ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ATHENS UNIVERSITY OF ECONOMICS AND BUSINESS

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΜΕΤΑΠΤΥΧΙΑΚΟ ΔΙΠΛΩΜΑ ΕΙΔΙΚΕΥΣΗΣ (MSc)

στα ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

“ Mobile and Web Banking Cyber Security Threat Analysis”

Παναγιώτης Πάγκας

Α.Μ. P3341813

ΑΘΗΝΑ, Σεπτέμβριος 2020

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ


ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Ευχαριστίες

Η παρούσα εργασία αποτελεί διπλωματική εργασία στα πλαίσια του μεταπτυχιακού προγράμματος στα Πληροφοριακά Συστήματα του τμήματος Πληροφορικής του Οικονομικού Πανεπιστημίου Αθηνών. Η εργασία δεν θα ήταν δυνατό να ολοκληρωθεί χωρίς την συνεχή και ουσιαστική καθοδήγηση του επιβλέποντα καθηγητή μου Δρ. Δρίτσα Στυλιανού, τον οποίο αισθάνομαι και την υποχρέωση να ευχαριστήσω ιδιαιτέρως τόσο για την άμεση όσο και την έμμεση συνεισφορά του καθ' όλη την διάρκεια της εκπόνησης της εργασίας. Η πολύτιμη βοήθεια, η εμπιστοσύνη και η εκτίμηση που μου έδειξε αποτέλεσαν το δίαυλο προς την γνώση καθώς και την πηγή έμπνευσης και δημιουργικότητας.

Ιδιαίτερα θερμές ευχαριστίες θα ήθελα να δώσω στην οικογένεια μου τόσο για την συνεχή συμπαράσταση όσο και για την πολύτιμη στήριξη τους καθ' όλη την διάρκεια των σπουδών μου.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Περίληψη

Με την ανάπτυξη και την εξέλιξη τόσο του διαδικτύου όσο και των νέων τεχνολογιών που βρίσκουν ευρεία εφαρμογή σε αυτό, δημιουργήθηκαν νέες ευκαιρίες για τον τραπεζικό τομέα και τα χρηματοπιστωτικά ιδρύματα. Η τελευταία δεκαετία έφερε νέα τεχνολογικά επιτεύγματα, και δημιούργησε νέες δυνατότητες για τους χρήστες του διαδικτύου και της ηλεκτρονικής τραπεζικής. Όλες αυτές οι αλλαγές ήταν το έναυσμα για τη δημιουργία νέων αναγκών και απαιτήσεων που έπρεπε να ικανοποιηθούν για την ομαλή λειτουργία της κοινωνίας.

Προκειμένου να ανταποκριθούν σε αυτές τις αλλαγές, τα χρηματοπιστωτικά ιδρύματα έπρεπε να υιοθετήσουν τις νέες τεχνολογίες χρησιμοποιώντας τις δυνατότητες του διαδικτύου, ελπίζοντας ότι η εγγύηση πρωτοποριακής θέσης στον τομέα των εφαρμογών νέων τεχνολογικών μεθόδων και του Διαδικτύου μπορεί να εξασφαλίσει μια αποτελεσματική άμυνα στις κλιμακούμενες αλλαγές καθώς και ένα ανταγωνιστικό πλεονέκτημα. Όμως, η αυξημένη χρήση του web και Mobile Banking, δίνει πολλές ευκαιρίες στους κακόβουλους χρήστες και στους εγκληματίες του κυβερνοχώρου να επιτεθούν και να υποκλέψουν οικονομικά στοιχεία, να παραβιάσουν τραπεζικούς λογαριασμούς, αριθμούς πιστωτικών καρτών κτλ. Έτσι, εγείρονται πολλά ζητήματα ασφάλειας γύρω από την χρήση του web και mobile banking για ποικίλους λόγους.

Σκοπός της εργασίας είναι η μελέτη της τρέχουσας κατάστασης του web και του Mobile Banking, η καταγραφή των απειλών και των επιθέσεων τους, καθώς και η συστηματική ανάλυση αυτών. Η εργασία δομείται σε έξι βασικά κεφάλαια. Το πρώτο κεφάλαιο, εστιάζει στην τρέχουσα κατάσταση του e-banking και σε εισαγωγικά στοιχεία αναφορικά με αυτό. Το δεύτερο κεφάλαιο, παρουσιάζει την τρέχουσα κατάσταση του Web Banking, και στην συνέχεια παρουσιάζονται τα είδη των απειλών και των επιθέσεων που υφίστανται οι διαδικτυακές εφαρμογές, στις οποίες οι χρήστες έχουν πρόσβαση στο Web Banking. Στην συνέχεια, στο τρίτο κεφάλαιο, παρουσιάζονται η τρέχουσα κατάσταση του Mobile Banking, και στην συνέχεια παρουσιάζονται τα είδη των απειλών και των επιθέσεων που υφίστανται σε κινητές συσκευές, στις οποίες οι χρήστες έχουν πρόσβαση σε mobile Banking εφαρμογές. Στο τέταρτο κεφάλαιο, ορισμένα μοντέλα, σκοπός των οποίων είναι να πραγματοποιηθεί μια ανάλυση των απειλών (Threat Analysis) που παρουσιάστηκαν στα δύο προηγούμενα κεφάλαια.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Έπειτα, στο πέμπτο κεφάλαιο εξετάζονται οι μηχανισμοί ασφάλειας στο web και mobile banking. Στο έκτο κεφάλαιο, παρουσιάζονται ορισμένες από τις πιο σημαντικές κακόβουλες επιθέσεις, που έχουν συμβεί στο παρελθόν, σε πλατφόρμες και εφαρμογές E-banking καθώς και οι συνέπειες που είχαν τα χρηματοπιστωτικά ιδρύματα στα οποία έλαβαν χώρα.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Abstract

Through the development and evolution of the internet and new technologies, new opportunities have been arised for the banking sector and financial institutions. The last decade has brought new technological achievements, and created new possibilities for internet and e-banking users. All these changes were the trigger for the creation of new needs and requirements that had to be met for the smooth functioning of the society.

In order to respond to these changes, financial institutions had to adopt new technologies using the internet, hoping that securing a leading position in new technology and Internet applications could ensure an effective defense against escalating change as well as a competitive advantage. However, the increased use of the web and Mobile Banking, gives many opportunities for malicious users and cybercriminals to attack and steal financial data, breach bank accounts, credit card numbers etc. Thus, many security issues arise around the use of the web and mobile banking for a variety of reasons.

The purpose of this thesis, is to study the current state of the web and Mobile Banking, to record their threats and attacks, as well as their systematic analysis. The assignment is structured in six basic chapters. First chapter focuses on the current state of e-Banking and presents relative knowledge information. Second chapter presents the current state of Web Banking, and then presents the types of threats and attacks that exist on web applications, in which users have access to Web Banking. Then, third chapter presents the current state of Mobile Banking, and then presents the types of threats and attacks that exist on mobile devices, in which users have access to mobile Banking applications. Fourth Chapter presents some models the purpose of which is to carry out an analysis of the threats (Threat Analysis) presented in the previous two chapters. In the fifth chapter, security mechanisms, applied to the web and mobile banking are presented.

The sixth chapter presents some of the most significant malicious attacks that have occurred in the past on E-banking platforms and applications, as well as the consequences for the financial institutions in which they took place.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Πίνακας περιεχομένων

ΚΕΦΑΛΑΙΟ 1- ΕΙΣΑΓΩΓΗ 11
1.1. Οριοθέτηση Προβλήματος 11
1.2. Σκοπός της Εργασίας 13
1.3. Δομή της Εργασίας 13
ΚΕΦΑΛΑΙΟ 2- Το Web banking 15
2.1. Τι είναι το Web banking 15
2.2. Η Τρέχουσα κατάσταση του Web banking 17
2.2.1. Χρήση του Web Banking στην Ευρώπη 17
2.2.2. Πλατφόρμες και λογισμικά που χρησιμοποιούνται 19
2.3. Προκλήσεις και ζητήματα σε θέματα ασφάλειας του Web Banking 22
2.3.1. Προκλήσεις στην ασφάλεια των τραπεζικών οργανισμών 22
2.4. Ευπάθειες στο Web Banking 25
2.5. Συνήθεις Απειλές Ηλεκτρονικής Τραπεζικής 29
2.5.1. Denial-of-service (Άρνηση Παροχής Υπηρεσίας) 30
2.5.2. Advanced persistent threats (APT) 30
2.5.3. Phishing (Ηλεκτρονικό ψάρεμα) 34
2.5.4. Malware (κακόβουλο λογισμικό) 35
2.5.5. Botnet 36
2.5.6. Spamming 36
2.5.7. Spoofing 37
2.6 Κίνδυνοι και Απειλές Ασφαλείας Εφαρμογών Διαδικτύου 38
ΚΕΦΑΛΑΙΟ 3- ΤΟ Mobile Banking 45
3.1. Τι είναι το Mobile Banking 45
3.2. Πλεονεκτήματα - Μειονεκτήματα της κινητής τραπεζικής 46
3.3. Η Τρέχουσα κατάσταση του Mobile Banking 49
3.4. Προκλήσεις και ζητήματα σε θέματα ασφάλειας του Mobile Banking 53
3.5. Είδη Απειλών και Επιθέσεων στο Mobile Banking 54

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

3.6. Η ασφάλεια των λειτουργικών συστημάτων των κινητών συσκευών και το Mobile Banking 58
3.6.1. Android 62
3.6.2. IOS (Apple) 71
3.7 Κίνδυνοι και Απειλές Ασφάλειας Εφαρμογών Κινητών 75
ΚΕΦΑΛΑΙΟ 4- Μοντέλα Ανάλυσης Απειλών (Models of Threat Analysis) 79
4.1. Μοντέλα Ανάλυσης Απειλών για χρηματοπιστωτικά Ιδρύματα (Threat Modeling Framework for FSS Institutions) 80
4.2. Χρήση του μοντέλου STRIDE 82
4.3. Χρήση του μοντέλου CAPEC 89
ΚΕΦΑΛΑΙΟ 5- ΜΗΧΑΝΙΣΜΟΙ ΑΣΦΑΛΕΙΑΣ ΣΤΟ WEB ΚΑΙ MOBILE BANKING 97
5.1. Ταξινόμηση μηχανισμών Ασφάλειας 98
5.2. Μηχανισμοί ασφάλειας στο Web Banking 100
5.2.1 Κρυπτογράφηση 101
5.2.2 Έλεγχοι ταυτότητας 102
5.2.3 Διακριτικό ασφάλειας 103
5.2.4 Κωδικοί Ταυτοποίησης - One-time password (OTP) tokens 104
5.3. Μηχανισμοί ασφάλειας στο Mobile Banking 105
5.3.1. Κρυπτογράφηση ασύρματου καναλιού (WPKI) 106
5.3.2. Έλεγχος ταυτότητας συσκευής 107
5.3.3. QRP (Quick Response Protocol) 111
5.3.4. QR codes 111
5.3.5. Βιομετρική ταυτοποίηση 115
ΚΕΦΑΛΑΙΟ 6- ΕΠΙΘΕΣΕΙΣ ΣΤΟ WEB-MOBILE BANKING ΚΑΙ ΟΙ ΣΥΝΕΠΕΙΕΣ ΤΟΥΣ 119
6.1. Το Κυβερνοέγκλημα στον τραπεζικό τομέα 119
6.2. Επιπτώσεις 122
6.3. Οικονομικές επιπτώσεις 124
6.4 Timeline Επιθέσεων 129

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ΒΙΒΛΙΟΓΡΑΦΙΑ 142

Κατάλογος Σχημάτων

Σχήμα 1- Ποσοστό πληθυσμού σε χώρες της Ευρωπαϊκής Ένωσης που χρησιμοποιούν το InternetBanking για το έτος 2017 18
Σχήμα 2- Ποιος είναι ο βασικός λόγος που ξεκινήσατε να κάνατε χρήση του Mobile Banking , Απαντήσεις ανά χώρα 49
Σχήμα 3- Βασικός λόγος για την αποφυγή χρησιμοποίησης του Mobile Banking, απαντήσεις ανά χώρα 50
Σχήμα 4- Ποσοστά χρηστών του Mobile Banking ανά χρηματοοικονομική δραστηριότητα που πραγματοποιούν 52
Σχήμα 5- Τύποι βιομετρικής αναγνώρισης..... 66
Σχήμα 6- Μοντέλα ανάλυσης Απειλών..... 80
Σχήμα 7- Τα τρία Επίπεδα των μοντέλων ανάλυσης Απειλών 81
Σχήμα 8- Ταυτοποίηση Συσκευής με το πιστοποιητικό X.509..... 109
Σχήμα 9- Τρόπος λειτουργίας του πρωτοκόλλου QRP..... 111
Σχήμα 10- Δημιουργία QR code 112
Σχήμα 11- Δομή ενός QR code.....113

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

(Αυτή η σελίδα είναι σκόπιμα κενή)

ΚΕΦΑΛΑΙΟ 1- ΕΙΣΑΓΩΓΗ

1.1. Οριοθέτηση Προβλήματος

Οι θεμελιώδεις αλλαγές στον τομέα της τεχνολογίας τα τελευταία χρόνια και ειδικότερα την τελευταία δεκαετία επηρέασαν καταλυτικά την οικονομία, είχαν μεγάλες συνέπειες και προκάλεσαν αλλαγές στην τεχνολογία. Όλες αυτές οι αλλαγές ήταν το έναυσμα για τη δημιουργία νέων αναγκών και απαιτήσεων που έπρεπε να ικανοποιηθούν για την ομαλή λειτουργία της κοινωνίας. Προκειμένου να ανταποκριθούν σε αυτές τις αλλαγές, τα χρηματοπιστωτικά ιδρύματα έπρεπε να υιοθετήσουν τις νέες τεχνολογίες χρησιμοποιώντας το διαδίκτυο, ελπίζοντας ότι η εγγύηση πρωτοποριακής θέσης στον τομέα των εφαρμογών νέων τεχνολογικών μεθόδων και του Διαδικτύου μπορεί να εξασφαλίσει μια αποτελεσματική άμυνα στις κλιμακούμενες αλλαγές καθώς και ένα ανταγωνιστικό πλεονέκτημα.

Συγκεκριμένα, τα χρηματοπιστωτικά ιδρύματα συνεργάζονται και συνήθως αναθέτουν σε εξειδικευμένες εταιρείες που δραστηριοποιούνται στον κλάδο των τηλεπικοινωνιών και του Διαδικτύου ή ενσωματώνονται με τέτοιες εταιρείες για τη δυναμική τους είσοδο στις νέες αγορές. Το όφελος από τις χρηματοδοτικές υπηρεσίες υποστηρίζεται ουσιαστικά από την επεξεργασία και τη διαβίβαση πληροφοριών, όπου η τεχνολογία διαδραματίζει θεμελιώδη ρόλο. Η χρήση νέων τεχνολογικών εφαρμογών συμβαδίζει με τη δημιουργία νέων χρηματοπιστωτικών προϊόντων και υπηρεσιών και των εναλλακτικών δικτύων διανομής τους και συμβάλλει στην ανάπτυξη και τη διανομή της ηλεκτρονικής τραπεζικής (Santouridis Kyritsi, 2014).

Με την ανάπτυξη και την ραγδαία επέκταση - εξάπλωση των κινητών τεχνολογιών (mobile technologies), τα κινητά τηλέφωνα δίνουν την δυνατότητα στους χρήστες να εκτελούν πλήθος διαφορετικών λειτουργιών και ενεργειών χρησιμοποιώντας απλά τις κινητές συσκευές τους. Στις μέρες μας οι πλατφόρμες-

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

εφαρμογές κινητών τηλεφώνων δημιουργούν μεγάλες ευκαιρίες στις επιχειρήσεις ιδίως εξαιτίας των δυνατοτήτων τους καθώς και της πληθυσμιακής κάλυψης. Προκειμένου να κάνουν χρήση αυτών των δυνατοτήτων που προσφέρουν οι εφαρμογές-πλατφόρμες οι περισσότερες τράπεζες έχουν κατασκευάσει τις δικές τους εφαρμογές κινητών τηλεφώνων είτε έχουν επεκτείνει τις διαδικτυακές εφαρμογές-πλατφόρμες τους στα κινητά τηλέφωνα. Ένα από τα σημαντικά πλεονεκτήματα που προσφέρουν οι τραπεζικές εφαρμογές κινητών τηλεφώνων είναι η δυνατότητα που δίνεται στους χρήστες να εκτελούν οποιαδήποτε συναλλαγή από οποιαδήποτε μέρος του κόσμου οποιαδήποτε στιγμή. Ενώ οι προσδοκίες αρχικά ήταν μεγαλύτερες, το ποσοστό των κατόχων κινητών τηλεφώνων που χρησιμοποιεί τραπεζικές εφαρμογές δεν ξεπερνά το 30%! Το παραπάνω συμβαίνει διότι οι χρήστες αισθάνονται μη ασφαλείς πραγματοποιώντας συναλλαγές από τα κινητά τους (Shah & Clarke, 2009).

Ορισμένα στοιχεία από την οπτική της ασφάλειας των διαδικτυακών και κινητών εφαρμογών των τραπεζών είναι τα παρακάτω:

- Ο τραπεζικός τομέας έχει δεχτεί τριπλάσιες επιθέσεις σε σχέση με άλλους τομείς
- Οι παραβιάσεις των πληροφοριών (data breaches) μπορούν να οδηγήσουν σε εκθετικά κόστη για τις τράπεζες
- Υπάρχει μια αύξηση στην χρήση βιομετρικών για είσοδο σε διαδικτυακές εφαρμογές καθώς επίσης και περαιτέρω αναγνώρισή τους και εδραίωσής τους από τις τράπεζες
- Οι καταναλωτές προτιμούν όλο και περισσότερο να χρησιμοποιούν κινητές συσκευές για τις συναλλαγές τους κάτι το οποίο οδηγεί τον τραπεζικό τομέα να αυξήσει το επίπεδο ασφάλειας και να διατηρήσει ακέραιες τις υπάρχουσες διαδικασίες χωρίς ωστόσο να επηρεάσει την εμπειρία και την ευκολία χρήσης της εφαρμογής από τους καταναλωτές.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

1.2. Σκοπός της Εργασίας

Σκοπός της εργασίας είναι η μελέτη της τρέχουσας κατάστασης του web και του Mobile Banking, η καταγραφή των απειλών και των επιθέσεων τους, καθώς και η συστηματική ανάλυση αυτών. Τα παραπάνω, θα παρουσιαστούν, μετά από την ανάλυση της σχετικής βιβλιογραφίας. Ειδικότερα, η παρούσα εργασία στοχεύει να απαντήσει στα εξής ερευνητικά ερωτήματα:

1. Ποια είναι η παρούσα κατάσταση των εφαρμογών Web Banking που χρησιμοποιούν οι τράπεζες;
2. Ποια είναι η παρούσα κατάσταση των εφαρμογών Mobile Banking που χρησιμοποιούν οι τράπεζες;
3. Ποιες είναι οι προκλήσεις της ασφάλειας των πληροφοριακών συστημάτων και ποιες οι απειλές όταν χρησιμοποιούμε τραπεζικές εφαρμογές στο διαδίκτυο;
4. Ποιοι είναι οι έλεγχοι και τα κατάλληλα μέτρα που πρέπει να εφαρμοστούν προκειμένου να αντιμετωπιστούν οι προκλήσεις της χρήσης τραπεζικών εφαρμογών;

1.3. Δομή της Εργασίας

Η εργασία δομείται σε έξι βασικά κεφάλαια. Το πρώτο κεφάλαιο, εστιάζει στην τρέχουσα κατάσταση του e-banking και σε εισαγωγικά στοιχεία αναφορικά με αυτό. Το δεύτερο κεφάλαιο, παρουσιάζει την τρέχουσα κατάσταση του Web Banking, και στην συνέχεια παρουσιάζονται τα είδη των απειλών και των επιθέσεων που υφίστανται σε διαδιακτυακές εφαρμογές, μέσω των οποίων οι χρήστες έχουν πρόσβαση στο Web Banking. Στην συνέχεια, στο τρίτο κεφάλαιο, παρουσιάζονται την τρέχουσα κατάσταση του Mobile Banking, και στην συνέχεια παρουσιάζονται τα είδη των

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

απειλών και των επιθέσεων που υφίστανται σε κινητές συσκευές, στις οποίες οι χρήστες έχουν πρόσβαση σε mobile Banking εφαρμογές. Στο τέταρτο κεφάλαιο, ορισμένα μοντέλα, σκοπός των οποίων είναι να πραγματοποιηθεί μια ανάλυση των απειλών (Threat Analysis) που παρουσιάστηκαν στα δύο προηγούμενα κεφάλαια.

Έπειτα, στο πέμπτο κεφάλαιο εξετάζονται οι μηχανισμοί ασφάλειας στο web και mobile banking. Στο έκτο κεφάλαιο, παρουσιάζονται ορισμένες από τις ποιο σημαντικές κακόβουλες επιθέσεις, που έχουν συμβεί στο παρελθόν, σε πλατφόρμες και εφαρμογές E-banking καθώς και οι συνέπειες που είχαν τα χρηματοπιστωτικά ιδρύματα στα οποία έλαβαν χώρα.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ΚΕΦΑΛΑΙΟ 2- Το Web banking

Στο κεφάλαιο αυτό, παρουσιάζονται: η τρέχουσα κατάσταση του Web Banking, με επίσημα στατιστικά στοιχεία, οι ευπάθειες των συστημάτων και των διαδικτυακών εφαρμογών Web Banking, τις οποίες εκμεταλλεύονται οι κακόβουλοι χρήστες, καθώς και οι εσωτερικές και εξωτερικές απειλές που υφίστανται στην χρήση των συστημάτων Web Banking που υπάρχουν στο διαδίκτυο.

2.1. Τι είναι το Web banking

Καθώς οι τεχνολογία εξελίσσεται με ραγδαίους ρυθμούς, και η χρήση του Διαδικτύου αυξάνεται ολοένα και περισσότερο σε παγκόσμιο επίπεδο, είναι προφανές ότι αυξάνεται συνεχώς και η χρήση της ηλεκτρονικής τραπεζικής (Web Banking). Στην βιβλιογραφία, υπάρχει η χρήση πολλών όρων για την χρήση των υπηρεσιών των χρηματοπιστωτικών και τραπεζικών υπηρεσιών. Για παράδειγμα, χρησιμοποιούνται οι όροι: Web Banking, Online Banking, Mobile Banking, ή απλά E-Banking. Αν και οι παραπάνω όροι φαίνονται να είναι συναφείς, όμως στην πραγματικότητα, υπάρχουν ορισμένες διαφορές. Οι Hertzum et al. (2004) ορίζουν την ηλεκτρονική τραπεζική ως την διαδικτυακή τραπεζική. Με άλλα λόγια, ο όρος E- banking ή Web Banking είναι ίδιοι, και αναφέρονται στις τραπεζικές συναλλαγές, η οποία γίνεται μέσω του World Wide Web. Όσον αναφορά το Mobile Banking, θα γίνει εκτενής αναφορά και μελέτη στο επόμενο κεφάλαιο, αλλά θα πρέπει να αναφερθεί ότι ο όρος χρησιμοποιείται για την χρήση των τραπεζικών υπηρεσιών μέσω κινητών συσκευών (Smartphones, Tablets κτλ) (Alawneh, 2009).

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Σύμφωνα με τους Mai et al. (2007), το Web Banking, αναφέρεται στην ανάπτυξη μέσω του Διαδικτύου τραπεζικών υπηρεσιών λιανικής και χονδρικής (εταιρικής) τραπεζικής. Περιλαμβάνει μεμονωμένους και εταιρικούς πελάτες. Περιλαμβάνει επίσης τις τραπεζικές μεταφορές, τις πληρωμές και τους διακανονισμούς, τις εισπράξεις και πιστώσεις εγγράφων, τη δανειοδότηση επιχειρήσεων και νοικοκυριών, καθώς και τις συναλλαγές με κάρτες.

Ο όρος PC Banking, χρησιμοποιείται για να περιγράψει την χρήση των τραπεζικών υπηρεσιών, αλλά με την χρήση ειδικού λογισμικού και υλικού που ο χρήστης πρώτα πρέπει να προμηθευτεί από την τράπεζά του. Αντίθετα, το Web banking δεν απαιτεί από το χρήστη να έχει κάποιο ειδικό λογισμικό, παρά μόνο πρόσβαση στο διαδίκτυο από οποιαδήποτε συσκευή (Υπολογιστής κτλ.) (Hamid et al 2007).

Η τραπεζική στο Διαδίκτυο ενισχύεται από την ικανότητα των πελατών να πραγματοποιούν τραπεζικές συναλλαγές οποτεδήποτε και οπουδήποτε, ταχύτερα και με χαμηλότερα τέλη σε σύγκριση με τη χρήση παραδοσιακών τραπεζικών καταστημάτων (Sayar and Wolfe, 2007).

Ως εκ τούτου, οι τράπεζες έχουν εκμεταλλευτεί τον Παγκόσμιο Ιστό για να αξιοποιήσουν τα πλεονεκτήματα της δύναμης και της εμβέλειας του διαδικτύου, για να αντιμετωπίσουν τον επιταχυνόμενο ρυθμό των αλλαγών στο επιχειρηματικό περιβάλλον (Mai et al, 2007). Η τραπεζική μέσω Διαδικτύου παρέχει άμεση πρόσβαση σε χρηματοοικονομικές πληροφορίες και αναλαμβάνει οικονομικές συναλλαγές χωρίς να χρειάζεται να μεταβεί στην τράπεζα (Rotchanakitumnual and Speece, 2003). Ως εκ τούτου, μια τραπεζική υπηρεσία δεν είναι πλέον συνδεδεμένη με το χρόνο ή τις γεωγραφικές περιοχές.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

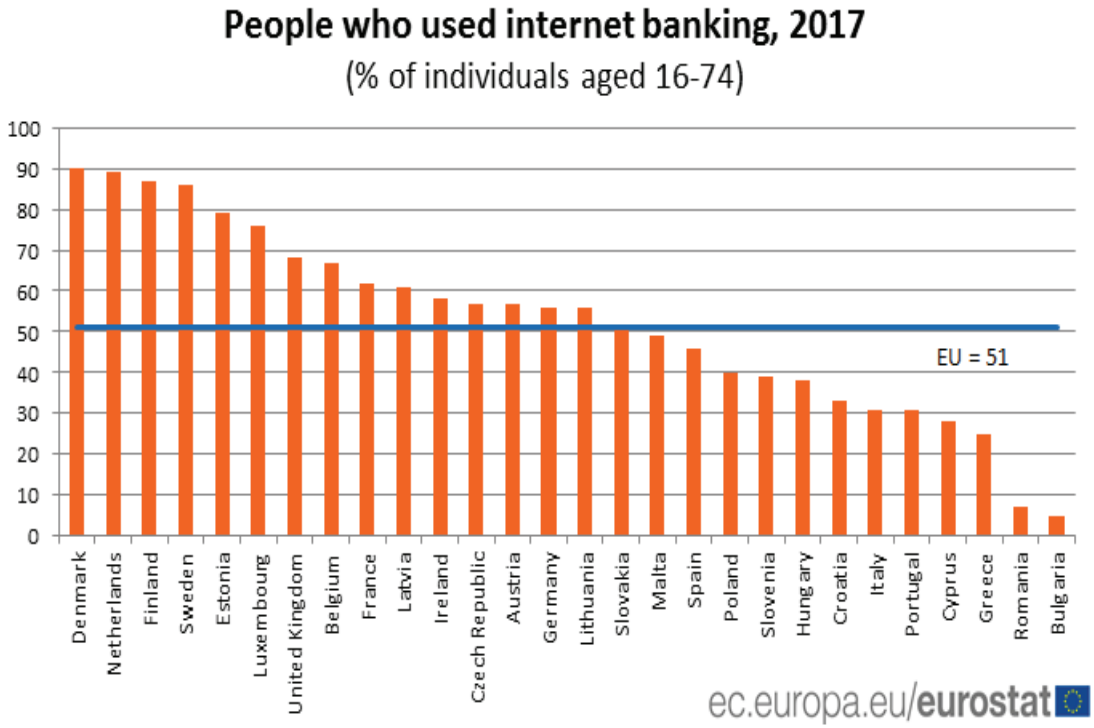
2.2. Η Τρέχουσα κατάσταση του Web banking

2.2.1. Χρήση του Web Banking στην Ευρώπη

Σύμφωνα με επίσημα στοιχεία της Eurostat, το 51% και πλέον των ενήλικων Ευρωπαίων χρησιμοποιούν τραπεζικές υπηρεσίες μέσω του Διαδικτύου. Το ποσοστό αυτό αυξάνεται διαρκώς και έχει διαπλαστεί από το 2007, όπου ήταν 25%. Το Web Banking είναι ιδιαίτερα δημοφιλές μεταξύ των ατόμων ηλικίας 25 έως 34 ετών, ενώ ο μέσος όρος του ποσοστού χρήσης του στις χώρες της ΕΕ είναι 68%. Επίσης, η χρήση του Web Banking τείνει να αυξάνεται ανάλογα με το επίπεδο εκπαίδευσης του χρήστη. Μολονότι μόνο το 24% των ατόμων με χαμηλή εκπαίδευση χρησιμοποιούν την ηλεκτρονική τραπεζική, το 77% των ατόμων με υψηλή εκπαίδευση χρησιμοποιούν αυτή την υπηρεσία.

Μεταξύ των κρατών μελών της ΕΕ, το Web Banking χρησιμοποιείται περισσότερο στην Δανία (90%), στην Ολλανδία (89%) , στην Φινλανδία (87%) και στην Σουηδία (86%). Αντίθετα, τα χαμηλότερα ποσοστά, καταγράφονται στην Βουλγαρία (5%) και στη Ρουμανία (7%). Στην Ελλάδα καταγράφτηκε ποσοστό χρήσης (25%) και στην Κύπρο (28%) για χρήστες ηλικίας 16 έως 74 ετών.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ



Σχήμα 1- Ποσοστό πληθυσμού σε χώρες της Ευρωπαϊκής Ένωσης που χρησιμοποιούν το Internet Banking για το έτος 2017

Πηγή: Eurostat (2018)[1]

[1]https://ec.europa.eu/eurostat/web/products-eurostat-news/-/DDN-20180115-1

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

2.2.2. Πλατφόρμες και λογισμικά που χρησιμοποιούνται

Όπως είναι γνωστό, οι τράπεζες , είναι οι μεσάζοντες, οι οποίοι συλλέγουν μια κατάθεση χρημάτων, από διάφορες οντότητες και παρέχουν σε όσους την χρειάζονται, με την ανάλογη προμήθεια (τόκοι). Σήμερα βέβαια, οι τράπεζες, με τη βοήθεια της τεχνολογίας όχι μόνο συλλέγουν και εκταμιεύουν χρήματα σε διαφορετικές οντότητες αλλά και παρέχουν πολλές υπηρεσίες σε διάφορες οντότητες που διευκολύνουν τις επιχειρηματικές τους δραστηριότητες. Ένας από τους βασικούς σκοπούς των τραπεζών, είναι η μείωση του κόστους, και η αύξηση της αποτελεσματικότητας. Όλα τα παραπάνω όμως προϋποθέτουν την προστασία των πελατών, την διασφάλιση και διατήρησης των πελατών και της προστασίας των προσωπικών δεδομένων, των χρημάτων τους, και όλα αυτά με την χρήση της τεχνολογίας και αποτελεσματικών μηχανισμών ασφαλείας (Turnbull, 2007).

Στον τραπεζικό τομέα, οι σχέσεις μεταξύ των ιδρυμάτων και των πελατών τους είναι κρίσιμες (Seybold & Foss, 2001) και η τεχνολογία όπως τα ATM, POS, SMS Banking, Online Banking και Mobile Banking είναι ο διαμεσολαβητής σε αυτή την αλληλεπίδραση. Οι τεχνολογικές εξελίξεις επιτρέπουν στενές και μακροπρόθεσμες σχέσεις με τους πελάτες (Chairlone, 2009). Για αυτές τις τράπεζες νέας γενιάς το τεχνολογικό γονίδιο ονομάζεται Core Banking Solutions (CBS). To Core Banking Solution, μιας τράπεζας, ο «κινητήρας» του e-Banking, καθορίζει για κάθε τράπεζα τι πρόκειται να προσφέρει και πόσο αποτελεσματικά μπορεί εξυπηρετήσει την υλοποίηση παράλληλων διαδικασιών και συναλλαγών μεγάλου όγκου πελατών (Gartner, 2011).

Οι προγραμματιστές των τραπεζικών συστημάτων CBS, προσθέτουν συνεχώς νέα χαρακτηριστικά για να επιτρέψουν στις τράπεζες να αποκτήσουν ανταγωνιστικά πλεονεκτήματα στην αγορά. Όπως το ERP, έτσι και το CBS έχει εξαλείψει την ανάγκη για διαφορετικό λογισμικό για διάφορες λειτουργίες (Boot 2009). Ωστόσο, ένα έργο υλοποίησης CBS, όπως και όλα τα άλλα μεγάλα επενδυτικά έργα πληροφορικής, είναι

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

δαπανηρό, χρονοβόρο και πολύπλοκο. Λόγω αυτού, μόνο το 25% των έργων CBS εφαρμόστηκαν με επιτυχία και το υπόλοιπο 50% παρουσίασε υπέρβαση κόστους και προγραμματισμού και άλλα απέτυχαν (Adamson, Chan & Handfor, 2003). Οι πρόσφατες εξελίξεις στα συστήματα και τις διαδικτυακές πλατφόρμες του Web Banking, περιλαμβάνουν τεχνολογίες και αρχιτεκτονικές για επιχειρησιακά συστήματα μέσω διαδικτύου, ασφάλεια, επιχειρησιακή ευφυΐα (business Intelligence), ολοκλήρωση συστημάτων, πολυκατευθυνόμενα συστήματα, αύξηση του αριθμού προϊόντων και υπηρεσιών που προσφέρονται διαδικτυακά και χρήση των καινοτομιών του Web 2.0.

Τα συστήματα της ηλεκτρονικής τραπεζικής, χρησιμοποιούν τις πιο εξελιγμένες μορφές αρχιτεκτονικών και συστημάτων ασφαλείας, καθώς χρησιμοποιούνται από εκατοντάδες εκατομμύρια χρήστες σε όλο τον κόσμο, και οι βάσεις δεδομένων των τραπεζών, εμπεριέχουν ευαίσθητα προσωπικά δεδομένα και χρηματικούς λογαριασμούς πελατών. Συνήθως, οι διαδικτυακές πλατφόρμες των τραπεζών υλοποιούνται από εξειδικευμένους προγραμματιστές με την χρήση γλωσσών ASP, PHP, JSP κλπ., χρησιμοποιώντας πολυεπίπεδη αρχιτεκτονική, που αναπτύσσεται συχνά με τεχνολογίες ιστού, όπως το .Net και το JEE . Τα συστήματα αυτά επωφελούνται επίσης από την τεχνολογία SOA, η οποία παρέχει δυνατότητες ευελιξίας, διαλειτουργικότητας, μεταφορά δεδομένων, και ενοποίησης για την εσωτερική λειτουργικότητα του συστήματος (Mitropoulos and Douligeris, 2011).

Επιπλέον, οι υπηρεσίες Web Services (WS) χρησιμοποιούνται για την αλληλεπίδραση και την συνεργασία, μεταξύ της διαδικτυακής πλατφόρμας των τραπεζών και άλλων εξωτερικών συστημάτων. Στην υπηρεσία Web Banking, οι υπηρεσίες web χρησιμοποιούνται ως επί το πλείστων για πολύπλοκες συναλλαγές, όπως οι ηλεκτρονικές πληρωμές. Τα συστήματα τραπεζικού συστήματος Web έχουν πρόσβαση και χειρίζονται ένα μεγάλο αριθμό δεδομένων σε καθημερινή βάση και κατά συνέπεια πρέπει να υποστηρίζονται από ισχυρά συστήματα διαχείρισης βάσεων

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

δεδομένων, όπως SQL Server ή το Oracle. Η Ασφάλεια των διαδικτυακών πλατφορμών των τραπεζών, αποτελεί ύψιστης σημασίας ζήτημα, και για αυτό τον λόγο οι τράπεζες επενδύουν μεγάλα χρηματικά ποσά για την ενίσχυση της ασφάλειας των συστημάτων τους. Ένα σύστημα τραπεζικής στο Διαδίκτυο είναι πιο ευάλωτο σε απειλές, καθώς μπορεί εύκολα να το προσεγγίσει κανείς μέσω του Διαδικτύου. Ως εκ τούτου, είναι σημαντικό να αναλύονται όλες οι πιθανές απειλές και να λαμβάνονται όλα τα απαραίτητα βήματα, προκειμένου να διασφαλιστεί η ασφάλεια του συστήματος. Κάθε βαθμίδα της αρχιτεκτονικής Web Banking πρέπει να διασφαλιστεί και η ίδια η εφαρμογή πρέπει να σχεδιαστεί και να αναπτυχθεί με τεχνικές ασφαλείας που καλύπτουν στο μεγαλύτερο δυνατό βαθμό όλες τις προοπτικές ασφάλειας (Mitropoulos et al., 2013).

Η μοντελοποίηση των ηλεκτρονικών τραπεζικών συστημάτων, βασίζεται και αποτελείται από πολλές πολύπλοκες συναλλαγές και διαδικασίες, γεγονός που απαιτεί λεπτομερή ανάλυση πριν από την ανάπτυξη και την ανάπτυξή του. Η UML είναι μια πολύ δημοφιλής γλώσσα μοντελοποίησης που υποστηρίζει όλες τις φάσεις της ανάλυσης και ανάπτυξης του συστήματος, παρέχοντας τεχνικές μοντελοποίησης οι οποίες είναι και αντικειμενοστραφείς. Τα διαγράμματα ροής εργασίας χρησιμοποιούνται επίσης για τον ορισμό ορισμένων διαδικασιών του συστήματος καθώς και των αλληλεπιδράσεων του συστήματος. Αυτά τα θέματα ανάλυσης και μοντελοποίησης είναι πολύ σημαντικά για τη συνολική επιτυχία του κύκλου ζωής του συστήματος ανάπτυξης (Mitropoulos et al., 2013). Η τεχνολογία «Business Intelligence» (BI) έχει προσελκύσει εδώ και χρόνια, τους ειδικούς που σχεδιάζουν και υλοποιούν διαδικτυακές πλατφόρμες Web Banking, καθώς μπορούν να βοηθήσουν τις τράπεζες να προσελκύσουν περισσότερους πελάτες και να βελτιώσουν τη σχέση τους με τις υπάρχουσες. Τα συστήματα τραπεζών του Διαδικτύου μπορούν να επωφεληθούν από τη διαχείριση των σχέσεων με τους πελάτες και την ανάλυση των δεδομένων,

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

οδηγώντας σε πιο εξατομικευμένα προϊόντα και υπηρεσίες που καλύπτουν τις ανάγκες των πελατών της τράπεζας.

2.3. Προκλήσεις και ζητήματα σε θέματα ασφάλειας του Web Banking

2.3.1. Προκλήσεις στην ασφάλεια των τραπεζικών οργανισμών

Την τελευταία δεκαετία, η ικανότητα και τα κίνητρα των απειλών για τον χρηματοπιστωτικό τομέα μετασχηματίστηκαν από τα ευκαιριακά εγκλήματα μικρής κλίμακας σε προσπάθειες για την υπονόμευση ολόκληρων δικτύων και συστημάτων πληρωμών. Οι περισσότερες από τις επιθέσεις που έχουν πραγματοποιηθεί μέχρι σήμερα, εκμεταλλεύτηκαν ευπάθειες, όπως αδύναμη άμυνα και τα υπάρχοντα τρωτά σημεία, και δεν απαιτούν σημαντικούς υπολογιστικούς πόρους. Καθώς τα εργαλεία hacking έγιναν πιο εύκολα διαθέσιμα και οι υπηρεσίες που τους παρέχονταν μετατράπηκαν, ομάδες οικονομικών επιτιθέμενων σχημάτισαν και ανέπτυξαν τα δικά τους λογισμικά και εργαλεία, και ορισμένοι προσφέρθηκαν για να τους προσφέρουν τις υπηρεσίες τους(Sabout & Parthiban, 2015)

Σήμερα, οι στοχευμένες εισβολές έχουν γίνει ο κανόνας. Οι πωλητές υπηρεσιών ασφάλειας έχουν αυξήσει την ευαισθητοποίηση σχετικά με την απειλή μέσω της δημοσιοποίησης πληροφοριών σχετικά με εκστρατείες υψηλού επιπέδου, αλλά αυτή η δημοσιότητα έχει επίσης εξάψει τη γνώση σχετικά με τον τρόπο κατασκευής προηγμένων εργαλείων και λειτουργίας κρυφών. Η διάδοση μέσω της δημοσίευσης έχει δώσει σε όλους, από τον ερασιτέχνη hacker μέχρι τις εθνικές κρατικές υπηρεσίες, περισσότερες πληροφορίες για την ανάπτυξη και τη διεξαγωγή των επιθέσεων τους(Azeez, 2010).

