτη, ανοικτή και να υποστηρίζει μια ευρεία γκάμα συσκευών, από smartphones και tablets έως τηλεοράσεις, αυτοκίνητα και άλλες συσκευές. Αυτή η δομή του επιτρέπει στους προγραμματιστές να δημιουργούν εφαρμογές που λειτουργούν απρόσκοπτα σε διάφορες πλατφόρμες και μεγέθη οθονών.



Εικόνα 25. Αρχιτεκτονική Android

Πηγή : https://developer.android.com/guide/platform

Ας δούμε τα βασικά συστατικά της αρχιτεκτονικής του Android:

- ✓ **Πυρήνας Linux (Linux Kernel):** Το Android βασίζεται σε ένα προσαρμοσμένο πυρήνα Linux, που παρέχει τις βασικές λειτουργίες του συστήματος όπως η διαχείριση μνήμης, η διαχείριση ενέργειας, οι δικτυακές λειτουργίες κ.λπ.
- ✓ **Βιβλιοθήκες και Υποσυστήματα (Libraries and Subsystems):** Το Android χρησιμοποιεί διάφορες βιβλιοθήκες και υποσυστήματα για τη διαχείριση διάφορων λειτουργιών, όπως η γραφική διεπαφή χρήστη (UI), οι κινητήρες γραφικών (Graphics Engines), η διαχείριση των εισόδων/εξόδων (I/O) κ.ά.
- ✓ **Εφαρμογές Framework (Application Framework):** Παρέχει ένα σύνολο βιβλιοθηκών που επιτρέπουν τη δημιουργία εφαρμογών Android, συμπεριλαμβανομένων των εργαλείων ανάπτυξης, των διαχειριστών συστήματος, της διαχείρισης χρηστών κ.ά.
- ✓ **Εφαρμογές (Applications):** Το Android περιλαμβάνει τις εφαρμογές που τρέχουν επάνω σε αυτό, συμπεριλαμβανομένων των εφαρμογών προεγκατεστημένων από τον κατασκευαστή, των εφαρμογών από το Google Play Store και των εφαρμογών που οι χρήστες εγκαθιστούν.

3.1.2 Android Application Components

Τα στοιχεία εφαρμογών του Android (Android Application Components) είναι τα διαφορετικά μέρη μιας εφαρμογής Android που συνδυάζονται για να δημιουργήσουν την πλήρη λειτουργικότητα της εφαρμογής. Κάθε στοιχείο επιτελεί ένα συγκεκριμένο ρόλο στη λειτουργία της εφαρμογής.

Εικόνα 26. Android Application Components

Πηγή : https://techvidvan.com/tutorials/android-application-components/

Τα βασικά στοιχεία εφαρμογών του Android περιλαμβάνουν τα εξής:

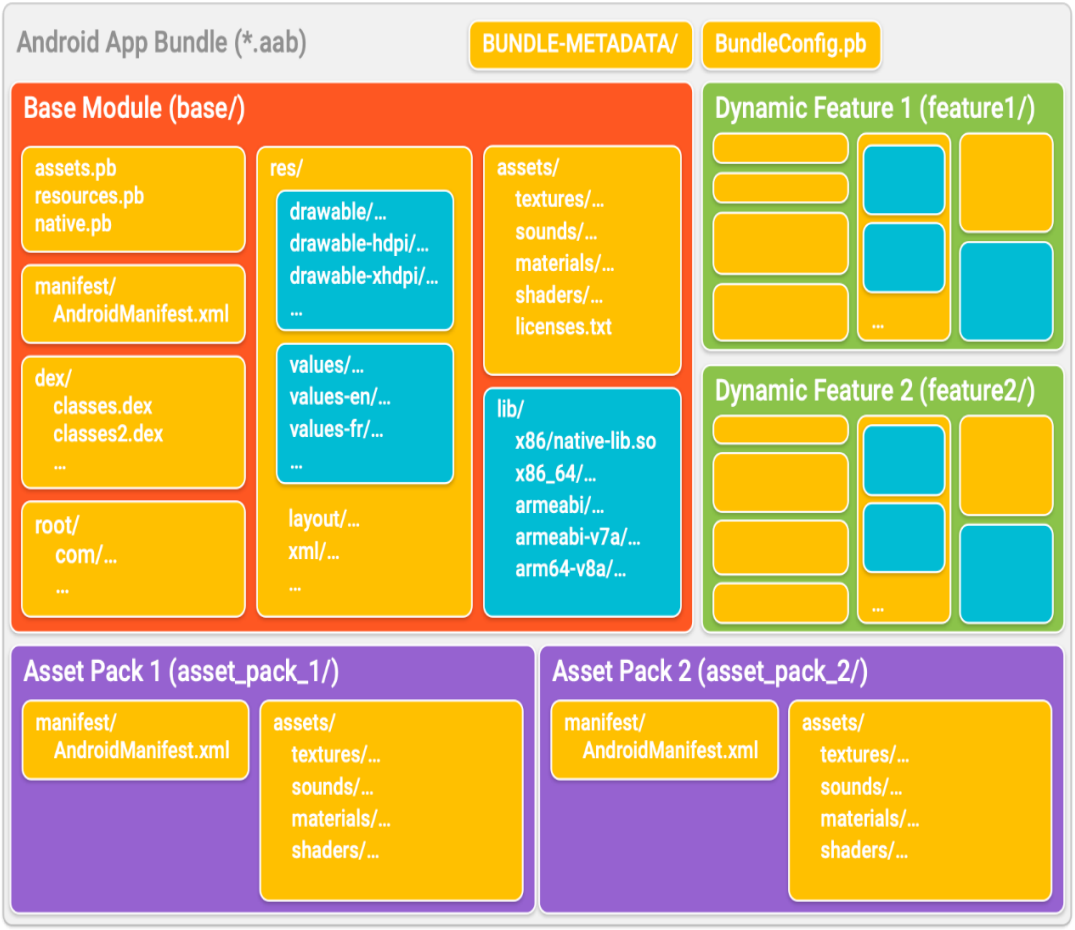
- **Δραστηριότητες (Activities):** Είναι ένα από τα βασικά στοιχεία της αρχιτεκτονικής των εφαρμογών του Android. Κάθε Activity αντιπροσωπεύει μια οθόνη με την οποία ο χρήστης αλληλοεπιδρά με την εφαρμογή. Κάθε Activity έχει τη δική της διάταξη (layout) που ορίζει την εμφάνισή της και τα στοιχεία ελέγχου (widgets) που περιλαμβάνει, όπως κουμπιά, κείμενα, εικόνες κ.λπ. Μπορούν να περιλαμβάνουν επίσης λειτουργίες όπως εικόνες, βίντεο, λίστες, φόρμες, και άλλα στοιχεία που βοηθούν τον χρήστη να αλληλοεπιδρά με την εφαρμογή. Ένα Activity ξεκινά όταν ο χρήστης εκτελεί την εφαρμογή και τερματίζει όταν ο χρήστης μεταπηδάει σε ένα άλλο Activity ή κλείνει την εφαρμογή. Ακόμα μπορούν να αλληλοεπιδρούν μεταξύ τους μέσω διάφορων μηχανισμών όπως η μετάβαση από ένα Activity σε ένα άλλο μετά από κλικ σε ένα κουμπί ή η αποστολή δεδομένων από ένα Activity σε ένα άλλο. Τα Activities είναι σημαντικά για την καλή ροή και την ευχρηστία μιας εφαρμογής Android, καθώς κάθε Activity παρέχει στον χρήστη μια διαφορετική εμπειρία και λειτουργικότητα. Ένας καλός σχεδιασμός των Activities μπορεί να καθιστά την εφαρμογή πιο εύχρηστη και ελκυστική για τους χρήστες.
- **Υπηρεσίες (Services)**: Στο Android αντιπροσωπεύουν συστήματα που εκτελούνται στο παρασκήνιο χωρίς την ανάγκη παρέχοντας διεπαφή χρήστη. Αυτές οι υπηρεσίες εκτελούνται ανεξάρτητα από τις δραστηριότητες της εφαρμογής και χρησιμοποιούνται για να εκτελέσουν μακροχρόνιες διεργασίες, όπως η αναπαραγωγή μουσικής, η λήψη δεδομένων από το διαδίκτυο, η ενημέρωση δεδομένων από μια βάση δεδομένων ή η αποστολή ενημερώσεων προειδοποίησης στον χρήστη. Οι υπηρεσίες επιτρέπουν στις εφαρμογές να διατηρούν τη λειτουργικότητά τους ακόμα και όταν ο χρήστης δεν αλληλεπιδρά με την εφαρμογή απευθείας. Για παράδειγμα, μια εφαρμογή μπορεί να έχει μια υπηρεσία που αναλαμβάνει να λαμβάνει νέα μηνύματα από έναν διακομιστή, ακόμα και όταν ο χρήστης δεν χρησιμοποιεί αυτή την εφαρμογή. Οι υπηρεσίες μπορούν να τρέχουν σε φόντο, προσφέροντας έτσι τη δυνατότητα στις εφαρμογές να εκτελούν εργασίες που απαιτούν χρόνο χωρίς να επηρεάζουν την απόκριση της διεπαφής χρήστη. Ταυτόχρονα, μπορούν να επικοινωνούν με άλλα στοιχεία της εφαρμογής ή άλλες εφαρμογές μέσω διάφορων μηχανισμών επικοινωνίας, όπως οι δέκτες εκπομπών και οι παροχείς περιεχομένου. Επομένως, οι υπηρεσίες αποτελούν σημαντικό στοιχείο στην αρχιτεκτονική του Android, επιτρέποντας στις εφαρμογές να προσφέρουν πλούσια λειτουργικότητα και να διατηρούνται ενεργές και αποτελεσματικές ακόμα και μετά την αποχώρηση του χρήστη από αυτές.
- **Δέκτες εκπομπών (Broadcast Receivers):** Είναι ένα σημαντικό στοιχείο της αρχιτεκτονικής του Android που επιτρέπει σε μια εφαρμογή να αντιδράσει σε διάφορα γεγονότα και εκδηλώσεις που συμβαίνουν στο σύστημα ή σε άλλες εφαρμογές. Ουσιαστικά, οι δέκτες εκπομπών λειτουργούν ως ακροατές που παρακολουθούν για συγκεκριμένα γεγονότα και αντιδρούν αναλόγως. Ένας

δέκτης εκπομπών μπορεί να είναι καταχωρημένος στο σύστημα Android για να ακούει για εκδηλώσεις όπως η λήψη ενός νέου μηνύματος SMS, η αλλαγή της κατάστασης της σύνδεσης δικτύου, η αναπαραγωγή μουσικής ή η ενεργοποίηση της συσκευής. Όταν εκδηλώνεται ένα από αυτά τα γεγονότα, ο δέκτης εκπομπών ενεργοποιείται και μπορεί να εκτελέσει κώδικα που έχει οριστεί για να αντιδράσει σε αυτό το συγκεκριμένο γεγονός. Για παράδειγμα, μια εφαρμογή μπορεί να θέλει να αντιδράσει σε ένα εισερχόμενο μήνυμα SMS για να ειδοποιήσει τον χρήστη, ή μια εφαρμογή μουσικής μπορεί να θέλει να ξεκινήσει την αναπαραγωγή μουσικής όταν ο χρήστης συνδέει ακουστικά. Επίσης, οι δέκτες εκπομπών επιτρέπουν στις εφαρμογές να επικοινωνούν μεταξύ τους και να συνεργάζονται για την εκτέλεση συγκεκριμένων εργασιών , δηλώνονται στο αρχείο manifest της εφαρμογής Android και έχουν ορισμένες διακριτικές ενέργειες που εκτελούνται όταν εκδηλώνεται το συγκεκριμένο γεγονός. Η σωστή χρήση των δεκτών εκπομπών είναι σημαντική για την αποτελεσματική ανταπόκριση της εφαρμογής σε διάφορα γεγονότα και για τη βελτίωση της εμπειρίας χρήστη.

- **Παροχείς περιεχομένου (Content Providers)**: Στο Android αποτελούν ένα σημαντικό τμήμα της αρχιτεκτονικής του συστήματος. Βασικά, λειτουργούν ως ενδιάμεσο μεταξύ διαφορετικών εφαρμογών για την ανταλλαγή και τη διαχείριση δεδομένων. Μέσω των providers περιεχομένου, οι εφαρμογές μπορούν να αποθηκεύουν και να ανακτούν πληροφορίες σε κοινές βάσεις δεδομένων, επιτρέποντας την κοινή χρήση δεδομένων από διαφορετικές πηγές. Αυτό διευκολύνει την ανάπτυξη εφαρμογών που απαιτούν πρόσβαση σε πληροφορίες από διάφορες πηγές, ενώ παράλληλα εξασφαλίζει τη σωστή διαχείριση και προστασία των δεδομένων. Όπως και τα παραπάνω, έτσι και οι content providers πρέπει να δηλωθούν στο αρχείο manifest.xml.

3.1.3 Android Application Package (APK)

Το Android Application Package (APK) είναι το αρχείο που περιέχει όλα τα στοιχεία μιας εφαρμογής Android. Αυτό το αρχείο APK είναι η μονάδα εγκατάστασης για τις εφαρμογές Android. Κάθε φορά που εγκαθίσταται μια εφαρμογή από το Google Play Store ή από άλλες πηγές, όπως ενδεχομένως από το διαδίκτυο ή από email, εγκαθιστάται ουσιαστικά ένα αρχείο APK στη συσκευή μας. Το αρχείο APK περιέχει τον κώδικα της εφαρμογής Android, τα αρχεία πόρων (όπως εικόνες, ήχοι και γραφικά), το αρχείο manifest που περιγράφει τις πληροφορίες της εφαρμογής και άλλα απαραίτητα αρχεία για την εκτέλεση της εφαρμογής. Το αρχείο APK είναι επίσης υπεύθυνο για τον μηχανισμό εγκατάστασης και ενημέρωσης της εφαρμογής. Όταν εγκαθιστάται ένα APK στη συσκευή μας, η συσκευή αποσυμπιέζει το αρχείο και εκτελεί τη διαδικασία εγκατάστασης της εφαρμογής σύμφωνα με τις οδηγίες που περιέχονται στο αρχείο.



Εικόνα 27. The Android App Bundle format

Πηγή : https://developer.android.com/guide/app-bundle/app-bundle-format

3.1.4 Rooting Android

Κάθε κατασκευαστής smartphone εφαρμόζει ορισμένους ελέγχους προστασίας στο λογισμικό που συνοδεύει το τηλέφωνο, προκειμένου να αποτρέψει επιθέσεις ιών, κακόβουλου λογισμικού ή μη εξουσιοδοτημένες αλλαγές λογισμικού. Αυτό γίνεται για λόγους ασφάλειας. Το λειτουργικό σύστημα Android έχει εφαρμόσει πολλές τεχνικές προστασίας μέσα στα χρόνια. Μια τεχνική είναι η καθιέρωση του συστήματος σε λειτουργία Read Only. Εάν αυτό είναι ενεργοποιημένο, κανείς δεν μπορεί να αλλάξει τα αρχεία του συστήματος ενώ το λειτουργικό σύστημα εκτελείται. Αυτό ρυθμίζεται στον πίνακα συστήματος αρχείων (fstab), το οποίο είναι μέρος του συστήματος.

Ο μόνος τρόπος να τροποποιηθούν τα αρχεία του συστήματος είναι μέσω του Recovery. Καθώς στο Recovery όλα τα partition γίνονται mount σε λειτουργία Read Write. Αυτό είναι δυνατό μόνο μέσω ενός custom recovery. Το Official/stock Recovery δεν θα το επιτρέψει αυτό γιατί οι κατασκευαστές αποκλείουν τροποποιήσεις στο λογισμικό τους. Εάν ο bootloader είναι ξεκλείδωτος και στη συνέχεια ο χρήστης προσπαθεί να αναβαθμίσει ένα custom recovery και να εκκινήσει στο recovery σε αυτή τη στιγμή, θα μπορεί να τροποποιήσει τα αρχεία του συστήματος. Αφού ο χρήστης

αποκτήσει τέτοια πρόσβαση εγγραφής, το πρώτο πράγμα είναι να τροποποιήσει το fstab και να κάνει το σύστημα mount σε λειτουργία Ανάγνωσης/Εγγραφής. Έτσι, στην επόμενη εκκίνηση, το σύστημα θα γίνει mount σε λειτουργία Ανάγνωσης/Εγγραφής. Ένας άλλος μηχανισμός προστασίας είναι ο ορισμός των δικαιωμάτων πρόσβασης του χρήστη στα αρχεία. Το Linux υποστηρίζει πολλούς χρήστες και από προεπιλογή υπάρχουν δύο: ο άνθρωπος που χρησιμοποιεί το smartphone και ο “root” (επίσης γνωστός ως Super User) ο οποίος έχει όλα τα προνόμια για να κάνει οτιδήποτε στο λειτουργικό σύστημα. Όλα τα αρχεία συστήματος είναι προσβάσιμα μόνο από τον χρήστη root. Αυτό σημαίνει ότι ο άνθρωπος που αγόρασε το τηλέφωνο δεν έχει πραγματικά τον πλήρη έλεγχο όλων των μερών του.

Το Rooting είναι το σύνολο όλων των διαδικασιών περιλαμβανομένου του Custom Recovery, της injecting su binary και της αλλαγής της πρόσβασης του συστήματος σε λειτουργία ανάγνωσης-εγγραφής (read-write). Σε βασικό επίπεδο, το rooting ενός τηλεφώνου Android σημαίνει τη χορήγηση πρόσβασης superuser, αλλά τα τηλέφωνα Android από προεπιλογή δεν μας δίνουν αυτήν την επιλογή. Η διασφάλιση απεριόριστης πρόσβασης στο χρήστη μπορεί να προκαλέσει προβλήματα όπως η ζημιά των εφαρμογών και η διάλυση του τηλεφώνου. Ωστόσο, για ορισμένους ανθρώπους, το Rooting είναι σχεδόν απαραίτητο γιατί τότε ο χρήστης μπορεί να "αναβαθμίσει" παραλλαγές του λειτουργικού συστήματος Android και να εγκαταστήσει εφαρμογές με περισσότερες δυνατότητες.

Εικόνα 28. Rooting Android

Πηγή : https://www.lifewire.com/root-or-not-root-android-1616838

3.2 Λειτουργικό Σύστημα iOS

Το iOS είναι το λειτουργικό σύστημα της Apple για κινητές συσκευές, το οποίο πρωτοεμφανίστηκε το 2007 με το πρώτο iPhone. Από τότε, έχει γνωρίσει σημαντική εξέλιξη, επεκτείνοντας τη χρήση του σε iPad, iPod Touch και άλλες συσκευές της Apple. Το iOS σχεδιάστηκε με έμφαση στην ευχρηστία και την ασφάλεια,

προσφέροντας μια ομαλή και ενιαία εμπειρία χρήστη μέσω του οικοσυστήματος της Apple.

Η πρώτη έκδοση του iOS κυκλοφόρησε το 2007 και ονομαζόταν αρχικά "iPhone OS". Αυτή η έκδοση παρουσίασε έναν καινοτόμο τρόπο αλληλεπίδρασης με κινητές συσκευές μέσω της οθόνης αφής και της χρήσης gestures, όπως το tap, το swipe και το pinch. Ο σχεδιασμός του iOS επικεντρώθηκε στην ευκολία χρήσης, καθιστώντας τις λειτουργίες του προσιτές ακόμη και σε άτομα χωρίς προηγούμενη εμπειρία σε smartphones.

Το 2008, η Apple παρουσίασε το App Store, επιτρέποντας στους προγραμματιστές να δημιουργούν και να διανέμουν εφαρμογές για το iPhone και το iPod Touch. Αυτή η κίνηση άνοιξε το δρόμο για την ανάπτυξη μιας πλούσιας οικολογίας εφαρμογών που βοήθησε στην αύξηση της δημοτικότητας του iOS. Το App Store έγινε σύντομα ένας από τους κύριους λόγους για την επιτυχία του iPhone, προσφέροντας στους χρήστες πρόσβαση σε εκατοντάδες χιλιάδες εφαρμογές.

Το iOS 3.0, που κυκλοφόρησε το 2009, προσέφερε νέες δυνατότητες όπως την υποστήριξη για το MMS, το tethering, το Spotlight Search και την αρχική μορφή του App Store, που επέτρεψε στους χρήστες να αγοράζουν και να κατεβάζουν εφαρμογές απευθείας από τις συσκευές τους. Το MMS, ή Multimedia Messaging Service, επέτρεψε την αποστολή μηνυμάτων με εικόνες, βίντεο και ήχο, προσθέτοντας μια νέα διάσταση στην επικοινωνία μέσω κινητών.

Το Spotlight Search έφερε μια ευέλικτη λειτουργία αναζήτησης στο iOS, επιτρέποντας στους χρήστες να αναζητούν περιεχόμενο σε όλη τη συσκευή τους, από εφαρμογές και email μέχρι μουσική και επαφές. Αυτή η δυνατότητα βελτίωσε σημαντικά την παραγωγικότητα, επιτρέποντας στους χρήστες να βρίσκουν γρήγορα τις πληροφορίες που χρειάζονταν.

3.2.1 Μεταβατικές Εξελίξεις (2011-2015)

Η κυκλοφορία του iCloud το 2011 αποτέλεσε σημαντικό σημείο καμπής, προσφέροντας λύσεις cloud storage και συγχρονισμού δεδομένων. Αυτό επέτρεψε στους χρήστες να αποθηκεύουν και να συγχρονίζουν δεδομένα μεταξύ των συσκευών τους, καθιστώντας το iOS ακόμα πιο ελκυστικό. Το iCloud παρέχει διάφορες υπηρεσίες, όπως το iCloud Drive, το iCloud Photos και το iCloud Backup, διευκολύνοντας την αποθήκευση και την κοινή χρήση δεδομένων μεταξύ συσκευών.

Το iOS 7, που κυκλοφόρησε το 2013, ήταν ένα σημείο καμπής για το iOS. Το νέο flat design και οι δυναμικές κινούμενες εικόνες έδωσαν στο iOS μια πιο σύγχρονη εμφάνιση και αίσθηση. Το Control Center προσέφερε γρήγορη πρόσβαση σε βασικές λειτουργίες όπως η ρύθμιση της φωτεινότητας, ο έλεγχος της μουσικής και η ενεργοποίηση του Wi-Fi, ενώ το AirDrop διευκόλυνε την κοινή χρήση αρχείων μεταξύ συσκευών iOS.

Το iOS 8 (2014) εισήγαγε το HealthKit, το οποίο επέτρεψε στους προγραμματιστές να δημιουργούν εφαρμογές υγείας που μπορούν να μοιράζονται δεδομένα μεταξύ τους και με το σύστημα υγείας της συσκευής. Το HealthKit επιτρέπει στις εφαρμογές να συλλέγουν και να μοιράζονται δεδομένα υγείας και φυσικής κατάστασης, προσφέροντας στους χρήστες μια ενοποιημένη εικόνα της υγείας τους. Το iOS 9 (2015) επικεντρώθηκε στη βελτίωση της απόδοσης και της σταθερότητας, προσθέτοντας επίσης τη λειτουργία Split View για το iPad, επιτρέποντας τη χρήση δύο εφαρμογών ταυτόχρονα.

3.2.2 Σύγχρονες Εκδόσεις (2016-σήμερα)

Οι πιο πρόσφατες εκδόσεις του iOS συνεχίζουν να προσθέτουν νέες δυνατότητες και βελτιώσεις. Για παράδειγμα, το iOS 10 (2016) έφερε αναβαθμίσεις στη Siri και το iMessage, ενώ το iOS 11 (2017) εισήγαγε το ARKit, καθιστώντας δυνατή τη δημιουργία εφαρμογών επαυξημένης πραγματικότητας. Το ARKit προσφέρει στους προγραμματιστές ένα ισχυρό εργαλείο για τη δημιουργία εφαρμογών που συνδυάζουν τον φυσικό και τον ψηφιακό κόσμο.

Το iOS 12 (2018) επικεντρώθηκε στη βελτίωση της απόδοσης και της σταθερότητας, ειδικά για παλαιότερες συσκευές, ενώ εισήγαγε επίσης το Screen Time, το οποίο επιτρέπει στους χρήστες να παρακολουθούν και να περιορίζουν τον χρόνο που περνούν στις συσκευές τους. Το iOS 13 (2019) έφερε το Dark Mode, βελτιώσεις στην απόδοση και νέες δυνατότητες ασφάλειας, ενώ το iOS 14 (2020) εισήγαγε widgets στην αρχική οθόνη, τη βιβλιοθήκη εφαρμογών και το App Clips.

Οι τελευταίες εκδόσεις, όπως το iOS 15 (2021) και το iOS 16 (2022), προσέφεραν νέα εργαλεία για την προσαρμογή της οθόνης Αφετηρίας, βελτιώσεις στην ασφάλεια και την ιδιωτικότητα, καθώς και νέα χαρακτηριστικά όπως οι βελτιώσεις στις βιντεοκλήσεις μέσω FaceTime και οι νέες δυνατότητες επικοινωνίας μέσω των εφαρμογών Messages και Mail.

Εικόνα 29. iOS versions

Πηγή : https://medium.com/@vpradeep071997/ios-versions-a-history-of-apples-mobile-operating-system-ec82f24d71b7

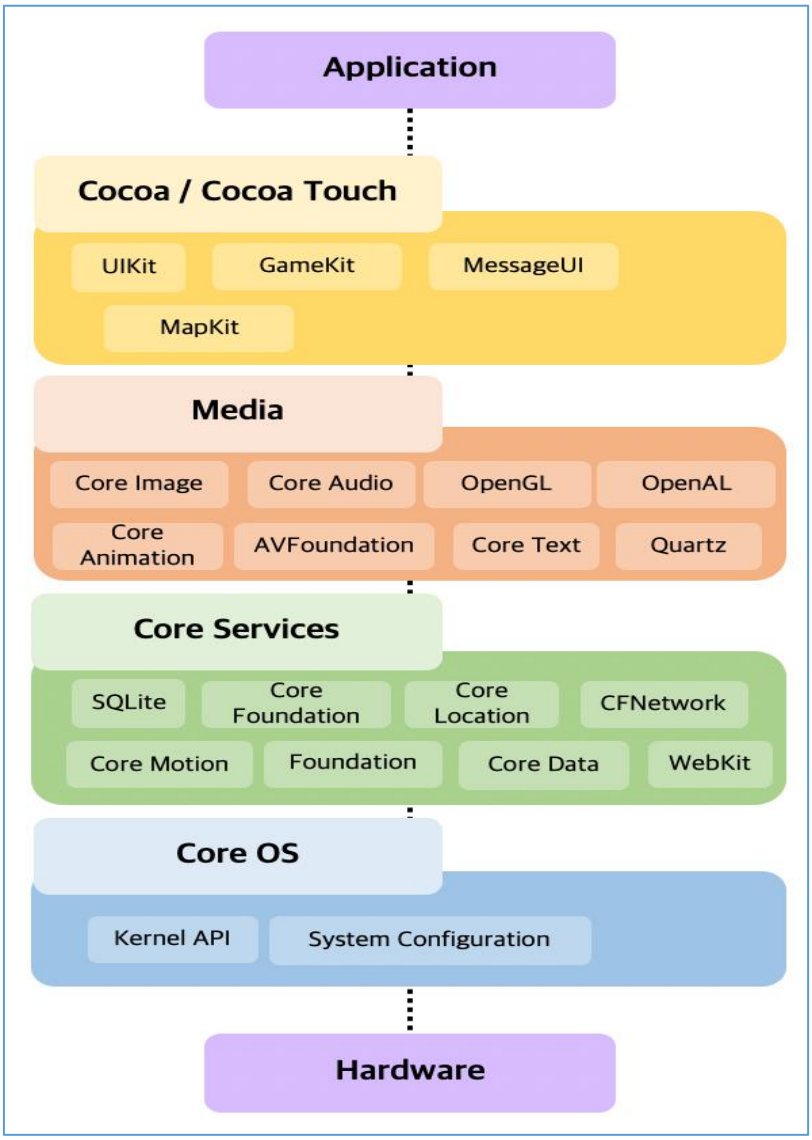
3.2.3 Αρχιτεκτονική του iOS

Η αρχιτεκτονική του iOS αποτελείται από πέντε κύρια επίπεδα:

- **Core OS:** Το βασικό επίπεδο του iOS που παρέχει τις χαμηλού επιπέδου λειτουργίες του συστήματος, όπως η διαχείριση μνήμης, το file system, οι δικτυακές συνδέσεις και οι drivers για το hardware. Περιλαμβάνει επίσης τα θεμελιώδη στοιχεία ασφαλείας του συστήματος, όπως το Secure Enclave και το Data Protection. Το Secure Enclave είναι ένας συνεπεξεργαστής που ενσωματώνεται σε συσκευές της Apple για την προστασία των κρυπτογραφικών κλειδιών και την εκτέλεση ασφαλών λειτουργιών. Χρησιμοποιείται για την προστασία των βιομετρικών δεδομένων που σχετίζονται με το Touch ID και το Face ID, καθώς και για την κρυπτογράφηση αρχείων και μηνυμάτων.
- **Core Services:** Περιλαμβάνει βασικές υπηρεσίες συστήματος όπως το Core Foundation, το Foundation Framework και το SQLite για διαχείριση βάσεων δεδομένων. Αυτές οι υπηρεσίες παρέχουν λειτουργίες όπως η διαχείριση των δεδομένων, η επικοινωνία μεταξύ των διεργασιών και η υποστήριξη για διεργασίες στο παρασκήνιο. Το Core Data παρέχει ένα ισχυρό εργαλείο για τη διαχείριση αντικειμένων και τη μοντελοποίηση δεδομένων. Το Core Data επιτρέπει στους προγραμματιστές να διαχειρίζονται τα δεδομένα της εφαρμογής τους μέσω ενός αντικειμενοστραφούς API. Παρέχει υποστήριξη για διάφορους τύπους αποθήκευσης δεδομένων, όπως SQLite, XML και binary, διευκολύνοντας τη δημιουργία και τη διαχείριση των δεδομένων της εφαρμογής.
- **Media:** Αυτό το επίπεδο περιλαμβάνει τα γραφικά, τον ήχο και τις τεχνολογίες βίντεο. Περιλαμβάνει το Core Graphics για δισδιάστατα γραφικά, το Core Animation για κινούμενες εικόνες και το AVFoundation για αναπαραγωγή πολυμέσων. Το Metal προσφέρει ένα σύγχρονο API για υψηλής απόδοσης γραφικά και υπολογισμούς, επιτρέποντας στους προγραμματιστές να δημιουργούν σύνθετα και αποδοτικά γραφικά περιβάλλοντα. Το AVFoundation είναι ένα ισχυρό framework που επιτρέπει στους προγραμματιστές να διαχειρίζονται και να αναπαράγουν ήχο και βίντεο. Παρέχει εργαλεία για την επεξεργασία πολυμέσων, την καταγραφή ήχου και βίντεο και την ενσωμάτωση λειτουργιών πολυμέσων στις εφαρμογές τους.
- **Cocoa Touch:** Το επίπεδο Cocoa Touch παρέχει τα πλαίσια για τη δημιουργία εφαρμογών για την πλατφόρμα iOS. Περιλαμβάνει το UIKit για τη δημιουργία και διαχείριση της διεπαφής χρήστη, το MapKit για την ενσωμάτωση χαρτών και το GameKit για την ανάπτυξη παιχνιδιών. Το UIKit είναι το κύριο εργαλείο για τη δημιουργία της διεπαφής χρήστη στο iOS, προσφέροντας πλούσια λειτουργικότητα και ευελιξία για την ανάπτυξη εφαρμογών με φιλικό και ελκυστικό περιβάλλον χρήστη. Το UIKit παρέχει εργαλεία και κλάσεις για τη διαχείριση των στοιχείων της διεπαφής χρήστη, όπως τα κουμπιά, τα πλαίσια

κειμένου και οι πίνακες. Προσφέρει επίσης υποστήριξη για την αναγνώριση gestures, την επεξεργασία κειμένου και την προσαρμογή της διεπαφής χρήστη στις ανάγκες της εφαρμογής.

