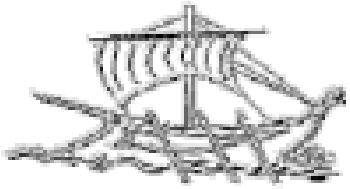


ΑΕΙ ΠΕΙΡΑΙΑ Τ.Τ.
ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΚΩΝ ΕΦΑΡΜΟΓΩΝ
ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ Τ.Ε.

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Μελέτη στην ασφάλεια χρηματικών συναλλαγών τραπεζικών δικτύων

Μπίρμπας Γρηγόρης

Εισηγητής: Δρ Παναγιώτης Γιαννακόπουλος, Καθηγητής

ΑΘΗΝΑ
ΔΕΚΕΜΒΡΙΟΣ 2016

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Σχεδίαση ολοκληρωμένου συστήματος συγγραφής πτυχιακής εργασίας

Μπίρμπας Γρηγόρης

Α.Μ. 38276

Εισηγητής:

Δρ Παναγιώτης Γιαννακόπουλος, Καθηγητής

Εξεταστική Επιτροπή:

Δρ Παναγιώτης Γιαννακόπουλος, Καθηγητής
Δρ Νικόλαος Ζάχαρης, Καθηγητής
Δρ Δημήτριος Νικολόπουλος, Καθηγητής

Ημερομηνία εξέτασης:

ΔΗΛΩΣΗ ΣΥΓΓΡΑΦΕΑ ΠΤΥΧΙΑΚΗΣ ΕΡΓΑΣΙΑΣ

Ο κάτωθι υπογεγραμμένος *Μπίρμπας Γρηγόριος*, του *Παναγιώτη*, με αριθμό μητρώου *38276* φοιτητής του Τμήματος Μηχανικών Η/Υ Συστημάτων Τ.Ε. του Α.Ε.Ι. Πειραιά Τ.Τ. πριν αναλάβω την εκπόνηση της Πτυχιακής Εργασίας μου, δηλώνω ότι ενημερώθηκα για τα παρακάτω:

«Η Πτυχιακή Εργασία (Π.Ε.) αποτελεί προϊόν πνευματικής ιδιοκτησίας τόσο του συγγραφέα, όσο και του Ιδρύματος και θα πρέπει να έχει μοναδικό χαρακτήρα και πρωτότυπο περιεχόμενο.

Απαγορεύεται αυστηρά οποιοδήποτε κομμάτι κειμένου της να εμφανίζεται αυτούσιο ή μεταφρασμένο από κάποια άλλη δημοσιευμένη πηγή. Κάθε τέτοια πράξη αποτελεί προϊόν λογοκλοπής και εγείρει θέμα Ηθικής Τάξης για τα πνευματικά δικαιώματα του άλλου συγγραφέα. Αποκλειστικός υπεύθυνος είναι ο συγγραφέας της Π.Ε., ο οποίος φέρει και την ευθύνη των συνεπειών, ποινικών και άλλων, αυτής της πράξης.

Πέραν των όποιων ποινικών ευθυνών του συγγραφέα σε περίπτωση που το Ίδρυμα του έχει απονείμει Πτυχίο, αυτό ανακαλείται με απόφαση της Συνέλευσης του Τμήματος. Η Συνέλευση του Τμήματος με νέα απόφασης της, μετά από αίτηση του ενδιαφερόμενου, του αναθέτει εκ νέου την εκπόνηση της Π.Ε. με άλλο θέμα και διαφορετικό επιβλέποντα καθηγητή. Η εκπόνηση της εν λόγω Π.Ε. πρέπει να ολοκληρωθεί εντός τουλάχιστον ενός ημερολογιακού 6μήνου από την ημερομηνία ανάθεσης της. Κατά τα λοιπά εφαρμόζονται τα προβλεπόμενα στο άρθρο 18, παρ. 5 του ισχύοντος Εσωτερικού Κανονισμού.»

ΕΥΧΑΡΙΣΤΙΕΣ

Η παρούσα πτυχιακή εργασία ολοκληρώθηκε μετά από σταθερή και επίμονη δουλειά. Στο σημείο αυτό θα ήθελα να ευχαριστήσω τον Δρ. Παναγιώτη Γιαννακόπουλο για την πολύτιμη βοήθειά του καθώς και την ευκαιρία που μου έδωσε να ασχοληθώ με ένα θέμα της επιλογής και του ενδιαφέροντός μου. Σημαντικό επίσης, θεωρώ ότι χρειάζεται να ευχαριστήσω την οικογένειά μου για την στήριξή της κατά τη διάρκεια των σπουδών μου καθώς και το κοντινό φιλικό μου περιβάλλον.

ΠΕΡΙΛΗΨΗ

Σκοπός της παρούσας πτυχιακής είναι να γίνει η μελέτη για την Ηλεκτρονική Τραπεζική και την ασφάλεια των συναλλαγών. Η Ηλεκτρονική Τραπεζική (E-banking) είναι μια υπηρεσία ιδιαίτερα ενδιαφέρουσα όσων αφορά την λειτουργία της αλλά και συνεχώς εξελίξιμη στην εποχή μας. Τα παραπάνω χαρακτηριστικά με ώθησαν στο να μελετήσω το πώς λειτουργεί η ηλεκτρονική τραπεζική, ποια είναι τα πρωτόκολλα ασφαλείας καθώς και τις καθημερινές επιθέσεις που λαμβάνουν χώρο. Ένα ενδεικτικό πλάνο εργασίας για την υλοποίηση της πτυχιακής είναι ως εξής:

1. Ιστορική αναδρομή του E-banking

2. Σκοπό εργασίας (Ασφάλεια και προστασία συναλλαγών)

3. Περιεχόμενα μελέτης
   3.1. Μορφές κακόβουλου λογισμικού
   3.2. Ηλεκτρονικές μορφές επιθέσεων
   3.3. Η έννοια της κρυπτογραφίας
   3.4. Η κρυπτογραφία ιστορικά
   3.5. Αλγόριθμοι κρυπτογράφησης δεδομένων
   3.6. Ηλεκτρονικές Υπογραφές

4. Η Ελληνική πραγματικότητα

5. Βιβλιογραφία

ABSTRACT

The purpose of this dissertation is the study of the security of the transactions through e-banking. E-banking is a service which is especially interesting regarding its operation, and continuously evolving nowadays. The continuous evolution of e-banking inspired me to study: the way of that this service operates, the nature of the security protocols and the finally, the frequency of the cyber-attacks that are related with the aforementioned service. This dissertation will be structured as follows:

1. History of E-banking

2. Aim of the study (Security and Protection of Transactions)

3. Content
   - 3.1. Malware
   - 3.2. Cyber attacks
   - 3.3. Encryption
   - 3.4. History of Encryption
   - 3.5. Encryption Algorithms
   - 3.6. E-signatures

4. The Greek Reality

5. Bibliography

ΠΕΡΙΕΧΟΜΕΝΑ

Περιεχόμενα

ΚΑΤΑΛΟΓΟΣ ΣΧΗΜΑΤΩΝ

Περιεχόμενα

ΚΑΤΑΛΟΓΟΣ ΠΙΝΑΚΩΝ

Περιεχόμενα

ΕΙΣΑΓΩΓΗ

Στις μέρες μας ο άνθρωπος έχει συνδέσει την καθημερινότητά του με λέξεις όπως επιστήμη, αρχιτεκτονική, ιατρική, τεχνολογία, οικονομία, εξέλιξη κ.ο.κ.. Όλες αυτές οι έννοιες- επιστήμες έχουν αναδιαμορφωθεί άρδην τα τελευταία χρόνια και είναι όλες άρρηκτα συνδεδεμένες με την πληροφορική. Πληροφορική ονομάζεται *η επιστήμη που σχετίζεται με τα υπολογιστικά συστήματα και ερευνά τις εφαρμογές τους από την πλευρά της σχεδίασης, της ανάπτυξης, της υλοποίησης αλλά και της πρόσβασης στις πληροφορίες*. Συνέπεια της μεγάλης εξέλιξης των υπολογιστών αποτελεί η συνεχόμενη αλλαγή των κοινωνικών δομών, πλέον οι άνθρωποι έχουν εντελώς διαφορετική πρόσβαση στις νέες τεχνολογίες. Η αλλαγή αυτή οδηγεί στην συνεχή αναζήτηση νέων τεχνολογιών με στόχο την καλύτερη πρόσβαση στην πληροφορία. Οι περισσότεροι σήμερα επιθυμούν να μαθαίνουν τα νέα στον κόσμο , να συνομιλούν με άλλους ανθρώπους, αλλά ακόμα και να κάνουν τις «δουλειές» τους εύκολα, γρήγορα, με το πάτημα ενός κουμπιού από το κινητό τους. Αποτέλεσμα αυτής της κοινωνικής αλλαγής είναι η συνεχής ενασχόληση όλο και περισσότερων ανθρώπων, κάθε ηλικίας, με το διαδίκτυο και τις εφαρμογές του. Την ανάγκη των ανθρώπων «να επιταχύνουν» τις καθημερινές συναλλαγές τους βρέθηκε να καλύψει η υπηρεσία της Ηλεκτρονικής Τραπεζικής. Με έναν απλό και σύντομο ορισμό θα λέγαμε ότι η υπηρεσία αυτή υλοποιεί όλες τις τραπεζικές συναλλαγές που θα μπορούσε να πραγματοποιήσει ο καθένας, συμπιεσμένες στην οθόνη του κινητού, του tablet ή του ηλεκτρονικού υπολογιστή. Σε ένα περιβάλλον ιδιαίτερα φιλικό και κατανοητό ακόμα και για τον πλέον αρχάριο χρήστη μπορούν να ρυθμιστούν πληρωμές, μεταφορές χρημάτων εύκολα από ένα λογαριασμό σε άλλον και πολλές άλλες τραπεζικές διαδικασίες. Ο χρόνος που απαιτείται χάρη στην Ηλεκτρονική Τραπεζική είναι σημαντικά μικρότερος από το χρόνο που θα χρειαζόταν παλαιότερα για ανάλογες εργασίες. Εύκολα λοιπόν συμπεραίνουμε ότι σε επίπεδο ταχύτητας υπάρχει εξαιρετικά μεγάλη πρόοδος και εξέλιξη. Ωστόσο μείζον θέμα αποτελεί η αξιοπιστία και η ασφάλεια της Ηλεκτρονικής Τραπεζικής. Η τοποθέτηση αυτή θα αποτελέσει βασικό άξονα μελέτης στην παρούσα εργασία με στόχο την καλύτερη παρουσίαση κάθε πτυχής της προαναφερθείσας υπηρεσίας.

ΚΕΦΑΛΑΙΟ 1°: E-BANKING

ΕΙΣΑΓΩΓΗ

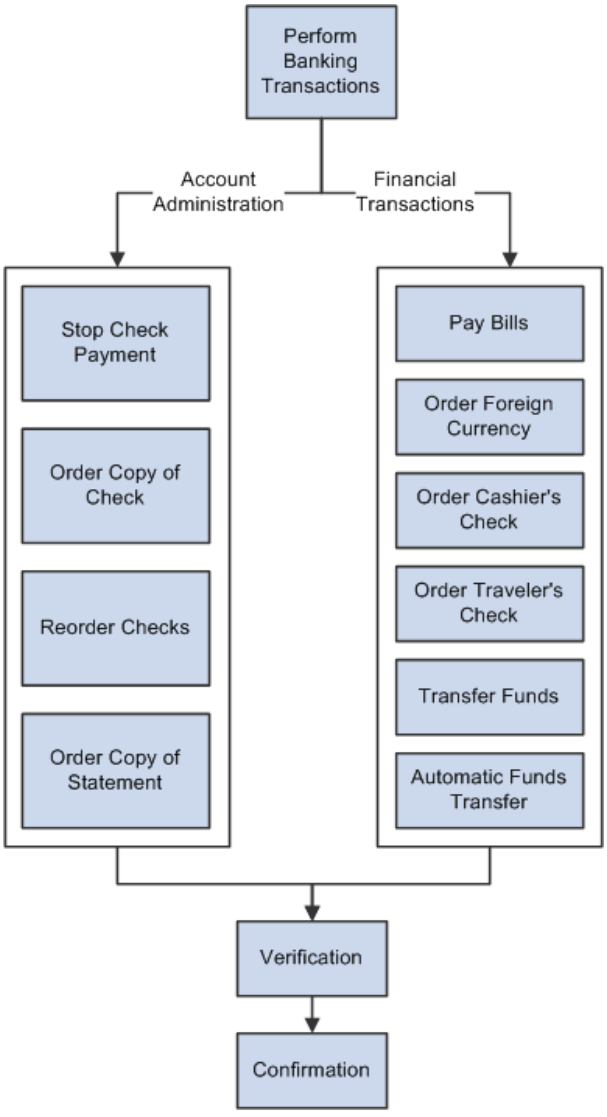
Σε αυτό το κεφάλαιο ορίζεται το αντικείμενο της πτυχιακής εργασίας και γίνεται μια ιστορική αναδρομή γύρω από την εξέλιξή της Ηλεκτρονικής Τραπεζικής.

1.1 Ορισμός της Ηλεκτρονικής Τραπεζικής (E-Banking)

1.2 Ιστορική αναδρομή

1.1 Τι είναι το E-banking;

Ως E-banking(Ηλεκτρονική τραπεζική) ορίζεται *η ηλεκτρονική εκτέλεση λιανικών και εταιρικών συναλλαγών όπως πληρωμές, μεταφορές χρημάτων, δανεισμό, πιστωτικές κάρτες κ.α. Με έναν απλούστερο ορισμό το E-banking εξυπηρετεί τον χρήστη να εκτελεί τις συναλλαγές του από απόσταση*. Στον παρακάτω πίνακα μπορούμε να δούμε μερικές από τις συναλλαγές που μπορεί να εκτελέσει ένας απλός χρήστης.



Πίνακας 1.1:Κυριότερες υπηρεσίες ηλεκτρονικής τραπεζικής (*Oracle docs- Setting Up Internet Banking*)

1.2 Ιστορική αναδρομή του E-Banking

- Η πρώτη επίσημη έκδοση του internet banking ξεκίνησε στην Νέα Υόρκη το 1981 όπου 4 μεγάλες τράπεζες , οι οποίες ήταν οι εξής: Citibank, Chase Manhattan, Chemical Bank and Manufacturers Hanover, εισήγαγαν την έννοια του Home banking το οποίο παρείχε στον χρήστη την δυνατότητα να εκτελεί τις βασικές τραπεζικές συναλλαγές, αλλά η αποδοχή του κόσμου δεν ήταν η αναμενόμενη με αποτέλεσμα το πρώτο πείραμα του internet banking να αποτύχει.