Επί του παρόντος, η απειλή του κυβερνοχώρου από κακόβουλους φορείς και χρήστες παρουσιάζει μεγάλες διαστάσεις στον χρηματοπιστωτικό τομέα. Παραδείγματα πρόσφατων επιτυχημένων επιθέσεων περιλαμβάνουν την επίθεση του

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Απριλίου 2018 κατά του εγχώριου μεσογειακού δικτύου πληρωμών SPEI του Μεξικού, όπου 15 εκατομμύρια δολάρια κλάπηκαν από πολλά χρηματοπιστωτικά ιδρύματα και η επίθεση του Μάϊου του 2018 στη Banco de Chile, η οποία έχασε 10 εκατομμύρια δολάρια μέσω διεθνών μεταφορών πληρωμών. Οι επιτιθέμενοι της Banco de Chile υιοθέτησαν μια γνωστή τεχνική επίθεσης γνωστή και ως «smoke screen attack» η οποία ουσιαστικά προσομοιάζει μια επίθεση της οποίας η δραστηριότητα καλύπτεται από μια οθόνη καπνού. Ουσιαστικά αναφερόμαστε σε επιθέσεις οι οποίες στοχεύουν στο δίκτυο και είναι σχεδιασμένες με κατάλληλο τρόπο ώστε να προκαλούν σύγχυση και αποπροσανατολισμό στους υπεύθυνους της ασφάλειας των πληροφοριακών συστημάτων του εκάστοτε οργανισμού ή επιχείρησης. Ανέπτυξαν λοιπόν κακόβουλο λογισμικό εκκαθάρισης αρχείων το οποίο κατέστρεψε αρκετές χιλιάδες συστήματα στο δίκτυο της τράπεζας με τις λειτουργίες των τραπεζών να είναι μη διαθέσιμες για αρκετές ημέρες. Στα τέλη του 2018, υπήρξαν και άλλες επιθέσεις - η Cosmos Bank στην Ινδία, η τράπεζα Islami στο Πακιστάν και η Red banc στη Χιλή υπέστησαν παρόμοιες εισβολές και επιπτώσεις στις επιχειρηματικές τους δραστηριότητες. Τον Φεβρουάριο του 2019, οι επιτιθέμενοι έθεσαν σε κίνδυνο τα συστήματα πληρωμών μιας τράπεζας της Μάλτας και προσπάθησαν να μεταφέρουν 13 εκατομμύρια ευρώ από αυτήν σε άλλους λογαριασμούς (Singh et al., 2019).

Οι τράπεζες και τα χρηματοπιστωτικά ιδρύματα, έχουν να αντιμετωπίσουν σε καθημερινή βάση τις απειλές και τις επιθέσεις των εγκληματιών του κυβερνοχώρου. Συνεπώς, η ασφάλεια των πληροφοριακών συστημάτων ενός χρηματοπιστωτικού ιδρύματος θα πρέπει να είναι αρκετά ισχυρή ώστε να αντέχει σε κακόβουλες επιθέσεις. Τα λογισμικά προστασίας, θα πρέπει να ενημερώνονται σε πραγματικό χρόνο και οι έλεγχοι ασφαλείας των συστημάτων για τον εντοπισμό ευπαθειών και επιθέσεων θα πρέπει να γίνονται συνεχώς.

Είναι ευθύνη του κάθε εμπλεκόμενου φορέα χρηματοπιστωτικού ιδρύματος που είναι επιφορτισμένος με την ευθύνη ως φύλακας του χαρτοφυλακίου των

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ηλεκτρονικών πληροφοριών να καταβάλλει όλες τις απαραίτητες ενέργειες ώστε να εξασφαλίσει την προστασία των προσωπικών δεδομένων, την ακεραιότητα των τραπεζικών συναλλαγών και την ταυτοποίηση των πελατών. Δυστυχώς, οι επιθέσεις στον κυβερνοχώρο κλιμακώνονται ολοένα και περισσότερο, και οι εγκληματίες του διαδικτύου χρησιμοποιούν δημιουργικές τεχνικές, εκμεταλλεύονται τις ευπάθειες των συστημάτων και του λογισμικού που χρησιμοποιούν οι τράπεζες, και πολλές φορές καταφέρνουν να παρακάμψουν τα επίπεδα ασφαλείας τους, με πολλές οικονομικές και άλλες επιπτώσεις (Marshall, 2010).

Σε αυτήν την προσπάθεια, οι τραπεζικοί οργανισμοί θα πρέπει να συνεργαστούν σε παγκόσμιο επίπεδο, εναντίον όλων και όσων επιδιώκουν να προκαλέσουν ανεπιθύμητες συνέπειες, επενδύοντας στην μέγιστη ασφάλεια των συστημάτων λογισμικών που χρησιμοποιούνται στις πλατφόρμες του Web Banking, δημιουργώντας κοινές βάσεις δεδομένων που θα εμπεριέχουν δεδομένα και στοιχεία, με σκοπό την παρακολούθηση και τον εντοπισμό των εγκληματιών στον κυβερνοχώρο, τα εγκλήματά τους, τα πρότυπα των επιθέσεων και ενεργειών τους, την συμπεριφορά τους και τις δραστηριότητές τους.

Μία άλλη σημαντική πρόκληση των τραπεζικών ιδρυμάτων είναι ότι έχουν την ευθύνη να ενημερώνουν τους πελάτες-χρήστες τους για τους ενδεχόμενους κινδύνους και απειλές, ώστε αλλά και τα μέτρα προστασίας που θα πρέπει να λαμβάνουν, ώστε να αποφύγουν τους κινδύνους των κακόβουλων χρηστών(Singh et al., 2019).

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

2.4. Ευπάθειες στο Web Banking

Οι Ευπάθειες των συστημάτων του Web Banking είναι πολλές. Οι ευπάθειες που συναντώνται σήμερα στον τομέα της ηλεκτρονικής τραπεζικής, σύμφωνα με τους Singh et al. (2019), είναι οι ακόλουθες:

Υψηλά επίπεδα Επιθέσεων: Το γεγονός ότι το Web Banking είναι διαθέσιμο από οπουδήποτε, δημιουργεί από μόνο του μια ευπάθεια στην ασφάλεια των τραπεζικών συναλλαγών. Με άλλα λόγια, δίνει την ευκαιρία και στους κακόβουλους χρήστες να εκμεταλλευτούν και να αξιοποιήσουν την δυνατότητα αυτή ώστε να επιτύχουν μια κακόβουλη επίθεση.

Οι διασυνδεδεμένες διεπαφές και οι διεπαφές προγραμματισμού εφαρμογών (APIs): Τα API χρησιμοποιούνται για την επικοινωνία και τη διαχείριση δεδομένων με τράπεζες. Η ευπάθεια μπορεί να προκαλέσει τυχόν προβλήματα στην ασφάλεια των διεπαφών, δηλαδή των API που χρησιμοποιούν στις πλατφόρμες του Web Banking

Υπερχείλιση Προσωρινής Μνήμης (Buffer Overflow): Ένα φαινόμενο υπερχείλισης προσωρινής μνήμης συμβαίνει όταν ένα πρόγραμμα υπολογιστή σε μια πύλη διακομιστή / πληρωμής αποθηκεύει επιπλέον δεδομένα σε μνήμη προσωρινής αποθήκευσης (προσωρινή περιοχή αποθήκευσης δεδομένων). Τα πρόσθετα δεδομένα μπορούν να υπερχειλίσουν παρακείμενα buffer κάτι το οποίο δύναται να προκαλέσει την καταστροφή ή αντικατάσταση των υπαρχόντων έγκυρων δεδομένων. Γενικά, μπορεί να συμβεί και τυχαία μέσω σφάλματος προγράμματος υπολογιστή. Η υπερχείλιση προσωρινής μνήμης θεωρείται επίσης ένα ιδιαίτερο είδος επίθεσης ασφαλείας που προκάλεσε πρόβλημα ακεραιότητας δεδομένων(European Payment Council, 2019).

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Ευπάθειες Πλατφόρμας: Ορισμένες από τις ευπάθειες της πλατφόρμας του χρηματοπιστωτικού ιδρύματος (Λειτουργικό σύστημα, δίκτυο κ.λπ.) αποτελούν επιθέσεις cross-site scripting και SQL injection. Εάν εισαχθεί κακόβουλος κώδικας στα πεδία δεδομένων ενός τυποποιημένου ερωτήματος SQL με τον οποίο ένας εισβολέας παίρνει παράνομη πρόσβαση στις βάσεις δεδομένων, αυτός ο τύπος επίθεσης είναι γνωστός ως SQL injection Attack. Στην επίθεση cross-site scripting(XSS), κακόβουλος κώδικας προγραμματισμού εισάγεται σε περιεχόμενο ιστοτόπου, αναγκάζοντας έτσι έναν ιστότοπο να εκτελέσει τους κώδικες που παρέχονται από τον εισβολέα.

Βελτίωση Τεχνολογίας: Η βελτίωση της τεχνολογίας των υπολογιστών, η αύξηση του εύρους ζώνης του διαδικτύου, η διαθεσιμότητα κακόβουλων μεθόδων, εργαλείων ή προγραμμάτων στο Διαδίκτυο αποτελούν κάποιο υποστηρικτικό εξοπλισμό για τους κακόβουλους χρήστες του διαδικτύου.

Ειδικότερα οι ευπάθειες των συστημάτων Web Banking μπορούν να ταξινομηθούν στις παρακάτω κατηγορίες (Laerte et al., 2011):

Ψηφιακά Πιστοποιητικά:Τα ψηφιακά πιστοποιητικά χρησιμοποιούνται για να υλοποιείται η αυθεντικοποίηση των χρηστών και του τραπεζικού συστήματος. Αυτό το είδος αυθεντικοποίησης βασίζεται στην κρυπτογραφία δημοσίου κλειδιού καθώς και στην ύπαρξη μιας έμπιστης αρχής πιστοποίησης η οποία υπογράφει τα πιστοποιητικά και επικυρώνει την εγκυρότητά τους. Σε περίπτωση που για οποιοδήποτε λόγο ο κακόβουλος εισχωρήσει και πάρει τον έλεγχο μιας αρχής πιστοποίησης τότε ενδέχεται να δοθεί η δυνατότητα σε άλλους κακόβουλους χρήστες να αυθεντικοποιηθούν από τα τραπεζικά ιδρύματα με παράνομο τρόπο.

OTP Token (κωδικός μίας χρήσης) : Ο κωδικός που δημιουργείται μπορεί να καταγραφεί και να χρησιμοποιηθεί σε πραγματικό χρόνο. Ο κακόβουλος χρήστης μπορεί να αποκτήσει και να χρησιμοποιήσει τον εν λόγω κωδικό πρόσβασης για μη εξουσιοδοτημένες συναλλαγές μέσω της χρήσης της κοινωνικής μηχανικής. Το OTP

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Card Malware μπορεί να συλλέξει κωδικούς πρόσβασης ή να προκαλέσει τον χρήστη για να τους ενημερώσει (European Payment Council, 2019). Σε μερικά τραπεζικά συστήματα οι κωδικοί μιας χρήσης δεν χρησιμοποιούνται μόνο μία φορά κάτι το οποίο καθιστά το σύστημα ευπαθές σε replayattacks.

Προστασία προγράμματος περιήγησης: Στην περίπτωση των τραπεζικών συναλλαγών το σύστημα διασφαλίζεται κυρίως στο επίπεδο του περιηγητή που ουσιαστικά ευθύνεται για την εξασφάλιση και την εδραίωση της επικοινωνίας με χρήση και άλλως τεχνολογιών. Οι ιστοσελίδες πλαστών ηλεκτρονικών τραπεζικών συστημάτων, οι οποίες εμποδίζουν την σωστή φόρτωση της προστασίας, μπορούν να χρησιμοποιηθούν για την εισαγωγή των ευαίσθητων δεδομένων των χρηστών (όπως κωδικοί πρόσβασης) σε περιβάλλον που δεν είναι ασφαλές.

Εικονικό πληκτρολόγιο: Σε αυτή την κατηγορία ανήκουν γνωστά εργαλεία, όπως Screenloggers, mouseloggers ή keyloggers, μπορούν να καταγράψουν ευαίσθητες πληροφορίες. Η εγκατάσταση αντίστοιχων προγραμμάτων στα πληροφοριακά συστήματα ενέχει πολλούς κινδύνους κλοπής και χρήσης των προσωπικών διαπιστευτηρίων από μη εξουσιοδοτημένους χρήστες.

CAPTCHA: Οι μέθοδοι που χρησιμοποιούνται για την αναδίπλωση των πληροφοριών στην εικόνα είναι πολύ απλές, καθιστώντας δυνατή την εξαγωγή των επιθυμητών πληροφοριών χρησιμοποιώντας λογισμικό OCR.

Υπηρεσία σύντομων μηνυμάτων (SMS): Ο κακόβουλος χρήστης μπορεί να αλλάξει τον αριθμό τηλεφώνου (sim swap) στον οποίο αποστέλλονται τα μηνύματα εξουσιοδότησης. Χαρακτηριστικά αναγνώρισης συσκευής που θεωρείται ότι είναι μοναδικά στη συσκευή του χρήστη μπορούν να αναπαραχθούν.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Ταυτοποίηση Συσκευής: πληροφορίες ταυτοποίησης που πιστεύεται ότι είναι γνωστές μόνο από τον χρήστη ενδέχεται να διαρρεύσουν στο διαδίκτυο και τεχνικές κοινωνικής μηχανικής μπορούν να χρησιμοποιηθούν για την ανεύρεση τέτοιων πληροφοριών.

Ταυτοποίηση Ιδιωτικών-Προσωπικών πληροφοριών: πληροφορίες τις οποίες ο χρήστης απαιτείται να εισάγει σύστημα ως επιπρόσθετο μέτρο ασφάλειας και ταυτοποίησης (πολλαπλή αυθεντικοποίηση – 2fa). Οι εν λόγω πληροφορίες αποτελούν κρυφές – μυστικές πληροφορίες που γνωρίζει μόνο ο χρήστης και έχει καταχωρήσει στο σύστημα κατά την αρχική εγκατάσταση και ενεργοποίηση της εκάστοτε εφαρμογής.

Ερωτήσεις Ασφαλείας Χρήστη (Pass-Phrase): Σε αυτήν την κατηγορία ανήκουν εργαλεία όπως τα screenloggers, keyloggers ή mouseloggers, μπορούν να χρησιμοποιηθούν για την καταγραφή των μυστικών πληροφοριών.

Παρακολούθηση Συναλλαγών: Σε αυτή την κατηγορία ανήκουν τα πρόσφατα κακόβουλα προγράμματα, τα οποία δημιουργούν προφίλ συμπεριφοράς και ενεργειών των χρηστών που τους επιτρέπουν να χρησιμοποιούν άλλα προφίλ χρηστών χωρίς να γίνεται αυτό αντιληπτό από το σύστημα.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

2.5. Συνήθεις Απειλές Ηλεκτρονικής Τραπεζικής

Οι απειλές στον κυβερνοχώρο μπορούν να περιλαμβάνουν στοχευμένες και μη στοχευμένες επιθέσεις που ενδέχεται να επηρεάσουν δυσμενώς τους υπολογιστές, το λογισμικό, το δίκτυο, τη βιομηχανία ή το ίδιο το Διαδίκτυο. Ο δυνητικός αντίκτυπος αυτών των απειλών ενισχύεται από τη συνδεσιμότητα μεταξύ των πληροφοριακών συστημάτων, του Διαδικτύου και άλλων υποδομών. Στην ενότητα αυτή θα αναφερθούν οι απειλές της κυβερνοασφάλειας που υφίστανται και στον τομέα του Web Banking. Πολλές φορές, ένας κακόβουλος χρήστης μπορεί είτε να χρησιμοποιήσει μεμονωμένα κάποια επίθεση, ή ακόμα και να συνδυάσει διάφορες μεθόδους επίθεσης, για καλύτερα αποτελέσματα.

Για παράδειγμα, μια επίθεση άρνησης εξυπηρέτησης (Denial of Service) θα μπορούσε να κάνει το σύστημα πληροφορικής ενός οργανισμού να καταρρεύσει, και ταυτόχρονα, ο κακόβουλος χρήστης να χρησιμοποιήσει και κάποια άλλη μέθοδο επίθεσης. Με αυτόν τον τρόπο, θα καταφέρει να μην εντοπιστεί ποτέ η επίθεση του , καθώς τα συστήματα του οργανισμού θα είναι εκτός λειτουργίας.

Επιπλέον, πολύ εξελιγμένες και εξειδικευμένες απειλές (Advanced Persistent Threats), χρησιμοποιούνται όλο και περισσότερο για την παραβίαση των συστημάτων πληροφοριών των κυβερνητικών και εμπορικών φορέων για να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση στα δεδομένα. Αυτές οι απειλές και επιθέσεις που ανήκουν σε αυτήν την κατηγορία (η οποία θα αναλυθεί εκτενώς παρακάτω), μπορεί να μην είναι ανιχνεύσιμες για μεγάλες περιόδους (Damodaran, 2017).

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

2.5.1. Denial-of-service (Άρνηση Παροχής Υπηρεσίας)

Μια επίθεση που εμποδίζει ή παρεμποδίζει την εξουσιοδοτημένη χρήση δικτύων, συστημάτων ή εφαρμογών εξαντλώντας πόρους. Σαν υποκατηγορία σε αυτόν το τύπο απειλής, ανήκει η μέθοδος Distributed denial-of-service, η οποία είναι μια παραλλαγή της επίθεσης άρνησης παροχής υπηρεσίας που χρησιμοποιεί πολλούς χρήστες (δίκτυο χρηστών) για να εκτελέσει την επίθεση (More et al., 2016).

2.5.2. Advanced persistent threats (APT)

Οι εξελιγμένες και εξειδικευμένες APT, συχνά αποτελούν οργανωμένες επιθέσεις, με κοινή συνεννόηση πολλών εγκληματιών του κυβερνοχώρου, οι οποίοι διαθέτουν υψηλά επίπεδα γνώσης και σημαντικούς υπολογιστικούς πόρους, και επιτίθενται επανειλημμένα τους στόχους τους, για μεγάλο χρονικό διάστημα, αυξάνοντας τους κινδύνους για το πληροφοριακό σύστημα που δέχεται την επίθεση. Το γεγονός αυτό, κάνει αυτήν την κατηγορία επιθέσεων-απειλών να διαφέρει από τις υπόλοιπες. Δημιουργώντας οργανωμένες επιθέσεις, δημιουργούν ένα λεγόμενο «beachhead» (ομάδα επίθεσης), και με αυτό τον τρόπο δρουν αδιάκοπα, μέχρι να καταφέρουν την επίθεση που έχουν σχεδιάσει και να αποκτήσουν πρόσβαση σε ευαίσθητες πληροφορίες και δεδομένα. Οι στόχοι επιλέγονται βάσει των απαιτούμενων δεδομένων ή των δεδομένων επιλογής. Συνήθως, οι επιθέσεις APT, στοχεύουν να υποκλέψουν δεδομένα με τεράστια οικονομική αξία. Για αυτή την κατηγορία, αξίζει να γίνει εκτενής αναφορά του τρόπου λειτουργίας της, καθώς συνδυάζονται διάφοροι μέθοδοι από τους κακόβουλους χρήστες.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Στάδια Υλοποίησης Επιθέσεων APT

Στάδιο 1: Επιλογή στόχων. Αρχικά, οι κακόβουλοι χρήστες, επιλέγουν το δίκτυο το οποίο στοχεύουν να κάνουν την επίθεση, αναζητώντας για τυχόν ευπάθειες. Οι δοκιμές που χρησιμοποιούνται συνήθως για να διαπιστωθεί η ευπάθεια μιας βάσης δεδομένων ή ενός δικτύου είναι η SQL Injection, κακόβουλο λογισμικό ή άλλα επιβλαβή προγράμματα (Bushin, 2017).

Στάδιο 2: Συλλογή πληροφοριών. Ο επιτιθέμενος, μετά τη μείωση του οργανισμού-στόχου, συγκεντρώνει πληροφορίες σχετικά με τον στόχο της επιλογής. Οι πληροφορίες που εξάγονται σε αυτό το σημείο είναι πολύ σημαντικές για την επιτυχία της επίθεσης. Σε αυτό το σημείο λαμβάνεται υπόψη ο ασθενέστερος κρίκος, ο οποίος αποδείχθηκε ότι είναι ο ανθρώπινος παράγοντας. Πολλοί οργανισμοί υιοθετούν υψηλά πρότυπα ασφαλείας, ωστόσο, με την παρουσία ενός ανθρώπου στη λειτουργία του συστήματος, δημιουργεί ευπάθεια σε αυτόν τον οργανισμό. Η διαδικασία που χρησιμοποιείται για τη συλλογή των πληροφοριών αναφέρεται ως αναγνώριση. Οι επιθέσεις APT συχνά απασχολούν μεγάλο αριθμό ερευνητών, οι οποίοι μπορούν να περάσουν μήνες μελετώντας τους στόχους τους και να εξοικειωθούν με τα συστήματα, τις διαδικασίες και τους ανθρώπους τους. Οι πληροφορίες μπορούν να συγκεντρωθούν τόσο σε απευθείας σύνδεση όσο και χρησιμοποιώντας συμβατικές μεθόδους επιτήρησης.

Στάδιο 3: Πρόσβαση. Μετά την φάση της συλλογής των πληροφοριών, ο κακόβουλος χρήστης μπορεί πλέον να επιλέξει τον κατάλληλο στόχο, αφού αξιολογήσει τις ευπάθειες του συστήματος του στόχου. Σε αυτή την φάση, πλέον ο κακόβουλος χρήστης έχει στην διάθεση του τις κατάλληλες πληροφορίες και μπορεί πλέον να αποκτήσει πρόσβαση στο δίκτυο ή την βάση δεδομένων του οργανισμού-στόχου, χρησιμοποιώντας συνδυασμούς διάφορων μεθόδων επίθεσης, όπως κακόβουλο λογισμικό, παρακίνηση ανυποψίαστων υπαλλήλων να κάνουν κλικ σε συνδέσμους ή

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

να ανοίξουν συνημμένα που φαίνεται να προέρχονται από έμπιστους συνεργάτες. Σε αντίθεση με την τυπική επίθεση phishing, τέτοιες τεχνικές τροφοδοτούνται συχνά από διεξοδική έρευνα σχετικά με τον οργανισμό-στόχο. Τα συστήματα ασφαλείας του οργανισμού, τις περισσότερες φορές αποτυγχάνουν να εντοπίσουν αυτές τις επιθέσεις, οι οποίες μέρα με την μέρα αντλούν όλο και περισσότερες πληροφορίες και ευάλωτα σημεία του συστήματος

Στάδιο 4: Εκμετάλλευση. Η Εκμετάλλευση είναι το στάδιο, το οποίο βρίσκεται αμέσως μετά την λειτουργία ενός κακόβουλου προγράμματος που κατάφερε να αποκτήσει πρόσβαση στα δεδομένα ενός δικτύου. Στο στάδιο αυτό, συνήθως δημιουργείται μια σύνδεση με έναν διακομιστή C & C, ο οποίος παρακάμπτει την ασφάλεια χρησιμοποιώντας ασφαλείς θύρες όπως η θύρα 443, χρησιμοποιώντας νόμιμα εργαλεία και υπηρεσίες για να μειώσει την υποψία και την πιθανή ανίχνευση. Επιπλέον, παρέχει πλήρη εκμετάλλευση του δικτύου του οργανισμού, καθώς οι εντολές μπορούν να εκδοθούν από μια απομακρυσμένη τοποθεσία στις πληροφορίες του οργανισμού στόχου σε συστήματα. Ο διακομιστής C&C (command and control) είναι υπεύθυνος για την αναβάθμιση και ενημέρωση του κακόβουλου λογισμικού για καλύτερη απόδοση καθώς και για την έκδοση εντολών στα κατειλημμένα συστήματα.

Στάδιο 5: Λειτουργία. Όταν μια σύνδεση δημιουργείται και ασφαλίζεται με το διακομιστή C&C (command and control), το προηγούμενο ανεπτυγμένο κακόβουλο λογισμικό προσπαθεί να εξαπλωθεί (μολύνει) σε άλλα μηχανήματα μέσα στο δίκτυο μετά από σάρωση για ευάλωτα συστήματα. Ο εισβολέας μέσω του διακομιστή C&C χρησιμοποιεί αυτή τη μέθοδο για να αποκτήσει πρόσβαση σε ένα σύστημα με εξαιρετικά πολύτιμες πληροφορίες. Αυτό το στάδιο περιλαμβάνει κάποια εσωτερική αναγνώριση για να βοηθήσει στην εύρεση εμπιστευτικών δεδομένων που αναζητούνται. Σε αυτό το σημείο η ανίχνευση μιας εισβολής στο σύστημα γίνεται πολύ δύσκολη. Το κακόβουλο λογισμικό σε αυτό το σημείο μεταλλάσσεται συνεχώς και

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

αλλάζει τη θέση του, γεγονός που βοηθά το κακόβουλο λογισμικό να αποφύγει εύκολα την ανίχνευση.

Στάδιο 6: Ανακάλυψη και συλλογή δεδομένων. Η πλευρική μετακίνηση του κακόβουλου περιεχομένου γύρω από τον οργανισμό δημιουργεί ένα κανάλι για τη μετάδοση δεδομένων από τον οργανισμό. Στο σημείο αυτό τα δεδομένα υψηλής αξίας εντοπίζονται και συλλέγονται σε μία ή λιγότερες θέσεις για εύκολη απομάκρυνση των δεδομένων από τον οργανισμό και σε μια απομακρυσμένη τοποθεσία. Μόλις εισέλθει, ο επιτιθέμενος χαρτογραφεί τα συστήματα του οργανισμού και ανιχνεύει αυτόματα για εμπιστευτικά δεδομένα ή, στην περίπτωση ορισμένων APTs, επιχειρησιακές οδηγίες και λειτουργικότητα. Η ανακάλυψη μπορεί να περιλαμβάνει μη προστατευμένα δεδομένα και δίκτυα καθώς και ευπάθειες λογισμικού και υλικού, εκτεθειμένα διαπιστευτήρια και διαδρομές σε πρόσθετους πόρους ή σημεία πρόσβασης. Εδώ και πάλι, όπου οι πιο στοχευμένες επιθέσεις είναι ευκαιριακές, οι επιθέσεις APT είναι πιο μεθοδικές για να αποφευχθεί η ανίχνευση.

Το APT έχει σχεδιαστεί για να συλλαμβάνει πληροφορίες για μεγάλο χρονικό διάστημα. Για παράδειγμα, μια επιχείρηση μεγάλης κλίμακας κατασκοπείας που ονομάζεται GhostNet, που ανακαλύφθηκε τον Μάρτιο του 2009, μπόρεσε να διεισδύσει σε συστήματα υπολογιστών σε 103 χώρες, συμπεριλαμβανομένων των πρεσβειών, των υπουργείων εξωτερικών και άλλων κυβερνητικών γραφείων, και των κέντρων εξορίας του Θιβέτ στο Ινδία. Σύμφωνα με μια αναφορά του Warfare Monitor, το GhostNet άρχισε να συλλαμβάνει δεδομένα στις 22 Μαΐου 2007 και συνέχισε τουλάχιστον μέχρι τις 12 Μαρτίου 2009. Κατά μέσο όρο, ο χρόνος που ένας οικοδεσπότης ήταν μολυσμένος ενεργά από ένα APT ήταν 145 ημέρες, με το μεγαλύτερο χρονικό διάστημα μόλυνσης να είναι 660 ημέρες (Raviadaran et al., 2019).

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

2.5.3. Phishing (Ηλεκτρονικό ψάρεμα)

Μια ψηφιακή μορφή κοινωνικής μηχανικής που χρησιμοποιεί αυθεντικά, αλλά ψεύτικα, ηλεκτρονικά μηνύματα για να ζητήσει πληροφορίες από χρήστες ή να τα κατευθύνει σε έναν ψεύτικο ιστότοπο που ζητά πληροφορίες. Οι επιθέσεις " phishing " χρησιμοποιούνται συχνά από άτομα που διεξάγουν στοχευμένες και όχι ευκαιριακές επιθέσεις(Gao, 2015).

Υπάρχουν διάφορες τεχνικές ηλεκτρονικού "ψαρέματος", συμπεριλαμβανομένου του phishing για τα διαπιστευτήρια, ή για κωδικούς πρόσβασης, ή κωδικούς ταυτοποίησης μίας χρήσης- OTP. Επίσης, εκτός από το phishing, χρησιμοποιούνται και οι όροι «smishing» και "vishing", οι οποίοι αφορούν ειδικά στο phishing μέσω μηνυμάτων (SMS) ή φωνητικών καναλιών. Η συντριπτική πλειονότητα των περιπτώσεων ηλεκτρονικού "ψαρέματος" υιοθετεί μία από τις παρακάτω προσεγγίσεις:

• Ένα μήνυμα ηλεκτρονικού ταχυδρομείου ή ένα μήνυμα SMS προέρχεται από έναν αξιόπιστο οργανισμό με έναν σύνδεσμο που φαίνεται να οδηγεί στη σελίδα σύνδεσης αυτής της ιστοσελίδας του οργανισμού.

• Ένα αναδυόμενο παράθυρο ή μια επικάλυψη σε έναν υπολογιστή ή μια κινητή συσκευή προκαλεί-ωθεί τους χρήστες να εκθέσουν διαπιστευτήρια, δεδομένα κάρτας ή άλλες ευαίσθητες πληροφορίες προς ένα ψεύτικο περιβάλλον χρήστη. Μια τυπική διαδικασία εξαπάτησης (ηλεκτρονικού ψαρέματος/phishing) μπορεί να εκτελεστεί ως εξής:

Ο απατεώνας μπορεί να προσποιηθεί μια δημόσια αρχή (π.χ. Αστυνομικός) και να στείλει κάποιο Email ότι κινδυνεύει να διωχθεί ποινικά αν δεν στείλει άμεσα κάποιο χρηματικό ποσό. Πολλές φορές, το θύμα εμπιστεύεται τον κακόβουλο χρήστη και τελικά στέλνει χρήματα π.χ. με χρήση Western Union ή bitcoin ώστε να μην εντοπιστεί

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ο παραλήπτης/ κακόβουλος χρήστης. Αυτός ο ψυχολογικός συνδυασμός του επείγοντος, και ο φόβος της απώλειας χρημάτων και η ευγενική εξυπηρέτηση μπορεί να ξεπεράσουν την καχυποψία και την απροθυμία του στόχου/θύματος να εκθέσει κωδικούς ή διαπιστευτήρια.

2.5.4. Malware (κακόβουλο λογισμικό)

Κακόβουλο λογισμικό που έχει σχεδιαστεί για την εκτέλεση ενοχλητικών ή επιβλαβών ενεργειών. Μόλις εγκατασταθεί, το κακόβουλο λογισμικό συχνά μπορεί να μετατραπεί σε χρήσιμα προγράμματα ή να ενσωματωθεί σε χρήσιμα προγράμματα, έτσι ώστε οι χρήστες να προκληθούν στην ενεργοποίηση του προγράμματος και έτσι να εξαπλωθεί το κακόβουλο λογισμικό σε άλλες συσκευές. Ένα κακόβουλο λογισμικό μπορεί να ανήκει στις παρακάτω υποκατηγορίες:

Trojan Horse: Ένα πρόγραμμα υπολογιστή που φαίνεται να έχει μια χρήσιμη λειτουργία, αλλά έχει επίσης κρυμμένη και δυνητικά κακόβουλη λειτουργία, η οποία αποφεύγει τους μηχανισμούς ασφαλείας. για παράδειγμα, με τη μεταμφίεση ως ένα χρήσιμο πρόγραμμα που ένας χρήστης θα μπορούσε να εκτελέσει (Gao, 2015).

Ιός (Virus): Ένα πρόγραμμα υπολογιστή που μπορεί να αντιγραφεί και να μολύνει έναν υπολογιστή χωρίς την άδεια ή τη γνώση του χρήστη. Ένας ιός μπορεί να καταστρέψει ή να διαγράψει δεδομένα σε έναν υπολογιστή, να χρησιμοποιήσει προγράμματα ηλεκτρονικού ταχυδρομείου για να εξαπλωθεί σε άλλους υπολογιστές ή να διαγράψει τα πάντα σε έναν σκληρό δίσκο. Σε αντίθεση με ένα σκουλήκι υπολογιστή (worm), ένας ιός απαιτεί την ανθρώπινη ανάμιξη (συνήθως άγνοια) για να διαδοθεί. (Bushin, 2017).

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Τα τελευταία χρόνια μπορούμε να αναφέρουμε ότι τα είδη των κακόβουλων λογισμικών/προγραμμάτων έχουν αυξηθεί διευρύνοντας τις δυνατότητες καθώς και το εύρος δράσης τους. Μεταξύ άλλων τα συνηθέστερα είναι τα spywares, ransomwares, worms, adwares, fileless malwares,hybrids, exotic forms και άλλα.

2.5.5. Botnet

Ένα δίκτυο ελεγχόμενων εξ αποστάσεως συστημάτων που χρησιμοποιούνται για τον συντονισμό των επιθέσεων και τη διανομή κακόβουλων προγραμμάτων, spam και απατών ηλεκτρονικού "ψαρέματος".Τα ρομπότ(bots)είναι προγράμματα που είναι κρυφά εγκατεστημένα σε ένα στοχευμένο σύστημα που επιτρέπει σε έναν μη εξουσιοδοτημένο χρήστη να ελέγχει εξ αποστάσεως τον υποβαθμισμένο υπολογιστή για διάφορους κακόβουλους σκοπούς(Gao, 2015).

2.5.6. Spamming

Αποστολή ανεπιθύμητων διαφημίσεων μέσω ηλεκτρονικού ταχυδρομείου για προϊόντα, υπηρεσίες και ιστότοπους. Το Spam μπορεί επίσης να χρησιμοποιηθεί ως μηχανισμός παράδοσης για κακόβουλο λογισμικό και άλλες απειλές στον κυβερνοχώρο.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

2.5.7. Spoofing

Ο όρος αυτός αναφέρεται στην χειραγώγηση με τέτοιο τρόπο της επικοινωνίας μεταξύ 2 οντοτήτων ώστε να φαίνεται πως είναι απολύτως νόμιμη και κανονική. Περιπτώσεις spoofingείναι μεταξύ άλλων η δημιουργία ενός ψεύτικου ιστότοπου, προφίλ, χρήστη, συστήματος που μιμείται έναν πραγματικό αλλά εκτελείται από ένα άλλο μέρος. Φυσικά το spoofingμπορεί να εφαρμοστεί και σε πολύ πιο τεχνικά στοιχεία της επικοινωνίας 2 οντοτήτων όπως είναι η ip διεύθυνση, η φυσική διεύθυνση των συστημάτων κτλ. Το spoofing γίνεται αντιληπτό και στην επικοινωνίας ηλεκτρονικού ταχυδρομείου εμφανίζεται όταν η διεύθυνση του αποστολέα και άλλα τμήματα μιας κεφαλίδας ηλεκτρονικού ταχυδρομείου τροποποιούνται ώστε να εμφανίζονται σαν να προέρχονται τα μηνύματα ηλεκτρονικού ταχυδρομείου από διαφορετική πηγή.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

2.6 Κίνδυνοι και Απειλές Ασφαλείας Εφαρμογών Διαδικτύου

Οι παραπάνω κατηγορίες απειλών αποτελούν μόνο λίγες από τις ήδη υπάρχουσες και αναφέρονται κυρίως σε απειλές που αφορούν τραπεζικά συστήματα, τραπεζικές εφαρμογές σε κινητά τηλέφωνα και διαδικτυακές πλατφόρμες. Προκειμένου να αναλύσουμε σε μεγαλύτερο βαθμό τις απειλές των διαδικτυακών εφαρμογών κρίνεται απαραίτητο να αναφερθούμε στις 10 πιο σημαντικές κατηγορίες απειλών που αναφέρει ο OWASP (Owasp.org, 2017):

1. Injection

Αναφερόμαστε σε μη εξουσιοδοτημένη εκτέλεση ερωτημάτων σε βάσεις και συστήματα οργάνωσης-αποθήκευσης δεδομένων όπως sql, nosql, OS, LDAP κτλ, με σκοπό την αποστολή δεδομένων για αλλαγή, ερώτηση για εμφάνιση δεδομένων ή και την πρόκληση αλλαγών στα αξιόπιστα δεδομένα των εν λόγω συστημάτων. Τα δεδομένα που αποστέλλονται από τον κακόβουλο χρήστη ή εισβολέα μπορούν να εξαπατήσουν τον διερμηνέα του εκάστοτε συστήματος να εκτελέσει ακούσιες εντολές ή να αποκτήσει πρόσβαση σε δεδομένα χωρίς την κατάλληλη εξουσιοδότηση.

Threat Agents

Σε αυτή την κατηγορία απειλή αποτελεί κάθε πηγή δεδομένων όπως μεταβλητές του συστήματος, παράμετροι, εξωτερικές και εσωτερικές διαδικτυακές υπηρεσίες καθώς και όλοι οι τύποι των χρηστών. Η υλοποίηση τέτοιου είδους απειλής μπορεί να λάβει χώρα όταν κάποιος επιτιθέμενος αποστείλει στον εκάστοτε διερμηνέα του συστήματος δεδομένα που αποσκοπούν σε κακόβουλο σκοπό.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

2. Broken Authentication

Οι λειτουργίες εφαρμογής που σχετίζονται με την αυθεντικοποίηση και τη διαχείριση περιόδου λειτουργίας και χρήσης της συνόδου επικοινωνίας μεταξύ περιηγητή και εξυπηρετητή συχνά εφαρμόζονται λανθασμένα, επιτρέποντας στους εισβολείς να θέσουν σε κίνδυνο κωδικούς πρόσβασης, κλειδιά ή διακριτικά περιόδου σύνδεσης ή να εκμεταλλευτούν άλλα ελαττώματα εφαρμογής για να χρησιμοποιήσουν προσωρινά ή μόνιμα τις ταυτότητες άλλων χρηστών.

Threat Agents

Σε αυτή την κατηγορία απειλή αποτελεί το γεγονός ότι οι επίδοξοι κακόβουλοι ή επιτιθέμενοι έχουν πρόσβαση σε εκατοντάδες εκατομμύρια συνδυασμούς έγκυρων κωδικών και ονομάτων χρηστών σε βάσεις αποθήκευσης διαπιστευτηρίων, λίστες προεπιλεγμένων διαχειριστικών λογαριασμών, εργαλεία χρήση λεξιλογίου καθώς και βίαιης εξεύρεσης κωδικών. Οι επιθέσεις που σχετίζονται με την διαχείριση της συνόδου είναι πλήρως κατανοητές ιδιαίτερα σε σχέση με τις συνόδους επικοινωνίας που βασίζονται σε tokens τα οποία δεν λήγουν.

3. Sensitive Data Exposure

Πολλές εφαρμογές ιστού και API δεν προστατεύουν σωστά ευαίσθητα δεδομένα, όπως οικονομικά, υγειονομική περίθαλψη και PII. Οι εισβολείς ενδέχεται να κλέψουν ή να τροποποιήσουν τέτοια ασθενώς προστατευμένα δεδομένα για να διαπράξουν απάτη με πιστωτική κάρτα, κλοπή ταυτότητας ή άλλα εγκλήματα. Τα ευαίσθητα δεδομένα ενδέχεται να παραβιαστούν χωρίς επιπλέον προστασία, όπως είναι η κρυπτογράφηση σε δεδομένα σε βάσεις δεδομένων και σε δίσκους ή και δεδομένα που μεταφέρονται. Προκειμένου να προστατευτούμε από την εν λόγω απειλή

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

απαιτούνται πολλές ειδικές προφυλάξεις κατά την ανταλλαγή με το πρόγραμμα περιήγησης αλλά και αναφορικά με τον τρόπο ασφαλής μεταφοράς και αποθήκευσης των δεδομένων αυτών.

Threat Agents

Σε αυτή την κατηγορία οι επιτιθέμενοι – κακόβουλοι χρήστες, αντί να επιτεθούν απευθείας στα συστήματα, κλέβουν κλειδιά, εκτελούν man in the middle attacks, η κλέβουν μη κρυπτογραφημένα δεδομένα απευθείας από τους εξυπηρετητές ενώ αυτά βρίσκονται σε μεταφορά είτε σε κάποιο τερματικό χρήστη π.χ περιηγητής.

4. XML External Entities (XXE)

Πολλοί παλαιότεροι ή μη επαρκώς παραμετροποιημένοι επεξεργαστές XML αξιολογούν εξωτερικές αναφορές οντοτήτων εντός εγγράφων XML. Οι εξωτερικές οντότητες μπορούν να χρησιμοποιηθούν για την αποκάλυψη εσωτερικών αρχείων χρησιμοποιώντας το χειριστή URI αρχείων, εσωτερικές κοινοποιήσεις αρχείων, σάρωση εσωτερικής θύρας, εκτέλεση απομακρυσμένου κώδικα και επιθέσεις άρνησης υπηρεσίας.

Threat Agents

Σε αυτή την περίπτωση οι επιτιθέμενοι μπορούν να εκμεταλλευθούν αδυναμίες σε επεξεργαστές XML αν μπορούν να μεταφορτώσουν αρχεία XML ή να συμπεριλάβουν κακόβουλο περιεχόμενο σε ένα έγγραφο XML εκμεταλλευόμενοι ευάλωτο – μη ασφαλή κώδικα, εξαρτήσεις αυτού ή ενσωματώσεις.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

5. Broken Access Control

Οι περιορισμοί σχετικά με το τι επιτρέπεται να κάνουν οι επικυρωμένοι χρήστες συχνά δεν εφαρμόζονται σωστά. Οι εισβολείς μπορούν να εκμεταλλευτούν αυτά τις αδυναμίες-ελαττώματα για να αποκτήσουν πρόσβαση σε μη εξουσιοδοτημένη λειτουργικότητα ή / και δεδομένα, όπως πρόσβαση σε λογαριασμούς άλλων χρηστών, προβολή ευαίσθητων αρχείων, τροποποίηση δεδομένων άλλων χρηστών, αλλαγή δικαιωμάτων πρόσβασης κ.λπ.

Threat Agents

Η εκμετάλλευση του ελέγχου εισόδου αποτελεί ένα από μία από τις βασικές δυνατότητες των επιτιθέμενων. Τα εργαλεία SAST και DAST έχουν την δυνατότητα να εντοπίσουν την απουσία ελέγχου εισόδου αλλά δεν μπορούν να πιστοποιήσουν αν είναι λειτουργικός όταν υφίσταται. Αν είναι λειτουργικός, ο έλεγχος εισόδου είναι ανιχνεύσιμος χρησιμοποιώντας χειροκίνητα μέσα και μεθόδους είτε πιθανώς μέσω αυτοματοποίησης αλλά για την απουσία ελέγχου μόνο σε συγκεκριμένα πλαίσια και δομές.

