Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακό Πρόγραμμα Σπουδών *Ασφάλεια Υπολογιστών και Δικτύων*

Μεταπτυχιακή Διατριβή

Προστασία προσωπικών δεδομένων στο Διαδίκτυο: αποτίμηση της αξιοποίησης του πρωτοκόλλου TLS

Δημήτριος Κοντογεώργης

Επιβλέπων Καθηγητής
Δρ. Κωνσταντίνος Λιμνιώτης

Μάιος 2018

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακό Πρόγραμμα Σπουδών *Ασφάλεια Υπολογιστών και Δικτύων*

Μεταπτυχιακή Διατριβή

Προστασία προσωπικών δεδομένων στο Διαδίκτυο: αποτίμηση της αξιοποίησης του πρωτοκόλλου TLS

Δημήτριος Κοντογεώργης

Επιβλέπων Καθηγητής
Δρ. Κωνσταντίνος Λιμνιώτης

Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε προς μερική εκπλήρωση των απαιτήσεων για απόκτηση μεταπτυχιακού τίτλου σπουδών στην Ασφάλεια Υπολογιστών και Δικτύων από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών του Ανοικτού Πανεπιστημίου Κύπρου

Μάιος 2018

Περίληψη

Οι χρήστες του Διαδικτύου στις μέρες μας αυξάνονται με ταχείς ρυθμούς, καθώς αποτελεί ένα πεδίο δραστηριότητας με πολλαπλές χρήσεις. Η πλοήγηση όμως σε αυτό εγκυμονεί πολλαπλούς κινδύνους, καθώς οι χρήστες συχνά εισάγουν στις ιστοσελίδες προσωπικές πληροφορίες καθώς και οικονομικά στοιχεία. Για το λόγο αυτό η ασφάλεια που παρέχουν οι ιστοσελίδες, είναι μείζονος σημασία για την προστασία των δεδομένων των χρηστών. Στο πλαίσιο αυτό, το πρωτόκολλο SSL/TLS αποτελεί ένα κατά κάποιο τρόπο «πρότυπο» για την ασφαλή πλοήγηση. Ωστόσο, παρά το γεγονός ότι συνεχώς ανακαλύπτονται «αδύναμα» σημεία είτε σε παλαιότερες εκδόσεις του πρωτοκόλλου είτε σε συγκεκριμένες υλοποιήσεις αυτού, πολλοί ιστότοποι εξακολουθούν να παρέχουν τις ευπαθείς αυτές υλοποιήσεις.

Στόχος την παρούσας μεταπτυχιακής διατριβής είναι η καταγραφή και η αξιολόγηση της υλοποίησης των πρωτόκολλων SSL/TLS που εφαρμόζουν οι ελληνικές ιστοσελίδες οι οποίες εμφανίζουν υψηλή επισκεψιμότητα. Για τον λόγο αυτό αξιολογήθηκαν 241 συνολικά ιστοσελίδες με χρήση δύο διαφορετικών και διεθνώς αναγνωρισμένων εργαλείων. Παράλληλα, μέσω διαδικτυακού ερωτηματολογίου, εξετάστηκε το επίπεδο της γνώσης που έχουν οι χρήστες όσον αφορά το τι σημαίνει το TLS και πώς εξετάζουν οι ίδιοι την ασφάλεια των ιστοσελίδων. Οι 773 απαντήσεις που συλλέχθηκαν, αφού επεξεργάστηκαν, έγινε στατιστική ανάλυσή τους για την εξαγωγή των συμπερασμάτων. Από τα αποτελέσματα τις διατριβής προκύπτει το συμπέρασμα ότι οι ελληνικές ιστοσελίδες βρίσκονται σε αρκετά καλή κατάσταση, ως προς την ασφάλεια που παρέχουν στους χρήστες αν και υπάρχουν σημαντικά περιθώρια βελτίωσης, ενώ το μεγαλύτερο ποσοστό είναι έτοιμο για την μετάβαση στην καινούργια έκδοση TLS 1.3. Ωστόσο σε ένα σημαντικό ποσοστό παρατηρείται η ύπαρξη γνωστών αδυναμιών αλλά και η υποστήριξη ξεπερασμένων εκδόσεων του SSL/TLS. Η μελέτη κατέδειξε επίσης ορισμένα κενά ως προς τις γνώσεις των χρηστών και τις πρακτικές που ακολουθούν αναφορικά με την ασφάλεια των ιστοτόπων. Από τα αποτελέσματα καταδεικνύεται ότι μόνο 1 στους 3 γνωρίζει την οικογένεια πρωτοκόλλων SSL/TLS ενώ 4 στους 10 δεν γνωρίζουν την διαφορά http και https. Γενικά, οι ερωτηθέντες εμπιστεύονται τις ιστοσελίδες των τραπεζών, των e-shop και των δημόσιων φορέων στο ότι λαμβάνουν όλα τα απαραίτητα μέτρα για την ασφάλεια, ενώ είναι επιφυλακτικοί με τα κοινωνικά δίκτυα και τους ειδησεογραφικούς ιστοτόπους.