- Ταυτόχρονα στο Ηνωμένο βασίλειο το 1983 η τράπεζα “Bank of Scotland” μέσω του συστήματος “Homelink” επέτρεπε στους χρήστες να βλέπουν τις δηλώσεις, τραπεζικές μεταφορές και τους λογαριασμούς τους στην οθόνη.

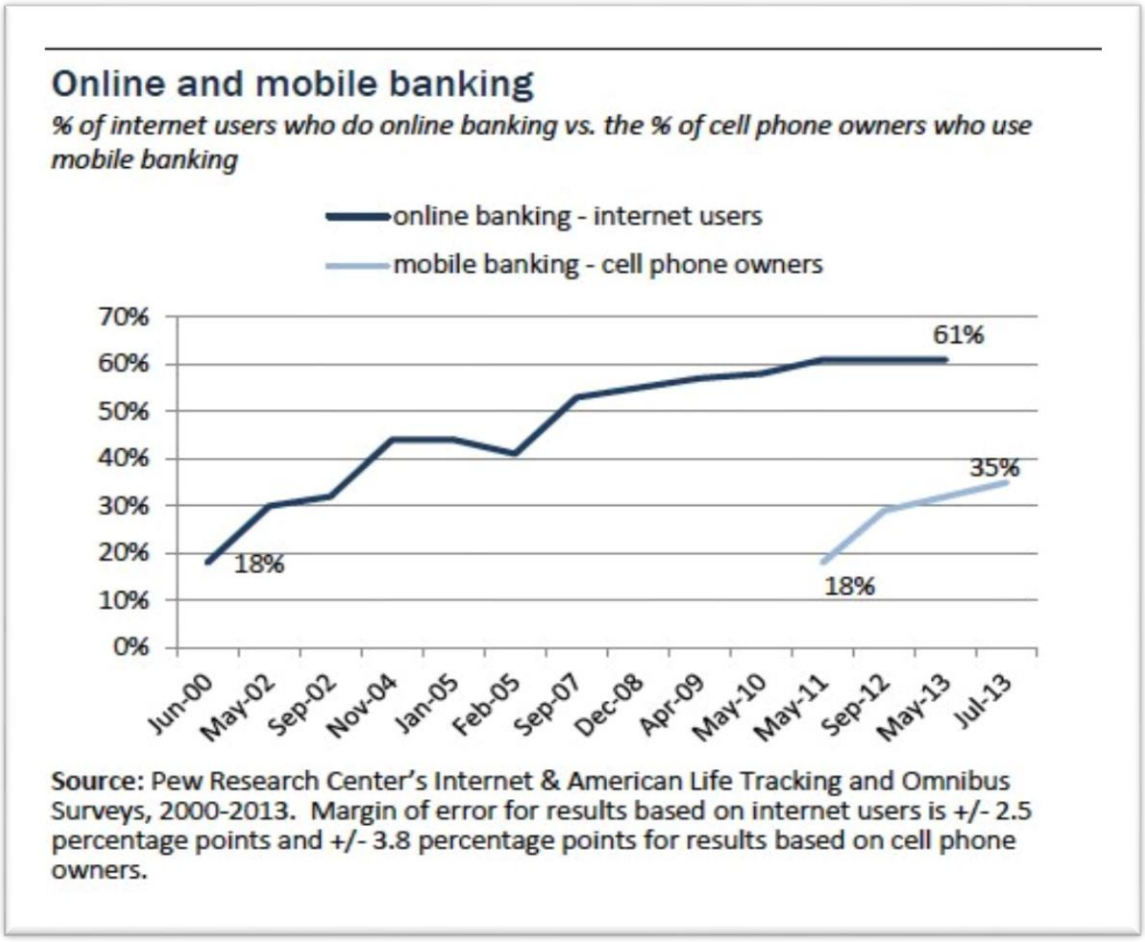
- Το 1994 στην Αμερική, η τράπεζα Stanford Federal Credit Union έγινε η πρώτη που πρόσφερε σε όλους τους πελάτες της Internet Banking.

- Το 1995 η Αμερικάνικη Ομοσπονδιακή τράπεζα προσφέρει στους πελάτες της πρόσβαση στους λογαριασμούς τους σε πραγματικό χρόνο.

- Η εξέλιξη και η επιτυχία του Internet banking προήλθε από την αποκλειστικά ηλεκτρονική τράπεζα Netbank η οποία ιδρύθηκε το 1996 και έκλεισε το 2007.Το domain αλλά και το όνομα της εξαγοράστηκαν από την Αμερικάνικη ομοσπονδιακή τράπεζα Bofl το 2012

- Το 1999 ιδρύεται η “Bank of internet Usa” η οποία ως μέρος της Bofl εγκαινιάζει το ηλεκτρονικό τραπεζικό σύστημα και για επιχειρήσεις.

- Από το 2000 και ύστερα το 80% των αμερικάνικων τραπεζών παρείχαν ηλεκτρονικές υπηρεσίες στους πελάτες τους.



Πίνακας 1.2:Εξέλιξη του online banking αλλά και του mobile banking στην Αμερική από τις αρχές του 2000 μέχρι σήμερα. (*Pew Research Center's Internet & American Life Tracking and Omnibus Surveys*).

ΚΕΦΑΛΑΙΟ 2°: ΥΠΗΡΕΣΙΕΣ E-BANKING

ΕΙΣΑΓΩΓΗ

Σε αυτό το κεφάλαιο αναλύονται εκτενέστερα οι μορφές , υπηρεσίες και τα πλεονεκτήματα-μειονεκτήματα της Ηλεκτρονικής Τραπεζικής.

2.1 Κυριότερες μορφές του E-Banking

2.2 Υπηρεσίες που προσφέρει το E-banking

2.3 Πλεονεκτήματα και οφέλη της χρήσης του E-banking

2.4 Μειονεκτήματα της χρήσης του E-banking

2.1 Κυριότερες μορφές του E-Banking

1. *Web Banking*: Η βασικότερη υπηρεσία toy E-banking μέσω της οποίας ο χρήστης μπορεί να εκτελέσει την πλειοψηφία χρηματικών και μη, τραπεζικών συναλλαγών. Μπορεί να έχει πρόσβαση στο χαρτοφυλάκιό του βλέποντας τα προϊόντα του (χρεωστικές κάρτες, πιστωτικές κάρτες, δάνεια, επενδυτικά προϊόντα κοκ.), προβάλλοντας την τρέχουσα αξία. Μπορεί να έχει πρόσβαση σε ιστορικά δεδομένα καθώς και την εκτέλεση πράξεων που κυμαίνονται από μεταφορές, εμβάσματα και πληρωμές λογαριασμών προς ένα ευρύ φάσμα δικαιούχων.

2. *Phone Banking*: Το ίδιο φάσμα υπηρεσιών που απαριθμούνται παραπάνω προσφέρονται επίσης μέσω μιας ειδικής τηλεφωνικής γραμμής, όπου ο χρήστης εξουσιοδοτεί έναν υπάλληλο τηλεφωνικού κέντρου για να πραγματοποιήσει μια ή περισσότερες συναλλαγές για λογαριασμό του.

3. *Mobile Banking*:Συγκεκριμένα όλες οι λειτουργίες που μπορεί να εκτελέσει ο χρήστης από τον υπολογιστή του μέσω του web banking,μπορούν να εκτελεστούν και μέσω εφαρμογών πλέον με τα smartphones σε μια «ελαφρύτερη» έκδοση

4. *Sms Banking*: Ένα υποσύνολο του web banking όπου ο χρήστης μπορεί να εγκρίνει συναλλαγές ή να λάβει ενημερώσεις σχετικά με την κατάσταση ή την αξία του χαρτοφυλακίου του στο κινητό του μέσω μηνυμάτων sms.

2.2 Υπηρεσίες που προσφέρει το E-banking

Για να γνωρίσει αυτή την ανάπτυξη που έχει τώρα το online banking θα έπρεπε ένα μεγάλο μέρος των υπηρεσιών που μπορεί ένας χρήστης να πραγματοποιήσει στην τράπεζα να είναι σε θέση να κάνει το ίδιο και από την οθόνη του υπολογιστή του. Συγκεκριμένα το online banking προσφέρει στον απλό χρήστη την δυνατότητα:

- Να εποπτεύει το ιστορικό των συναλλαγών του.
- Βλέπει τα υπόλοιπα των λογαριασμών του.
- Να “κατεβάζει” τις τραπεζικές του δηλώσεις ή οτιδήποτε σχετικό με την τράπεζα.
- Να παραγγέλνει προϊόντα όπως μπλοκ επιταγών.
- Να “κατεβάζει” τραπεζικές εφαρμογές όπως mobile banking.
- Να μεταφέρει κεφάλαια μεταξύ των λογαριασμών του.
- Να μεταφέρει κεφάλαια προς τρίτους.

- Να πληρώνει λογαριασμούς.
- Να εκτελεί εμβάσματα στο εξωτερικό.
- Να αιτηθεί έκδοση πιστωτικής κάρτας.
- Να εκτελεί πάγιες εντολές.
- Να αγοράζει επενδύσεις/μετοχές αλλά και να πουλάει.
- Σε επιχειρήσεις θα μπορούσε ακόμη ένας χρήστης να εκτελεί μαζικές πληρωμές στο προσωπικό αλλά και σε προμηθευτές.

2.3 Πλεονεκτήματα και οφέλη της χρήσης του E-banking

Το E-banking είναι και αυτό ένα εργαλείο που έχει γνωρίσει τεράστια ανάπτυξη στον απλό χρήστη την τελευταία δεκαπενταετία από το 2000 και ύστερα όπως τα περισσότερα συστήματα υπολογιστών. Βέβαια τα πλεονεκτήματα που προσφέρει δικαιολογούν τελείως αυτήν την ανάπτυξη. Με το e-banking:

- Μπορείς να έχεις απευθείας 24ώρη πρόσβαση από το κινητό, υπολογιστή,tablet κοκ. σε οποιοδήποτε σημείο βρίσκεσαι. Αυτό είναι και το κυριότερο όφελος του ότι ο χρήστης έχει πρόσβαση όποτε σκεφτεί να χρησιμοποιήσει την υπηρεσία. Στην τράπεζα υπάρχει χρονικό περιθώριο αφού είναι μόνο το πρωί διαθέσιμη στο κοινό. Το online banking παρέχει πρόσβαση στις τραπεζικές υπηρεσίες ακόμα και το Σαββατοκύριακο.
- Είναι εξαιρετικά γρήγορο. Με την εισαγωγή των κωδικών ο χρήστης έχει άμεση πρόσβαση στο interface του λογαριασμού και μπορεί να εκτελέσει μεταφορές άμεσα από έναν λογαριασμό σε έναν άλλο κτλ. Με το πάτημα μερικών κουμπιών.

- Είναι ασφαλές και αξιόπιστο. Περισσότερη μνεία θα δοθεί παρακάτω έτσι και αλλιώς το αντικείμενο το οποίο πραγματεύεται η πτυχιακή εργασία είναι η ασφάλεια των online τραπεζικών συναλλαγών αλλά η πραγματικότητα είναι πως το internet banking είναι 100% ασφαλές και αξιόπιστο. Υπάρχουν αλγόριθμοι που έχουν εφευρεθεί και εταιρίες που έχουν αυτό τον σκοπό αλλά ακόμα και οι ίδιες οι τράπεζες από μόνες δίνουν μεγάλη έμφαση στην ασφάλεια και αξιοπιστία των συναλλαγών. Άλλωστε είναι τόσο λεπτό το ζήτημα της ασφάλειας που αν υπήρχαν λάθη και “ηλεκτρονικές ληστείες” το internet banking θα είχε καταστραφεί.

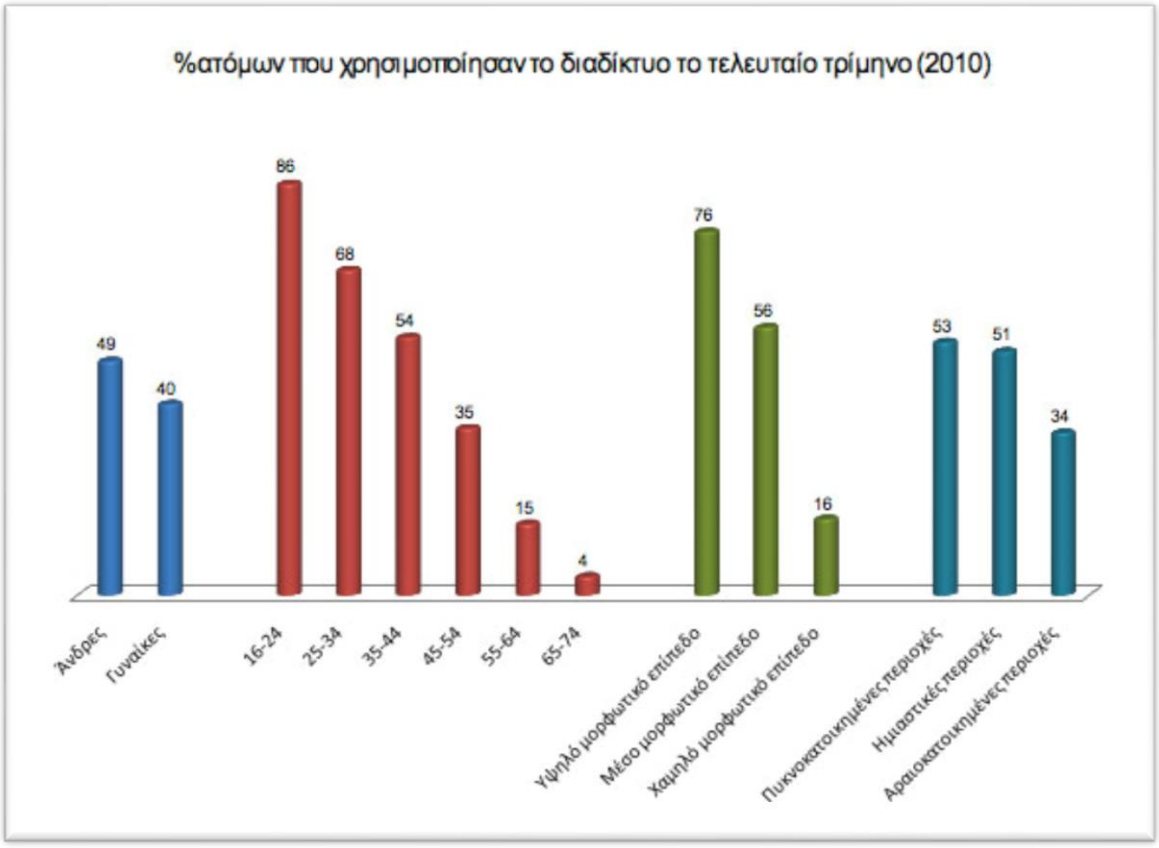
- Μείωση και παράλληλα βελτίωση του περιβάλλοντος. Όλα πλέον με την χρήση του internet banking γίνονται ψηφιακά με αποτέλεσμα να μειώνεται ο τεράστιος όγκος κατανάλωσης χαρτιού. Πλέον ο χρήστης εκτυπώνει την ενημέρωση που επιθυμεί και παραλείπει τα υπόλοιπα σχετικά χαρτιά που παλαιότερα θα λάμβανε.