- **User Experience:** Το επίπεδο αυτό περιλαμβάνει όλα τα χαρακτηριστικά που αλληλοεπιδρούν άμεσα με τον χρήστη, όπως τα γραφικά στοιχεία της διεπαφής χρήστη, τα animations και οι gestures. Το iOS παρέχει μια συνεπή και ευέλικτη εμπειρία χρήστη μέσω του Human Interface Guidelines, που καθοδηγεί τους προγραμματιστές στο σχεδιασμό εφαρμογών με φιλικό και κατανοητό περιβάλλον χρήστη. Το Human Interface Guidelines περιλαμβάνει οδηγίες για το σχεδιασμό της διεπαφής χρήστη, την αλληλεπίδραση με τον χρήστη και την προσβασιμότητα. Αυτές οι οδηγίες βοηθούν τους προγραμματιστές να δημιουργούν εφαρμογές που είναι εύχρηστες και προσβάσιμες σε όλους τους χρήστες, ανεξαρτήτως των ικανοτήτων τους.



Εικόνα 30. iOS Architecture

Πηγή : https://medium.com/@ganeshrajugalla/ios-ios-introduction-and-structure-fdd7ecf08c4c

3.2.4 Τεχνικές Λεπτομέρειες και Αναλύσεις

Η **διαχείριση μνήμης** στο iOS γίνεται μέσω του Automatic Reference Counting (ARC), που αυτοματοποιεί τη διαχείριση της διάρκειας ζωής των αντικειμένων, αποφεύγοντας διαρροές μνήμης και διευκολύνοντας τους προγραμματιστές στη δημιουργία αποδοτικών εφαρμογών. Το ARC διασφαλίζει ότι τα αντικείμενα αποδεσμεύονται αυτόματα όταν δεν χρειάζονται πλέον, ελαχιστοποιώντας τον κίνδυνο διαρροών μνήμης. Το ARC χρησιμοποιεί αναφορές καταμέτρησης για να παρακολουθεί πόσες αναφορές υπάρχουν σε κάθε αντικείμενο. Όταν ο αριθμός των αναφορών ενός αντικειμένου γίνει μηδέν, το αντικείμενο αποδεσμεύεται αυτόματα, απελευθερώνοντας τη μνήμη που κατείχε.

Η **ασφάλεια** αποτελεί βασικό στοιχείο του iOS, με ενσωματωμένα χαρακτηριστικά όπως το Touch ID, το Face ID και το Secure Enclave. Το Secure Enclave αποθηκεύει και προστατεύει τα βιομετρικά δεδομένα και τα κρυπτογραφικά κλειδιά, ενώ το Data Protection κρυπτογραφεί τα δεδομένα της συσκευής για την προστασία της ιδιωτικότητας των χρηστών. Το Touch ID και το Face ID παρέχουν ασφαλείς και γρήγορους τρόπους επαλήθευσης της ταυτότητας του χρήστη, χρησιμοποιώντας δακτυλικά αποτυπώματα και αναγνώριση προσώπου αντίστοιχα. Αυτά τα συστήματα ασφαλείας χρησιμοποιούν προηγμένες τεχνολογίες για την αποθήκευση και την επεξεργασία των βιομετρικών δεδομένων, εξασφαλίζοντας ότι τα δεδομένα αυτά παραμένουν προστατευμένα και ιδιωτικά.

Το **Data Protection** χρησιμοποιεί κρυπτογράφηση AES-256 για την προστασία των δεδομένων της συσκευής, διασφαλίζοντας ότι τα δεδομένα των χρηστών παραμένουν ασφαλή ακόμη και αν η συσκευή χαθεί ή κλαπεί. Η κρυπτογράφηση των δεδομένων πραγματοποιείται αυτόματα και διαφανώς για τον χρήστη, παρέχοντας μια επιπλέον στρώση προστασίας χωρίς να απαιτείται επιπλέον προσπάθεια από τον χρήστη.

3.2.5 Παραδείγματα Εφαρμογών iOS

Οι **εφαρμογές υγείας** στο iOS, όπως το HealthKit, επιτρέπουν τη συλλογή και την κοινή χρήση δεδομένων υγείας. Για παράδειγμα, μια εφαρμογή παρακολούθησης φυσικής κατάστασης μπορεί να συλλέγει δεδομένα από τους αισθητήρες της συσκευής και να τα μοιράζεται με άλλες εφαρμογές υγείας, προσφέροντας μια ολοκληρωμένη εικόνα της υγείας του χρήστη. Το HealthKit παρέχει ένα κοινό πρωτόκολλο για τη διαχείριση δεδομένων υγείας, επιτρέποντας στις εφαρμογές να συνεργάζονται και να μοιράζονται δεδομένα με ασφάλεια. Αυτό διευκολύνει τη δημιουργία εφαρμογών που προσφέρουν ολοκληρωμένες λύσεις για την παρακολούθηση και τη βελτίωση της υγείας του χρήστη.

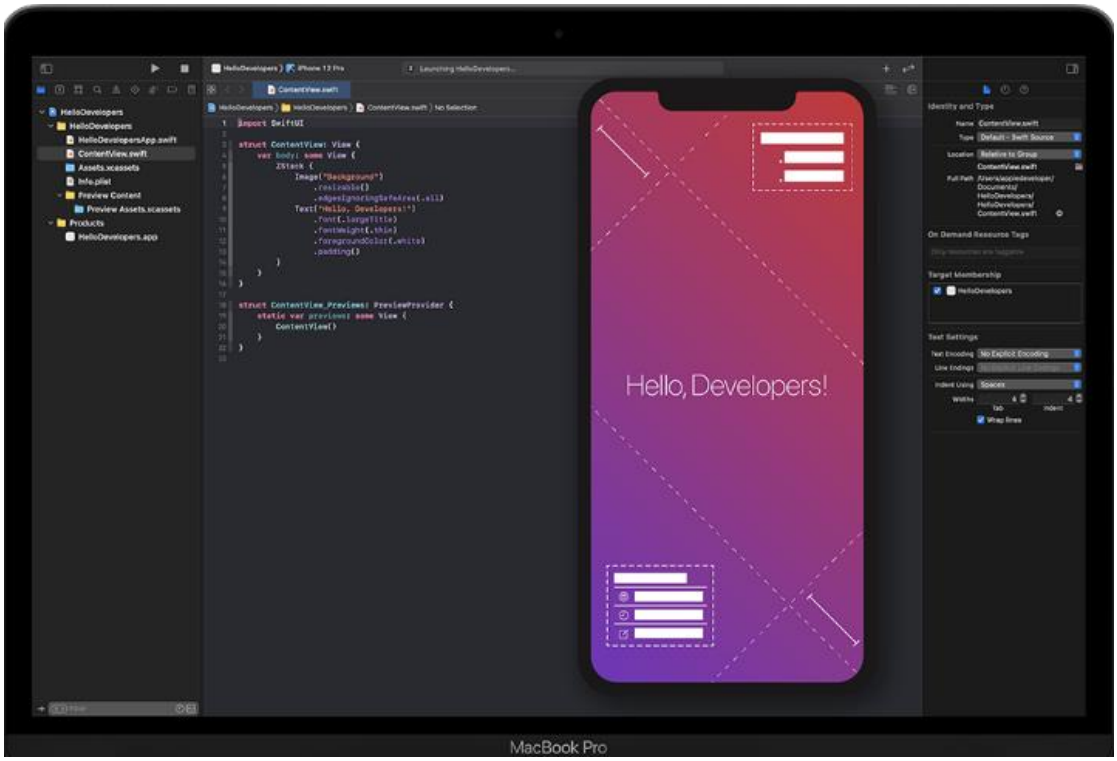
Το **ARKit** επιτρέπει τη δημιουργία εφαρμογών επαυξημένης πραγματικότητας που ενσωματώνουν εικονικά αντικείμενα στον φυσικό κόσμο. Για παράδειγμα, μια εφαρμογή διακόσμησης εσωτερικών χώρων μπορεί να επιτρέπει στους χρήστες να τοποθετούν εικονικά έπιπλα στο δωμάτιό τους, βλέποντας πώς θα φαίνονται πριν τα

αγοράσουν. Το ARKit χρησιμοποιεί την κάμερα της συσκευής και αισθητήρες για την ανίχνευση του περιβάλλοντος και την τοποθέτηση εικονικών αντικειμένων στον φυσικό κόσμο. Παρέχει ακριβή ανίχνευση επιπέδων, φωτισμού και κίνησης, επιτρέποντας τη δημιουργία ρεαλιστικών και αποδοτικών εφαρμογών επαυξημένης πραγματικότητας.

3.2.6 Ανάπτυξη Εφαρμογών για το iOS

Η ανάπτυξη εφαρμογών για το iOS γίνεται κυρίως μέσω της χρήσης της γλώσσας προγραμματισμού Swift και του IDE Xcode. Οι προγραμματιστές έχουν πρόσβαση σε ένα ευρύ φάσμα εργαλείων και frameworks που τους επιτρέπουν να δημιουργούν εφαρμογές με πλούσια λειτουργικότητα και υψηλή απόδοση.

Το **Xcode** είναι το ολοκληρωμένο περιβάλλον ανάπτυξης της Apple για τη δημιουργία εφαρμογών iOS, macOS, watchOS και tvOS. Προσφέρει όλα τα απαραίτητα εργαλεία για την ανάπτυξη, τη δοκιμή και την αποσφαλμάτωση εφαρμογών. Περιλαμβάνει το Interface Builder για τον σχεδιασμό γραφικών διεπαφών χρήστη, το Simulator για την εκτέλεση και τη δοκιμή εφαρμογών σε εικονικές συσκευές και το Instruments για την ανάλυση της απόδοσης και της κατανάλωσης ενέργειας των εφαρμογών.

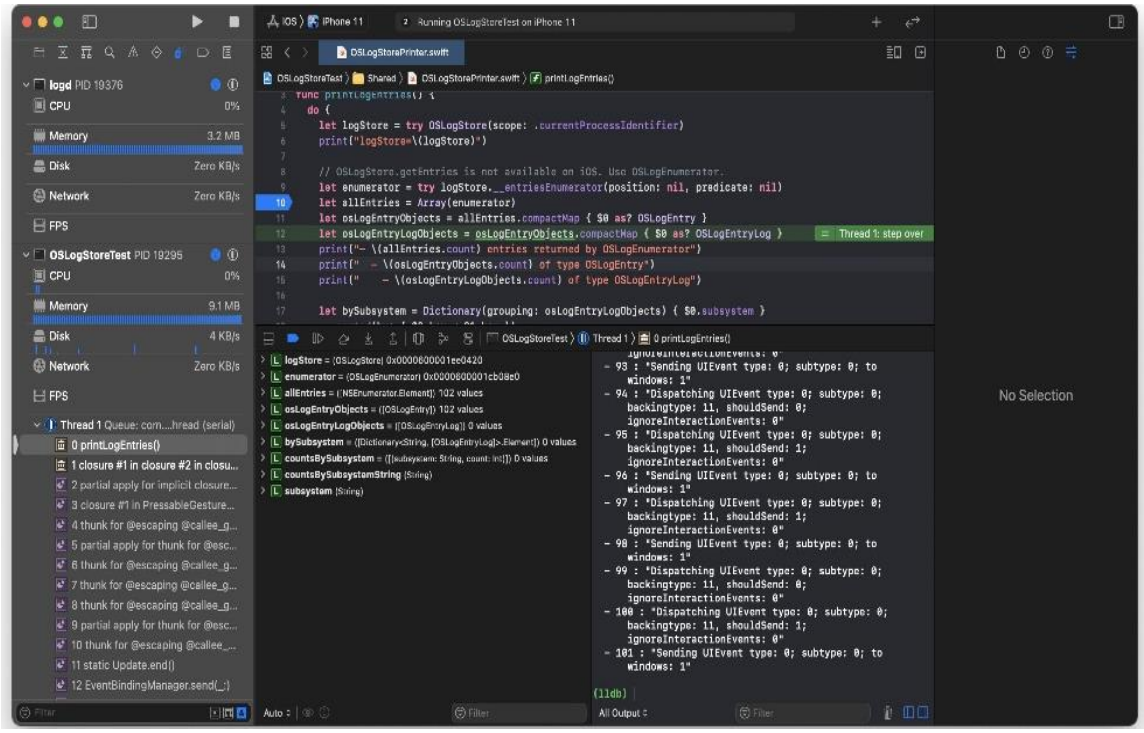


Εικόνα 31. Xcode

Πηγή : https://developer.apple.com/xcode/resources/

Η **Swift** είναι μια σύγχρονη γλώσσα προγραμματισμού που αναπτύχθηκε από την Apple για τη δημιουργία εφαρμογών iOS, macOS, watchOS και tvOS. Προσφέρει μια

καθαρή και ευανάγνωστη σύνταξη, καθώς και ισχυρά χαρακτηριστικά όπως η ασφάλεια τύπων και η αυτόματη διαχείριση μνήμης. Η Swift είναι σχεδιασμένη για να είναι ταυτόχρονα ισχυρή και εύκολη στη χρήση, επιτρέποντας στους προγραμματιστές να δημιουργούν αποδοτικές και ασφαλείς εφαρμογές με λιγότερο κώδικα. Η Swift παρέχει υποστήριξη για διάφορα σύγχρονα χαρακτηριστικά προγραμματισμού, όπως τα closures, τα generics και τα protocols, επιτρέποντας στους προγραμματιστές να δημιουργούν κώδικα που είναι ευέλικτος και επαναχρησιμοποιήσιμος. Η γλώσσα έχει επίσης ενσωματωμένα εργαλεία για την ασφάλεια και την αποφυγή σφαλμάτων, όπως τα optional types, που βοηθούν στην αποφυγή null pointer exceptions.



Εικόνα 32. Swift

Πηγή : https://steipete.com/posts/logging-in-swift/

Το **Interface Builder** επιτρέπει στους προγραμματιστές να σχεδιάζουν και να διαμορφώνουν τις διεπαφές χρήστη των εφαρμογών τους χρησιμοποιώντας ένα γραφικό περιβάλλον. Παρέχει εργαλεία για τη δημιουργία και τη διαχείριση των στοιχείων της διεπαφής χρήστη, διευκολύνοντας τη διαδικασία ανάπτυξης και καθιστώντας τη σχεδίαση της διεπαφής πιο αποτελεσματική και αποδοτική.

Το **Simulator** επιτρέπει στους προγραμματιστές να εκτελούν και να δοκιμάζουν τις εφαρμογές τους σε εικονικές συσκευές, προσομοιώνοντας διάφορα μοντέλα iPhone και iPad. Αυτό διευκολύνει τη διαδικασία δοκιμής και το debugging, επιτρέποντας στους προγραμματιστές να εντοπίζουν και να επιδιορθώνουν προβλήματα πριν την κυκλοφορία της εφαρμογής.

Το **Instruments** είναι ένα ισχυρό εργαλείο ανάλυσης που επιτρέπει στους προγραμματιστές να παρακολουθούν και να αναλύουν την απόδοση της εφαρμογής

τους. Παρέχει λεπτομερή δεδομένα για την κατανάλωση CPU, τη χρήση μνήμης, την κατανάλωση ενέργειας και την απόδοση του δικτύου, βοηθώντας τους προγραμματιστές να βελτιστοποιήσουν τις εφαρμογές τους για καλύτερη απόδοση και αποδοτικότητα.

3.2.7 Frameworks και APIs

Η Apple παρέχει μια μεγάλη ποικιλία frameworks και APIs που επιτρέπουν στους προγραμματιστές να προσθέτουν πλούσια λειτουργικότητα στις εφαρμογές τους. Αυτά περιλαμβάνουν το UIKit για τη δημιουργία διεπαφών χρήστη, το Core Data για τη διαχείριση δεδομένων, το AVFoundation για την αναπαραγωγή πολυμέσων και το Core ML για την ενσωμάτωση μηχανικής μάθησης.

Το Core ML είναι ένα ισχυρό framework που επιτρέπει στους προγραμματιστές να ενσωματώνουν μοντέλα μηχανικής μάθησης στις εφαρμογές τους. Υποστηρίζει διάφορους τύπους μοντέλων, όπως νευρωνικά δίκτυα, δέντρα αποφάσεων και αλγόριθμους στατιστικής μάθησης, επιτρέποντας τη δημιουργία εφαρμογών με προηγμένες δυνατότητες ανάλυσης και πρόβλεψης. Το Core ML επιτρέπει στους προγραμματιστές να χρησιμοποιούν προεκπαιδευμένα μοντέλα ή να εκπαιδεύουν τα δικά τους μοντέλα χρησιμοποιώντας εργαλεία όπως το Create ML και το Turi Create. Τα μοντέλα μπορούν να ενσωματωθούν στις εφαρμογές iOS και να χρησιμοποιηθούν για διάφορες λειτουργίες, όπως η αναγνώριση εικόνων, η ανάλυση κειμένου και η πρόβλεψη δεδομένων.

3.2.8 Οικοσύστημα iOS

Το iOS αποτελεί μέρος ενός ευρύτερου οικοσυστήματος συσκευών και υπηρεσιών της Apple, που περιλαμβάνει το macOS, το watchOS, το tvOS και το iCloud. Η ενσωμάτωση αυτών των συσκευών και υπηρεσιών επιτρέπει στους χρήστες να απολαμβάνουν μια ενιαία και συντονισμένη εμπειρία χρήστη.

Συγχρονισμός και Συνεργασία: Η ενσωμάτωση του iOS με άλλες συσκευές και υπηρεσίες της Apple, όπως το iCloud, το Handoff και το Continuity, επιτρέπει τον απρόσκοπτο συγχρονισμό και τη συνεργασία μεταξύ συσκευών. Το Handoff επιτρέπει στους χρήστες να ξεκινούν μια δραστηριότητα σε μια συσκευή και να την ολοκληρώνουν σε μια άλλη, ενώ το Continuity επιτρέπει τη χρήση χαρακτηριστικών όπως το Universal Clipboard και οι κλήσεις από το Mac. Το Universal Clipboard επιτρέπει στους χρήστες να αντιγράφουν και να επικολλούν κείμενο, εικόνες και άλλα δεδομένα μεταξύ συσκευών iOS και macOS. Αυτή η δυνατότητα διευκολύνει τη μεταφορά δεδομένων μεταξύ συσκευών, καθιστώντας την εργασία πιο αποτελεσματική και παραγωγική. Οι κλήσεις από το Mac επιτρέπουν στους χρήστες να πραγματοποιούν και να δέχονται τηλεφωνικές κλήσεις απευθείας από το Mac τους, χρησιμοποιώντας τη σύνδεση του iPhone τους. Αυτό διευκολύνει την επικοινωνία, επιτρέποντας στους χρήστες να παραμένουν συνδεδεμένοι χωρίς να χρειάζεται να αλλάζουν συσκευές.

Οικοσύστημα Εφαρμογών: Το App Store παρέχει πρόσβαση σε εκατομμύρια εφαρμογές, καλύπτοντας ένα ευρύ φάσμα κατηγοριών, από παιχνίδια και ψυχαγωγία έως επιχειρήσεις και παραγωγικότητα. Η αυστηρή διαδικασία έγκρισης της Apple εξασφαλίζει ότι οι εφαρμογές πληρούν υψηλά πρότυπα ποιότητας και ασφάλειας. Η διαδικασία έγκρισης της Apple περιλαμβάνει μια σειρά ελέγχων για τη διασφάλιση της ποιότητας και της ασφάλειας των εφαρμογών. Οι εφαρμογές πρέπει να πληρούν τις κατευθυντήριες γραμμές της Apple για το σχεδιασμό, τη λειτουργικότητα και την ασφάλεια πριν εγκριθούν για κυκλοφορία στο App Store. Αυτή η διαδικασία εξασφαλίζει ότι οι χρήστες μπορούν να εμπιστεύονται τις εφαρμογές που κατεβάζουν και να απολαμβάνουν μια ασφαλή και αποδοτική εμπειρία χρήστη.

3.2.9 Ανάπτυξη και Υποστήριξη

Η Apple παρέχει συνεχή υποστήριξη για το iOS μέσω τακτικών ενημερώσεων και αναβαθμίσεων λογισμικού, διασφαλίζοντας ότι οι συσκευές παραμένουν ασφαλείς και ενημερωμένες με τις τελευταίες δυνατότητες. Οι προγραμματιστές έχουν πρόσβαση σε εκτενή τεκμηρίωση, παραδείγματα κώδικα και υποστήριξη μέσω της κοινότητας των προγραμματιστών της Apple. Η Apple παρέχει τακτικές ενημερώσεις λογισμικού που περιλαμβάνουν βελτιώσεις ασφάλειας, διορθώσεις σφαλμάτων και νέες δυνατότητες. Αυτές οι ενημερώσεις διασφαλίζουν ότι οι συσκευές παραμένουν ασφαλείς και αποδοτικές, ενώ παρέχουν στους χρήστες πρόσβαση στις τελευταίες τεχνολογίες και δυνατότητες. Η κοινότητα των προγραμματιστών της Apple παρέχει υποστήριξη και καθοδήγηση στους προγραμματιστές, επιτρέποντάς τους να μοιράζονται γνώσεις, να ανταλλάσσουν ιδέες και να συνεργάζονται για την ανάπτυξη καλύτερων εφαρμογών. Η Apple διοργανώνει επίσης το ετήσιο Worldwide Developers Conference (WWDC), όπου οι προγραμματιστές μπορούν να μάθουν για τις τελευταίες τεχνολογίες και να συμμετάσχουν σε εργαστήρια και παρουσιάσεις.

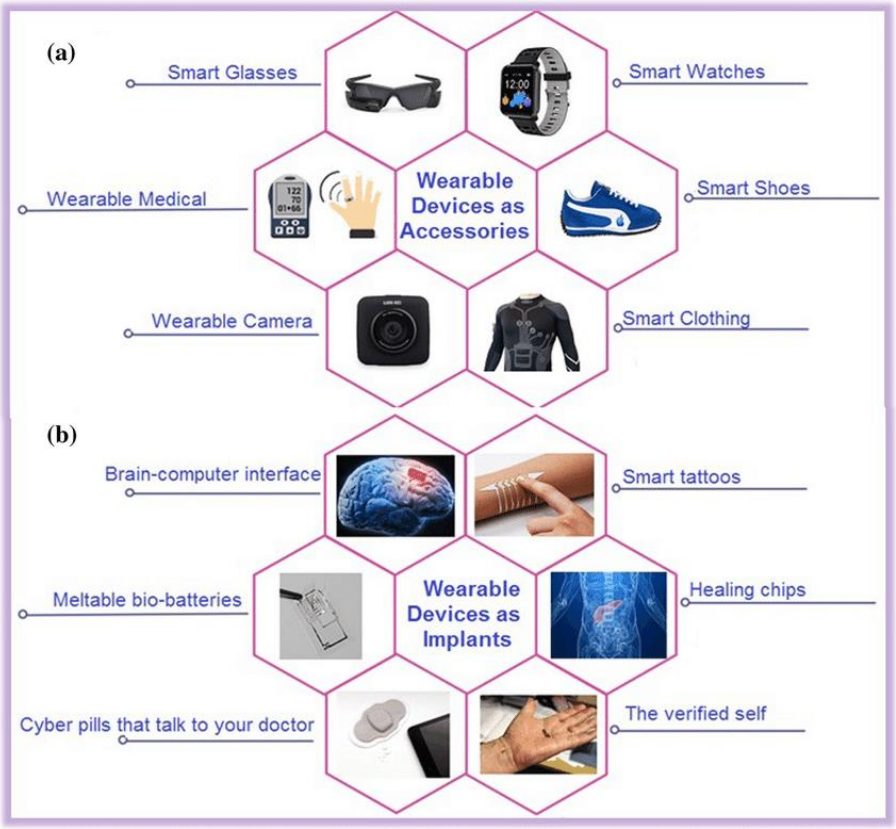
3.3 Mobile Attack Vectors

Η τεχνολογία του Android έχει πολλές εφαρμογές στην καθημερινή ζωή. Τα κινητά με λειτουργικό σύστημα Android χρησιμοποιούνται σε εστιατόρια και ξενοδοχεία, στις χρηματοοικονομικές υπηρεσίες, στον δημόσιο τομέα, στο λιανικό εμπόριο και σε άλλους τομείς. Μεγάλες εταιρείες χρησιμοποιούν κινητές εφαρμογές για το branding, το μάρκετινγκ και πολλά επαγγελματικά έργα, ενώ και οι μικρές και μεσαίες επιχειρήσεις δημιουργούν τις δικές τους εφαρμογές. Υπάρχουν πολλές τάσεις στην τεχνολογία Android που καθηλώνουν τους χρήστες και ενδιαφέρουν τις επιχειρήσεις. Αναμένεται αυτές οι τάσεις να εξελιχθούν γρήγορα στα επόμενα χρόνια, ανοίγοντας το δρόμο για νέες εξελίξεις και νέες εφαρμογές των κινητών Android. Μερικές από αυτές τις τάσεις περιλαμβάνουν την εξάπλωση των συσκευών Internet of Things (IoT), την υιοθέτηση των Accelerated Mobile Pages (AMP), την άνοδο των εφαρμογών πληρωμών μέσω κινητού, τη δημοτικότητα των εφαρμογών on-demand για υπηρεσίες, την ανάπτυξη εφαρμογών επιχειρήσεων που προσαρμόζονται στις ανάγκες

της επιχείρησης, τη μετάβαση σε εφαρμογές βασισμένες στο cloud, και την εμφάνιση των Android Instant Apps. Καθώς η τεχνολογία Android συνεχίζει να κυριαρχεί σε διάφορους τομείς, η διασφάλιση της ασφάλειας αυτών των εφαρμογών γίνεται πρωταρχικής σημασίας. Οι ειδικοί στον τομέα θα πρέπει να επικεντρωθούν στην εφαρμογή αξιόπιστων μέτρων ασφαλείας για την προστασία των δεδομένων και της ιδιωτικότητας των χρηστών μέσα στον αυξανόμενο πολύπλοκο και εξελισσόμενο κόσμο των κινητών τεχνολογιών.

3.3.1 Internet of Things (IoT) and Wearable Apps

Το Διαδίκτυο των Πραγμάτων (Internet of Things - IoT) δεν αντιπροσωπεύει απλώς μια προσωρινή τάση, αλλά μια προσπάθεια για την αυτοματοποίηση και διευκόλυνση διαφόρων επιχειρηματικών προγραμμάτων. Έννοιες όπως έξυπνα σπίτια, έξυπνες πόλεις, βιομηχανικό IoT, αυτοκινητοβιομηχανία, έξυπνη υγεία και έξυπνο λιανικό αναπτύσσονται. Παρόλο που μπορεί να απαιτηθεί λίγο περισσότερος χρόνος για το IoT να εξελιχθεί πλήρως, είναι σίγουρα ένας αναπτυσσόμενος τομέας. Το Διαδίκτυο των Πραγμάτων (IoT) αναφέρεται στην αυξανόμενη διασύνδεση διαφόρων έξυπνων συσκευών μέσω του Διαδικτύου. Αυτές οι συσκευές διαθέτουν αισθητήρες και συνδεσιμότητα στο Διαδίκτυο που τους επιτρέπει να λαμβάνουν, να συλλέγουν και να μεταδίδουν πληροφορίες.



Εικόνα 33. Examples of types of wearable devices

Πηγή :
https://www.researchgate.net/publication/359293792_The_status_and_perspectives_of_nanostructured_materials_and_fabrication_processes_for_wearable_piezoresistive_sensors/figures?lo=1

Οι περισσότερες έξυπνες συσκευές λειτουργούν με το λειτουργικό σύστημα Android της Google. Οποιοσδήποτε είναι εξοικειωμένος με τα έξυπνα τηλέφωνα γνωρίζει επίσης αυτό το λειτουργικό σύστημα. Ο λόγος για τον οποίο το IoT συσχετίζεται τόσο πολύ με την τεχνολογία Android είναι οι εφαρμογές που χρησιμοποιεί το IoT. Το Android είναι αυτή τη στιγμή η μεγαλύτερη πλατφόρμα εφαρμογών στον κόσμο λόγω του ανοικτού χαρακτήρα του. Οι συσκευές με την κατάλληλη εφαρμογή μπορούν να προσαρμοστούν εύκολα στις ανάγκες του χρήστη. Οι αισθητήρες στις συσκευές συνήθως κατασκευάζονται σε λειτουργικό σύστημα Linux ή Android και η συνδυασμένη χρήση συμβατού υλικού με λογισμικό είναι αυτό που καθιστά εύκολη τη δημιουργία φορητών συσκευών ή συσκευών που διευκολύνουν την καθημερινή ζωή.

3.3.2 Mobile Payments

Οι κινητές πληρωμές αντιπροσωπεύουν έναν ταχέως επεκτεινόμενο τομέα εντός της τεχνολογίας του Android. Σήμερα, οι πελάτες συχνά χρησιμοποιούν τα κινητά τους τηλέφωνα για να πραγματοποιούν συναλλαγές, καθιστώντας τις κινητές πληρωμές αναπόσπαστο κομμάτι της καθημερινότητας. Πολλές εταιρείες προσφέρουν εφαρμογές που σχεδιάστηκαν ειδικά για να διευκολύνουν τις ασφαλείς πληρωμές και άλλες συναλλαγές. Οι μεγάλες τράπεζες έχουν αναπτύξει τις δικές τους κινητές εφαρμογές, μετατρέποντας τα smartphones σε ψηφιακά πορτοφόλια. Με μέτρα ασφαλείας που αντιστοιχούν σε αυτά των ιστοσελίδων ηλεκτρονικής τραπεζικής, οι χρήστες είναι όλο και πιο άνετοι να υιοθετήσουν αυτές τις λύσεις πληρωμών μέσω κινητού.

Ενώ ο τραπεζικός τομέας αποτελεί ένα εμφανές παράδειγμα, οι διαδικτυακοί λιανοπωλητές προσπαθούν επίσης να κερδίσουν την προσοχή των πελατών προσφέροντας άνετες εμπειρίες πληρωμών. Τα κρυπτονομίσματα και άλλα ψηφιακά νομίσματα συμβάλλουν επίσης στη διάδοση των διαδικτυακών υπηρεσιών πληρωμών, συχνά εκμεταλλευόμενα εφαρμογές για τη διευκόλυνση των συναλλαγών. Αυτές οι εφαρμογές πληρωμών είναι συμβατές όχι μόνο με κινητές συσκευές, αλλά και με φορητές τεχνολογίες. Οι χρήστες μπορούν εύκολα να εγκαταστήσουν και να χρησιμοποιήσουν αυτές τις εφαρμογές, αισθανόμενοι ασφάλεια λόγω των μέτρων που έχουν ληφθεί από τους παρόχους. Για παράδειγμα, αν μια τράπεζα εγγυάται ασφάλεια στην ιστοσελίδα της, οι χρήστες μπορούν να εμπιστευτούν ότι το ίδιο επίπεδο ασφαλείας ισχύει και για τις συναλλαγές μέσω κινητού.