Summary

Internet users nowadays are growing rapidly as they are a field of activity with multiple uses. However, navigation in this system poses multiple risks as users often enter personal and financial information on the websites. For this reason, the security provided by the websites is major importance for the protection of user data. In this context, the SSL / TLS protocol is somewhat "standard" for safe navigation. However, despite the fact that weak points and vulnerabilities are constantly discovered either in earlier versions of the protocol or in specific implementations of the protocol, many sites still provide these vulnerable implementations.

The aim of this dissertation is to record and evaluate the implementation of SSL / TLS protocols implemented by Greek websites that display high traffic. For this reason, 241 sites were evaluated using two different and internationally recognized tools. At the same time, through an online questionnaire, the user's level of knowledge about what TLS means and how they are looking at the security of the web pages themselves has been examined. The 773 responses gathered, after being processed, became their statistical analysis to draw conclusions. From the results of the dissertation it is concluded that the Greek websites are in a good state of the art with regard to the security they provide to the users, although there is considerable room for improvement, while the majority is ready for the transition to the new version of TLS 1.3. However, there is a significant percentage of known weaknesses as well as support for outdated SSL / TLS versions. The study also highlighted some gaps in users' knowledge and practices regarding website security. The results show that only 1 in 3 knows the SSL / TLS protocols family while 4 out of 10 are unaware of the difference between http and https. In general, respondents trust the websites of banks, e-shops and public bodies to take all necessary security measures while being skeptical about social networks and news sites.

Ευχαριστίες

Σε σχέση με τη μεταπτυχιακή διατριβή, θα ήθελα να ευχαριστήσω τον επιβλέποντα Καθηγητή μου Δρ. Κωνσταντίνο Λιμνιώτη. Τον ευχαριστώ θερμά για τη βοήθεια του, την υπομονή που έδειξε μέχρι να ολοκληρώσω τη μελέτη αυτή εν μέσω πολλαπλών παράλληλων υποχρεώσεων και κυρίως για την ευκαιρία που μου έδωσε να ασχοληθώ σε βάθος με ένα θέμα τόσο φλέγον για την ασφάλεια του διαδικτύου που όχι μόνο αφορά άμεσα τη δουλειά μου, αλλά έχει και σημαντικές κοινωνικές προεκτάσεις. Επιπλέον θα ήθελα να ευχαριστήσω την σύζυγο μου Ελίνα Γκάνα, τον γιό μου Κωνσταντίνο και τα νεογέννητα δίδυμα από τους οποίους δανείστηκα πολύτιμο χρόνο και που πάντα με στηρίζουν.

Περιεχόμενα

Περιεχόμενα 7
Κεφάλαιο 1 Εισαγωγή 10
Κεφάλαιο 2 Βιβλιογραφική ανασκόπηση 13
2.1 Είδη κρυπτογραφίας 13
2.1.1 Συμμετρική κρυπτογραφία 13
2.1.2 Ασύμμετρη κρυπτογραφία 15
2.1.3 Κρυπτογραφικά Εργαλεία 15
2.2 Ιστορική αναδρομή του SSL/TLS 24
2.2.1 Secure Network Programming API 25
2.2.2 SSL 1.0, 2.0 & 3.0 26
2.2.3 TLS 1.0 (SSL 3.1) 27
2.2.4 TLS 1.1 (SSL 3.2) 28
2.2.5 TLS 1.2 (SSL 3.3) 28
2.2.6 TLS 1.3 29
2.3 Δομή του πρωτοκόλλου 32
2.4 Χειραψία TLS 33
2.4.1 Client hello 34
2.4.2 Server hello 35
2.4.3 Server hello done 36
2.4.4 Client Key Exchange 36
2.4.5 Server receives the Pre-Master Secret 37
2.4.6 Client sends "Change cipher spec 37
2.4.7 Connection established 37
2.5 Εφαρμογές 38
2.6 Ευπάθειες-Συμβάντα 39
2.6.1 2001 40
2.6.2 2008 41
2.6.3 2009 42
2.6.4 2010 43
2.6.5 2011 43
2.6.6 2012 44
2.6.7 2013 45
2.6.8 2014 47