6. Security Misconfiguration

Η εσφαλμένη είτε ελλιπής παραμετροποίηση ασφαλείας είναι το πιο συχνό πρόβλημα. Αυτό είναι συνήθως αποτέλεσμα μη ασφαλών προεπιλεγμένων ρυθμίσεων, ελλιπείς ή κατά περίπτωση – περιστασιακών παραμετροποιήσεων, απομακρυσμένου χώρου αποθήκευσης χωρίς εξασφάλιση της ασφάλειας, εσφαλμένης παραμετροποίησης Κεφαλίδων HTTP και αναλυτικών-λεπτομερών μηνυμάτων σφάλματος που περιέχουν ευαίσθητες πληροφορίες. Όχι μόνο πρέπει όλοι τα λειτουργικά συστήματα, τα πλαίσια,

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

οι βιβλιοθήκες και οι εφαρμογές να παραμετροποιηθούν με ασφάλεια, αλλά πρέπει γίνει αναβαθμίσεις και ενημερώσεις ασφαλείας ανά τακτά χρονικά διαστήματα.

Threat Agents

Οι επιτιθέμενοι συχνά προσπαθούν να εκμεταλλευτούν μη διορθωμένα ελαττώματα ή λογαριασμούς προεπιλεγμένη πρόσβαση, σελίδες που δεν χρησιμοποιούνται, αρχεία χωρίς προστασία και απροστάτευτους καταλόγους και συστήματα αρχείων κ.λπ. για να κερδίσουν μη εξουσιοδοτημένη πρόσβαση ή να αποκτήσουν γνώση συστήματος.

7. Cross Site Scripting (XSS)

Ευπάθειες XSS εμφανίζονται κάθε φορά που μια εφαρμογή περιλαμβάνει μη αξιόπιστα δεδομένα σε μια νέα ιστοσελίδα χωρίς κατάλληλη επικύρωση ή ενημερώνει μια υπάρχουσα ιστοσελίδα με δεδομένα που παρέχονται από τον χρήστη χρησιμοποιώντας ένα API προγράμματος περιήγησης που μπορεί να δημιουργήσει HTML ή JavaScript. Το XSS επιτρέπει στους εισβολείς να εκτελούν κώδικα στο πρόγραμμα περιήγησης του θύματος που μπορεί να εισβάλει παράνομα σε συνόδους σύνδεσης χρηστών, να παραμορφώσεις ή να μιμηθεί ιστότοπους ή ακόμα να ανακατευθύνει τον χρήστη σε κακόβουλους ιστότοπους.

Threat Agents

Αυτοματοποιημένα εργαλεία μπορούν να εντοπίσουν και εκμεταλλευτούν και τις τρεις μορφές XSS, και υπάρχει ελεύθερα διαθέσιμα πλαίσια εκμετάλλευσης

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

8. Insecure Deserialization

Η επισφαλής μετατροπή του κώδικά και των δεδομένων στο αρχικό αντικείμενο οδηγεί συχνά σε απομακρυσμένη εκτέλεση κώδικα. Ακόμα κι αν οι ατέλειες της εν λόγω μετατροπής δεν καταλήγουν σε απομακρυσμένη εκτέλεση κώδικα, μπορούν να χρησιμοποιηθούν για την εκτέλεση επιθέσεων, επιθέσεων επανάληψης αποστολής συγκεκριμένων – επιλεγμένων πακέτων επικοινωνίας , επιθέσεις μη εξουσιοδοτημένης αποστολής δεδομένων στις βάσεις και στο σύστημα και επιθέσεις κλιμάκωσης προνομίων.

Threat Agents

Η εκμετάλλευση της παραπάνω μετατροπής είναι κάπως δύσκολη, όπως και οι εκμεταλλεύσεις του συστήματός μας σπάνια λειτουργούν χωρίς αλλαγές ή τροποποιήσεις στον υποβόσκων εκμεταλλεύσιμο κώδικα.

9. Using Components with Known Vulnerabilities

Επιμέρους στοιχεία, όπως βιβλιοθήκες, πλαίσια και άλλες λειτουργικές μονάδες του λογισμικού, λειτουργούν με το ίδια προνόμια και δικαιώματα όπως οι εφαρμογές. Εάν ένα ευάλωτο στοιχείο των παραπάνω κατηγοριών αξιοποιηθεί με κακόβουλο τρόπο, μια τέτοια επίθεση μπορεί να διευκολύνει σε σοβαρή απώλεια δεδομένων ή ακόμα και την κατάληψη του διακομιστή. Εφαρμογές και API που χρησιμοποιούν στοιχεία με γνωστές ευπάθειες και αδυναμίες ενδέχεται να υπονομεύσουν την άμυνα των εφαρμογών και να επιτρέψουν διάφορες επιθέσεις και επιπτώσεις.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Threat Agents

Ενώ είναι εύκολο να το βρεθούν έτοιμοι γραμμένοι τρόποι εκμετάλλευσης διαφόρων γνωστών ευπαθειών και αδυναμιών συστημάτων, άλλες ευπάθειες απαιτούν συγκεντρωμένη και μεγαλύτερη προσπάθεια για αναπτύξει κανείς έναν προσαρμοσμένο τρόπο εκμετάλλευσης.

10. Insufficient Logging & Monitoring

Ανεπαρκής καταγραφή και παρακολούθηση των ενεργειών και της πληροφορίας, σε συνδυασμό με ελλιπή ή αναποτελεσματική συσχέτιση των παραπάνω με τις ενέργειες που λαμβάνονται στα διάφορα περιστατικά του συστήματος, επιτρέπει στους επιτιθέμενους να διεξάγουν περαιτέρω επιθέσεις, να διατηρούν τις επιθέσεις τους για μεγάλα χρονικά διαστήματα, να εισέρχονται σε περισσότερα συστήματα, να υλοποιούν παραβίαση, εξαγωγή ή καταστροφή δεδομένων. Οι περισσότερες μελέτες που σχετίζονται με την παραβίαση δεδομένων δείχνουν ότι ο χρόνος εντοπισμού μιας παραβίασης μπορεί να ξεπερνά και τις 200 ημέρες. Συνήθως ανιχνεύονται από τρίτες εξωτερικές οντότητες και όχι από εσωτερικές διαδικασίες ή μέσω παρακολούθησης των συστημάτων.

Threat Agents

Η Εκμετάλλευση ανεπαρκούς καταγραφής και η παρακολούθηση των συστημάτων αποτελεί το θεμέλιο σχεδόν για κάθε σοβαρό περιστατικό. Οι επιτιθέμενοι στηρίζονται στην έλλειψη παρακολούθησης και έγκαιρη ανταπόκρισης για να επιτύχουν τους στόχους τους χωρίς να γίνουν αντιληπτοί

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ΚΕΦΑΛΑΙΟ 3- ΤΟ Mobile Banking

3.1. Τι είναι το Mobile Banking

Η κινητή τραπεζική (Mobile Banking), είναι ένα σύστημα που επιτρέπει στους πελάτες ενός χρηματοπιστωτικού ιδρύματος να πραγματοποιήσουν μια σειρά χρηματοπιστωτικών συναλλαγών μέσω με την χρήση κάποιας κινητής συσκευής όπως ένα κινητό τηλέφωνο ή ένα προσωπικός ψηφιακός βοηθός ή ένα tablet. Για να μην υπάρξει σύγχυση, θα πρέπει να διευκρινιστεί ότι το Mobile banking δεν είναι οι πληρωμές που γίνονται εξ αποστάσεως, με την χρήση χρεωστικών ή πιστωτικών καρτών, μέσω των συστημάτων EFTPOS. Το Mobile Banking αναφέρεται σε χρήση χρηματοοικονομικών υπηρεσιών και συναλλαγών, και προϋποθέτει ο χρήστης να έχει μια κινητή συσκευή, λήψη της απαραίτητης εφαρμογής (application) και εγγραφή, πιστοποίηση και αυθεντικοποίηση του χρήση από την τράπεζα για την πρόσβαση τους στην εφαρμογή mobile banking.

Η πρώτη μορφή του mobile banking, ξεκίνησε το 1997 , με την ονομασία SMS Banking, στην οποία ο χρήστης είχε την δυνατότητα να αποστείλει SMS από το κινητό του τηλέφωνο (αφού είχε πιστοποιηθεί πρώτα από την τράπεζα), και με αυτόν τον τρόπο έδινε εντολή για την πραγματοποίηση χρηματοοικονομικής συναλλαγής. Λίγο αργότερα, το 1999 , όταν ξεκίνησε η χρήση πιο εξελιγμένων κινητών τηλεφώνων, με υποστήριξη WAP, και την εξάπλωση των υπηρεσιών και τεχνολογιών web, το Mobile banking άρχισε να παίρνει σιγά-σιγά την σημερινή μορφή του.

Συνεπώς, ορίζοντας το Mobile Banking, είναι η παροχή και αξιοποίηση τραπεζικών και χρηματοοικονομικών υπηρεσιών με τη βοήθεια συσκευών κινητής τηλεφωνίας και την χρήση ειδικών εφαρμογών ή πλατφορμών. Το εύρος των προσφερόμενων υπηρεσιών μπορεί να περιλαμβάνει διευκολύνσεις για τραπεζικές και

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

χρηματιστηριακές συναλλαγές, διαχείριση λογαριασμών και πρόσβαση σε προσαρμοσμένες πληροφορίες

Όπως συμβαίνει στο Web Banking, έτσι και στο mobile banking, υπάρχουν αρκετά ζητήματα που αφορούν την προστασία των προσωπικών δεδομένων, και την ασφάλεια της εκτέλεσης των συναλλαγών.

3.2. Πλεονεκτήματα - Μειονεκτήματα της κινητής τραπεζικής

Τα σημαντικότερα πλεονεκτήματα, από την χρήση του mobile banking είναι τα ακόλουθα:

Εξοικονόμηση χρόνου: Αντί ο χρήστης να ξοδεύει χρόνο για την μετάβαση σε κάποιο υποκατάστημα τράπεζας και τον χρόνο αναμονής στις ουρές των ταμείων, μπορεί απλά να εγγραφεί στην αντίστοιχη υπηρεσία mobile banking και με αυτό τον τρόπο να πραγματοποιήσει σχεδόν όλες τις χρηματοπιστωτικές συναλλαγές μέσα από τις επιλογές της εφαρμογής (Kavitha, 2015).

Απομακρυσμένη Διαχείριση: Σήμερα, οι τράπεζες έχουν δώσει την δυνατότητα, στους πελάτες τους, να κάνουν μεταφορές χρημάτων, άνοιγμα online λογαριασμών, επένδυση στο χρηματιστήριο, online, πληρωμές λογαριασμών, αιτήσεις για πιστωτικές κάρτες ακόμη και online αιτήσεις για την λήψη δανείων. Συνεπώς, δεν απαιτείται η μετάβαση του πελάτη και η φυσική παρουσία του σε κάποια τράπεζα, έτσι μπορεί με το πάτημα μερικών κουμπιών να πραγματοποιήσει σχεδόν κάθε υπηρεσία που θα του παρέχονταν σε κάποιο φυσικό κατάστημα τράπεζας (Kavitha, 2015).

Ασφάλεια: Σήμερα, όπως είναι γνωστό στους περισσότερους χρήστες, η ασφάλεια του mobile banking έχει εξελιχθεί, και σχεδόν σε όλες τις συναλλαγές απαιτείται κωδικός μιας χρήσης (OTP)που αποστέλλεται στον πιστοποιημένο αριθμό

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

κινητού τηλεφώνου. Με αυτόν τρόπο, εξασφαλίζεται ότι δεν θα γίνουν μη εξουσιοδοτημένες συναλλαγές. Και ο χρήστης μπορεί να νιώθει ασφαλής.

24ωρη πρόσβαση: Ο χρήστης που διαθέτει υπηρεσία Mobile Banking, μπορεί όποια ώρα της ημέρας το επιθυμεί, να πραγματοποιήσει οποιαδήποτε συναλλαγή. Στην πλειοψηφία των περιπτώσεων οι συναλλαγές γίνονται άμεσα και σε πραγματικό χρόνο. Αντίθετα, όπως είναι γνωστό, το ωράριο των τραπεζικών καταστημάτων είναι συγκεκριμένο, και όποιος δεν διαθέτει mobile banking ή web banking δεν μπορεί να κάνει αρκετές συναλλαγές (Lee et al., 2013).

Ταχύτητα Συναλλαγών: Ένα άλλο πλεονέκτημα θα μπορούσαμε να δεχτούμε την ευκολία χρήσης και την ταχύτητα των συναλλαγών. Όλα τα προϊόντα που προσφέρει η τράπεζα είναι συγκεντρωμένα σε μια ιστοσελίδα. Με ένα απλό πάτημα κουμπιού μπορεί να ολοκληρωθεί μια χρονοβόρα διαδικασία, οπως η πληρωμή ενός λογαριασμού ή καταχώρηση αίτησης για δάνειο. Ο χρήστης έτσι γλιτώνει και χρόνο και κόπο ακόμα και σε σχέση με τη χρήση του ATM για την διεξαγωγή συναλλαγών (Lee et al., 2013).

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Μειονεκτήματα της κινητής τραπεζικής

Από την άλλη πλευρά, η χρήση του Mobile Banking, έχει ορισμένα μειονεκτήματα, και ενέχει ορισμένους κινδύνους. Ειδικότερα:

Κίνδυνος Απάτης: Οι χρήστες κινητών τραπεζών κινδυνεύουν να λάβουν ψεύτικα μηνύματα SMS και μπορεί να εξαπατηθεί και να γίνουν παράνομες συναλλαγές (Chawla et al., 2012).

Περίπτωση απώλειας ή κλοπής της κινητής συσκευής: Σε περίπτωση απώλειας ή κλοπής της κινητής συσκευής του κατόχου, υπάρχει και εδώ, περίπτωση να πραγματοποιηθούν μη εξουσιοδοτημένες συναλλαγές.

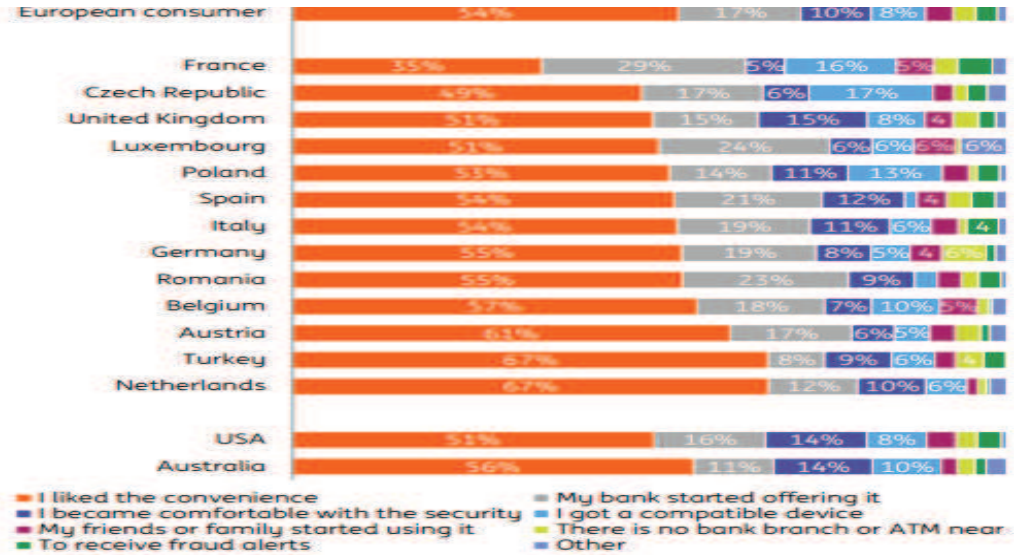
Ασυμβατότητα κινητών συσκευών: Οι χρήστες κινητών συσκευών, υπάρχει περίπτωση να διαθέτουν κινητή συσκευή που δεν είναι συμβατή με τις εφαρμογές Mobile Banking των τραπεζών τους. Για παράδειγμα, πολλοί άνθρωποι σήμερα δεν διαθέτουν έξυπνα τηλέφωνα, ή διαθέτουν έξυπνα τηλέφωνα που το λειτουργικό τους σύστημα είναι απαρχαιωμένο και χρειάζεται ή να γίνει ενημέρωση ή αρκετές φορές να αγοράσουν μια νέα πιο εξελιγμένη συσκευή (Chawla et al., 2012).

Επίπεδο ασφάλειας: Ορισμένες τράπεζες δεν προσφέρουν το ίδιο επίπεδο προστασίας για τις τραπεζικές υπηρεσίες κινητής τηλεφωνίας που κάνουν για ηλεκτρονικές συναλλαγές ή για προσωπικές συναλλαγές. Επειδή οι κίνδυνοι εξακολουθούν να είναι εν γένει άγνωστοι, ορισμένες τράπεζες αργούν να κάνουν υποσχέσεις σχετικά με το τι θα καλύψει ή δεν θα καλύψει όταν χρησιμοποιούμε τραπεζικές υπηρεσίες Mobile Banking (Ahmad et al., 2011).

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

3.3. Η Τρέχουσα κατάσταση του Mobile Banking

Είναι γνωστό, ότι σήμερα, σχεδόν όλοι οι χρήστες διαθέτουν ένα έξυπνο τηλέφωνο. Για παράδειγμα σύμφωνα με έρευνα της ING (2017), στην οποία συμμετείχαν 8000 άτομα, στην Ευρώπη, το 86% των χρηστών διαθέτει ένα smartphone[2]. Επίσης, από τους χρήστες που έχουν στην κατοχή τους ένα έξυπνο τηλέφωνο, το 58% έχουν τουλάχιστον μία εγκαταστημένη μια εφαρμογή τραπεζικής, δηλαδή εφαρμογή Mobile Banking εφαρμογή. Στην ερώτηση, ποιος ήταν ο βασικός λόγος για τον οποίο οι χρήστες ξεκίνησαν να κάνουν χρήση του Mobile Banking, Οι περισσότεροι χρήστες δήλωσαν ότι είναι βολικός τρόπος (σχήμα).



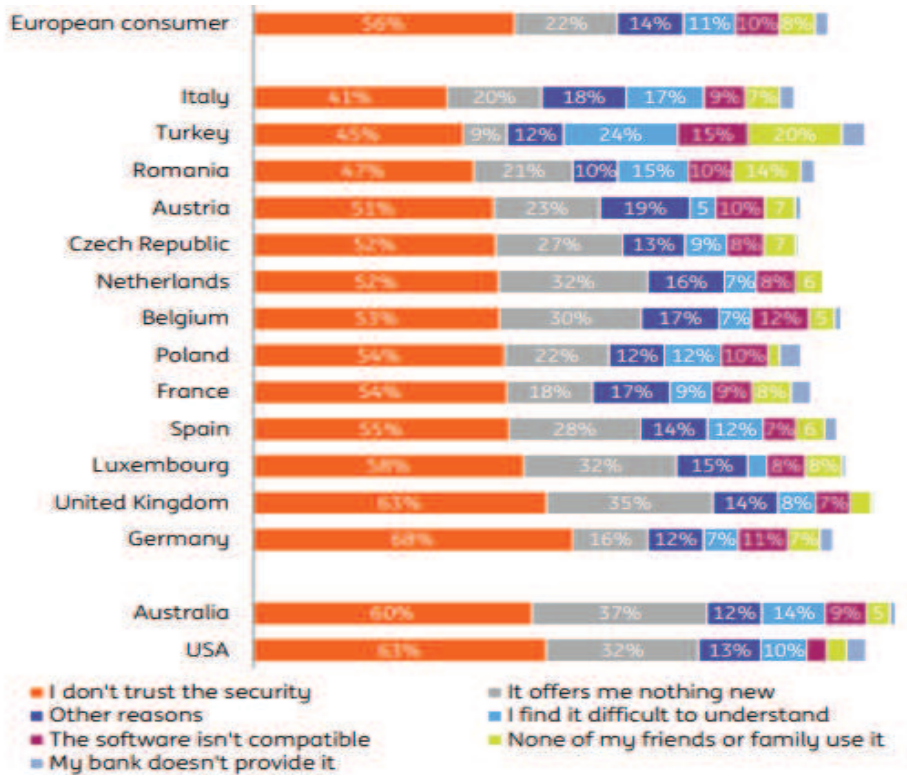
Σχήμα 2- Ποιος είναι ο βασικός λόγος που ξεκινήσατε να κάνατε χρήση του Mobile Banking , Απαντήσεις ανά χώρα

Πηγή: ING(2017)

[2] ING International Survey Mobile Banking 2017 – Newer Technologies May 2017

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Ένα άλλο σημαντικό στοιχείο από την έρευνα, είναι το γεγονός, ότι από τον αριθμό των χρηστών που δεν χρησιμοποιούν το Mobile Banking, το 56% πιστεύει ότι η χρήση του Mobile Banking δεν είναι ασφαλής, και είναι ένας από τους σημαντικότερους λόγους που διστάζουν να κάνουν χρήση του Mobile Banking. Ειδικότερα, το σχήμα , παρουσιάζει τον βασικό λόγο, για τον οποίο οι χρήστες δεν χρησιμοποιούν το Mobile Banking



Σχήμα 3- Βασικός λόγος για την αποφυγή χρησιμοποίησης του Mobile Banking, απαντήσεις ανά χώρα

Πηγή: ING (2017)

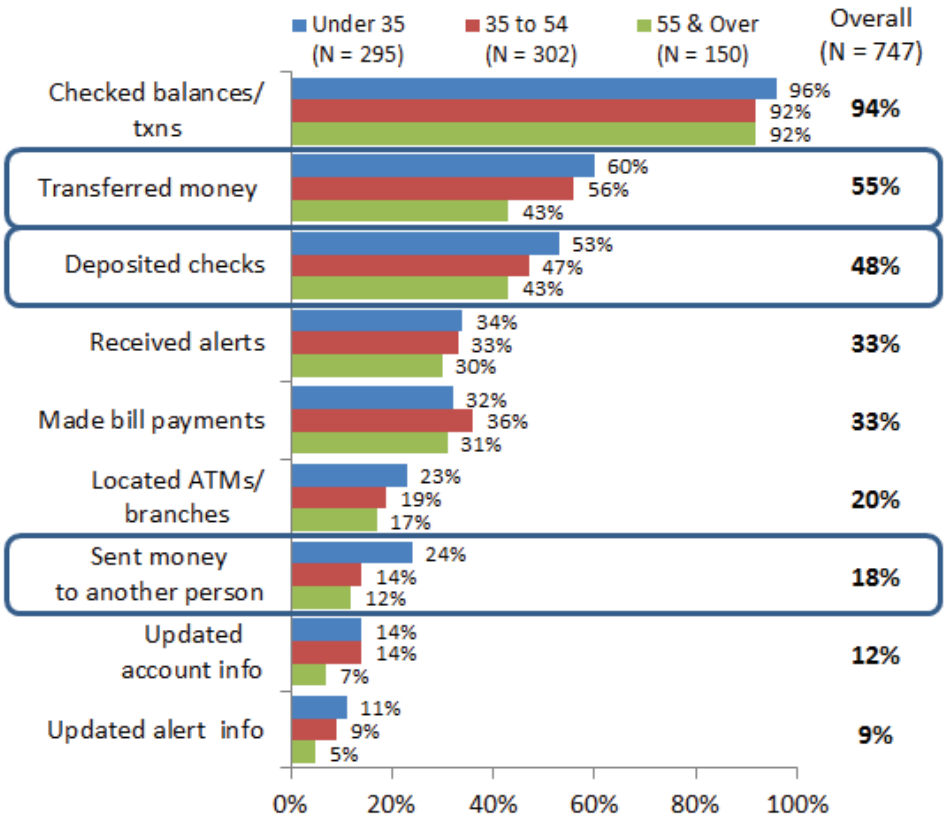
ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Σε άλλη έρευνα που πραγματοποιήθηκε στις ΗΠΑ το 2017, το 8% των χρηστών smartphone των ΗΠΑ έχουν κατεβάσει μια εφαρμογή κινητής τηλεφωνίας για τον κύριο λογαριασμό ελέγχου και το 50% των χρηστών smartphone των ΗΠΑ (συμπεριλαμβανομένων 68% εκείνων κάτω των 35 και 31% των 55 ετών και άνω) είναι ενεργοί χρήστες. Το 75% των χρηστών κινητών τραπεζών συνδέονται εβδομαδιαίως, κυρίως για να ελέγξουν τα υπόλοιπα / το ιστορικό συναλλαγών τους. Τα ευρήματα βασίζονται σε αποτελέσματα της έρευνας του Απριλίου 2017 για 1.503 Αμερικανούς καταναλωτές ηλικίας 18 ετών και άνω, οι οποίοι έχουν smartphone και τραπεζικές σχέσεις.

Τα ευρήματα από τη μελέτη δείχνουν ότι (σχήμα 4) :

1. Το mobile banking, επεκτείνεται από ένα παθητικό κανάλι παρακολούθησης σε ένα ενεργό κανάλι συναλλαγών.
2. Ο κύριος λόγος για τον οποίο οι χρήστες συνδέονται σε εφαρμογές Mobile Banking, την κινητή τραπεζική είναι να ελέγξουν τα υπόλοιπα ή / και το ιστορικό συναλλαγών τους, που αναφέρονται από το 95% + χρηστών κινητών τραπεζών.
3. Οι νεότεροι χρήστες κινητών τραπεζών επιδεικνύουν μεγαλύτερη προθυμία διαπραγμάτευσης μέσω της κινητής τραπεζικής, ωστόσο: είναι πιθανότερο να έχουν καταθέσει επιταγές, να μεταφέρουν κεφάλαια και να αποστέλλουν πληρωμές μέσω P2P.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ



Σχήμα 4- Ποσοστά χρηστών του Mobile Banking ανά χρηματοοικονομική δραστηριότητα που πραγματοποιούν

Πηγή: mobile payments world(2017)

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

3.4. Προκλήσεις και ζητήματα σε θέματα ασφάλειας του Mobile Banking

Όπως έχουμε αναφέρει ξανά το Mobile Banking είναι βολικό για τους χρήστες, και για αυτό το λόγο, πολλοί χρήστες το προτιμούν ακόμη και περισσότερο από το Web Banking. Ωστόσο, η ευρεία χρήση των smartphones συνοδεύεται επίσης από μια εξίσου ανησυχητική αύξηση του κακόβουλου λογισμικού για κινητά (Seo, Gupta, Sallam, Bertino, & Yim, 2012). Η ασφάλεια θεωρείται προτεραιότητα για πολλούς πελάτες κινητών τραπεζών. Στην έρευνα του Heggestuen (2014), διαπιστώθηκε ότι όταν πρόκειται για το Mobile Banking, το 31% των πελατών είναι πρόθυμοι να πληρώσουν για πρόσθετα χαρακτηριστικά ασφαλείας, το 63% είναι διατεθειμένο να αλλάξει λογαριασμούς για ένα με καλύτερα χαρακτηριστικά ασφαλείας και το 71% είναι πρόθυμο να αλλάξει τους λογαριασμούς σε ένα εγγυημένο όπου οι ζημίες θα επιστραφούν.

Οι ειδικοί στον τομέα της ασφάλειας, υποστηρίζουν ότι οι επιθέσεις στον κυβερνοχώρο κατά των χρηματοπιστωτικών υπηρεσιών καθίστανται πιο συχνές και πιο εξελιγμένες (Cuomo, 2014, Ryan, 2014). Γενικότερα, υπάρχουν πολλές ανησυχίες σχετικά με την ασφάλεια του κυβερνοχώρου όσον αφορά το Mobile Banking. Οι μηχανισμοί ασφάλειας στον τομέα του Mobile Banking, αποτελεί ακόμα μεγαλύτερη πρόκληση, συγκριτικά με την ασφάλεια του Web Banking, λόγω της περιπλοκότητας που δημιουργείται από μια ποικιλία διαφορετικών συσκευών κι λειτουργικών συστημάτων (He et al., 2015) . Οι εφαρμογές Mobile Banking, που δημιουργούνται από τα χρηματοπιστωτικά ιδρύματα διατίθενται για κινητές συσκευές, οι οποίες έχουν εγκατεστημένα τα λειτουργικά συστήματα Android και IOS(iphone Operating System) (Lee, Zhang, & Chen, 2013).

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Συνεπώς, η ασφάλεια και η προστασία της ιδιωτικής ζωής, καθώς και των ευαίσθητων οικονομικών δεδομένων αποτελεί μία από τις κύριες ανησυχίες όσον αφορά την αποδοχή και την χρήση των εφαρμογών Mobile Banking (Elkhodr, Shahrestani & Kourouche, 2012). Η περιορισμένη προστασίας της ιδιωτικότητας, και οι λιγότεροι πόροι ανεξάρτητων προγραμματιστών μειώνουν την αποτελεσματικότητα της προστασίας της ασφάλειας, που αφορά τις εφαρμογές κινητής τηλεφωνίας (Balebako & Cranor, 2014). Και στην περίπτωση του Mobile Banking, τα χρηματοπιστωτικά ιδρύματα. Στην επόμενη ενότητα, θα γίνει εκτενής αναφορά, στις ευπάθειες και τις απειλές που καλούνται να αντιμετωπίσει ο τομέας της ασφάλειας του Mobile Banking.

3.5. Είδη Απειλών και Επιθέσεων στο Mobile Banking

3.5.1. Ευπάθειες

Οι ευπάθειες του Mobile Banking, προέρχονται κατά μεγάλο μέρος, από τις ίδιες τις ευπάθειες των λειτουργικών συστημάτων των κινητών συσκευών, που χρησιμοποιούνται για την λήψη και την εκτέλεση των εφαρμογών Mobile Banking. Ως εκ τούτου, οι ευπάθειες των λειτουργικών συστημάτων Android και IOS(Iphone Operating System) καθιστούν την κινητή συσκευή ευπαθή σε επιθέσεις κακόβουλων χρηστών.

Επίσης, εκτός από τις ευπάθειες των λειτουργικών συστημάτων, υπάρχει πληθώρα εφαρμογών (Playstore και Appstore), που περιέχουν κρυμμένο κακόβουλο λογισμικό (malware). Συνεπώς, η συνύπαρξη και η ταυτόχρονη εκτέλεση αυτών των εφαρμογών με εφαρμογές Mobile Banking δημιουργούν πολλούς κινδύνους υποκλοπής προσωπικών στοιχείων και κίνδυνο μη εξουσιοδοτημένων χρηματοπιστωτικών

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

συναλλαγών. Πληθώρα κακόβουλων εφαρμογών όπως Zitmo, Banker, Perkel / Hesperbot, Wrob, Bankum, ZertSecurity, DroidDream και Keyloggers μπορεί να υποκλέψουν πολύτιμους κωδικούς των εφαρμογών Mobile Banking, να πραγματοποιήσουν με εξουσιοδοτημένες συναλλαγές, και να δημιουργήσουν τεράστιες οικονομικές απώλειες (Webroot, 2014 · Shih et al., 2008).

3.5.2. Απειλές

Κακόβουλο λογισμικό

Οι εγκληματίες του κυβερνοχώρου και οι κακόβουλοι χρήστες, έχουν τις απαραίτητες γνώσεις και τις δεξιότητες, ώστε να μπορούν να δημιουργήσουν εφαρμογές που όμως κρύβουν καλά στον κώδικα τους κακόβουλο κώδικα, με στόχο να εκτελεστεί χωρίς να το αντιληφθεί κάποιο, και έτσι μπορούν να υποκλέψουν τους κωδικούς πρόσβασης, ή να παρακολουθήσουν τα πλήκτρα που πληκτρολογεί ο χρήστης (key loggers). Ακόμα και οι επίσημοι ιστότοποι playstore και Applestore, συμπεριλαμβάνουν εφαρμογές που υποτίθεται, έχουν ελεγχθεί για την ασφάλεια, αλλά όπως έχει αποδειχθεί, πολλές εφαρμογές καθημερινά αφαιρούνται από την βάση δεδομένων τους, καθώς εντοπίστηκε κακόβουλο λογισμικό εκ των υστέρων. Αυτό όμως σημαίνει ότι ήδη εκατοντάδες χιλιάδες χρήστες έχουν ήδη εγκαταστήσει αυτές τις εφαρμογές, με κίνδυνο να έχουν μολύνει ήδη τις κινητές τους συσκευές, από ιούς ή Trojans.

Phishing

Όπως και στην περίπτωση του Web Banking, έτσι και στην περίπτωση του Mobile Banking, και γενικότερα στο διαδίκτυο, το ηλεκτρονικό ψάρεμα(phishing), αποτελεί και θα αποτελεί μία από τις βασικότερες απειλές για την υποκλοπή στοιχείων και κωδικών πρόσβασης (Huang, 2015).

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Μη κρυπτογραφημένα ασύρματα δίκτυα Wi-Fi

Συνήθως μια κινητή συσκευή, συνδέεται πολλές φορές σε δημόσια ασύρματα δίκτυα Wi-Fi, όπως για παράδειγμα σε καφετέριες, βιβλιοθήκες, αεροδρόμια, ξενοδοχεία, αλλά και σε υπαίθριους χώρους. Όμως, αποτελεί συχνό φαινόμενο, αυτά τα δίκτυα να μην είναι ασφαλή, και αυτή η αδυναμία εκμεταλλεύονται οι κακόβουλοι χρήστες, με σκοπό να παρακολουθήσουν την κίνηση του δικτύου και των κινητών συσκευών και να υποκλέψουν ευαίσθητες πληροφορίες, καθώς και κωδικούς πρόσβασης. (Legnitto, 2013).

Reverse engineering

Πολλές εφαρμογές Mobile Banking, δεν προστατεύονται από το λεγόμενο reverse engineering (αντίστροφη μηχανική του κώδικα) και κατά συνέπεια, οι κακόβολοι χρήστες μπορούν να επαναδημιουργήσουν και να αναλύσουν τον πηγαίο κώδικα για να υποκλέψουν πληροφορίες λογαριασμού και άλλες ευαίσθητες πληροφορίες (white Cryption, 2014)

Κωδικοί πρόσβασης

Τα απαραίτητα στοιχεία, για μια επιτυχημένη είσοδο του χρήστη σε μια εφαρμογή web banking, είναι ένας προσωπικός κωδικός χρήστη (username) και ένας μυστικός κωδικός (password) που δίνονται από την τράπεζα. Αυτοί οι κωδικοί είναι υποχρεωτικοί για την είσοδο του χρήστη στην ιστοσελίδα αλλά και για την ταυτοποίησή του. Οι κωδικοί αυτοί δίνονται από την τράπεζα στον πελάτη ξεχωριστά ο ένας από τον άλλο για περισσότερη ασφάλεια. Οι τράπεζες ακολουθούν μια πρακτική σύμφωνα με την οποία σε περίπτωση κάποιων λανθασμένων προσπαθειών εισόδου, συνήθως τρεις φορές, μπλοκάρονται οι κωδικοί του, αφού θεωρείται ύποπτη η

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

διαδικασία, και δεν μπορεί ο χρήστης να εισέλθει και να πραγματοποιήσει την συναλλαγή. Στην συνέχεια απαιτείται η επικοινωνία και η ταυτοποίηση του χρήστη από το τραπεζικό ίδρυμα και η επανέκδοση του κωδικού ασφαλείας του.

Κωδικοί TAN και κωδικοί μίας Χρήσης

Ο αριθμός αυθεντικότητας της συναλλαγής ή TAN (transaction authentication number) είναι ο αριθμός που απαιτείται για τη διεκπεραίωση των διαχειριστικών ή εγχρήματων συναλλαγών του πελάτη μέσω του διαδικτύου. Υποχρεωτική είναι και η χρήση των κωδικών password και UserlD για την ολοκλήρωση της συναλλαγής του πελάτη μαζί με τη χρήση του αριθμού TAN. Οι αριθμοί TAN υποκαθιστούν τη χειρόγραφη υπογραφή του πελάτη, επιβεβαιώνουν την εντολή του συγκεκριμένου πελάτη για την πραγματοποίηση των ανωτέρω συναλλαγών μέσω του διαδικτύου και επιβεβαιώνουν τόσο την βούλησή του για την εκτέλεση της συναλλαγής όσο και ότι η βούλησή του απευθύνεται στο συγκεκριμένο πιστωτικό ίδρυμα από τον ίδιο.

Στο επόμενο κεφάλαιο, θα γίνει εκτενής ανάλυση και αναφορά των απειλών που αφορούν το Mobile Banking, χρησιμοποιώντας μοντέλα ανάλυσης (Threat Model Analysis)

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

3.6. Η ασφάλεια των λειτουργικών συστημάτων των κινητών συσκευών και το Mobile Banking

Τα λειτουργικά συστήματα των κινητών συσκευών είναι ένας σχετικά νέος κλάδος λειτουργικών συστημάτων, καθώς υπάρχουν λιγότερο από 15 χρόνια , αντίθετα από τα λειτουργικά συστήματα των υπολογιστών που υπάρχουν παραπάνω από 50 χρόνια. Το γεγονός αυτό, καθιστά τα λειτουργικά συστήματα των κινητών σχετικά μικρά σε σύγκριση με τα παραδοσιακά λειτουργικά συστήματα των υπολογιστών όπως τα Windows. Τα δύο βασικά λειτουργικά συστήματα κινητών, τα οποία θα αναλυθούν παρακάτω, είναι:

A) Android

b) IOS (Apple)

Για να αναλυθούν και να συγκριθούν τα δυο βασικά λειτουργικά συστήματα των συσκευών κινητής τηλεφωνίας, πρέπει να ρίξουμε μια ματιά στα διάφορα μέρη των έξυπνων κινητών συσκευών (smartphone). Θα διαχωρίσουμε την ασφάλεια του λειτουργικού συστήματος σε τέσσερις διαφορετικές κατηγορίες(Ahmed et al., 2019):

- Ασφαλής εκκίνηση
- Κρυπτογράφηση και ασφαλής πρόσβαση στα δεδομένα
- Ασφάλεια εφαρμογών
- Ασφάλεια συσκευής (Φυσική)

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Ασφαλής εκκίνηση

Το πρώτο βήμα για να διασφαλιστεί ότι ένα λειτουργικό σύστημα είναι ασφαλές, είναι να διαθέτει κάποιον ασφαλή μηχανισμό εκκίνησης. Είναι σημαντικό να διασφαλιστεί η ακεραιότητα του λειτουργικού συστήματος μεταξύ διαδοχικών εκκινήσεων και κάθε επανεκκίνησης, έτσι ώστε να γνωρίζουμε ότι κανείς δεν έχει παραβιάσει το λειτουργικό σύστημα ενώ η συσκευή ήταν απενεργοποιημένη είτε σε λειτουργία εκμεταλλευόμενοι κάποια ευπάθεια του εκάστοτε συστήματος. Ένας τύπος απειλών που μπορεί να επιτεθεί σε ένα λειτουργικό σύστημα με αυτόν τον τρόπο είναι τα "rootkits". Ένα rootkit είναι ένα εργαλείο που δίνει σε έναν χρήστη ή μια διαδικασία ένα μη εξουσιοδοτημένο επίπεδο πρόσβασης στους πόρους του συστήματος. Είναι σημαντικό ο μηχανισμός εκκίνησης της συσκευής να αποτρέπει τη φόρτωση μη εξουσιοδοτημένου κώδικα πριν ή κατά την εκκίνηση του λειτουργικού συστήματος (Galterio, et al., 2018).

Κρυπτογράφηση και ασφαλής πρόσβαση στα δεδομένα

Αφού ολοκληρωθεί η εκκίνηση του λειτουργικού συστήματος, θα πρέπει να είμαστε σε θέση να βεβαιώσουμε ότι ο χρήστης έχει ασφαλή πρόσβαση στα αρχεία του. Αυτό επιτυγχάνεται χρησιμοποιώντας κρυπτογράφηση σε δεδομένα χρήστη και άλλα αρχεία συστήματος στη συσκευή. Ενώ η κρυπτογράφηση αρχείων ακούγεται σαν μια εύκολη εργασία, είναι επίσης σημαντικό το λειτουργικό σύστημα να εγγυάται τρεις ιδιότητες: Εμπιστευτικότητα, Ακεραιότητα και Διαθεσιμότητα οι οποίες αποτελούν και παραδοσιακά τις βασικές αρχές της ασφάλειας των πληροφοριακών συστημάτων. Είναι σημαντικό το λειτουργικό σύστημα να διατηρεί πλήρη πρόσβαση σε πόρους και δεδομένα για να διατηρεί την ιδιότητα διαθεσιμότητας (Macek, 2017).

Όλες αυτές οι ιδιότητες υποστηρίζουν ότι η κρυπτογράφηση δεδομένων είναι ενσωματωμένη στο λειτουργικό σύστημα. Έχοντας όλα τα αρχεία κρυπτογραφημένα από το λειτουργικό σύστημα, θα πρέπει να είναι δυνατή η εγγύηση ότι τα δεδομένα

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

χρήστη διατηρούνται εμπιστευτικά μόνο σε εξουσιοδοτημένους χρήστες, διασφαλίζεται η ακεραιότητα των δεδομένων, δεδομένου ότι ο κατακερματισμός δεδομένων θα μπορούσε να αποκαλύψει εάν το αρχείο έχει παραβιαστεί και η κρυπτογράφηση κλειδώνει το αρχείο για να αποτραπεί η παραβίαση. Επιπλέον πρέπει να δίνεται εγγύηση ότι διασφαλίζεται η διαθεσιμότητα και ότι οι μη εξουσιοδοτημένοι χρήστες δεν θα πρέπει να μπορούν να κλειδώνουν και να θέτουν εκτός διαθεσιμότητας μη εξουσιοδοτημένα αρχεία και υπηρεσίες (Galterio, et al., 2018).

Ασφάλεια εφαρμογών

Σχεδόν κάθε έξυπνη κινητή συσκευή (smartphone) λειτουργεί ή είναι σε θέση να εκτελεί εφαρμογές τρίτων εταιρειών σήμερα. Αυτές οι εφαρμογές τρίτων είναι εφαρμογές που έχει κατεβάσει ο χρήστης μέσω μιας ολοκληρωμένης υπηρεσίας λήψης ή μέσω της ενεργοποίησης απευθείας από το διαδίκτυο. Αυτές οι εφαρμογές δημιουργούν κάποια ανασφάλεια εάν έχουν πρόσβαση σε κρίσιμα μέρη του λειτουργικού συστήματος ή των υπηρεσιών συστήματος. Εφαρμογές τρίτων που δημιουργούν ανασφάλειες και έχουν πρόσβαση σε μια εξουσιοδοτημένες περιοχές των δεδομένων ονομάζονται «κακόβουλο λογισμικό». Το κακόβουλο λογισμικό είναι ένα πρόγραμμα υπολογιστή που είτε μολύνει συστήματα και τα χρησιμοποιεί κακόβουλα είτε ένα πρόγραμμα που προσπαθεί να παραβιάσει μία από τις βασικές ιδιότητες της ασφάλειας των πληροφοριακών συστημάτων (CIA) και το λειτουργικό σύστημα πρέπει να εφαρμόζει μηχανισμούς προστασίας έναντι τέτοιων εφαρμογών (Sabhanayagam et al., 2018).