Επιπλέον, οι εταιρείες μάρκετινγκ εκμεταλλεύονται τη δυνατότητα της τεχνολογίας κινητών πληρωμών. Μέσω της ανάλυσης δεδομένων, αυτές οι εταιρείες αποκτούν πολύτιμες πληροφορίες για τις προτιμήσεις των πελατών, βελτιώνοντας κατ' επέκταση τις μεθόδους πληρωμών για τη βελτίωση της εμπειρίας του χρήστη. Μέσω της ανάλυσης υπαρχουσών εφαρμογών και συμπεριφορών πελατών, αυτές οι εταιρείες μπορούν να προβλέψουν τις μελλοντικές τάσεις και να προσφέρουν συμπληρωματικές υπηρεσίες σε διαδικτυακά καταστήματα. Αν και υπάρχουν αμφιβολίες σχετικά με την ασφάλεια και την εμπειρία χρήστη των πληρωμών μέσω κινητού, οι τραπεζικές

ιδρύσεις κινούνται προς την ψηφιακή εξέλιξη λόγω του χαμηλού κόστους. Παρά τις ανησυχίες, η ευκολία και η αποτελεσματικότητα των κινητών πληρωμών συνεχίζουν να ωθούν την υιοθέτησή τους από τους καταναλωτές.

Εικόνα 34. Mobile Payments

Πηγή : https://www.cronj.com/blog/mobile-payment-app-development-how-to-develop-complete-guide/

3.3.3 On-Demand Apps

Οι εφαρμογές κατά παραγγελία δημιουργούνται και προσαρμόζονται σύμφωνα με συγκεκριμένες ανάγκες των χρηστών. Βασικά, αυτές οι εφαρμογές λειτουργούν ως μεσάζοντες μεταξύ των πελατών και των παρόχων διαφόρων υπηρεσιών. Αντί να αφιερώνουν χρόνο και προσπάθεια για να λάβουν αυτό που επιθυμούν, οι χρήστες προτιμούν να πληρώσουν ένα μικρό τέλος για έναν πιο γρήγορο και βολικό τρόπο που προσφέρονται από αυτού του τύπου τις εφαρμογές. Αυτές οι εφαρμογές καθιστούν τη ζωή των χρηστών πιο εύκολη και βολική, και μπορούν να τις χρησιμοποιήσουν σε υπηρεσίες καθαριότητας, υπηρεσίες ομορφιάς, παράδοση φαγητού, υπηρεσίες ταξί και πολλά άλλα πεδία. Η δημοφιλία τους οφείλεται στην ικανότητά τους να προσφέρουν ανεπανάληπτη βολικότητα, να παρέχουν πληροφορίες σχετικά με τη διαθεσιμότητα υπηρεσιών στην περιοχή και συχνά να υποστηρίζουν επίσης εύκολες μεθόδους

πληρωμής. Το Android αναδεικνύεται ως η ιδανική πλατφόρμα για την υλοποίηση τέτοιων λύσεων, καθώς προσφέρει ένα ελεύθερο και ανοικτό περιβάλλον για την προώθηση υπηρεσιών σε ένα ευρύ κοινό.

Εικόνα 35. Categories of on-demand service apps

Πηγή : https://vilmate.com/blog/on-demand-service-apps/

3.3.4 Enterprise Apps and BYOD

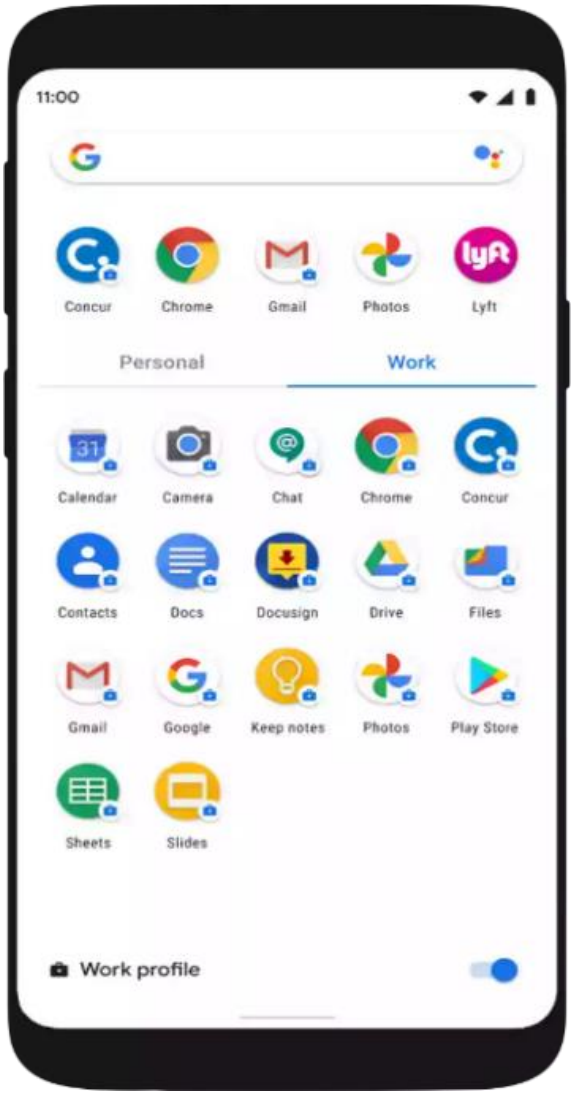
Ολοένα και περισσότεροι οργανισμοί υιοθετούν το μοντέλο "Φέρε τη Δική σου Συσκευή" (BYOD), με πολλούς να έχουν ήδη επενδύσει σε πρωτοβουλίες BYOD για τους εργαζομένους τους. Ωστόσο, η εφαρμογή αυτού του μοντέλου έχει τις προκλήσεις της. Ενώ η εργασία από το σπίτι μπορεί να σημαίνει χρήση προσωπικών συσκευών με επαγγελματικό λογισμικό, η εξασφάλιση αυτής της ομαλής ενσωμάτωσης δεν είναι πάντα εύκολη. Οι απαιτήσεις άδειας για προγράμματα μπορούν να προσθέσουν σημαντικά κόστη στους οργανισμούς, δυσχεραίνοντας το τοπίο του BYOD. Οι επιχειρησιακές εφαρμογές προσφέρουν μια απλοποιημένη λύση, επιτρέποντας στους εργαζομένους να εργάζονται από οπουδήποτε, ακόμα και από τα κινητά τους τηλέφωνα, ενώ παράλληλα παρέχουν στους διαχειριστές IT τη δυνατότητα να προσαρμόσουν προσαρμοσμένες ρυθμίσεις για αυτές τις εφαρμογές.

Οι υβριδικές εφαρμογές, λειτουργώντας ως κινητές ιστοσελίδες εντός του πλαισίου μιας εφαρμογής, επεκτείνουν ακόμη περισσότερο τις επιλογές για απομακρυσμένη εργασία. Οι ενσωματωμένες δυνατότητες διαχείρισης του Android επιτρέπουν στους διαχειριστές IT να διαχειρίζονται πλήρως τις συσκευές που χρησιμοποιούνται αποκλειστικά για εργασία.

Τόσο για τις συσκευές BYOD όσο και για τις εταιρικές συσκευές που χρησιμοποιούνται για προσωπικούς και επαγγελματικούς λόγους, οι διαχειριστές

μπορούν να δημιουργήσουν και να διαχειριστούν ξεχωριστά προφίλ εργασίας. Οι εφαρμογές που εγκαθίστανται μέσω του διαχειριζόμενου Google Play εγκαθίστανται στο προφίλ εργασίας, δίνοντας στους διαχειριστές πλήρη έλεγχο επί της εφαρμογής και των δεδομένων της, ενώ τα apps ή τα δεδομένα εκτός του προφίλ εργασίας παραμένουν ιδιωτικά για τον χρήστη.

Επιπλέον, το Android παρουσιάζει τον έννοια των προσωρινών χρηστών, ιδανική για περιπτώσεις όπου πολλοί χρήστες μοιράζονται μια μοναδική αφιερωμένη συσκευή. Αυτό περιλαμβάνει δημόσιες συνεδρίες χρήστη σε συσκευές, καθώς και μόνιμες συνεδρίες μεταξύ μιας σταθερής ομάδας χρηστών σε συσκευές, για παράδειγμα, για εργαζομένους που εργάζονται κατά βάρδιες. Η διαχειριζόμενη έκδοση του Google Play είναι διαθέσιμη για επιχειρήσεις και τους εργαζομένους τους για να έχουν πρόσβαση σε ένα πλούσιο οικοσύστημα εφαρμογών εργασίας και παραγωγικότητας και να βοηθήσουν τους οργανισμούς να μειώσουν το λειτουργικό κόστος και να αυξήσουν την παραγωγικότητα των εργαζομένων.



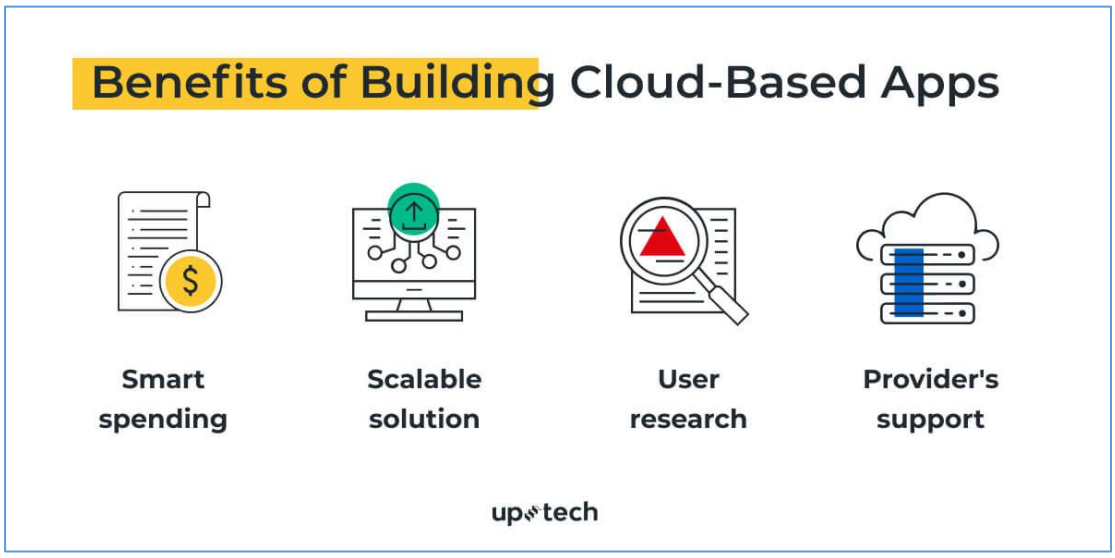
Εικόνα 36. Android Work Profile

Πηγή : https://www.appaloosa.io/android-work-profile

3.3.5 Cloud-based Apps

Με την αυξανόμενη χρήση της τεχνολογίας cloud, έχει γίνει πολύ πιο γρήγορο και εύκολο να αποκτηθούν δεδομένα χωρίς να επηρεάζεται η εσωτερική μνήμη του κινητού σας, επομένως οι προγραμματιστές κινητών εφαρμογών σχεδιάζουν περισσότερες εφαρμογές κινητής τηλεφωνίας που λειτουργούν με cloud. Με το Dropbox, το Google Drive και διάφορες άλλες εφαρμογές cloud, οι εφαρμογές κινητής τηλεφωνίας που λειτουργούν με cloud αυξάνονται ολοένα και περισσότερο. Οι εφαρμογές κινητής τηλεφωνίας που βασίζονται στο cloud είναι ιδιαίτερα ελκυστικές για τις επιχειρήσεις καθώς θα ανακουφίσουν σε μεγάλο βαθμό τα ζητήματα ασφάλειας δεδομένων που είναι ιδιαίτερα προβληματικά στο πλαίσιο της πολιτικής Bring Your Own Device (BYOD).

Ωστόσο, το cloud computing συνεπάγεται και με σημαντικές ανησυχίες όσον αφορά την ασφάλεια των δεδομένων. Προστατεύοντας ευαίσθητα εταιρικά δεδομένα σε συσκευές χρηστών μπορεί να αποτελέσει συνεχή πρόκληση, ειδικά όταν τα μέτρα κρυπτογράφησης και προστασίας με κωδικό πρόσβασης δεν υλοποιούνται σωστά. Μια παραβίαση ασφάλειας σε τέτοιες περιπτώσεις μπορεί να έχει σοβαρές συνέπειες. Επιπλέον, τα θέματα απόδοσης και συνδεσιμότητας αποτελούν άλλη συζήτηση, καθώς εξαρτώνται από την τοποθεσία του χρήστη. Ωστόσο, η cloud computing αντιπροσωπεύει σίγουρα το μέλλον της κινητής τεχνολογίας. Με την επέκταση της κάλυψης και τις συνεχείς τεχνολογικές προόδους, αναμένεται ότι αυτές οι ανησυχίες θα μειωθούν με τον καιρό.



Εικόνα 37. Benefits Of Developing Cloud-Based Apps

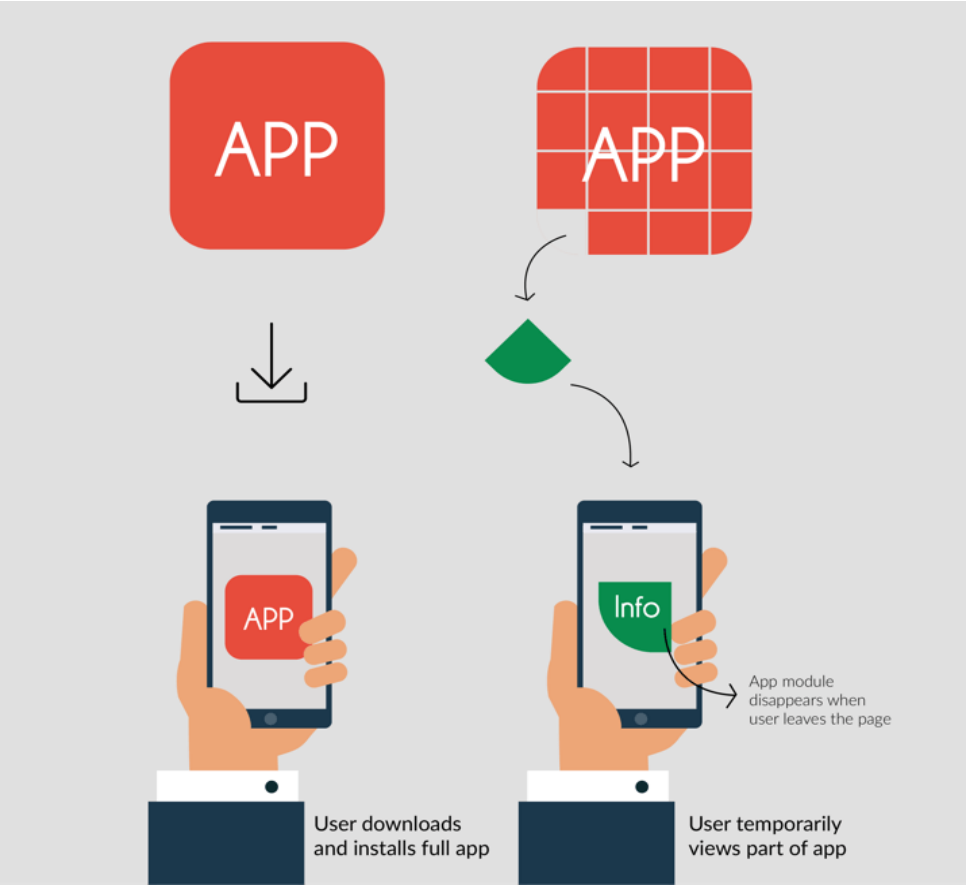
Πηγή : https://www.uptech.team/blog/cloud-based-application-development

3.3.6 Android Instant Apps

Τα Android Instant Apps επιτρέπουν σε φυσικές εφαρμογές Android να λειτουργούν χωρίς να χρειάζεται να εγκατασταθούν, ενεργοποιούμενες με την

εκκίνηση ενός URL. Αυτές οι άμεσες εφαρμογές μπορούν να χρησιμοποιούν διάφορες APIs του Android. Όταν το Google Play λαμβάνει ένα αίτημα για ένα URL που ταιριάζει με μια άμεση εφαρμογή, αποστέλλει τα απαραίτητα αρχεία κώδικα στη συσκευή Android που έστειλε το αίτημα. Στην ουσία, τα Android Instant Apps λειτουργούν διαμερίζοντας μια κινητή εφαρμογή σε μικρότερα μέρη που μπορούν να ληφθούν ξεχωριστά. Αυτά τα μέρη εκδίδονται στο Google Play. Όταν ένας χρήστης αναζητά ένα σχετικό ερώτημα στο Google, του παρέχεται ένας σύνδεσμος προς την αντίστοιχη Άμεση Εφαρμογή.

Τεχνικά, οι Android Instant Apps λειτουργούν με τον διαχωρισμό των φυσικών εφαρμογών σε μικρότερα μέρη, καθένα από τα οποία περιέχει συγκεκριμένα στοιχεία του πλήρους προϊόντος. Αυτές οι Άμεσες Εφαρμογές λειτουργούν ως συμπυκνωμένες εκδόσεις κινητών εφαρμογών, προσβάσιμες μέσω ιστότοπων. Ο τροχιόμετρος των Android Instant Apps μπορεί να είναι συγκρίσιμος με αυτόν των κανονικών ιστοσελίδων. Στον τομέα της ανάπτυξης εφαρμογών κινητής τηλεφωνίας κατά απαίτηση, ο στόχος δεν είναι να δημιουργηθούν εντελώς νέες εφαρμογές, αλλά να αναπτυχθούν δύο εκδόσεις: μια κανονική φυσική εφαρμογή και μια εκδοχή Άμεσης Εφαρμογής. Αυτές οι τεχνολογικές καινοτομίες έχουν σημαντικές προοπτικές ανάπτυξης, ειδικά σε βιομηχανίες όπως η ηλεκτρονική εμπορία, η ψυχαγωγία και τα ψώνια.



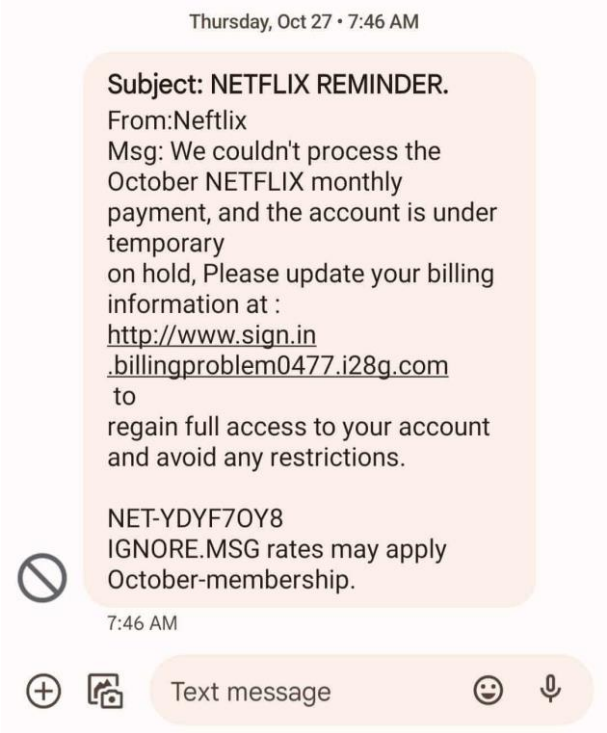
Εικόνα 38. Android Instant Apps

Πηγή : https://clevertap.com/blog/how-to-get-started-with-android-instant-apps/

3.3.7 Text Messaging

Τα μηνύματα αποτελούν ένα από τα πιο διαδεδομένα χαρακτηριστικά στις κινητές συσκευές, επιτρέποντας στους χρήστες να στέλνουν και να λαμβάνουν γρήγορα μηνύματα κειμένου (SMS). Παρά τους περιορισμούς στο μέγεθος, τα μηνύματα κειμένου διευκολύνουν τη σχεδόν άμεση επικοινωνία. Τα SMS, μαζί με τα ηλεκτρονικά μηνύματα, αποτελούν τον κύριο τρόπο γραπτής επικοινωνίας, εισάγοντας ένα νέο μονοπάτι για επιθέσεις κοινωνικής μηχανικής. Παραδοσιακά, το email ήταν το κύριο μέσο για ανεπιθύμητα μηνύματα και απάτες, αλλά οι προηγμένες λύσεις φιλτραρίσματος spam έχουν καταστήσει σχετικά εύκολο τον περιορισμό τέτοιων απειλών. Επιπλέον, οι χρήστες έχουν γίνει πιο προσεκτικοί σχετικά με τους κινδύνους που συνδέονται με το άνοιγμα email από άγνωστους αποστολείς.

Ωστόσο, τα SMS παρουσιάζουν έναν πιο διακριτικό προβληματισμό. Προσφέρουν έναν πιο προσωπικό τρόπο επικοινωνίας, καθώς οι παραλήπτες μπορούν εύκολα να αναγνωρίσουν τον αποστολέα και να αποφασίσουν εάν θα αλληλεπιδράσουν με το μήνυμα. Συνήθως, εκτός αν ένας αριθμός είναι αποκλεισμένος ή βρίσκεται σε μαύρη λίστα, τα μηνύματα SMS παραδίδονται απευθείας στη συσκευή του παραλήπτη, κάνοντάς τα ιδανικά για επιθέσεις spam και phishing. Οι κοινές τακτικές περιλαμβάνουν διαφημίσεις σε κινητά και προσπάθειες απάτης μέσω SMS, συχνά περιέχοντας συνδέσμους που προτρέπουν τους χρήστες να συνδεθούν σε ένα παιχνίδι ή μια υπηρεσία. Μία ανησυχητική τάση είναι τα μηνύματα SMS που χρεώνουν τον χρήστη χωρίς τη συγκατάθεσή του. Αυτοί οι τύποι επιθέσεων αναμένεται να αυξηθούν με την πάροδο του χρόνου.



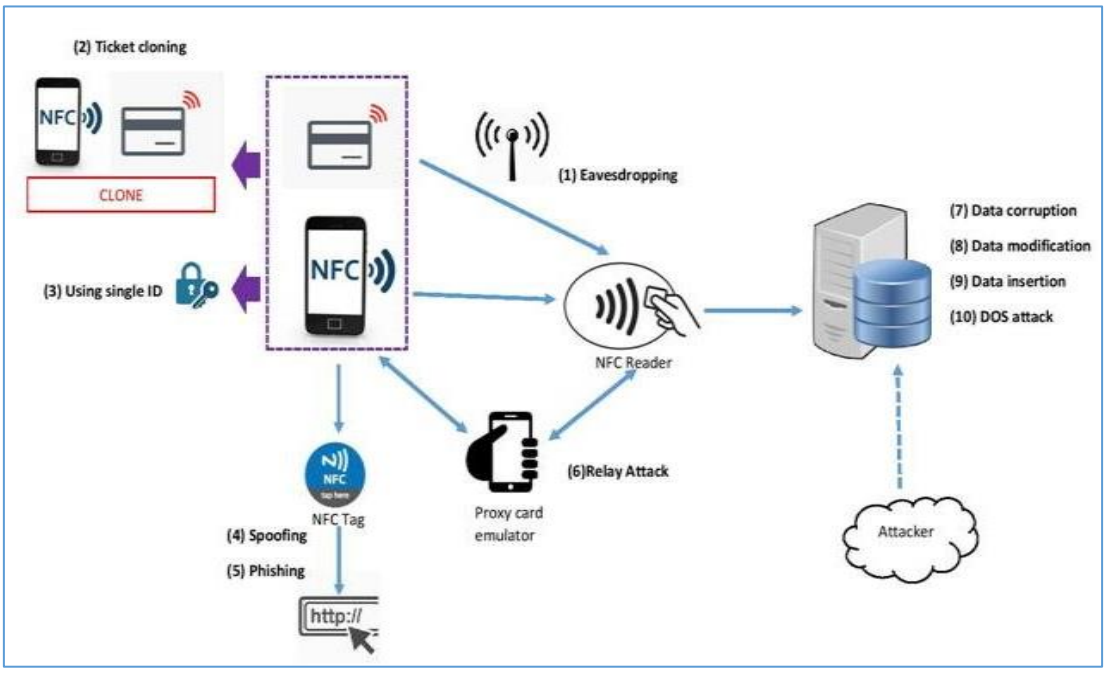
Εικόνα 39. Spam Text Message

Πηγή : https://blog.textingbase.com/how-to-identify-spam-text-messages

Ενδιαφέρον παρουσιάζει το γεγονός ότι, ενώ οι χρήστες ενδέχεται να είναι προσεκτικοί όταν αντιμετωπίζουν ύποπτα email, εξακολουθούν να είναι ευάλωτοι στο να κάνουν κλικ σε τυχαίους συνδέσμους σε μηνύματα κειμένου. Ωστόσο, αυτοί οι σύνδεσμοι μπορεί να ανοίξουν στον κινητό περιηγητή ή σε άλλες εφαρμογές που μπορεί να περιέχουν πρόσθετες ευπάθειες, ενισχύοντας τους κινδύνους ασφάλειας.

3.3.8 Near Field Communication

Οι κινητές συσκευές παρουσιάζουν άλλο έναν δυνητικό τρόπο επιθέσεων: την επικοινωνία κοντινού πεδίου, ή NFC. Αυτή η τεχνολογία επιτρέπει στις συσκευές να ανταλλάσσουν δεδομένα όταν βρίσκονται σε κοντινή απόσταση, συνήθως εντός 4 εκατοστών (1,6 ιντσών) μεταξύ τους. Το NFC χρησιμοποιείται όχι μόνο για την ανταλλαγή δεδομένων, αλλά παίζει επίσης ένα κρίσιμο ρόλο στα συστήματα ασύρματης πληρωμής, παρόμοια με αυτά που χρησιμοποιούνται σε πιστωτικές κάρτες και ηλεκτρονικές κάρτες εισιτηρίων. Αυτή η δυνατότητα επιτρέπει στις κινητές συσκευές να χρησιμοποιηθούν για πληρωμές, είτε αντί για είτε σε συνδυασμό με τις παραδοσιακές μεθόδους πληρωμής. Ωστόσο, το NFC παρουσιάζει επίσης έναν επιπλέον τρόπο επιθέσεων μέσω κοινωνικής μηχανικής. Για παράδειγμα, ερευνητές έχουν δείξει πώς το NFC μπορεί να χρησιμοποιηθεί για να εκτελέσει επιθέσεις σε συσκευές Android, μεταφέροντας κακόβουλα δεδομένα σε ευάλωτες εφαρμογές. Παρά τον κίνδυνο εκμετάλλευσης, οι χρήστες θα πρέπει να παραμείνουν προσεκτικοί και να διασφαλίζουν ότι οι ασύρματες συναλλαγές πραγματοποιούνται μόνο μέσω νόμιμων και εξουσιοδοτημένων πηγών.



Εικόνα 40. Types of NFC Security Attacks

Πηγή:
https://www.researchgate.net/publication/329642316_Near_Field_Communication_NFC_Technology_Security_Vulnerabilities_and_Countermeasures/figures?lo=1

3.3.9 QR Codes

Ένας κωδικός QR, ο οποίος σημαίνει "γρήγορη απόκριση", είναι ένας τύπος γραμμωτού κώδικα που αποτελείται από ένα πλέγμα κουκκίδων. Μπορεί να διαβαστεί χρησιμοποιώντας έναν αναγνώστη QR ή ένα έξυπνο τηλέφωνο με ενσωματωμένη κάμερα. Όταν γίνει σάρωση, το λογισμικό στη συσκευή ερμηνεύει τη διάταξη των κουκκίδων εντός του κώδικα και το μεταφράζει σε αριθμούς ή μια ακολουθία χαρακτήρων. Για παράδειγμα, η σάρωση ενός κωδικού QR με το έξυπνο τηλέφωνό σας μπορεί να ενεργοποιήσει το άνοιγμα ενός URL στον περιηγητή ιστού του τηλεφώνου σας. Ωστόσο, οι κωδικοί QR μπορούν επίσης να συνιστούν κίνδυνο για την ασφάλεια. Για παράδειγμα, ένας κωδικός QR που εμφανίζεται σε ένα φυλλάδιο ενδέχεται να μην κατευθύνει τον χρήστη στο περιεχόμενο που περιγράφει. Κακόβουλοι κωδικοί QR μπορούν να χρησιμοποιηθούν ως απλός τρόπος εγκατάστασης κακόβουλου λογισμικού (όπως ένα αρχείο APK) σε ένα κινητό τηλέφωνο, πιθανώς δημιουργώντας ένα μονοπάτι για μη εξουσιοδοτημένη επικοινωνία με άλλη συσκευή.

Εικόνα 41. QR Code Phishing

Πηγή : https://www.linkedin.com/pulse/qr-code-phishing-step-by-step-ankush-johar/

3.4 Προκλήσεις Ασφαλείας σε κινητές πλατφόρμες Android και iOS

Οι κινητές συσκευές [26] μοιράζονται ορισμένες ομοιότητες με τους παραδοσιακούς υπολογιστές, όπως τα λειτουργικά συστήματα και τα βασικά πρωτόκολλα επικοινωνίας. Ωστόσο, διαθέτουν επίσης ξεχωριστά χαρακτηριστικά που εισάγουν νέα διανύσματα επίθεσης και πρωτόκολλα. Κάποια από αυτά τα χαρακτηριστικά έχουν για χρόνια αποτελέσει πηγή ευπαθειών ασφαλείας, παρόμοιων με αυτές που βρίσκονται σε υπολογιστές. Ταυτόχρονα, εμφανίζονται νέες ανησυχίες που αφορούν τα πρωτόκολλα επικοινωνίας που είναι ειδικά για τις κινητές συσκευές, παρουσιάζοντας νέες προκλήσεις στον τομέα της ασφάλειας.

Εικόνα 42. Mobile Security Threats Prediction for 2023

Πηγή : https://www.efani.com/blog/mobile-threats-prediction-2023

3.5 Αντιμετώπιση Απειλών σε κινητές πλατφόρμες Android

Οι απειλές για τις κινητές συσκευές [25] , ιδίως για τα smartphones Android, τα οποία αποτελούν τους πρωταρχικούς στόχους όλων των κακόβουλων προγραμμάτων για κινητά, συνεχίζουν να αυξάνονται. Τα πιο συνηθισμένα κακόβουλα προγράμματα εκμεταλλεύονται τη συχνή χρήση των app store από τους χρήστες κινητών τηλεφώνων με επιλογές πληρωμής με ένα κλικ. Η στατιστική δείχνει ότι οι εφαρμογές κακόβουλου λογισμικού μπορούν να επηρεάσουν το store παρά τα πολυάριθμα χαρακτηριστικά ασφαλείας της Google. Το Android, λόγω του ανοιχτού του περιβάλλοντος, είναι η πλατφόρμα που ερευνάται περισσότερο από τους ειδικούς για ευπάθειες. Σύμφωνα με το cvedetails.com το 2023 μόνο για το Android βρέθηκαν 1422 ευπάθειες. Ωστόσο, το πρόβλημα δεν είναι μόνο τα τρωτά σημεία στο λογισμικό, αλλά ειδικά τα κενά στο υλικό.

Το Meltdown και το Spectre, τα σοβαρά κενά ασφαλείας στους επεξεργαστές, τα οποία υπάρχουν και στις κινητές συσκευές, κατέδειξαν και πάλι πόσο σημαντική

είναι μια ταχεία διαδικασία ασφαλείας, ώστε οι χρήστες να λαμβάνουν γρήγορα τις νέες ενημερώσεις. Αυτό οφείλεται στο γεγονός ότι η πλειονότητα των επιθέσεων στον κυβερνοχώρο εκμεταλλεύεται κενά ασφαλείας που είναι ήδη γνωστά. Η παρεμπόδιση των ενημερώσεων ασφαλείας για κινητά θα μπορούσε να είναι μια άλλη πηγή σοβαρών προβλημάτων στο σύστημα.

Όταν οι πάροχοι υπηρεσιών κινητής τηλεφωνίας εντοπίζουν κακόβουλο λογισμικό, προσπαθούν να διανείμουν στους πελάτες μια ενημερωμένη έκδοση ασφαλείας για κινητά για να καθαρίσουν και να προστατεύσουν τις συσκευές τους. Οι επιτιθέμενοι γνωρίζουν τη στρατηγική του παρόχου και προσπαθούν να δημιουργήσουν εφαρμογές που κατεβάζουν κακόβουλο λογισμικό, το οποίο εμποδίζει το smartphone να επικοινωνήσει με την πάροχο κινητής τηλεφωνίας και αφήνει το κακόβουλο λογισμικό να παραμείνει στο τηλέφωνο του θύματος.