- Παρακινεί τον κόσμο στην εκμάθηση των νέων τεχνολογιών. Το online banking είναι και αυτό ένα κομμάτι της εξέλιξης της τεχνολογίας και σε μεγαλύτερο βαθμό της κοινωνίας.

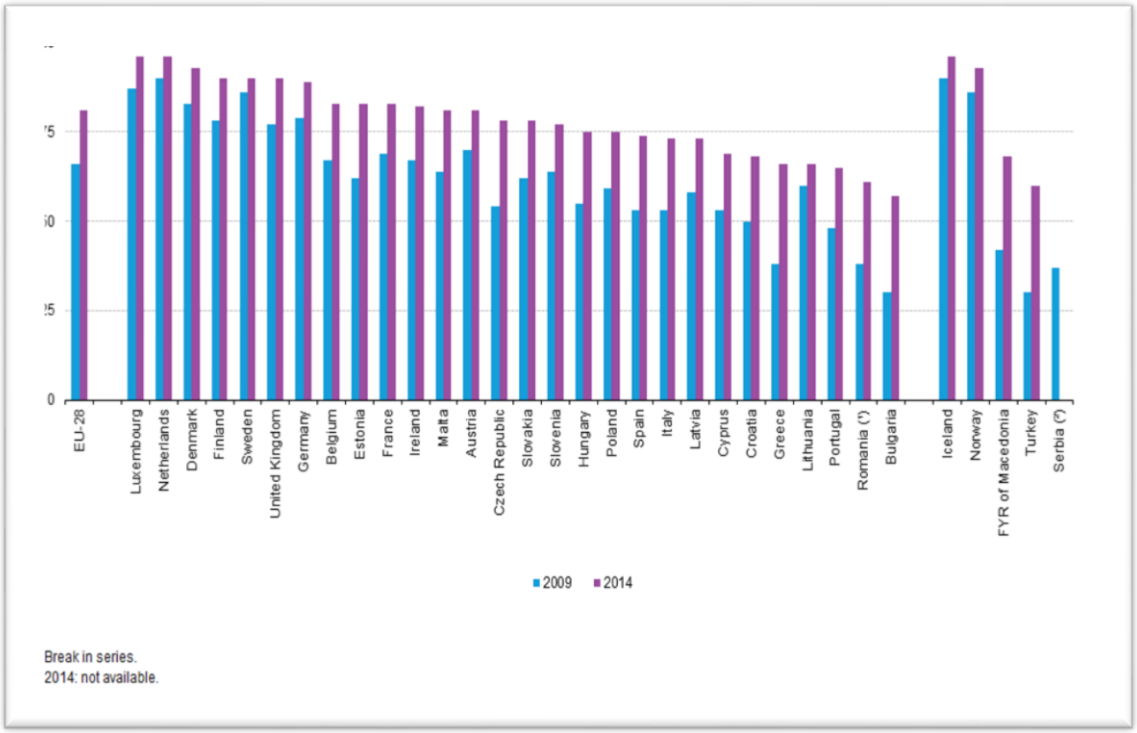
- Ένα ακόμα πλεονέκτημα του E-banking σε θεωρητικό επίπεδο είναι ότι μπορεί να εξαλείψει την φοροδιαφυγή. Οι ηλεκτρονικές συναλλαγές έχουν το προνόμιο αυτό διότι καταγράφονται τα πάντα σε βάσεις δεδομένων και έτσι το κράτος έχει πλήρη εποπτεία για τις κινήσεις ιδιωτών αλλά και επιχειρήσεων. Γίνεται κρατική προσπάθεια με τον όρο του πλαστικού χρήματος και πλέον κάθε επιχείρηση είναι υποχρεωμένη να έχει. Σε οποιαδήποτε άλλη περίπτωση το πρόστιμο ξεκινάει από 1000 €.

2.4 Μειονεκτήματα της χρήσης του E-banking

Το E-banking από μόνο του, για τον λόγο ότι χρησιμοποιείται σε μια διαδικτυακή πλατφόρμα κάνει την χρήση του αμέσως δύσκολη για συγκεκριμένες κοινωνικές ομάδες. Οι άνθρωποι μεγαλύτερης ηλικίας χρειάζονται περισσότερο χρόνο για να κατανοήσουν την έννοια του E-banking αλλά ακόμη περισσότερο για να το χρησιμοποιήσουν. Αυτό βέβαια με τα χρόνια θα εξαλειφτεί διότι οι κοινωνίες εισέρχονται όλο και περισσότερο στην επιστήμη της πληροφορικής με αποτέλεσμα οι νέοι να έχουν πλήρη εικόνα για τις δυνατότητες του διαδικτύου και της χρήσης του.



Πίνακας 2.1: Τα ποσοστά χρηστών του διαδικτύου το πρώτο τρίμηνο του 2010.Έτσι παρατηρείται ότι στις ηλικίες 45-75+ ετών το διαδίκτυο δεν είναι τόσο διαδεδομένο όσο στις ηλικίες 16-45 ετών. Επίσης ένας άλλος παράγοντας που αποτρέπει τους χρήστες από το διαδίκτυο είναι το ποσοστό μορφωτικού επιπέδου αλλά και της οικονομικής κατάστασης . Νοικοκυριά τα οποία δεν αντέχουν οικονομικά την ύπαρξη ηλεκτρονικού υπολογιστή δυσκολεύονται να αφομοιώσουν τέτοιες έννοιες όπως το E-banking.Προσπάθειες βέβαια γίνονται από την σκοπιά της εκπαίδευσης για να χρησιμοποιούν οι νέοι περισσότερο τον ηλεκτρονικό υπολογιστή έτσι ώστε να μην αντιμετωπίζουν προβλήματα αργότερα σε ότι έχει να κάνει με αυτόν αλλά και με την εξέλιξη της τεχνολογίας γενικότερα (*Eurostat*).



Πίνακας 2.2: Στον παραπάνω πίνακα επίσης παρατηρείται το ποσοστό χρήσης του διαδικτύου συγκριτικά τις χρονιές 2009-2014 στις ηλικίες 16-75 ετών. Αυτός ο πίνακας εξηγεί ότι στα επόμενα χρόνια στην Ελλάδα ο όρος υπολογιστής ,δίκτυο και συγκριμένα E-banking θα είναι έννοιες αναγνωρίσιμες σε ποσοστά της τάξεως του 90%(*Eurostat*).

Ένα μείζον πρόβλημα σχετικά με το E-banking είναι η αβεβαιότητα που έχουν οι χρήστες σχετικά με τις συναλλαγές τους. Παλαιότερα ο καθένας πήγαινε στην τράπεζα και για κάθε του συναλλαγή έπαιρνε και απόδειξη. Πλέον με την ύπαρξη της ηλεκτρονικής απόδειξης ένας αρχάριος χρήστης δυσκολεύεται στο να πειστεί και να χρησιμοποιήσει αυτές τις τεχνολογίες. Αυτό είναι λογικό αν σκεφτεί κανείς τις καθημερινές επιθέσεις από χρήστες που γίνονται στο διαδίκτυο. Οι τράπεζες όμως έχουν αναπτύξει ομάδες και συστήματα ειδικά για την ασφάλεια αυτών των συναλλαγών. Δεκάδες άνθρωποι και εταιρίες δουλεύουν πάνω σε αλγόριθμους ασφάλειας και κρυπτογραφίας για να αποτρέπουν τέτοιες επιθέσεις για τις οποίες θα αναφερθούμε παρακάτω.

ΚΕΦΑΛΑΙΟ 3°: Ασφάλεια και Κρυπτογράφηση

ΕΙΣΑΓΩΓΗ

Στην ενότητα αυτή θα παρουσιαστούν οι μορφές κακόβουλου λογισμικού , ηλεκτρονικές επιθέσεις. Επίσης αναλύεται η έννοια της κρυπτογραφίας και τέλος οι ηλεκτρονικές υπογραφές.

Το E-banking προσφέρει πολλά πλεονεκτήματα αλλά το κύριο πρόβλημα που αποτρέπει τον απλό χρήστη από το να το εκμεταλλευτεί τις δυνατότητές του είναι η έλλειψη γνώσης σχετικά με το τι γίνεται με τις συναλλαγές και αν υπάρχει πιθανότητα κλοπής. Κάτι το οποίο είναι λογικό αν δούμε τις καθημερινές επιθέσεις που γίνονται στο διαδίκτυο με διάφορες μορφές επιθέσεων αλλά ας εξετάσουμε πρώτα τις απλές μορφές κακόβουλων προγραμμάτων που μπορεί να συναντήσει ένας απλός χρήστης στην πλοήγησή του στο διαδίκτυο.

3.1 Μορφές κακόβουλου λογισμικού

3.2 Ηλεκτρονικές μορφές επιθέσεων

3.3 Η έννοια της κρυπτογραφίας

3.4 Η κρυπτογραφία ιστορικά

3.5 Αλγόριθμοι Κρυπτογράφησης Δεδομένων

3.6 Ηλεκτρονικές Υπογραφές

3.1 Μορφές κακόβουλου λογισμικού

- Κακόβουλο λογισμικό (Malware)

Οι περισσότεροι χρήστες μπερδεύουν το κακόβουλο λογισμικό με τον ιό. Δηλαδή όταν έχουν να αντιμετωπίσουν κάποιο πρόβλημα θεωρούν γενικά ότι έχουν κάποιον ιό πράγμα που είναι λάθος. Ένα κακόβουλο λογισμικό (Malware) θεωρείται μια γενική έννοια του προβλήματος και ο ιός ένα ειδικό κακόβουλο λογισμικό που θα εξηγηθεί παρακάτω.

- Ιός(Virus)

Ο ιός είναι ένα κακόβουλο λογισμικό που στην ουσία μολύνει τα προγράμματα του υπολογιστή αλλά έχει και την δυνατότητα να αναπαραχθεί και για αυτό τον λόγο ονομάστηκε έτσι. Ουσιαστικά προσκολλάται σε κάποιο σημείο του δίσκου και απλά αναπαράγει τον κώδικά του. Μπορεί επίσης να εξαπλωθεί από έναν υπολογιστή σε κάποιον άλλο μέσω διαδικτύου ή μέσω ενός φορητού μέσου αποθήκευσης όπως κάποιου σκληρού ή USB.

- Δούρειος ίππος(Trojan horse)

Ο Δούρειος ίππος πήρε το όνομά του από την Ηλιάδα του Ομήρου για τον λόγο ότι ξεγελάει τον χρήστη νομίζοντας ότι χρησιμοποιεί κάποιο ασφαλές λογισμικό αλλά στην ουσία εγκαθιστά στον υπολογιστή διάφορα άλλα κακόβουλα προγράμματα τα οποία μπορούν να υποκλέψουν και σημαντικές πληροφορίες από τον υπολογιστή.

- Σκουλήκι Υπολογιστή (Computer Worm)

Το σκουλήκι του υπολογιστή είναι παρόμοιο κακόβουλο λογισμικό με τον ιό απλά με την διαφορά ότι δεν αναπαράγεται στον τοπικό υπολογιστή του χρήστη με την βοήθεια του ιδίου, αλλά χρησιμοποιεί δίκτυο υπολογιστών για να στέλνει αντίγραφα του κώδικά του σε άλλους υπολογιστές που είναι συνδεδεμένοι σε αυτό.

- Λογισμικό Κατασκοπίας(Spyware)

Το Spyware διεισδύει στο λογισμικό του υπολογιστή και εκτελείται στο παρασκήνιο κάνοντας διάφορες διαδικασίες και έχει μερικές φορές ως αποτέλεσμα στο να καθυστερεί ο υπολογιστής πέραν του συνηθισμένου. Κοινώς φυλακίζει τους πόρους του υπολογιστή και επηρεάζει την λειτουργία του. Επίσης μπορεί να συγκεντρώνει στοιχεία του χρήστη όπως κωδικούς πρόσβασης, ιστοσελίδες που επισκέπτεται κτλ .Εκτιμάται ότι πάνω από το 80% των προσωπικών υπολογιστών είναι μολυσμένο από αυτό το είδος ιού.