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Ασφάλεια συσκευής (Φυσική)

Κάθε κινητή συσκευή κινδυνεύει να χαθεί ή να κλαπεί. Αυτό από μόνο του αποτελεί απειλή για τη συσκευή και κάθε συσκευή πρέπει να διαθέτει μηχανισμούς και περαιτέρω λειτουργικότητα προκειμένου να διασφαλίζει και την φυσική ασφάλειας της συσκευής. Οι κανονικές λειτουργίες ασφαλείας μπορεί να είναι κωδικοί PIN ή προστασία κωδικού πρόσβασης καθώς και βιομετρικά στοιχεία, όπως δακτυλικό αποτύπωμα η σάρωση της ίριδας του ματιού. Οι κωδικοί πρόσβασης της συσκευής ή οι κωδικοί PIN πρέπει να διαχειρίζονται από το Διαχειριστή συσκευής κινητής τηλεφωνίας (Mobile Device Manager- MDM) και το MDM θα πρέπει να είναι σε θέση να επιβάλλει διαφορετικές πολιτικές ασφαλείας, όπως η επιβολή ενός κωδικού πρόσβασης μήκους τουλάχιστον 8 ψηφίων ή ο εξαναγκασμός του χρήστη να χρησιμοποιεί χαρακτήρες, αριθμητικά ψηφία, σύμβολα και σημεία στίξης στον κωδικό πρόσβασης. Επιπλέον πρέπει να επεκτείνεται η λειτουργικότητα ασφάλειας της συσκευής σε μηχανισμούς και εφαρμογές εντοπισμού, κλειδώματος και απομακρυσμένης διαχείρισης των κινητών συσκευών.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

3.6.1. Android

Το λειτουργικό σύστημα Android διαθέτει τη μεγαλύτερη βάση εγκατάστασης οποιουδήποτε λειτουργικού συστήματος για κινητά μέχρι σήμερα. Κυκλοφορεί στην αγορά από το 2008 και από τότε έχουν κυκλοφορήσει 18 μεγάλες εκδόσεις. Η πιο πρόσφατη έκδοση είναι η έκδοση με την ονομασία android 11 (19 Φεβρουαρίου 2020). Οι προγραμματιστές πίσω από το Android έχουν επικεντρωθεί στην ενίσχυση των λειτουργιών ασφαλείας του Android κατά τις τελευταίες σημαντικές ενημερώσεις για να βεβαιωθούν ότι αυτή η πλατφόρμα είναι ένα από τα πιο ασφαλή λειτουργικά συστήματα για κινητά που διατίθενται στην αγορά.

Ασφαλής εκκίνηση του Android

Οι τελευταίες εκδόσεις του Android έχουν ασφαλή εκκίνηση ως ενσωματωμένη προαιρετική δυνατότητα ασφαλείας χρήστη. Αυτή η υπηρεσία ονομάζεται device-mapper-verity (dm-verity) και εφαρμόζεται ως μέτρο για να αποτρέψει το rootkits να εκμεταλλεύονται ευπάθειες κατά την εκκίνηση. Αυτή η δυνατότητα ασφαλείας εφαρμόζεται στον πυρήνα που χρησιμοποιεί το Android και εάν το κακόβουλο λογισμικό φορτωθεί με επιτυχία πριν ξεκινήσει η διαδικασία εκκίνησης του πυρήνα, θα εξακολουθήσει να μπορεί να αποτελεί απειλή για την ακεραιότητα του συστήματος.

Το dm-verity χαρακτηριστικό των σύγχρονων εκδόσεων android εξετάζει αν οι τιμές που έχουν προκύψει από την κρυπτογράφηση (συνήθως sha256) του block devicetου λειτουργικού συστήματος είναι ίδιες με τις αναμενόμενες και αποφασίζει για την ακεραιότητα των δεδομένων του συστήματος αντίστοιχα.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Κρυπτογράφηση και πρόσβαση δεδομένων στο Android

Το Android χρησιμοποιεί τον πυρήνα Linux ως θεμελιώδες στοιχείο για το λειτουργικό σύστημα. Αυτό σημαίνει ότι το Android μπορεί να χρησιμοποιήσει όλες τις δυνατότητες ασφαλείας που προσφέρει ο πυρήνας Linux. Ο πυρήνας Linux χρησιμοποιείται από εκατομμύρια υπολογιστές παγκοσμίως. Λόγω της ηλικίας και της μεγάλης διάρκειας ζωής του πυρήνα, πιστεύεται ότι είναι σταθερό και ασφαλές στη χρήση. Ο πυρήνας Linux είναι ανοιχτού κώδικα (open source). Αυτό σημαίνει ότι ο πυρήνας υπόκειται σε έρευνα, ότι πολλοί ενδιαφέρονται στο να εντοπίσουν τις ευπάθειες και τα ευάλωτα σημεία, και κατά συνέπεια προτείνονται από τους χρήστες βελτιώσεις της ασφάλειας και της λειτουργικότητάς του. Επίσης, δεδομένου ότι δεν υπάρχουν μυστικά στον κώδικα, αυτό εγγυάται επίσης ότι όποιος επιδιορθώνει ευπάθειες δεν μπορεί να κρύψει σκόπιμα τυχόν ευπάθειες χωρίς οι άλλοι να το αντιληφθούν. Ο πυρήνας Linux βρίσκεται ακόμη υπό ανάπτυξη και αντιμετωπίζονται όλες οι σημαντικές ευπάθειες που ανακαλύπτονται και ο πυρήνας ενημερώνεται με νέες εκδόσεις του λειτουργικού συστήματος Android.

Εφόσον το Android χρησιμοποιεί τον πυρήνα Linux, επωφελείται από τη λειτουργικότητα ασφαλείας που είναι ήδη ενσωματωμένη. Μία από αυτές τις λειτουργίες είναι η λειτουργικότητα διαχείρισης χρηστών. Ο πυρήνας Linux έχει σχεδιαστεί έτσι ώστε να μπορεί να έχει πολλούς χρήστες στην ίδια συσκευή. Ένα από τα βασικά χαρακτηριστικά ασφαλείας είναι η απομόνωση διαφορετικών πόρων χρηστών μεταξύ τους. Αυτό το επιτυγχάνει με την αποτροπή του χρήστη Α από την ανάγνωση αρχείων χρήστη Β. Επιπλέον, η κρυπτογράφηση στο λειτουργικό σύστημα Android πραγματοποιείται χρησιμοποιώντας 128-bit AES με αλυσίδα cipher block (CBC) και ESSIV: SHA256.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Ασφάλεια εφαρμογών στο Android

Το Android χρησιμοποιεί τη λειτουργικότητα ασφάλειας διαχείρισης χρήστη όταν εγκαθιστά και εκτελεί τόσο τυπικές εφαρμογές όσο και εφαρμογές τρίτων. Σε κάθε νέα εφαρμογή εκχωρείται το δικό του μοναδικό αναγνωριστικό χρήστη (UID) και κάθε εφαρμογή εκτελείται ως νέα διαδικασία με αυτό το UID. Αυτή η διαδικασία απομόνωσης κάθε εφαρμογής είναι σχεδόν τέλεια αφού αναγκάζει κάθε εφαρμογή να τρέχει στο δικό της περιβάλλον. Με την εκτέλεση εφαρμογών στο δικό της περιβάλλον δοκιμών, ενδεχομένως να αποτρέπονται τα σφάλματα μνήμης που μπορεί να θέσουν σε κίνδυνο το λειτουργικό σύστημα. Άλλες εφαρμογές ή το λειτουργικό σύστημα δεν μπορούν να χρησιμοποιήσουν τη φυσική μνήμη που έχει εκχωρηθεί αποκλειστικά για την εκτέλεση της εφαρμογής. Χρησιμοποιώντας αυτό το είδος απομόνωσης μπορούμε να υποθέσουμε ότι η ασφάλεια εφαρμογών στο Android είναι κάτι παραπάνω από αρκετά ανθεκτική.

Όμως, μία από τις αδυναμίες στον τρόπο με τον οποίο το Android διαχειρίζεται εφαρμογές τρίτων είναι ο τρόπος με τον οποίο η εφαρμογή μπορεί να ζητήσει πρόσβαση σε ευαίσθητα API (Application Programming Interface). Από προεπιλογή, το Android θα προστατεύσει τους χρήστες του περιορίζοντας την πρόσβαση σε μια σειρά API. Για παράδειγμα, μια εφαρμογή δεν θα έχει πρόσβαση στον αισθητήρα GPS χωρίς την άμεση συγκατάθεση του χρήστη. Ο χρήστης θα πρέπει να παραχωρήσει ρητά πρόσβαση στο εν λόγω API και αυτό γίνεται συνήθως κατά τη διαδικασία εγκατάστασης. Κατά την εγκατάσταση της εφαρμογής, παρουσιάζεται στον χρήστη μια λίστα API στα οποία θα πρέπει να παραχωρήσει πρόσβαση προκειμένου η εφαρμογή να λειτουργεί σωστά. Εάν ο χρήστης αρνηθεί την πρόσβαση της εφαρμογής σε ένα ή περισσότερα από τα API, τότε η εγκατάσταση θα ακυρωθεί. Αυτό θέτει τον χρήστη υπεύθυνο για τον τύπο δεδομένων που μπορεί να έχει πρόσβαση κάθε εφαρμογή, αλλά υπάρχουν και κάποιες αδυναμίες. Ορισμένες εφαρμογές μπορούν να μοιράζονται δεδομένα μέσω Inter Process Communication (IPC).

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Μια άλλη αδυναμία, της ασφάλειας του Android λειτουργικού συστήματος είναι ότι οι χρήστες μπορούν να κατεβάσουν με μη αυτόματο τρόπο τα Πακέτα Εφαρμογών Android (APK) και να τα εγκαταστήσουν χωρίς να χρειαστεί να χρησιμοποιήσουν το Google Play store. Αυτό σημαίνει ότι οι προγραμματιστές μπορούν να δημιουργήσουν εφαρμογές και να τις διανείμουν μέσω πλαστών μηνυμάτων ηλεκτρονικού ταχυδρομείου ή ενός ιστότοπου με σκοπό να βλάψουν την κινητή συσκευή. Η επαλήθευση των εφαρμογών μπορεί να είναι ένα εξαιρετικό μέτρο για τέτοιου είδους απειλές, αλλά αυτή η υπηρεσία είναι προαιρετική και είναι απενεργοποιημένη από προεπιλογή. Δεδομένου ότι ο χρήστης πρέπει να ενεργοποιήσει χειροκίνητα την υπηρεσία, δεν μπορεί να μετρηθεί ως βασική λειτουργικότητα ασφαλείας.

Ασφάλεια Συσκευής – Τύποι Ταυτοποίησης

Οι τελευταίες εκδόσεις του Android προσφέρουν αρκετούς τύπους ασφάλειας συσκευών:

α) κωδικός PIN,

β) Κωδικός πρόσβασης συστήματος

γ) Μοτίβο.

δ) Σάρωση δακτυλικού αποτυπώματος

ε) Σάρωση ίριδας ματιού

στ) Αναγνώριση προσώπου

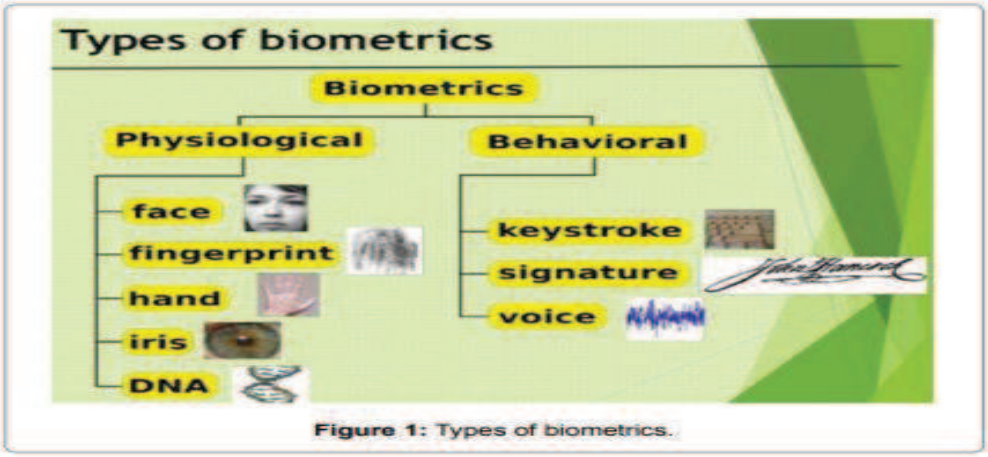
Το λειτουργικό σύστημα κρυπτογραφεί όλα τα αρχεία της συσκευής χρησιμοποιώντας τον κωδικό PIN, τον κωδικό πρόσβασης ή το μοτίβο που παρέχεται ως κλειδί. Αυτό διασφαλίζει ότι δεν είναι δυνατή η πρόσβαση στα αρχεία δεδομένων χωρίς να δημιουργηθεί το κλειδί ασφάλειας στη συσκευή με την χρήση ενός από τους

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

παραπάνω τρόπους. Εάν ο χρήστης επιλέξει να μην χρησιμοποιήσει την προεπιλεγμένη επιλογή ασφαλείας, όλα τα αρχεία εξακολουθούν να κρυπτογραφούνται χρησιμοποιώντας έναν τυπικό κωδικό πρόσβασης.

Απειλές που σχετίζονται με την ασφάλεια της συσκευής

Η βιομετρική αναγνώριση σημαίνει τον έλεγχο ταυτότητας του χρήστη χρησιμοποιώντας διαφορετικά βιολογικά χαρακτηριστικά, όπως πρόσωπο, δακτυλικό αποτύπωμα, αμφιβληστροειδή, ίριδα (φυσικό χαρακτηριστικό), γεωμετρία χεριού και φωνή, υπογραφή, πληκτρολογήσεις (χαρακτηριστικό συμπεριφοράς). Αυτά τα χαρακτηριστικά (γνωρίσματα) είναι γνωστά ως απλά βιομετρικά ή βιομετρικά αναγνωριστικά. Ένα βιομετρικό σύστημα μπορεί να λειτουργήσει είτε σε λειτουργία αναγνώρισης είτε σε κατάσταση επαλήθευσης, αλλά πριν μπορέσει το σύστημα να τεθεί σε λειτουργία αναγνώρισης ή επαλήθευσης, πρέπει να δημιουργηθεί ένα σύστημα βάσης δεδομένων που αποτελείται από πρότυπα (βιομετρικά) μέσω της διαδικασίας εγγραφής. Καθώς ο κόσμος γίνεται πιο ψηφιακός και συνδεδεμένος, η ασφάλεια στον κυβερνοχώρο έχει ύψιστη σημασία. (Bali et al., 2019)



Σχήμα 5- Τύποι βιομετρικής αναγνώρισης

Πηγή: Kalyni (2017)

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Οι κακόβουλοι χρήστες μπορούν να δημιουργήσουν ένα δίκτυο και να κάνουν τεράστιες ζημιές κλείνοντας τα ψηφιακά συστήματα συντονισμού και προκαλώντας αδυναμία εξυπηρέτησης πρόσβασης. Ως εκ τούτου, οι κινητές συσκευές χρειάζεται να έχουν ισχυρές μεθόδους ασφάλειας και ταυτοποίησης. Ο κωδικός πρόσβασης είναι πάντα το πιο αδύναμο μέσο σε ολόκληρη την αλυσίδα, ακόμη και σε οργανισμούς που ξοδεύουν εκατομμύρια δολάρια για ασφάλεια. Αυτό είναι το σημείο όπου τα βιομετρικά συστήματα μπορούν να διαδραματίσουν σημαντικό ρόλο στην ενίσχυση της ασφάλειας και της ιδιωτικής ζωής των συστημάτων στον κυβερνοχώρο. Ως εκ τούτου, μια αναγνώριση δακτυλικών αποτυπωμάτων ή της ίριδας του ματιού, χρησιμοποιείται λόγω των λιγότερων πιθανών επιθέσεων. Οι μηχανές αναγνώρισης και ελέγχου ταυτότητας είναι οι βιομετρικές συσκευές που διατίθενται στην αγορά. Αυτές οι βιομετρικές συσκευές χρησιμοποιούν αυτοματοποιημένες μεθόδους που έχουν φυσιολογικά χαρακτηριστικά όπως εκτυπώσεις Iris, εικόνες προσώπου, δακτυλικά αποτυπώματα και αναγνώριση φωνής για την αναγνώριση ενός ατόμου. Βελτιώνει την ευκολία της συνήθους συναλλαγής και αυξάνει την αποτελεσματικότητα στη μείωση της απάτης.

Παρ' ότι η βιομετρική αναγνώριση μπορεί να λειτουργήσει σαν εργαλείο για την διατήρηση της ιδιωτικότητας κάποιου, περιορίζοντας την πρόσβαση στις δικές του προσωπικές πληροφορίες (πχ ιατρικό ιστορικό), την ίδια στιγμή, η χρήση βιομετρικών μπορεί από μόνη της, να δημιουργεί ζητήματα ιδιωτικότητας. Αυτό γιατί τα βιομετρικά χαρακτηριστικά που μας ξεχωρίζουν και μας ταυτοποιούν, παρέχουν έναν μόνιμο σύνδεσμο με την ταυτότητα του κάθε ατόμου. Μη εξουσιοδοτημένη αποκάλυψη ευαίσθητων προσωπικών πληροφοριών μπορεί να προκαλέσει αντικειμενικές (πχ οικονομική απάτη, άρνηση παροχής υπηρεσιών) και υποκειμενικές απώλειες (όπου απλά και μόνο η γνώση προσωπικών πληροφοριών από ένα δεύτερο πρόσωπο ή τρίτο πρόσωπο θεωρείται ζημία). Όταν μία παραβίαση της ασφάλειας σε ένα πληροφοριακό σύστημα έχει σαν αποτέλεσμα προσωπική και υποκειμενική ζημία για κάποιο άτομο,

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

μπορεί να κατηγοριοποιηθεί ως απώλεια της ιδιωτικότητας (privacy). Η ιδιωτικότητα αναφέρεται στο δικαίωμα ενός ατόμου να παραμένει ανώνυμος και να ελέγχει την πρόσβαση σε δικές του προσωπικές πληροφορίες. Παρ' όλο που η ανάγκη για ιδιωτικότητα (privacy) είναι τυπικά μία προτίμηση του καθενός, υπάρχουν περιπτώσεις όπου η προστασία της πληροφορίας μπορεί να απαιτείται για το δημόσιο συμφέρον (πχ εθνική ασφάλεια).

Οι περισσότερο πιθανές επιθέσεις που μπορεί να γίνουν εναντίον των διαφορετικών μονάδων ενός βιομετρικού συστήματος είναι οι παρακάτω:

- Επίθεση δημιουργίας αντίγραφου (spoofing attack) ή επίθεση μίμησης (mimicry attack): ανάλογα αν μιλάμε για ανατομικά βιομετρικά στοιχεία ή για βιομετρικά στοιχεία που βασίζονται στην συμπεριφορά. Αυτές οι επιθέσεις αντιγράφουν με διάφορα μέσα και μεθόδους, το βιομετρικό στοιχείο του εγγεγραμμένου χρήστη και το χρησιμοποιούν για να ξεγελάσουν το σύστημα.
- Επίθεση επιβολής βίας: το πραγματικό βιομετρικό παρουσιάζεται αλλά χωρίς την θέληση του χρήστη, π.χ. ένας απατεώνας επιβάλλει σε κάποιον χρήστη κάτω από κάποιου είδους απειλή, να του δώσει πρόσβαση στο σύστημα
- Αντικατάσταση συσκευής: αντικατάσταση της αυθεντικής συσκευής καταγραφής με μία παραποιημένη ή άλλη συσκευή.
- Άρνηση εξυπηρέτησης (Denial of service): μαζικές επιθέσεις στο σύστημα που έχουν σαν συνέπεια την μη σωστή λειτουργία του συστήματος.
- Ο εξαγωγέας χαρακτηριστικών θα μπορούσε να είναι υπό τον έλεγχο κάποιου και να παράγει προεπιλεγμένα χαρακτηριστικά, με το να εισάγει δικά του δεδομένα.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

- Ο συγκριτής μπορεί να είναι στόχος, έχοντας σαν σκοπό την παραγωγή ψευδών βαθμολογιών. Αυτό μπορεί να γίνει με διάφορους τρόπους:
- Τροποποίηση των βαθμολογιών ομοιότητας: αποκτώντας και αλλάζοντας την τιμή μίας βαθμολογίας ομοιότητας πριν επηρεάσει την απόφαση
- Επίθεση με επανάληψη: καταγεγραμμένα πραγματικά δεδομένα εμφυτεύονται στο κανάλι.
- Αντικατάσταση κάποιου μέρους: αλλαγή ενός από τα hardware / Software μέρη με σκοπό να ελέγχεται η συμπεριφορά του.
- Επίθεση αναρρίχησης (Hill climbing attack): κλιμακούμενη επαναλαμβανόμενη επίθεση που μπορεί να επιτευχθεί όταν κάποιος έχει πρόσβαση στις βαθμολογίες ομοιότητας. Πιο συγκεκριμένα, σε ένα δείγμα επιφέρεται μία μικρή τροποποίηση και αν η βαθμολογία ομοιότητας βελτιωθεί, τότε η τροποποίηση διατηρείται, αλλιώς απορρίπτεται. Αυτή η διαδικασία επαναλαμβάνεται μέχρι η βαθμολογία ομοιότητας κάποια στιγμή να ξεπεράσει το ορισμένο όριο αποδοχής.
-

Ένα βιομετρικό σύστημα μπορεί να είναι ευάλωτο λόγω επιθέσεων προς αυτό, αλλά και από κακή σχεδίαση. Ένα σύστημα που χαρακτηρίζεται από υψηλό δείκτη λανθασμένων αποδοχών (False Acceptance Rate) είναι πιθανό να παραβιαστεί έπειτα από έναν αριθμό βιομετρικών χαρακτηριστικών που θα παρουσιαστούν τυχαία στο σύστημα, καθώς θα βρεθεί κάποιο που να ταιριάζει. Αυτό μπορεί να συμβεί ακόμα και αν δεν υπάρχει κάποιος που να επιθυμεί να επιτεθεί στο σύστημα, αυτή η περίπτωση ονομάζεται επίθεση μηδενικής-προσπάθειας (zero effort attack).

Κανάλια επικοινωνίας που συνδέουν τα διάφορα μέρη ενός βιομετρικού συστήματος, όπως το κανάλι μεταξύ του αισθητήρα και του εξαγωγέα χαρακτηριστικών, μεταξύ του εξαγωγέα χαρακτηριστικών και του συγκριτή, μεταξύ

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

της βάσης δεδομένων και του συγκριτή, και μεταξύ του συγκριτή και της εφαρμογής, μπορεί να παρακολουθούνται και να ελέγχονται από μη εξουσιοδοτημένα άτομα. Ανάμεσα στις πιθανές επιθέσεις είναι:

- παθητική παρακολούθηση (eavesdropping attack): η κρυφή παρακολούθηση της μετάδοσης βιομετρικών δεδομένων.
- επίθεση ενδιάμεσου ατόμου (Man-in-the-middle attack): ένας κακόβουλος χρήστης είναι ικανός να παραποιεί τα μηνύματα που ανταλλάσσονται μεταξύ δύο σημείων χωρίς να γνωρίζουν οι συμμετέχοντες ότι η γραμμή έχει παραβιαστεί.
- επίθεση Brute force attack: εξαντλητική παρουσίαση ενός μεγάλου συνόλου από βιομετρικά δείγματα προς το σύστημα αναγνώρισης με σκοπό να βρεθεί ένα το οποίο να δουλεύει.
- επίθεση επανάληψης (Replay attack)
- επίθεση αναρρίχησης (hill climbing attack)

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

3.6.2. IOS (Apple)

Η εταιρία Apple ανακοίνωσε και κυκλοφόρησε την πρώτη της έξυπνη κινητή συσκευή (smartphone) το 2007, το γνωστό iPhone, που έγινε το πρώτο τηλέφωνο σε μια ολόκληρη νέα γενιά έξυπνων κινητών τηλεφώνων. Με την κυκλοφορία του πρώτου iPhone, η Apple άλλαξε επίσης τον τρόπο σχεδίασης των τηλεφώνων, καθώς χρησιμοποίησε μια τροποποιημένη έκδοση του πυρήνα του λειτουργικού συστήματος OS X των υπολογιστών.

Ασφαλής εκκίνηση του iOS

Το θεμέλιο για το iOS είναι ο πυρήνας OS X, ο οποίος χρησιμοποιείται επίσης στο λειτουργικό σύστημα της Apple. Το πρώτο λειτουργικό σύστημα OS X κυκλοφόρησε το 2001 και αυτό σημαίνει ότι ο πυρήνας έχει χρησιμοποιηθεί και δοκιμαστεί για σχεδόν 20 χρόνια. Η Apple έχει δημοσιοποιήσει τον κώδικα του πυρήνα για να διασφαλίσει ότι θα υπάρχει η διασφάλιση της διαφάνειας. Αν κάποιος θέλει να ανακαλύψει ευπάθειες στον πυρήνα, επιτρέπεται και μπορεί να το κάνει. Το iOS εφαρμόζει έναν ασφαλή μηχανισμό εκκίνησης. Για κάθε μέρος της αλυσίδας εκκίνησης το σύστημα ελέγχει εάν η επόμενη μονάδα κώδικα υπογράφεται από την Apple και ότι δεν έχει παραβιαστεί. Αυτό γίνεται για να διασφαλιστεί η ακεραιότητα του συστήματος, ακόμη και αν το σύστημα έχει απενεργοποιηθεί. Εάν έχει παραβιαστεί οποιοσδήποτε κώδικας στο μηχανισμό εκκίνησης, η συσκευή δεν θα ξεκινήσει από τότε που η αλυσίδα εμπιστοσύνης σπάσει. Τα στοιχεία που περιλαμβάνονται στην αλυσίδα εμπιστοσύνης είναι οι boot loaders, πυρήνας, επεκτάσεις πυρήνα και υλικολογισμικό. Ο μηχανισμός εκκίνησης στο iOS ξεκινά με ένα root-oftrust υλικού. Πρόκειται για ένα πρόγραμμα που φορτώνει σε ένα τσιπ μνήμης μόνο για ανάγνωση (ROM). Ο κώδικας εκκίνησης σε αυτό το τσιπ είναι ασφαλής από παραβίαση,

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

δεδομένου ότι είναι ένα τσιπ ROM που εγκαθίσταται κατά την παραγωγή της συσκευής. Από αυτό το root-of-trust ο επόμενος κώδικας στον μηχανισμό εκκίνησης επικυρώνεται και τότε και μόνο τότε εκτελείται (Hayran et al., 2016).

Κρυπτογράφηση και πρόσβαση δεδομένων στο λειτουργικό σύστημα iOS

Όλες οι νέες συσκευές iOS διαθέτουν ενσωματωμένο μηχανισμό κρυπτογράφησης. Πρόκειται για έναν αποκλειστικό μηχανισμό AES 256 bit που κρυπτογραφεί όλα τα αρχεία στο δίσκο. Το iOS χρησιμοποιεί δύο κύρια κλειδιά. Ένα κλειδί υλικού που κρυπτογραφεί τα μετα-δεδομένα αρχείων και ένα ξεχωριστό κλειδί που μαζί με το κλειδί υλικού κρυπτογραφεί το περιεχόμενο του αρχείου. Το κλειδί υλικού δημιουργείται όταν το λειτουργικό σύστημα είναι εγκατεστημένο στη συσκευή και για την πρόσβαση στα δεδομένα απαιτείται αυτό το κλειδί(Surekha et al., 2017). Η υπηρεσία MDM από την Apple ονομάζεται iCloud και το iCloud δίνει στον χρήστη τη δυνατότητα να διαγράψει εξ αποστάσεως το κλειδί υλικού από τη συσκευή. Αυτό θα έχει ως αποτέλεσμα να μην είναι προσβάσιμα όλα τα αρχεία δεδομένων της συσκευής.

Κάθε εφαρμογή που είναι εγκατεστημένη στη συσκευή εκτελείται σε πλήρη απομόνωση μεταξύ τους. Κάθε εφαρμογή εκχωρεί τον δικό της αρχικό φάκελο στο δίσκο και τον δικό της χώρο μνήμης. Ο χώρος μνήμης προστατεύεται χρησιμοποιώντας ASLR και κάθε αρχικός φάκελος κλειδώνεται σε ένα συγκεκριμένο UID όπως στο Android. Επειδή αυτό λειτουργεί σαν περιβάλλον δοκιμών, κάθε εφαρμογή είναι ασφαλής από άλλες εφαρμογές που εκτελούνται στην ίδια συσκευή. Η πλειονότητα των εφαρμογών και διαδικασιών στο IOS λειτουργεί με δικαιώματα μη προνομιούχου χρήστη, όπως και όλες οι εφαρμογές τρίτων. Αυτό κάνει τις εφαρμογές τρίτων να μην έχουν πρόσβαση σε αρχεία δεδομένων που ανήκουν στο root (Kalyani, 2017).

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Ασφάλεια εφαρμογών του λειτουργικού συστήματος iOS

Η Apple επικεντρώθηκε στην ασφάλεια εφαρμογών κατά το σχεδιασμό του λειτουργικού συστήματος iOS. Έχουν εφαρμόσει μια σειρά διαφορετικών εμποδίων – υποχρεωτικών σταδίων που πρέπει να περάσει ένας προγραμματιστής για να είναι σε θέση να αναπτύξει και να διανείμει εφαρμογές. Για να διανείμει μια εφαρμογή με δυνατότητα εκτέλεσης σε συσκευή iOS, ο προγραμματιστής πρέπει να υποβάλει τον κώδικά του για έλεγχο από έναν υπάλληλο της Apple. Ο κωδικός πρέπει να υπογραφεί και από τον προγραμματιστή χρησιμοποιώντας ένα ιδιωτικό πιστοποιητικό και πρέπει να υπογραφεί από τον υπάλληλο της Apple. Αυτό επεκτείνει στην πραγματικότητα την αλυσίδα της εμπιστοσύνης από το λειτουργικό σύστημα σε όλες τις εφαρμογές που εκτελούνται στη συσκευή

Ασφάλεια της συσκευής iOS

Το iOS προσφέρει τη δυνατότητα προστασίας με κωδικό πρόσβασης συσκευών. Το λειτουργικό σύστημα ζητά από τον χρήστη κατά την εγκατάσταση ζητώντας από τον χρήστη να ορίσει έναν τετραψήφιο κωδικό PIN. Ο χρήστης μπορεί να ζητήσει ρητά ότι ο κωδικός πρόσβασης πρέπει να είναι μεγαλύτερος αλφαριθμητικός κωδικός αντί για τετραψήφιο PIN. Το iOS προσφέρει πολιτικές κωδικού πρόσβασης μέσω MDM, γεγονός που καθιστά δυνατή την επιβολή ισχυρότερων κωδικών πρόσβασης. Μαζί με την ασφάλεια της συσκευής που προσφέρει το λειτουργικό σύστημα κατά την εγκατάσταση, το iOS προσφέρει επίσης μια δυνατότητα κλειδώματος ενεργοποίησης. Η ίδια η συσκευή συνδέεται με έναν λογαριασμό iCloud και δεν είναι δυνατή η επανεγκατάσταση του λειτουργικού συστήματος, εκτός εάν η συσκευή μας αποσυνδεθεί από τον λογαριασμό iCloud. Αυτό καθιστά τις συσκευές iOS λιγότερο επιθυμητούς στόχους για κλοπή, καθώς ο αρχικός κάτοχος θα πρέπει να ξεκλειδώσει τη συσκευή (Yang et al., 2019).

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Μέθοδοι ταυτοποίησης στο λειτουργικό σύστημα iOS

Όπως στο λειτουργικό σύστημα Android, έτσι και στο iOS, χρησιμοποιούνται οι εξής μέθοδοι ταυτοποίησης:

α) κωδικός PIN,

β) Κωδικός πρόσβασης συστήματος

γ) Μοτίβο.

δ) Σάρωση δακτυλικού αποτυπώματος

ε) Σάρωση ίριδας ματιού

στ) Αναγνώριση προσώπου

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

3.7 Κίνδυνοι και Απειλές Ασφάλειας Εφαρμογών Κινητών

Προκειμένου να σχηματίσουμε μια περισσότερη σαφή και ολοκληρωμένη εικόνα αναφορικά με τις απειλές που υπάρχουν στην χρήση των κινητών συσκευών που φιλοξενούν διαδικτυακές εφαρμογές είτε συνδέονται απευθείας σε κάποια διαδικτυακή πλατφόρμα πρέπει να λάβουμε υπόψιν μας την έρευνα του OWASP όπου έχουν κατηγοριοποιηθεί οι κίνδυνοι και οι απειλές της χρήσης των κινητών συσκευών όπως παρακάτω (Owasp.org, 2016) :

1. Improper Platform Usage - Threat Agents

Αυτή η κατηγορία καλύπτει όλες τις περιπτώσεις που σχετίζονται με την κακή χρήση μιας δυνατότητας της διαδικτυακής πλατφόρμας ή τις περιπτώσεις αποτυχίας εφαρμογής των στοιχείων ελέγχου ασφάλειας της εκάστοτε πλατφόρμας. Μπορεί να περιλαμβάνει μηνύματα ή πληροφορία εσωτερικής επικοινωνίας σε λειτουργικά συστήματα Android, δικαιώματα σε διαδικτυακές πλατφόρμες, κακή χρήση του TouchID ή του Keychain ή κάποιον άλλο έλεγχο ασφαλείας που αποτελεί μέρος του λειτουργικού συστήματος των κινητών συσκευών.

2. Insecure Data Storage - Threat Agents

Σε αυτή τη κατηγορία οι παράγοντες απειλής ενδέχεται να περιλαμβάνουν τα ακόλουθα: έναν κακόβουλο ή αντίπαλο που έχει επιτύχει να αποκτήσει (παράνομα) μία χαμένη / κλεμμένη κινητή συσκευή., ένα κακόβουλο λογισμικό που ενεργεί για λογαριασμό του αντιπάλου / κακόβουλου χρήστη και εκτελείται στην κινητή συσκευή.

3. Insecure Communication - Threat Agents

Κατά το σχεδιασμό μιας εφαρμογής για κινητά, τα δεδομένα και η πληροφορία που ανταλλάσσονται συνήθως με το μοντέλο πελάτη-διακομιστή. Όταν η εφαρμογή μεταδίδει τα δεδομένα της, πρέπει να διασχίσει υποχρεωτικά το δίκτυο φορέα/παρόχου της κινητής συσκευής και φυσικά το Διαδίκτυο. Οι κακόβουλοι χρήστες /παράγοντες

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

απειλής ενδέχεται να εκμεταλλευτούν τρωτά σημεία για να παρακολουθούν ευαίσθητα δεδομένα ενώ ταξιδεύουν κατά μήκος του καλωδίου επικοινωνίας. Υπάρχουν οι ακόλουθοι παράγοντες απειλής:

- Ένας αντίπαλος/κακόβουλος χρήστης που μοιράζεται το τοπικό σας δίκτυο (παραβιασμένο δίκτυο ή παρακολουθούμενο).
- Παραβιασμένες δικτυακές συσκευές ή ενδιάμεσοι κόμβοι του δικτύου (δρομολογητές, πύργοι κινητής τηλεφωνίας, διακομιστές μεσολάβησης κ.λπ.).
- Κακόβουλο λογισμικό εγκατεστημένο στην κινητή συσκευή.

4. Insecure Authentication - Threat Agents

Οι κακόβουλοι χρήστες σε αυτήν την κατηγορία εκμεταλλεύονται τρωτά σημεία ελέγχου ταυτότητας και το κάνουν συνήθως μέσω αυτοματοποιημένων επιθέσεων για τις οποίες χρησιμοποιούν εργαλεία που βρίσκουν διαθέσιμα στο διαδίκτυο είτε εργαλεία και εφαρμογές που έχουν δημιουργήσει οι ίδιοι .

5. Insufficient Cryptography - Threat Agents

Παράγοντες απειλής σε αυτήν περίπτωση αποτελούν τα ακόλουθα:

- έχει φυσική πρόσβαση σε δεδομένα που έχουν κρυπτογραφηθεί εσφαλμένα
- κακόβουλο λογισμικό για κινητά που ενεργεί για λογαριασμό του αντιπάλου/κακόβουλου χρήστη.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

6. Insecure Authorization - Threat Agents

Σε αυτή την κατηγορία οι κακόβουλοι χρήστες εκμεταλλεύονται τρωτά σημεία εξουσιοδότησης/αυθεντικοποίησης και το επιτυγχάνουν συνήθως μέσω αυτοματοποιημένων επιθέσεων τις οποίες υλοποιούν χρησιμοποιώντας διαθέσιμα εργαλεία-εφαρμογές του διαδικτύου είτε εργαλεία/εφαρμογές που έχουν δημιουργήσει οι ίδιοι.

7. Poor Code Quality - Threat Agents

Οι κακόβουλοι χρήστες σε αυτή την περίπτωση αποτελούν οντότητες που μπορούν να μεταβιβάσουν μη αξιόπιστες πληροφορία και δεδομένα σε κλήσεις και μεθόδους που πραγματοποιούνται κατά εντός του κώδικα της εφαρμογής ή ενός συστήματος κινητής συσκευής. Αυτοί οι τύποι ζητημάτων δεν είναι απαραίτητα ζητήματα ασφαλείας από μόνα τους αλλά οδηγούν σε ευπάθειες ασφαλείας. Για παράδειγμα, η υπερχείλιση της προσωρινής μνήμης ενός προγράμματος-εφαρμογής σε παλαιότερες εκδόσεις του Safari (μια ευπάθεια χαμηλής ποιότητας κώδικα) οδηγούσε σε υψηλού κινδύνου Jailbreak επιθέσεις. Οι κώδικες χαμηλού επιπέδου ποιότητας τυπικά εκμεταλλεύονται μέσω κακόβουλου λογισμικού ή απάτες ηλεκτρονικού ψαρέματος (phishing).

8. Code Tampering - Threat Agents

Συνήθως, ένας εισβολέας θα εκμεταλλευτεί τροποποιημένο κώδικα μέσω κακόβουλων μορφών και εκδόσεων των εφαρμογών που φιλοξενούνται σε ιστότοπους με εφαρμογές τρίτων (εταιρείες λογισμικού ή προγραμματιστές). Ο εισβολέας μπορεί επίσης να εξαπατήσει τον χρήστη να εγκαταστήσει την εφαρμογή μέσω επιθέσεων ηλεκτρονικού ψαρέματος (phishing).

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

9. Reverse Engineering - Threat Agents

Ένας εισβολέας συνήθως θα κατεβάσει μια εφαρμογή που έχει βάλει ως στόχο από ένα κατάστημα εφαρμογών και θα την αναλύσει στο δικό του τοπικό περιβάλλον χρησιμοποιώντας μια σουίτα διαφορετικών εργαλείων.

10. Extraneous Functionality - Threat Agents

Συνήθως, ένας εισβολέας προσπαθεί να κατανοήσει τις ξένες λειτουργίες σε μια εφαρμογή για κινητά, προκειμένου να ανακαλύψει κρυφές λειτουργίες σε συστήματα back end. Ο εισβολέας θα εκμεταλλευτεί τυπικά ξένη λειτουργικότητα απευθείας από τα δικά του συστήματα χωρίς καμία εμπλοκή από τελικούς χρήστες.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ΚΕΦΑΛΑΙΟ 4- Μοντέλα Ανάλυσης Απειλών (Models of Threat Analysis)

Τα μοντέλα ανάλυσης απειλών, αποτελούν μια πολύ σημαντική πτυχή του τομέα της μηχανικής όσο αναφορά την δημιουργία λογισμικών. Η μοντελοποίηση, είναι ένας βολικός και αποδεδειγμένα αποτελεσματικός τρόπος εύρεσης σφαλμάτων ασφαλείας και σφαλμάτων ασφαλείας σε ένα πρόγραμμα ή ένα σύστημα και, εάν εφαρμοστεί σωστά, βοηθάει σε ικανοποιητικό βαθμό να σχεδιάσουμε και να εφαρμόσουμε προγράμματα και συστήματα που είναι πιο ασφαλή από επιθέσεις.

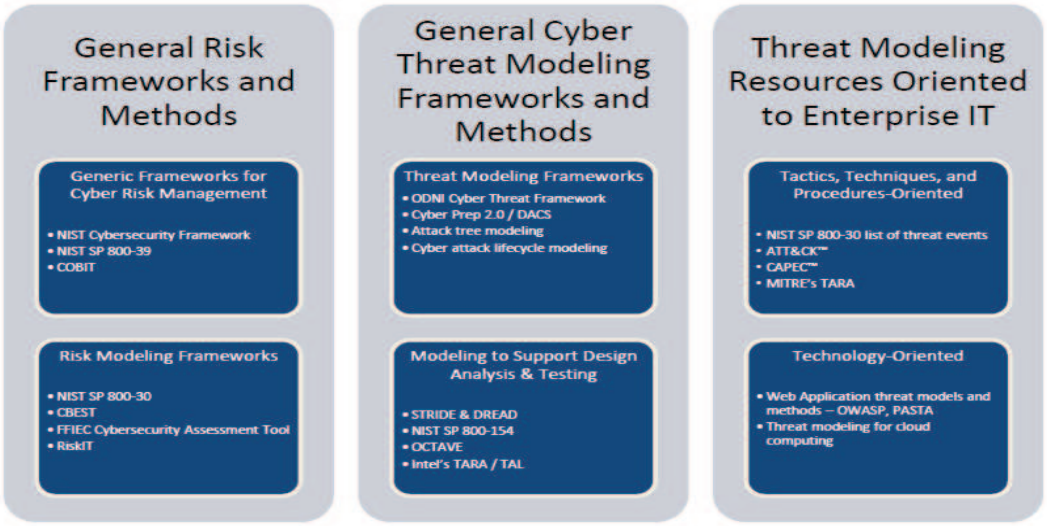
Κάθε σημαντικό πρόγραμμα υπολογιστή, χρειάζεται ένα αντίστοιχο μοντέλο απειλής για να εξεταστεί αν πληροί τις καθορισμένες απαιτήσεις ασφαλείας. Είναι φυσικό για τους ανθρώπους να δημιουργούν μοντέλα απειλών. Υποσυνείδητα, δημιουργούμε ένα μοντέλο ανάλυσης απειλών, κάθε φορά που παίρνουμε μια απόφαση και το αποτέλεσμα της εν λόγω ανάλυσης, μπορεί να επηρεάσει άμεσα το αποτέλεσμα της απόφασής μας.