Οι κινητές συσκευές περιέχουν τεράστιες ποσότητες σημαντικών και ευαίσθητων δεδομένων. Μηνύματα, μηνύματα ηλεκτρονικού ταχυδρομείου, λίστες επαφών, αρχεία, δεδομένα τοποθεσίας - τα smartphones μπορούν δυνητικά να φιλοξενήσουν τόσο ευαίσθητο εταιρικό υλικό όσο και οι φορητοί υπολογιστές εργασίας. Ένας ρεαλιστικός κίνδυνος για την ασφάλεια των κινητών τηλεφώνων έγκειται σε επιθέσεις zero-day. Αυτό θα μπορούσε να οδηγήσει σε διαρροή δεδομένων ή σε μη προσβάσιμα δεδομένα. Οι επιθέσεις zero-day μπορούν να χτυπήσουν οπουδήποτε, ανά πάσα στιγμή, επειδή η χρήση του Android έχει μπει στην καθημερινότητά μας λόγω των αυξανόμενων δυνατοτήτων του.

Οι συγγραφείς κακόβουλου λογισμικού για κινητά έχουν θέσει ως στόχο τους την κερδοφορία, έχουν πάρει τον παραδοσιακό φορέα επίθεσης σε υπολογιστές, τα τραπεζικά Trojans, και έχουν προσθέσει δυνατότητες ransomware για να δημιουργήσουν μια νέα απειλή στην κινητή πλατφόρμα. Αυτό οφείλεται στο γεγονός ότι οι τραπεζικές και χρηματοοικονομικές εφαρμογές για κινητά γίνονται όλο και πιο δημοφιλείς στους χρήστες και δημιουργούν κενά ασφαλείας που θα μπορούσαν να εκμεταλλευτούν οι εγκληματίες του κυβερνοχώρου.

Ενώ εστιάζουμε στις πλατφόρμες κινητών τηλεφώνων, θα πρέπει να σημειωθεί ότι το Διαδίκτυο των πραγμάτων (IoT) κατασκευάζεται συνήθως σε τεχνολογία android. Όλες οι κινητές απειλές θα μπορούσαν να εμπεριέχονται ανεξέλεγκτα στο IoT. Αυτές οι συσκευές, ενώ προσφέρουν ευκολία και ευκολία, επεκτείνουν επίσης σημαντικά το εύρος των επιθέσεων. Οι περισσότερες από αυτές τις συσκευές έχουν επικεντρωθεί στο χρόνο διάθεσης στην αγορά και στην ευκολία, χωρίς να έχουν σκεφτεί καθόλου την ασφάλεια.

Η προεπιλεγμένη αδυναμία ασφαλείας είναι ότι οι συσκευές αυτές υποστηρίζουν τη διαλειτουργικότητα και τη διασύνδεση με προσωπικούς υπολογιστές και κινητά τηλέφωνα. Παρόλο που οι αναφορές για hijacked IP cameras έχουν ευαισθητοποιήσει τους χρήστες σχετικά με την πιθανή κατασκοπεία, είναι ένα νέο ερευνητικό πεδίο το τι σημαίνει να έχουμε τόσα πολλά πιθανά σημεία επίθεσης στα σπίτια μας.

3.5.1 Περιορισμοί δικαιωμάτων

Οι **περιορισμοί δικαιωμάτων** αποτελούν σημαντικό μέτρο ασφαλείας που εφαρμόζεται σε κινητές πλατφόρμες όπως το Android, με στόχο την προστασία της ιδιωτικότητας των χρηστών και τη μείωση του κινδύνου ανεπιθύμητων επιθέσεων από εφαρμογές. Ας αναλύσουμε τους περιορισμούς δικαιωμάτων σε πλατφόρμα Android:

- **Αρχή του Ελάχιστου Προνομίου (Principle of Least Privilege):** Σύμφωνα με αυτή την αρχή, μια εφαρμογή θα πρέπει να έχει μόνο τα δικαιώματα που χρειάζεται για να λειτουργήσει σωστά και να παρέχει τις λειτουργίες τις οποίες υπόσχεται στον χρήστη. Αυτό σημαίνει ότι οι εφαρμογές πρέπει να ζητούν μόνο τα απαραίτητα δικαιώματα κατά την εγκατάστασή τους.
- **Διαχείριση Δικαιωμάτων από τον Χρήστη:** Οι χρήστες έχουν τη δυνατότητα να ελέγχουν και να διαχειρίζονται τα δικαιώματα που ζητούν οι εφαρμογές κατά την εγκατάστασή τους. Αυτό σημαίνει ότι ο χρήστης μπορεί να αποδεχθεί ή να απορρίψει τις αιτήσεις δικαιωμάτων κάθε εφαρμογής.
- **Runtime Permissions:** Από την έκδοση Android 6.0 (Marshmallow) και μετά, η Google εισήγαγε τη δυνατότητα των runtime permissions. Αυτό σημαίνει ότι οι εφαρμογές θα ζητούν δικαιώματα κατά τη χρήση τους, αντί να τα ζητούν όλα κατά την εγκατάσταση. Αυτό επιτρέπει στους χρήστες να δώσουν ή να αρνηθούν πρόσβαση σε δεδομένα και λειτουργίες όπως την κάμερα, το μικρόφωνο, κλπ.
- **Διαχείριση Δικαιωμάτων από τον Χρήστη:** Οι χρήστες έχουν τη δυνατότητα να ελέγχουν και να διαχειρίζονται τα δικαιώματα που ζητούν οι εφαρμογές κατά την εγκατάστασή τους. Αυτό σημαίνει ότι ο χρήστης μπορεί να αποδεχθεί ή να απορρίψει τις αιτήσεις δικαιωμάτων κάθε εφαρμογής.
- **Ασφάλεια του Λειτουργικού Συστήματος:** Η Google παρέχει συστηματικά ενημερώσεις ασφαλείας για το λειτουργικό σύστημα Android, οι οποίες διορθώνουν γνωστές ευπάθειες και επιτρέπουν στους χρήστες να παραμένουν προστατευμένοι από δυνητικές απειλές ασφαλείας.

Εικόνα 43. Android security Tips

Πηγή : https://aglowiditsolutions.com/blog/android-vs-ios-security/

3.5.2 Αναβαθμίσεις Ασφαλείας

Οι **αναβαθμίσεις ασφαλείας** αποτελούν κρίσιμο μέτρο για τη διασφάλιση της ασφάλειας σε κινητές πλατφόρμες όπως το Android . Ας εξετάσουμε πιο αναλυτικά τις αναβαθμίσεις ασφαλείας στο Android:

- **Τακτικές Ενημερώσεις Ασφαλείας:** Η Google παρέχει τακτικές ενημερώσεις ασφαλείας για το λειτουργικό σύστημα Android. Αυτές οι ενημερώσεις περιλαμβάνουν διορθώσεις για γνωστές ευπάθειες και επιθέσεις που μπορεί να επηρεάζουν την ασφάλεια των συσκευών.
- **Υποστήριξη Ασφαλείας για Παλαιότερες Εκδόσεις:** Η Google συνεχίζει να παρέχει ενημερώσεις ασφαλείας για παλαιότερες εκδόσεις του Android, τουλάχιστον για ένα συγκεκριμένο χρονικό διάστημα μετά την κυκλοφορία τους, προστατεύοντας έτσι τις συσκευές που δεν έχουν αναβαθμιστεί σε πιο πρόσφατες εκδόσεις.
- **Ενημερώσεις Πλαισίου και Υπηρεσιών Google Play:** Η Google αναβαθμίζει συχνά το πλαίσιο Android και τις υπηρεσίες του Google Play για να προστατεύσει τις εφαρμογές και τις συσκευές από απειλές.
- **Συνεργασία με Κατασκευαστές Συσκευών:** Η Google συνεργάζεται με κατασκευαστές συσκευών για να διασφαλίσει ότι οι ενημερώσεις ασφαλείας διανέμονται γρήγορα στους χρήστες των διάφορων μοντέλων συσκευών.

3.5.3 Διαχωρισμός των Δεδομένων

Ο **διαχωρισμός των δεδομένων** είναι ένας σημαντικός μηχανισμός ασφαλείας που εφαρμόζεται σε κινητές πλατφόρμες όπως το Android. Αυτός ο μηχανισμός αποσκοπεί στο να προστατεύσει την ιδιωτικότητα των χρηστών και την ασφάλεια των δεδομένων τους με το να διαχωρίζει τα δεδομένα μεταξύ διαφορετικών εφαρμογών και χρηστών.

- **Διαχωρισμός Χρήστη-Εφαρμογής:** Στο Android, κάθε εφαρμογή λειτουργεί σε έναν διακριτό χώρο χρήστη (user space). Αυτό σημαίνει ότι τα δεδομένα μιας εφαρμογής είναι προσβάσιμα μόνο από αυτήν την εφαρμογή και δεν μπορούν να προσπελαστούν από άλλες εφαρμογές, εκτός αν οριστεί ρητώς από τον χρήστη.
- **Διαχωρισμός Διαφορετικών Χρηστών:** Κάθε χρήστης σε μια συσκευή Android έχει έναν ξεχωριστό χώρο χρήστη, όπου τα δεδομένα του είναι απομονωμένα από τους άλλους χρήστες της συσκευής.
- **Χρήση του Android Sandbox:** Η Android λειτουργεί με ένα σύστημα ασφαλείας που ονομάζεται Sandbox, το οποίο περιορίζει την πρόσβαση των εφαρμογών σε ευαίσθητα συστήματα και δεδομένα, προστατεύοντας έτσι το σύστημα από πιθανές απειλές.

3.5.4 Application Sandboxing

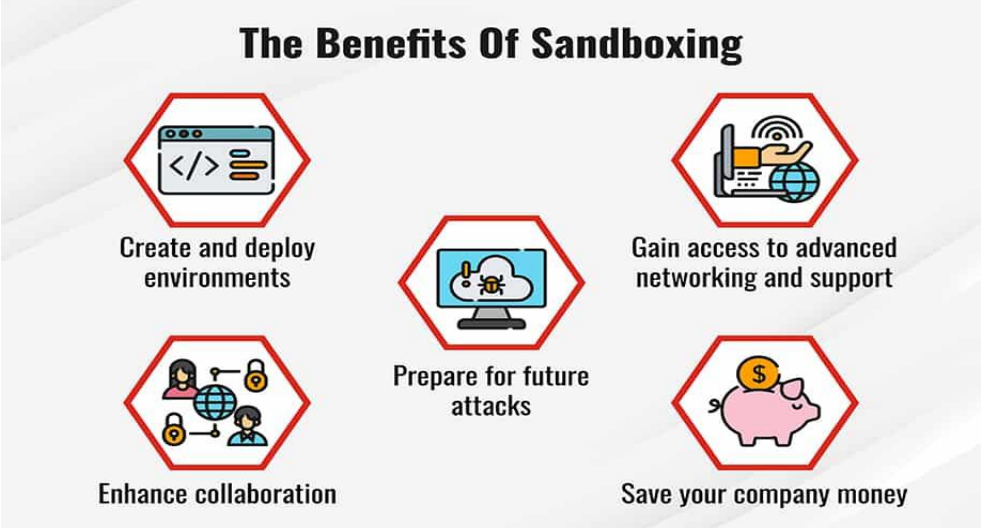
Ανάλογα με την ευρύτερη αρχιτεκτονική του συστήματος, το πλαίσιο ασφαλείας [27] του Android αξιοποιεί τις λειτουργίες ασφάλειας που παρέχει ο πυρήνας του Linux. Το Linux, ως πολυχρηστικό λειτουργικό σύστημα, επιτρέπει στον πυρήνα να απομονώνει τους πόρους του χρήστη, παρόμοια με τον τρόπο που απομονώνει τις διεργασίες. Σε ένα περιβάλλον Linux, ένας χρήστης συνήθως δεν μπορεί να έχει πρόσβαση στα αρχεία ενός άλλου χρήστη εκτός εάν του δοθούν εκτεταμένες άδειες. Το Android αξιοποιεί αυτό το μηχανισμό απομόνωσης χρήστη, αλλά αποκλίνει από την κανονική εγκατάσταση του Linux, όπως αυτή που βρίσκεται σε γραφείο ή διακομιστή.

Σε ένα παραδοσιακό σύστημα Linux, ένας μοναδικός αναγνωριστικός (UID) αποδίδεται είτε σε ένα φυσικό χρήστη που μπορεί να συνδεθεί στο σύστημα και να εκτελέσει εντολές μέσω του shell, είτε σε μια υπηρεσία συστήματος (daemon) που λειτουργεί στο παρασκήνιο. Αυτή η προσέγγιση στοχεύει στο να μειώσει τους κινδύνους, ιδιαίτερα για τους (daemons) συστήματος που είναι προσβάσιμοι μέσω του δικτύου, περιορίζοντας τις επιπτώσεις σε έναν αφιερωμένο UID σε περίπτωση που γίνει παραβίαση.

Ωστόσο, η σχεδίαση του Android, που αρχικά δημιουργήθηκε για έξυπνα τηλέφωνα, αντικατοπτρίζει την προσωποποιημένη φύση των κινητών συσκευών. Συνεπώς, η έννοια της εγγραφής διαφορετικών φυσικών χρηστών στο σύστημα είναι περιττή. Αντίθετα, ο φυσικός χρήστης είναι σιωπηλός, και τα UID χρησιμοποιούνται κυρίως για να διαφοροποιήσουν τις εφαρμογές μεταξύ τους. Αυτή η διάκριση αποτελεί τη βάση του μηχανισμού sandboxing εφαρμογών του Android.

Κατά την εγκατάσταση, το Android αυτόματα αναθέτει ένα μοναδικό αναγνωριστικό, γνωστό ως app ID ή UID, σε κάθε εφαρμογή. Αυτό το UID χρησιμοποιείται για την εκτέλεση της εφαρμογής σε έναν αφιερωμένο διεργασία. Επιπλέον, σε κάθε εφαρμογή αντιστοιχίζεται ένας διακριτός κατάλογος δεδομένων με αποκλειστικές άδειες ανάγνωσης και εγγραφής. Ως εκ τούτου, οι εφαρμογές απομονώνονται, τόσο στο επίπεδο διεργασίας όσο και στο επίπεδο αρχείων.

Στο επίπεδο της διεργασίας, κάθε εφαρμογή λειτουργεί μέσα στη δική της αφιερωμένη διεργασία, ενώ στο επίπεδο των αρχείων έχει αποκλειστική πρόσβαση στον καθορισμένο κατάλογο δεδομένων της. Αυτό δημιουργεί ένα sandbox εφαρμογών στο επίπεδο του πυρήνα, εξασφαλίζοντας απομόνωση για όλες τις εφαρμογές, ανεξαρτήτως εάν λειτουργούν σε φυσικές ή εικονικές διεργασίες. Οι daemons συστήματος και οι εφαρμογές λειτουργούν υπό συγκεκριμένα, προκαθορισμένα UID, με πολύ λίγους daemons να λειτουργούν υπό τον χρήστη root (UID 0). Σε αντίθεση με τα παραδοσιακά συστήματα, το Android δε χρησιμοποιεί το αρχείο /etc/password για τη διαχείριση των χρηστών. Αντίθετα, τα UID του συστήματος ορίζονται στατικά εντός του αρχείου κεφαλίδας android filesystem config.h.



Εικόνα 44. Benefits of Sandboxing

Πηγή : https://www.fortinet.com/resources/cyberglossary/what-is-sandboxing

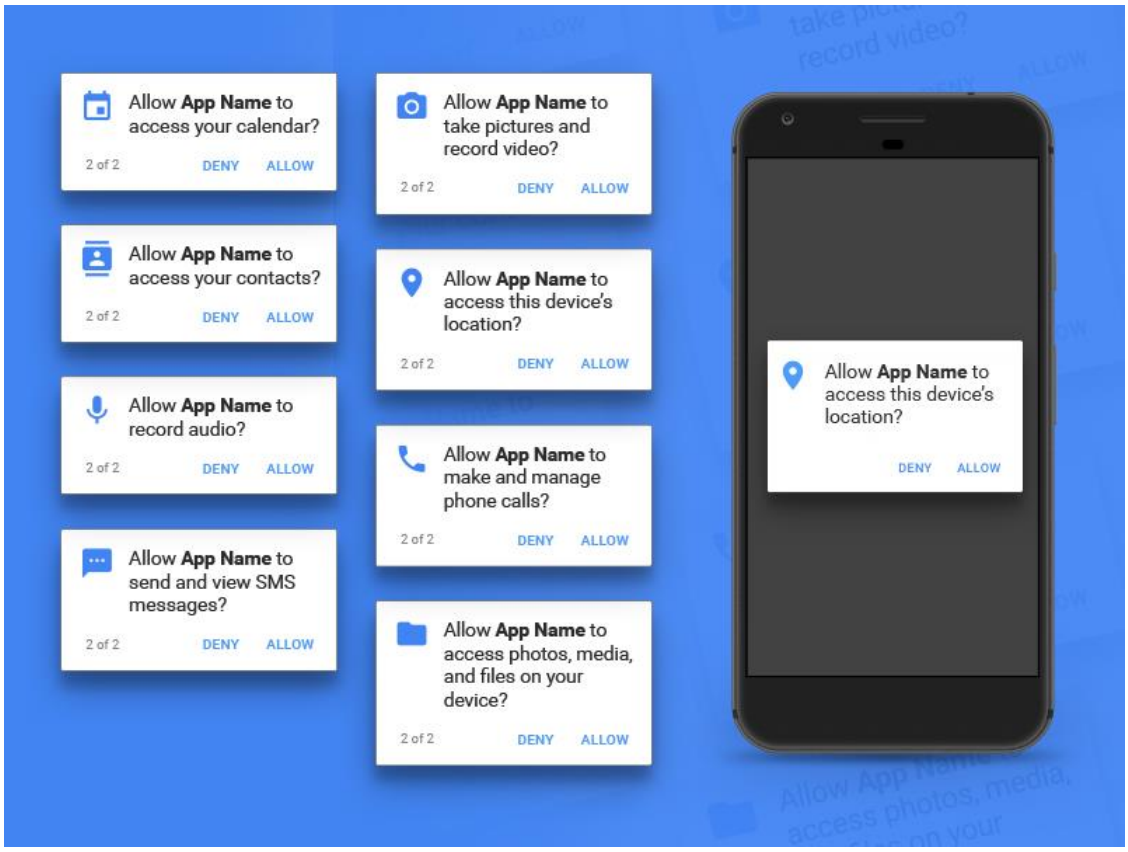
3.5.5 Permissions

Καθώς το Android απομονώνει τις εφαρμογές μεταξύ τους μέσα σε sandboxes, συχνά χρειάζονται να μοιράζονται πόρους και δεδομένα για να βελτιώσουν τη λειτουργικότητά τους. Αυτή η ανάγκη προκύπτει όταν οι εφαρμογές χρειάζονται επιπλέον δυνατότητες πέρα από το βασικό περιβάλλον sandbox, όπως η πρόσβαση σε λειτουργίες συσκευών όπως η κάμερα. Για να το επιτύχει αυτό, το Android μπορεί να παρέχει στις εφαρμογές λεπτομερείς δικαιώματα πρόσβασης, γνωστά ως άδειες, επιτρέποντας έτσι τη βελτιωμένη λειτουργικότητα.

Οι άδειες ρυθμίζουν την πρόσβαση σε διάφορους πόρους, συμπεριλαμβανομένων των συσκευών υλικού, της σύνδεσης στο διαδίκτυο, των δεδομένων και των υπηρεσιών του λειτουργικού συστήματος. Μόλις χορηγηθούν, οι άδειες δεν μπορούν να ανακληθούν και είναι προσβάσιμες στην εφαρμογή χωρίς περαιτέρω επιβεβαίωση. Ορισμένες άδειες είναι αποκλειστικά διαθέσιμες για εφαρμογές που είναι αναπόσπαστο μέρος του λειτουργικού συστήματος Android, είτε επειδή είναι προεγκατεστημένες είτε επειδή είναι υπογεγραμμένες με το ίδιο κλειδί με το λειτουργικό σύστημα. Οι εφαρμογές τρίτων μπορούν να ορίσουν προσαρμοσμένες άδειες και να επιβάλουν παρόμοιους περιορισμούς, γνωστούς ως επίπεδα προστασίας άδειας. Αυτή η πρακτική εξασφαλίζει ότι η πρόσβαση στις υπηρεσίες και τους πόρους μιας εφαρμογής περιορίζεται σε εφαρμογές που δημιουργήθηκαν από τον ίδιο συγγραφέα.

Οι άδειες μπορούν να επιβάλλονται σε διάφορα επίπεδα, ανάλογα με τους πόρους που πρόκειται να αποκτηθούν. Οι πόροι του χαμηλότερου επιπέδου του συστήματος, όπως τα αρχεία συσκευής, επιβάλλονται από τον πυρήνα του Linux, ο οποίος ελέγχει το UID ή το GID της διεργασίας έναντι του ιδιοκτήτη του πόρου και των δικαιωμάτων πρόσβασης. Εν τω μεταξύ, η επιβολή για τα στοιχεία Android υψηλότερου επιπέδου

γίνεται είτε από το ίδιο το λειτουργικό σύστημα Android είτε από κάθε μεμονωμένο στοιχείο.



Εικόνα 45. Android Permissions

Πηγή : https://www.sketchappsources.com/free-source/2328-android-permissions-dialog-templates-sketch-freebie-resource.html

3.5.6 Security-Enhanced Linux in Android

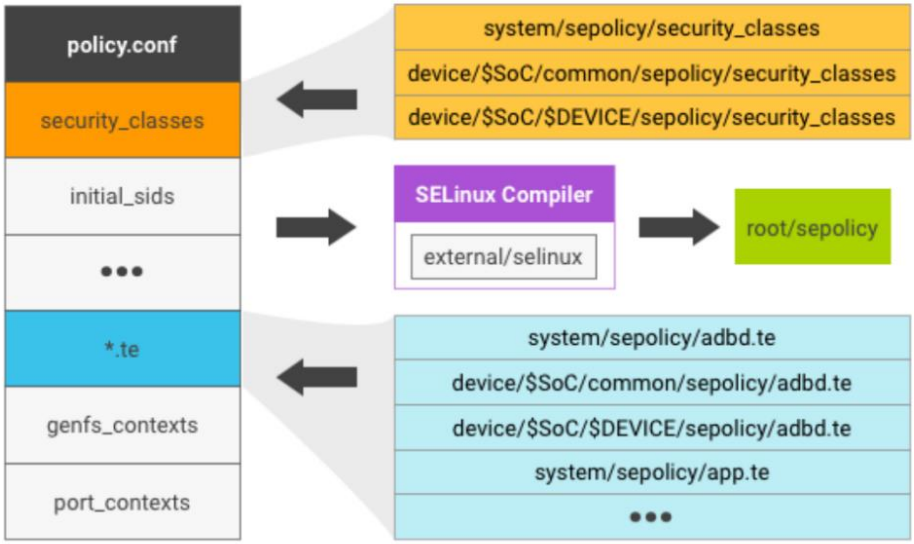
Ως μέρος του μοντέλου ασφάλειας του Android, το Android χρησιμοποιεί το SELinux για την επιβολή υποχρεωτικού ελέγχου πρόσβασης (MAC) σε όλες τις διεργασίες, συμπεριλαμβανομένων αυτών που λειτουργούν με προνομιούχες άδειες root/superuser, γνωστές και ως Linux δυνατότητες. Η ενσωμάτωση του SELinux ενισχύει τα μέτρα ασφαλείας του Android διαχειριζόμενος τις προνομιούχες διεργασίες και διευκολύνοντας τη δημιουργία πολιτικών ασφαλείας.

Το SELinux λειτουργεί με βάση την αρχή της προεπιλεγμένης απόρριψης: οτιδήποτε δεν επιτρέπεται ρητά απορρίπτεται αυτόματα. Μπορεί να λειτουργήσει σε δύο κύρια καθεστώτα:

- Permissive mode : Σε αυτή τη λειτουργία, οι απορρίψεις άδειας καταγράφονται αλλά δεν επιβάλλονται ενεργά.
- Enforcing mode : Εδώ, οι απορρίψεις άδειας καταγράφονται και επιβάλλονται αυστηρά.

Ξεκινώντας από την έκδοση Android 5.0, το SELinux μετέβηκε σε πλήρη επιβολή, βασιζόμενο στην προηγούμενη περιορισμένη εκδοχή του Android 4.3 και τη μερική επιβολή του Android 4.4. Αυτή η μετάβαση σημαίνει ότι το Android τώρα επιβάλλει πολιτικές SELinux σε μια ευρύτερη γκάμα τομέων, σε σύγκριση με προηγούμενες εκδόσεις.

- Όλα τα στοιχεία λειτουργούν σε κατάσταση επιβολής στο Android 5.x και σε μεταγενέστερες εκδόσεις.
- Μόνο η διαδικασία init πρέπει να λειτουργεί στον τομέα init.
- Οποιαδήποτε γενική απόρριψη, όπως για ένα block device, socket device ή default service, υποδηλώνει ότι μια συγκεκριμένη συσκευή απαιτεί έναν ειδικό τομέα.



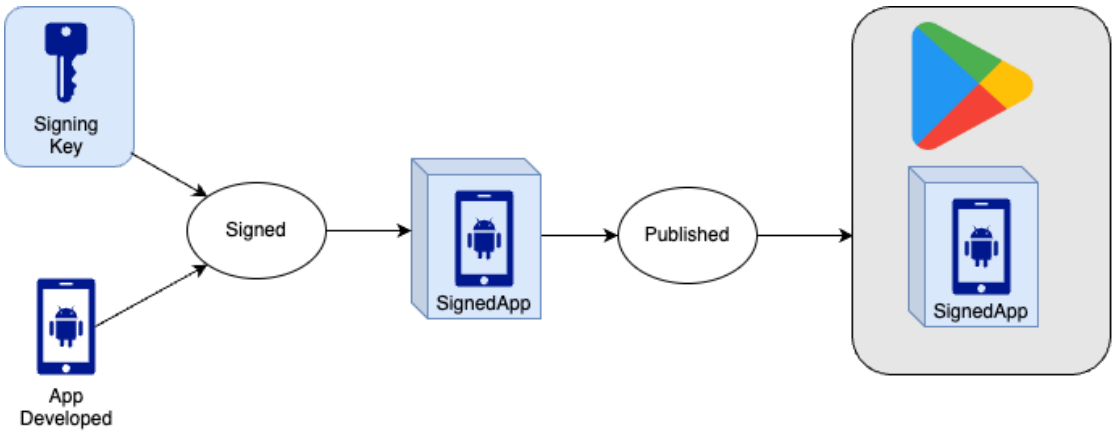
Εικόνα 46. SELinux policy file

Πηγή : https://source.android.com/docs/security/features/selinux/build

3.5.7 Application signing

Η υπογραφή εφαρμογής λειτουργεί ως κρίσιμος μηχανισμός για τους προγραμματιστές, επιτρέποντάς τους να καθορίζουν την ταυτότητά τους και να διευκολύνουν τις αναβαθμίσεις των εφαρμογών τους χωρίς την ανάγκη για περίπλοκες διεπαφές και δικαιώματα. Κάθε εφαρμογή που εκτελείται στην πλατφόρμα Android πρέπει να έχει υπογραφεί από τον προγραμματιστή της. Οι εφαρμογές που προσπαθούν να εγκατασταθούν χωρίς υπογραφή θα απορριφθούν είτε από το Google Play είτε από τον εγκαταστάτη πακέτων στη συσκευή Android. Όλες οι εφαρμογές Android, συμπεριλαμβανομένων των συστημικών εφαρμογών, πρέπει να έχουν υπογραφεί από τους προγραμματιστές τους. Καθώς τα αρχεία APK του Android είναι ουσιαστικά μια επέκταση της μορφής πακέτου Java JAR, η διαδικασία υπογραφής κώδικα βασίζεται στις αρχές υπογραφής JAR. Η υπογραφή APK στο Android εξυπηρετεί δύο βασικούς σκοπούς ασφάλειας: εξασφαλίζει ότι οι ενημερώσεις για μια εφαρμογή προέρχονται

από τον ίδιο συγγραφέα (γνωστό ως η ίδια πολιτική προέλευσης) και θεσπίζει σχέσεις εμπιστοσύνης μεταξύ των εφαρμογών. Αυτά τα χαρακτηριστικά ασφαλείας εφαρμόζονται με τον συγκριτικό έλεγχο του πιστοποιητικού υπογραφής της εγκατεστημένης εφαρμογής με αυτό της ενημέρωσης ή της σχετικής εφαρμογής. Οι συστημικές εφαρμογές υπογράφονται με ένα σύνολο κλειδιών πλατφόρμας. Όταν διαφορετικά συστατικά του συστήματος υπογράφονται με το ίδιο κλειδί πλατφόρμας, μπορούν να μοιραστούν πόρους και να λειτουργήσουν εντός της ίδιας διαδικασίας.



Εικόνα 47. Android App Signing

Πηγή : https://medium.com/mobile-app-development-publication/android-app-signing-a-refresher-9cb8f664cfcf

3.6 Αντιμετώπιση Απειλών σε κινητές πλατφόρμες iOS

Η **ασφάλεια της συσκευής** στο **iOS** [27] είναι ένας σημαντικός παράγοντας που αποτελεί προτεραιότητα για την Apple και τους χρήστες της. Ας αναλύσουμε μερικά σημαντικά στοιχεία ασφάλειας της συσκευής iOS

- **Κλείδωμα Οθόνης (Screen Lock):** Η ενεργοποίηση του κλειδώματος οθόνης με το Touch ID ή το Face ID βοηθά στην προστασία των προσωπικών δεδομένων σας από μη εξουσιοδοτημένη πρόσβαση.
- **Κρυπτογράφηση Δεδομένων:** Τα δεδομένα που αποθηκεύονται στη συσκευή iOS είναι κρυπτογραφημένα, πράγμα που δυσχεραίνει την πρόσβαση σε αυτά αν η συσκευή χαθεί ή κλαπεί.
- **Ασφάλεια Λειτουργικού Συστήματος:** Η Apple παρέχει τακτικές ενημερώσεις για το iOS, συμπεριλαμβανομένων διορθώσεων ασφαλείας, προκειμένου να αντιμετωπίσει γνωστές ευπάθειες ασφαλείας.
- **Find My iPhone:** Η λειτουργία "Find My iPhone" επιτρέπει στους χρήστες να εντοπίζουν και να διαχειρίζονται απομακρυσμένα τις συσκευές τους σε περίπτωση απώλειας ή κλοπής.
- **Ελεγχόμενη Πρόσβαση σε Εφαρμογές:** Οι χρήστες μπορούν να περιορίσουν την πρόσβαση σε ευαίσθητα δεδομένα και λειτουργίες για κάθε εφαρμογή μέσω των ρυθμίσεων απορρήτου και ασφάλειας του iOS.

- **Διαδικασία Επαλήθευσης Ταυτότητας (Two-Factor Authentication - 2FA):** Η ενεργοποίηση της διπλής παροχής ταυτότητας για το Apple ID αυξάνει την ασφάλεια του λογαριασμού σας και των συσκευών που το χρησιμοποιούν.
- **Ελέγχος Εφαρμογών:** Η Apple διενεργεί μια αυστηρή διαδικασία πιστοποίησης για τις εφαρμογές πριν αυτές διατεθούν στο App Store, προκειμένου να διασφαλιστεί η ασφάλειά τους.