- Λογισμικό Ανεπιθύμητων Διαφημίσεων **(**Adware**)**

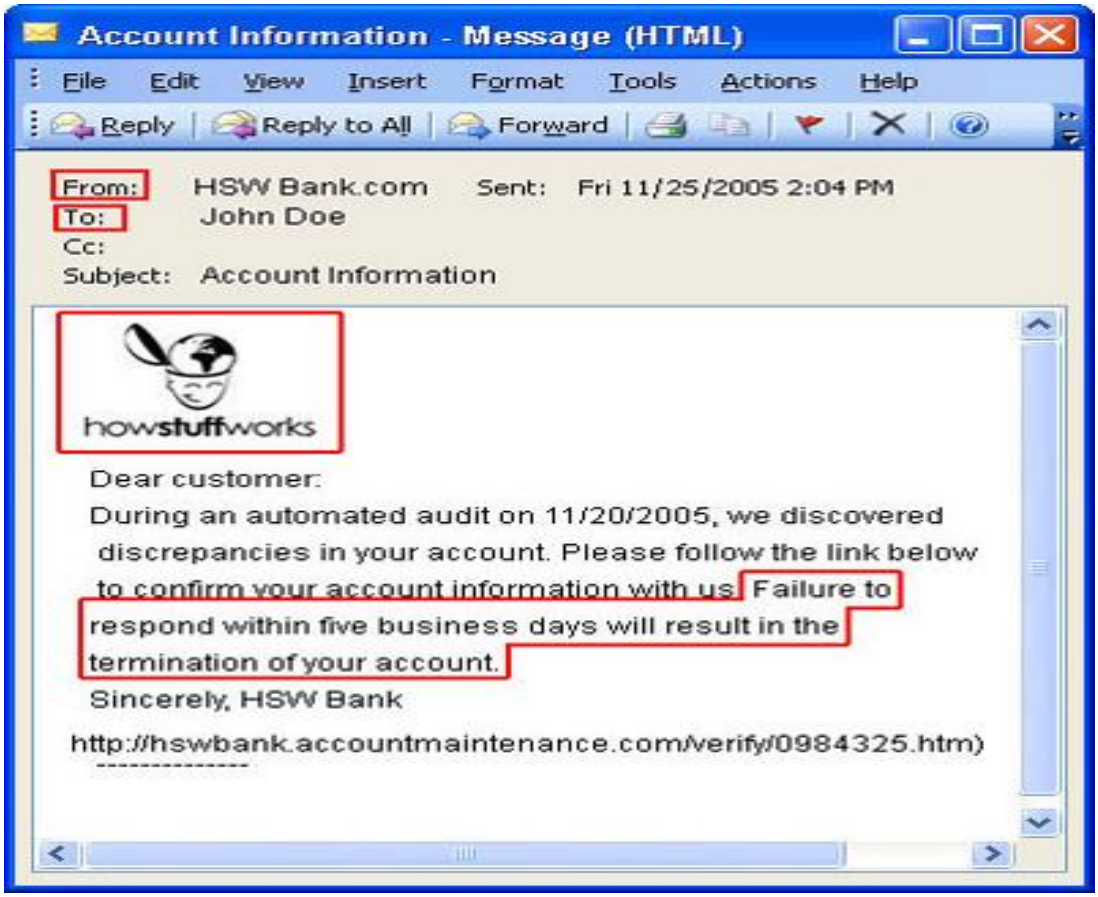
Είναι το κακόβουλο λογισμικό που διεισδύει στο λογισμικό του υπολογιστή όταν κάποιος χρήστης εν αγνοία του θα κάνει κλικ σε μια προτεινόμενη διαφήμιση άγνωστης πηγής. Στην συνέχεια έχοντας μολύνει τον υπολογιστή οι διαφημίσεις και τα αναδυόμενα παράθυρα μπορούν να κάνουν από δύσχρηστη έως αδύνατη την πλοήγηση ενός χρήστη.

- Καταγραφή Πληκτρολόγησης (Keylogger)

Η καταγραφή πληκτρολόγησης είναι ένα κακόβουλο λογισμικό που έχει σαν στόχο το να καταγράψει το τι πληκτρολογεί κάθε φορά ο χρήστης έτσι ώστε να συγκεντρώσει διάφορα στοιχεία. Τα στοιχεία αυτά ως συνήθως είναι usernames, κωδικοί πρόσβασης, αριθμοί καρτών τραπέζης κτλ.

- Ηλεκτρονικό Ψάρεμα(Phishing)

Το phishing είναι ένας τρόπος επίθεσης ο οποίος ξεγελά τον χρήστη παραπλανώντας τον ότι είναι ένα αξιόπιστο εργαλείο ή οντότητα και του ζητάει πληροφορίες οι οποίες είναι πολύτιμες για αυτόν όπως κωδικούς πρόσβασης, αριθμούς καρτών κοκ. Ενδεικτικό παράδειγμα στην παρακάτω εικόνα ότι η υποτιθέμενη τράπεζα ζητάει από τον χρήστη μέσω email να ανακατευθυνθεί στον σύνδεσμο που του υπαγορεύει διαφορετικά θα του απενεργοποιήσουν τον λογαριασμό.



Εικόνα 3.1:Παράδειγμα Ηλεκτρονικού Ψαρέματος

- Spam

Τα spam είναι ανεπιθύμητα ηλεκτρονικά μηνύματα (emails) που αποστέλλονται μαζικά σε διάφορους χρήστες ηλεκτρονικού ταχυδρομείου. Ο στόχος τους είναι να προσπαθήσουν να κάνουν τον χρήστη αγοράσει διάφορα προϊόντα ή υπηρεσίες. Για να παραπλανήσουν τον χρήστη χρησιμοποιούν ψευδή στοιχεία αποστολέα και στο θέμα του μηνύματος προσπαθούν να τραβήξουν την προσοχή του χρήστη με παραδείγματα όπως: «Ο 1^{ος} υπερτυχερός», «Κέρδισες στην κλήρωση για ένα ταξίδι» κ.ο.κ..

3.2 ΗΛΕΚΤΡΟΝΙΚΕΣ ΜΟΡΦΕΣ ΕΠΙΘΕΣΕΩΝ

Dos Attacks

Οι κυριότερες μορφές επιθέσεων που έχουν καταγραφεί στο διαδίκτυο σε μεγάλες εταιρίες και γίνονται σε καθημερινή βάση ανά τον κόσμο και ονομάζονται επιθέσεις άρνησης υπηρεσιών ή παγκοσμίως dos (denial of service) attacks.Οι επιθέσεις αυτές έχουν σκοπό να προσβάλουν τον υπολογιστή-εξυπηρετητή(Server) ή μια υπηρεσία της εταιρίας. Οι επιθέσεις είναι 2 ειδών:

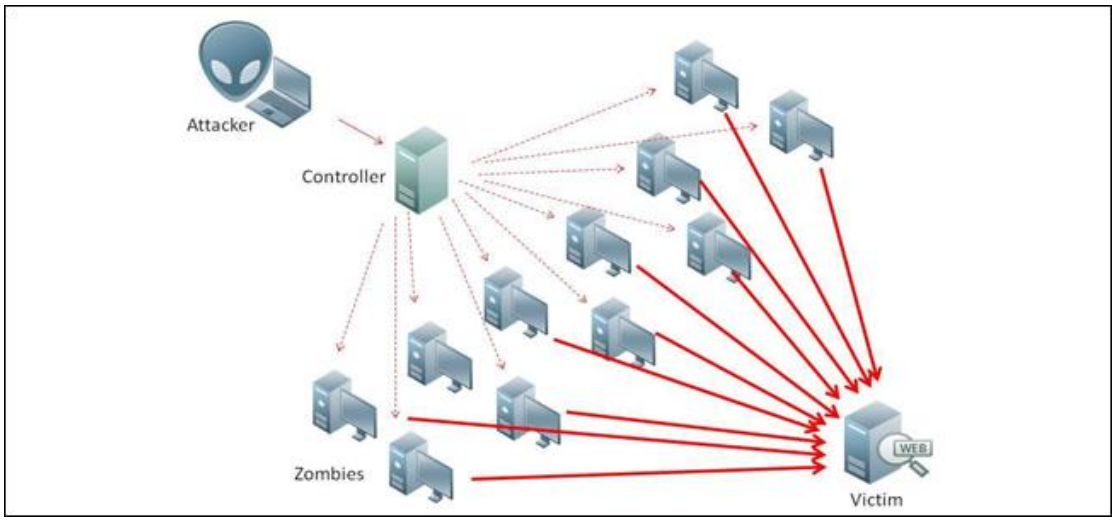
1. Η μία είναι η επίθεση κατά την οποία ο εξυπηρετητής ή η υπηρεσία αναγκάζεται να καταρρεύσει και να πρέπει να επανεκκινηθεί.
2. Η δεύτερη είναι η αποστολή υπερβολικά μεγάλου αριθμού ψεύτικων αιτήσεων για εξυπηρέτηση με αποτέλεσμα η υπηρεσία να μην μπορεί να εξυπηρετήσει τους νόμιμους χρήστες που θέλουν την υπηρεσία.

Ddos Attacks

Οι κατανεμημένες επιθέσεις άρνησης υπηρεσιών ή αλλιώς Ddos (distributed denial of service) attacks εκτελούν πολλαπλές επιθέσεις μέσω άλλων θυμάτων ή και θυτών έτσι ώστε να προσβάλλουν το τελικό θύμα που επιθυμούν.

Υπολογιστής Zombie

Για να καταφέρουν τις παραπάνω επιθέσεις οι χρήστες «hackers» χρησιμοποιούν τους υπολογιστές zombie.Υπολογιστής zombie θεωρείται: *συνδεδεμένος διαδικτυακά υπολογιστής τον οποίο ελέγχει ο χρήστης που κάνει την επίθεση.* Ένας υπολογιστής zombie συνήθως αποτελεί μέρος ενός μεγαλύτερου δικτύου υπολογιστών zombie ο οποίο ανήκει σε κάποιον χρήστη και χρησιμοποιείται για την διεξαγωγή επιθέσεων άρνησης υπηρεσιών. Οι περισσότεροι χρήστες υπολογιστών zombie δεν γνωρίζουν ότι ο υπολογιστής τους έχει περιέλθει σε αυτήν την κατάσταση και χρησιμοποιείται από κάποιον τρίτο για άλλους σκοπούς.



Εικόνα 3.2:Κατανεμημένη επίθεση άρνησης υπηρεσιών

Τα συνηθέστερα συμπτώματα αυτών των επιθέσεων είναι:

- Πρωτοφανής καθυστέρηση στις συγκεκριμένες ιστοσελίδες.
- Μη διαθέσιμη πρόσβαση αλλά και γενικότερη αδυναμία πρόσβασης στο διαδίκτυο .
- Αύξηση των ανεπιθύμητων μηνυμάτων (Spam).

Υπάρχουν και κάποιες άλλες πιο σπάνιες περιπτώσεις όπως:

- Μη πρόσβαση στο διαδίκτυο.

- Συνεχόμενη αδυναμία πρόσβασης στις συγκεκριμένες ιστοσελίδες για μεγάλο χρονικό διάστημα.

Κατηγορίες Dos Attacks

Μερικοί από τους πιο γνωστούς τρόπους επιθέσεων είναι οι παρακάτω:

- Ping of Death

Αυτή η τεχνική επίθεσης είχε στόχο να παγώσει(hang) το σύστημα ή να πάθει κατάρρευση(crash) ή και να επανεκκινηθεί(reboot). Η μέθοδος είναι αρκετά απλή. Ένα πακέτο ping έχει κανονικά μέγεθος 64 bytes. Πολλοί τύποι ηλεκτρονικών υπολογιστών δεν μπορούν να χειριστούν πακέτα ping που έχουν μέγεθος μεγαλύτερο από 65535 bytes, δηλαδή το μέγιστο επιτρεπτό από το πρωτόκολλο IP. Κατά συνέπεια, η επίθεση Ping Of Death περιλαμβάνει την συνεχή αποστολή μεγάλων πακέτων ping σε κάποιον υπολογιστή μέχρι ο τελευταίος να τεθεί εκτός λειτουργίας.

- ICMP flood

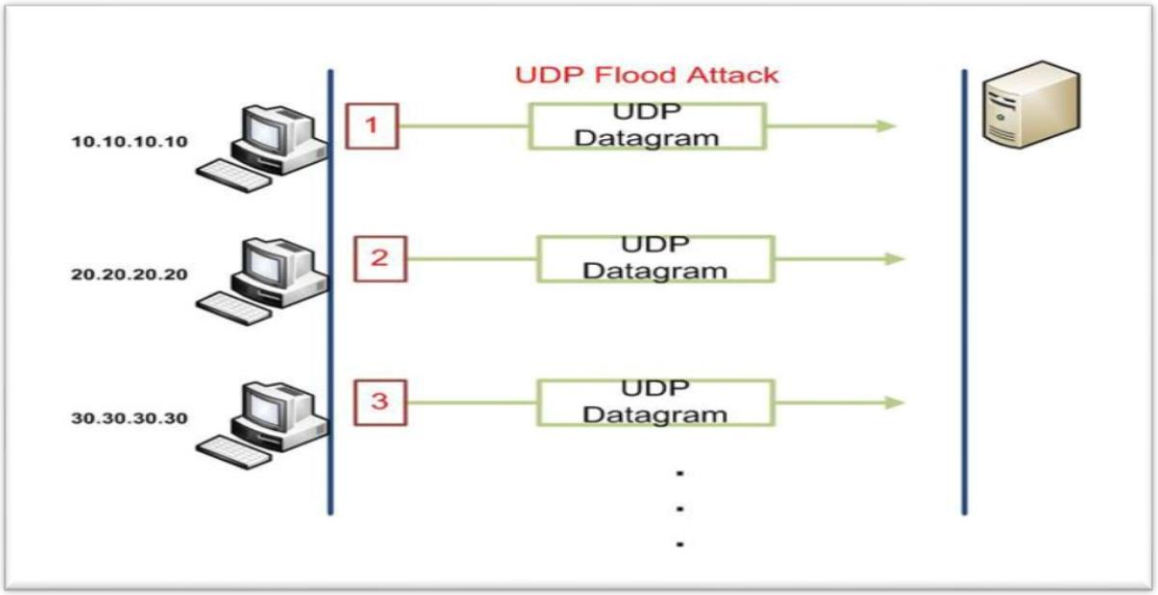
Τα ICMP(Internet Control Message Protocol) πακέτα είναι από τα βασικά πρωτόκολλα διαδικτύου. Χρησιμοποιείται κυρίως για τον έλεγχο λαθών ενός δικτύου για την ανταλλαγή μηνυμάτων. Κατά την ανταλλαγή των μηνυμάτων ο αποστολέας στέλνει ένα πακέτο «ECHO_REQUEST» και περιμένει από τον παραλήπτη ένα πακέτο «ECHO_REPLY».Στην περίπτωση της επίθεσης ICMP flood ο αποστολέας-θύτης βομβαρδίζει τον παραλήπτη-θύμα με πακέτα «ECHO_REQUEST» έτσι ώστε να τον κρατάει συνεχώς απασχολημένο από οποιαδήποτε άλλη ωφέλιμη εργασία.

- Smurf attack

Η συγκεκριμένη επίθεση έχει αρκετά στοιχεία της προηγούμενης επίθεσης. Κατά την έναρξη της επίθεσης πολλαπλά πακέτα «ECHO_REQUEST» σε IP broadcast διευθύνσεις δικτύων. Δεδομένου ότι στέλνονται στις broadcast διευθύνσεις των δικτύων στέλνονται και σε όλους τους υπολογιστές που είναι συνδεδεμένοι σε αυτά. Με αποτέλεσμα να έχουν ένα τεράστιο αριθμό πακέτων «ECHO_REPLY» και έτσι οι εξυπηρετητές-θύματα και γενικότερα όλο το δίκτυο να καταρρεύσει.