Στην ασφάλεια πληροφοριών, η μοντελοποίηση απειλών είναι μια συστηματική προσέγγιση που χρησιμοποιείται για την ανακάλυψη απειλών και την κατανόηση των απαιτήσεων ασφάλειας ενός προγράμματος υπολογιστή ή ενός συστήματος υπολογιστή. Με τη μοντελοποίηση απειλών, οι προγραμματιστές μπορούν να καταλάβουν πώς θα μπορούσαν να πραγματοποιηθούν διαφορετικές απειλές και, στη συνέχεια, πώς να αποφύγουν τέτοιου είδους επιθέσεις.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

4.1. Μοντέλα Ανάλυσης Απειλών για χρηματοπιστωτικά Ιδρύματα (Threat Modeling Framework for FSS Institutions)

Σε μια έρευνα τους, οι Bodeau et al. (2018) διεξήγαγαν μια ερευνητική ανάλυση αναφορικά με τα μοντέλα απειλών στον κυβερνοχώρο και τα πλαίσια μοντελοποίησης απειλών που σχετίζονται με τους στόχους και τις περιπτώσεις χρήσης του προγράμματος NGCI Apex. Αυτή η έρευνα περιελάβανε μια βιβλιογραφική ανάλυση για 21 μοντέλα απειλών και πλαίσια που χρησιμοποιούνται ευρέως για τη διαχείριση της ασφάλειας στον κυβερνοχώρο, καθώς και συνεντεύξεις με στελέχη σε 11 μεγάλα χρηματοπιστωτικά ιδρύματα (FSS) που είναι υπεύθυνα για τη μοντελοποίηση απειλών στον κυβερνοχώρο, την αξιολόγηση κινδύνου και την αντιμετώπιση των διάφορων απειλών και επιθέσεων. Η Εικόνα 2 απεικονίζει το εύρος των μοντέλων και των πλαισίων που ερευνήθηκαν.

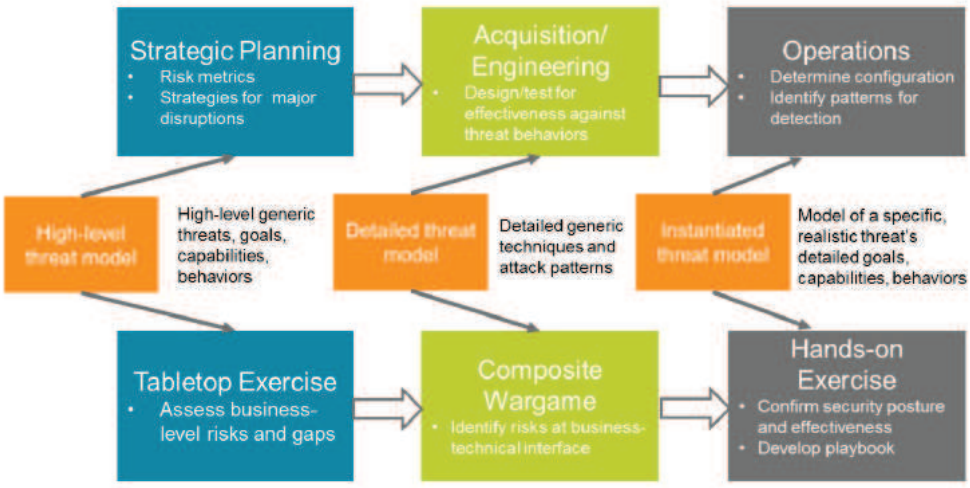


Σχήμα 6- Μοντέλα ανάλυσης Απειλών

Πηγή: Bodeau(2018)

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Η έρευνα Bodeau (2018), καθόρισε κριτήρια για την αξιολόγηση των χαρακτηριστικών των διαφόρων μοντέλων απειλής και την καταλληλόλητά τους για το NGCI Apex. Η ανάλυση διαπίστωσε ότι τα μοντέλα συγκεντρώθηκαν σε ομάδες που ταιριάζουν είτε σε στρατηγικό σχεδιασμό, είτε μηχανική και ανάκτηση πληροφορίας, είτε σε επιχειρησιακές λειτουργίες. Δεν υπήρχε κανένα μοντέλο, ούτε μια συνεκτική σουίτα μοντέλων, κατάλληλη για χρήση σε αυτά τα τρία διαφορετικά επίπεδα λεπτομέρειας. Επίσης, αποφασίστηκε ότι θα υπήρχε αξία σε μια συντονισμένη σειρά μοντέλων απειλής που θα επιτρέψουν τη σαφή και συνεπή επικοινωνία και θα ελαχιστοποιήσουν τα κενά, τόσο εντός όσο και μεταξύ των ιδρυμάτων FSS ή άλλων επιχειρήσεων. Ως εκ τούτου, καθορίστηκε ένα πλαίσιο εντός του οποίου μια τέτοια συνεκτική σειρά μοντέλων απειλής μπορεί να καθοριστεί και να συμπληρωθεί, βασιζόμενη σε εκτεταμένους πόρους πληροφοριών επίθεσης στον κυβερνοχώρο που διατηρούνται και μοιράζονται στην κοινότητα της ασφάλειας στον κυβερνοχώρο. Αυτό απεικονίζεται στην εικόνα 3.



Σχήμα 7- Τα τρία Επίπεδα των μοντέλων ανάλυσης Απειλών

Πηγή: Bodeua (2018),

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

4.2. Χρήση του μοντέλου STRIDE

Η μέθοδος STRIDE είναι μια προσέγγιση για την μοντελοποίηση απειλών που προτάθηκε το 1999, από τους Loren Kohnfelder και Praerit Garg. Είναι ένα πλαίσιο που αναπτύχθηκε για να βοηθήσει τους υπεύθυνους της ασφάλειας πληροφοριών, να εντοπίζουν τις απειλές στα υπολογιστικά συστήματα, και να διαμορφώνουν τα πληροφοριακά συστήματα με μεγαλύτερη προσοχή. Οι υπεύθυνοι της ασφάλειας των πληροφοριών, είναι προγραμματιστές με ειδικές γνώσεις της ασφάλειας των πληροφοριών, και συμμετέχουν στη διαδικασία ανάπτυξης λογισμικού και συστημάτων υπολογιστών. Το ακρωνύμιο STRIDE προέρχεται από τις λέξεις: Spoofing, Tampering, Repudiation, Information disclosure (privacy breach or data leak), Denial of service, Elevation of privilege, που αντίστοιχα μεταφράζονται ως: πλαστογράφηση, παραβίαση (δεδομένων), απόρριψη, αποκάλυψη πληροφοριών, άρνηση παροχής υπηρεσίας και ανύψωση προνομίων. Όλες αυτές οι λέξεις αντιπροσωπεύουν μια ολόκληρη ομάδα ή κατηγορία απειλών. Αυτή η κατηγοριοποίηση των απειλών διευκολύνει τον εντοπισμό απειλών σε ορισμένες πτυχές ενός συστήματος υπολογιστή (Shostack & Long, 2014).

Κάθε στοιχείο στο STRIDE παρουσιάζει στην πραγματικότητα μια πιθανή παραβίαση ή μια ιδιότητα που παραβιάζεται. Οι άλλες ιδιότητες που ενδέχεται να παραβιαστούν είναι η ακεραιότητα, η μη απόρριψη, η εμπιστευτικότητα, η διαθεσιμότητα και η εξουσιοδότηση. Τώρα που αναφέρθηκαν οι ιδιότητες που πρέπει να χειριστούμε στο μοντέλο απειλής, μπορούμε να δούμε ένα απλό παράδειγμα.

Έστω ότι ένα χρηματοπιστωτικό ίδρυμα διαθέτει μια βάση δεδομένων που περιέχει όλες τις απαραίτητες πληροφορίες σχετικά με τους πελάτες του. Αυτά τα δεδομένα είναι εξαιρετικά ευαίσθητα (προσωπικά δεδομένα) και οποιαδήποτε παραβίαση ασφαλείας της βάσης δεδομένων θα έχει σοβαρές συνέπειες για το

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

χρηματοπιστωτικό ίδρυμα. Μερικά παραδείγματα απειλών της βάσης δεδομένων μπορεί να είναι (Shostack & Long, 2014).:

• Κάποιος προσποιείται ότι είναι εκπρόσωπος εξυπηρέτησης πελατών, για να αποκτήσει πρόσβαση στη βάση δεδομένων.

• Ένας δυσαρεστημένος υπάλληλος με κακόβουλη πρόθεση αποφασίζει να αλλάξει όλους τους αριθμούς τηλεφώνου στους πελάτες των χρηματοπιστωτικών ιδρυμάτων στη βάση δεδομένων.

• Ο ίδιος δυσαρεστημένος υπάλληλος αρνείται την αλλαγή αριθμών τηλεφώνου σε όλους τους πελάτες.

• Ορισμένα άγνωστα αρχεία που περιέχουν το μελλοντικό πρόγραμμα απόλυσης εργαζομένων στα ιδρύματα διατίθενται σε όλους τους εργαζομένους.

• Η βάση δεδομένων δεν είναι διαθέσιμη λόγω υψηλού φορτίου.

• Οι πελάτες έχουν δικαίωμα να διαβάζουν έγγραφα που δεν προορίζονται για αυτούς.

Παραβίαση του ελέγχου ταυτότητας

Μπορεί να φαίνεται προφανές σε πολλούς ότι μια παραβίαση του ελέγχου ταυτότητας μπορεί να είναι ένα άτομο που χρησιμοποιεί το όνομα χρήστη και τον κωδικό πρόσβασης ενός άλλου συναδέλφου για πρόσβαση σε αρχεία ή πληροφορίες στις οποίες δεν έχει δικαίωμα πρόσβασης, αλλά τα προβλήματα ελέγχου ταυτότητας μπορεί να είναι πολύ περισσότερα και σοβαρότερα από αυτό. Η πλαστογράφηση είναι γενικά όταν κάποιος ισχυρίζεται ότι είναι κάποιος που δεν είναι. Αυτό μπορεί να κυμαίνεται από την πρόσβαση σε αρχεία χρησιμοποιώντας τον κωδικό πρόσβασης των συναδέλφων του, έως την αξίωση ότι είναι ο δικηγόρος ενός πρόσφατα αποθανόντος

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

μέλους της βρετανικής αριστοκρατίας χωρίς κληρονόμο. Και στις δύο περιπτώσεις κάποιος προσπαθεί να κρύψει την πραγματική του ταυτότητα, ενώ εκτελεί ή ισχυρίζεται ότι εκτελεί εργασίες που δεν είναι πραγματικά επικυρωμένες (Shostack & Long, 2014).

Παραβίαση της ακεραιότητας

Είναι κοινώς αποδεκτό, ότι δεν πρέπει ποτέ να εμπιστευόμαστε αυτά που διαβάζουμε και ότι πρέπει πάντα να ελέγχουμε τις πηγές προτού αποδεχτούμε κάτι ως γεγονός. Αυτό ακριβώς συμβαίνει και στην περίπτωση της ακεραιότητας. Για παράδειγμα, η ερώτηση: "Είναι αυτό το αρχείο το πραγματικό αρχείο ή έχει τροποποιηθεί, ή έχει αλλάξει ή έχει τοποθετηθεί εκεί για να το βρω;", είναι μια πιθανή ερώτηση όσον αφορά την ασφάλεια των πληροφοριών. Η παραβίαση των δεδομένων είναι ένα σοβαρό πρόβλημα για όλα τα είδη επιχειρήσεων. Ένα παράδειγμα ακεραιότητας, είναι η περίπτωση ενός δυσαρεστημένου υπαλλήλου, ο οποίος έχει τροποποιήσει όλους τους αριθμούς τηλεφώνου που είναι εγγεγραμμένοι σε όλους τους πελάτες στη βάση δεδομένων, ενός χρηματοπιστωτικού ιδρύματος. Αυτό έχει ως αποτέλεσμα, ολόκληρη η βάση δεδομένων να αχρηστευτεί, δεδομένου ότι περιέχει ψευδή δεδομένα και δεν μπορεί κάποιος να εμπιστευτεί ξανά τη βάση δεδομένων, καθώς έχει αλλοιωθεί.

Συνήθως, η παραβίαση τροποποιεί δεδομένα που βρίσκονται στο δίσκο, αλλά είναι επίσης δυνατό να υπάρχει τροποποίηση δεδομένων στο δίκτυο ή στη μνήμη. Ενώ η παραβίαση των δεδομένων στο δίσκο ενδέχεται να επιτευχθεί με την επεξεργασία ενός ήδη υπάρχοντος αρχείου, είναι επίσης δυνατό να δημιουργηθούν κακόβουλα αρχεία στο δίσκο. Πρόκειται για μια τυπική επίθεση παραβίασης όπου ένας εισβολέας δημιουργεί ένα αρχείο το οποίο υποτίθεται ότι θα δημιουργήσει ένα πρόγραμμα, απλώς για να εισάγει ψευδή δεδομένα σε αυτό πριν το πρόγραμμα προλάβει να κλειδώσει την

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

πρόσβαση του αρχείου. Σε κάθε περίπτωση, ο στόχος είναι να παραποιηθούν τα δεδομένα για να τα κάνουν να χάσουν την αξία και την χρηστικότητα τους (Stene, 2015).

Παραβίαση της μη αποποίησης

Η φράση "Δεν το έκανα" αποτελεί μια κοινή φράση που λέγεται όταν κάτι πήγε στραβά σε κάποια διαδικασία. Η μη αποκήρυξη ή η λογοδοσία είναι μια κατάσταση όπου δεν είναι δυνατόν να αμφισβητηθεί σε μια πράξη, όπως μπορεί να ισχυριστεί κάποιος, ότι δεν παραβίασε τους αριθμούς τηλεφώνου στη βάση δεδομένων πελατών. Αυτό είναι ένα κρίσιμο μέρος της ασφάλειας των πληροφοριών, ώστε να είναι σε θέση να διασφαλίσει την υπευθυνότητα σε ένα σύστημα. Για όλους τους χρήστες, τους διαχειριστές ή άλλα άτομα που έχουν πρόσβαση σε ένα πληροφοριακό σύστημα, θα πρέπει να είναι δυνατό να αποδείξουν ότι έκαναν ή δεν έκαναν κάτι. Ο ευκολότερος τρόπος για να διασφαλιστεί ότι είναι πιθανό να μην υπάρχει αποποίηση ευθύνης σε ένα σύστημα είναι να έχουμε, να διατηρούμε και να αναλύουμε αρχεία καταγραφής για κάθε ενέργεια. Όπως και με τον δυσαρεστημένο υπάλληλο που αρνείται ότι έχει αλλάξει όλους τους αριθμούς τηλεφώνου στη βάση δεδομένων, καταγράφοντας ποιος πράγματι διέπραξε τις αλλαγές στα αρχεία καταγραφής της βάσης δεδομένων, το χρηματοπιστωτικό ίδρυμα πρέπει να έχει αρκετές αποδείξεις για να διαψεύσει τη δήλωση του υπαλλήλου (Stene, 2015).

Παραβίαση της εμπιστευτικότητας

Στις περισσότερες περιπτώσεις, η αποκάλυψη πληροφοριών θεωρείται όταν ένα άτομο αποκαλύπτει μια πληροφορίας σε ένα άλλο άτομο, οποίο δεν πρέπει να γνωρίζει ή δεν έχει την άδεια να γνωρίζει. . Παρόλο που πρέπει να καταγράψουμε πράγματα που

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

συμβαίνουν στο σύστημά μας, πρέπει επίσης να επιλέξουμε προσεκτικά τι πρέπει να καταγράψουμε και ποια δεδομένα μπορούμε να παραλείψουμε από κάθε καταχώριση καταγραφής. Η αποκάλυψη πληροφοριών μπορεί να συμβεί γράφοντας κατά λάθος μυστικά δεδομένα σε αρχεία καταγραφής που περιέχουν χαμηλότερα επίπεδα εξουσιοδότησης από το αρχικό αρχείο. Εάν το αφεντικό του χρηματοπιστωτικού ιδρύματος προσπαθεί να αποθηκεύσει ένα αρχείο στον εφεδρικό διακομιστή του με το όνομα Termination Letter for Alice.docx αλλά αποτυγχάνει και μια καταχώριση καταγραφής τοποθετείται στα αρχεία καταγραφής ΣΦΑΛΜΑ: Δεν ήταν δυνατή η αποθήκευση της «Επιστολής τερματισμού για την Alice. docx », ο δίσκος είναι γεμάτος, τότε υπάρχει διαρροή πληροφοριών (Stene, 2015).

Το ίδιο το όνομα αρχείου αποτελεί δεδομένο, που έπρεπε να είναι ευαίσθητα και να είναι προσβάσιμα μόνο από τον υπολογιστή ή τον λογαριασμό χρήστη του αφεντικού, αλλά είναι πλέον προσβάσιμο σε οποιονδήποτε έχει δικαιώματα να δει τα αρχεία καταγραφής σφαλμάτων των εφεδρικών δίσκων.

Παραβίαση Διαθεσιμότητας

Οι επιχειρήσεις πρέπει να λειτουργούν αδιάλειπτα και να προσφέρουν τις υπηρεσίες τους συνεχώς στους πελάτες τους.. Αν όμως, για κάποιο λόγο, η βάση δεδομένων των πελατών της εταιρίας δεν είναι διαθέσιμη, τότε οι πελάτες δεν θα είναι σε θέση να αγοράζουν υπηρεσίες ή τα προϊόντα από την ιστοσελίδα της εταιρίας (Stene, 2015).

Για τα χρηματοπιστωτικά ιδρύματα μπορεί να είναι υπηρεσίες όπως αιτήσεις δανείων, άνοιγμα λογαριασμών και πώληση ασφαλιστικών συμβολαίων. Η άρνηση υπηρεσίας είναι μια πολύ σοβαρή απειλή για τις επιχειρήσεις και μπορεί να συμβεί τόσο εκ προθέσεως όσο και ακούσια. Είναι επομένως σημαντικό να εφαρμόζονται διασφαλίσεις που θα προστατεύουν το σύστημα από αυτούς τους τύπους απειλών. Μία

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

από τις πιο κοινές απειλές είναι οι επιθέσεις Distributed Denial of Service (DDOS) και μπορούν να προληφθούν χρησιμοποιώντας ένα σύστημα εξισορρόπησης φορτίου.

Παραβίαση της εξουσιοδότησης

Αυτή είναι η πιο σημαντική απειλή που πρέπει να εντοπίζεται και να μετριάζεται. Η απόκτηση μη εξουσιοδοτημένης πρόσβασης, επιτρέπει σε κάποιον να κάνει κάτι που δεν έχει το δικαίωμα ή την απαραίτητη άδεια. Ένα τέτοιο άτομο μπορεί να είναι ένας χρήστης που εκτελεί κάποιο πρόγραμμα σε έναν υπολογιστή ως διαχειριστής ή κάποιος που εκτελεί λειτουργίες από λογαριασμό χρήστη που δεν του ανήκει. Υπάρχουν δύο διαφορετικοί τύποι παραβιάσεων που σχετίζονται με δικαιώματα. Αυτό μπορεί να επιτευχθεί καταστρέφοντας μια διαδικασία σε έναν υπολογιστή, αλλά αυτό θα λειτουργήσει μόνο με την προϋπόθεση ότι ένας πιθανός εισβολέας έχει ήδη κάποιον έλεγχο του υπολογιστή ή του συστήματος. Ο δεύτερος τύπος των απειλών ανύψωσης-αύξησης δικαιωμάτων συμβαίνει όταν το σύστημα διαθέτει ελαττωματικούς ελέγχους πρόσβασης ή μπορεί να μην έχει καθόλου ελέγχους πρόσβασης (Stene, 2015).

Χρήση του STRIDE σε διαγράμματα ροής δεδομένων

Το STRIDE είναι ένα εργαλείο μοντελοποίησης απειλών που είναι εξαιρετικό για χρήση σε διαγράμματα ροής δεδομένων (DFDs). Τα DFDs είναι διαγράμματα που απεικονίζουν ποια μέρη ενός συστήματος ή ενός προγράμματος υπολογιστή επικοινωνούν μεταξύ τους καθώς και προς τα που κατευθύνεται η συνολική επικοινωνία. Σε πολλές περιπτώσεις υπάρχει μόνο ένας τρόπος επικοινωνίας από μέρη που απαιτούν χαμηλότερα επίπεδα προνομίων σε μέρη που απαιτούν υψηλότερα. Στη συνέχεια, τα δεδομένα διαβιβάζονται μεταξύ τμημάτων και ενδέχεται να υπόκεινται σε

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

απειλές, αλλά σε αυτήν την περίπτωση δεν είναι σημαντικό, καθώς τα δεδομένα διαβιβάζονται σε μέρη του συστήματος που έχουν υψηλότερο προνόμιο (Shostack & Long, 2014).

Η βασική αρχή σε αυτή την περίπτωση είναι η αποσύνθεση του συστήματος ή του προγράμματος υπολογιστή σε μέρη και ο έλεγχος ότι κάθε μέρος δεν είναι ευαίσθητο σε σχετικές απειλές. Ένα κανονικό DFD χρησιμοποιεί τέσσερα διαφορετικά στοιχεία που χρησιμοποιούνται στη μοντελοποίηση ενός συστήματος:

- Ροές δεδομένων
- Αποθήκευση δεδομένων
- Διεργασίες
- Αλληλεπιδράσεις.

Το STRIDE είναι ένα πολύ εύκολο εργαλείο στη χρήση κατά την αναζήτηση απειλών και υπάρχουν διάφορες παραλλαγές του STRIDE που μπορεί να είναι σημαντικά συμπληρώματα στο παραδοσιακό μοντέλο STRIDE (Shostack & Long, 2014).

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

4.3. Χρήση του μοντέλου CAPEC

Σε αυτό το κεφάλαιο, θα παρουσιαστεί ένα μοντέλο ανάλυσης απειλών, χρησιμοποιώντας τη λεπτομερή βιβλιοθήκη επίθεσης CAPEC. Το CAPEC είναι μια βιβλιοθήκη επίθεσης που βρίσκεται πολύ κοντά στο όριο πρακτικότητας και σε αυτό το κεφάλαιο εξετάζουμε πολλά μοτίβα επίθεσης από αυτήν τη βιβλιοθήκη. Η ανάλυση απειλών με την μέθοδο CAPEC, περιλαμβάνει 16 διαφορετικές κατηγορίες απειλών. Για την βαθμολόγηση και την αξιολόγηση των απειλών, θα χρησιμοποιηθεί το ίδιο σύστημα βαθμολογίας που χρησιμοποιείται και στην μέθοδο STRIDE. Αναλυτικότερα (Masrek et al., 2012):

Βαθμολογία 1: Δεν ισχύει ή μη εφαρμόσιμο - Αυτή η απειλή είτε έχει ήδη αντιμετωπιστεί πλήρως είτε δεν είναι δυνατή η αντιμετώπιση λόγω άλλων παραγόντων.

Βαθμολογία 2: Πιθανή απειλή - Αυτή η απειλή είναι είτε πολύ δύσκολο να εκτελεστεί, είτε όχι δυνατή, και μπορεί να θεωρηθεί ακίνδυνη.

Βαθμολογία 3: Τρέχουσα απειλή - Αυτή η απειλή είναι πολύ πιθανό να εκτελεστεί.

Παραβίαση JSON (γνωστό και ως json injections)

Η παραβίαση JSON (JavaScript Object Notation) ή αλλιώς η παραβίαση JavaScript αποτελεί μία μορφή επίθεσης στην οποία, ένας κακόβουλος χρήστης εκμεταλλεύεται τις ευπάθειες των αιτημάτων σε μορφή JSON, τα οποία αποστέλλονται από έναν υπολογιστή προς ένα εξυπηρετητή (server). Δεδομένου ότι μία εφαρμογή Mobile Banking χρησιμοποιεί αντικείμενα JSON για τη αποστολή των δεδομένων, υπάρχει πιθανή απειλή ένας κακόβουλος χρήστης να στείλει ψευδή αιτήματα.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Μία πιθανή αντιμετώπιση μιας τέτοιας απειλής, είναι να μπορεί ο διακομιστής (server) της τράπεζας να διακρίνει τα νόμιμα αιτήματα JSON και να απορρίπτει τα ψευδή αιτήματα και να υπάρχει ένας μηχανισμός ασφαλείας ώστε οι διευθύνσεις URL που χρησιμοποιεί το σύστημα να αποδέχονται με δυναμικό τρόπο αιτήματα JSON, ώστε να είναι μοναδικά για κάθε περίοδο σύνδεσης χρήστη (Faisal et al., 2017).

Στιγμιότυπα οθόνης εφαρμογής

Το λειτουργικό σύστημα iOS των κινητών συσκευών της εταιρίας Apple, χρησιμοποιεί μια διαχείριση εργασιών γραφικών. Αυτός ο διαχειριστής εργασιών, που ονομάζεται επίσης multitask switcher, χρησιμοποιεί στιγμιότυπα οθόνης όλων των εφαρμογών που εκτελούνται για να βοηθήσει τον χρήστη κατά την εναλλαγή μεταξύ εφαρμογών. Αυτά τα στιγμιότυπα οθόνης αποθηκεύονται στη συσκευή χρήστη και ο κακόβουλος χρήστης, μπορεί είτε να αποκτήσει πρόσβαση σε αυτά τα στιγμιότυπα οθόνης (με την μέθοδο jailbraking της μονάδας), είτε με φυσική πρόσβαση στο τηλέφωνο και με χρήση του multitask διαχειριστή εργασιών. Και στις δύο περιπτώσεις, ο εισβολέας χρειάζεται φυσική πρόσβαση στη συσκευή (Faisal et al., 2017).

Χρησιμοποιώντας αυτά τα στιγμιότυπα οθόνης, κάποιος μπορεί να αποκτήσει μη εξουσιοδοτημένη πρόσβαση σε πολύτιμες πληροφορίες. Αυτή η επίθεση αποτελεί απειλή τόσο για το λειτουργικό σύστημα των κινητών που διαθέτουν λειτουργικό σύστημα iOS, όσο και για την εφαρμογή mobile banking που εκτελείται στο σύστημα. Συνεπώς, το λειτουργικό σύστημα δεν πρέπει να αποθηκεύει αυτά τα στιγμιότυπα οθόνης για μεγάλο χρονικό διάστημα. Υπάρχουν δυνατότητες αντιμετώπισης αυτής της απειλής, αλλά οι περισσότερες από τις μεγάλες τράπεζες δεν έχουν φροντίσει να αντιμετωπίσουν αυτήν την απειλή σε ικανοποιητικό βαθμό. Πιθανές λύσεις, στην ευπάθεια που περιγράφηκε παραπάνω, περιλαμβάνει την απόκρυψη στοιχείων που

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

εμφανίζουν ευαίσθητα δεδομένα κατά την εναλλαγή μεταξύ ενεργών και μη εφαρμογών.

Εφαρμογή Αναφοράς Σφαλμάτων

Όλες οι πλατφόρμες, το Bank ID και οι εφαρμογές μπορούν να παρέχουν υπηρεσίες καταγραφής σφαλμάτων. Ένας εισβολέας μπορεί να προσπαθήσει να αποκτήσει πρόσβαση και να αξιοποιήσει το γεγονός ότι οι εφαρμογές αναφέρουν σφάλματα, ελέγχοντας επανειλημμένα το σύστημα και αναλύοντας τον τρόπο με τον οποίο το σύστημα αντιδρά σε σφάλματα. Αυτή η επίθεση μπορεί να είναι απειλή για την εφαρμογή. Εάν η εφαρμογή αποθηκεύει αρχεία καταγραφής στη συσκευή και οι πληροφορίες καταγραφής είναι σε απλό κείμενο, τότε ένας εισβολέας ενδέχεται να χρησιμοποιήσει αυτά τα αρχεία καταγραφής για να αναλύσει το σύστημα. Αυτή η επίθεση μπορεί να αντιμετωπιστεί εν μέρει, δημιουργώντας κωδικοποιημένα αρχεία καταγραφής. Ένα κωδικοποιημένο αρχείο καταγραφής δεν θα εμφανίζει ποτέ σφάλμα σε απλό κείμενο, αλλά μάλλον θα χρησιμοποιούσε ένα σύστημα κωδικού σφάλματος για την προστασία των πληροφοριών. Αυτό θα μετριάσει μόνο τις απειλές, αρκεί το αρχείο της πηγής του κώδικα να είναι μυστικό. Άλλες τεχνικές αντιμετώπισης θα είναι να μην πραγματοποιηθεί καταγραφή των αρχείων σφαλμάτων στη συσκευή, αλλά να γίνει αποστολή όλων των σφαλμάτων (κατά προτίμηση αποστολή με κρυπτογραφημένους κωδικούς σφάλματος) στον διακομιστή.

Διερεύνηση Πληροφοριών Λειτουργικών Συστημάτων (OS Fingerprinting)

Ένας κακόβουλος χρήστης μπορεί να προσπαθήσει να αποκτήσει πολύτιμες πληροφορίες σχετικά με το λειτουργικό σύστημα (OS) που εκτελείται σε διακομιστές συστήματος, εκτελώντας επιθέσεις fingerprinting. Με τη γνώση του λειτουργικού

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

συστήματος που εκτελείται σε διακομιστές συστήματος, ο κακόβουλος χρήστης μπορεί να σχεδιάσει πιο λεπτομερείς επιθέσεις με βάση το λειτουργικό σύστημα έναντι του συστήματος. Αυτό το είδος επίθεσης επηρεάζει όλα τα συστήματα σε αυτό το μοντέλο απειλής. Ένας εισβολέας μπορεί να αναζητήσει συσκευές με παλαιότερα λειτουργικά συστήματα κινητής τηλεφωνίας για να δοκιμάσει και να χρησιμοποιήσει αυτές τις συσκευές. Αυτό είναι ιδιαίτερα σημαντικό πρόβλημα με συσκευές που χρησιμοποιούν το εκάστοτε ευπαθές λειτουργικό σύστημα. Αυτή η επίθεση δεν έχει προτεινόμενη μέθοδο μετριασμού από την βιβλιοθήκη CAPEC και είναι πολύ δύσκολο να κρυφτεί η έκδοση του λειτουργικού συστήματος. Ο μόνος τρόπος αντιμετώπισης είναι προσωρινός και είναι η διατήρηση όλων των συστημάτων, διορθωμένων και ενημερωμένων, σύμφωνα με τις επίσημες εκδόσεις των λειτουργικών συστημάτων (Shostack & Long, 2014).

HTTP DoS

Ένας κακόβουλος χρήστης εκτελεί επιθέσεις DoS (Denial of Service), χρησιμοποιώντας αιτήματα HTTP σε διακομιστή προορισμού. Αυτός ο τύπος επίθεσης άρνησης υπηρεσίας απαιτεί λιγότερη επισκεψιμότητα και συνεπώς είναι πιο δύσκολο να εντοπιστεί. Αυτό το είδος επίθεσης μπορεί να επηρεάσει τους διακομιστές Bank ID / FOI και μπορεί να επηρεάσει εφαρμογές Mobile Banking που χρησιμοποιούν web browsers. Δεδομένου ότι αυτή η επίθεση χρησιμοποιεί το HTTP πρωτόκολλο, όλες οι εφαρμογές mobile banking που χρησιμοποιούν αίτημα HTTP για τη λήψη πληροφοριών από διακομιστές ιστού είναι πιθανώς ευάλωτες σε τέτοιου είδους επιθέσεις. Αυτή η επίθεση μπορεί να αντιμετωπιστεί εν μέρει ή πλήρως με τη διαμόρφωση διακομιστών ιστού για τον περιορισμό της περιόδου αναμονής σε συνεδρίες HTTP και με την εφαρμογή συστημάτων εξισορρόπησης φορτίου (load balance systems). Τα συστήματα εξισορρόπησης φορτίου δεν μετριάζουν εντελώς μια

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

απόπειρα μεγάλη επίθεση HTTP DoS, αλλά μπορεί να μετριάσουν τις μικρότερες επιθέσεις (Stene, 2015).

Checksum Spoofing

Το Checksum spoofing λαμβάνει χώρα όταν ένας κακόβουλος χρήστης πλαστογραφεί ένα μήνυμα checksum που αποστέλλεται σε έναν πελάτη ή σε έναν διακομιστή με σκοπό να κάνει ένα συγκεκριμένο φορτίο πληροφορίας που μεταφέρεται στο δίκτυο φαίνεται να είναι έγκυρο και ότι έχει σταλεί από έμπιστη πηγή. Αυτά τα είδη αθροίσματος ελέγχου χρησιμοποιούνται για την επαλήθευση της ακεραιότητας ενός μηνύματος μεταξύ του πελάτη και του διακομιστή. Όταν ο εισβολέας υποκλέψει ένα μήνυμα, αλλάζει το σώμα του μηνύματος και αλλάζει επίσης το αντίστοιχο άθροισμα ελέγχου ώστε να ταιριάζει με αυτό του σώματος του αρχικού μηνύματος. Ούτε αυτός ο τύπος επίθεσης, διαθέτει κάποια προτεινόμενη μέθοδο αντιμετώπισης, σύμφωνα με την μέθοδο CAPEC. Παρόλο που οι τράπεζες και άλλα ιδρύματα έχουν τονίσει και έχουν κάνει ανακοινώσεις, ώστε οι χρήστες Web Banking να μην αποκαλύπτουν ποτέ ευαίσθητες πληροφορίες μέσω email, εκτός εάν έχουν επικοινωνήσει απευθείας με την τράπεζα, αυτό εξακολουθεί να συμβαίνει. Εφόσον μεγάλος αριθμός χρηστών εξακολουθεί να είναι επιρρεπής στο να πείθεται και να παρέχει ευαίσθητες πληροφορίες όταν ερωτάται, τότε αυτές οι επιθέσεις δεν μπορούν να αντιμετωπιστούν πλήρως. Σαφώς η τεχνολογία πλέον έχει αυξήσει την αποτελεσματικότητα του ελέγχου της ακεραιότητας των δεδομένων χρησιμοποιώντας κρυπτογραφικές συναρτήσεις και συναρτήσεις hash.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Πλαστή Υπογραφή (spoof signature)

Με τη δημιουργία μηνυμάτων ή δεδομένων που ξεγελούν τον παραλήπτη για να πιστεύουν ότι το μπλοκ δεδομένων ή το μήνυμα δημιουργήθηκε και υπογράφηκε κρυπτογραφικά από αξιόπιστη πηγή, ο κακόβουλος χρήστης μπορεί να εξαπατήσει το θύμα (άτομο, εφαρμογή ή σύστημα) να εκτελέσει πολύτιμες ενέργειες. Αυτό το είδος επίθεσης μπορεί ενδεχομένως να επηρεάσει μια εφαρμογή mobile banking. Επειδή το σύστημα του Mobile Banking βασίζεται στη μεταφορά δεδομένων μεταξύ ενός πελάτη και ενός διακομιστή, μπορεί να θέσει σε κίνδυνο ολόκληρο το σύστημα. Προτεινόμενη μέθοδο αντιμετώπισης, αυτής της απειλής, είναι η χρήση PKI (Albarqi et al., 2015).

Ένα PKI αποτελείται από τα εξής συστατικά:

• **Αρχή Πιστοποίησης (Certification Authority).** Η Αρχή Πιστοποίησης είναι το κεντρικό συστατικό ενός PKI. Αποτελεί την έμπιστη τρίτη οντότητα η οποία είναι υπεύθυνη για την πιστοποίηση των δημόσιων κλειδιών των μελών. Η ακεραιότητα όλης της υποδομής συγκεντρώνεται στην Αρχή Πιστοποίησης.

• **Αρχή Εγγραφής (Registration Authority).** Η Αρχή Εγγραφής είναι προαιρετική. Εμφανίσθηκε κυρίως για εμπορικούς λόγους και στην περίπτωση απουσίας αυτής, τα καθήκοντά της αναλαμβάνει η Αρχή Πιστοποίησης. Η Αρχή Εγγραφής είναι υπεύθυνη για την αρχική εξακρίβωση των στοιχείων του μέλους, προτού πιστοποιηθεί το δημόσιό του κλειδί.

• **Εντολέας (Principal).** Είναι η οντότητα η οποία πιστοποιείται από την Αρχή Πιστοποίησης. Οι οντότητες με τις οποίες έχουμε ασχοληθεί είναι τα επικοινωνούντα μέλη, τα οποία είναι φυσικά πρόσωπα, αλλά μπορούν να είναι και υπολογιστές που βρίσκονται σε δίκτυο, μηχανές ATM των τραπεζών, κτλ.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

• **Πιστοποιητικό δημόσιου κλειδιού (Public key certificate).** Το πιστοποιητικό δημόσιου κλειδιού είναι μια δομή δεδομένων η οποία αποτελείται από ένα σύνολο στοιχείων που περιλαμβάνει δύο μέρη. Το πρώτο μέρος αποτελείται από την περιγραφή του εντολέα και το δημόσιο κλειδί του. Το δεύτερο μέρος του πιστοποιητικού αποτελείται από την ψηφιακή υπογραφή της Αρχής Πιστοποίησης επάνω στα στοιχεία του πρώτου μέρους.

• **Αποθήκη πιστοποιητικών (certificate repository).** Αποτελεί τον χώρο αποθήκευσης των πιστοποιητικών ενός PKI. Στην πράξη αυτό υλοποιείται από υπηρεσία καταλόγου (directory service) στο οποίο μπορούν να απευθυνθούν τα μέλη προκειμένου να παραλάβουν το δημόσιο κλειδί του μέλους με το οποίο επιθυμούν να επικοινωνήσουν.

Pharming

Μια επίθεση «Pharming», συμβαίνει όταν ένα στοχευμένο θύμα εξαπατάται να εισάγει ευαίσθητα δεδομένα σε έναν ιστότοπο που ο χρήστης πιστεύει ότι είναι αξιόπιστος. Αυτό γίνεται συνήθως αντιγράφοντας τη διάταξη και το σχεδιασμό από έναν ιστότοπο και, στη συνέχεια, στέλνοντας μηνύματα ηλεκτρονικού ταχυδρομείου με έναν σύνδεσμο προς τον ψεύτικο ιστότοπο όπου ο χρήστης έχει εντολή να εισαγάγει ευαίσθητα δεδομένα. Αυτού του είδους οι επιθέσεις είναι ένα υποσύνολο του κύριου μοτίβου επίθεσης. Η προτεινόμενη τεχνική αντιμετώπισης είναι να βεβαιωθεί ο χρήστης ότι όλα τα ευαίσθητα δεδομένα μεταδίδονται μέσω ασφαλούς σύνδεσης. Οι τελικοί χρήστες πρέπει να διασφαλίζουν ότι παρέχουν ευαίσθητες πληροφορίες μόνο σε ιστότοπους που εμπιστεύονται, μέσω ασφαλούς σύνδεσης με έγκυρο πιστοποιητικό που εκδίδεται από μια γνωστή αρχή έκδοσης πιστοποιητικών (Stene, 2015).

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Clickjacking

Το Clickjacking, γνωστό και ως "επίθεση επανόρθωσης UI (User Interface)",συμβαίνει όταν ένας εισβολέας χρησιμοποιεί πολλαπλά διαφανή ή αδιαφανή επίπεδα για να εξαπατήσει έναν χρήστη να κάνει κλικ σε ένα κουμπί ή να συνδεθεί σε άλλη σελίδα ενώ είχε σκοπό να κάνει κλικ στη σελίδα του ανωτέρου επιπέδου. Έτσι, ο εισβολέας "παγιδεύει" τα κλικ που προορίζονται για τη σελίδα του και τα δρομολογεί σε μια άλλη σελίδα, που πιθανότατα ανήκει σε άλλη εφαρμογή, τομέα ή και τα δύο. Χρησιμοποιώντας μια παρόμοια τεχνική, οι πληκτρολογήσεις μπορούν επίσης να καταγραφούν. Με έναν προσεκτικά σχεδιασμένο συνδυασμό stylesheets, iframes και πλαισίων κειμένου, ένας χρήστης μπορεί να οδηγηθεί να πιστέψει ότι πληκτρολογεί τον κωδικό πρόσβασης στο ηλεκτρονικό ταχυδρομείο ή τον τραπεζικό λογαριασμό του, αλλά αντ' αυτού γράφει σε ένα αόρατο πλαίσιο που ελέγχεται από τον εισβολέα

Συνεπώς, αν κάποιος χρήστης φορτώσει την εφαρμογή mobile banking μέσω web browser του κινητού, ο κακόβουλος χρήστης μπορεί να τοποθετήσει κουμπιά επικάλυψης και έτσι μπορεί να συλλέξει ευαίσθητες πληροφορίες, εξαπατώντας το θύμα, το οποίο πιστεύει ότι τα στοιχεία που πληκτρολογεί δίνονται σε ένα ασφαλή ιστότοπο. Μία λύση για την αντιμετώπιση αυτής της απειλής είναι η απενεργοποίηση JavaScript, Flash και CSS (Stene, 2015).