Εικόνα 48. iOs Security Tips

Πηγή : https://aglowiditsolutions.com/blog/android-vs-ios-security/

3.6.1 Έλεγχος Εφαρμογών

είναι ένας σημαντικός μηχανισμός για τη διασφάλιση της ασφάλειας και της ακεραιότητας των εφαρμογών που τρέχουν σε συσκευές iPhone και iPad. Ας αναλύσουμε τους βασικούς τρόπους ελέγχου των εφαρμογών στο iOS:

- **Έλεγχος Αναφοράς Πηγαίου Κώδικα (Source Code Review):** Ο έλεγχος του πηγαίου κώδικα των εφαρμογών είναι ένας σημαντικός τρόπος για τον εντοπισμό πιθανών ευπαθειών και κενών ασφαλείας στην υλοποίηση της εφαρμογής.
- **Διαδικασία Πιστοποίησης Εφαρμογών (App Certification Process):** Η Apple διενεργεί μια διαδικασία πιστοποίησης για κάθε εφαρμογή πριν αυτή διατεθεί στο App Store. Κατά τη διάρκεια αυτής της διαδικασίας, οι ειδικοί αξιολογούν την εφαρμογή για πιθανές προβληματικές καταστάσεις και παραβιάσεις των κανόνων του App Store.
- **Χρήση Υπογεγραμμένων Εφαρμογών (Code Signing):** Η Apple χρησιμοποιεί την τεχνική του code signing για να επιβεβαιώσει την αυθεντικότητα και την ακεραιότητα των εφαρμογών πριν αυτές εγκατασταθούν σε συσκευές iOS. Αυτό εμποδίζει την εγκατάσταση μη εξουσιοδοτημένων εφαρμογών.
- **Ελέγχος Δικαιωμάτων (Permissions Check):** Κατά την εγκατάσταση μιας εφαρμογής στο iOS, ο χρήστης ζητείται να δώσει συγκεκριμένες άδειες (permissions) για την πρόσβαση σε ευαίσθητες πληροφορίες, όπως τον

προσωπικό του φάκελο, τις φωτογραφίες κλπ. Ο έλεγχος αυτών των δικαιωμάτων είναι σημαντικός για να διασφαλιστεί ότι η εφαρμογή έχει μόνο την πρόσβαση που χρειάζεται και όχι περισσότερη.

- **Ενημέρωση των Εφαρμογών:** Η Apple παρέχει τακτικές ενημερώσεις για το λειτουργικό σύστημα iOS και τις εφαρμογές του, περιλαμβανομένων διορθώσεων ασφαλείας. Οι χρήστες πρέπει να ενημερώνουν τις εφαρμογές τους σε τακτική βάση για να διασφαλίσουν την ασφάλεια των δεδομένων τους.

3.6.2 Απομόνωση Εφαρμογών

Η **απομόνωση εφαρμογών** στο **iOS** αποτελεί σημαντικό μέτρο ασφαλείας που βοηθά στην προστασία της ιδιωτικότητας και της ασφάλειας των δεδομένων του χρήστη. Αν και το iOS έχει σχεδιαστεί με αυτόματους μηχανισμούς ασφαλείας, η απομόνωση εφαρμογών προσθέτει ένα επιπλέον επίπεδο προστασίας. Ας αναλύσουμε πώς λειτουργεί αυτή η απομόνωση.

- **Απομόνωση Χώρου Εφαρμογής (App Sandbox):** Κάθε εφαρμογή στο iOS λειτουργεί σε ένα απομονωμένο περιβάλλον, γνωστό ως Sandbox. Αυτό σημαίνει ότι η εφαρμογή έχει περιορισμένη πρόσβαση μόνο σε συγκεκριμένους φακέλους και λειτουργίες του συστήματος.
- **Περιορισμένη Πρόσβαση σε Δεδομένα:** Οι εφαρμογές στο iOS έχουν περιορισμένη πρόσβαση σε ευαίσθητα δεδομένα, όπως τα προσωπικά σας φωτογραφίες ή το ηλεκτρονικό ταχυδρομείο σας. Αυτό εμποδίζει τις εφαρμογές να έχουν πρόσβαση σε πληροφορίες που δεν χρειάζονται για τη λειτουργία τους.
- **Διαχωρισμός Χρηστών:** Κάθε χρήστης σε μια συσκευή iOS έχει έναν διακριτό χώρο, όπου οι εφαρμογές και τα δεδομένα τους είναι απομονωμένα από τους άλλους χρήστες.
- **Περιορισμένες Δυνατότητες Εφαρμογών:** Οι εφαρμογές στο iOS περιορίζονται σε σχέση με τις λειτουργίες που μπορούν να εκτελέσουν. Για παράδειγμα, ορισμένες λειτουργίες, όπως η πρόσβαση στο σύστημα αρχείων ή η εγκατάσταση εφαρμογών εκτός του App Store, είναι περιορισμένες.
- **Έλεγχος Δικαιωμάτων:** Κατά την εγκατάσταση μιας εφαρμογής, ο χρήστης πρέπει να δώσει συγκεκριμένες άδειες για την πρόσβαση σε ευαίσθητα δεδομένα. Ο έλεγχος αυτών των δικαιωμάτων είναι σημαντικός για τη διασφάλιση της ασφάλειας της συσκευής.

3.6.3 Κρυπτογράφηση

Η κρυπτογράφηση είναι μια βασική τεχνολογία που χρησιμοποιείται για την προστασία των δεδομένων σε κινητές πλατφόρμες iOS. Η Apple εφαρμόζει διάφορους μηχανισμούς κρυπτογράφησης για να διασφαλίσει την ασφάλεια των πληροφοριών που αποθηκεύονται και μεταφέρονται από τις συσκευές iOS. Ακολουθεί μια ανάλυση

των κύριων τύπων και τεχνικών κρυπτογράφησης που χρησιμοποιούνται στις συσκευές iOS:

3.6.3.1 Κρυπτογράφηση Δεδομένων στην Αποθήκευση

Οι συσκευές iOS χρησιμοποιούν κρυπτογράφηση υλικού για να προστατεύουν όλα τα δεδομένα που αποθηκεύονται στη συσκευή. Η κρυπτογράφηση αυτή επιτυγχάνεται μέσω των παρακάτω μηχανισμών:

- **File System Encryption:** Κάθε αρχείο στη συσκευή κρυπτογραφείται με ένα μοναδικό κλειδί που παράγεται κατά τη δημιουργία του αρχείου. Αυτά τα κλειδιά αποθηκεύονται με ασφάλεια και προστατεύονται από την κύρια κρυπτογραφική μηχανή της συσκευής.
- **Data Protection Classes:** Η Apple έχει εισαγάγει κλάσεις προστασίας δεδομένων (Data Protection Classes) που επιτρέπουν τη ρύθμιση της πρόσβασης στα δεδομένα ανάλογα με την κατάσταση κλειδώματος της συσκευής. Αυτές οι κλάσεις περιλαμβάνουν:
- **Complete Protection:** Τα δεδομένα προστατεύονται έως ότου ο χρήστης ξεκλειδώσει τη συσκευή με τον κωδικό πρόσβασης ή το βιομετρικό στοιχείο.
- **Protected Until First User Authentication:** Τα δεδομένα προστατεύονται μέχρι την πρώτη επιτυχή επαλήθευση του χρήστη μετά την εκκίνηση της συσκευής.
- **Protected Unless Open:** Τα δεδομένα προστατεύονται μέχρι να ανοιχτούν και παραμένουν προστατευμένα όσο η συσκευή είναι κλειδωμένη.
- **No Protection :** Τα δεδομένα δεν προστατεύονται μέσω κρυπτογράφησης.

3.6.3.2 Κρυπτογράφηση Δικτύου

Οι συσκευές iOS χρησιμοποιούν κρυπτογράφηση για την προστασία των δεδομένων που μεταφέρονται μέσω δικτύων. Οι βασικοί μηχανισμοί περιλαμβάνουν:

- **SSL/TLS:** Όλες οι συνδέσεις στο Διαδίκτυο χρησιμοποιούν πρωτόκολλα SSL (Secure Sockets Layer) ή TLS (Transport Layer Security) για την ασφαλή μετάδοση δεδομένων μεταξύ της συσκευής και των διακομιστών. Αυτό προστατεύει τις πληροφορίες από υποκλοπές και παραβιάσεις κατά τη μετάδοσή τους.
- **VPN (Virtual Private Network):** Οι χρήστες μπορούν να χρησιμοποιήσουν VPN για να δημιουργήσουν ασφαλείς συνδέσεις σε απομακρυσμένα δίκτυα, προστατεύοντας τα δεδομένα τους από κακόβουλες επιθέσεις κατά τη μετάβαση από μη ασφαλή δίκτυα Wi-Fi.

3.6.3.3 Βιομετρική Κρυπτογράφηση

Οι συσκευές iOS χρησιμοποιούν βιομετρικά δεδομένα, όπως το Face ID και το Touch ID, για την επαλήθευση της ταυτότητας του χρήστη. Αυτά τα δεδομένα

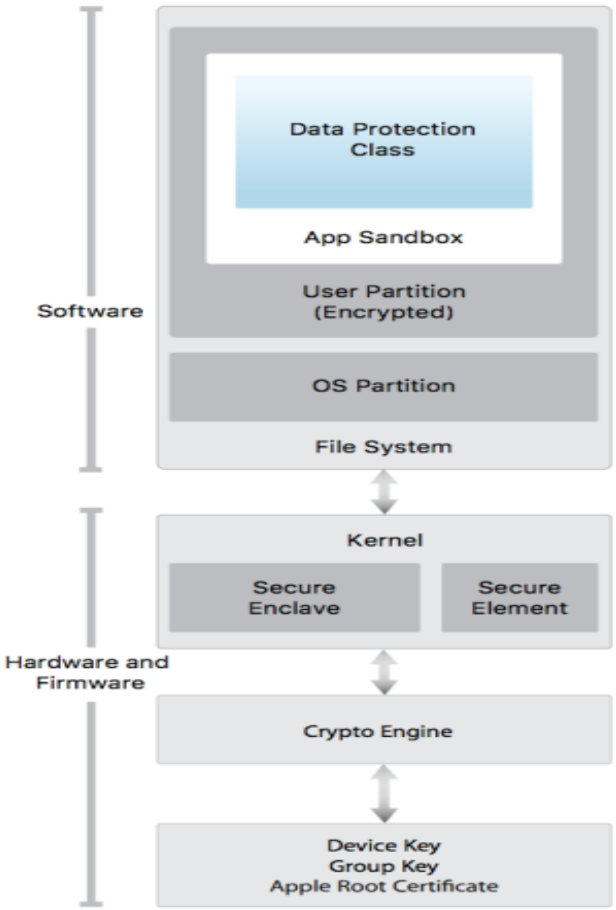
κρυπτογραφούνται και αποθηκεύονται με ασφάλεια στο Secure Enclave, ένα ξεχωριστό μέρος του επεξεργαστή που είναι απομονωμένο από το υπόλοιπο σύστημα.

- **Face ID και Touch ID:** Τα βιομετρικά δεδομένα δεν αποθηκεύονται ποτέ στο διακομιστή ή στα αντίγραφα ασφαλείας του iCloud. Αντίθετα, αποθηκεύονται τοπικά στη συσκευή και χρησιμοποιούνται μόνο για την επαλήθευση της ταυτότητας του χρήστη.

3.6.3.4 Κρυπτογράφηση Backups

Τα δεδομένα που δημιουργούνται αντίγραφα ασφαλείας (backups) από τις συσκευές iOS μπορούν να κρυπτογραφηθούν για πρόσθετη προστασία.

- **iTunes Backup Encryption:** Οι χρήστες μπορούν να ενεργοποιήσουν την κρυπτογράφηση για τα αντίγραφα ασφαλείας που δημιουργούνται μέσω του iTunes στον υπολογιστή τους, διασφαλίζοντας ότι τα δεδομένα τους είναι προστατευμένα ακόμη και στα αντίγραφα ασφαλείας.
- **iCloud Backup Encryption:** Τα δεδομένα που αποθηκεύονται στα αντίγραφα ασφαλείας του iCloud κρυπτογραφούνται κατά τη μετάδοση και την αποθήκευση, προσφέροντας αυξημένη ασφάλεια στα δεδομένα των χρηστών.



Εικόνα 49. iOS Security Review

Πηγή : https://mobile-jon.com/2018/07/18/ios-security-overview/

3.6.4 Εκπαίδευση και Ευαισθητοποίηση Χρηστών

Εκπαίδευση Χρηστών: Η Apple παρέχει οδηγίες και ενημερώσεις στους χρήστες σχετικά με τις βέλτιστες πρακτικές ασφάλειας και τους κινδύνους από κακόβουλες επιθέσεις. Η ενημέρωση των χρηστών για το πώς να αναγνωρίζουν και να αποφεύγουν τις απειλές είναι κρίσιμη για τη συνολική ασφάλεια.

Αναφορές και Ειδοποιήσεις: Οι χρήστες ενημερώνονται για ύποπτες δραστηριότητες και μπορούν να αναφέρουν τυχόν ανησυχητικές ενέργειες στη συσκευή τους. Αυτό βοηθά στην ταχεία ανταπόκριση και την αποτροπή πιθανών επιθέσεων.

4. ΜΕΛΕΤΕΣ ΠΕΡΙΠΤΩΣΗΣ ΑΞΙΟΛΟΓΗΣΗΣ ΕΥΠΑΘΕΙΩΝ & ΔΟΚΙΜΩΝ ΔΙΕΙΣΔΥΣΗΣ

4.1 Μοντελοποίηση πλαισίου δοκιμών διείσδυσης κινητών εφαρμογών

A. Static Analysis: Για την εξασφάλιση της ασφάλειας των κινητών εφαρμογών, μπορεί να γίνει ανάλυση των πληροφοριών που παρέχει η εφαρμογή χωρίς να εγκατασταθεί στη συσκευή, για να διαπιστωθεί αν είναι επιβλαβής. Στο πλαίσιο της μελέτης, επιλέγουμε το Qark για εφαρμογές iOS και τα Androbugs και APKTool για εφαρμογές Android για στατική ανάλυση. Με την ανάλυση αυτή, μπορούν να ληφθούν πληροφορίες για τη συμπεριφορά της εφαρμογής. Το μεγαλύτερο πλεονέκτημα της στατικής ανάλυσης είναι η ανίχνευση επιβλαβών συμπεριφορών χωρίς την εγκατάσταση της εφαρμογής στη συσκευή, αποφεύγοντας έτσι τις πιθανές επιπτώσεις από κακόβουλο λογισμικό.

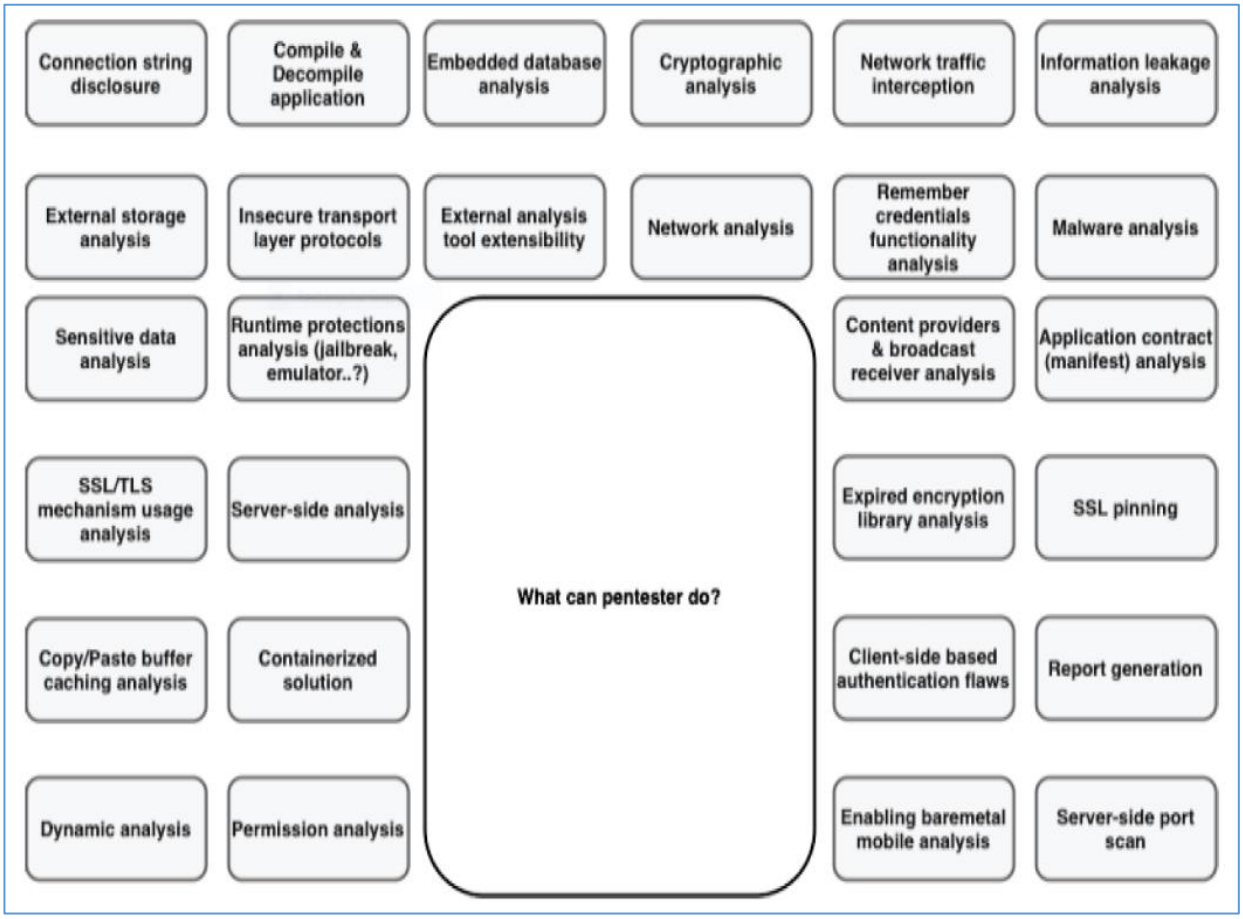
B. Dynamic Analysis: Η δυναμική ανάλυση είναι η δοκιμή και αξιολόγηση λογισμικού μέσω της εκτέλεσής του σε πραγματικό χρόνο. Στόχος είναι η ανίχνευση σφαλμάτων κατά την εκτέλεση του προγράμματος, αντί της επαναλαμβανόμενης ανασκόπησης του κώδικα εκτός σύνδεσης. Κατά τη δυναμική ανάλυση των κινητών εφαρμογών, η εφαρμογή εγκαθίσταται σε εικονική ή πραγματική συσκευή και αναλύεται με δοκιμές σε πραγματικό χρόνο. Συλλέγονται δεδομένα σε πραγματικό χρόνο για την εφαρμογή και εφαρμόζονται διάφορες εισροές και δοκιμές για να παραχθεί ανώμαλη συμπεριφορά. Στη μελέτη, προτείνεται το Cydia για εφαρμογές iOS και το Drozer για εφαρμογές Android για δυναμική ανάλυση.

C. Network Analysis: Σε μια κινητή εφαρμογή, η επικοινωνία μεταξύ της συσκευής και του εξυπηρετητή γίνεται μέσω διαδικτυακών πρωτοκόλλων. Αυτό αφορά την ασφάλεια της επικοινωνίας πελάτη-εξυπηρετητή και τη μεταφορά δεδομένων. Για παράδειγμα, όταν εισάγεις τα διαπιστευτήρια σου σε μια τραπεζική εφαρμογή, αν αυτές οι πληροφορίες δεν εγκριθούν από τον εξυπηρετητή, δεν μπορείς να εισέλθεις στο σύστημα. Η ασφάλεια των δεδομένων κατά την αποστολή τους, το αν η εφαρμογή στέλνει προσωπικά δεδομένα προς τα έξω, αν υπάρχει διαρροή δεδομένων, ο έλεγχος των υπηρεσιών της εφαρμογής, τα πρωτόκολλα κρυπτογράφησης που χρησιμοποιεί και αν υπάρχουν αδυναμίες σε αυτά τα πρωτόκολλα είναι αποτελέσματα που μπορούν να προκύψουν από την ανάλυση δικτύου. Εργαλεία όπως το BurpSuite ή το Wireshark μπορούν να χρησιμοποιηθούν για την ανάλυση της κίνησης του δικτύου.

D. Hybrid Analysis: Η υβριδική ανάλυση είναι ένας συνδυασμός στατικής, δυναμικής και ανάλυσης δικτύου. Περιλαμβάνει χαρακτηριστικά από όλους αυτούς τους τύπους αναλύσεων. Η υβριδική ανάλυση έχει μεγαλύτερη πολυπλοκότητα σε σύγκριση με άλλους τύπους και καταναλώνει περισσότερους πόρους. Είναι ικανή να συλλέγει πληροφορίες από τη στατική ανάλυση του πηγαίου κώδικα, την

ανάλυση της εκτέλεσης των εφαρμογών σε πραγματικό χρόνο και τα δεδομένα που μεταφέρονται μέσω του δικτύου.

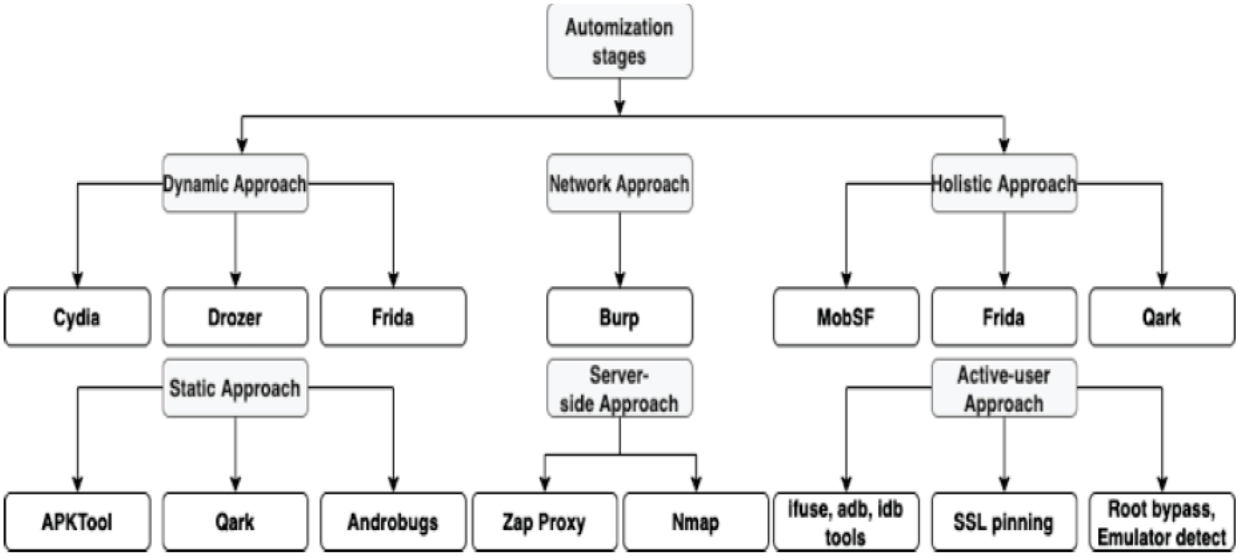
Στο πλαίσιο της τρέχουσας μελέτης [28] , στόχος είναι να προστεθεί ευελιξία στον αναλυτή κινητών εφαρμογών κατά την ανάλυση. Οι αναλυτές ασφαλείας θα έχουν την ευκολία πρόσβασης σε διάφορα εργαλεία μέσω ενός ενιαίου πλαισίου εφαρμογής. Επίσης, θα μπορούν να αποθηκεύουν και να εξάγουν τις αναφορές που προκύπτουν από την ανάλυση των εφαρμογών. Η εικόνα 50 δείχνει τον χάρτη δυνατοτήτων του αναλυτή δοκιμών διείσδυσης. Επιπλέον, οι αναλυτές ασφαλείας θα μπορούν να αποκτούν αυτά τα δεδομένα με ουσιαστικό τρόπο, ζητώντας την επεξεργασία των αποτελεσμάτων που προκύπτουν από τα εργαλεία ανάλυσης ασφαλείας, χάρη σε αλγορίθμους συγχώνευσης δεδομένων.



Εικόνα 50. Example of what pentester can do with framework

Ο αναλυτής θα ανεβάσει το αρχείο (".apk" για Android ή ".ipa" για iOS) που θέλει να αναλύσει. Ανάλογα με το αρχείο, θα εμφανίζονται τα κατάλληλα εργαλεία ανάλυσης. Αν το αρχείο δεν είναι συμβατό με τα εργαλεία ανάλυσης, ο αναλυτής προειδοποιείται. Το πλαίσιο εφαρμογής επιτρέπει την επιλογή από υπάρχοντα εργαλεία ανάλυσης ασφαλείας και ενημερώνει τον αναλυτή για τους περιορισμούς τους. Για παράδειγμα, αν ένα εργαλείο υποστηρίζει μόνο Android και ο αναλυτής ανεβάσει

αρχείο .ipa, θα προειδοποιηθεί. Επίσης, αν απαιτείται πρόσβαση στη συσκευή ή δικαιώματα root κατά τη δυναμική ανάλυση, ο αναλυτής προειδοποιείται. Το Σχήμα 2 δείχνει την αυτοματοποίηση του πλαισίου δοκιμών διείσδυσης ανά τύπο ανάλυσης.

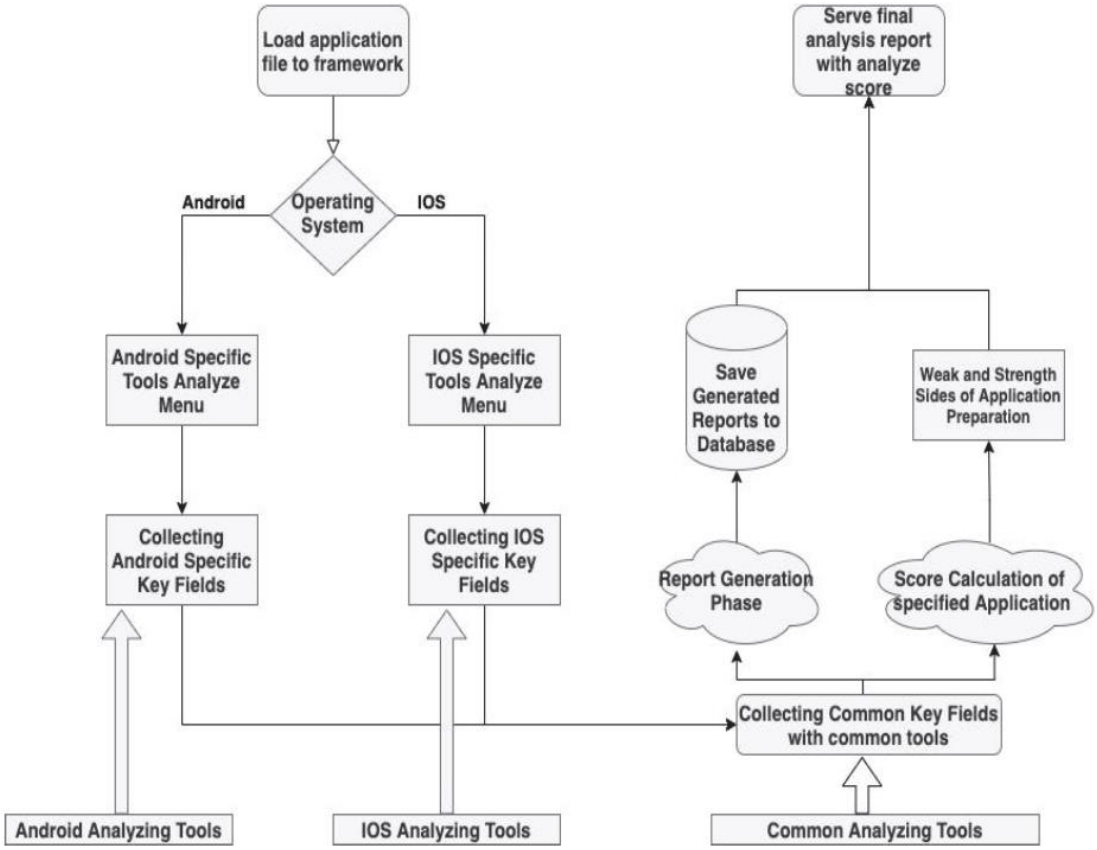


Εικόνα 51. Example of Automation steps

Η συγχώνευση δεδομένων (data fusion) είναι η διαδικασία ερμηνείας πληροφοριών από διαφορετικές πηγές μέσω φίλτρου. Οι εφαρμογές Android και iOS έχουν κοινά βασικά πεδία όπως παράκαμψη ταυτοποίησης, ανάλυση manifest, σύγχυση πηγαίου κώδικα, ενσωματωμένοι κωδικοί πρόσβασης, σάρωση URL και κακόβουλου λογισμικού. Κάθε πεδίο έχει σκορ και ο αλγόριθμος συγχώνευσης υπολογίζει το τελικό σκορ για την εφαρμογή, καθοδηγώντας τους αναλυτές. Τα πεδία αυτά συλλέγονται μέσω δυναμικής, στατικής, δικτυακής, ολιστικής, ενεργού χρήστη και προσέγγισης από την πλευρά του διακομιστή.

Με το πλαίσιο αυτό, οι αναλυτές δοκιμών διείσδυσης μπορούν να αυτοματοποιήσουν επιθέσεις όπως SQL Injection, έλεγχος αποθήκευσης κωδικών πρόσβασης, ενημέρωση αλγορίθμων κρυπτογράφησης, εκτέλεση εντολών κελύφους, σάρωση κακόβουλου λογισμικού, ανάλυση πηγαίου κώδικα και έλεγχος root. Οι αναφορές ανάλυσης μπορούν να αποθηκευτούν και να μοιραστούν μέσω email.

Στη φάση ερμηνείας δεδομένων, οι αναλυτές μπορούν να υποβάλουν τις αναφορές ανάλυσης που έχουν αποκτηθεί με το πλαίσιο ανάλυσης ασφαλείας για κινητές εφαρμογές, σε καθορισμένη μορφή, στο πλαίσιο εφαρμογής για επεξεργασία με αλγορίθμους συγχώνευσης δεδομένων για ερμηνεία.