- UDP flood

Σε αυτή την κατηγορία επίθεσης χρησιμοποιούνται πακέτα UDP.Η αντίστοιχη μορφή επίθεσης υπάρχει και για πακέτα TCP και μάλιστα είναι πολύ πιο συνηθισμένη. Στην επίθεση UDP flood ο αποστολέας στέλνει πολλαπλά και μεγάλα πακέτα UDP σε διάφορες ports του παραλήπτη. Ο παραλήπτης προκειμένου να διαπιστώσει να στις random ports «ακούει» διαφορετικά πρέπει να απαντήσει με ένα ICMP Destination Unreachable.Έτσι ο υπολογιστής θύμα αναγκάζεται να απαντήσει σε ένα μεγάλο αριθμό πακέτων οπότε είναι δεδομένο ότι δεν θα μπορεί να εξυπηρετήσει άλλους χρήστες.



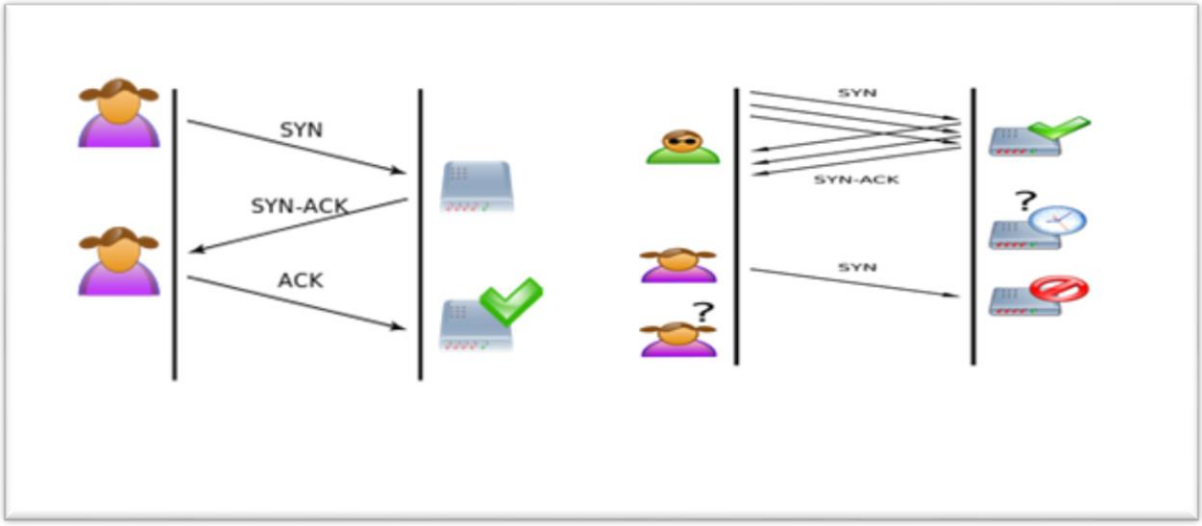
Εικόνα 3.3:Παράδειγμα επίθεσης UDP Flood

- **TCP SYN flood**

Η επίθεση SYN flood είναι η επίθεση κατά την οποία ο θύτης στέλνει πολλαπλές αιτήσεις SYN(Synchronization) στο θύμα. Το πρωτόκολλο TCP απαιτεί για να γίνει σύνδεση μεταξύ 2 υπολογιστών με τα εξής 3 βήματα:

- Ο αποστολέας στέλνει ένα πακέτο SYN(Synchronize)
- Ο παραλήπτης απαντάει με ένα πακέτο SYN-ACK(Synchronize Acknowledge)
- Ο αποστολέας ύστερα στέλνει ένα τελευταίο πακέτο ACK και η σύνδεση θεωρείται επιτυχής.

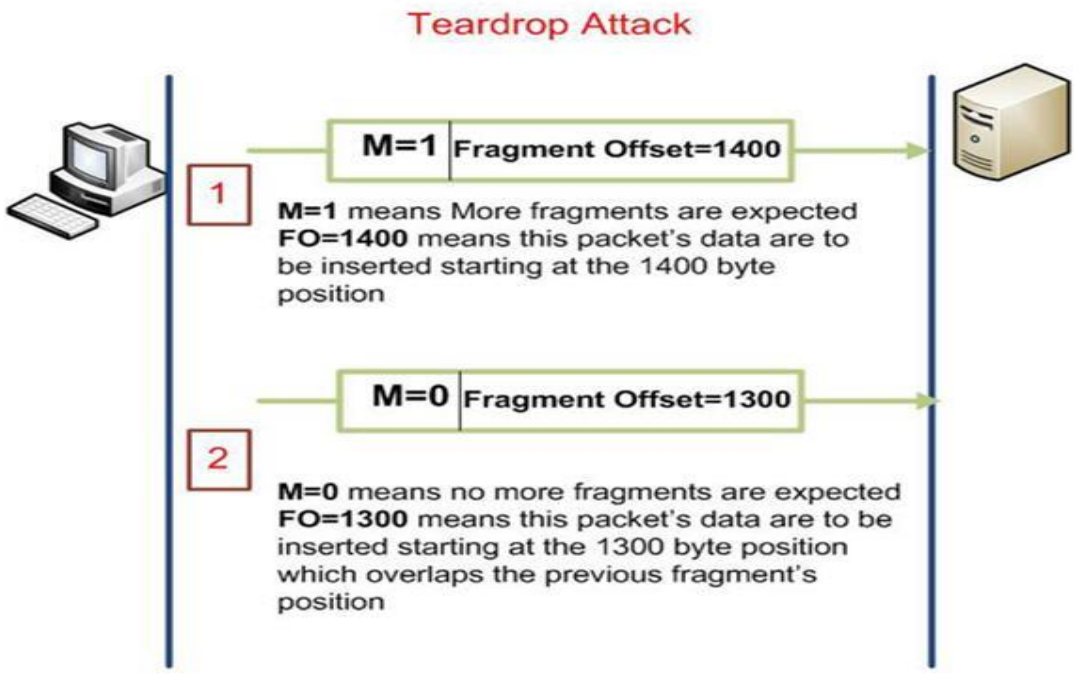
Η τεχνική της επίθεσης είναι πολύ απλή όπου ο επιτιθέμενος στέλνει πολλαπλές αιτήσεις SYN και δεν στέλνει ACK έτσι η διαδικασία συνεχίζεται επ' άπειρον με αποτέλεσμα ο υπολογιστής-θύμα να εξαντλεί σημαντικούς υπολογιστικούς πόρους και να μην μπορεί να εξυπηρετήσει τους νόμιμους χρήστες.



Εικόνα 3.4:Παράδειγμα επίθεσης TCP SYN flood

- Teardrop attack

Αυτός ο τύπος επίθεσης έχει να κάνει με κατακερματισμένα IP πακέτα και την επανασυναρμολόγησή του. Μια κεφαλίδα(header) του πρωτοκόλλου IP είναι ο δείκτης εντοπισμού τμήματος «Fragment offset» ο οποίος προσδιορίζει την θέση ενός συγκεκριμένου κομματιού, από την αρχή του αρχικού ακομμάτιαστου αυτοδύναμου πακέτου. Το πρώτο κομμάτι έχει δείκτη εντοπισμού τμήματος 0. Αυτό επιτρέπει έναν μέγιστο αριθμό θέσεων (213 – 1) × 8 = 65,528 bytes, το οποίο και ξεπερνά το μέγιστο μήκος του IP πακέτου, που είναι 65535 bytes, εάν συμπεριλάβουμε και το μήκος της επικεφαλίδας (65,528 + 20 = 65,548 bytes). Οπότε κοινώς εντοπίζει την σειρά των πακέτων που αποστέλλονται στον υπολογιστή. Εάν ο επιτιθέμενος στέλνει πακέτα τα οποία υπερκαλύπτουν το ένα το άλλο , καταστούν τον δείκτη εντοπισμού ανίκανο και έτσι δεν μπορεί να δημιουργήσει ποτέ το πακέτο που του αποστέλλεται. Ένα απλό παράδειγμα είναι το παρακάτω:

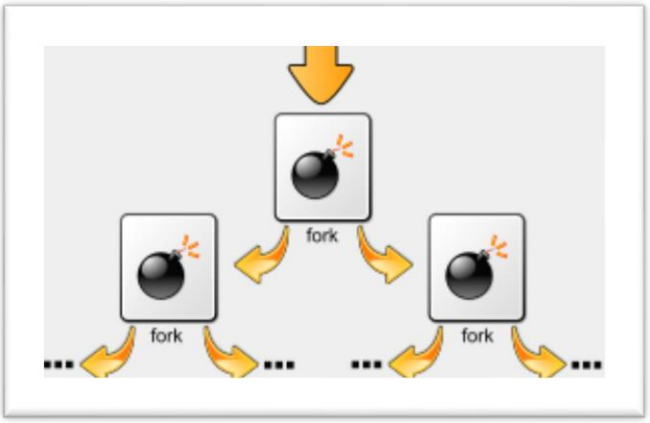


Εικόνα 3.5 : Παράδειγμα επίθεσης Teardrop attack

- Fork bombs

Η επίθεση fork bomb έχει να κάνει με την προγραμματιστική συνάρτηση fork.Τρέχοντας την διεργασία fork δημιουργείται μια καινούργια διεργασία ή οποία με την σειρά της δημιουργεί και αυτή μια νέα διεργασία και αυτό συνεχίζεται. Έτσι ο διαθέσιμος χώρος στον δίσκο μειώνεται σημαντικά και τελικά το σύστημα καταρρέει διότι δεν υπάρχει χώρος για μια διεργασία που θα σταματήσει το ατέρμονο αυτό πρόγραμμα. Η εικόνα παρακάτω αναπαριστά την επίθεση σχηματικά.

Εικόνα 3.6 : Παράδειγμα επίθεσης Fork bombs



- Email bombs

Ο όρος email bomb αναφέρεται σε ένα είδος επίθεσης κατά την οποία ο επιτιθέμενος στέλνει μία τεράστια ποσότητα ηλεκτρονικών μηνυμάτων σε μία διεύθυνση ηλεκτρονικού ταχυδρομείου με σκοπό να γεμίσει τον διαθέσιμο χώρο στον δίσκο και να προκαλέσει δυσλειτουργία στον email server. Μία μορφή email bomb που είναι αρκετά συνηθισμένη ονομάζεται ZIP bomb. Μία ZIP bomb είναι ένα email που περιέχει ένα συμπιεσμένο αρχείο ως επισυναπτόμενο. Αυτό το συμπιεσμένο αρχείο περιλαμβάνει ένα τεράστιο αρχείο κειμένου αρκετών GB, το οποίο αποτελεί ουσιαστικά συνεχή επανάληψη ενός γράμματος (πχ α). Ένα τέτοιο αρχείο έχει το εξής χαρακτηριστικό: Όταν είναι συμπιεσμένο καταλαμβάνει ελάχιστο χώρο, αλλά όταν αποσυμπιεστεί ο χώρος που δεσμεύει είναι τεράστιος. Άρα, όταν ο email server προσπαθήσει να αποσυμπιέσει το αρχείο για να ελέγξει το περιεχόμενό του, τότε το αποσυμπιεσμένο αρχείο θα δεσμεύσει μία τεράστια ποσότητα υπολογιστικής ισχύος, μνήμης RAM, και σκληρού δίσκου. Αυτό έχει πολλές φορές ως συνέπεια το πάγωμα του υπολογιστή.

3.3 Η έννοια της κρυπτογραφίας

Βλέποντας ότι πολλοί τρόποι επίθεσης και κακόβουλα λογισμικά αναπτύσσονται στον χώρο της πληροφορικής και με τον φόβο ότι η πληροφορία είναι επισφαλής , αναπτύχθηκε ένα διεπιστημονικό γνωστικό πεδίο που ασχολείται με τη μελέτη, την ανάπτυξη και τη χρήση τεχνικών κρυπτογράφησης και αποκρυπτογράφησης με σκοπό την απόκρυψη του περιεχομένου των μηνυμάτων το οποίο ονομάζεται κρυπτογραφία. Η κρυπτογραφία ασχολείται με την μελέτη της ασφαλούς επικοινωνίας.

Η κρυπτογραφία αν την εξετάσει κανείς από μια θεωρητική σκοπιά έχοντας ως γνωστικό υπόβαθρο μόνο την λέξη και τον ορισμό της τότε θα πιστέψει ότι είναι μια δυσνόητη αλλά και δύσκολη επιστήμη. Στην πραγματικότητα είναι εξαιρετικά απλή. Η κρυπτογραφία χρησιμοποιείται για τη μετατροπή της πληροφορίας μηνυμάτων από μια κανονική, κατανοητή μορφή σε έναν «γρίφο», που χωρίς τη γνώση του κρυφού μετασχηματισμού θα παρέμενε ακατανόητος. Ο όρος 'κρυπτογραφία' αναφέρεται σε ένα σύνολο τεχνικών που χρησιμοποιούνται για να διασφαλίσουν ότι τα δεδομένα δεν μπορούν να διαβαστούν από οποιονδήποτε δεν είναι μέτοχος στη δημιουργία και τη διάδοσή τους. Περιλαμβάνει την μετατροπή ενός συνόλου δεδομένων (το αποκαλούμενο απλό κείμενο) σε μια περιπλεγμένη μορφή (κρυπτογραφημένο κείμενο).

3.4 Η κρυπτογραφία ιστορικά

- Η πρώτη γραφή που ανακαλύφθηκε από τα αρχαία χρόνια είναι τα ιερογλυφικά και την αρχαία Αίγυπτο τα οποία χρησιμοποιούνταν από το 3200 π.Χ. και είναι το παλαιότερο γνωστό σύστημα γραφής. Η συγκεκριμένη γραφή αποκρυπτογραφήθηκε το 1822 από τον Γάλλο φιλόσοφο Jean-François Champollion.

- Αργότερα ανακαλύφθηκε η Γραμμική Ά το 1900 από τον Άγγλο αρχαιολόγο Arthur Evans. Η Γραμμική Ά χρονολογείται από το 1800 π.Χ μέχρι το 1450 π.Χ. και θεωρείται Μυκηναϊκή γραφή. Η Γραμμική Ά δεν έχει αποκρυπτογραφηθεί και αποτελεί ένα από τα μεγαλύτερα μυστήρια της σύγχρονης αρχαιολογίας. Η αποκρυπτογράφησή της θα αποκαλύψει τη γλώσσα και ενδεχομένως και την καταγωγή των Μινωιτών.