2.6.9 2015 ... 48
2.6.10 2016 ... 50
2.6.11 2017 ... 51
2.6.12 2018 ... 52
2.7 Ευρωπαϊκός Κανονισμός για την Προστασία Γενικών Δεδομένων (GDPR) ... 52
Κεφάλαιο 3 Ανάλυση επιπέδου ασφάλειας Ιστοτόπων ... 54
3.1 Εισαγωγή ... 54
3.2 Μεθοδολογία ... 54
3.2.1 Εργαλείο A (SSL Labs) ... 55
3.2.2 Εργαλείο B (High-Tech Bridge) ... 58
3.2.3 Πληροφορίες που καταγράφηκαν ... 60
3.3 Κατηγορίες ... 62
3.3.1 E-Shop ... 63
3.3.2 Εταιρείες ... 66
3.3.3 Ενημερωτικά ... 69
3.3.4 Τηλεπικοινωνίες ... 72
3.3.5 Εκπαίδευση ... 75
3.3.6 Οικονομικές Υπηρεσίες ... 78
3.3.7 Δημόσιοι Οργανισμοί ... 81
3.3.8 Συνολικά ... 84
3.4 Συμπεράσματα ... 87
Κεφάλαιο 4 Ερωτηματολόγιο ... 91
4.1 Εισαγωγή ... 91
4.2 Σκοπός μελέτης ... 92
4.3 Μεθοδολογία ... 92
4.3.1 Ερευνητικό εργαλείο συλλογής δεδομένων ... 92
4.3.2 Εγκυρότητα και αξιοπιστία της έρευνας ... 94
4.3.3 Ανάλυση δεδομένων ... 94
4.4 Ερωτηματολόγιο ... 99
4.4.1 Ενότητα Α: Δημογραφικά στοιχεία ... 99
4.4.2 Ενότητα Β: Πληροφορίες σχετικά με την χρήση διαδικτύου ... 100
4.4.3 Ενότητα Γ: Ευαισθητοποίηση σχετικά με την ασφαλή πλοήγηση ... 102
4.4.4 Ενότητα Δ: Απαιτήσεις χρηστών κατά την πλοήγηση ... 104
4.4.5 Ενότητα Ε: Γνώσεις σε θέματα ασφαλούς πλοήγησης ... 105
4.4.6 Ενότητα ΣΤ: Συμπεριφορά χρηστών κατά την πλοήγηση ... 107

4.5 Αποτελέσματα και συζήτηση 108
4.5.1 Ενότητα Α: Δημογραφικά στοιχεία 108
4.5.2 Ενότητα Β: Πληροφορίες σχετικά με την χρήση διαδικτύου 111
4.5.3 Εννοιολογική κατασκευή Α: «Γνώσεις σε θέματα ασφαλούς πλοήγησης» 120
4.5.4 Εννοιολογική κατασκευή Β: «Ευαισθητοποίηση/ πεποιθήσεις σχετικά με την ασφαλή πλοήγηση» 123
4.5.5 Εννοιολογική κατασκευή Γ: «Απαιτήσεις χρηστών κατά την πλοήγηση» 125
4.5.6 Εννοιολογική κατασκευή Δ: «Συμπεριφορά χρηστών κατά την πλοήγηση» 127
4.5.7 Συγκρίσεις μεταξύ εννοιολογικών κατασκευών 128
4.5.8 Συμπεράσματα 130
Κεφάλαιο 5 Επίλογος 133
Βιβλιογραφία 1
Παράρτημα Α 1
Παράρτημα Β 1
Παράρτημα Γ 1
Παράρτημα Δ 1

Κεφάλαιο 1

Εισαγωγή

Το Διαδίκτυο αποτελεί, στις μέρες μας, αδιαμφισβήτητα ένα καθημερινό και βασικό εργαλείο στη ζωή του σύγχρονου ανθρώπου. Κυριότερες δραστηριότητες που πραγματοποιούνται δια μέσου αυτού είναι η αναζήτηση πληροφορίας και γνώσης, η επικοινωνία μεταξύ των ατόμων, οι αγορές μέσω διαδικτύου, αλλά και διάφοροι τρόποι ψυχαγωγίας. Γίνεται, συνεπώς, αντιληπτό ότι οι δυνατότητες που προσφέρει το Διαδίκτυο είναι τεράστιες. Αυτό το καθιστά ένα μέσο αρκετά ελκυστικό, διότι με χαμηλό κόστος είναι δυνατό κανείς να εμπλακεί σε πλήθος δραστηριοτήτων.