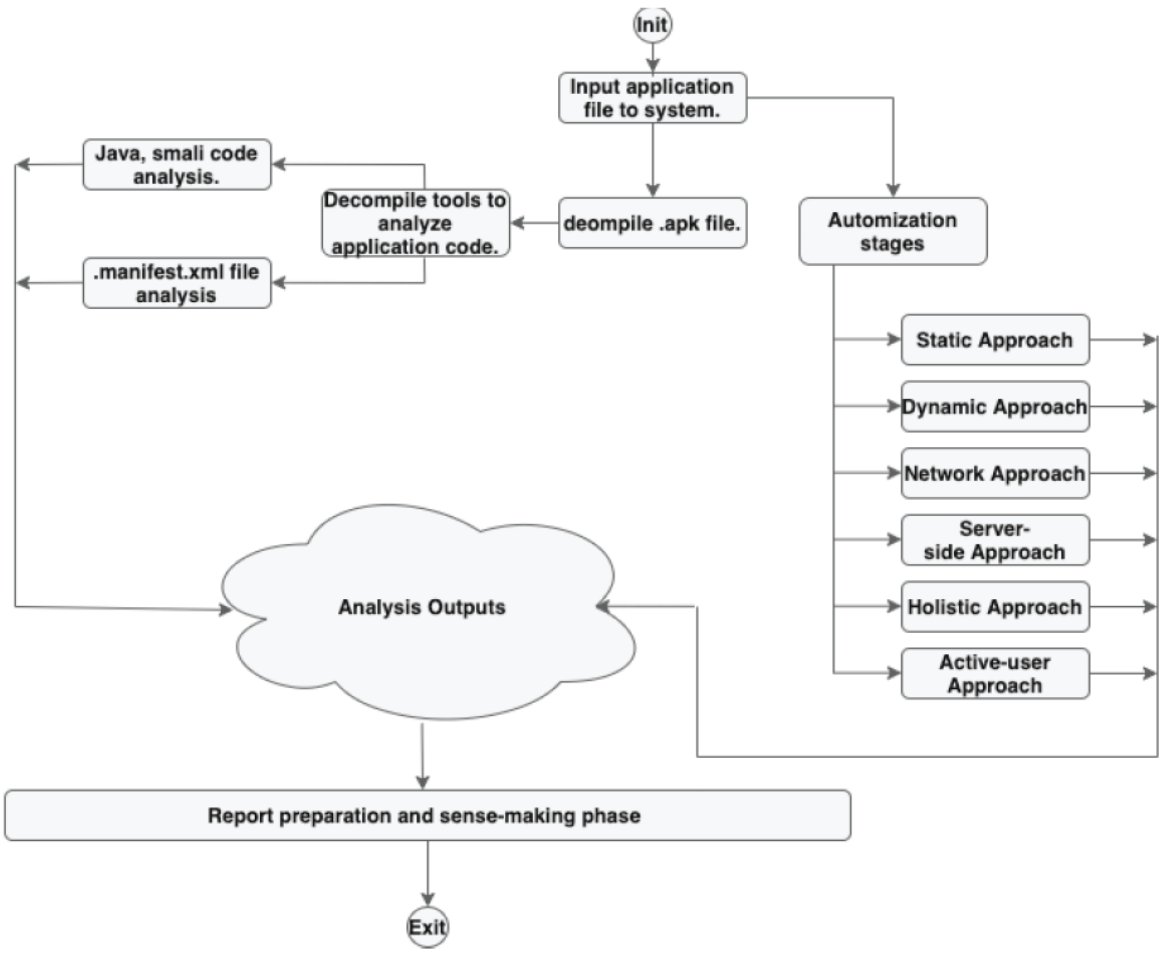
Εικόνα 52. Sense-making and fusion phase of framework

Το Mobile Application Penetration Test Framework στοχεύει να παρουσιάσει τα βήματα που πρέπει να ακολουθηθούν στη φάση ανάλυσης ασφαλείας των κινητών εφαρμογών, ως μια κατευθυντήρια λύση που ακολουθεί τον OWASP Mobile Security Testing Guide. Αυτό το πλαίσιο στοχεύει να είναι ένα πλαίσιο που μπορεί να καθοδηγήσει τους αναλυτές ασφάλειας να οδηγήσουν τη διαδικασία αναθεώρησης των αποτελεσμάτων ανάλυσης, μειώνοντας τον χρόνο ανάλυσης και κατευθύνοντας τους αναλυτές στα σημεία που πρέπει να εστιαστούν. Επίσης, πολλά εργαλεία ανάλυσης ασφαλείας κινητών εφαρμογών θα γίνουν προσβάσιμα μέσω του πλαισίου.

Αυτό το πλαίσιο θα έχει τη δυνατότητα να πραγματοποιεί στατική ανάλυση, δυναμική ανάλυση, δυαδική ανάλυση, συλλογή πληροφοριών συστατικών της εφαρμογής, διαπλοκή στην εφαρμογή, πρόσβαση στον πηγαίο κώδικα της εφαρμογής και στον πηγαίο κώδικα από αρχεία apk, μεταγλωττισμένες κλάσεις Java. Επίσης, εκτελεί ανάλυση στυλ κώδικα, ελέγχει εάν περιέχει εντολές κελύφους, αναλύει κακόβουλο λογισμικό, πραγματοποιεί έλεγχο επικοινωνίας μεταξύ διεργασιών της εφαρμογής, έχει πρόσβαση στη μνήμη που είναι εκχωρημένη στην εφαρμογή, ερευνά εάν υπάρχει αδυναμία κώδικα για επίθεση SQL Injection στην εφαρμογή και ελέγχει ενσωματωμένους κωδικούς πρόσβασης κ.λπ. Η εικόνα 53 δείχνει τη ροή του μοντέλου.

Επιπλέον, ο ερευνητής θα μπορεί να καταγράφει και να αποθηκεύει τα αποτελέσματα ως έκθεση που θα προκύπτουν με το πλαίσιο εφαρμογής. Μια άλλη

λειτουργία του πλαισίου είναι ότι ο ερευνητής θα μπορεί να ερμηνεύει τα δεδομένα από τις αναφορές που προκύπτουν ως αποτέλεσμα της ανάλυσης. Για την ερμηνεία των δεδομένων, θα χρησιμοποιούνται τεχνικές και αλγόριθμοι συγχώνευσης δεδομένων. Αυτά τα input, που περνούν μέσα από τους αλγόριθμους ερμηνείας και συγχώνευσης δεδομένων, στοχεύουν να παρέχουν στον ερευνητή ένα συγχωνευμένο αποτέλεσμα που δίνει λεπτομερείς πληροφορίες σχετικά με την ανάλυση της εφαρμογής.



Εικόνα 53. Flow diagram of Mobile Application Penetration Test Framework

Έρευνες έχουν δείξει ότι τα εργαλεία ασφάλειας κινητών δεν είναι πλήρως αυτοματοποιημένα. Ένα πλαίσιο που περιλαμβάνει όλα τα απαραίτητα εργαλεία μπορεί να απλοποιήσει αισίως τη φάση ανάλυσης. Επίσης, η χρήση τεχνικών συγχώνευσης βοηθά τους αναλυτές παρέχοντας μια επισκόπηση της εφαρμογής. Επιπλέον, θα εξοικονομήσει χρόνο και πολυπλοκότητα στους αναλυτές κατά τη διάρκεια της ανάλυσης. Αυτό το πλαίσιο δοκιμών διείσδυσης μπορεί να επεκταθεί προσθέτοντας περισσότερα εργαλεία δοκιμών διείσδυσης. Επίσης, για μελλοντικές εργασίες, το μοντέλο μπορεί να υλοποιηθεί και να αναπτυχθεί προσαρμόζοντας διάφορα εργαλεία ασφαλείας στο σύστημα.

4.2 Μελέτη Περίπτωσης Ανίχνευση Ευπαθειών σε δημοφιλείς εφαρμογές Android

Η ανάπτυξη και η χρήση εφαρμογών κινητών τηλεφώνων έχει εκτοξευθεί τα τελευταία χρόνια, ενώ οι ασφαλείς εφαρμογές απαιτούν ολοένα και περισσότερη προσοχή. Με την αύξηση του αριθμού των χρηστών και των διαθέσιμων εφαρμογών, αυξάνονται και οι ανησυχίες για την ασφάλεια. Η έλλειψη ενημέρωσης των προγραμματιστών και η ανεπαρκής δοκιμή των εφαρμογών πριν από τη διάθεσή τους στο κοινό αποτελούν μεγάλες αδυναμίες, καθιστώντας τις ευάλωτες σε επιθέσεις.

Σε αυτή την εργασία [29] , αρχικά εξετάστηκαν οι αιτίες και οι επιπτώσεις των αδυναμιών των εφαρμογών Android, καθώς και οι τρόποι εξάλειψής τους. Επιλέχτηκαν ορισμένες εφαρμογές από το Play Store και τις δοκιμάστηκαν με ορισμένα γνωστά εργαλεία δοκιμής. Ανακαλύφτηκε ότι όλες οι επιλεγμένες εφαρμογές είναι ευάλωτες σε έναν ή περισσότερους κινδύνους που δοκιμάσαμε. Αυτή η εργασία αναλύει τις αιτίες και τις επιπτώσεις αυτών των ευπαθειών και προτείνει τρόπους αντιμετώπισής τους. Τις έχουμε χωρίσει σε τρεις κατηγορίες: πέντε εφαρμογές κοινωνικών μέσων, πέντε που σχετίζονται με την οικονομία και πέντε διασκεδαστικές εφαρμογές. Αυτές οι εφαρμογές είναι δωρεάν για χρήση. Σε αυτή την εργασία, χρησιμοποιήθηκαν τρία εργαλεία ανοικτού κώδικα για τη δοκιμή εφαρμογών για ευπάθειες. Αυτά τα εργαλεία καλύπτουν ευρέως τις ευπάθειες που συζητούνται σε αυτό το έγγραφο, ενώ είναι επίσης δωρεάν και συμβατά με τα περισσότερα λειτουργικά συστήματα. Επιλέχτηκαν εσκεμμένα εργαλεία που επιτρέπουν τη μελλοντική επέκταση σε περίπτωση εντοπισμού επιπλέον ευπαθειών.

Βιβλιογραφική Αναφορά

Η έρευνα από τους Shezan εξετάζει τις κοινές ευπάθειες που εντοπίζονται σε τοπικές και ξένες εφαρμογές. Αναφέρουν οκτώ ευπάθειες και χρησιμοποιούν τρεις δοκιμαστές για να ελέγξουν τις εφαρμογές, ενώ εντοπίζουν κοινές αδυναμίες σε τοπικές και ξένες εφαρμογές.

Ο Jalal B. Hur και ο Jawwad A. Shamsi παρουσιάζουν τις προσπάθειες για την προστασία των πληροφοριών με διαφορετικά μέσα κρυπτογράφησης και επισημαίνουν επτά ευπάθειες. Μέσω μελέτης διάφορων τύπων επιθέσεων, αναλύουν τις προκλήσεις ασφάλειας και εξερευνούν πως μπορούν να αντιμετωπιστούν ανάλογες απειλές και επιθέσεις.

Ο Sebastien Salva και η Stassia R. Zafimiharisoa αναλύουν τη διαρροή δεδομένων ασφάλειας μέσω ανάλυσης ευπαθειών για εφαρμογές Android. Περιγράφουν μοντέλο ορισμού, μεθοδολογία δοκιμής ασφάλειας και πειραματισμό.

Οι Pingfan Kong, Li Li, Jun Gao, Kui Liu, Tegawende F. Bissyande και Jacques Klein μελετούν τον αυτοματοποιημένο έλεγχο των εφαρμογών Android. Αναλύουν τη μεθοδολογία της εργασίας τους και προτείνουν μια βιβλιογραφική ανασκόπηση.

Οι Sriramulu Bojjagani και V.N. Sastry ερευνούν τον έλεγχο ευπαθειών για εφαρμογές κινητής τραπεζικής σε Android. Αναφέρονται σε σενάρια απειλών και αναλύουν την επιφάνεια επίθεσης, τη στρατηγική ελέγχου και την ανάλυση ευπαθειών.

Η έρευνα των Mahmood και συνεργατών του εξετάζει μια αυτοματοποιημένη μέθοδο δοκιμής ασφάλειας για εφαρμογές Android στο cloud, η οποία χρησιμοποιεί μια διαφανή προσέγγιση που ονομάζεται white box testing.

Ανάλυση στην ασφάλεια των εφαρμογών

Οι εφαρμογές μπορούν συχνά να εκμεταλλευτούν από επιτιθέμενους για να αποκτήσουν πρόσβαση σε ευαίσθητα δεδομένα των χρηστών. Για να αποτρέψουμε τέτοιου είδους επιθέσεις, είναι ουσιώδες να προστατεύουμε συγκεκριμένα χαρακτηριστικά που είναι ευάλωτα στην εκμετάλλευση. Ένας τρόπος για να επιτευχθεί αυτό είναι μέσω λογισμικού ελέγχου ευπάθειας της εφαρμογής, το οποίο σαρώνει την εφαρμογή για εξουσιοδοτημένα προνόμια που μπορούν να εκμεταλλευτούν κακόβουλοι επιτιθέμενοι. Αυτά τα χαρακτηριστικά απαιτούν ιδιαίτερη προσοχή, καθώς μπορούν να παρέχουν ένα σημείο εισόδου για επιτιθέμενους για την απόκτηση προσωπικών δεδομένων των χρηστών. Με τον εντοπισμό και την αντιμετώπιση αυτών των ευπαθειών, οι προγραμματιστές εφαρμογών μπορούν να εξασφαλίσουν την ασφάλεια των εφαρμογών τους και να αποτρέψουν παραβιάσεις δεδομένων. Επομένως, το λογισμικό ελέγχου ευπάθειας της εφαρμογής είναι ένα κρίσιμο εργαλείο για την προστασία της ιδιωτικότητας των χρηστών και τη βελτίωση της συνολικής ασφάλειας των κινητών εφαρμογών.

A. **Implicit Intent:** Η εφαρμογή Android χρησιμοποιεί μια verifiable πρόθεση για να στείλει ευαίσθητα δεδομένα σε άλλες εφαρμογές. Δεδομένου ότι αυτός ο τύπος πρόθεσης δεν καθορίζει την εφαρμογή παραλήπτη, οποιαδήποτε εφαρμογή μπορεί να την χειριστεί χρησιμοποιώντας ένα φίλτρο πρόθεσης για αυτόν τον σκοπό.
B. **Ασφάλεια SSL:**Το σφάλμα Heartbleed μπορεί να αποτελεί μια ευπάθεια μέσα στο OpenSSL, ένα δημοφιλές βιβλιοθήκη κρυπτογράφησης ανοικτού κώδικα που επιτρέπει την υλοποίηση των πρωτοκόλλων SSL και TLS. Αυτό το σφάλμα επιτρέπει σε επιτιθέμενους να αποκτήσουν προσωπικά κλειδιά που σχετίζονται με πιστοποιητικά SSL, ονόματα χρηστών, κωδικούς πρόσβασης και άλλες ευαίσθητες πληροφορίες χωρίς να αφήσουν κανένα ίχνος.
C. **Αποκάλυψη Ευαίσθητων Πληροφοριών:** Συμβαίνει όταν μια εφαρμογή δεν προστατεύει επαρκώς ευαίσθητα δεδομένα τα οποία μπορεί να αποκαλυφθούν σε μέρη που δεν έχουν πρόσβαση σε αυτά. Οι ευαίσθητες πληροφορίες μπορεί να περιλαμβάνουν δεδομένα που σχετίζονται με την εφαρμογή, όπως τα session tokens, τα ονόματα αρχείων, οι αναφορές στο stack, ή προσωπικά δεδομένα, όπως κωδικοί πρόσβασης, πληροφορίες πιστωτικών καρτών και τον πηγαίο κώδικα του προϊόντος
D. **Μη Προστατευμένη Δραστηριότητα:** Στις εφαρμογές Android, ένα στοιχείο μπορεί να εξαχθεί για χρήση από άλλες εφαρμογές. Ωστόσο, εάν η πρόσβαση στο εξαγόμενο στοιχείο δεν περιοριστεί κατάλληλα, μπορεί να αποτελέσει πιθανό κίνδυνο για την ασφάλεια της εφαρμογής.

E. **Μη Προστατευμένη Υπηρεσία:** Ο διαμοιρασμός μιας υπηρεσίας με άλλες εφαρμογές σε μια συσκευή μπορεί να καθιστά την υπηρεσία προσβάσιμη από οποιαδήποτε άλλη εφαρμογή. Μια υπηρεσία είναι ένα στοιχείο που εκτελεί μια λειτουργία στο παρασκήνιο όταν κληθεί από ένα άλλο στοιχείο.

F. **Κλειδοθήκη Hacker:** Το σύστημα Android KeyStore προστατεύει τα κλειδιά από μη εξουσιοδοτημένη χρήση. Καταρχάς, αποτρέπει τη μη εξουσιοδοτημένη εξαγωγή του υλικού κλειδιών από εφαρμογές και τη συσκευή Android ως σύνολο. Επιπλέον, αποτρέπει τη μη εξουσιοδοτημένη χρήση του υλικού κλειδιών στη συσκευή Android, απαιτώντας από τις εφαρμογές να δηλώνουν την εξουσιοδότησή τους για τη χρήση των κλειδιών και επιβάλλοντας αυτούς τους περιορισμούς εκτός των διεργασιών των εφαρμογών.

G. **Πρόσβαση σε Εξωτερική Αποθήκευση:** Η αποθήκευση δεδομένων τοπικά μπορεί να είναι μια συνηθισμένη εργασία για κινητές εφαρμογές. Αυτά τα δεδομένα περιλαμβάνουν αρχεία μεταξύ άλλων. Ένα χρήσιμο μέσο για την αποθήκευση αρχείων είναι η χρήση της εξωτερικής αποθήκευσης αρχείων, η οποία συνήθως προσφέρει μεγαλύτερο χώρο αποθήκευσης σε σύγκριση με την εσωτερική αποθήκευση.

H. **Εκτέλεση Απομακρυσμένου Ελέγχου Webview:** Υπάρχει μια ευπάθεια ασφάλειας για εκτέλεση απομακρυσμένου κώδικα σε επίπεδο API του Android 16 και προηγούμενων εκδόσεων. Η ευπάθεια οφείλεται στο γεγονός ότι το πρόγραμμα δεν περιορίζει σωστά τη χρήση της Web View.

I. **Η Εφαρμογή Περιλαμβάνει Privacy Trackers:** Χωρίς πληροφορίες επαφής, τα δεδομένα μιας ενέργειας της εφαρμογής παρακολουθούνται από ένα αναγνωριστικό συσκευής, ένα μοναδικό αναγνωριστικό (δηλαδή, ένα αναγνωριστικό για διαφημιστές ή IDFA) που καθιστά εύκολη την παρακολούθηση ενός χρήστη μέσω άλλων εφαρμογών, υπηρεσιών και ιστότοπων.

J. **Το Λειτουργικό Επίπεδο της Δραστηριότητας δεν είναι Standard:** Συνήθως, αυτή είναι η προεπιλεγμένη λειτουργία εκκίνησης μιας δραστηριότητας (εάν δεν έχει καθοριστεί αλλιώς). Εκκινεί μια νέα περίπτωση της δραστηριότητας εντός της εργασίας από την οποία ξεκίνησε.

Εργαλεία που χρησιμοποιήθηκαν

Η ασφάλεια των προσωπικών μας συσκευών και πληροφοριών είναι ζωτικής σημασίας στον σημερινό κόσμο, και οι αξιολογήσεις ασφαλείας εφαρμογών παίζουν κρίσιμο ρόλο στη διασφάλισή τους. Εξετάζοντας προσεκτικά τις εφαρμογές που χρησιμοποιούμε, μπορούμε να εντοπίσουμε πιθανές ευπάθειες που θα μπορούσαν να αποτελέσουν απειλή για την ασφάλειά μας σε περίπτωση που εκμεταλλευτούν. Υπάρχουν διάφορες προσεγγίσεις για την πραγματοποίηση αυτών των αξιολογήσεων, συμπεριλαμβανομένων επιλογών βασισμένων σε ανάλυση που εντοπίζουν και επισημαίνουν οποιαδήποτε ύποπτη συμπεριφορά εντός των εφαρμογών, και επιλογών

βασισμένων σε ανίχνευση που στοχεύουν στην αποτροπή της εγκατάστασης εφαρμογών που μπορεί να απειλήσουν τις συσκευές μας.

Για την πραγματοποίηση αυτών των βημάτων, οι ειδικοί μπορεί να χρησιμοποιήσουν είτε στατική ανάλυση, η οποία εξετάζει τον κώδικα της εφαρμογής χωρίς να την εκτελεί, είτε δυναμική αξιολόγηση, η οποία περιλαμβάνει τη δοκιμή της εφαρμογής κατά τη διάρκεια της λειτουργίας της. Ανεξαρτήτως της μεθόδου που χρησιμοποιείται, ο τελικός στόχος είναι να εξασφαλιστεί ότι οι συσκευές και οι πληροφορίες μας παραμένουν ασφαλείς από κίνδυνο, επιτρέποντάς μας να απολαμβάνουμε τα οφέλη της τεχνολογίας χωρίς να θέτουμε σε κίνδυνο τον εαυτό μας. Για την εντοπισμό ευπαθειών στις εφαρμογές μας, χρησιμοποιήθηκαν τα εργαλεία Androbugs, Quixxi και MobSF.

Androbugs

Με το υψηλά αποτελεσματικό και ακριβές σύστημα ανάλυσης ευπαθειών στο Android του AndroBugs Framework, είναι δυνατό να σαρώνονται γρήγορα οι εφαρμογές Android σε λιγότερο από δύο λεπτά. Αυτό το σύστημα ανιχνεύει μια σειρά ευπαθειών που σχετίζονται με την ασφάλεια και που μπορεί να αποτελέσουν κινδύνους για την ασφάλεια της εφαρμογής. Αυτό καθιστά το AndroBugs την κορυφαία επιλογή για ολοκληρωμένη ανάλυση ασφαλείας εφαρμογών. Οι δυνατότητες του AndroBugs περιλαμβάνουν τον εντοπισμό ευπαθειών ασφάλειας σε μια εφαρμογή Android, ελέγχους για την απουσία εξαιρετικών πρακτικών στον κωδικό, ελέγχους για επικίνδυνες εντολές κελύφους, καθώς και ελέγχους της ασφάλειας της εφαρμογής.

Quixxi

Το Quixxi είναι μια ολοκληρωμένη λύση ασφαλείας για κινητές εφαρμογές που προσφέρει ευελιξία και προστασία. Με τη δυνατότητα αξιολόγησης των εφαρμογών για ευπάθειες και τον περιορισμό της προσβασιμότητας σε κακοβουλό λογισμικό, παρέχει επιπλέον επίπεδα ασφαλείας που εγγυώνται την ακεραιότητα των δεδομένων και των λειτουργιών των εφαρμογών. Το Quixxi αναλαμβάνει την αναγνώριση και αντιμετώπιση των ευπαθειών με σαφή αναφορά των ευρημάτων και προτάσεις για τη βελτίωση της ασφαλείας, ενώ παράλληλα παρέχει προστασία από εξωτερικούς κινδύνους με την εφαρμογή ασφαλούς κρυπτογράφησης για τις εφαρμογές και τα δεδομένα τους.

Mobile Security Framework (MobSF)

Το Mobile Security Framework (MobSF) είναι ένα εργαλείο ασφαλείας για κινητές εφαρμογές (Android/iOS/Windows) που προσφέρει αυτοματοποιημένες δοκιμές διείσδυσης, ανάλυση κακοβουλίας και εκτίμηση ασφαλείας. Το εργαλείο API Fuzzer για δοκιμές ασφαλείας των διεπαφών web API μπορεί να εκτελέσει πολλές λειτουργίες, συμπεριλαμβανομένης της μαζικής επεξεργασίας δεδομένων και της ανάλυσης ασφαλείας κινητών εφαρμογών. Επίσης, προσφέρει υποστήριξη για πολλές πλατφόρμες, συμπεριλαμβανομένων των Android και iOS.

Vulnerability Name	AndroBugs	Quixxi	MobSF
Implicit Intent	Y	Y	N
SSL Security	Y	Y	N
Sensitive Information	Y	Y	Y
Unprotected Activity	N	N	Y
Unprotected Service	N	N	Y
KeyStore Hacker	Y	N	N
External Storage Accessing	Y	Y	Y
WebView Remote Code Execution	Y	Y	Y
Application containing Privacy Trackers	N	N	Y
Activity Launch Mode is not standard	N	N	Y

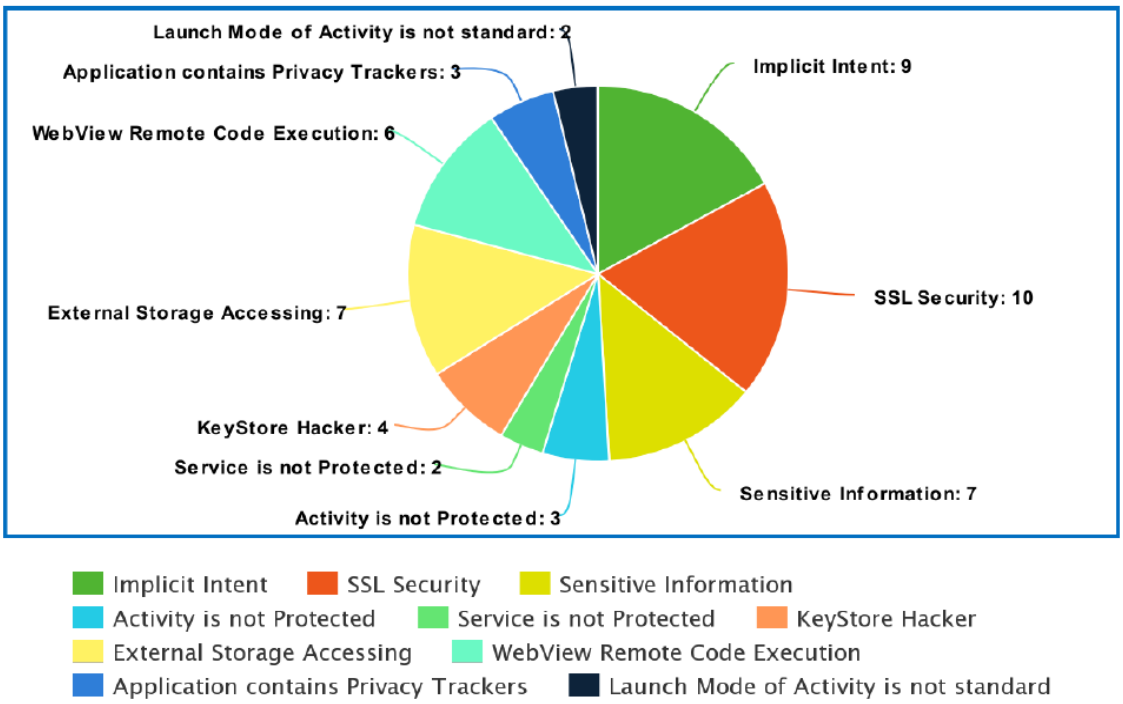
Εικόνα 54. Tools Supporting Different Tests

Ανάλυση και Αποτελέσματα: Αξιολογήθηκαν 15 εφαρμογές Android που ληφθήκαν από το Google Play Store σε τρεις κατηγορίες: οικονομικές, παιχνίδια και κοινωνικά μέσα. Αυτές οι εφαρμογές επιλέχθηκαν λόγω της μαζικής χρήσης τους από τους χρήστες. Οι επιθέσεις από χάκερς προς τους χρήστες συμβαίνουν συχνότερα μέσω αυτών των εφαρμογών. Για να διεξαχθεί μια ισορροπημένη δοκιμή μεταξύ των τριών κατηγοριών, δεν επιλέξαμε περισσότερες εφαρμογές, καθώς είναι όλες περίπου παρόμοιες μεταξύ τους. Μια από τις επιλεγμένες εφαρμογές, το bKash, είναι μια εφαρμογή για μεταφορά μετρητών μέσω κινητού τηλεφώνου από μια τοποθεσία σε μια άλλη. Σύμφωνα με τα αποτελέσματα των δοκιμών, όλες οι επιλεγμένες εφαρμογές ανακαλύφθηκαν να περιέχουν μία ή περισσότερες ευπάθειες. Από την εικόνα 57, το Candy Crush βρίσκεται στην κορυφή της λίστας με περισσότερες από έξι ευπάθειες. Το bKash, το DBBL, το Google Pay, το 8 Ball Pool και το Imo επίσης εμφανίζουν πέντε ευπάθειες η καθεμία. Αντίθετα, το Nagad, το Luno, το Hill Climb Racing, το Facebook, το Instagram, το Messenger και το WhatsApp Messenger ήταν ευάλωτα σε τρεις προβλήματα η καθεμία. Το Among Us και το Temple Run περιέχουν από δύο ευπάθειες.

App Name	Combined Test Outcome
bKash	Read/Write access to External Storage. Cleartext Storage of Sensitive Information in source code. WebView loads files from external storage. Deprecated implementation of SSL Sockets.
Nagad	Implicit Intent. External Storage Accessing. Sensitive Information.
DBBL	Cleartext Storage of Sensitive Information in source code. Read/Write access to External Storage. Deprecated implementation of SSL Sockets. WebView loads files from external storage.
Google Pay	Implicit Intent. SSL Security. Sensitive Information. WebView Remote Code Execution.
Luno	Activity is not Protected. Service is not Protected. Application contains Privacy Trackers.

Εικόνα 55. Chosen applications and analysis outcomes (category:finance)

Η ευπάθεια της ασφάλειας SSL είναι η πιο διαδεδομένη αδυναμία σε περισσότερες από 10 εφαρμογές και βρέθηκε σε 66,6% των εφαρμογών. Οι ευπάθειες Implicit Intent και Ευαίσθητων Πληροφοριών είναι επίσης προβληματικές, παρουσιάζονται σε 9 και 7 εφαρμογές αντίστοιχα. Από την εικόνα 58 βλέπουμε ότι αυτές οι εφαρμογές έχουν χαμηλότερο ρυθμό ευπαθειών από αυτές των εικόνων 55 και 57. Το Nagad, το WhatsApp Messenger, το Messenger, το Instagram, το Facebook και το Luno.



Εικόνα 56. Occurrence of vulnerabilities in selected apps

App Name	Combined Test Outcome
Among Us	Activity is not Protected. Service is not Protected.
Hill Climb Racing	Activity is not Protected. Application contains Privacy Trackers. Launch Mode of Activity is not standard.
Candy Crush	KeyStore Hacker. Implicit Intent. SSL Security. WebView Remote Code Execution. External Storage Accessing. Sensitive Information.
8 Ball Pool	Implicit Intent. SSL Security. WebView Remote Code Execution. External Storage Accessing. Sensitive Information.
Temple Run	Application contains Privacy Trackers. Launch Mode of Activity is not standard.

Εικόνα 57. Chosen applications and analysis outcomes (category: game)

App Name	Combine Test Outcome
Facebook	Implicit Intent. SSL Security. KeyStore Hacker.
Instagram	KeyStore Hacker. Implicit Intent. SSL Security.
Messenger	Implicit Intent. SSL Security. KeyStore Hacker.
Imo	Implicit Intent. SSL Security. WebView Remote Code Execution. External Storage Accessing. Sensitive Information.
WhatsApp Messenger	SSL Security. Implicit Intent. External Storage Accessing.

Εικόνα 58. Chosen applications and analysis outcomes (category: social

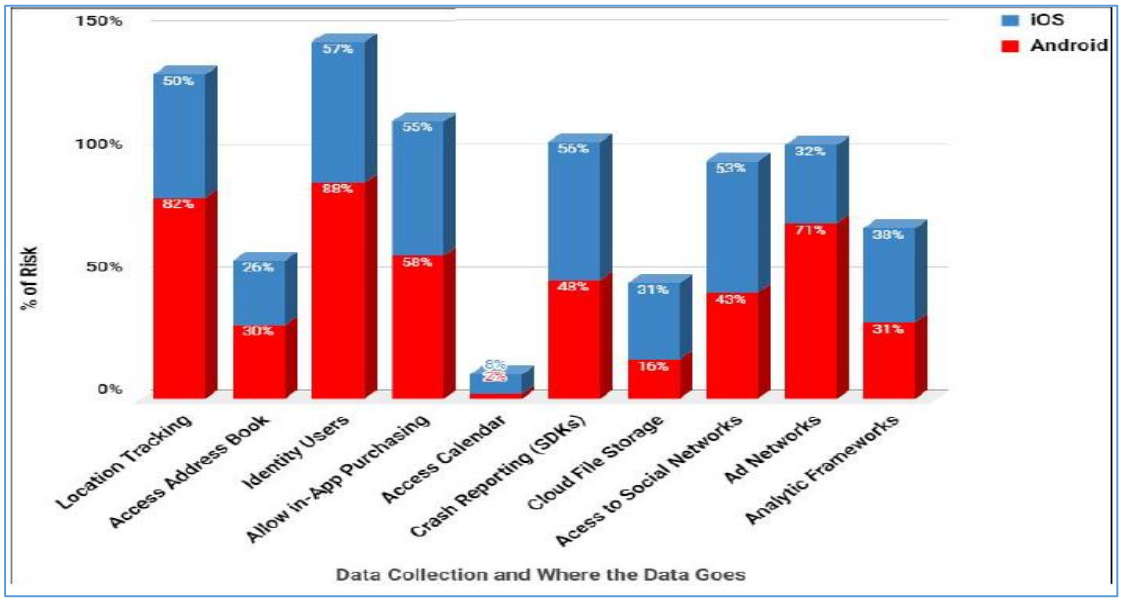
Από τότε που δημιουργήθηκε το Android, ειδικοί στην ασφάλεια ψάχνουν για ευπάθειες και προτείνουν λύσεις για τη βελτίωση της ασφάλειας των εφαρμογών Android. Για αυτό δοκιμάστηκαν μερικές εφαρμογές από το Google Play Store χρησιμοποιώντας τρία διαφορετικά εργαλεία online και συνοψίστηκαν τα ευρήματα σε έναν πίνακα. Δυστυχώς, διαπιστώθηκε ότι η ασφάλεια SSL ήταν ένα μείζον πρόβλημα σε πολλές εφαρμογές, ενώ το implicit intent ήταν επίσης κοινό σε 9 από τις 15 δοκιμασμένες εφαρμογές. Είναι αναγκαία άμεση δράση για την αντιμετώπιση αυτών των ανησυχιών και τα τεστ θα συνεχιστούν σε αυτόν τον τομέα στο μέλλον.