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ΚΕΦΑΛΑΙΟ 5- ΜΗΧΑΝΙΣΜΟΙ ΑΣΦΑΛΕΙΑΣ ΣΤΟ WEB ΚΑΙ MOBILE BANKING

Στο κεφάλαιο αυτό, θα παρουσιαστούν οι μηχανισμοί ασφάλειας που χρησιμοποιούνται σήμερα στο Web και στο Mobile Banking. Τα διάφορα τραπεζικά ιδρύματα χρησιμοποιούν έναν συνδυασμό από τους παρακάτω μηχανισμούς ασφάλειας, σε μία προσπάθεια να αποτραπεί η υποκλοπή στοιχείων εισόδου στις εφαρμογές Web banking. Θα πρέπει να σημειωθεί ότι δεν υπάρχει καμία στρατηγική που να αντιμετωπίζει με αποτελεσματικότητα όλους τους κινδύνους και τις απειλές (που έχουν αναφερθεί αναλυτικά σε προηγούμενο κεφάλαιο) του web και mobile Banking. Συνεπώς, η βέλτιστη λύση είναι ο συνδυασμός των προσεγγίσεων για την μεγιστοποίηση της ασφάλειας του συστήματος και για την προστασία των συμφερόντων των καταναλωτών, συμπεριλαμβανομένου ενός συνδυασμού διαφορετικών παραγόντων που το επιτρέπουν (Vrancianu et al., 2010) :

• Εφαρμογή συμπληρωματικής προστασίας για την συσκευή του τελικού χρήστη.

• Κοινοποίηση της πιθανής απάτης συναλλαγών στον τελικό χρήστη και εφαρμογή πολιτικών διαφάνειας.

• Προστασία της διαδικασίας ελέγχου ταυτότητας από κακόβουλες δραστηριότητες που μπορούν να επηρεάσουν την λειτουργία της συσκευής μέσω της οποίας συνδέεται ο πελάτης της τράπεζας (υπολογιστής, κινητό τηλέφωνο κ.α.).

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

• Παροχή στρατηγικών ελέγχου ταυτότητας χρήστη σε ιστότοπο που επιτρέπουν στον τελικό χρήστη να επαληθεύσει ότι η σύνδεση έχει πράγματι δημιουργηθεί με τη σωστή τοποθεσία.

• Εφαρμογή παραγόντων ελέγχου ταυτότητας που εξαλείφουν τις αποφάσεις των χρηστών από τη διαδικασία ελέγχου ταυτότητας.

5.1. Ταξινόμηση μηχανισμών Ασφάλειας

Σύμφωνα με τους Lao et al.(2010), η ταξινόμηση των μηχανισμών ασφάλειας στο web banking χωρίζονται σε τρεις κατηγορίες. Στην πρώτη κατηγορία, βρίσκονται οι μηχανισμοί ασφαλείας μετάδοσης και ελέγχου ταυτότητας, που είναι κυρίως οι μηχανισμοί τεχνικής ασφάλειας του Διαδικτύου. Στην δεύτερη κατηγορία, βρίσκονται οι μηχανισμοί ασφάλειας πληρωμών, οι οποίοι ανήκουν κυρίως στους μηχανισμούς ασφάλειας προστασίας κωδικού πρόσβασης πληρωμής και αφορούν κατά βάση τον τελικό χρήστη. Στην Τρίτη κατηγορία, ανήκουν οι μηχανισμοί προστασίας από ασυνήθιστη χρήση λογαριασμού.

Οι μηχανισμοί ασφαλείας μετάδοσης και ελέγχου ταυτότητας περιλαμβάνουν τα ακόλουθα μέτρα (Lao et al.(2010):

• Κρυπτογραφημένη μετάδοση SSL.

• Πιστοποιητικό CA του ιστότοπου.

• Πιστοποιητικό πελάτη.

• Έλεγχος ταυτότητας πληροφοριών ασφαλείας.

• Προστασία ιστότοπων από ηλεκτρονικό ψάρεμα (phishing).

• Προστασία λογαριασμού και υπενθύμιση.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Οι μηχανισμοί ασφάλειας πληρωμών περιλαμβάνουν τα ακόλουθα μέτρα:

- Έλεγχος διπλού κωδικού πρόσβασης.
- Δυναμική κάρτα κωδικού πρόσβασης.
- Εικονικό πληκτρολόγιο.
- Δοκιμή ισχύος κωδικού πρόσβασης και πολιτική αντικατάστασης.
- Ενεργός έλεγχος Χ.
- Αυτόματη παράταση.

Οι μηχανισμοί προστασίας από ασυνήθιστη χρήση λογαριασμού περιλαμβάνουν τα ακόλουθα μέτρα:

- Μηχανισμός για να παγώσει τον λανθασμένο κωδικό πρόσβασης.
- Κωδικός επαλήθευσης γραφικών.
- Έλεγχος εμπόρων.
- Το ποσό ελέγχου συναλλαγών.
- Ειδοποίηση πληροφοριών λογαριασμού μέσω SMS.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

5.2. Μηχανισμοί ασφάλειας στο Web Banking

Όπως αναφέρθηκε και σε προηγούμενο κεφάλαιο της παρούσης εργασίας, υπάρχουν διάφορες μέθοδοι επιθέσεων που στοχεύουν στην υποκλοπή στοιχείων κατά την πραγματοποίηση Online τραπεζικών συναλλαγών. Για αυτό το λόγο, τα χρηματοπιστωτικά ιδρύματα έχουν επενδύσει πολλά χρήματα, ώστε να αναπτυχθούν ισχυροί μηχανισμοί ασφάλειας. Ως εκ τούτου, οι περισσότεροι οργανισμοί αναζητούν πιο ασφαλείς μεθόδους για την προστασία των πελατών και των υπαλλήλων τους. Το πρώτο και το πιο σημαντικό στοιχείο στην ασφάλεια του Web Banking Προφανώς, είναι οι πελάτες ενός τραπεζικού ιδρύματος να εμπιστεύονται τα συστήματα web banking. Ειδικότερα, οι χρήστες του web banking θα πρέπει να νιώθουν σίγουροι ότι θα υπάρχει ασφάλεια από τις επιθέσεις κακόβουλων χρηστών, σχετικά με τα προσωπικά τους δεδομένα και θα εξασφαλίζεται η αποφυγή της κλοπής εμπιστευτικών πληροφοριών. Οι πλατφόρμες E-Banking προσφέρουν διάφορες μεθόδους για την εξασφάλιση υψηλού επιπέδου ασφάλειας:

(α) αναγνώριση και έλεγχο ταυτότητας

(β) κρυπτογράφηση

(γ) μηχανισμός τείχους προστασίας (firewalls).

Η αναγνώριση μιας διαδικτυακής τράπεζας έχει τη μορφή γνωστής διεύθυνσης Διαδικτύου ή Uniform Resource Locator (URL), ενώ ο πελάτης αναγνωρίζεται από το αναγνωριστικό σύνδεσης και τον κωδικό πρόσβασής του για να διασφαλίσει ότι μόνο εξουσιοδοτημένοι χρήστες μπορούν να έχουν πρόσβαση στους λογαριασμούς τους. Από την άλλη πλευρά, τα μηνύματα μεταξύ πελατών και διαδικτυακών τραπεζών είναι όλα κρυπτογραφημένα, έτσι ώστε ένα άλλο άτομο να μην

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

μπορεί να δει το περιεχόμενο των μηνυμάτων. Το κοινό πρότυπο κρυπτογράφησης που υιοθετήθηκε από τα περισσότερα προγράμματα περιήγησης ονομάζεται Secure Socket Layer (SSL) ή το πλέον διαδομένο tls που το αντικαθιστά.

Το τείχος προστασίας είναι ένα σύνολο σχετικών προγραμμάτων, που βρίσκονται σε διακομιστή πύλης δικτύου που προστατεύει τους πόρους ενός τραπεζικού δικτύου από χρήστες από άλλα δίκτυα. Είναι ένα σύνολο συσκευών που έχουν διαμορφωθεί ώστε να επιτρέπουν, να απορρίπτουν, να κρυπτογραφούν ή να αποκρυπτογραφούν όλη την κίνηση του υπολογιστή μεταξύ διαφορετικών τομέων ασφαλείας βάσει ενός συνόλου κανόνων. Μια πολυεπίπεδη αρχιτεκτονική ασφαλείας που περιλαμβάνει τείχη προστασίας, δρομολογητές φιλτραρίσματος, κρυπτογράφηση και ψηφιακή πιστοποίηση μπορεί να διασφαλίσει ότι οι πληροφορίες λογαριασμού πελατών προστατεύονται από μη εξουσιοδοτημένη πρόσβαση (Vrancianu et al., 2010).

5.2.1 Κρυπτογράφηση

Η κρυπτογράφηση είναι αναγκαία, καθώς αποτρέψει τυχόν απόπειρες από τους κακόβουλους χρήστες από την παραβίαση των συστημάτων web banking και την αποφυγή της υποκλοπής των ευαίσθητων πληροφοριών των πελατών τους. Η διαδικασία κρυπτογράφησης γίνεται ψηφιακά χρησιμοποιώντας μια υπογραφή που θα μπορούσε να αποθηκευτεί σε έξυπνες κάρτες ή σε οποιοδήποτε μέσο μνήμης (Khelifi et al., 2013).

Σήμερα, οι πιο ευρέως χρησιμοποιούμενοι αλγόριθμοι κρυπτογράφησης, φαίνεται να είναι οι μέθοδοι κρυπτογράφησης δύο κλειδιών, η κρυπτογράφηση με τριπλό DES και RC4 για συμμετρική κρυπτογράφηση για να διασφαλιστεί η

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

εμπιστευτικότητα των δεδομένων των συναλλαγών που πραγματοποιούνται σε διαδικτυακά τραπεζικά συστήματα. Επίσης, αποτελεσματική είναι η μέθοδος κρυπτογράφησης με τον αλγόριθμο RSA 1024-bit για ασύμμετρη κρυπτογράφηση και η χρήση της ψηφιακής υπογραφής και SHA-1/2 για μια λειτουργία κατακερματισμού σύμφωνα με τα διεθνή πρότυπα και οδηγίες που σχετίζονται με τις χρηματοοικονομικές συναλλαγές.

Οι περισσότεροι από αυτούς τους συμβατικούς αλγόριθμους κατακερματισμού κρυπτογράφησης υποστηρίζουν πολλές ψηφιακές υπογραφές και άλλα σχήματα ασφαλείας που χρησιμοποιούνται σε ολόκληρη τη διεθνή κοινότητα. Χρησιμοποιούνται ευρέως στον τραπεζικό τομέα αλλά και στο ηλεκτρονικό εμπόριο. Ωστόσο, είναι πολύ δύσκολο να διασφαλιστεί επαρκής ασφάλεια χρησιμοποιώντας τους συμβατικούς αλγόριθμους για μεγάλο χρονικό διάστημα, λόγω των πρόσφατων εξελίξεων όπως η υψηλή πρόοδος στις τεχνικές κρυπτανάλυσης, η βελτίωση των δεξιοτήτων υπολογιστών και οι συνεχείς δοκιμές εισβολής. Οι επιθέσεις εναντίον συμβατικών αλγορίθμων κρυπτογράφησης θα συνεχίσουν να αυξάνονται και να βελτιώνονται, καθιστώντας τις τεχνικές κρυπτανάλυσης πολύ πιο γρήγορες-αποδοτικές, έξυπνες και πιο προσιτές. Όλα αυτά καταδεικνύουν τη μεγάλη έλλειψη προστασίας και άμυνας στα χρηματοπιστωτικά ιδρύματα και τις εταιρείες επενδύσεών μας εάν επιμείνουμε να χρησιμοποιούμε μόνο αυτούς τους συμβατικούς κρυπτογραφικούς αλγόριθμους (Khelifi et al., 2013).

5.2.2 Έλεγχοι ταυτότητας

Το στάδιο σύνδεσης ενός πελάτη σε ένα σύστημα Web banking, χωρίζεται σε δύο επίπεδα ασφαλείας, το πρώτο χρησιμοποιεί το αναγνωριστικό χρήστη και τον κωδικό πρόσβασης συναλλαγής και το δεύτερο επίπεδο ασφαλείας με κωδικό

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

πρόσβασης χρησιμοποιεί προηγμένο σύστημα, όπως έναν κωδικό πρόσβασης μίας χρήσης, κάρτα εξουσιοδότησης δικτύου, κωδικός QR, βιομετρικά συστήματα, ερωτήσεις ασφαλείας και ηλεκτρονικό σήμα κ.λπ. Όλα αυτά τα συστήματα ασφαλείας έχουν αναπτυχθεί για την προστασία των τραπεζικών λογαριασμών του πελάτη από οποιοδήποτε μέλος της κοινότητας των εγκληματιών του κυβερνοχώρου. Οι τραπεζικές πληροφορίες μπορούν να τεθούν σε κίνδυνο από κακόβουλους χρήστες, τροποποιώντας το ηλεκτρονικό σύστημα πληροφοριών ενός χρηματοπιστωτικού ιδρύματος, διαδίδοντας κακόβουλους ιούς, κατεστραμμένα δεδομένα και υποβαθμίζοντας την ποιότητα της απόδοσης ενός συστήματος πληροφοριών. Έτσι, τα συστήματα ασφαλείας κωδικού πρόσβασης υψηλού επιπέδου χρησιμοποιούνται από τις τράπεζες για την προστασία από τέτοιου είδους επιθέσεις(Oppliger et al., 2009)

Έχει αποδειχθεί ότι οι κωδικοί μίας χρήσης, ο έλεγχος ταυτότητας δύο παραγόντων, η επαλήθευση ψηφιακού πιστοποιητικού παρέχουν περισσότερη ασφάλεια σε σύγκριση με την χρήση PIN ή κωδικών, τα οποία αποτελούν εύκολο στόχο για τους κακόβουλους χρήστες. Ο έλεγχος ταυτότητας είναι η διαδικασία επαλήθευσης της εγκυρότητας μιας ταυτότητας. Είναι ένας τρόπος να διασφαλιστεί ότι οι χρήστες είναι αυτοί που ισχυρίζονται ότι είναι όταν έχουν πρόσβαση στο σύστημα. Υπάρχουν τρεις παγκοσμίως αναγνωρισμένοι παράγοντες ελέγχου ταυτότητας:

- κωδικοί πρόσβασης
- βιομετρικά στοιχεία
- Μοναδικοί αριθμοί (κωδικοί) μιας χρήσης

5.2.3 Διακριτικό ασφάλειας

Το διακριτικό ασφαλείας είναι μια συσκευή υλικού που παρέχεται για την εξουσιοδότηση του χρήστη. Αναφέρεται επίσης ως διακριτικό ελέγχου ταυτότητας ή

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

κρυπτογραφικό διακριτικό. Τα κουπόνια διατίθενται σε δύο μορφές: υλικό και λογισμικό. Τα διακριτικά υλικού είναι μικρές συσκευές που είναι μικρές και μπορούν να μεταφερθούν εύκολα. Μερικά από αυτά τα διακριτικά αποθηκεύουν κρυπτογραφικά κλειδιά ή βιομετρικά δεδομένα, ενώ άλλα εμφανίζουν ένα PIN που αλλάζει με την πάροδο του χρόνου. Ανά πάσα στιγμή, όταν ένας χρήστης επιθυμεί να συνδεθεί, δηλαδή να κάνει έλεγχο ταυτότητας, χρησιμοποιεί το PIN που εμφανίζεται στο διακριτικό εκτός από τον κανονικό κωδικό πρόσβασης του λογαριασμού του. Τα διακριτικά λογισμικού είναι προγράμματα που εκτελούνται σε υπολογιστές και παρέχουν PIN που αλλάζει με την πάροδο του χρόνου.

5.2.4 Κωδικοί Ταυτοποίησης - One-time password (OTP) tokens

Οι αλγόριθμοι OTP είναι κρίσιμοι για την ασφάλεια των συστημάτων που χρησιμοποιούν, καθώς οι μη εξουσιοδοτημένοι χρήστες δεν θα πρέπει να μπορούν να μαντέψουν τον επόμενο κωδικό πρόσβασης στη σειρά. Η ακολουθία πρέπει να είναι τυχαία στο μέγιστο δυνατό βαθμό, απρόβλεπτη και μη αναστρέψιμη. Παράγοντες που μπορούν να χρησιμοποιηθούν στη δημιουργία OTP περιλαμβάνουν ονόματα, χρόνο, καρφίτσες ATM κ.λπ. Υπάρχουν αρκετά εμπορικά συστήματα ελέγχου ταυτότητας δύο παραγόντων όπως το BesBoken του BestBuy, το SecurID της RSA και το Secure Computing's Safeword Using tokens. και διανομή, έλεγχος ταυτότητας χρηστών και διακριτικών και ανάκληση χρηστών και διακριτικών μεταξύ άλλων. Ενώ τα διακριτικά παρέχουν πολύ πιο ασφαλές περιβάλλον για τους χρήστες, μπορεί να είναι πολύ δαπανηρό για τους οργανισμούς. Για παράδειγμα, μια τράπεζα με ένα εκατομμύριο πελάτες θα πρέπει να αγοράσει, να εγκαταστήσει και να συντηρήσει ένα εκατομμύριο μάρκες.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Επιπλέον, η τράπεζα πρέπει να παρέχει συνεχή υποστήριξη για την εκπαίδευση πελατών σχετικά με τον τρόπο χρήσης των κουπονιών. Οι τράπεζες πρέπει επίσης να είναι έτοιμες να παράσχουν αντικαταστάσεις εάν ένα διακριτικό σπάσει ή κλαπεί. Η αντικατάσταση ενός διακριτικού είναι πολύ πιο ακριβή από την αντικατάσταση μιας κάρτας ATM ή την επαναφορά ενός κωδικού πρόσβασης. Από την πλευρά του πελάτη, η κατοχή λογαριασμού σε περισσότερες από μία τράπεζες σημαίνει την ανάγκη μεταφοράς και διατήρησης πολλών μαρκών που αποτελούν μεγάλη αναστάτωση και μπορεί να οδηγήσει σε απώλεια, κλοπή ή καταστροφή των μαρκών. Σε πολλές περιπτώσεις, οι πελάτες χρεώνονται για κάθε διακριτικό. Προτείνουμε λοιπόν ένα διακριτικό λογισμικού για κινητά που θα εξοικονομήσει στους οργανισμούς το κόστος αγοράς και συντήρησης των διακριτικών υλικού. Ως εκ τούτου, θα ανησυχούν μόνο για τα κινητά τους τηλέφωνα αντί να ανησυχούν για πολλά διακριτικά υλικού (Chikomo et al., 2006).

Η παραπάνω διαδικασία πλέον υλοποιείται με αποστολή του μοναδικού κωδικού στο κινητό τηλέφωνο του πελάτη και συγκεκριμένα στον μοναδικό επίσημα καταχωρημένο προσωπικό αριθμό κινητού τηλεφώνου. Έτσι η τράπεζα πλέον γλυτώνει την συντήρηση μεγάλου σε αριθμό συσκευών καθώς επίσης και την ενημέρωση - εκπαίδευση των πελατών αναφορικά με την χρήση τους. Ωστόσο όπως έχουμε προαναφέρει μέγιστη ασφάλεια δεν υφίσταται ποτέ καθώς και σε αυτήν την περίπτωση παρατηρούμε να λαμβάνουν χώρα επιθέσεις sim swap σε πολλούς χρήστες τραπεζικών εφαρμογών κινητών τηλεφώνων.

5.3. Μηχανισμοί ασφάλειας στο Mobile Banking

Το mobile banking έχει δύο ζώνες ασφαλείας (Εικ. 2):

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

A) Ζώνη χειρός και ζώνη χειριστή κινητής τηλεφωνίας.

B) Εταιρείες κινητής τηλεφωνίας και ζώνες τραπεζικών συστημάτων.

Τα ζητήματα της ασφάλειας πληροφοριών στο mobile banking είναι περισσότερα σε σύγκριση με το web banking, καθώς οι κακόβουλοι χρήστες, έχουν πρόσβαση σε υπηρεσίες και πόρους, όπως ασύρματη πρόσβαση, υπηρεσίες αποστολής SMS. Η λειτουργία Mobile Banking μεταφέρει πληροφορίες μέσω ασύρματου δικτύου δεδομένων. Τα ασύρματα δίκτυα λαμβάνουν και στέλνουν δεδομένα , διαμορφώνουν και μεταδίδουν τα δεδομένα ως ραδιοκύματα. Συνεπώς, οι εμπιστευτικές τραπεζικές πληροφορίες ενδέχεται να διαρρεύσουν, να χαθούν ή να παραμορφωθούν κατά την μετάδοση των δεδομένων από τις κινητές συσκευές (Nie & Hu, 2008).

5.3.1. Κρυπτογράφηση ασύρματου καναλιού (WPKI)

Το WPKI (Υποδομή ασύρματου δημόσιου κλειδιού) αναπτύσσεται σταδιακά για να ανταποκρίνεται στις ανάγκες ενός ελέγχου ταυτότητας και κρυπτογράφησης ασύρματου δικτύου. Αυτή η τεχνολογία εισάγεται στο περιβάλλον ασύρματου δικτύου βάσει των μηχανισμών ασφαλείας PKI ηλεκτρονικού εμπορίου για να ακολουθήσει ένα σετ των καθιερωμένων προτύπων για το σύστημα πλατφορμών διαχείρισης κλειδιών και πιστοποιητικών.

Βέβαια, το WPKI δεν είναι ένα νέο πρότυπο, χρησιμοποιεί βελτιστοποιημένη κρυπτογράφηση ελλειπτικής καμπύλης ECC και ψηφιακά πιστοποιητικά X.509, χρησιμοποίησε επίσης δημόσιους οργανισμούς διεθνώς αναγνωρισμένους – Αρχές πιστοποίησης (CA) για να επαληθεύσει την ταυτότητα του χρήστη, αυτά βοηθούν

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

αποτελεσματικά στην καθιέρωση ασφάλειας και αξιόπιστου περιβάλλοντος ασύρματου δικτύου και διασφάλιση της ασφάλειας πληροφοριών, όπως δεδομένα σχετικά με τη μετάδοση, την ακεραιότητα των δεδομένων, τον έλεγχο ταυτότητας χρήστη και τη μη αποποίηση των συναλλαγών. Το WPKI βασίζεται στη βελτιστοποίηση του PKI.

Κατά την παράδοση ενός μηνύματος, ο αποστολέας χρησιμοποιεί το δημόσιο κλειδί σε ψηφιακά πιστοποιητικά δέκτη για την κρυπτογράφηση δεδομένων και, στη συνέχεια, οι παραλήπτες χρησιμοποιούν το δικό τους ιδιωτικό κλειδί για την αποκρυπτογράφηση. Με αυτόν τον τρόπο, αυτές οι πληροφορίες μπορούν να φτάσουν με ασφάλεια στους προορισμούς τους. Χρησιμοποιώντας την τεχνολογία WPKI, το mobile banking εγγυάται το απόρρητο των δεδομένων, την ακεραιότητα, την αυθεντικότητα και την ταυτότητα της μη αποποίησης συναλλαγών για την εξάλειψη του κινδύνου του χρήστη στη συναλλαγή. Η ανάπτυξη και βελτίωση της σχετικής τεχνολογίας στο WPKI, η διάρκεια των δεδομένων και η δυσκολία χειρισμού της πιστοποίησης WPKI θα μειωθούν περαιτέρω και που επιτυγχάνουν διαλειτουργικότητα μεταξύ WPKI και τυπικού PKI για τη δημιουργία καλύτερου περιβάλλοντος ασφάλειας για την ανάπτυξη κινητών τραπεζών (Nie & Hu, 2008).

5.3.2. Έλεγχος ταυτότητας συσκευής

Σε έρευνα που διεξήχθη από τους Narendiran et al. (2008) αναφορικά με τον έλεγχο ταυτότητας συσκευής και τον ρόλο του πιστοποιητικού X.509 κατέληξαν στα παρακάτω:

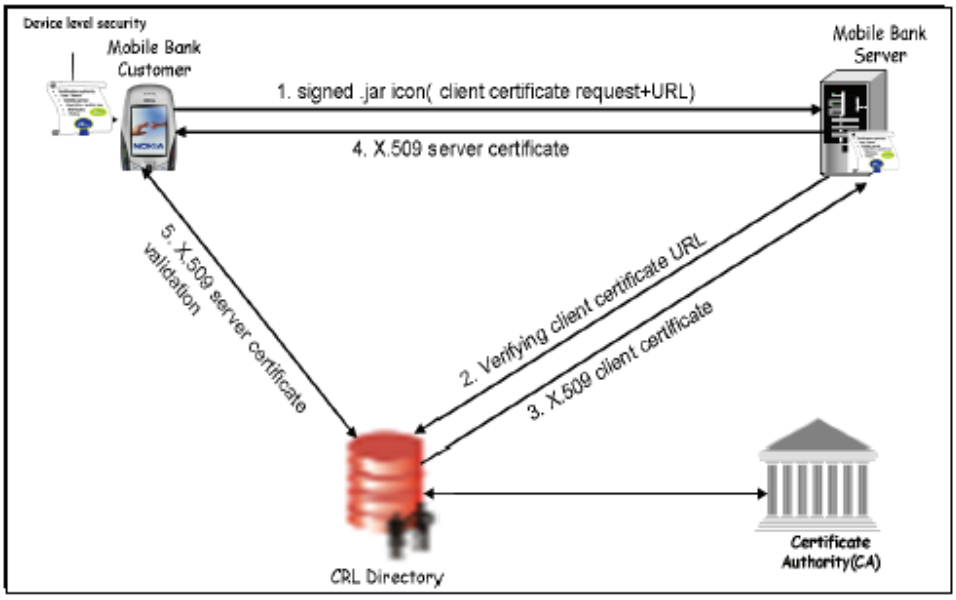
Το πιστοποιητικό πελάτη X.509 εφαρμόζεται για την επαλήθευση μιας κινητής συσκευής, η οποία συνδέεται με ένα αρχείο bank.jar χρησιμοποιώντας την ασύρματη εργαλειοθήκη J2ME 2.5 και αναπτύσσεται στη συσκευή με δυνατότητα MIDP. Επειδή

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

το πιστοποιητικό X.509 που ανήκει σε κινητή συσκευή επαληθεύεται επίσης από διακομιστή τράπεζας. Ο χρήστης του mobile banking μπορεί να ξεκινήσει να επικοινωνεί με το τραπεζικό Online σύστημα, μέσω του υπογεγραμμένου εικονιδίου bank.jar στην κινητή συσκευή. Στη συνέχεια, η κινητή συσκευή μπορεί να στείλει το πιστοποιητικό πελάτη και τη διεύθυνση URL του στον διακομιστή τράπεζας μέσω σύνδεσης GPRS. Ο διακομιστής τράπεζας μπορεί να αποκτήσει το πιστοποιητικό χρήστη μέσω της διεύθυνσης URL πελάτη (πιστοποιητικό πελάτη) από την CA και να επαληθεύσει με τον διακομιστή χρησιμοποιώντας το δημόσιο κλειδί πελάτη. Ταυτόχρονα, για τον διακομιστή χρησιμοποιείται X.509 βραχυπρόθεσμο πιστοποιητικό.

Εάν ο διακομιστής τράπεζας αποστέλλει πιστοποιητικό X.509 σε πελάτη κινητής τηλεφωνίας για επικύρωση πιστοποιητικού διακομιστή, ενδέχεται να απαιτείται αποτελεσματικό και ελαφρύ σχήμα επικύρωσης πιστοποιητικού στην κινητή συσκευή. Η κινητή συσκευή χρησιμοποιεί ένα πρωτόκολλο κατάστασης πιστοποιητικού στο Διαδίκτυο (OCSP) για την επικύρωση του πιστοποιητικού διακομιστή τράπεζας και όχι την επικύρωση από το ίδιο το κινητό τηλέφωνο (Narendiran et al. (2008). Το πιστοποιητικό του διακομιστή τράπεζας (βραχυπρόθεσμα) δεν έχει επεκτάσεις που χρησιμοποιούνται για επικύρωση διαδρομής πιστοποιητικού και έχει έγκυρη περίοδο για σύντομο χρονικό διάστημα. Επαληθεύεται μόνο εάν η υπογραφή της ΑΠ και η έγκυρη περίοδος για την επικύρωση πιστοποιητικού είναι έγκυρες. Εάν είναι έγκυρο πιστοποιητικό, τότε η συσκευή αναγνωρίζεται και ο έλεγχος ταυτότητας εμφανίζεται στο σχήμα 5.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ



Σχήμα 8- Ταυτοποίηση Συσκευής με το πιστοποιητικό X.509

Πηγή: Narendiranetal. (2008).

Μέσω μιας ασφαλούς σύνδεσης, το περιβάλλον εργασίας χρήστη bank.jar μπορεί να ξεκινήσει και να ζητήσει το αναγνωριστικό πελάτη (CID) και τον αριθμό pin (Pin num). Όταν ένας χρήστης εγγράφεται για να χρησιμοποιήσει τις υπηρεσίες κινητής τραπεζικής, ένας διακομιστής τράπεζας δημιουργεί ένα μυστικό κλειδί χρησιμοποιώντας τον αριθμό πελάτη. Το δημιουργημένο μυστικό κλειδί αποθηκεύεται στην εγγραφή της βάσης δεδομένων του πελάτη και το ίδιο πρέπει να χρησιμοποιείται από τις υπηρεσίες διακομιστή ελέγχου ταυτότητας και επεξεργασίας επιλογών.

Χρησιμοποιώντας αυτό το μυστικό κλειδί ο διακομιστής τράπεζας κρυπτογραφεί το δημόσιο κλειδί του διακομιστή στο πιστοποιητικό διακομιστή. Αυτό το υπογεγραμμένο πιστοποιητικό διακομιστή CA περιλαμβάνεται ως μέρος της εφαρμογής. Αυτό το πιστοποιητικό εκδίδεται για τον έλεγχο ταυτότητας του κατόχου

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

λογαριασμού στο τηλέφωνο. Όταν ένας χρήστης εισάγει το CID και το Pin-num του, το περιβάλλον εργασίας χρήστη δημιουργεί ένα μυστικό κλειδί χρησιμοποιώντας αυτό το Pin-num. Χρησιμοποιώντας αυτό το κλειδί, η διεπαφή χρήστη πελάτη προσπαθεί να αποκρυπτογραφήσει το δημόσιο κλειδί του διακομιστή στο πιστοποιητικό του διακομιστή. Εάν το δημόσιο κλειδί του διακομιστή αποκρυπτογραφηθεί επιτυχώς, ο αρχικός έλεγχος ταυτότητας πελάτη ολοκληρώθηκε ή αλλιώς ζητείται από τον πελάτη να εισαγάγει ξανά τον κωδικό πρόσβασης.

Ο πιο σημαντικός παράγοντας είναι ότι ο πελάτης επιτρέπεται μόνο σε ορισμένες προσπάθειες σύνδεσης, εάν η σύνδεση αποτύχει σε αυτές τις προσπάθειες ο λογαριασμός έχει αποκλειστεί. Μετά τον επιτυχή έλεγχο ταυτότητας πελατών, ο διακομιστής αναλαμβάνει τον δεύτερο έλεγχο ταυτότητας χρήστη και ο πελάτης κρυπτογραφεί το CID του χρησιμοποιώντας το μυστικό κλειδί και το στέλνει στον διακομιστή μαζί με το δημόσιο κλειδί του πελάτη. Ο διακομιστής ξεκινά εξάγοντας το δημόσιο κλειδί του πελάτη και τον χρησιμοποιεί ως παράμετρο στο ερώτημα βάσης δεδομένων στον πίνακα που περιέχει τις πληροφορίες χρήστη.

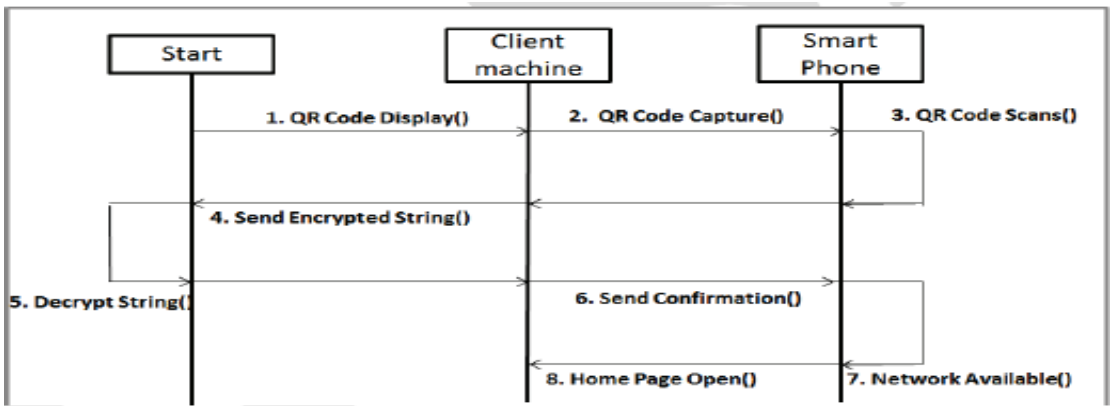
Εάν το ερώτημα επιστρέψει μηδενικό αποτέλεσμα, δηλαδή ο αιτούμενος χρήστης της τράπεζας κινητής τηλεφωνίας δεν έχει καμία καταχώριση στον πίνακα βάσης δεδομένων, ο διακομιστής τράπεζας στέλνει ένα μήνυμα "Δεν επιτρέπεται η πρόσβαση" στον πελάτη της κινητής τράπεζας. Εάν το ερώτημα επιστρέψει ένα έγκυρο αποτέλεσμα, ο διακομιστής εξάγει το μυστικό κλειδί, το αναγνωριστικό πελάτη και τον αριθμό pin που αντιστοιχούν στον πελάτη που ελήφθη στο αίτημα. Το κλειδί χρησιμοποιείται για την αποκρυπτογράφηση του ληφθέντος αιτήματος: εάν το αναγνωριστικό πελάτη και ο αριθμός pin που ανακτήθηκαν από τη βάση δεδομένων ταιριάζουν με το αναγνωριστικό πελάτη που έχει αποσταλεί από τον πελάτη, τότε ο πελάτης έχει πιστοποιηθεί. Ο διακομιστής τράπεζας στέλνει επίσης στον πελάτη ένα

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

μήνυμα καλωσορίσματος που επιβεβαιώνει τον έλεγχο ταυτότητας. Ο πελάτης μπορεί τώρα να προχωρήσει για να δει τη λίστα επιλογών ή υπηρεσιών που παρέχονται από την εφαρμογή διακομιστή τράπεζας (Narendiran et al., 2008).

5.3.3. QRP (Quick Response Protocol)

Το QRP είναι ένα πρωτόκολλο γρήγορης απόκρισης και αποτελεί ένα ασφαλές σύστημα ελέγχου ταυτότητας που χρησιμοποιεί έλεγχο ταυτότητας δύο παραγόντων συνδυάζοντας έναν κωδικό πρόσβασης και ένα κινητό τηλέφωνο με κάμερα, όπου το κινητό τηλέφωνο λειτουργεί ως διακριτικό ελέγχου ταυτότητας. Είναι πολύ ασφαλές και επίσης πολύ εύκολο στη χρήση για κρυπτογραφημένα δεδομένα. Είναι πολύ ασφαλές πρωτόκολλο για χρήση σε μη αξιόπιστους υπολογιστές. Η λειτουργία του συστήματος QRP παρουσιάζεται στην εικόνα 4.



Σχήμα 9- Τρόπος λειτουργίας του πρωτοκόλλου QRP

5.3.4. QR codes

Οι δισδιάστατοι γραμμωτοί κωδικοί (2D barcode) είναι ανοιχτά πρότυπα (ανοιχτούκώδικα), ενώ άλλοι είναι ιδιόκτητοι όπως Somacodes, Spotcodes, Rohs'visualcodes, ColorCode, Cybercode, MobileTag, VeriCode, ShotCode, eZcodes,

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

HotScan, Codablock F, Aztec, FP CCode (Fine Picture Code - Fujitsu) και BeeTagg (connVision). Τα PDF417 (Portable Data File) και MaxiCode χρησιμοποιούνται σύμφωνα με την AIM International ISO standardization.

Οι δύο πιο γνωστοί δισδιάστατοι ραβδοκώδικες είναι οι Data Matrix και QR code (ISO / IEC 18004: 2000). Δεν υπάρχει χρέωση άδειας για πληρωμή για τη χρήση ούτε Data Matrix ούτε QR-code. Παρόλο που μια μελέτη που τους συγκρίνει παραθέτει εξηγώντας την κωδικοποίηση ανωτερότητας, οι κωδικοί QR είναι πιο συνηθισμένοι στην Ασία και ιδιαίτερα δημοφιλείς στην Ιαπωνία (Lee et al., 2015).

Ο κωδικός QR είναι ένας δισδιάστατος γραμμικός κώδικας που εισήχθη από την ιαπωνική εταιρεία Denso-Wave το 1994. Αυτό το είδος γραμμικού κώδικα χρησιμοποιήθηκε αρχικά για την παρακολούθηση της απογραφής στην κατασκευή ανταλλακτικών οχημάτων και τώρα χρησιμοποιείται ευρέως σε μια ποικιλία βιομηχανιών. Το QR σημαίνει "Γρήγορη απόκριση", καθώς ο δημιουργός σκόπευε τον κώδικα να επιτρέψει την αποκωδικοποίηση του περιεχομένου του με υψηλή ταχύτητα. Κάθε σύμβολο κωδικού QR αποτελείται από μια περιοχή κωδικοποίησης και μοτίβα λειτουργιών, όπως φαίνεται στην εικόνα 5.

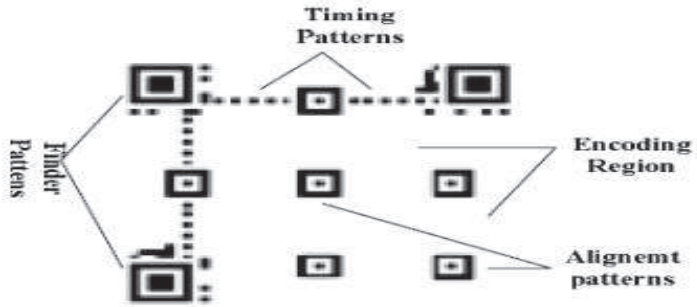


Σχήμα 10- Δημιουργία QR code

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Πηγή: Lee et al., 2015

Τα μοτίβα λειτουργιών περιλαμβάνουν εύρεση, διαχωριστικό, μοτίβα χρονισμού και μοτίβα ευθυγράμμισης. Τα μοτίβα εύρεσης βρίσκονται σε τρία άτομα του συμβόλου που προορίζονται να βοηθήσουν στην εύκολη θέση της θέσης, του μεγέθους και της κλίσης του. Ο κωδικός QR είναι ένας κωδικός μήτρας που αναπτύχθηκε και κυκλοφόρησε κυρίως για να είναι ένα σύμβολο που ερμηνεύεται εύκολα από τον εξοπλισμό σαρωτή. Περιέχει πληροφορίες τόσο σε κάθετες όσο και σε οριζόντιες κατευθύνσεις, ενώ ένας κλασικός γραμμικός κώδικας έχει μόνο μία κατεύθυνση δεδομένων (συνήθως την κάθετη) (Lee et al., 2015).



Σχήμα 11- Δομή ενός QR code

Πηγή: Πηγή: Lee et al., 2015

Σε σύγκριση με έναν γραμμικό κώδικα 1D, ένας κωδικός QR μπορεί να περιέχει έναν πολύ μεγαλύτερο όγκο πληροφοριών: 7.089 χαρακτήρες για αριθμητικά, 4.296 χαρακτήρες για αλφαριθμητικά δεδομένα, 2.953 bytes δυαδικών ψηφίων (8 bit) και 1.817 χαρακτήρες Ιαπωνικών συμβόλων Kanji / Kana. Εκτός αυτού, ο QR code έχει επίσης δυνατότητα διόρθωσης σφαλμάτων. Τα δεδομένα μπορούν να αποκατασταθούν ακόμη και όταν ουσιαστικά μέρη του κώδικα παραμορφωθούν ή καταστραφούν.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Στο πρότυπο QR-code, οι comers επισημαίνονται και υπολογίζονται έτσι ώστε ο εσωτερικός κώδικας να μπορεί να σαρωθεί. Η διαδικασία αναγνώρισης γραμμικού κώδικα έχει 5 βήματα:

(1) ανίχνευση άκρων

(2) ανίχνευση σχήματος

(3) αναγνώριση της γραμμής ελέγχου γραμμωτού κώδικα

(4) αναγνώριση του προσανατολισμού του γραμμικού κώδικα, των διαστάσεων και της πυκνότητας bit χρησιμοποιώντας τη γραμμή ελέγχου

(5) υπολογισμός της τιμής του γραμμικού κώδικα.

Για τηλέφωνα με κάμερα και PDA (Προσωπικός Ψηφιακός Βοηθός) που δεν είναι εξοπλισμένοι με συσκευές ανάγνωσης κωδικών QR, υπάρχουν μερικά πρόσθετα εργαλεία που αποκωδικοποιούν τους κωδικούς QR απλά τοποθετώντας τη συσκευή μπροστά από τον κωδικό. Αυτό γίνεται αυτόματα εντός της ροής και ο χρήστης δεν χρειάζεται να τραβήξει μια φωτογραφία του QR-code. Οι αναγνώστες QuickMark [11] και 1-nigma [12] είναι καλά παραδείγματα δωρεάν εργαλείων που χρησιμοποιούν αυτήν την τεχνική που είναι διαθέσιμα για πολλά κατασκευασμένα μοντέλα και συσκευές. Το QuickMark παρέχει λειτουργίες επέκτασης σε κωδικούς QR, επιτρέποντας μερική ή ολική κρυπτογράφηση κωδικών. Ένα άλλο ενδιαφέρον χαρακτηριστικό είναι το "Magic Jigsaw": αυτή η επιλογή κωδικοποιεί δυαδικά δεδομένα (για παράδειγμα μια εικόνα) ως μια αλυσίδα κωδικών QR που ο χρήστης μπορεί να σαρώσει για να ανακτήσει το αρχικό περιεχόμενο. Εναλλακτικά, εάν δεν υπάρχει διαθέσιμη σύνδεση δικτύου, η διαχείριση του κώδικα θα πρέπει να γίνει από

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

την κινητή συσκευή με αυτόνομο τρόπο. Εάν ο τελικός χρήστης χρειάζεται μόνο να σαρώσει κωδικούς και να δει τα αποτελέσματα των μηνυμάτων, το παραπάνω λογισμικό είναι αρκετά. Ωστόσο, οι προγραμματιστές, οι οποίοι πρέπει να διαχειριστούν τους κωδικούς QR, ορισμένα SDK (κιτ ανάπτυξης λογισμικού) ανακοινώνονται και μερικά είναι ήδη διαθέσιμα στην αγορά. Για έργα του Microsoft Windows Live Barcode, το OpenNetCF, το QRCode Library για το .NET Compact Framework και το έργο Google ZXing (Zebra Crossing) θα είναι σύντομα διαθέσιμα. Το Twit88 [13] παρέχει ένα έργο ανοιχτού κώδικα σε κωδικούς QR.