- Ο απόγονο της Γραμμικής Ά είναι η γραμμική ΄Β, την οποία ανακάλυψε ο Arthur Evans που είχε ανακαλύψει και την Γραμμική Ά. Η Γραμμική ΄Β χρονολογείται περίπου από το 1450 π.Χ. έως το 1200 π.Χ. και αποκρυπτογραφήθηκε το 1952 από τον αρχιτέκτονα Michael Ventris. Ο Ventris ζήτησε τη βοήθεια του κλασικού φιλολόγου John Chadwick.

- Οι επόμενες μορφές κρυπτογραφίας τοποθετούνται στις περιόδους των παγκοσμίων πολέμων I και II. Τα κρυπτοσυστήματα αυτής της περιόδου αρχίζουν να γίνονται πολύπλοκα, και να αποτελούνται από μηχανικές και ηλεκτρομηχανικές κατασκευές, οι οποίες ονομάζονται «κρυπτομηχανές». Η κρυπτανάλυσή τους, απαιτεί μεγάλο αριθμό προσωπικού ενώ ταυτόχρονα γίνεται εξαιρετικά αισθητή η ανάγκη για μεγάλη υπολογιστική ισχύ. Το γνωστότερο τότε σύστημα υπήρξε το Enigma.

3.5 Αλγόριθμοι Κρυπτογράφησης Δεδομένων

- Αλγόριθμος του Καίσαρα

Από τις παλιότερες μεθόδους κρυπτογράφησης είναι ο *αλγόριθμος του Καίσαρα* , όπου αν ένα γράμμα στο αρχικό κείμενο είναι το *Ν*ιοστό στο αλφάβητο ,αντικαθίσταται από το (*N+K)* ιοστό γράμμα του αλφαβήτου, όπου *K* είναι ένας σταθερός ακέραιος (για τον αλγόριθμο του Καίσαρα *K=3*).Ένα απλό παράδειγμα παρακάτω θα μας διευκολύνει στο να καταλάβουμε ακριβώς τον αλγόριθμο. Αν υποθέσουμε ότι θέλουμε να κρυπτογραφήσουμε την λέξη κρυπτογραφία με τον συγκεκριμένο αλγόριθμο θα πάρουμε την λέξη:

Κρυπτογραφία→Νυψτχσζυγωμγ

Απλούστερα μεταθέτουμε το γράμμα της αλφαβήτου κατά K=3 φορές.

- Κρυπτογράφηση με πίνακα κλειδί

Μια καλύτερη μέθοδος είναι να χρησιμοποιήσουμε ένα γενικό πίνακα που θα ορίζει την αλλαγή που θα γίνει για κάθε γράμμα του κειμένου προς κρυπτογράφηση, ο πίνακας θα μας πει ποιο γράμμα να βάλουμε στο κρυπτογραφημένο κείμενο .

Γράμματα = [α β γ δ ε ζ η θ ι κ λ μ ν ξ ο π ρ σ τ υ φ χ ψ ω ! . , ; *]

Πίνακας = [κ ο α π λ ν ι β μ ε υ φ σ ξ γ τ ζ ς δ θ ρ ω η χ γ ? ! * ,]

Άρα η λέξη κρυπτογραφία με αυτή την μέθοδο θα κρυπτογραφηθεί ως εξής:

Κρυπτογραφία!→Εςρζθτπςκψμκ?

- Αλγόριθμος Vigenere (Vigenere cipher)

Ο αλγόριθμος κρυπτογράφησης Vigenere είναι μία μέθοδος κρυπτογράφησης σε αλφαβητικό κείμενο στο οποίο εφαρμόζονται διαφορετικοί αλγόριθμοι κρυπτογράφησης Καίσαρα με βάση τη θέση των γραμμάτων μιας λέξης ή φράσης κλειδί. Σε ένα κρυπτογράφημα Καίσαρα, κάθε γράμμα της αλφαβήτου μετατοπίζεται κατά ένα αριθμό θέσεων. Για παράδειγμα, σε ένα κρυπτογράφημα Καίσαρα με μετατόπιση 3, το *B* θα γίνει *E*, το *K* θα γίνει *N* και ούτω καθεξής. Η κρυπτογράφηση Vigenère αποτελείται από πολλούς αλγόριθμους κρυπτογράφησης του Καίσαρα με διαφορετικές τιμές μετατόπισης που χρησιμοποιούνται σε ακολουθία. Για την κρυπτογράφηση, ένας πίνακας του αλφάβητου μπορεί να χρησιμοποιηθεί, ως πίνακας αντικατάστασης. Αποτελείται από το αλφάβητο, που αναγράφεται σε διαφορετικές γραμμές (ή στήλες) τόσες φορές όσες και τα γράμματα του αλφαβήτου και κάθε αλφάβητο μετατοπίζεται κυκλικά σε σχέση με το προηγούμενο αλφάβητο, ώστε να υπάρχουν όλοι οι πιθανοί αλγόριθμοι κρυπτογράφησης του Καίσαρα. Κατά τη διαδικασία κρυπτογράφησης, χρησιμοποιείται διαφορετικό αλφάβητο σε κάθε ένα από τα γράμματα. Για παράδειγμα παίρνοντας τον πίνακα αντικατάστασης παρακάτω:

	α	β	γ	δ	ε	ζ	η	θ	ι	κ	λ	μ	ν	ξ	ο	π	ρ	σ	τ	υ	φ	χ	ψ	ω
Α	Α	Β	Γ	Δ	Ε	Ζ	Η	Θ	Ι	Κ	Λ	Μ	Ν	Ξ	Ο	Π	Ρ	Σ	Τ	Υ	Φ	Χ	Ψ	Ω
Β	Β	Γ	Δ	Ε	Ζ	Η	Θ	Ι	Κ	Λ	Μ	Ν	Ξ	Ο	Π	Ρ	Σ	Τ	Υ	Φ	Χ	Ψ	Ω	Α
Γ	Γ	Δ	Ε	Ζ	Η	Θ	Ι	Κ	Λ	Μ	Ν	Ξ	Ο	Π	Ρ	Σ	Τ	Υ	Φ	Χ	Ψ	Ω	Α	Β
Δ	Δ	Ε	Ζ	Η	Θ	Ι	Κ	Λ	Μ	Ν	Ξ	Ο	Π	Ρ	Σ	Τ	Υ	Φ	Χ	Ψ	Ω	Α	Β	Γ
Ε	Ε	Ζ	Η	Θ	Ι	Κ	Λ	Μ	Ν	Ξ	Ο	Π	Ρ	Σ	Τ	Υ	Φ	Χ	Ψ	Ω	Α	Β	Γ	Δ
Ζ	Ζ	Η	Θ	Ι	Κ	Λ	Μ	Ν	Ξ	Ο	Π	Ρ	Σ	Τ	Υ	Φ	Χ	Ψ	Ω	Α	Β	Γ	Δ	Ε
Η	Η	Θ	Ι	Κ	Λ	Μ	Ν	Ξ	Ο	Π	Ρ	Σ	Τ	Υ	Φ	Χ	Ψ	Ω	Α	Β	Γ	Δ	Ε	Ζ
Θ	Θ	Ι	Κ	Λ	Μ	Ν	Ξ	Ο	Π	Ρ	Σ	Τ	Υ	Φ	Χ	Ψ	Ω	Α	Β	Γ	Δ	Ε	Ζ	Η
Ι	Ι	Κ	Λ	Μ	Ν	Ξ	Ο	Π	Ρ	Σ	Τ	Υ	Φ	Χ	Ψ	Ω	Α	Β	Γ	Δ	Ε	Ζ	Η	Θ
Κ	Κ	Λ	Μ	Ν	Ξ	Ο	Π	Ρ	Σ	Τ	Υ	Φ	Χ	Ψ	Ω	Α	Β	Γ	Δ	Ε	Ζ	Η	Θ	Ι
Λ	Λ	Μ	Ν	Ξ	Ο	Π	Ρ	Σ	Τ	Υ	Φ	Χ	Ψ	Ω	Α	Β	Γ	Δ	Ε	Ζ	Η	Θ	Ι	Κ
Μ	Μ	Ν	Ξ	Ο	Π	Ρ	Σ	Τ	Υ	Φ	Χ	Ψ	Ω	Α	Β	Γ	Δ	Ε	Ζ	Η	Θ	Ι	Κ	Λ
Ν	Ν	Ξ	Ο	Π	Ρ	Σ	Τ	Υ	Φ	Χ	Ψ	Ω	Α	Β	Γ	Δ	Ε	Ζ	Η	Θ	Ι	Κ	Λ	Μ
Ξ	Ξ	Ο	Π	Ρ	Σ	Τ	Υ	Φ	Χ	Ψ	Ω	Α	Β	Γ	Δ	Ε	Ζ	Η	Θ	Ι	Κ	Λ	Μ	Ν
Ο	Ο	Π	Ρ	Σ	Τ	Υ	Φ	Χ	Ψ	Ω	Α	Β	Γ	Δ	Ε	Ζ	Η	Θ	Ι	Κ	Λ	Μ	Ν	Ξ
Π	Π	Ρ	Σ	Τ	Υ	Φ	Χ	Ψ	Ω	Α	Β	Γ	Δ	Ε	Ζ	Η	Θ	Ι	Κ	Λ	Μ	Ν	Ξ	Ο
Ρ	Ρ	Σ	Τ	Υ	Φ	Χ	Ψ	Ω	Α	Β	Γ	Δ	Ε	Ζ	Η	Θ	Ι	Κ	Λ	Μ	Ν	Ξ	Ο	Π
Σ	Σ	Τ	Υ	Φ	Χ	Ψ	Ω	Α	Β	Γ	Δ	Ε	Ζ	Η	Θ	Ι	Κ	Λ	Μ	Ν	Ξ	Ο	Π	Ρ
Τ	Τ	Υ	Φ	Χ	Ψ	Ω	Α	Β	Γ	Δ	Ε	Ζ	Η	Θ	Ι	Κ	Λ	Μ	Ν	Ξ	Ο	Π	Ρ	Σ
Υ	Υ	Φ	Χ	Ψ	Ω	Α	Β	Γ	Δ	Ε	Ζ	Η	Θ	Ι	Κ	Λ	Μ	Ν	Ξ	Ο	Π	Ρ	Σ	Τ
Φ	Φ	Χ	Ψ	Ω	Α	Β	Γ	Δ	Ε	Ζ	Η	Θ	Ι	Κ	Λ	Μ	Ν	Ξ	Ο	Π	Ρ	Σ	Τ	Υ
Χ	Χ	Ψ	Ω	Α	Β	Γ	Δ	Ε	Ζ	Η	Θ	Ι	Κ	Λ	Μ	Ν	Ξ	Ο	Π	Ρ	Σ	Τ	Υ	Φ
Ψ	Ψ	Ω	Α	Β	Γ	Δ	Ε	Ζ	Η	Θ	Ι	Κ	Λ	Μ	Ν	Ξ	Ο	Π	Ρ	Σ	Τ	Υ	Φ	Χ
Ω	Ω	Α	Β	Γ	Δ	Ε	Ζ	Η	Θ	Ι	Κ	Λ	Μ	Ν	Ξ	Ο	Π	Ρ	Σ	Τ	Υ	Φ	Χ	Ψ

Εικόνα 3.6:Πίνακας Αντικατάστασης(Αλγόριθμος Vigenere)

Για παράδειγμα, ας υποθέσουμε ότι το κείμενο για κρυπτογράφηση είναι:

Κρυπτογραφία

Το άτομο που στέλνει το μήνυμα επιλέγει μια λέξη-κλειδί και την επαναλαμβάνει μέχρι να ταιριάζει με το μήκος του απλού κειμένου, για παράδειγμα, η (άτονη) λέξη "εγω":

εγωεγωεγωεγω

Κάθε στήλη περιέχει τον αλγόριθμο αντικατάστασης του Καίσαρα για ένα γράμμα της λέξης κλειδί. Παρά το γεγονός ότι υπάρχουν εικοσιτέσσερις στήλες θα χρησιμοποιήσουμε μόνο τις στήλες που έχουν σαν κεφαλίδα τα γράμματα της

λέξης κλειδί. Επομένως θα χρησιμοποιήσουμε μόνο τις τρεις στήλες **ε, γ, ω**. Για το πρώτο γράμμα του μηνύματος θα χρησιμοποιήσουμε τη στήλη του "ε". Για το δεύτερο γράμμα του μηνύματος θα χρησιμοποιήσουμε τη στήλη που αντιστοιχεί στο "γ" κοκ.

Κρυπτογραφία→ΞΣΤΥΦΞΗΤΩΑΛΩ

- Αλγόριθμος RSA

Ο αλγόριθμος RSA ανακαλύφθηκε το 1978 από μια ομάδα στο M.I.T. και είναι γνωστός με τα αρχικά των εφευρετών του (Rivest, Shamir, Adleman). Η μέθοδος αυτή έχει επιβιώσει από όλες της προσπάθειες σπασίματος εδώ και περισσότερο από ένα τέταρτο του αιώνα και θεωρείται πολύ ισχυρή. Το κύριο μειονέκτημά του είναι ότι απαιτεί κλειδιά με μήκος τουλάχιστον 1024 bit για ασφάλεια, γεγονός που τον καθιστά αρκετά αργό. Η μέθοδος RSA βασίζεται σε ορισμένες αρχές από την θεωρία αριθμών. Θα συνοψίσουμε τώρα τον τρόπο λειτουργίας της.

1. Επιλογή δύο μεγάλων πρώτων αριθμών, p και q
2. Υπολογισμός των n=p*q και z=(p-1)*(q-1)
3. Επιλογή ενός αριθμού που είναι αμοιβαία πρώτος με τον z, τον οποίο ονομάζουμε d.
4. Εντοπισμός του e ώστε e*d=1 mod z.

Για την εύρεση πρώτων αριθμών χρησιμοποιούνται πιθανολογικοί αλγόριθμοι. Συνηθισμένες επιλογές για το e είναι το 3, 7 και 216 + 1. Μικροί αριθμοί οδηγούν σε ταχύτερους υπολογισμούς αλλά και σε πιο αδύνατη ασφάλεια. Τα κλειδιά είναι τα εξής:

- δημόσιο: (n, e)
- ιδιωτικό: (n, d)

Μπορούμε τώρα να δημοσιεύσουμε το πρώτο κλειδί, δίνοντας έτσι τη δυνατότητα σε οποιονδήποτε να μας στείλει κρυπτογραφημένα μηνύματα που μόνο εμείς (χάρη στο ιδιωτικό κλειδί) μπορούμε να αποκρυπτογραφήσουμε.