4.3 Μελέτη Περίπτωσης Αξιολόγησης Ευπαθειών σε Εφαρμογές Κινητής Τραπεζικής (Mobile Banking Applications)

Η χρήση των κινητών συσκευών έχει αυξηθεί δραματικά τα τελευταία χρόνια, οδηγώντας σε μια ανάλογη αύξηση των εφαρμογών κινητής τραπεζικής (Mobile Banking Applications - MBAs). Οι εφαρμογές αυτές, που αποθηκεύουν και μεταδίδουν ευαίσθητα δεδομένα, αποτελούν σημαντικό στόχο για επιθέσεις. Οι καταναλωτές χρησιμοποιούν MBAs για να εκτελούν οικονομικές συναλλαγές, να διαχειρίζονται τους τραπεζικούς τους λογαριασμούς και να εκτελούν άλλες χρηματοοικονομικές δραστηριότητες. Σύμφωνα με το National Institute of Standards and Technology (NIST) κάθε MBA θα πρέπει να έχει βασικά χαρακτηριστικά ασφαλείας όπως εμπιστευτικότητα (confidentiality), έλεγχος ταυτότητας (authentication) και ακεραιότητα (integrity) των δεδομένων χρήστη. Αλλά τα περισσότερα MBA είναι ελλιπή και γίνονται vulnerable. Σε αυτή τη μελέτη, θα αναλύσουμε τις ευπάθειες των MBAs σε Android και iOS, προτείνοντας ένα μοντέλο απειλών για την ανίχνευση και μετριασμό των ευπαθειών αυτών.

Σε αυτή τη μελέτη αναλύονται 5 Android και 3 iOS MBAs, τα οποία έχουν εκατομμύρια εγκαταστάσεις. Σύμφωνα με την πρόσφατη έκθεση έρευνας [40], το 95%

των κορυφαίων 200 δωρεάν εφαρμογών iOS και Android παρουσιάζουν τουλάχιστον μία επικίνδυνη συμπεριφορά. Στην έκθεση Appthority αναφέρεται ότι το 91% των εφαρμογών iOS και το 85% των εφαρμογών Android έδειξαν κάποιο ρίσκο απειλής στη παρακολούθηση τοποθεσίας, τις λίστες επαφών για να αναγνωρίζεται ένας χρήστης, τα οποία εμφανίζονται στο παρακάτω διάγραμμα.



Εικόνα 59. Top 10 Risky Behaviors: (Appthority Report)

Οι κύριοι στόχοι της μελέτης αυτής είναι:

1) Να προσδιορίσουμε τις κύριες κατηγορίες ευπαθειών στις MBAs.
2) Να αναπτύξουμε ένα μοντέλο απειλών που θα βοηθήσει στην ανίχνευση και τον μετριασμό αυτών των ευπαθειών.
3) Να αξιολογήσουμε την αποτελεσματικότητα του προτεινόμενου μοντέλου μέσω της ανάλυσης πραγματικών εφαρμογών Android και iOS.
4) Να προτείνουμε βέλτιστες πρακτικές και μέτρα ασφαλείας για την ενίσχυση της ασφάλειας των MBAs.

Category of Security Testing	Research Works	Type of program analysis					Platform
		Static	Dynamic	Hybrid	Automatic	Manual	
Application Level Security	iCryptoTracer [6]	Yes	Yes	Yes	Yes	Yes	iOS
	ClusteringiOS [7]	Yes	No	No	Yes	No	iOS
	PiOS [8]	Yes	Yes	Yes	No	No	iOS
	PSiOS [15]	Yes	Yes	Yes	No	No	iOS
	STAMBA [48]	Yes	Yes	Yes	No	No	Android
	Amandroid [9]	Yes	Yes	Yes	No	No	Android
	DroidJust [10]	Yes	Yes	Yes	No	No	Android
	Droidalarm [11]	Yes	No	No	Yes	No	Android
	AppCracker [42]	Yes	No	No	Yes	No	Android
Communication Level Security	Open Wi-Fi [17]	NA	NA	NA	NA	NA	iOS
	SSL:proxy [16]	Yes	Yes	Yes	No	No	iOS/Android
	Dangerous Wi-Fi [43]	No	Yes	No	No	Yes	Android
	SMV-HUNTER [13]	Yes	Yes	Yes	No	No	Android
	AndroSSL [12]	Yes	Yes	Yes	No	No	Android
	StaDyna [14]	Yes	Yes	Yes	Yes	No	Android
Device Level Security	DroidVulMon [18]	Yes	Yes	Yes	Yes	No	Android
	Xing et al. [19]	No	Yes	No	Yes	No	Android

Εικόνα 60. Classification of Literature on Mobile Security Testing

4.3.1 Proposed Threat Model

Τα MBA που υπάρχουν στο Android play store & iOS app store δεν έχουν επαληθευτεί και ελεγχθεί εξαντλητικά ως προς την ασφάλειά τους. Για αυτό σε αυτό κεφάλαιο αναλύονται οι τύποι απειλών.

- **V1. Ανασφαλής Αποθήκευση Δεδομένων (Insecure Data Storage)**
  Πολλές εφαρμογές αποθηκεύουν ευαίσθητα δεδομένα χωρίς κρυπτογράφηση, καθιστώντας τα ευάλωτα σε επιθέσεις μέσω rooting ή jailbreaking. Αυτό μπορεί να περιλαμβάνει διαπιστευτήρια σύνδεσης, tokens αυθεντικοποίησης και άλλα ευαίσθητα δεδομένα. ©Παραδείγματα περιλαμβάνουν την αποθήκευση κωδικών πρόσβασης σε απλό κείμενο ή τη χρήση μη ασφαλών αποθηκευτικών χώρων όπως Shared Preferences χωρίς κρυπτογράφηση.

- **V2. Έλλειψη Προστασίας Δυαδικών Αρχείων (Lack of Binary Protection)**
  Οι εφαρμογές που δεν προστατεύονται μπορούν εύκολα να αντιστραφούν και να αναλυθούν από επιτιθέμενους, επιτρέποντας την αποκάλυψη ευαίσθητων λειτουργιών και δεδομένων. Η ανακατασκευή των εφαρμογών μπορεί να αποκαλύψει τις διαδικασίες ασφαλείας και να επιτρέψει την τροποποίηση του κώδικα για κακόβουλες ενέργειες. Τεχνικές όπως η obfuscation, η χρήση packers και η εφαρμογή μεθόδων anti-tampering μπορούν να συμβάλλουν στη δυσκολία της ανάλυσης των δυαδικών αρχείων.

- **V3. Ακούσια Διαρροή Δεδομένων (Unintended Data Leakage)**
  Οι προγραμματιστές ενδέχεται να αποθηκεύουν δεδομένα σε μη ασφαλείς τοποθεσίες, καθιστώντας τα προσβάσιμα από άλλες εφαρμογές ή επιτιθέμενους. Η ακούσια διαρροή μπορεί να συμβεί μέσω καταγραφών (logs), προσωρινών αρχείων ή ακόμη και μέσω κακόβουλων βιβλιοθηκών που χρησιμοποιούνται από την εφαρμογή. Είναι σημαντικό οι προγραμματιστές να διασφαλίζουν ότι τα ευαίσθητα δεδομένα δεν αποθηκεύονται σε προσιτές περιοχές του συστήματος αρχείων και ότι εφαρμόζονται πρακτικές ασφαλούς προγραμματισμού.

- **V4. Κακόβουλα Προγράμματα στις Εφαρμογές (Malware in Apps)**
  Τα δημοφιλή apps ανακατασκευάζονται και διανέμονται σε τρίτα καταστήματα εφαρμογών με κακόβουλο κώδικα. Οι χρήστες που κατεβάζουν εφαρμογές από ανεπίσημες πηγές διατρέχουν τον κίνδυνο να εγκαταστήσουν εφαρμογές που περιέχουν κακόβουλο λογισμικό. Αυτό το κακόβουλο λογισμικό μπορεί να συλλέξει ευαίσθητα δεδομένα, να εκτελέσει μη εξουσιοδοτημένες ενέργειες ή να προκαλέσει άλλες βλάβες στη συσκευή και τα δεδομένα του χρήστη.

- **V5. Αδύναμη Κρυπτογράφηση (Weak Cryptography)**
  Η χρήση αδύναμων αλγορίθμων κρυπτογράφησης ή η εσφαλμένη εφαρμογή τους καθιστά τις εφαρμογές ευάλωτες. Η χρήση απαρχαιωμένων ή αδύναμων αλγορίθμων όπως το MD5 και το SHA-1 μπορεί να οδηγήσει σε παραβιάσεις δεδομένων. Εφαρμογές που χρησιμοποιούν κλειδιά κρυπτογράφησης με

ανεπαρκές μήκος ή που δεν ακολουθούν βέλτιστες πρακτικές κρυπτογράφησης είναι ευάλωτες σε επιθέσεις brute force και άλλες κρυπτογραφικές επιθέσεις.

- **V6. Ελλιπής Προστασία Επίπεδου Μεταφοράς (Insufficient Transport Layer Protection)**
  Τα δεδομένα πρέπει να μεταφέρονται με ασφαλή πρωτόκολλα. Οι λανθασμένες ρυθμίσεις SSL μπορούν να οδηγήσουν σε επιθέσεις Man-in-the-Middle (MitM), replay, phishing και session hijacking. Οι επιτιθέμενοι μπορούν να εκμεταλλευτούν ευάλωτες διαμορφώσεις SSL/TLS για να παρακολουθήσουν και να χειριστούν την επικοινωνία μεταξύ της εφαρμογής και του διακομιστή, υποκλέπτοντας ευαίσθητες πληροφορίες.

- **V7. Privilege Escalation Attack**
  Τα δικαιώματα των εφαρμογών Android αποτελούν ένα προηγμένο μοντέλο ασφαλείας, το οποίο λειτουργεί κυρίως σε επίπεδο εφαρμογής και αξιοποιεί τεχνολογία sandbox. Επιτρέπει στους προγραμματιστές και τους χρήστες να περιορίζουν την εγκατάσταση μιας εφαρμογής στα δικαιώματα που της έχουν εκχωρηθεί κατά τη διάρκεια της εγκατάστασης. Έτσι, η εκμετάλλευση των τρωτών σημείων στον κώδικα πηγής θεωρείται ότι περιορίζεται εντός των ορίων των δικαιωμάτων του sandbox μιας εφαρμογής.

Αυτά τα κενά ασφαλείας οδηγούν στις παρακάτω επιθέσεις.

- **A1. Man-in-the-Middle Attack (MitM)**
  Ο επιτιθέμενος παρεμβάλλεται στην επικοινωνία μεταξύ χρήστη και διακομιστή, κατασκοπεύοντας ή τροποποιώντας τα δεδομένα. Αυτός ο τύπος επίθεσης είναι ιδιαίτερα επικίνδυνος σε δημόσια δίκτυα Wi-Fi, όπου οι επιτιθέμενοι μπορούν εύκολα να παρεμβάλλονται στην κυκλοφορία δικτύου. Οι χρήστες πρέπει να εκπαιδεύονται για τους κινδύνους της χρήσης μη ασφαλών δικτύων και οι εφαρμογές πρέπει να εφαρμόζουν αυστηρά πρωτόκολλα SSL/TLS για την κρυπτογράφηση της επικοινωνίας.

- **A2. Phishing Attack**
  Οι χρήστες παρασύρονται σε ψεύτικους ιστότοπους που μοιάζουν με τους πραγματικούς για να αποκαλύψουν τα διαπιστευτήριά τους. Οι επιτιθέμενοι χρησιμοποιούν τεχνικές κοινωνικής μηχανικής για να πείσουν τους χρήστες να εισάγουν τα στοιχεία τους σε κακόβουλους ιστότοπους. Οι εφαρμογές πρέπει να περιλαμβάνουν μηχανισμούς για την ανίχνευση και την αποτροπή phishing και να ειδοποιούν τους χρήστες όταν ανιχνεύονται ύποπτες δραστηριότητες.

- **A3. Replay Attack**
  Οι επιτιθέμενοι υποκλέπτουν και επαναλαμβάνουν την επικοινωνία, εκτελώντας ανεπιθύμητες ενέργειες. Αυτό μπορεί να επιτρέψει στους επιτιθέμενους να επαναλάβουν νόμιμες συναλλαγές ή ενέργειες χωρίς τη γνώση του χρήστη. Η χρήση nonce και timestamps μπορεί να αποτρέψει αυτές τις επιθέσεις, εξασφαλίζοντας ότι κάθε αίτημα είναι μοναδικό και δεν μπορεί να επαναληφθεί από επιτιθέμενους.

- **A4. Session Hijacking**

  Οι επιτιθέμενοι αποκτούν τον έλεγχο μιας ενεργής συνεδρίας χρήστη, εκμεταλλευόμενοι ευπάθειες στη διαχείριση συνεδριών. Η απόκτηση της συνεδρίας μπορεί να επιτρέψει στους επιτιθέμενους να εκτελέσουν ενέργειες ως ο νόμιμος χρήστης. Η χρήση tokens για τη διαχείριση των συνεδριών και η ανανέωση των tokens μετά από κάθε αίτημα μπορεί να μειώσει τον κίνδυνο hijacking συνεδριών.

- **A5. Masquerade Attack**

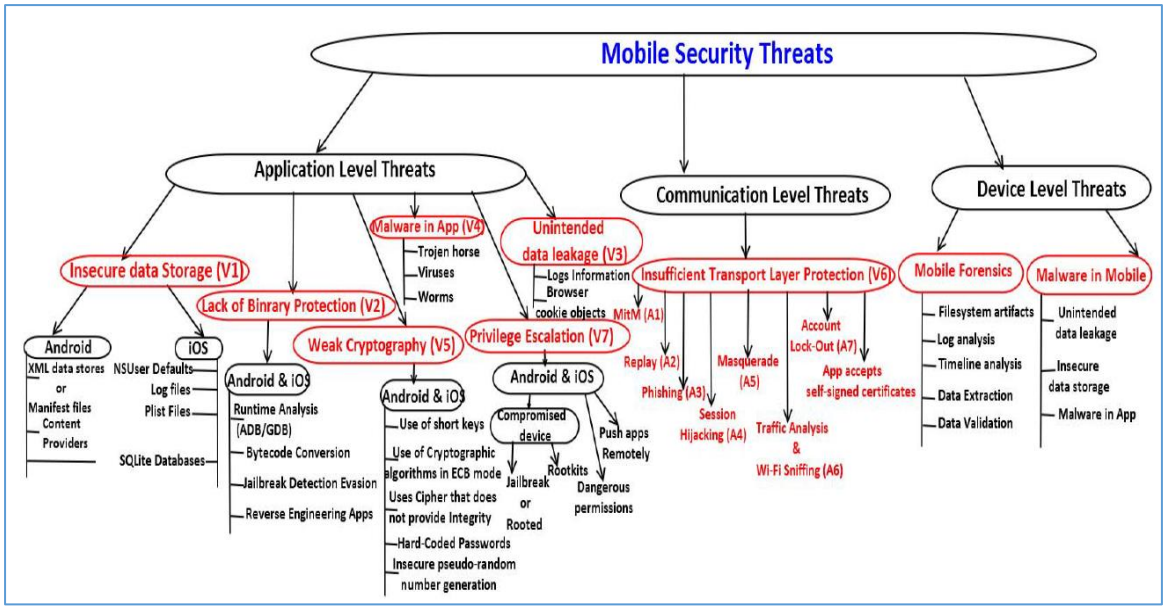
  Επιθέσεις κατά τις οποίες ο επιτιθέμενος προσποιείται ότι είναι νόμιμος χρήστης για την πρόσβαση σε ευαίσθητες πληροφορίες. Αυτές οι επιθέσεις συχνά πραγματοποιούνται μέσω της υποκλοπής πιστοποιητικών ή της εκμετάλλευσης ευπαθειών στην ταυτοποίηση χρηστών.

- **A6. Traffic Analysis and Wi-Fi Sniffing**

  Ένας επιτιθέμενος μπορεί να καταφέρει να υποκλέψει δεδομένα χρησιμοποιώντας μια συσκευή σημείου πρόσβασης (access point) και να συλλάβει τα πακέτα δεδομένων κατά τη μετάδοσή τους τα οποία είναι σχετικά με την παρακολούθηση δραστηριοτήτων στο δίκτυο, τη φυσική θέση του σημείου πρόσβασης και το πρωτόκολλο επικοινωνίας.

- **A7. Account Lock-out attack**

  Ως μέτρο ασφαλείας, οι περισσότεροι πάροχοι χρηματοοικονομικών υπηρεσιών περιορίζουν τον αριθμό των προσπαθειών σύνδεσης από τους χρήστες. Μετά από έναν συγκεκριμένο αριθμό προσπαθειών εισόδου με λάθος κωδικό πρόσβασης, ο λογαριασμός χρήστη κλειδώνει στον διακομιστή. Ένας επιτιθέμενος μπορεί να εκμεταλλευτεί αυτόν τον μηχανισμό ασφαλείας πραγματοποιώντας πολλές προσπάθειες σύνδεσης με λάθος κωδικό πρόσβασης για έναν συγκεκριμένο λογαριασμό χρήστη, μέχρι να επιτευχθεί επίθεση αποκλεισμού λογαριασμού.



Εικόνα 61. A Typical threat classification model for MBAs in context

4.3.2 Security Testing Framework

Το Penetration Testing (Pentesting) είναι μια μεθοδολογία ελέγχου ασφαλείας εφαρμογών για τον εντοπισμό κενών ασφαλείας που δεν είναι εμφανή με την πρώτη ματιά. Σκεφτείτε το σαν μια προσομοίωση κυβερνοεπίθεσης σε ελεγχόμενο περιβάλλον, με στόχο να βρεθούν αδυναμίες πριν τις εκμεταλλευτούν κακόβουλοι χρήστες. Το Static και το Dynamic analysis βοηθούν στο εντοπισμό κενών ασφαλείας τεστάροντας τις κινητές εφαρμογές.

4.3.2.1 Static Analysis

Εξετάζει τον κώδικα της εφαρμογής για να εντοπίσει πιθανά προβλήματα ασφαλείας, όπως χρήση μη ασφαλών λειτουργιών ή αδυναμίες στη διαχείριση δεδομένων. Στην περίπτωση των **Android MBA**, η στατική ανάλυση εστιάζει στο αρχείο APK της εφαρμογής.

Η στατική ανάλυση εξετάζει τη δομή του κώδικα μιας εφαρμογής για να προβλέψει την πιθανή συμπεριφορά της. Θεωρείται συντηρητική και αξιόπιστη μέθοδος, καθώς δεν απαιτεί την εκτέλεση της εφαρμογής. Στην περίπτωση των Android MBA, η στατική ανάλυση επικεντρώνεται κυρίως στα δεδομένα του αρχείου APK, το οποίο περιλαμβάνει:

- Το αρχείο εκδήλωσης (manifest file): AndroidManifest.xml
- Τον μεταγλωττισμένο κώδικα από την διαδικασία της ανάστροφης μηχανικής (reverse engineering) των αρχείων classes.dex

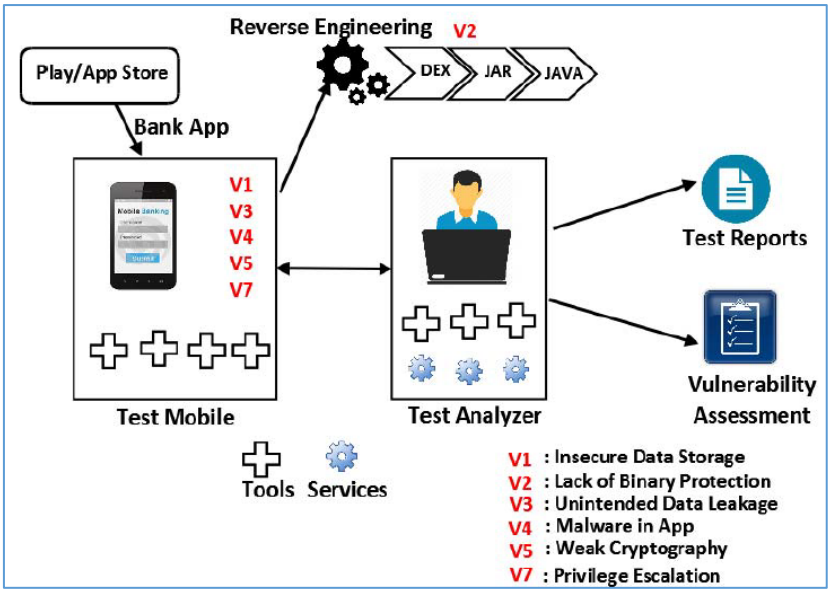
Στόχος της στατικής ανάλυσης είναι:

- ✓ Να εντοπίσει μη ασφαλείς λειτουργίες API που χρησιμοποιεί η εφαρμογή.
- ✓ Να εξετάσει τη ροή των πληροφοριών μέσα στον κώδικα για να ανακαλύψει πιθανώς επικίνδυνο χειρισμό των δεδομένων εισόδου της εφαρμογής.
- ✓ Η διεξαγωγή στατικών ελέγχων σε μια συσκευή Android μπορεί να γίνει με διάφορα εργαλεία και υπηρεσίες, τα οποία παρουσιάζονται στην Εικόνα 53.

Για να πραγματοποιηθεί στατική ανάλυση, απαιτείται αρχικά η εγκατάσταση του αρχείου APK στη συσκευή Android. Αυτό μπορεί να γίνει με δύο τρόπους:

1) Χρησιμοποιώντας την εντολή "adb install filename.apk" μέσω της Android Debug Bridge (ADB).
2) Απευθείας από το Google Play Store.

Η στατική ανάλυση σε εφαρμογές για κινητές συσκευές **iOS MBA** απαιτεί κάποια πρόσθετα βήματα σε σχέση με τις Android εφαρμογές.



Εικόνα 62. Testing Process of Static Analysis

Πριν ξεκινήσει η στατική ανάλυση, χρειάζεται το περιβάλλον δοκιμών για τις εφαρμογές iOS. Αυτό περιλαμβάνει και τη διαδικασία του jailbreak. Το jailbreak είναι μια διαδικασία που εκμεταλλεύεται ευπάθειες στο λειτουργικό σύστημα iOS και επιτρέπει την απόκτηση δικαιωμάτων διαχειριστή (root access) στη συσκευή.

Για να πραγματοποιηθεί μια ολοκληρωμένη στατική ανάλυση σε μια εφαρμογή iOS MBA, χρειάζεται πρόσβαση σε όλα τα δεδομένα της συσκευής. Αυτό περιλαμβάνει δεδομένα που είναι αποθηκευμένα στην κάρτα μνήμης (SD card) αλλά και δεδομένα που αποστέλλονται μέσω του δικτύου. Δυστυχώς, το iOS περιορίζει την πρόσβαση σε αυτά τα δεδομένα για λόγους ασφαλείας. Το jailbreak "ξεκλειδώνει" αυτήν την πρόσβαση, επιτρέποντας στον αναλυτή να εξετάσει πλήρως την εφαρμογή. Το jailbreak μπορεί να επηρεάσει την σταθερότητα και την ασφάλεια της συσκευής. Συνιστάται να γίνεται σε ξεχωριστή συσκευή που δεν χρησιμοποιείται για καθημερινές εργασίες.

Name of the device	Category of Security Testing	List of software	Platform	Purpose of Testing	Vulnerabilities
Test Mobiles:	**Application Level Security**	Drozer [2]	Android	Applications, Providers etc.,	V1-V3, V7
1. SAMSUNG GalaxyS2 (Rooted)		Virus-Total [5]	Android	Malware in App	V1, V4
2. iPhone 4s (Jailbroken device)		Apktool analyzer [3]	Android	Receivers, Services etc.,	V2-V3
3. iPhone 6s (Non-Jailbroken)		Dex2jar [28]	Android	Mobile decryption, unpacking & conversion	V1-V2
Access Point (AP):		Clutch [29]	iOS	Mobile decryption, unpacking & conversion	V5
1. CISCO-LinksysPUUU0M300147		baksmali [30]	Android	Static binary analysis: disassembly, decompilation	V2
BurpSuite Hosts:		Keychain Dumper [37]	iOS/Mac OS	App reverse engineering tools	V1-V2
1. HP ProBook 4540s (Android)		class-dump-z [23]	iOS/Mac OS	Static binary analysis: information dumping	V1-V2
2. Macbook Pro A1278 (iOS)		Introspy-Android [27]	Android	Dynamic binary analysis: debugging, tracing	V7
		Introspy-iOS [26]	iOS	Dynamic binary analysis: debugging, tracing	V7
		Cydia Substrate [24]	Android/iOS	Runtime manipulation: code injection, patching	V1, V3
		Cycript [25]	iOS/Mac OS	Runtime manipulation: method swizzling	V5-V6
		idb tool [33]	iOS/Mac OS	Exploit run-time vulnerabilities in iOS apps	V1-V3, V5-V7
		SQLite browser [34]	Android/iOS/Mac OS	Exploit database vulnerabilities in Andrid &iOS apps	V1, V3
		Xcode [35]	iOS/Mac OS	Detection of vulnerabilities in plist, SQL database	V1, V3
		FindBugs [4]	Android	Permissions	V1, V7
	Communication Level Security	BurpSuite V1.7.0 [21]	iOS/Android	Interception of network	V1-V7
		Wireshark [22]	iOS/Android	Packet analysis	V1-V7
		Connectify Hotspot		HTTP proxy	
	Device Level Security	Andriller [20]	Android	Android forensic tool	V1, V3, V5
		BlackBag Blacklight [36]	iOS/Android	Data analysis forensic toolkit	V1, V5
		iPhone Backup Unlocker [38]	iOS	Analyze an iDevice encrypted backup	V1, V5
		Encase forensics V7 [55]	Android/iOS	Log file and event log analysis	V1, V5
		Slueth Kit+Autopsy Browser [56]	Android/iOS	Efficiently analyze hard drives and smart phones.	V1, V5

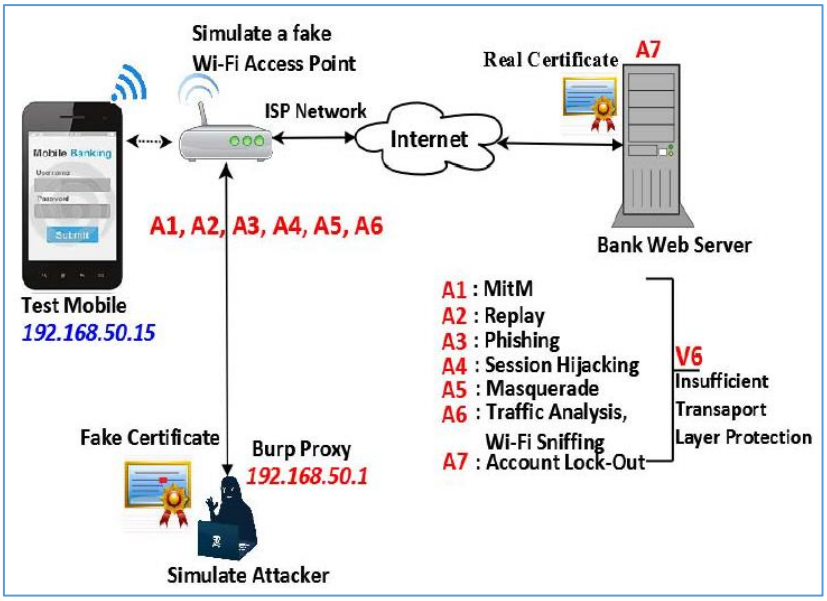
Εικόνα 63. List of penetration testing tools, software's, and devices used for our demonstration of vulnerability detection

4.3.2.2 Dynamic Analysis

Για να πραγματοποιηθεί προσομοίωση επίθεσης MitM (Man-in-the-Middle) κατά τη διάρκεια της δυναμικής ανάλυσης μιας εφαρμογής τραπεζικής για κινητές συσκευές, χρησιμοποιήθηκε ένα περιβάλλον δοκιμών που αποτελείται από τέσσερις συσκευές:

1) Ένας φορητός υπολογιστής HP που λειτουργεί ως ο κατεστραμμένος σημείο πρόσβασης (access point).
2) Ένα ασύρματο σημείο πρόσβασης CISCO Linksys PUUU0M300147.
3) Ένα smartphone Samsung Galaxy GT-19100LKAINU με διπύρηνο επεξεργαστή 1.2 GHz, 1 GB RAM και λειτουργικό σύστημα Android 4.1.2 (Jelly Bean).
4) Ένας διακομιστής web της τράπεζας για την υλοποίηση της επίθεσης MitM.

Σε αυτό το σενάριο δοκιμής δυναμικής ανάλυσης, ο δοκιμαστής μιμείται έναν πραγματικό επιτιθέμενο και στοχεύει τα θύματα και τους διακομιστές web. Το σενάριο δοκιμής απεικονίζεται στο Σχήμα 55. Πρόκειται για επίθεση MitM που χρησιμοποιεί το Burp proxy (192.168.50.1) του BurpSuite.



Εικόνα 64. Testing Process of Dynamic Analysis

Ο επιτιθέμενος δημιουργεί ένα ψεύτικο σημείο πρόσβασης Wi-Fi και όταν ο χρήστης του κινητού τηλεφώνου (192.168.50.15) συνδεθεί στο διαδίκτυο μέσω αυτού του σημείου, οποιαδήποτε επικοινωνία δικτύου μεταξύ της εφαρμογής MBA και του αντίστοιχου διακομιστή της τράπεζας θα περάσει πλέον μέσα από το Burp Proxy. Έτσι, ο υπολογιστής στον οποίο εκτελείται το BurpSuite λειτουργεί ως επιτιθέμενος MitM. Το Burp Proxy μπορεί να δημιουργήσει ένα μη έγκυρο πιστοποιητικό (self-signed certificate). Αυτό το ψεύτικο πιστοποιητικό αποθηκεύεται στο χώρο χρήστη (user space) αντί για το χώρο διαχειριστή (root space) του χώρου αποθήκευσης κλειδιών της κινητής συσκευής, προκειμένου να μιμηθεί ένα πραγματικό σενάριο επίθεσης, καθώς δεν απαιτεί δικαιώματα διαχειριστή.