5.3.5. Βιομετρική ταυτοποίηση

Ένα βιομετρικό σύστημα είναι ουσιαστικά ένα σύστημα αναγνώρισης προτύπων το οποίο αναγνωρίζει ένα άτομο καθορίζοντας την αυθεντικότητα ενός συγκεκριμένου φυσικού χαρακτηριστικού ή συμπεριφοράς του ατόμου. Κατά τον σχεδιασμό του συστήματος αυτού πρέπει να καθοριστεί πρώτα ο τρόπος με τον οποίο ένα άτομο αναγνωρίζεται. Σύμφωνα με το είδος της αναγνώρισης το σύστημα μπορεί να χωριστεί στις παρακάτω δυο κατηγορίες:

a) Σύστημα ταυτοποίησης (Identification) βιομετρικών δεδομένων.

b) Σύστημα εξακρίβωσης (Verification) βιομετρικών δεδομένων

Η βιομετρική μέθοδος είναι γνωστό ότι είναι πολύ ασφαλής και χρησιμοποιείται σε πληθώρα οργανισμών και χρηματοπιστωτικών ιδρυμάτων, αλλά δεν χρησιμοποιείται πολύ για την εξασφάλιση διαδικτυακών συναλλαγών ή μηχανημάτων ATM, δεδομένου του ακριβού υλικού που απαιτείται για την αναγνώριση του θέματος και του κόστους συντήρησης κ.λπ. Αντ 'αυτού, τράπεζες και εταιρείες χρησιμοποιούν διακριτικά ως μέσο ελέγχου ταυτότητας δύο παραγόντων (Aithal, 2016).

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Ένα σύστημα εξακρίβωσης βιομετρικών δεδομένων, αναγνωρίζει την αυθεντικότητα της γνησιότητας της ταυτότητας ενός ατόμου συγκρίνοντας τα αποκτηθέντα από το σύστημα βιομετρικά χαρακτηριστικά με τα πρότυπα βιομετρικά χαρακτηριστικά του ατόμου με την γνήσια ταυτότητα, που έχουν αποθηκευτεί προηγουμένως στο σύστημα. Ένα σύστημα εξακρίβωσης απορρίπτει ή δέχεται ένα άτομο που ισχυρίζεται ότι έχει την συγκεκριμένη ταυτότητα σύμφωνα με τον βαθμό γνησιότητας των βιομετρικών χαρακτηριστικών του. Ακολούθως το σύστημα ταυτοποίησης αναγνωρίζει ένα άτομο αναζητώντας σε μια μεγάλη βάση δεδομένων, με βιομετρικά χαρακτηριστικά ,την ταυτότητα του ατόμου προς αναγνώριση.

Το σύστημα αυτό συγκρίνει ένα προς ένα τα αποθηκευμένα βιομετρικά χαρακτηριστικά της βάσης δεδομένων του συστήματος με τα βιομετρικά χαρακτηριστικά του ατόμου προς αναζήτηση, προκειμένου να εντοπίσει την ταυτότητα του ατόμου. Εάν τα χαρακτηριστικά του ατόμου δεν υπάρχουν στην βάση δεδομένων τότε το σύστημα αποτυγχάνει να τα εντοπίσει (fail). Σε ένα σύστημα ταυτοποίησης δεν υπάρχει ο ισχυρισμός του ατόμου προς αναγνώριση, για την γνησιότητα των βιομετρικών δεδομένων του. Ακολούθως παρουσιάζονται στο παρακάτω σχήμα ο τρόπος με τον οποίο γίνεται η εγγραφή (enrollment), η εξακρίβωση (verification) και η ταυτοποίηση (identification) (Tao, 2018).

Η διαδικασία της εγγραφής (enrolment) των βιομετρικών χαρακτηριστικών ενός ατόμου στην βάση δεδομένων (System DB) στο σύστημα αναγνώρισης γίνεται και στα δυο είδη αναγνώρισης. Κατά την εγγραφή καταχωρούνται στην βάση δεδομένων του συστήματος. Κατά την διαδικασία της εγγραφής, το βιομετρικό χαρακτηριστικό του ατόμου αποτυπώνεται από κάποιον αισθητήρα βιομετρικών χαρακτηριστικών και μετατρέπεται σε ψηφιακό σήμα. Ακολούθως πραγματοποιείται ένας έλεγχος ποιότητας (Quality checker) με σκοπό να επιβεβαιωθεί ότι το συγκεκριμένο δείγμα του

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

βιομετρικού χαρακτηριστικού μπορεί να επεξεργαστεί επιτυχώς στα επόμενα στάδια επεξεργασίας (Wang, 2018).

Στο επόμενο στάδιο ακολουθεί μια προεπεξεργασία (Preprocessing) με σκοπό την βελτίωση κάποιων χαρακτηριστικών του δείγματος, ώστε να επιτευχθεί η καλύτερη εξαγωγή των χαρακτηριστικών αυτών (Feature Extractor), τα οποία στο στάδιο της σύγκρισης (Matcher) θα χρησιμοποιηθούν για την αναζήτηση από την βάση δεδομένων. Η εξαγωγή κάποιων συγκεκριμένων χαρακτηριστικών γίνεται τόσο για να μειώσει των χρόνο αναζήτησης από την βάση όσο και να αυξήσει την αξιοπιστία της αναζήτηση. Τα χαρακτηριστικά (templates) που παράγονται από το στάδιο εξαγωγής (Feature Extractor) θα χρησιμοποιηθούν για την αναγνώριση, γι' αυτό αποθηκεύονται σε μια βάση βιομετρικών δεδομένων (System DB) μαζί με το όνομα του ατόμου (Template name) που αντιστοιχούν αυτά τα χαρακτηριστικά (Mittal et al., 2015).

Κατηγορίες μηχανισμών βιομετρικής αναγνώρισης.

Σήμερα, ανάλογα με τις κινητές συσκευές ή τις δυνατότητες που έχει ένας υπολογιστής, στο Web Και Mobile banking, χρησιμοποιούνται οι παρακάτω μέθοδοι βιομετρικής αναγνώρισης (Aithal, 2016):

• Αναγνώριση δακτυλικών αποτυπωμάτων: Επιβεβαίωση ταυτότητας με βάση τη σύγκριση δύο δακτυλικών αποτυπωμάτων. Αυτή η μέθοδος είναι ιδιαίτερα δημοφιλής στις φορητές συσκευές.

• Αναγνώριση φωνής / ηχείου: Αναφέρεται στην αναγνώριση ενός ατόμου από τα χαρακτηριστικά της φωνής του (σε αντίθεση με την αναγνώριση ομιλίας, η οποία αναγνωρίζει τι λέγεται).

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

• Αναγνώριση προσώπου: Χρήση διαφόρων τεχνολογιών όπως αλγόριθμοι υπολογιστών ή αισθητήρες 3D για την αναγνώριση ενός προσώπου χρησιμοποιώντας μέτρα όπως σχετική θέση, σχήμα ή μέγεθος ματιών, μύτης, σιαγόνων και άλλα.

• Αναγνώριση ίριδας: Αξιοποιεί τα περίπλοκα μοτίβα των ιρίδων στο μάτι κάθε ατόμου.

• Σάρωση του αμφιβληστροειδούς: Συχνά συγχέεται με την αναγνώριση της ίριδας, αναφέρεται στην αναγνώριση των αιμοφόρων αγγείων στον ανθρώπινο αμφιβληστροειδή.

• Χειρόγραφη υπογραφή: Χρήση χειρόγραφων μοτίβων υπογραφής για την αναγνώριση ενός ατόμου.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ΚΕΦΑΛΑΙΟ 6- ΕΠΙΘΕΣΕΙΣ ΣΤΟ WEB-MOBILE BANKING ΚΑΙ ΟΙ ΣΥΝΕΠΕΙΕΣ ΤΟΥΣ

Ο κυβερνοχώρος έχει αναγνωριστεί ως ο πέμπτος τομέας των πολεμικών επιχειρήσεων μετά την ξηρά, τον αέρα, τη θάλασσα και το διάστημα, με τη διαφορά ότι είναι ο μόνος που έχει δημιουργηθεί εξ' ολοκλήρου από τον άνθρωπο. Η αδιάκοπη εξάρτηση των ανθρώπινων δραστηριοτήτων από τις υποδομές πληροφοριών εγείρει το ζήτημα της ασφάλειας. Οι πιο επιζήμιες επιθέσεις στον κυβερνοχώρο είναι εκείνες κατά των κρίσιμων υποδομών και των πληροφοριακών συστημάτων. Στο κεφάλαιο αυτό θα παρουσιαστούν οι σημαντικότερες επιπτώσεις των επιθέσεων που σχετίζονται με το Web και Mobile Banking.

6.1. Το Κυβερνοέγκλημα στον τραπεζικό τομέα

Σήμερα το χρηματοπιστωτικό σύστημα αντιμετωπίζει ένα ιδιαίτερα σοβαρό κίνδυνο να προκληθεί παράπλευρη ζημιά σε μια ευρύτερη επίθεση σε κρίσιμες εθνικές υποδομές. Μια τέτοια επίθεση θα μπορούσε να κλονίσει την εμπιστοσύνη στο παγκόσμιο σύστημα χρηματοπιστωτικών υπηρεσιών, προκαλώντας σύγχυση ή πανικό στις τράπεζες, στις επιχειρήσεις και στους καταναλωτές γεγονός που με τη σειρά του θα μπορούσε να έχει σημαντικό αρνητικό αντίκτυπο στην παγκόσμια οικονομική δραστηριότητα(Mee & Schermann, 2018) .

Το έγκλημα στον κυβερνοχώρο σύμφωνα με τον Douglas and Loader (2000) μπορεί να οριστεί ως δραστηριότητες μέσω των υπολογιστών που διεξάγονται μέσω παγκόσμιων ηλεκτρονικών δικτύων οι οποίες είτε είναι παράνομες είτε θεωρούνται παράνομες από ορισμένα μέρη. Στον τραπεζικό τομέα, τα εγκλήματα στον κυβερνοχώρο που διαπράττονται μέσω διαδικτυακών τεχνολογιών για την παράνομη κατάργηση ή μεταφορά χρημάτων σε διαφορετικό λογαριασμό επισημαίνονται ως

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

τραπεζικές απάτες (Wall, 2001). Τα εγκλήματα στον κυβερνοχώρο σύμφωνα με τον Wall (2001) μπορούν να ταξινομηθούν σε τέσσερις κύριες κατηγορίες, δηλαδή εξαπάτηση στον κυβερνοχώρο, πορνογραφία στον κυβερνοχώρο, βία στον κυβερνοχώρο και παράβαση στον κυβερνοχώρο.

Οι τραπεζικές απάτες υποκατηγοριοποιούνται σε κυβερνο-απάτες που μπορεί να οριστούν ως ανήθικη δραστηριότητα, όπως κλοπή, απάτη με πιστωτικές κάρτες και παραβιάσεις πνευματικής ιδιοκτησίας (Anderson et al., 2012). Υπάρχουν πολλές απάτες ή εγκλήματα στον κυβερνοχώρο που παρατηρούνται στον τραπεζικό τομέα, όπως απάτες ATM, ξέπλυμα χρημάτων στον κυβερνοχώρο και απάτες με πιστωτικές κάρτες. Ωστόσο, σε γενικές γραμμές όλες οι απάτες εκτελούνται με απώτερο στόχο την απόκτηση πρόσβασης στον τραπεζικό λογαριασμό του χρήστη, την κλοπή χρημάτων και τη μεταφορά τους σε κάποιον άλλο τραπεζικό λογαριασμό.

Σε ορισμένες περιπτώσεις, οι εγκληματίες στον κυβερνοχώρο χρησιμοποιούν τα τραπεζικά διαπιστευτήρια όπως το PIN, τον κωδικό πρόσβασης, τα πιστοποιητικά κ.λπ. για να αποκτήσουν πρόσβαση σε λογαριασμούς και να κλέψουν ελάχιστο χρηματικό ποσό λαμβάνοντας υπόψη ότι σε άλλες περιπτώσεις μπορεί να θέλουν να κλέψουν όλα τα χρήματα και να μεταφέρουν τα χρήματα σε παράτυπους-παράνομους λογαριασμούς είτε σε λογαριασμούς νόμιμων χρηστών στους οποίους έχουν αποκτήσει πρόσβαση παίρνοντας τον έλεγχο με παράνομο τρόπο εκμεταλλευόμενοι κάποια ευπάθεια. Μερικές φορές, η πρόθεση των εγκληματιών στον κυβερνοχώρο είναι απλώς να βλάψουν την εικόνα της τράπεζας και επομένως, μπλοκάρουν τους διακομιστές της τράπεζας έτσι ώστε οι πελάτες να μην μπορούν να έχουν πρόσβαση στους λογαριασμούς τους (Claessens et al., 2002; Hutchinson&Warren, 2003).

Καθώς υπάρχουν πολλές αδυναμίες στο αμυντικό σύστημα του τραπεζικού τομέα, υπάρχει ανάγκη να διερευνηθούν οι τρόποι ευαισθητοποίησης σχετικά με τα μέτρα που μπορούν να ληφθούν για την καταπολέμηση των εγκλημάτων στον

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

κυβερνοχώρο στον τραπεζικό τομέα. Ωστόσο, δεν έχουν διεξαχθεί στο παρελθόν πολλές μελέτες σε αυτόν τον τομέα που θα προτείνουν τρόπους για τον μετριασμό των κινδύνων και την καταπολέμηση τέτοιων εγκλημάτων (Florencio & Herley, 2011; McCullagh & Caelli, 2005). Για να κατανοήσουμε το σύστημα απάτης στον τραπεζικό τομέα θα πρέπει να κατανοήσουμε και να περιγράψουμε τους επιτιθέμενους και τους υπερασπιστές σε αυτό το περιβάλλον.

Το έγκλημα στον κυβερνοχώρο κοστίζει σε χώρες περισσότερα από 1 τρισεκατομμύριο δολάρια παγκοσμίως, πολύ περισσότερο από το ρεκόρ ζημιών 300 δισεκατομμυρίων δολαρίων λόγω φυσικών καταστροφών το 2017, σύμφωνα με αναλύσεις που έχουν πραγματοποιηθεί κατά καιρούς από εταιρείες και οργανισμούς. Οι διαδικτυακές επιθέσεις θεωρούνται σήμερα ως η μεγαλύτερη απειλή που αντιμετωπίζει ο επιχειρηματικός και τραπεζικός τομέας και συνεχίζουν να βρίσκονται πάνω από την τρομοκρατία, τις λανθασμένες προβλέψεις αξίας περιουσιακών στοιχείων και άλλους κινδύνους. Μια επίθεση σε ένα δίκτυο επεξεργασίας υπολογιστών ή επικοινωνιών θα μπορούσε να προκαλέσει οικονομική ζημιά 50 δισεκατομμυρίων έως 120 δισεκατομμυρίων δολαρίων, μια απώλεια που κατατάσσεται κάπου μεταξύ των τυφώνων Sandy και Katrina, σύμφωνα με πρόσφατες εκτιμήσεις. Ωστόσο, μια πολύ ευρύτερη και πιο εξουθενωτική επίθεση δεν είναι ατελής (Tariq, 2018).

Ένα πιθανό σενάριο θα ήταν μια επίθεση που ενδέχεται να πραγματοποιείται από κυβερνήσεις ή τρομοκρατικές ομάδες σε χρηματοπιστωτικά ιδρύματα ή σε μεγάλες υποδομές. Στη Βόρεια Κορέα, για παράδειγμα, ο Όμιλος Lazarus, επίσης γνωστός ως Hidden Cobra, αναζητά συστηματικά τρόπους για συμβιβασμό τραπεζών και εκμετάλλευση κρυπτονομισμάτων. Μια επίθεση σε μια τράπεζα, ένα επενδυτικό ταμείο, μια εταιρεία φύλαξης, ένα δίκτυο ATM ή το διατραπεζικό δίκτυο ανταλλαγής μηνυμάτων γνωστό ως SWIFT θα αποτελούσε άμεσο πλήγμα στο σύστημα χρηματοπιστωτικών υπηρεσιών. Μια άλλη περίπτωση επίθεσης θα είχαμε εάν ένας

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

λεγόμενος hacktivist ή ερασιτέχνης "script kiddy" χρησιμοποιούσε κακόβουλα προγράμματα για να ξεκινήσει μια κυβερνοεπίθεση χωρίς να ληφθούν δεόντως υπόψη οι συνέπειες. Μια τέτοια επίθεση θα μπορούσε να έχει αλυσιδωτή αντίδραση προκαλώντας ζημιά πολύ πέρα από την αρχική πρόθεση, επειδή οι κανόνες και οι αρχές επίθεσης/πολέμου, που είναι για παράδειγμα η συμβατική σοφία η οποία εφαρμόζεται σε όλες τις καταστάσεις πολέμου, δεν υπάρχουν με ουσιαστικό τρόπο στον ψηφιακό κόσμο (Mee & Schermann, 2018) .

6.2. Επιπτώσεις

Οι επιθέσεις κατά της ασφάλειας των πληροφοριακών συστημάτων έχουν αυξηθεί τα τελευταία πέντε χρόνια, όπως διαφαίνεται είτε μέσω σχετικών αναλύσεων καθώς είτε μέσω της ενημέρωσης που έχουμε από σχετικούς εξειδικευμένους οργανισμούς. Ο αντίκτυπος των επιθέσεων στον κυβερνοχώρο στον τομέα των χρηματοοικονομικών υπηρεσιών έχει βραχυπρόθεσμες και μακροπρόθεσμες επιπτώσεις σε ιδιώτες και σε χρηματοοικονομικούς οργανισμούς. Σύμφωνα με τον Choo (2011) υπάρχουν αρκετές επιπτώσεις λόγω των κυβερνοεπιθέσεων στον τραπεζικό τομέα:

- Υπάρχει επίδραση στην καθημερινή δραστηριότητα των χρηστών (επηρεάζοντας την ικανότητα του χρήστη να αλληλεπιδρά με το χρηματοοικονομικό σύστημα, συμπεριλαμβανομένων γεγονότων όπως η αδυναμία ανάληψης μετρητών από ένα ATM)
- Αντίκτυπο στις καθημερινές δραστηριότητες των επιχειρήσεων και των κυβερνήσεων (συμπεριλαμβανομένης της αδυναμίας πρόσβασης σε δεδομένα όταν τους ζητηθεί)

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

- Η πιθανότητα αξιοποίησης πληροφοριών προσωπικής ταυτοποίησης (PII), οι οποίες μπορούν να οδηγήσουν σε νομικές αγωγές από τον χρήστη έναντι χρηματοπιστωτικών ιδρυμάτων που ρυθμίζονται για την προστασία του PII ενός χρήστη

- Αύξηση του λειτουργικού κόστους των χρηματοπιστωτικών ιδρυμάτων λόγω του κόστους δαπανηρών στρατηγικών μετριασμού της ασφάλειας στον κυβερνοχώρο

- Αύξηση της κοινωνικής και πολιτικής δυσαρέσκειας έναντι του πολιτικού συστήματος και της χρηματοοικονομικής υποδομής

- Υπάρχει απροθυμία από τα χρηματοπιστωτικά ιδρύματα να αναφέρουν παραβιάσεις δεδομένων, λόγω κυβερνητικών παραγόντων (κανονισμών κ.λπ.) και πιθανών αρνητικών πιέσεων.

Συνεπώς, κρίνεται αναγκαίο, τα τραπεζικά ιδρύματα να λάβουν υπόψη τις παραπάνω επιπτώσεις. Σε έρευνα του ο Ali (2018), εξέτασε τα θέματα των εγκλημάτων στον κυβερνοχώρο διερεύνησε πώς οι δραστηριότητες του εγκλήματος στον κυβερνοχώρο επηρεάζουν την ανάπτυξη των επιχειρηματικών τομέων, ιδίως στην περιοχή του Συμβουλίου Χωρών του Κόλπου . Τα δεδομένα της έρευνας συλλέχτηκαν μέσω ερωτηματολογίου από υπαλλήλους τραπεζικών τομέων και από το ευρύ κοινό και διαμορφώνεται συζήτηση σχετικά με τον τρόπο με τον οποίο τα μέτρα ασφαλείας θα μπορούσαν να ενισχυθούν περαιτέρω για τη βελτίωση του επιπέδου διαδικτυακής τραπεζικής ασφάλειας καθώς και της ανάπτυξης των επιχειρήσεων στο Συμβουλίου Χωρών του Κόλπου.

Στην συγκεκριμένη έρευνα, έγινε επίσης εξέταση των πρόσθετων συσκευών ασφαλείας για την ενίσχυση των επιπέδων ασφάλειας των διαδικτυακών τραπεζών. Τα

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ευρήματα της παραπάνω έρευνας δείχνουν ότι το έγκλημα στον κυβερνοχώρο είναι ένα από τα σημαντικά ζητήματα που πρέπει να αντιμετωπιστούν σωστά από τον τραπεζικό και χρηματοπιστωτικό κλάδο, καθώς οι επιπτώσεις των εγκλημάτων στον κυβερνοχώρο είναι κάτι περισσότερο από την οικονομική ακεραιότητα των χρηματοπιστωτικών ιδρυμάτων και άλλων οργανισμών. Επιπλέον, για να εφαρμοστούν οι κατάλληλες μετρήσεις, οι οργανισμοί πρέπει να κατανοήσουν τις επιπτώσεις των εγκλημάτων στον κυβερνοχώρο. Οι χρηματοοικονομικοί οργανισμοί πρέπει να γνωρίζουν τις διαδικτυακές απειλές και πρέπει να λαμβάνουν υπόψη όλα αυτά τα μέτρα που μπορούν να βοηθήσουν στη βελτίωση της ευαισθητοποίησης των ατόμων σχετικά με την ασφάλεια και στη διατήρηση βιώσιμου χρηματοοικονομικού επιχειρηματικού περιβάλλοντος (Ali, 2018).

Σε άλλη έρευνα, ο Chevers (2019), προτείνει ένα ερευνητικό μοντέλο που μπορεί να χρησιμοποιηθεί για την αξιολόγηση της σημασίας του εγκλήματος στον κυβερνοχώρο στην αποτροπή της χρήσης της ηλεκτρονικής τραπεζικής στον χρηματοπιστωτικό τομέα. Στην συγκεκριμένη έρευνα, ο Chevers (2019), μέσω ερωτηματολογίου, προτείνει ένα μοντέλο το οποίο μπορεί να υιοθετηθεί από άλλους ερευνητές με σκοπό να εξεταστεί ποιες από τις παρακάω τρεις μεθόδους: α) ηλεκτρονικό "ψάρεμα" (phishing) β) κλοπή ταυτότητας και γ) hacking έχουν τον μεγαλύτερο αντίκτυπό στο τομέα του Web Banking.

6.3. Οικονομικές επιπτώσεις

Τον Φεβρουάριο του 2014, μια προσωρινή μνήμη (cache) προσωπικών δεδομένων που περιείχε διαπιστευτήρια για 360 εκατομμύρια λογαριασμούς και 1,25 δισεκατομμύρια διευθύνσεις ηλεκτρονικού ταχυδρομείου πωλήθηκε σε μια διαδικτυακή μαύρη αγορά, σε μια από τις οποίες θεωρείται ευρέως η μεγαλύτερη παραβίαση δεδομένων στην ιστορία. Η μαζική συλλογή δεδομένων αποκτήθηκε μέσω

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

επιθέσεων στο Google, το Yahoo και τη Microsoft, μεταξύ άλλων για τρεις εβδομάδες, συμπεριλαμβανομένης μιας ανάσυρσης σχεδόν 105 εκατομμυρίων εγγραφών (Damodaran et al., 2017).

Η παραβίαση του Φεβρουαρίου του 2014 είναι ενδεικτική μιας ολοένα και πιο απειλητικής τάσης εγκληματιών του κυβερνοχώρου που χρησιμοποιούν κυβερνοεπιθέσεις ως μέσο για να προκαλέσουν σημαντική ζημία στον ιδιωτικό τομέα και απειλή εθνικής και οικονομικής ασφάλειας. Μια έκθεση του Ινστιτούτου Ponemon του Οκτωβρίου 2013 διαπίστωσε ότι σε έξι χώρες και 234 πολυεθνικές εταιρείες σχεδόν όλες είχαν πέσει θύμα επίθεσης με κακόβουλο λογισμικό και το 57% παρουσίασε επιθέσεις Distributed Denial of Service (DDoS).

Σύμφωνα με την έκθεση, οι εταιρείες παραβιάστηκαν 1,3 φορές την εβδομάδα με ετήσιο κόστος περίπου 7,2 εκατομμύρια δολάρια. Η αύξηση της κακόβουλης δραστηριότητας δείχνει ότι οι οργανισμοί δεν μπορούν πλέον να αποφύγουν την αναπόφευκτη απειλή στον κυβερνοχώρο και πρέπει να προετοιμάσουν επαρκώς ή να διακινδυνεύσουν σημαντική απώλεια. Οι επιθέσεις στον κυβερνοχώρο έχουν αποδειχθεί ότι είναι μια δύναμη για ομάδες hacking και κρατικούς οργανισμούς που επιδιώκουν να ισορροπήσουν το πεδίο ανταγωνισμού με τους ανταγωνιστές.

Η απειλή των κακόβουλων χρηστών σε συνδυασμό με την τεράστια επικίνδυνη και δαπανηρή απειλή απάτης ή κλοπής πνευματικής ιδιοκτησίας από εσωτερικούς κακόβουλους (insider threats) έχει δημιουργήσει μια ασταθή κατάσταση στον ιδιωτικό τομέα. Ενώ η πλειονότητα των εσωτερικών παραβιάσεων οφείλεται σε αμέλεια των εργαζομένων ή σε ανθρώπινο λάθος, οι επιθέσεις από κακόβουλους εργαζόμενους με πρόσβαση σε ευαίσθητες πληροφορίες της εταιρείας έχουν αυξηθεί δραματικά τα τελευταία χρόνια. Η απειλή της οικονομικής απώλειας, η κλοπή ευαίσθητων πληροφοριών και η καταστροφή σε κρίσιμους τομείς έχουν καταστήσει την ασφάλεια στον κυβερνοχώρο κορυφαία προτεραιότητα στον κόσμο. Παράλληλα η

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

αύξηση της συχνότητας και της πολυπλοκότητας των επιθέσεων κατά της βιομηχανίας έχει αυξήσει την πιθανότητα του αιφνιδιασμού καθώς και του κινδύνου μη αναμενόμενου συμβάντος. Επίσης έχει επηρεάσει το κόστος πρόληψης και ανάκαμψης από κυβερνοεπιθέσεις.

Σύμφωνα με έρευνα του Financial Fraud Action. (2015), οι απώλειες από διαδικτυακή τραπεζική απάτη αυξήθηκαν κατά 48% το 2014 σε σύγκριση με το 2013, καθώς οι καταναλωτές χρησιμοποιούν όλο και περισσότερο το web και Mobile Banking για την πραγματοποίηση οικονομικών συναλλαγών. Η αύξηση των περιστατικών αυτών, οφείλεται στην αυξημένη χρήση κακόβουλου λογισμικού, το οποίο εγκαθίσταται στις συσκευές των χρηστών, αλλά και στην αύξηση των περιστατικών phishing, δηλαδή της απάτης μέσω ηλεκτρονικού ταχυδρομείου. Σύμφωνα με την παραπάνω έρευνα, οι συνολικές απώλειες οι οποίες προήλθαν από υποκλοπή στοιχείων χρεωστικών και πιστωτικών καρτών, στο Ηνωμένο Βασίλειο ανήλθαν σε £ 479 εκ. για το 2014, δηλαδή αύξηση 6% σε σύγκριση με το έτος 2013. Βέβαια, θα πρέπει να σημειωθεί, πως το έτος 2008, στο Ηνωμένο Βασίλειο το συνολικό ποσό από απώλειες περιστατικών υποκλοπής στοιχείων καρτών ήταν £ 609,9 εκ., πράγμα που σημαίνει μείωση κατά 20% περίπου.

Επίσης, τα στοιχεία της έρευνας, έδειξαν ότι οι απώλειες που προκλήθηκαν από εγκληματίες που χρησιμοποίησαν κάρτες του Ηνωμένου Βασιλείου παράνομα στο εξωτερικό, όπου μπορούν να παρακάμψουν ορισμένα χαρακτηριστικά ασφαλείας, αυξήθηκαν απότομα. Οι απώλειες αυξήθηκαν στα 150,3 εκ. £ το 2014, σημειώνοντας αύξηση 23% σε σχέση με το έτος 2013.

Σύμφωνα με την έκθεση της Assocham και της PwC, καθώς αυξήθηκε η χρήση των κινητών συσκευών για την πρόσβαση στο Mobile Banking, αυξήθηκαν παράλληλα και οι οικονομικές απάτες των πελατών των τραπεζικών ιδρυμάτων. Η έκθεση ανέφερε ότι οι οικονομικές απάτες οδήγησαν σε άμεσες απώλειες 20 δισεκατομμυρίων

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

δολαρίων (1,26 εκατομμυρίων Rs) ετησίως. Η έκθεση αναφέρει ότι επί το έτος 2015 , το 74% του πληθυσμού διαθέτει κινητά τηλέφωνα και αυτό οδήγησε σε μια σταθερή αύξηση των κυβερνοεγκληματιών (More et al., 2016).

Επιπλέον, σύμφωνα με τα στοιχεία της Reserve Bank of India, ο όγκος των συναλλαγών του Mobile Banking αυξήθηκε από περίπου 1.819 εκατομμύρια Rs το χρονικό διάστημα 2011–12 σε περίπου 1.01.851 εκατομμύρια Rs το διάστημα 2014-15. Ο τραπεζικός όμιλος Mahindra, δήλωσε ότι ο αριθμός των εγκλημάτων στον κυβερνοχώρο στη Ινδία αναμένεται να διπλασιαστεί και το έτος 2020. Σύμφωνα με τη παραπάνω έρευνα, τα εγκλήματα στον κυβερνοχώρο αυξάνονται με ρυθμό 107% σε ετήσια βάση, ενώ καταγράφηκαν περισσότερες από 12.000 περιπτώσεις κάθε μήνα. Ο αριθμός των περιπτώσεων των κυβερνοεγκλημάτων ήταν 13.301 το 2011, ακολουθούμενες από 22.060 τέτοιες υποθέσεις το 2012 και 71.780 περιπτώσεις το 2013. Μόνο τον Μάιο του 2014 στην Ινδία είχε σημειωθεί μια ραγδαία αύξηση σε υποθέσεις εγκλήματος στον κυβερνοχώρο και καταχωρήθηκαν 62.189 υποθέσεις. Η αυξανόμενη χρήση κινητών, έξυπνων τηλεφώνων, tablet για διαδικτυακές τραπεζικές συναλλαγές και χρηματοοικονομικές συναλλαγές έχει επίσης αυξηθεί σε μεγάλο βαθμό λόγω των ευπαθειών των συστημάτων (Moreetal., 2016).

Στις αρχές του 2017, σημειώθηκε ένα κύμα επιθέσεων με στόχο την επεξεργασία καρτών στην Ανατολική Ευρώπη. Έχοντας διεισδύσει στην υποδομή της τραπεζών, οι εγκληματίες απέκτησαν πρόσβαση σε συστήματα επεξεργασίας καρτών και αύξησαν τα όρια υπερανάληψης καρτών. Απενεργοποίησαν επίσης τα συστήματα καταπολέμησης της απάτης που συνήθως ειδοποιούν την τράπεζα για δόλιες συναλλαγές. Ταυτόχρονα, οι συνεργάτες τους πραγματοποιούσαν ανάληψη μετρητών από ATM σε άλλη χώρα. Οι εγκληματίες είχαν προηγουμένως αποκτήσει τραπεζικές κάρτες με πλαστά έγγραφα και ταξίδεψαν έξω από τη χώρα στην οποία βρίσκεται η τράπεζα του θύματος. Σε κάθε περίπτωση, το μέσο ποσό κλοπής ήταν περίπου 5 εκατομμύρια δολάρια (Khan, 2018).

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Δύο χρόνια νωρίτερα, παρόμοιες τακτικές εφαρμόστηκαν από την εγκληματική οργάνωση Metel. Έχοντας διεισδύσει στην υποδομή μιας τράπεζας, οι εγκληματίες μπόρεσαν να ακυρώσουν τις συναλλαγές με κάρτες και να επαναφέρουν τα υπόλοιπα, ενώ οι συνεργάτες τους μετακινήθηκαν από το ένα ATM στο άλλο, κλέβοντας εκατομμύρια ρούβλια (Abreu et al., 2018).

Το φθινόπωρο του 2017,εγκληματίες του κυβερνοχώρου επιτέθηκαν στη Διεθνή Τράπεζα της Άπω Ανατολής στην Ταϊβάν πραγματοποιώντας μεταφορές σε λογαριασμούς στην Καμπότζη, τη Σρι Λάνκα και 4 εκατομμύρια δολάρια στις ΗΠΑ. Ενώ οι τράπεζες στο Νεπάλ έκλεισαν για διακοπές, οι εγκληματίες χρησιμοποίησαν το SWIFT για να αποσύρουν χρήματα. Οι τράπεζες μπόρεσαν να παρακολουθήσουν τις συναλλαγές και να ανακτήσουν ένα σημαντικό μέρος των κλεμμένων κεφαλαίων μόνο λόγω έγκαιρης ανταπόκρισης. Στις αρχές Δεκεμβρίου, δημόσιες πηγές άρχισαν να αναφέρουν την εγκληματική οργάνωση Money Taker, η οποία είχε επιτεθεί σε χρηματοπιστωτικά ιδρύματα στη Ρωσία και στις Ηνωμένες Πολιτείες για ενάμιση χρόνο. Οι εγκληματίες επιτέθηκαν σε συστήματα επεξεργασίας καρτών και διατραπεζικών μεταφορών, με κλοπές κατά μέσο όρο 500.000 δολάρια στις ΗΠΑ και 72 εκατομμύρια RUB (~ 1,26 εκατομμύρια δολάρια) στη Ρωσία. Τον Δεκέμβριο του 2017, δημοσιεύθηκαν αναφορές για την πρώτη επιτυχή επίθεση SWIFT σε ρωσική τράπεζα. Το θύμα της επίθεσης ήταν η Globex, θυγατρική της VEB. Ύποπτη θεωρήθηκε η εγκληματική οργάνωση Cobalt, η οποία ειδικεύεται σε κυβερνοεπιθέσεις σε τράπεζες (Abreu et al., 2018).

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

6.4 Timeline Επιθέσεων

Στην ενότητα αυτή, παρουσιάζεται ένα χρονοδιάγραμμα των επιθέσεων που πραγματοποιήθηκαν σε διάφορες χώρες, οι οποίες έλαβαν χώρα από το έτος 2007 έως το έτος 2019.

Απρίλιος 2007- Εσθονία

Μετά την αμφισβητούμενη μετεγκατάσταση ενός αγάλματος της σοβιετικής εποχής στο Ταλίν, η Εσθονία έπεσε θύμα μιας σειράς συντονισμένων επιθέσεων DDoS εναντίον κυβερνητικών, τραπεζικών, πανεπιστημίων και ιστότοπων εφημερίδων που διήρκεσαν τρεις εβδομάδες. Οι επιθέσεις ξεκίνησαν στις 26 Απριλίου, όταν διακόπηκαν οι διακομιστές email και οι ιστότοποι κυβερνητικών και πολιτικών κομμάτων. Την επόμενη εβδομάδα, ξεκίνησε ένα δεύτερο κύμα που διέκοψε την πρόσβαση σε ιστότοπους ειδήσεων της Εσθονίας. Το τελευταίο κύμα, που ξεκίνησε στις 9 Μαΐου, ήταν το βαρύτερο και στοχεύει τον εσθονικό τραπεζικό τομέα. Η επίθεση ανάγκασε δύο μεγάλες Εσθονικές τράπεζες να αναστείλουν τις διαδικτυακές τραπεζικές συναλλαγές, απενεργοποιώντας τις συναλλαγές τραπεζικών καρτών και τις αναλήψεις ATM. Η διαταραχή δεν τελείωσε μέχρι τη λήξη των συμβολαίων botnet των επιτιθέμενων στις 19 Μαΐου. Οι επιθέσεις πραγματοποιήθηκαν από Ρώσους hacktivists επικοινωνώντας ανοιχτά σε συνομιλίες ρωσικής γλώσσας, όπου οι χρήστες κοινοποίησαν ακριβείς οδηγίες σχετικά με τον τρόπο διεξαγωγής των επιθέσεων. Η Εσθονία κατηγόρησε τη ρωσική κυβέρνηση ότι διέταξε τις επιθέσεις, αλλά δεν μπόρεσε να αποδείξει οριστικά (Carnegie, 2020).

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Σεπτέμβριος 2007

Στις 14 Σεπτεμβρίου 2007, η διαδικτυακή εταιρεία μεσιτείας TD Ameritrade αποκάλυψε ότι η βάση δεδομένων της ήταν ο στόχος μιας παραβίασης δεδομένων που οδήγησε σε κλοπή 6,3 εκατομμυρίων αρχείων λογαριασμών πελατών. Οι επιτιθέμενοι απέκτησαν πρόσβαση στη βάση δεδομένων της Ameritrade μέσω email ηλεκτρονικού ψαρέματος με θέμα την επένδυση. Σύμφωνα με την Ameritrade, δεν ήταν δυνατή η πρόσβαση σε ευαίσθητα δεδομένα στη βάση δεδομένων, όπως αριθμοί κοινωνικής ασφάλισης κατά τη διάρκεια της παραβίασης. Δεν εντοπίστηκε κλοπή αναγνώρισης μετά την παράβαση. Ωστόσο, οι πελάτες ισχυρίστηκαν ότι έχουν λάβει ανεπιθύμητα μηνύματα ηλεκτρονικού ταχυδρομείου. Το FBI και οι δημοσιονομικές αρχές των ΗΠΑ διερεύνησαν το περιστατικό, αλλά δεν αναφέρθηκαν συλλήψεις. Στις 13 Σεπτεμβρίου 2011, η TD Ameritrade συμφώνησε να πληρώσει στους πελάτες 6,5 εκατομμύρια δολάρια για να διευθετήσει μια αγωγή κατηγορίας σε σχέση με την παραβίαση (Carnegie, 2020).

Γαλλία 2008

Τον Ιανουάριο του 2008, ένας κατώτερος έμπορος στη γαλλική τράπεζα Société Générale πραγματοποίησε δόλιες συναλλαγές για να καλύψει ζημίες 7,2 δισεκατομμυρίων δολαρίων από επικίνδυνες μελλοντικές συναλλαγές. Ο αδίστακτος έμπορος έκρυψε τις απώλειές του, κάνοντας κράτηση για ψεύτικες συναλλαγές συμψηφισμού σε λογαριασμούς συναδέλφων και χρησιμοποιώντας γνώσεις από τον προηγούμενο ρόλο του στο back office για να αλλάξει εσωτερικούς ελέγχους κινδύνων, ώστε να μην προκαλεί εσωτερικές ειδοποιήσεις. Σε ένα σημείο, το χαρτοφυλάκιο μη εξουσιοδοτημένων συναλλαγών είχε αξία άνω των 50 δισεκατομμυρίων ευρώ, περίπου την ίδια αξία με ολόκληρη την εταιρεία. Ο υπάλληλος συνελήφθη και καταδικάστηκε σε ποινή φυλάκισης τριών ετών το 2010. Η τράπεζα υπέστη μία από τις μεγαλύτερες

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

εμπορικές απώλειες που καταγράφηκαν λόγω του συμβάντος και η γαλλική τραπεζική αρχή επέβαλε ποινή 6 εκατομμυρίων δολαρίων για τους χαλαρούς ελέγχους της εφαρμογής της τράπεζας.

Στις αρχές του 2008, ένας Ρώσος εισβολέας έκλεψε 2 εκατομμύρια δολάρια αφού διείσδυσε σε ένα δίκτυο ATM που σχετίζεται με τη Citibank σε όλη τη Νέα Υόρκη. Η ομάδα απέκτησε πρόσβαση σε έναν διακομιστή που επεξεργάστηκε τις αναλήψεις ATM σε καταστήματα 7-Eleven. Αυτό τους επέτρεψε να κλέψουν αριθμούς χρεωστικής κάρτας και PIN από 2.200 μηχανήματα, τα οποία χρησιμοποιούσαν για ανάληψη των 2 εκατομμυρίων δολαρίων. Τρία μέλη της ομάδας συνελήφθησαν και ομολόγησαν ενοχή για πολλές κατηγορίες απάτης και συνωμοσίας αργότερα εκείνο το έτος. Οι ερευνητές συνέδεσαν αργότερα αυτήν την κλοπή με ένα παγκόσμιο δίκτυο εγκληματιών του κυβερνοχώρου που είχαν κλέψει πληροφορίες καρτών ήδη από το 2005. Ένας εγκληματίας κυβερνοχώρου που αναγνωρίστηκε ως αρχηγός από τις αρχές φυλακίστηκε το 2010. Θα συνδεθεί επίσης με την εισβολή του Nasdaq δύο χρόνια αργότερα (Carnegie, 2020).