Κρυπτογράφηση

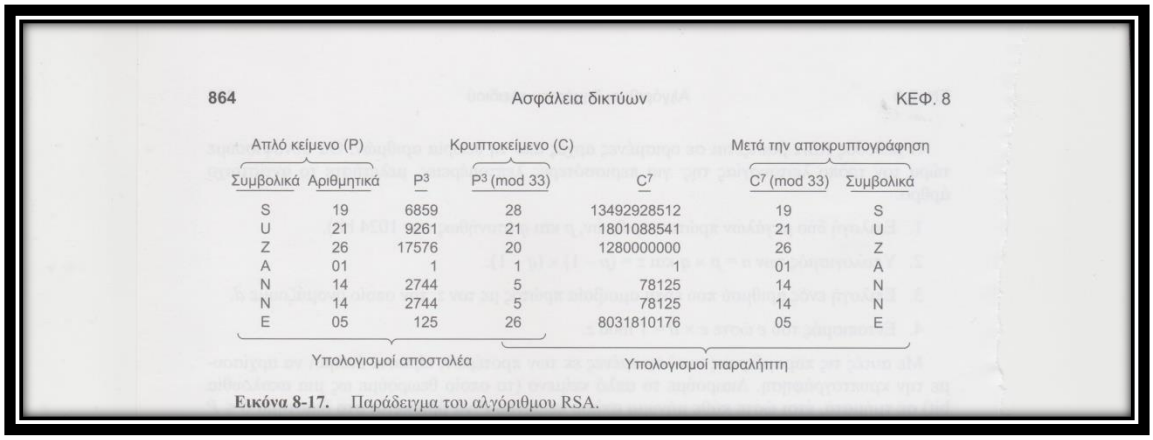
Το μήνυμα μπορεί να αντιπροσωπευθεί από έναν αριθμό m.Το κρυπτογραφημένο μήνυμα c υπολογίζεται με τον εξής τρόπο:

$$C=m_e \bmod n$$

Αποκρυπτογράφηση

Αφού ληφθεί ένα κρυπτογραφημένο μήνυμα c, για να διαβάσουμε το αρχικό μήνυμα προβαίνουμε στον ακόλουθο υπολογισμό:

Στην παρακάτω εικόνα φαίνεται ένα τετριμμένο παιδαγωγικό παράδειγμα σχετικά με τον τρόπο λειτουργίας του αλγορίθμου RSA. Για το παράδειγμα αυτό έχουμε επιλέξει p=3 και q=11, γεγονός που δίνει n=33 και z=20. Μια κατάλληλη τιμή για το d είναι το d=7 αφού το 7 και το 20 δεν έχουν κοινούς παράγοντες. Με τις επιλογές αυτές μπορούμε να υπολογίσουμε το e λύνοντας την εξίσωση $7e=1(\text{mod } 20)$, η οποία δίνει $e=3$.Το κρυπτοκείμενο c για ένα απλό κείμενο P δίνεται από τον τύπο $C=P3(\text{mod } 33)$. Το κρυπτοκείμενο αποκρυπτογραφείται από τον παραλήπτη με τον κανόνα $P=C7(\text{mod } 33)$.



864 Ασφάλεια δικτύων ΚΕΦ. 8

Απλό κείμενο (P)		Κρυπτοκείμενο (C)		Μετά την αποκρυπτογράφηση		
Συμβολικά	Αριθμητικά	P^3	P^3 (mod 33)	C^7	C^7 (mod 33)	Συμβολικά
S	19	6859	28	13492928512	19	S
U	21	9261	21	1801088541	21	U
Z	26	17576	20	1280000000	26	Z
A	01	1	1	1	01	A
N	14	2744	5	78125	14	N
N	14	2744	5	78125	14	N
E	05	125	26	8031810176	05	E

Υπολογισμοί αποστολέα — Υπολογισμοί παραλήπτη

Εικόνα 8-17. Παράδειγμα του αλγόριθμου RSA.

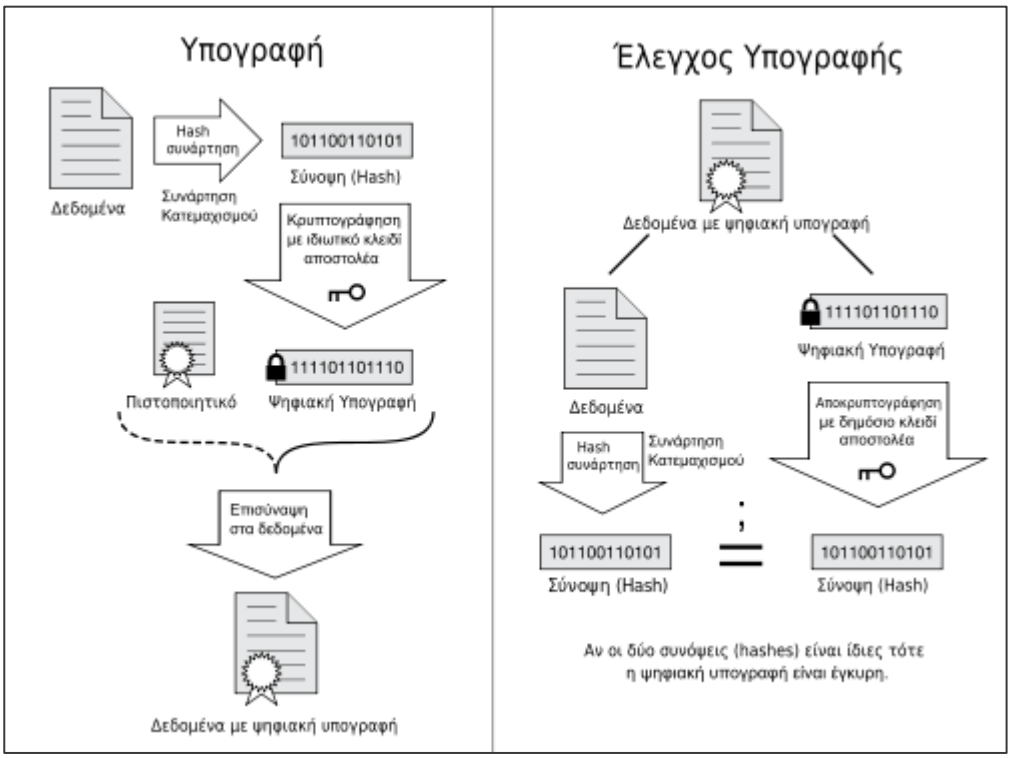
Εικόνα 3.7: Παράδειγμα του αλγορίθμου RSA

3.6 Ηλεκτρονικές Υπογραφές

Η ηλεκτρονική υπογραφή είναι για τον ηλεκτρονικό κόσμο το αντίστοιχο του διαβατηρίου για τον φυσικό κόσμο. Εκδίδεται από τον πάροχο Υπηρεσιών Πιστοποίησης (αρχή ψηφιακής πιστοποίησης) που εγγυάται για τα στοιχεία του κατόχου του, ακριβώς όπως η αρμόδια κρατική αρχή εγγυάται για την έκδοση του διαβατηρίου. Η κατοχή του ψηφιακού πιστοποιητικού διασφαλίζεται από την αποκλειστική κατοχή συγκεκριμένων ψηφιακών δεδομένων από το φυσικό πρόσωπο.

Οι ψηφιακές υπογραφές χρησιμοποιούν την κρυπτογραφία δημοσίου κλειδιού. Ο χρήστης διαθέτει δύο κλειδιά (το δημόσιο και το ιδιωτικό). Η σχέση των κλειδιών είναι τέτοια ώστε αν κάποιος γνωρίζει το ένα κλειδί να είναι πρακτικά αδύνατον να υπολογίσει το άλλο. Το ένα κλειδί χρησιμοποιείται για τη δημιουργία της υπογραφής και το άλλο για την επαλήθευσή της. Η διαφοροποίηση από την κρυπτογράφηση έγκειται στο ότι για τη δημιουργία της ηλεκτρονικής υπογραφής ο αποστολέας χρησιμοποιεί το ιδιωτικό του κλειδί και για την επαλήθευσή της ο παραλήπτης χρησιμοποιεί το δημόσιο κλειδί του αποστολέα. Στη διαδικασία της δημιουργίας και επαλήθευσης της υπογραφής εμπλέκεται και η έννοια της συνάρτησης κατακερματισμού. Με την εφαρμογή της συνάρτησης κατακερματισμού, από ένα μήνυμα ανεξαρτήτου του μεγέθους του, παράγεται η «σύνοψή του», η οποία είναι μία σειρά από bits συγκεκριμένου μεγέθους (π.χ. 128bits). Η σύνοψη του μηνύματος είναι μία ψηφιακή αναπαράσταση του μηνύματος και μοναδική για το μήνυμα και το αντιπροσωπεύει. Η συνάρτηση κατακερματισμού είναι μονόδρομη διότι από τη σύνοψη, που δημιουργεί. Η πιθανότητα δύο μηνύματα να έχουν την ίδια σύνοψη είναι εξαιρετικά μικρή. Αυτό σημαίνει ότι αν το μήνυμα του αποστολέα έχει κάποια συγκεκριμένη σύνοψη και το μήνυμα που λάβει ο παραλήπτης (χρησιμοποιώντας την ίδια συνάρτηση κατακερματισμού) παράγει διαφορετική σύνοψη, τότε το μήνυμα κατά τη μετάδοσή του έχει αλλοιωθεί (μη ακεραιότητα). Οποιαδήποτε αλλαγή σε ένα μήνυμα συνεπάγεται και τη δημιουργία διαφορετικής σύνοψης. Η ηλεκτρονική υπογραφή στην ουσία είναι η κρυπτογραφημένη με το ιδιωτικό κλειδί του αποστολέα σύνοψη. Δηλαδή, η ψηφιακή υπογραφή (σε αντίθεση με την ιδιόχειρη υπογραφή) είναι διαφορετική για κάθε μήνυμα. Μία ψηφιακή υπογραφή μπορεί να πλαστογραφηθεί εάν ο δικαιούχος του ιδιωτικού κλειδιού δεν το

έχει υπό τον πλήρη έλεγχό του (π.χ. απολέσει το μέσο στο οποίο έχει αποθηκευτεί το ιδιωτικό κλειδί).



Εικόνα 3.8: Διαδικασία ηλεκτρονικής υπογραφής

Secure Socket Layer- SSL

Θα έχετε παρατηρήσει ένα λουκέτο που εμφανίζεται στο κάτω μέρος της οθόνης του υπολογιστή σας, όταν το πρόγραμμα αναζήτησης βρίσκεται σε ασφαλές περιβάλλον. Πριν περάσετε σε αυτό το «ασφαλές περιβάλλον» (Secure Socket Layer - SSL), εμφανίζεται συνήθως ένα ή περισσότερα προειδοποιητικά μηνύματα από το πρόγραμμα αναζήτησης (browser). Ακόμα, θα προσέξατε ότι οι «ασφαλείς» σελίδες αρχίζουν από «https://» αντί από το σύνηθες «http://». Στο ασφαλές αυτό περιβάλλον, όλες οι πληροφορίες που διακινούνται από το πρόγραμμα αναζήτησης μέχρι το διακομιστή του ηλεκτρονικού καταστήματος είναι κρυπτογραφημένες. Υπάρχουν αρκετές εταιρείες που μπορεί να χρησιμοποιήσει ένας διακομιστής για να πετύχει την ασφαλή πρόσβαση. Θα

τη βρείτε σε αρκετούς τόπους e-banking στην Ελλάδα. Η πιστοποίηση της ταυτότητας του χρήστη και κάθε συναλλαγή του γίνονται με τη βοήθεια ενός μοναδικού ψηφιακού πιστοποιητικού (digital certificate). Αυτό το πιστοποιητικό αναγνωρίζει τον υπολογιστή του χρήστη και επιτρέπει τις συναλλαγές και τις μεταφορές χρημάτων μεταξύ λογαριασμών μόνο από τον συγκεκριμένο υπολογιστή. Τα πιστοποιητικά αυτά εξασφαλίζονται εγκαθιστώντας ένα πρόγραμμα από την αντίστοιχη εταιρεία πιστοποίησης. Οι οργανισμοί Visa και MasterCard σχεδίασαν και υιοθέτησαν το νέο πρότυπο 3D-Secure. Η υλοποίηση της Visa ονομάζεται Verified by Visa (VbV) και η αντίστοιχη της MasterCard λέγεται SecureCode. Με το 3D-Secure, κατά τη διάρκεια της πληρωμής και αμέσως μόλις ο χρήστης συμπληρώσει τα στοιχεία της κάρτας του, η τράπεζα (acquirer) (εφόσον έχει υλοποιήσει το πρότυπο) προσπαθεί να ζητήσει από την τράπεζα (issuer) να πιστοποιήσει την ταυτότητα του κατόχου της κάρτας. Αν η τράπεζα (issuer) έχει κι αυτή υλοποιήσει το 3D-Secure, ζητά από τον κάτοχο της κάρτας να εισάγει τον προσωπικό κωδικό που έχει επιλέξει για το σκοπό αυτό. Αυτό γίνεται σε ένα νέο αναδυόμενο παράθυρο της εφαρμογής πλοήγησης στο Internet, το οποίο παρουσιάζεται στον κάτοχο της κάρτας. Η τράπεζα (issuer) πιστοποιεί την ταυτότητα του κατόχου της κάρτας και απαντά αντίστοιχα στην τράπεζα (acquirer). Εννοείται ότι όλη η επικοινωνία γίνεται μέσω του αντίστοιχου οργανισμού (Visa/MasterCard) και με τη χρήση ειδικής τεχνολογίας που υλοποιεί το πρότυπο. Αν η τράπεζα (issuer) δεν έχει υλοποιήσει το 3D-Secure, η διαδικασία πιστοποίησης δεν προχωρά. Μετά την πιστοποίηση της ταυτότητας του κατόχου της κάρτας, η διαδικασία συνεχίζεται με τη λήψη έγκρισης για τη χρέωση της κάρτας, σύμφωνα με τον κλασικό τρόπο που περιγράφηκε παραπάνω. Το σημαντικό στοιχείο του 3D-Secure είναι ότι, είτε η τράπεζα (issuer) έχει υλοποιήσει το πρότυπο (οπότε μπορεί να πιστοποιήσει τον κάτοχο) είτε όχι, αν η τράπεζα (acquirer) προσπαθήσει να εφαρμόσει το πρότυπο, τότε η ευθύνη σε περίπτωση αμφισβήτησης της συναλλαγής (λόγω πλαστοπροσωπίας) μετατίθεται στην τράπεζα (issuer). Αυτή η τακτική αναμένεται να λειτουργήσει ως κίνητρο για την εφαρμογή του προτύπου, τόσο από τους acquirers (που απαλλάσσονται από αυτή την κατηγορία αμφισβητήσεων που είναι η συχνότερη), όσο και από τους issuers (που θα προσπαθήσουν να αποφύγουν την "τυφλή" ανάληψη της ευθύνης). Παράλληλα οι συναλλαγές με 3D-Secure δημιουργούν μικρότερη οικονομική επιβάρυνση στους acquirers, πράγμα που λειτουργεί ως επιπλέον κίνητρο για την εφαρμογή του

προτύπου. Το 3D-Secure έχει ήδη εφαρμοστεί σε πολλούς acquirers της Ευρώπης, καθώς και σε λιγότερους issuers, ενώ αναμένεται να εφαρμοστεί και στις ΗΠΑ.