Εάν μια εφαρμογή τραπεζικής προσπαθήσει να δημιουργήσει μια σύνδεση HTTPS με τον αντίστοιχο διακομιστή, το αίτημα πηγαίνει στο Burp Proxy και αυτό στέλνει το δικό του αυτό-δημιουργημένο πιστοποιητικό στην εφαρμογή. Επίσης, το Burp Proxy ζητά από τον διακομιστή να δημιουργήσει σύνδεση HTTPS και λαμβάνει το πραγματικό πιστοποιητικό από τον διακομιστή. Τελικά, δημιουργεί ένα ασφαλές κανάλι μεταξύ του ίδιου και του διακομιστή. Έτσι, δημιουργούνται δύο διαφορετικά ασφαλή κανάλια: ένα μεταξύ της κινητής συσκευής και του Burp Proxy και ένα μεταξύ του Burp Proxy και του διακομιστή. Αυτή η διαμόρφωση είναι δυνατή μόνο όταν ο λήπτης δεν ελέγχει την εγκυρότητα του πιστοποιητικού που λαμβάνει. Με αυτόν τον τρόπο, οποιαδήποτε κίνηση που δημιουργείται από μια εφαρμογή τραπεζικής που εκτελείται στην κινητή συσκευή μπορεί να διαβαστεί και να τροποποιηθεί στο Burp Proxy και στη συνέχεια να προωθηθεί στον διακομιστή και αντίστροφα.

4.3.3 Case Study

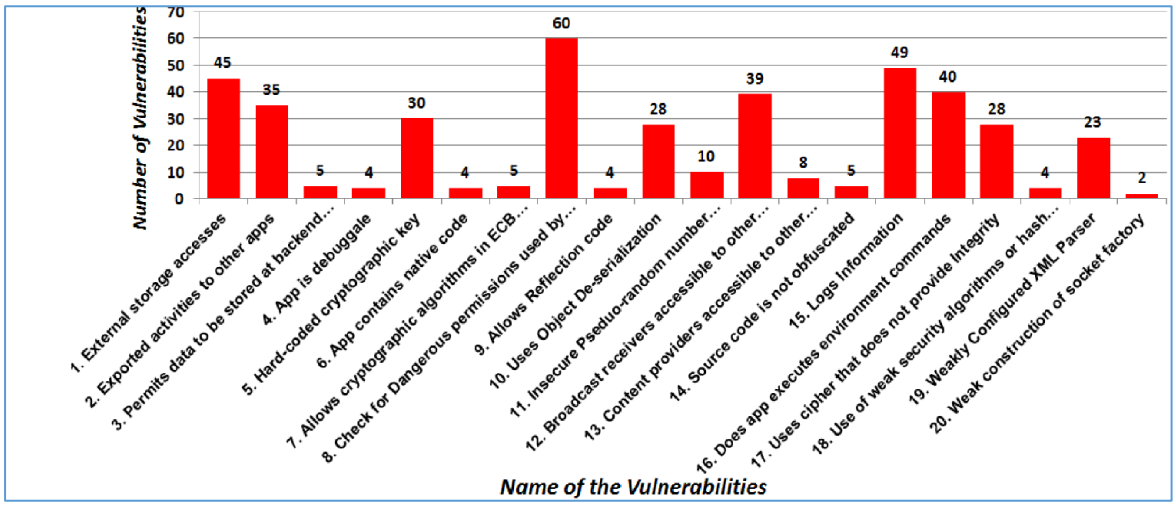
Για την αξιολόγηση της ασφάλειας εφαρμογών mobile banking, επιλέχθηκαν δείγμα 8 εφαρμογών (5 Android και 3 iOS) που χρησιμοποιούνται από δημόσιες τράπεζες στην Ινδία. Οι πραγματικοί συνδυασμοί τραπεζών και προγραμματιστών (ανάδοχοι D1, D2 κ.ο.κ.) δεν αποκαλύπτονται για λόγους ασφαλείας και φήμης.

Bank_App	Platform	No. of customers downloaded
D1-Bank_1	Android	10,000,000
D2-Bank_2	Android	1,000,000
D3-Bank_3	Android	5,000,000
D3-Bank_4	Android	500,000
D4-Bank_5	Android	500,000
D1-iBank_1	iOS	5,000,000
D2-iBank_2	iOS	500,000
D3-iBank_3	iOS	100,000

Εικόνα 65. Bank Apps

4.3.4 Results and Observations

Ύστερα από στατική ανάλυση των 5 Android MBAs, προκύπτουν οι παρακάτω ευπάθειες όπως φαίνονται στην παρακάτω εικόνα.



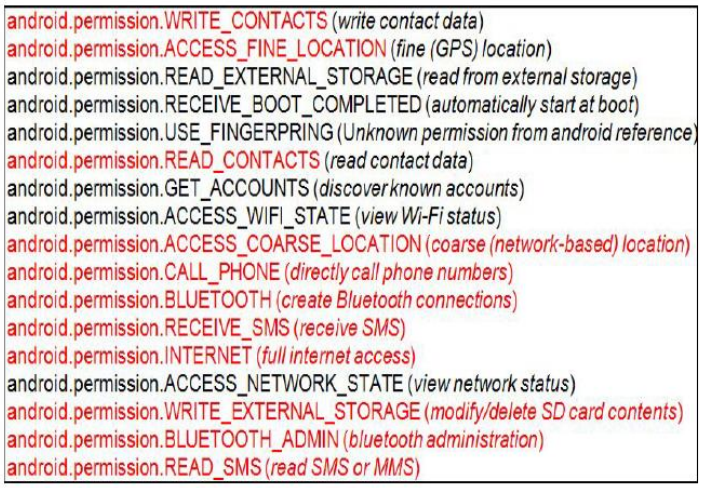
Εικόνα 66. Ευπάθειες που εντοπίστηκαν σε εφαρμογές Android MBAs

4.3.4.1 Static Analysis for Android MBAs

- **Αποθήκευση σε εξωτερικό χώρο**
  - Πρόσβαση στον εξωτερικό αποθηκευτικό χώρο (SD card).
  - Κίνδυνος για αποθήκευση ευαίσθητων πληροφοριών.
- **Εξαγόμενες δραστηριότητες σε άλλες εφαρμογές**
  - Εφαρμογές που εκκινούνται χωρίς άδειες και παρέχουν πρόσβαση σε εμπιστευτικές πληροφορίες.
- **Επιτρέπεται αποθήκευση και ανάκτηση δεδομένων σε βάσεις δεδομένων**
  - Κίνδυνος απόκτησης πρόσβασης σε ευαίσθητα δεδομένα από κακόβουλους χρήστες.
- **Η εφαρμογή είναι Debuggable**
  - Προστασία κατά της αναστροφής μηχανικής και εκτέλεσης αυθαίρετου κώδικα.
- **Hard-coded κρυπτογραφικό κλειδί**
  - Κίνδυνος αποκάλυψης του κλειδιού και συμβιβασμός ασφάλειας.
- **Περιέχει native code**
  - Ευπάθεια σε buffer overflows και άλλα σφάλματα μνήμης.
- **Χρήση αλγορίθμων κρυπτογράφησης σε ECB mode**
  - Μη ασφαλής τρόπος κρυπτογράφησης.
- **Επικίνδυνα δικαιώματα**
  - Δικαιώματα που επιτρέπουν πρόσβαση σε ευαίσθητα δεδομένα.
- **Χρήση reflection code**
  - Χρήση για επιθέσεις και δυσδιάκριτη κακόβουλη συμπεριφορά.
- **Deserialization αντικειμένων**
  - Πιθανές ευπάθειες από μη αξιόπιστες πηγές.
- **Ανασφαλής γεννήτρια ψευδοτυχαίων αριθμών**
  - Μη ασφαλής για κρυπτογραφικούς σκοπούς.
- **Δέκτες broadcast προσβάσιμοι από άλλες εφαρμογές**
  - Επιθέσεις με εκτέλεση αυθαίρετου κώδικα.
- **Πάροχοι περιεχομένου προσβάσιμοι από άλλες εφαρμογές και SQL Injection**
  - Προστασία από SQL injection.
- **Ο κώδικας δεν είναι συγκεχυμένος**
  - Ευκολία αναστροφής και κακόβουλης τροποποίησης.
- **Καταγραφή πληροφοριών**
  - Κίνδυνος διαρροής ευαίσθητων πληροφοριών.
- **Εκτέλεση εντολών περιβάλλοντος**
  - Κίνδυνος από μη κατάλληλη απολύμανση εισόδων.
- **Χρήση κρυπτογραφικών αλγορίθμων χωρίς παροχή integrity**
  - Κίνδυνος παραβίασης δεδομένων.
- **Χρήση αδύναμων αλγορίθμων ή hash functions**
  - Κίνδυνος από MD4, MD5, SHA1, RC4.

- **Αδύναμη ρύθμιση XML parser**
  - Ευπάθεια σε XXE και DoS επιθέσεις.
- **Αδύναμη κατασκευή socket factory**
  - Ευπάθεια σε Man-in-the-Middle επιθέσεις.

(a) Vulnerabilities are identified on the Attack Surface



(b) List of permissions used by the app

Εικόνα 67. Some examples of vulnerabilities detected by static analysis

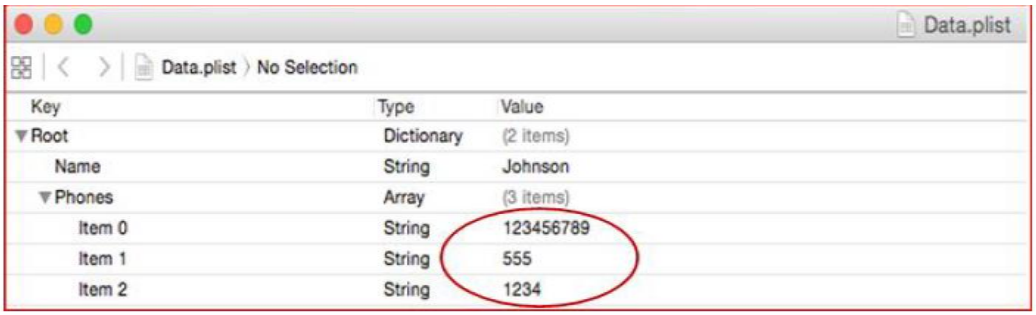
4.3.4.2 Static Analysis for iOS MBAs

Για εφαρμογές mobile banking στο iOS, δημιουργείται ένα εργαστηριακό περιβάλλον για τη διενέργεια ελέγχου διείσδυσης. Εδώ εξετάζεται την ανασφαλή αποθήκευση δεδομένων, η οποία αποτελεί έναν από τους κορυφαίους 10 κινδύνους του OWASP mobile security. Για τις συσκευές iOS, υπάρχουν διαφορετικές μορφές αποθήκευσης τοπικών δεδομένων όπως:

1. Core Data
2. XML και plist
3. Η κλάση NSUserDefaults
4. Δεδομένα Keychain
5. Αρχεία καταγραφής
6. Αρχεία SQLite

D1-iBank 1: Δοκιμάστηκαν τα αρχεία plist, τα οποία χρησιμοποιούνται για την αποθήκευση τυπικών δεδομένων, όπως αριθμοί, ακέραιοι και συμβολοσειρές. Μετά

την εισαγωγή των στοιχείων χρήστη, τα αρχεία της εφαρμογής μεταφέρθηκαν από το iOS στην Mac OS μέσω SFTP. Όταν άνοιξαν το αρχείο Data.plist, παρατηρήθηκε ότι τα εμπιστευτικά στοιχεία ήταν σε μορφή απλού κειμένου.



Εικόνα 68. User's credentials are in plain-text in plist files

Εικόνα 69. User's confidential data in plain-text

D1-iBank 2: Αναλύθηκαν βάσεις δεδομένων SQLite και NSUserDefaults. Παρόλο που οι βάσεις δεδομένων SQLite συνήθως είναι κρυπτογραφημένες, σε αυτή την περίπτωση οι πληροφορίες αποθηκεύτηκαν σε μη κρυπτογραφημένα αρχεία SQLite, καθιστώντας τα διαπιστευτήρια (όνομα χρήστη, κωδικός πρόσβασης) εύκολα προσβάσιμα. Στο NSUserDefaults, οι ευαίσθητες πληροφορίες αποθηκεύτηκαν επίσης σε απλό κείμενο.

4.3.4.3 Dynamic Analysis of Android and iOS MBAs

D1-Bank 1: Αυτή η εφαρμογή mobile banking απαιτεί από τον χρήστη να αποκτήσει userID και κωδικό πρόσβασης για την αρχική σύνδεση. Λόγω κακής υλοποίησης SSL/TLS, ο χρήστης μπορεί να γίνει εύκολα θύμα επίθεσης MitM. Οι παρατηρήσεις δείχνουν ότι το userID και ο κωδικός πρόσβασης δεν είναι κρυπτογραφημένα και τα δεδομένα αιτήματος σε μορφή JSON είναι ευάλωτα .

D2-Bank 2: Αυτή η εφαρμογή απαιτεί την εγγραφή του κινητού αριθμού του πελάτη και αποστολή OTP για συναλλαγές. Χρησιμοποιεί το πρωτόκολλο HTTP, το οποίο την καθιστά ευάλωτη σε επιθέσεις phishing και MitM. Ο επιτιθέμενος μπορεί να τροποποιήσει τις απαντήσεις από τον διακομιστή της τράπεζας και να τις προωθήσει στην εφαρμογή, επιτρέποντας παραποιημένες συναλλαγές.

```
POST /api/login HTTP/1.1

Content-Type: application/json

Content-Type: application/json; charset=utf-8

User-Agent: Dalvik/2.1.0 (Linux; U;  Android 5.1.1; SM-J200G Build/LMY47X)

Host: npatracker.D1-Bank_1

Connection: close

Content-Length: 40

Customer Credentials Details:

{

"userId" : "admin",

"password": "admin123"

}
```

Εικόνα 70. User ID & Password is shown as plain-text

Original Balance Request	*Fake Balance Request*
POST http://mobile.D2-Bank_2/gprs/HTTP/1/1 Content-Type: text/plain User-Agent: Dalvik/1.6.0 (Linux; U; Android 4.0.3; GT-I9100 Build/ML74K) Host mobile: D2-Bank_2 Connection: Close Accept-Encoding: gzip Content-Length: 63 MBSFTV0111 Bcv136,sLNDqzlvbE6WlaCDn3VDY0YZi3oDBaKfUUqUpjrvix0=	POST http://mobile.D2-Bank_2/gprs/HTTP/1/1 Content-Type: text/plain User-Agent: Dalvik/1.6.0 (Linux; U; Android 4.0.3; GT-I9100 Build/ML74K) Host mobile: D2-Bank_2 Connection: Close Accept-Encoding: gzip Content-Length: 63 MBSFTV0111 Bcv136,sLNDqzlvbE6WlaCDn3VDY0YZi3oDBaKfUUqUpjrvix0=

Εικόνα 71. Balance Enquiry Request Comparison

D3-Bank 3: Η εφαρμογή απαιτεί ισχυρό cust id και κωδικό πρόσβασης. Ο διακομιστής της τράπεζας στέλνει OTP σε απλό κείμενο, επιτρέποντας επιθέσεις MitM και υποκλοπής συνεδρίας. Αυτές οι επιθέσεις είναι δυνατές επειδή ο διακομιστής αποδέχεται ψεύτικα πιστοποιητικά.

```
POST/D3-BANK_3/servelt/NativeServlet01?ts=164672 HTTP/1.1
Content-Length: 164
Content-Type: application/x-www-form-urlencoded
Host: D3-BANK_3
Connection: close
Expect: 100-continue
Cookie: JSESSIONID=E6FB22137117580EED05A723C558ED45; LS
NONCEID=41e7a68b7e999af42f274724e9e2d343e28a0fb8dbdb1fe13fbf0a5868178872
Cookie2: $Version=1
BUILD_VERSION=14& USER_ID=215075231
&MOBILE_PIN=&FRM_OS=ANDROID&MOBILE_NUMBER=&METHOD_NAME=validateOTP&IMEI_NUM
BER=353327052273281&UNO=04785781714214074375&OTP=184176
```

Εικόνα 72. OTP is in plain-text, not encrypted

D4-Bank 5: Η εφαρμογή είναι ευάλωτη σε επίθεση κλειδώματος λογαριασμού στην πίσω πλευρά του διακομιστή, αλλά δεν μπορούσαμε να εκτελέσουμε επίθεση πρόβλεψης συνεδρίας. Ο διακομιστής δεν επαληθεύει την ακεραιότητα των δεδομένων, επιτρέποντας την τροποποίηση του κωδικού και το κλείδωμα του λογαριασμού παρά την εισαγωγή σωστών στοιχείων σύνδεσης.

4.3.4.4 Compliance of MBAs to the OWASP

Συνοψίζοντας τα ευρήματα και χαρτογραφώντας τις ευπάθειες που εντοπίστηκαν διαπιστώνουμε ότι ανιχνεύθηκαν 7 από τις κορυφαίες 10 ευπάθειες που περιέχονται στη λίστα OWASP mobile security.

- M1: Αδύναμοι Έλεγχοι στην Πλευρά του Διακομιστή
- M2: Ανασφαλής Αποθήκευση Δεδομένων
- M3: Ανεπαρκής Προστασία του Επιπέδου Μεταφοράς
- M4: Αθέλητη Διαρροή Δεδομένων
- M5: Κακή Εξουσιοδότηση και Αυθεντικοποίηση
- M6: Σπασμένη Κρυπτογραφία
- M7: Εισαγωγή Κώδικα στην Πλευρά του Πελάτη
- M8: Λήψη Αποφάσεων Ασφαλείας μέσω Μη Αξιόπιστων Εισόδων
- M9: Ακατάλληλος Χειρισμός Συνεδρίας
- M10: Έλλειψη Προστασίας Δυαδικού Κώδικα

Στις περισσότερες εφαρμογές mobile banking, έχει εντοπιστεί ότι το M3 είναι ένα κοινό σχεδιαστικό σφάλμα. Αυτό το σφάλμα εκθέτει τα δεδομένα ενός μεμονωμένου χρήστη και μπορεί να οδηγήσει σε κλοπή λογαριασμού. Αν ο επιτιθέμενος υποκλέψει έναν admin λογαριασμό, θα μπορούσε να εκθέσει ολόκληρο τον ιστότοπο. Η κακή εγκατάσταση SSL μπορεί επίσης να διευκολύνει επιθέσεις phishing και MitM. Οι προγραμματιστές εφαρμογών θα πρέπει να επικεντρωθούν στις πτυχές ασφαλείας κατά τη χρήση του HTTPs κατά την δημιουργία της σύνδεσης.

4.3.5 Conclusions and Future Work

Σε αυτήν την εργασία, παρουσιάστηκε ένα μοντέλο απειλών που βοηθά στη συστηματική δοκιμή και ανάλυση εφαρμογών mobile banking. Το μοντέλο αυτό βοηθά στην ανίχνευση και μετριασμό των ευπαθειών σε επίπεδο εφαρμογής και επικοινωνίας. Η παρούσα εργασία ασχολείται κυρίως με τον έλεγχο ασφάλειας για τις δύο κυρίαρχες πλατφόρμες, Android και iOS. Η εργασία αντιμετωπίζει διάφορες άγνωστες ευπάθειες στις εφαρμογές mobile banking και την υλοποίηση επιθέσεων MitM κατά τη διάρκεια δυναμικής ανάλυσης των εφαρμογών. Τα αποτελέσματα δείχνουν ότι η επίθεση MitM είναι εύκολα δυνατή, ακόμα και με τη χρήση του πρωτοκόλλου HTTPs, λόγω ανεπαρκούς προστασίας του επιπέδου μεταφοράς που οδηγεί σε κακή υλοποίηση του πλαισίου SSL στην πλευρά του διακομιστή της τράπεζας και στις εφαρμογές mobile.

Διεξάχθηκαν δοκιμές ασφάλειας σε rooted, jailbroken και μη jailbroken συσκευές, και εντοπίστηκαν κοινές ευπάθειες.

Ενώ προηγούμενες εργασίες προσδιόρισαν κάποιες επιθέσεις, δεν παρείχαν τεχνικές μετριασμού των ευπαθειών. Κάθε οργανισμός, χρηματοπιστωτικό ίδρυμα, τράπεζα και εργαστήριο τρίτων πρέπει να διενεργεί αξιολόγηση ευπαθειών σε βάθος, μία ή δύο φορές το χρόνο, για ανίχνευση ευπαθειών και εκμεταλλεύσεων στις εφαρμογές mobile banking. Αυτή η εργασία ασχολείται με τις πτυχές ασφαλείας για την ανάπτυξη εφαρμογών mobile banking.

Μελλοντική εργασία περιλαμβάνει εστίαση σε άλλες κινητές συσκευές που λειτουργούν σε άλλες πλατφόρμες. Ωστόσο, απαιτείται μια λεπτομερής μελέτη των απειλών ασφαλείας, η οποία απαιτεί πραγματικά διαπιστευτήρια χρήστη από την πλευρά της τράπεζας και ως εκ τούτου θα πραγματοποιηθεί στο μέλλον.

5. ΣΥΜΠΕΡΑΣΜΑΤΑ ΚΑΙ ΜΕΛΛΟΝΤΙΚΕΣ ΠΡΟΤΑΣΕΙΣ

Η παρούσα πτυχιακή εργασία εστιάζει στην αξιολόγηση ευπαθειών (Vulnerability Assessment) και στις δοκιμές διείσδυσης (Penetration Testing) σε κινητές πλατφόρμες Android και iOS, καθώς και στις εφαρμογές τους. Η ανάλυση επικεντρώθηκε στην εφαρμογή μεθοδολογιών όπως η NIST-SP 800-115, το Penetration Testing Execution Standard (PTES) και το OWASP Mobile Security Testing Guide (MSTG), οι οποίες ανέδειξαν κρίσιμα σημεία που μπορούν να εκμεταλλευτούν κακόβουλοι χρήστες. Από την έρευνα σε μελέτες περίπτωσης για δοκιμές διείσδυσης και αξιολόγηση ευπαθειών σε εφαρμογές κινητής τραπεζικής για τις πλατφόρμες Android και iOS. προέκυψαν τα εξής βασικά συμπεράσματα:

1. Ασφαλής Αποθήκευση Δεδομένων: Οι περισσότερες ευπάθειες σχετίζονται με την ανασφαλή αποθήκευση ευαίσθητων δεδομένων σε κινητές συσκευές, γεγονός που καθιστά τα δεδομένα ευάλωτα σε επιθέσεις.

2. Έλεγχοι Ταυτότητας και Εξουσιοδότησης: Ανεπαρκείς έλεγχοι ταυτότητας και εξουσιοδότησης μπορούν να επιτρέψουν μη εξουσιοδοτημένη πρόσβαση σε προσωπικά δεδομένα και λειτουργίες.

3. Ευπάθειες Δικτύου: Ελλείψεις στην ασφάλεια των δικτύων επικοινωνίας μπορούν να επιτρέψουν επιθέσεις τύπου man-in-the-middle, διακυβεύοντας την ακεραιότητα των δεδομένων που μεταφέρονται.

Η εργασία προτείνει λύσεις και μέτρα πρόληψης όπως η χρήση κρυπτογράφησης, η εφαρμογή αυστηρών πολιτικών διαχείρισης κωδικών και η εκπαίδευση των χρηστών στην αναγνώριση και αποφυγή κινδύνων. Ωστόσο, είναι αναγκαία η συνεχής αναθεώρηση και βελτίωση των μεθόδων ασφαλείας για να αντιμετωπίζονται οι νέες και εξελισσόμενες απειλές.

Για να αντιμετωπιστούν τα ευρήματα της παρούσας μελέτης και να βελτιωθεί η ασφάλεια των εφαρμογών κινητής τραπεζικής, προτείνονται οι ακόλουθες κατευθύνσεις για μελλοντική έρευνα και ανάπτυξη:

1. Ενσωμάτωση Τεχνολογιών Μηχανικής Μάθησης και Τεχνητής Νοημοσύνης:

- Χρήση τεχνικών μηχανικής μάθησης για την ανίχνευση ανωμαλιών στη χρήση των εφαρμογών και την πρόληψη επιθέσεων σε πραγματικό χρόνο.

- Ανάπτυξη μοντέλων πρόβλεψης που αναγνωρίζουν νέους τύπους επιθέσεων βασισμένων σε μοτίβα χρήσης και δεδομένα ιστορικών επιθέσεων.

2. Ανάπτυξη Προηγμένων Κρυπτογραφικών Μεθόδων

- Εξερεύνηση και εφαρμογή νέων κρυπτογραφικών τεχνικών που προσφέρουν μεγαλύτερη ασφάλεια στις μεταφορές δεδομένων.

- Χρήση τεχνολογιών όπως το Homomorphic Encryption για την επεξεργασία κρυπτογραφημένων δεδομένων χωρίς την ανάγκη αποκρυπτογράφησης.

3. Ενίσχυση της Ασφάλειας στην Επικοινωνία

- Ανάπτυξη και εφαρμογή πρωτοκόλλων ασφαλούς επικοινωνίας που αποτρέπουν επιθέσεις τύπου man-in-the-middle.

- Υιοθέτηση τεχνολογιών όπως το HTTPS Strict Transport Security (HSTS) για την εξασφάλιση της ασφάλειας των δικτυακών επικοινωνιών.

4. Εκπαίδευση και Ευαισθητοποίηση Χρηστών

- Δημιουργία προγραμμάτων εκπαίδευσης για τους χρήστες σχετικά με τους κινδύνους και τις πρακτικές ασφαλείας που πρέπει να ακολουθούν.

- Ανάπτυξη εργαλείων που βοηθούν τους χρήστες να κατανοούν και να αξιολογούν την ασφάλεια των εφαρμογών που χρησιμοποιούν.

5. Διερεύνηση Νέων Τεχνολογιών Ασφάλειας

- Εξέταση της εφαρμογής τεχνολογιών blockchain για την ενίσχυση της ασφάλειας και της διαφάνειας στις τραπεζικές συναλλαγές.

- Ενσωμάτωση βιομετρικών τεχνολογιών για την αυθεντικοποίηση χρηστών, όπως η αναγνώριση προσώπου και δακτυλικών αποτυπωμάτων.

6. Διεξαγωγή Τακτικών Ελέγχων Ασφαλείας

- Συνεχής αναθεώρηση και δοκιμή των εφαρμογών για νέες ευπάθειες.

- Υιοθέτηση της πρακτικής του continuous integration/continuous deployment (CI/CD) με ενσωματωμένες δοκιμές ασφαλείας.

Η υλοποίηση αυτών των προτάσεων μπορεί να συμβάλλει σημαντικά στη βελτίωση της ασφάλειας των εφαρμογών κινητής τραπεζικής, προστατεύοντας τόσο τους χρήστες όσο και τα χρηματοπιστωτικά ιδρύματα από μελλοντικές απειλές και επιθέσεις. Επιπλέον, η ενσωμάτωση τεχνητής νοημοσύνης μπορεί να φέρει επανάσταση στον τομέα της ασφάλειας, επιτρέποντας την ανίχνευση και αντιμετώπιση απειλών με μεγαλύτερη ακρίβεια και ταχύτητα.

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] "What is penetration testing? (Explained by a real hacker)," 25 October 2022. [Online]. Available: https://www.hackthebox.com/blog/what-is-penetration-testing#what_is_penetration_testing_. [Accessed 10 February 2024].

[2] "Introduction/README.md#Penetration-Testing," 12 March 2020. [Online]. Available: https://github.com/OWASP/www-project-web-security-testing-guide. [Accessed 10 February 10].

[3] "NIST SP 800-115 AND PENETRATION TESTING," [Online]. Available: https://www.softwaresecured.com/post/nist-sp-800-115-and-penetration-testing. [Accessed 15 February 2024].

[4] "PTES Technical Guideline," 16 August 2014. [Online]. Available: http://www.pentest-standard.org/index.php/Main_Page. [Accessed 15 February 2024].

[5] "OWASP MASTG," [Online]. Available: https://mas.owasp.org/MASTG/. [Accessed 15 February 2024].

[6] "MITRE ATT&CKÒ: Design and," March 2020. [Online]. Available: https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf . [Accessed 15 February 2024].

[7] "OSSTMM 3 – The Open Source Security Testing Methodology Manual," 14 December 2010. [Online]. Available: https://www.isecom.org/OSSTMM.3.pdf. [Accessed 16 February 2024].

[8] "privacy-and-security," 26 February 2024. [Online]. Available: https://developer.android.com/privacy-and-security. [Accessed 1 March 2024].

[9] "Apple Platform Security," May 2022. [Online]. Available: https://support.apple.com/el-gr/guide/security/welcome/web. [Accessed 17 February 2024].

[10] "what-is-kali-linux," 23 November 2023. [Online]. Available: https://www.kali.org/docs/introduction/what-is-kali-linux/. [Accessed 8 April 2024].

[11] "Nmap Description," [Online]. Available: https://nmap.org/book/man.html#man-description. [Accessed 5 April 2024].

[12] "what-is-maltego," 5 January 2024. [Online]. Available: https://docs.maltego.com/support/solutions/articles/15000019166-what-is-maltego-. [Accessed 8 April 2024].

[13] "Chapter 1. Introduction," [Online]. Available: https://www.wireshark.org/docs/wsug_html_chunked/ChapterIntroduction.html#ChIntroWhatIs. [Accessed 9 April 2024].

[14] "What is NESSUS and How Does it Work?," [Online]. Available: https://www.itperfection.com/network-security/network-monitoring/what-is-nessus-and-how-does-it-work-network-munitoring-vulnerabilit-scaning-security-data-windows-unix-linux/. [Accessed 8 April 2024].

[15] "Burp Suite documentation: desktop editions," 1 March 2024. [Online]. Available: https://portswigger.net/burp/documentation/desktop. [Accessed 8 April 2024].

[16] "ATTACKING WINDOWS 10 USING MIMIKATZ," 31 March 2021. [Online]. Available: https://shahrukhiqbal24.medium.com/attacking-windows-10-using-mimikatz-824c73eb9f3d. [Accessed 9 April 2024].

[17] "MobSF: Open-source security research platform for mobile apps," 24 March 2024. [Online]. Available: https://www.helpnetsecurity.com/2024/03/14/mobsf-open-source-mobile-security-framework/. [Accessed 8 April 2024].

[18] "Getting Started," [Online]. Available: https://www.zaproxy.org/getting-started/. [Accessed 9 April 2024].

[19] 20 July 2020. [Online]. Available: https://www.geeksforgeeks.org/kali-linux-aircrack-ng/. [Accessed 9 April 2024].

[20] "How to Use Hydra to Crack Passwords: The Complete Guide," 24 January 2024. [Online]. Available: https://www.stationx.net/how-to-use-hydra/. [Accessed 9 April 2024].

[21] "How to Use Social Engineering Toolkit(SET) – A Complete Guide," 6 April 2023. [Online]. Available: https://kalilinuxtutorials.com/social-engineering-toolkit-tutorial/. [Accessed 9 April 2024].

[22] "Bypassing MFA: A Forensic Look At Evilginx2 Phishing Kit," 20 February 2023. [Online]. Available: https://www.aon.com/cyber-solutions/aon_cyber_labs/bypassing-mfa-a-forensic-look-at-evilginx2-phishing-kit/. [Accessed 9 April 2024].

[23] [Online]. Available: https://sqlmap.org/. [Accessed 9 April 2024].

[24] "Platform architecture," [Online]. Available: https://developer.android.com/guide/platform. [Accessed 10 April 2024].

[25] "The 2023 McAfee," February 2023. [Online]. Available: https://media.mcafeeassets.com/content/dam/npcld/ecommerce/en-us/docs/reports/rp-mobile-threat-report-feb-2023.pdf. [Accessed 11 April 2024].

[26] G. Weidman, "Mobile Attack Vectors," 2014. [Online]. Available: https://repo.zenk-security.com/Magazine%20E-book/Penetration%20Testing%20-%20A%20hands-on%20introduction%20to%20Hacking.pdf. [Accessed 24 Apr 2024].

[27] N. Elenkov, "Android Security Internals : An In-Depth Guide to Android's Security Architecture," 2015. [Online]. Available: https://repo.zenk-security.com/Magazine%20E-book/Android_Security_Internals-An_In-Depth_Guide_to_Android_s_Security_Architecture.pdf. [Accessed 25 Apr 2024].