Απρίλιος 2008 Στις 18 Απριλίου, ένας υπάλληλος στα κεντρικά γραφεία της HSBC στο Λονδίνο κατάφερε να συνδέσει με δόλο 90 εκατομμύρια ευρώ σε λογαριασμούς στο Μάντσεστερ και το Μαρόκο. Ο υπάλληλος χρησιμοποίησε κωδικούς πρόσβασης που έχουν κλαπεί από συναδέλφους για να εκτελέσουν δύο συναλλαγές την Παρασκευή το απόγευμα. Πιάστηκε όταν ξέχασε να αφήσει τους αρχικούς λογαριασμούς με μηδενικά υπόλοιπα, τα οποία εντόπισε το προσωπικό της HSBC στη Μαλαισία το σαββατοκύριακο. Φυλακίστηκε για εννέα χρόνια και τα χρήματα επιστράφηκαν στους ιδιοκτήτες του. Οι ερευνητές στο Ηνωμένο Βασίλειο θα αποκαλύψουν αργότερα τη συμμορία που διέπραξε την απάτη.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Μεταξύ Ιουλίου και Αυγούστου, η Γεωργία έγινε θύμα μιας συντονισμένης επίθεσης DDoS που διέκοψε κυβερνητικούς και τραπεζικούς ιστότοπους κατά τη διάρκεια μιας διαμάχης με τη Ρωσία. Το πρώτο περιστατικό συνέβη στις 20 Ιουλίου, όταν ο ιστότοπος του τότε προέδρου της Γεωργίας Μιχαήλ Σαακασβίλι διακόπηκε από επίθεση DDoS, λίγες εβδομάδες πριν η Ρωσία εισέβαλε στη χώρα. Η επίθεση DDoS κατευθύνθηκε χρησιμοποιώντας ένα πλήθος κακόβουλου λογισμικού Pinch που χρησιμοποιείται συχνά στη Ρωσία, το οποίο πλημμύρισε ιστότοπους με επισκεψιμότητα που περιελάμβανε τη φράση "win+love+in+Russia".

Γεωργία: Αύγουστος 2008

Στο πλαίσιο της σύγκρουσης και του πολέμου που έλαβε χώρα από τις 7 έως τις 12 Αυγούστου 2008, πολλοί γεωργιανοί ιστότοποι κυβέρνησης και μέσων μαζικής ενημέρωσης παραμορφώθηκαν και διασπάστηκαν, συμπεριλαμβανομένων απεικονίσεων του Σαακασβίλι δίπλα στον Χίτλερ στον ιστότοπο του προέδρου. Ο μόνος αντίκτυπος στον χρηματοπιστωτικό τομέα σε όλη αυτήν την εκστρατεία ήταν η παραμόρφωση του ιστότοπου της Εθνικής Τράπεζας της Γεωργίας. Μια ομάδα με το όνομα Hack Crew της Νότιας Οσετίας ανέλαβε την ευθύνη για τις επιθέσεις. Ωστόσο, η Γεωργία θα αποδώσει αργότερα την επίθεση στην κυβέρνηση της Ρωσίας, η οποία αρνήθηκε τους ισχυρισμούς.

Μάρτιος 2009: Πολλαπλές τοποθεσίες

Μεταξύ 2007 και 2011, ένα Trojan malware γνωστό ως Zeus χρησιμοποιήθηκε σε πολλές εγκληματικές ενέργειες για κλοπή δεδομένων σε συσκευές Windows. Το Zeus αποτέλεσε αντικείμενο ευρείας διαπραγμάτευσης σε εγκληματικά φόρουμ ως τρόπος συλλογής διαδικτυακών διαπιστευτηρίων. Ο πηγαίος κώδικάς του

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

δημοσιοποιήθηκε το 2011 αφού ο δήθεν δημιουργός του ανακοίνωσε τη συνταξιοδότησή του, η οποία επέτρεψε τη διάδοση πολλών εκδόσεων. Το Trojan περιελάβανε ένα keylogger που κατέγραψε διαπιστευτήρια σύνδεσης τράπεζας και ένα botnet που εκτέλεσε επιθέσεις χρησιμοποιώντας μολυσμένες συσκευές (Carnegie, 2020).

Τον Μάρτιο του 2009, μια εταιρεία ασφαλείας ανακάλυψε μια διαδικτυακή ομάδα δεδομένων κλεμμένων πληροφοριών από 160.000 υπολογιστές που έχουν μολυνθεί από κακόβουλο λογισμικό Zeus, συμπεριλαμβανομένων συσκευών στο Metro CitiBank. Μια εγκληματική συμμορία χρησιμοποίησε επίσης τον Zeus σε ένα παγκόσμιο σχήμα για να μεταφέρει εκατομμύρια δολάρια από πέντε τράπεζες σε λογαριασμούς στο εξωτερικό, σύμφωνα με αξιωματούχους των ΗΠΑ και του Ηνωμένου Βασιλείου που πραγματοποίησαν περισσότερες από 100 συλλήψεις τον Οκτώβριο του 2010. Η συμμορία στρατολόγησε μουλάρια για να ξεπλένει τα κλεμμένα κεφάλαια και να αποσύρει χρήματα από ATM σε όλο τον κόσμο.

Η παραλλαγή Gameover Zeus ελέγχθηκε από μια ομάδα χάκερ στη Ρωσία και την Ουκρανία από τον Οκτώβριο του 2011 και μετά, σύμφωνα με το FBI. Μεταξύ των πολλών χρήσεων του ήταν ως πλατφόρμα για τη μόλυνση συστημάτων με Crypto locker ransomware. Η επιχείρηση Tovar, μια διεθνής προσπάθεια επιβολής του νόμου τον Ιούνιο του 2014, είχε ως αποτέλεσμα την κατάσχεση βασικών υποδομών Gameover Zeus και την απελευθέρωση έως και 1 εκατομμυρίου μηχανημάτων θυμάτων από το botnet. Οι αρχές πιστεύουν ότι η συμμορία έκλεψε περισσότερα από 100 εκατομμύρια δολάρια. Ο Ρώσος άντρας που κατηγορείται για συγγραφή τόσο του Δία όσο και του Gameover Zeus παραμένει ελεύθερος.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Ιούλιος 2009: ΗΠΑ – ΚΟΡΕΑ

Τον Ιούλιο του 2009, τα χρηματοπιστωτικά ιδρύματα στις Ηνωμένες Πολιτείες και τη Νότια Κορέα ήταν μεταξύ πολλών στόχων μιας εκτεταμένης επίθεσης DDoS. Το συμβάν, το οποίο ξεκίνησε κατά τη διάρκεια ενός Σαββατοκύριακου διακοπών στις ΗΠΑ, περιελάβανε τρία κύματα επιθέσεων που εκτείνονταν σε έξι ημέρες. Το botnet υπολογίζεται σε δίκτυο έως και 65.000 κόμβων.

Απρίλιος 2010:

Το 2010, ένας υπάλληλος της Bank of America κατηγορήθηκε για απάτη σε υπολογιστή μετά την εγκατάσταση κακόβουλου λογισμικού σε 100 ATM για να κλέψει 304.000 $ μέσα σε επτά μήνες Ο άντρας φυλακίστηκε για είκοσι επτά μήνες αφού παραδέχθηκε ότι είχε γράψει κώδικα που έδινε εντολή στα ATM να εκδίδουν μετρητά χωρίς καταγραφή της συναλλαγής. Απέσυρε τα χρήματά του κατά τη διάρκεια των επτά μηνών, σταματώντας τον Οκτώβριο του 2009 όταν τα συστήματα εσωτερικού ελέγχου της Bank of America εντόπισαν τις ύποπτες συναλλαγές(Carnegie, 2020).

Οκτώβριος 2010:

Τον Οκτώβριο του 2010, το FBI εντόπισε εισβολή σε διακομιστές που χρησιμοποίησε ο διαχειριστής χρηματοπιστωτικών αγορών Nasdaq. Περαιτέρω έρευνα από διάφορες αμερικανικές υπηρεσίες διαπίστωσε ότι οι χάκερ βρίσκονταν στο δίκτυο για περίπου ένα χρόνο. Είχαν χρησιμοποιήσει δύο zero-day exploits για να δημιουργήσουν την παρουσία τους στο δίκτυο του χρηματιστηρίου, και είχαν εγκαταστήσει κακόβουλο λογισμικό στο σύστημα Director's Desk, όπου οι διευθυντές εταιρειών που ανήκουν στο κοινό μοιράζονται εμπιστευτικές πληροφορίες. Ο Nasdaq είπε ότι δεν ελήφθησαν δεδομένα, και σύμφωνα με πληροφορίες δεν υπάρχουν

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

στοιχεία για ύποπτες συναλλαγές που θα μπορούσαν να βασίζονται σε πληροφορίες στο σύστημα. Το κακόβουλο λογισμικό περιλάμβανε επίσης καταστροφική ικανότητα, αλλά δεν είναι σαφές εάν η διακοπή ήταν στόχος ή απλά ένα εργαλείο που οι επιτιθέμενοι θα μπορούσαν να χρησιμοποιήσουν για να καλύψουν τα ίχνη τους. Ταυτόχρονα, μια ομάδα εγκληματιών διείσδυσε στον Nasdaq σε ένα περιστατικό που κάποιοι ερευνητές πίστευαν ότι ήταν συνδεδεμένοι. Το 2013, μετά από μια εκτεταμένη έρευνα, οι Ηνωμένες Πολιτείες κατηγόρησαν τέσσερις Ρώσους και έναν Ουκρανό άνδρα με μια σειρά διαδικτυακών επιθέσεων στο Nasdaq και σε άλλες εταιρείες που χρονολογούνται από το 2005. Οι Carrefour, 7-Eleven, Heartland Payment Systems και JC Penney ήταν μεταξύ των άλλων στόχων τους, χάνοντας μαζί 300 εκατομμύρια δολάρια ως αποτέλεσμα του σχεδίου. Η παραβίαση της Heartland εξέθεσε περισσότερες από 100 εκατομμύρια κάρτες πληρωμής, με αποτέλεσμα να κοστίσει τελικά στην εταιρεία 12 εκατομμύρια δολάρια σε πρόστιμα και τέλη.

Λίβανος Ιανουάριος 2011

Στις αρχές του 2011, ένας ιός με το όνομα Gauss χρησιμοποιήθηκε για να κλέψει πληροφορίες από πολλές τράπεζες του Λιβάνου. Ο Gauss, ο οποίος είχε ομοιότητες με το κακόβουλο λογισμικό Flame και Stuxnet, έκλεψε κωδικούς πρόσβασης, τραπεζικά διαπιστευτήρια και cookie προγράμματος περιήγησης από μολυσμένες συσκευές. Οι περισσότερες από τις 2.500 μολύνσεις που εντοπίστηκαν από ερευνητές του Kaspersky ήταν σε προσωπικούς υπολογιστές στο Λίβανο. Τα ειδησεογραφικά πρακτορεία έχουν υποθέσει ότι αυτό το εργαλείο επιτήρησης στον κυβερνοχώρο σχεδιάστηκε από τις ΗΠΑ και τις ισραηλινές κυβερνήσεις για να παρακάμψουν τους αυστηρούς νόμους περί τραπεζικού απορρήτου του Λιβάνου, οι οποίοι δυσκολεύαν την πρόσβαση των παγκόσμιων αρχών σε πληροφορίες για ύποπτα αδικήματα. Αυτές οι εικασίες τροφοδοτήθηκαν από μια δήλωση των Ηνωμένων

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Πολιτειών τον Μάρτιο του 2011, κατηγορώντας μια Λιβανέζικη τράπεζα ότι ξεπλένει χρήματα για ένα κύκλωμα ναρκωτικών του Μεξικού με συνδέσμους με τη Χεζμπολάχ (Carnegie, 2020).

Μάρτιος 2011: Νότια Κορέα

Η Νότια Κορέα επλήγη από μια εκτεταμένη επίθεση DDoS, σχεδόν δύο χρόνια μετά από μια παρόμοια επίθεση το 2009. Στόχοι περιελάμβαναν Hanabank, Jeilbank και Wooribank, καθώς και κυβερνητικούς ιστότοπους. Το Koredos Trojan χρησιμοποιήθηκε για τη διαγραφή δίσκων σε υπολογιστές που χρησιμοποιούνται ως διακομιστές εντολών και ελέγχου. Η Βόρεια Κορέα εικάζεται ότι βρίσκεται πίσω από το δεκαήμερο περιστατικό.

Ιανουάριος 2012: Βραζιλία

Από το 2012 έως το 2014, το Boleto Bancario, ένα σύστημα πληρωμών που χρησιμοποιήθηκε για σχεδόν τις μισές συναλλαγές χωρίς μετρητά στη Βραζιλία, στοχεύτηκε από κακόβουλο λογισμικό που χειρίστηκε το πρόγραμμα περιήγησης του θύματος για να ανακατευθύνει τις πληρωμές σε λογαριασμούς που ελέγχονται από εισβολείς. Η τεχνική έθεσε σε κίνδυνο 3,75 δισεκατομμύρια δολάρια σε πληρωμές εντός περιόδου δύο ετών, χρησιμοποιώντας αρκετές διαφορετικές εκδόσεις κακόβουλου λογισμικού, συμπεριλαμβανομένων των Eupuds, Boleteiro και Domingo, σύμφωνα με ερευνητές της RSA. Η άγνωστη συμμορία υπεύθυνη άλλαξε αργότερα τη στρατηγική «bolware» για να εισαγάγει δηλητηρίαση DNS ως μέσο για την εγκατάσταση του κακόβουλου λογισμικού, μειώνοντας την ανάγκη για ανεπιθύμητα μηνύματα ηλεκτρονικού ταχυδρομείου για τη διάδοση του κακόβουλου λογισμικού (Carnegie, 2020).

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Φεβρουάριος 2012:

Τον Φεβρουάριο του 2012, οι πάροχοι χρηματοοικονομικών συναλλαγών Nasdaq, CBOE και BATS επλήγησαν από επιθέσεις DDoS για αρκετές ημέρες, με αποτέλεσμα την ανεπαρκή πρόσβαση σε ιστότοπους εταιρειών, αλλά χωρίς διακοπή στις συναλλαγές. Η ακτιβιστική ομάδα Anonymous ανέλαβε την ευθύνη για το περιστατικό, λέγοντας ότι ενήργησε από συμπάθεια για τις διαδηλώσεις Occupy Wall Street στη Νέα Υόρκη.

Φεβρουάριος 2013:

Την παραμονή των Χριστουγέννων του 2013, η Τράπεζα της Δύσης ήταν το θύμα μιας επίθεσης DDoS που χρησιμοποιήθηκε για να συγκαλύψει 900.000 $ σε δόλιες μεταφορές από λογαριασμούς που ανήκουν στην Ascent Builders, μια κατασκευαστική εταιρεία της Καλιφόρνιας. Οι δράστες πραγματοποίησαν δόλιες, αυτοματοποιημένες υπηρεσίες εκκαθάρισης και τραπεζικού εμβάσματος προτού θέσουν τον ιστότοπο της τράπεζας εκτός σύνδεσης. Σύμφωνα με πληροφορίες χρησιμοποιήθηκε ένα δίκτυο περισσότερων από εξήντα bots για τη μεταφορά χρημάτων σε εγκληματικούς λογαριασμούς, καθιστώντας πιο δύσκολο τον εντοπισμό των χρημάτων.

Μάρτιος 2013: Κορέα

Τον Μάρτιο του 2013, σχεδόν ακριβώς δύο χρόνια από την τελευταία επίθεση DDoS στη Νότια Κορέα, οι τράπεζες Shinhan, Nonghyup και Jeju στοχεύτηκαν από έναν Trojan που διέγραψε δεδομένα και διέκοψε τα ATM, τις διαδικτυακές τραπεζικές συναλλαγές και τις πληρωμές μέσω κινητού. Το Trojan.Jokra χρησιμοποιήθηκε για να διαγράψει δεδομένα δίσκων, αλλά η επίθεση διέφερε από τους προκατόχους της στο

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ότι δεν περιελάμβανε επίθεση DDoS. Μετά από έξι μήνες επιθέσεων, η κυβέρνηση της Νότια Κορέας δήλωσε ότι αυτό το κύμα κόστισε στη χώρα οικονομική ζημιά σχεδόν 650 εκατομμυρίων δολαρίων, καθιστώντας την πολύ μεγαλύτερη από τις δύο προηγούμενες επιθέσεις. Το περιστατικό αποδόθηκε από ορισμένους στη συμμορία DarkSeoul, έναν εγκληματία κυβερνοχώρου που συνδέεται με το καθεστώς της Βόρειας Κορέας και αργότερα θα συνδεθεί με την παραβίαση της Sony το 2014.

Ιούλιος 2013:

Τον Ιούλιο του 2013, το CME Group, το οποίο λειτουργεί το μεγαλύτερο χρηματιστήριο συμβολαίων μελλοντικής εκπλήρωσης (forward options) στον κόσμο, ανακοίνωσε τον Νοέμβριο του 2013 ότι η υπηρεσία εκκαθάρισης ClearPort είχε παραβιαστεί τον προηγούμενο Ιούλιο. Η εταιρεία είπε ότι ορισμένα στοιχεία πελατών δημοσιεύτηκαν, αλλά ότι οι συναλλαγές δεν επηρεάστηκαν. Ενώ οι μεγάλες χρηματοοικονομικές εταιρείες δεν έχουν γενικά υποχρέωση δημοσιοποίησης παραβιάσεων δεδομένων, η εταιρεία ενημέρωσε τους επηρεαζόμενους πελάτες και ανακοίνωσε ότι συνεργάζεται με τις αρχές. Το FBI διερεύνησε το περιστατικό, αλλά δεν δημοσίευσε περαιτέρω πληροφορίες.

Σαγκάη 2015

Ξεκινώντας στις 12 Ιουνίου 2015, ο Shanghai Composite Index άρχισε να πέφτει και στις 19 Ιουνίου είχε μειωθεί κατά 13%. Οι κινεζικές χρηματιστηριακές αγορές συνέχισαν να πέφτουν όλο τον Ιούλιο και τον Αύγουστο, και πάλι τον Ιανουάριο και τον Φεβρουάριο του 2016. Παρόλο που δεν υπάρχουν δημόσια αποδεικτικά στοιχεία, ορισμένοι έχουν υποθέσει ότι η αρχική ξαφνική συντριβή μπορεί να προκλήθηκε από επίθεση στον κυβερνοχώρο.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Σουηδία 2015

Τον Νοέμβριο του 2015, ένας έφηβος καταδικάστηκε σε κοινωνική εργασία μετά από τέσσερις επιθέσεις DDoS εναντίον της Nordea και της Swedbank. Οι επιθέσεις απέκλεισαν πελάτες από τους ιστότοπους των τραπεζών για ώρες κάθε φορά.

2016: Αγγλία

Η Tesco Bank, μια λιανική τράπεζα που εδρεύει στο Ηνωμένο Βασίλειο, ήταν ο στόχος των επιτιθέμενων που χρησιμοποίησαν τρωτά σημεία στη διαδικασία έκδοσης καρτών για να μαντέψουν αριθμούς τραπεζικών καρτών και να κλέψουν 2,26 εκατομμύρια £ τον Νοέμβριο του 2016. Οι άγνωστοι εισβολείς πιθανότατα χρησιμοποίησαν έναν αλγόριθμο για τη δημιουργία αριθμών τραπεζικών καρτών που χρησιμοποίησαν τους αριθμούς αναγνώρισης της Tesco στην αρχή και συμμορφώθηκαν με το σύστημα επικύρωσης Luhn σε ολόκληρη τη βιομηχανία που βοηθά στην προστασία από τυχαία λάθη.

Υπάρχουν περίπου 1 δισεκατομμύριο πιθανοί αριθμοί καρτών για κάθε τράπεζα, αλλά οι ρυθμιστικές αρχές ανέφεραν ότι οι κάρτες της Tesco Bank είχαν ελλείψεις, όπως διαδοχικοί αριθμοί καρτών, που έκαναν την εκτίμηση των πλήρων αριθμών ευκολότερη. Η τράπεζα χρησιμοποίησε μόνο βασικούς ελέγχους για να εκτιμήσει εάν οι κάρτες ήταν γνήσιες, για παράδειγμα απλώς επιθεωρώντας εάν η χρεωστική κάρτα θα λήξει στο μέλλον αντί να βεβαιωθεί ότι η ακριβής ημερομηνία λήξης ταιριάζει με τα αρχεία της.

Η Visa και η Mastercard είχαν προηγουμένως προειδοποιήσει για αύξηση του τύπου απάτης που παρατηρήθηκε σε αυτήν την περίπτωση, η οποία χρησιμοποίησε τη μαγνητική ταινία για την επαλήθευση της συναλλαγής. Στις 5 Νοεμβρίου 2016, καθώς ξεκίνησε το Σαββατοκύριακο, η συμμορία άρχισε να κάνει δόλιες συναλλαγές με τα

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

στοιχεία της κάρτας που είχε υπολογίσει. Επηρεάστηκαν σχεδόν 9.000 λογαριασμοί ή το 6,6% της συνολικής πελατειακής βάσης της τράπεζας. Ένας πελάτης είχε είκοσι δύο δόλιες συναλλαγές συνολικού ύψους 65.000 £ στον λογαριασμό του.

2017: Κορέα

Σε μια επίδειξη του αυξανόμενου ρόλου της κρυπτογράφησης στους κύκλους εγκληματικότητας στο διαδίκτυο, το χρηματιστήριο bitcoin, το Youbit, παραβιάστηκε δύο φορές το 2017, αναγκάζοντάς το να υποβάλει αίτηση πτώχευσης. Το χρηματιστήριο της Νότιας Κορέας έχασε σχεδόν 4.000 bitcoin σε κλοπή τον Απρίλιο, την οποία οι αρχές της χώρας είχαν συνδέσει με τη Βόρεια Κορέα, σύμφωνα με τοπικά ΜΜΕ. Η επίθεση τον Δεκέμβριο οδήγησε στην απώλεια 17% του ψηφιακού νομίσματος του Youbit και την ανάγκασε να σταματήσει τις συναλλαγές. Οι κλοπές ήρθαν εβδομάδες μετά από ένα ρεκόρ bitcoin ύψους 70 εκατομμυρίων δολαρίων στο NiceHash, μια υπηρεσία εξόρυξης κρυπτονομισμάτων στη Σλοβενία, σε μια εποχή που η τιμή του νομίσματος είχε αυξηθεί πάνω από 15.000 $ (Carnegie, 2020).

Καναδάς 2018:

Το 2018, αποκαλύφθηκε ότι έως 90.000 πελάτες των καναδικών τραπεζών Simplii και Bank of Montreal (BMO) είχαν εκτεθεί από παραβίαση δεδομένων που κατηγόρησε ο οργανισμός σε αγνώστους επιτιθέμενους. Η Bank of Montreal είπε ότι υπήρχε απειλή να δημοσιοποιηθούν τα δεδομένα από την ομάδα, η οποία πιστεύει ότι βρίσκεται πίσω από τις κλοπές και από τις δύο τράπεζες. Οι Simplii και BMO αντιμετωπίζουν τώρα αγωγή κατηγορίας, με τους εμπλεκόμενους να υποστηρίζουν ότι οι τράπεζες απέτυχαν να προστατεύσουν σωστά ευαίσθητες πληροφορίες.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

2019: Χιλή

Τον Δεκέμβριο, οι χάκερ διεισδύουν στο διατραπεζικό δίκτυο ATM της Χιλής, Redbanc, αφού εξαπάτησαν έναν υπάλληλο κατάφεραν να κατεβάσουν ένα κακόβουλο πρόγραμμα κατά τη διάρκεια μιας ψεύτικης συνέντευξης εργασίας μέσω του Skype. Πιστεύεται ότι ο υπάλληλος της Redbanc είδε μια διαφήμιση εργασίας στο LinkedIn και παρακολούθησε μια συνέντευξη στο Skype, όπου οι εισβολείς του ζήτησαν να κατεβάσει ένα πρόγραμμα λογισμικού για να υποβάλει τη φόρμα αίτησής του. Οι επιτιθέμενοι εξαπάτησαν το θύμα να κατεβάσει κακόβουλο λογισμικό στο σύστημά του, δίνοντάς τους πρόσβαση στο δίκτυο της Redbanc. Η Redbanc ισχυρίζεται ότι η εκδήλωση δεν είχε καμία επίπτωση στις επιχειρηματικές της δραστηριότητες.

Ινδία 2019:

Η Κρατική Τράπεζα της Ινδίας, η μεγαλύτερη της χώρας, αρνήθηκε τους ισχυρισμούς ότι οι διακομιστές της παραβιάστηκαν κατά τη διάρκεια μιας πρόσφατης εισβολής. Πολλά μέσα ενημέρωσης ανέφεραν ότι ένας διακομιστής SBI δεν προστατεύεται και ως αποτέλεσμα οι εισβολείς μπόρεσαν να αποκτήσουν πρόσβαση στο σύστημα και να κλέψουν τα προσωπικά στοιχεία των χρηστών. Παρά τους ισχυρισμούς, η τράπεζα δήλωσε ότι η έρευνά τους αποκάλυψε ότι οι διακομιστές της SBI παρέμειναν πλήρως προστατευμένοι και ότι δεν είχε σημειωθεί παραβίαση (Carnegie, 2020).

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ΒΙΒΛΙΟΓΡΑΦΙΑ

ΞΕΝΗ

Albarqi, Aysha&Alzaid, Ethar&Alghamdi, Fatimah&Asiri, Somaya&Kar, Jayaprakash. (2015). Public Key Infrastructure: A Survey. Journal of Information Security. 06. 31-37. 10.4236/jis.2015.61004.

Ali, L. (2018). Cyber Crimes-A Constant Threat For The Business Sectors And Its Growth (A Study Of The Online Banking Sectors In GCC). *The Journal of Developing Areas, 53*, 267 - 279.

Chevers, D.A. (2019). The impact of cybercrime on e-banking: A proposed model. *CONF-IRM*.

NIDA TARIQ (2018), IMPACT OF CYBERATTACKS ON FINANCIAL INSTITUTIONS, Journal of Internet Banking and Commerce, June 2018, vol. 23, no. 2

Mee P., Schermann (2018). HOW A CYBERATTACK COULD CAUSE THE NEXT FINANCIAL CRISIS Frozen ATMs. Halted payments. Widespread panic. Here's what governments need to do to prevent catastrophe.,RISK JOURNAL | EMERGING RISKS

Al-Asri, Abbas & Sulaiman, Rossilawati. (2018). Protection of XML-Based Denial-of-Service and Http flooding Attacks in Web Services Using the Middleware Tool.

Ahmed, Omar & Bibo, Amira. (2019). Android Security: A Review. 6. 6.

Awojana, T. (2018). Threat Modelling and Analysis of Web Application Attacks.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Adamson, I., Chan, K.M., & Handford, D. 2003. Relationship marketing: Customer commitment and trust as a strategy for the smaller Hong Kong corporate banking sector. International Journal of Bank Marketing, 21(6/7): 347-358.

Ahmad, A. M. K., & Al-Zu'bi, H. A. (2011). E-banking functionality and outcomes of customer satisfaction: an empirical investigation. International Journal of Marketing Studies, 3(1), p50. Article 2

Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M. J. G., Levi, M., Moore, T., & Savage, S. 2012. Measuring the cost of cybercrime.

Douglas, T., & Loader, B. D. 2000. *Cybercrime: Security and surveillancein the information age*: Routledge

Alawneh, A. and Hattab, E. (2009) "E-Banking Diffusion in the Jordanian Banking Services Sector: An Empirical Analysis of Key Factors", International Journal of Actor-Network Theory and Technological Innovation, Vol.1 No. 2, PP. 50-65.

Bhasin, Madan. (2017). Mitigating Cyber Threats To Banking Industry. The Chartered Accountant. 1619-1624.

Azeez, Nureni & Irwin, Barry. (2010). CYBER SECURITY: CHALLENGES AND THE WAY FORWARD.. Computer Science & Telecommunications. 29.

Balebako, R., & Cranor, L. (2014). Improving App Privacy: Nudging App Developers to Protect User Privacy. Security & Privacy, IEEE, 12(4), 55-58.

CAPEC-89: Pharming. URL: http://capec.mitre.org/data/ definitions/89.html

Bali, Akanksha & Goswami, Shivangi & Sharma, Shagun. (2019). International Journal of Scientific and Technical Advancements Biometrics Security in Mobile Application Development & its Applications.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Chandramohan, M., & Tan, H. B. K. (2012). Detection of mobile malware in the wild. Computer, (9), 65-71.

Cuomo A. M. (2014). Report on Cyber Security in the Banking Sector. New York State Department of Financial Services

Chawla, S., & Sehgal, R. (2012). An Empirical Analysis of the Awareness and Satisfaction Level of Internet Banking Users with Respect to Demographic Profile. The IUP Journal of Marketing Management, 11(1), 62-83.

Damodaran, A., Di Troia, F., Visaggio, C. A., Austin, T. H., & Stamp, M. (2017). A comparison of static, dynamic, and hybrid analysis for

malware detection. Journal of Computer Virology and Hacking Techniques, 13(1), 1-12.

European Payment Council (2019).

2019 Payment Threats and Fraud Trends Report , EPC302-19 /Version 1.0 / Date issued: 9 December 2019

Hamid, M. R. (2007), A comparative analysis of Internet banking in Malaysia and Thailand. Journal of Internet Business(4),1-19.

Heggestuen, J. (2014). The Future Of Mobile And Online Banking: 2014. Διαθέσιμο σε: http://www.businessinsider.com/the-future-of-mobile-and-onlinebanking-2014-slide-deck-2014-10?op=1

Fatima, A. (2011). E-banking security issues–Is there a solution in biometrics. Journal of Internet Banking and Commerce, 16(2): 2011-08.

Faisal, Ali & Garba, Faisal. (2017). SECURED APPLICATION BASED MOBILE BANKING MODEL FOR NIGERIA.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

He, Wu & Tian, Xin & Shen, J.. (2015). Examining security risks of mobile banking applications through blog mining. CEUR Workshop Proceedings. 1353. 103-108.

Hertzum, M.,. Juul, N.C., Jørgensen, N. and Nørgaard, M. (2004) “Usable Security and E-Banking: Ease of Use vis-à-vis Security”, Technical Report. Available at URL: http://www.ruc.dk/~nielsj/research/papers/E-Banking-tr.pdf (Accessed 20 March 2011).

Ibbotson, P. and Moran, L. (2003) "E-banking and the SME/bank relationship in Northern Ireland", International Journal of Bank Marketing, Vol. 21 No. 2, pp. 94-103.77

ING (2017). International Survey Mobile Banking 2017 – Newer Technologies May 2017, διαθέσιμοσε https://think.ing.com/uploads/reports/IIS_Mobile_Banking_2017_Newer_Technologies_FINAL.pdf

Kavitha, K. (2015). Mobile Banking Supervising System- Issues, Challenges & Suggestions to improve Mobile Banking Services.

Lee, H., Zhang, Y., & Chen, K. L. (2013). An Investigation of Features and Security in Mobile Banking Strategy. Journal of International Technology and Information Management, 22(4),

Elkhodr, M., Shahrestani, S., & Kourouche, K. (2012). A proposal to improve the security of mobile banking applications. In

HAYRAN, AHMET & İĞDELİ, MURATCAN & Yilmaz, Atif & GEMCİ, CEMAL. (2016). Security Evaluation of IOS and Android. International Journal of Applied Mathematics, Electronics and Computers. 258-258. 10.18100/ijamec.270378.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ICT and Knowledge Engineering (ICT & Knowledge Engineering), 2012 10th International Conference on (pp. 260-265). IEEE.

Kalyani, Chenigaram. (2017). Various Biometric Authentication Techniques: A Review. Journal of Biometrics & BiOStatistics. 08. 10.4172/2155-6180.1000371.

Legnitto, J. (2013). Mobile Banking On Unsecure Wireless Networks Is Risky Business. Διαθέσιμο σε: http://www.privatewifi.com/title-mobile-banking-on-unsecurewireless-networks-is-risky-business/

Mallat, Matti, & Virpi, 2004, Nie & Hu, 2008, Lin, 2011, Elkhodr, Shahrestani & Kourouche, 2012).

Marshall Paul Jeffery (2010), Online Banking: Information Security vs. Hackers Research Paper, International Journal of Scientific & Engineering Research, Volume 1, ISSUE 1, ISSN 2229-5518, October-2010 1.

Masrek, Mohamad & Uzir, Nora'ayu & Khairuddin, Irni. (2012). Examining Trust In Mobile Banking: A Conceptual Framework.

Mia, M., Rahaman, M. and Uddin, M. (2007) "E-Banking: Evolution, Status and Prospects", The Cost and Management, Vol. 35 No. 1, pp. 36-48

Mitropoulos, Sarandis & Othonos, Christina & Douligeris, Christos. (2013). An effective and secure web banking system: Development and evaluation. International Journal of Business Information Systems. 12. 335-361. 10.1504/IJBIS.2013.052454.

More, Dr. Manisha & P.Jadhav, Mrs.Meenakshi & Dr.K.M.Nalawade,. (2016). Online Banking and Cyber Attacks: The Current Scenario. 5. 743-749.

Mobile payments world (2017): Mobile payments study – opportunities for banks, Διαθέσμο σε : https://www.mobilepaymentsworld.com

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Mistry, Nilay & Joshi, Dr & Dahiya, Ms. (2018). A Comprehensive Study of Vulnerability Assessment Techniques of Existing Banking Apps.

Nish a. (2019), Cyber Threat Landscape: Confronting Challenges to the Financial System, Carnegie Endowement for International Peace, Διαθέσιμο σε: https://carnegieendowment.org/2019/03/25/cyber-threat-landscape-confronting-challenges-to-financial-system-pub-78506

Petrova, K. & Mehra, Ridhima. (2010). Mobile Payment: An Exploratory Study of Customer Attitudes. Proceedings - 6th International Conference on Wireless and Mobile Communications, ICWMC 2010. 378 - 383. 10.1109/ICWMC.2010.59.

Mittal, Y., Varshney, A., Aggarwal, P., Matani, K., & Mittal, V. K. (2015, December). Fingerprint Biometric based Access Control and Classroom Attendance Management System. In India Conference (INDICON), 2015 Annual IEEE (pp. 1-6). IEEE

Sunardi, Sunardi & Riadi, Imam & Raharja, Pradana. (2019). Vulnerability Analysis of E-voting Application using Open Web Application Security Project (OWASP) Framework. International Journal of Advanced Computer Science and Applications. 10. 135-143.

Raghavan1, Latha Parthiban (2014), The effect of cybercrime on a Bank's finances, 2347-3215 Volume-2 Number 2 (February-2014) pp.173-178

Tao, Qian & Veldhuis, Raymond. (2018). Biometric Authentication System on Mobile Personal Devices. Instrumentation and Measurement, IEEE Transactions on. 59. 763 - 773. 10.1109/TIM.2009.2037873.

Owasp.org, (2017). Top 10 Web Application Security Risks- OWASP. [online] Διαθέσιμο σε https://owasp.org/www-project-top-ten/

Owasp.org, (2016). Top 10 Mobile Security Risks- OWASP. [online] Διαθέσιμο σε https://owasp.org/www-project-mobile-top-10/

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Shostack A., Carol Long (2014). Threat Modeling - designing for security. Wiley, 2014.

Poon, S. and Swatman, P. (1998) "An exploratory study of small business internet commerce issues", Information and Management, Vol. 35 No. 1, pp 9-18.

Stene Henrike Andre (2015).

Chairlone, S.G. 2009. Emerging banking systems. London, UK: Palgrave Macmillan.

Gartner. 2011. Core banking system selection: Criteria that matter. URL: https://goo.gl/Dxsedy.

GAO-U.S. Government Accountability Office GAO (2015). Cybersecurity: Bank and Other Depository Regulators Need Better Data Analytics and Depository Institutions Want More Usable Threat Information. Διαθέσιμοσε: https://www.gao.gov/assets/680/671105.pdf

Laerte, Peotta & Holtz, Marcelo & David, Bernardo & Deus, Flavio & de Sousa Junior, Rafael. (2011). A Formal Classification of Internet Banking Attacks and Vulnerabilities. International Journal of Computer Science & Information Technology. 3. 10.5121/ijcsit.2011.3113.

Raviadaran, H., Dastane, O., Ma'arif, M. Y., & Mohd Satar (2019). Impact of Service Quality Dimensions on Internet Banking Adoption, Satisfaction and Patronage. Journal International Journal of Management, Accounting and Economics. Volume 6 (10). 709-730.

Sayar, C. and Wolfe, S. (2007) "Internet banking market performance: Turkey versus the UK", International Journal of Bank Marketing, Vol. 25 No. 3, pp. 122-141.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Stockdale, R. and Standing, C. (2006) "A classification model to support SME ecommerce adoption initiatives", Journal of Small Business and Enterprise Development, Vol. 13 No. 3, pp. 381-394.

Seybold, P., & Foss, E. 2001. The customer revolution: How to thrive when customers are in control. New York, NY: Random House Business Books. DOI: 10.1571/0609607723

Sabout N. and Parthiban, 2015, Trusted framework for online banking in public cloud using multi-factor authentication and privacy protection gateway. Journal of Cloud Computing Advances, Systems and Applications 4:22

Seo, S. H., Gupta, A., Sallam, A. M., Bertino, E., & Yim, K. (2014). Detecting mobile malware threats to homeland security through static analysis. Journal of Network and Computer Applications, 38, 43-53.

Singh, Pratham and Rajput, R S, Cybersecurity Analysis in the Context of Digital Wallets (March 19, 2019). International Journal of Advanced Studies of Scientific Research, Vol. 4, No. 3, 2019. Available at SSRN: https://ssrn.com/abstract=3355789

Stene Henrike Andre (2015). Threat Analysis of Web Banking Platforms, University of Oslo, Department of Informatics.

Galterio, Mary & Shavit, Simi & Hayajneh, Thaier. (2018). A Review of Facial Biometrics Security for Smart Devices. Computers. 7. 37. 10.3390/computers7030037.

Maček, Nemanja & Milosavljević, Milan & Franc, Igor & Minchev, Zlatogor & Gnjatovic, Milan & Trenkić, Branimir. (2017). Secure Mobile Banking Biometric Authentication.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Sabhanayagam , Dr. V. Prasanna Venkatesan and Dr. K. Senthamaraikannan, " A Comprehensive Survey on Various Biometric Systems", International Journal of Applied Engineering Research ISSN.-4562 Volume 13, Number 5 pp. 2276-2297, 2018.

Sowndarajan, Karthick & Binu, Sumitra. (2017). Android security issues and solutions. 686-689. 10.1109/ICIMIA.2017.7975551.

Yang, Wencheng & Wang, Song & Hu, Jiankun & Guanglou, Zheng & Valli, Craig. (2019). Security and Accuracy of Fingerprint-Based Biometrics: A Review. Symmetry. 11. 141.

Turnbull, P.W. 2007. Using technology to market bank services: The importance of core systems. International Journal of Bank Marketing , 5: 1-5. Williams, B., Onsman, A., & Brown, T. 2010. Exploratory factor analysis: A five-step guide for novices. Australasian Journal of Paramedicine, 8(3): 1-13.

Wang, Shuo & Liu, Jing. (2018). Biometrics on mobile phone. 10.5772/17151.

whiteCryption (2014).whiteCryption Introduces New Level of Security for Mobile Payment Applications. Διαθέσιμο σε: http://www.prweb.com/releases/2014/01/prweb11531529.htm

More, Dr. Manisha & P.Jadhav, Mrs.Meenakshi & Dr.K.M.Nalawade,. (2016). Online Banking and Cyber Attacks: The Current Scenario. 5. 743-749.

Abreu, Rute & David, Fatima & Legcevic, Mena & Segura, Liliane & Formigoni, Henrique & Mantovani, Flavio. (2018). Ethics and fraud in E-banking services. 10.1109/CISTI.2015.7170491.

Choo, K. K. R. (2011). The cyber threat landscape:Challenges and future research directions. Computers & Security, 30(8), 719-731.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Damodaran, A., Di Troia, F., Visaggio, C. A., Austin, T. H., & Stamp, M. (2017). A comparison of static, dynamic, and hybrid analysis for malware detection. Journal of Computer Virology and Hacking Techniques, 13(1), 1-12.

Devadasan, Pradeep. (2018). A Study on the Cyber Crimes in the Technological Era.

Khan, S. I., & Hoque, A. S. (2018). Digital Health Data: A Comprehensive Review of Privacy and Security Risks and Some
Recommendations. Computer Science Journal of Moldova, 24(2(71)), 273-292.

Chikomo, Kelvin & Chong, Ming & Arnab, Alapan & Hutchison, Andrew. (2006). Security of mobile banking.

Khelifi, Adel & Aburrous, Maher & Talib, Manar & Shastry, P V Sriniwas. (2013). Enhancing Protection Techniques of E-Banking Security Services Using Open Source Cryptographic Algorithms. 89-95. 10.1109/SNPD.2013.47.

Lao, Guoling & Wang, Xinwang. (2010). Study of Security Mechanisms in Personal Internet Banking - Take China Merchants Bank as an Example. 10.1109/CISE.2010.5676896.

Narendiran, C. & Rabara, S. & Rajendran, Nishanth. (2008). Performance evaluation on end-to-end security architecture for mobile banking system. 1 - 5. 10.1109/WD.2008.4812913.

Nie, Jin & Hu, Xianling. (2008). Mobile Banking Information Security and Protection Methods. 587-590. 10.1109/CSSE.2008.1422.

Stepping Up Internet Banking Security Using Dynamic
Pattern Based Image Steganography
P. Thiyagarajan, G. Aghila, and V. Prasanna Venkatesan

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Oppliger, Rolf & Rytz, Ruedi & Holderegger, Thomas. (2009). Internet Banking: Client-Side Attacks and Protection Mechanisms. Computer. 42. 27 - 33. 10.1109/MC.2009.194.

Vrancianu, Marinela & Anica, Liana. (2010). Considerations Regarding the Security and Protection of E-Banking Services Consumers' Interests. The AMFITEATRU ECONOMIC journal. 12. 388-403.

Ιστότοποι

Carnegie (2020). Timeline of Cyber Incidents Involving Financial Institutions https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ


ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