ΚΕΦΑΛΑΙΟ 4°: Η Ελληνική πραγματικότητα

ΕΙΣΑΓΩΓΗ

Σε αυτό το κεφάλαιο καταγράφονται και παρουσιάζονται οι ελληνικές τράπεζες αλλά και οι υπηρεσίες E-banking της κάθε μιας.

Στην Ελλάδα σήμερα έχουν εδραιωθεί 5 μεγάλες τράπεζες ύστερα από συγχωνεύσεις αλλά και κλείσιμο πολλών τραπεζών οι οποίες είναι:

- Εθνική Τράπεζα
- Τράπεζα Πειραιώς
- Alpha Bank
- Eurobank Εργασίας
- Attica Bank

Τράπεζα	Συγχωνεύθηκε με	Εξαγοράστηκε από
Αγροτική		Τράπεζα Πειραιώς
Γενική Τράπεζα της Ελλάδος		Τράπεζα Πειραιώς
Δωρική Τράπεζα της Ελλάδος	Eurobank εργασίας	
Εγνατία Τράπεζα	Τράπεζα Πειραιώς	
Εμπορική Τράπεζα της Ελλάδος		Alpha Bank

Ιονική και Λαϊκή Τράπεζα		Alpha Bank
Marfin Egnatia Bank	Τράπεζα Πειραιώς	
Cyprus Popular Bank	Τράπεζα Πειραιώς	
Πανελλήνια Τράπεζα		Τράπεζα Πειραιώς
Proton Τράπεζα	Eurobank εργασίας	
Ταχυδρομικό Ταμιευτήριο Ελλάδος		Eurobank εργασίας
Probank	Εθνική Τράπεζα	
Millenium Bank		Τράπεζα Πειραιώς
Τράπεζα Χίου	Τράπεζα Πειραιώς	
Τράπεζα Κύπρου	Τράπεζα Πειραιώς	
Τράπεζα Μακεδονίας-Θράκης	Τράπεζα Πειραιώς	
T Bank		Alpha Bank
FBB Πρώτη Επιχειρηματική Τράπεζα		Εθνική Τράπεζα

Πίνακας 3:Συγχωνεύσεις και εξαγορές ελληνικών τραπεζών

Εν συνεχεία το e-banking παίζει σημαντικό ρόλο στην λειτουργία των Ελληνικών τραπεζών με νέες υπηρεσίες και προϊόντα. Οι πέντε μεγάλες Ελληνικές τράπεζες έχουν αναπτύξει τις ηλεκτρονικές εφαρμογές τους και στο μέλλον οι ψηφιακές συναλλαγές θα έχουν πρωταρχικό ρόλο στην καθημερινότητα των Ελλήνων πολιτών. Αναλυτικά η κάθε τράπεζα με το e-banking προσφέρει τις εξής δυνατότητες:

Εθνική Τράπεζα

ΕΘΝΙΚΗ ΤΡΑΠΕΖΑ

Η Εθνική Τράπεζα προσφέρει στους πελάτης 24 ώρες καθημερινά μέσω του Internet Banking τα εξής:

- Πληροφόρηση: για τους λογαριασμούς, τις πιστωτικές κάρτες ή το δάνειό σας
- Συναλλαγές: μεταφορές / εμβάσματα, πληρωμές Δημοσίου / Εταιρειών, χρηματιστηριακές συναλλαγές, πάγιες εντολές σε λογαριασμούς Εθνικής Τράπεζας κ.ά.
- Ενέργειες Διαχείρισης Προφίλ και Ασφάλειας, όπως αλλαγή Password, σύνδεση /αποσύνδεση / φιλικές ονομασίες λογαριασμών κ.ά.
- Εγγραφή σε Υπηρεσία Ειδοποιήσεων (ETE Alerts).
- Το Internet Banking επίσης προσφέρει άμεση κάλυψη των καθημερινών τραπεζικών υποχρεώσεων , προηγμένες και πρωτοποριακές μεθόδους διασφάλισης των συναλλαγών και ευελιξία στην εξυπηρέτησή των πελατών της όλο το 24ωρο.

Τράπεζα Πειραιώς

Με την υπηρεσία «*winbank web banking*» της τράπεζας Πειραιώς ο χρήστης μπορεί ανά πάσα στιγμή να εκτελέσει:

- Διαχείριση τραπεζικών προϊόντων (αλλαγή ορίων, τροποποίηση χαρακτηριστικών κ.λπ.)
- Μεταφορές
- Πληρωμές
- Εμβάσματα
- Χρηματιστηριακές συναλλαγές
- winbank alerts
- Αιτήσεις για νέα προϊόντα

Επιπλέον, με πρόσθετες υπηρεσίες της τράπεζας Πειραιώς κάθε χρήστης μπορεί να πραγματοποιήσει και τις παρακάτω υπηρεσίες:

- Λεφτά στο Λεπτό
- Διαχείριση Προπληρωμένης Κάρτας WEBUY
- Πολύ μεγαλύτερο εύρος συναλλαγών εξόφλησης λογαριασμών
- Συναλλαγές σε Διεθνή Χρηματιστήρια
- Ανανέωση χρόνου ομιλίας καρτοκινητού
- e-statement

ALPHA BANK

Με το «*Alpha e-Banking*» ο χρήστης θα μπορεί να:

- Εξοφλεί τα δάνεια ή τις κάρτες του αλλά και να πληρώνει και φορείς του Δημοσίου ή άλλους λογαριασμούς
- Μεταφορά ποσών σε λογαριασμούς Alpha Bank ή σε λογαριασμούς τρίτων
- Διαχειριστεί πάγιες εντολές
- Συλλέξει bonus πόντους από πληρωμές και αγορές
- Ενημερώνεται για τους λογαριασμούς ,τα δάνεια και τις κάρτες του οποιαδήποτε στιγμή
- Λαμβάνει ειδοποιήσεις μέσω email ή sms για εκκρεμείς συναλλαγές αλλά και διάφορα νέα προϊόντα
- Αποθηκεύει παλαιότερες κινήσεις που εκτελεί συχνά
- Ρυθμίζει τα όρια μεταφορών των συναλλαγών του.

Eurobank Εργασίας

Με την τράπεζα Eurobank, μέσω του e-Banking ο χρήστης μπορεί να:

- Ενημερώνεται διαδικτυακά για τους λογαριασμούς του, τις κάρτες και τα δάνεια του
- Να πραγματοποιεί εξόφληση των οφειλών ,της κάρτας ή του δανείου του
- Πραγματοποιεί πληρωμές σε λογαριασμούς δημοσίου αλλά και άλλους λογαριασμούς
- Να αγοράζει και να πουλά μετοχές σε πραγματικό χρόνο
- Λαμβάνει ειδοποιήσεις μέσω email ή sms για κινήσεις λογαριασμών και καρτών

Attica Bank

Τέλος με το e-banking της attica bank κάθε χρήστης έχει την δυνατότητα να:

- Πληροφορείται άμεσα για τους λογαριασμούς του, τις κινήσεις των καρτών και τα δάνεια του
- Πραγματοποιεί μεταφορές κεφαλαίων τους λογαριασμούς του αλλά και εμβάσματα προς τρίτους
- Πραγματοποιεί πληρωμές σε λογαριασμούς δημοσίου αλλά και άλλους λογαριασμούς
- Αλλάζει τα προσωπικά του στοιχεία (διεύθυνση κατοικίας , τηλέφωνο κλπ)
- Λαμβάνει ειδοποιήσεις μέσω email ή sms για κινήσεις λογαριασμών και καρτών
- Χορηγείται καρνέ επιταγών εφόσον το αιτηθεί

Όπως αποδεικνύεται οι πέντε μεγάλες Ελληνικές τράπεζες χρησιμοποιούν και διαφημίζουν το e-Banking ως το νέο μέσο τραπεζικών συναλλαγών και ενημερώνουν καθημερινά τους πολίτες με πληροφορίες αλλά και εγχειρίδια χρήσης για αυτό.

ΚΕΦΑΛΑΙΟ 5°: Βιβλιογραφία

5.1 Ενδεικτική Βιβλιογραφία

- Tanenbaum S.A , 2003 , *Δίκτυα Υπολογιστών ,* (Ξυλωμένος Γ. , μτφρ) , Αθήνα , Κλειδάριθμος.
- Κεντερλής Π. Δ. , 2009 , *Ανάπτυξη Διαδικτυακών Εφαρμογών ,Θεωρία και Πράξη ,* Αθήνα , Κεντερλής Π. Δ..
- Γιαννακόπουλος Π. Ηρ. , 2009 , *Πληροφορική και Κοινωνία , Αθήνα ,* Γιαννακόπουλος Π. Ηρ..
- Sedgewick R. , 2010 , Στεφανίδης Γ. (επιμ) , *Αλγόριθμοι σε C* , (Σταυρόπουλος Π. , Κωστάκης Δ. , μτφρ) , Αθήνα , Κλείδαριθμος.

5.2 Διαδικτυακές Πηγές

- Online Banking , http://www.investopedia.com/terms/o/onlinebanking.asp .
- Setting Up Internet Banking , https://docs.oracle.com/cd/E35909_01/crm91pbr1/eng/psbooks/cbtr/book.htm?File=cbtr/htm/cbtr04.htm .
- DEFINITION OF E-BANKING , http://sjecnotes.weebly.com/uploads/5/2/5/1/5251788/26494919-definition-of-e-banking.pdf .
- Ruth Sarreal , (2016) , HISTORY OF ONLINE BANKING: HOW INTERNET BANKING BECAME MAINSTREAM , https://www.gobankingrates.com/banking/history-online-banking/ .
- The Independent Financial Portal Financial Web , Online Banking - Advantages and Disadvantages , http://www.finweb.com/banking-credit/online-banking-advantages-and-disadvantages.html#axzz4SptzuLkJ .
- Eurostat Statistics Explained , (2015) , Στατιστικές για την κοινωνία της πληροφορίας - νοικοκυριά και άτομα , http://ec.europa.eu/eurostat/statistics-explained/index.php/Information_society_statistics_-_households_and_individuals/el .

- Areej M. A. , Madihah M.S., Bachok M. T. , Zul H. A. (2013) , An Efficient Trojan Horse Classification (ETC) , www.IJCSI.org , http://ijcsi.org/papers/IJCSI-10-2-3-96-104.pdf .
- Software Engineering Institute , (2000) , http://www.cert.org/historical/advisories/CA-1998-01.cfm .
- Evgeny Milanov , (2009) , The RSA Algorithm , https://sites.math.washington.edu/~morrow/336_09/papers/Yevgeny.pdf .
- The Vigenere Cipher -- A Polyalphabetic Cipher , http://user.it.uu.se/~olgag/Cryptology/vigenere.html .

5.3 Διαδικτυακές πηγές - Εικόνες

- Antoniou S. , (2009) , The PING of Death and Other DoS Network Attacks , (Εικ.) , https://www.pluralsight.com/blog/it-ops/ping-of-death-and-dos-attacks .
- InfoSec Resources , Dangerous DDoS (Distributed Denial of Service) on the rise , (Εικ.) , http://resources.infosecinstitute.com/dangerous-ddos-distributed-denial-of-service-on-the-rise/#gref .
- Sfetcu N. , (2015) , Fork bomb , (Εικ.) , https://www.setthings.com/en/fork-bomb/.

- Μάγκλαρης Β. , ΔΙΑΧΕΙΡΙΣΗ ΔΙΚΤΥΩΝ ΔΙΑΧΕΙΡΙΣΗ ΑΣΦΑΛΕΙΑΣ ΙΙ ΔΙΑΣΤΑΣΕΙΣ ΛΕΙΤΟΥΡΓΙΑΣ ΤΗΛΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΔΙΚΤΥΩΝ – ΣΗΜΑΤΟΔΟΣΙΑ & ΕΥΦΥΗ ΔΙΚΤΥΑ , (Εικ.) , http://slideplayer.gr/slide/1940960/ .
- Eurostat Statistics Explained , (2015) , Στατιστικές για την κοινωνία της πληροφορίας - νοικοκυριά και άτομα , (Εικ.) , http://ec.europa.eu/eurostat/statistics-explained/index.php/Information_society_statistics_-_households_and_individuals/el .
- Eurostat, Η χρήση του διαδικτύου από τους Έλληνες , (2011) , (Εικ.) , https://techblog.gr/internet/observatory-eurostat-greece-internet-3997/ .

- Mathman , Κρυπτογράφηση - Vigenere's Cipher , (Εικ.) , http://www.mathman.gr/component/content/article/11-Genika/1224-cryptography-vigenere-cipher.html .
- Geek Wolke , What are DoS and DDoS attacks? (2017) , (Εικ.) , http://geekwolke.com/2017/01/27/what-are-dos-and-ddos-attacks/ .
- Setting Up Internet Banking , (Εικ.) https://docs.oracle.com/cd/E35909_01/crm91pbr1/eng/psbooks/cbtr/book.htm?File=cbtr/htm/cbtr04.htm .
- WILSON T. V. , HOW STUFFWORKS TECH , How Phishing Works , (Εικ.) , http://computer.howstuffworks.com/phishing1.htm .