Από την άλλη μεριά, όμως, ανακύπτει έντονα το θέμα του αν υπάρχει επαρκής μέριμνα σε ότι αφορά τα ζητήματα της ασφάλειας των χρηστών, οι οποίοι πλοηγούνται στο Διαδίκτυο. Ένας υπολογιστής, που είναι συνδεδεμένος στο Διαδίκτυο, είναι πιθανό, να εκτίθεται σε αρκετούς κινδύνους, οι οποίοι σχετίζονται άμεσα με θέματα, όπως είναι η δέσμευση των πόρων του συστήματός του, η εγκατάσταση ιομορφικού λογισμικού κλπ. και τελικά μπορεί να αποβούν βλαβεροί για το υπολογιστικό σύστημα. Επίσης, τα τελευταία χρόνια εντείνεται όλο και περισσότερο το φαινόμενο της παραπλάνησης, όπου οι χρήστες με διάφορους τρόπους (π.χ. με παραπλανητικά ηλεκτρονικά μηνύματα, με εξαπάτηση μέσω κοινωνικών δικτύων κτλ.) παρέχουν τα προσωπικά τους δεδομένα σε άγνωστους, θεωρώντας ότι «συνομιλούν» αξιόπιστα (για παράδειγμα, μπορεί να εισάγουν τα δεδομένα τους σε μία μη γνήσια ιστοσελίδα άγνωστης προέλευσης, η οποία όμως μιμείται την αυθεντική).

Το TLS (Transport Layer Security) πρωτόκολλο, καθώς και ο προκάτοχος αυτού, το πρωτόκολλο SSL (Secure Sockets Layer), λειτουργούν πριν το TCP/IP και μετά τις εφαρμογές υψηλού επιπέδου, όπως είναι για παράδειγμα το HTTP (HyperText Transfer Protocol) (προβολή ιστοσελίδων), το File Transfer Protocol (FTP) (μεταφορά αρχείων) και το Internet Message Access Protocol (IMAP) (email). Δηλαδή, ανάμεσα στο 4ο (επίπεδο μεταφοράς) και στο 7ο (επίπεδο εφαρμογών) του μοντέλου αναφοράς OSI. Συνεπώς, βασικός ρόλος του SSL πρωτοκόλλου είναι η λήψη πληροφοριών από τις

εφαρμογές υψηλότερων επιπέδων, ώστε αυτές να κρυπτογραφηθούν και στη συνέχεια, η μετάδοσή τους στο διαδίκτυο προς τον ηλεκτρονικό υπολογιστή που έθεσε το αίτημα. Από την άλλη μεριά, το TLS εγγυάται ότι κατά την επικοινωνία εξυπηρετητή - πελάτη (Server - Client) μέσω του διαδικτύου δεν πρόκειται να μεσολαβήσει κάποιος άλλος χρήστης με σκοπό να υποκλέψει το περιεχόμενο της επικοινωνίας. Στην πραγματικότητα, δηλαδή τα δύο πρωτόκολλα έχουν τον ίδιο βασικό στόχο, απλά το SSL πρωτόκολλο αντικαταστάθηκε από το TLS, διότι οι αυξανόμενες ανάγκες στον τομέα της πληροφορικής οδήγησαν τα συστήματα σε πιο εξελιγμένες μορφής διατήρησης των συστημάτων με αποτέλεσμα να είναι απαραίτητος ο εκσυγχρονισμός του δικτύου για να επιτυγχάνεται η όσο το δυνατό μεγαλύτερη ασφάλεια για τον εκάστοτε χρήστη. Συνεπώς, το TLS είναι ένα πρωτόκολλο που έχει καθιερωθεί για την ασφαλή πλοήγηση στο Διαδίκτυο, παρέχοντας εμπιστευτικότητα και ακεραιότητα στα δεδομένα που μεταδίδονται (δηλαδή κανείς τρίτος δεν μπορεί να τα διαβάσει, ούτε όμως και να τα τροποποιήσει χωρίς αυτό να γίνει αντιληπτό στον παραλήπτη), αλλά και η αυθεντικοποίηση των χρηστών (δηλαδή ο χρήστης είναι σίγουρος ότι έχει μεταβεί στη σωστή έγκυρη ιστοσελίδα).

Ωστόσο, πολλά προβλήματα μένουν ακόμα ανοιχτά. Συγκεκριμένα:

1) Υπάρχουν γνωστές ευπάθειες σε συγκεκριμένες εκδόσεις και υλοποιήσεις των πρωτοκόλλων SSL/TLS, όπου δυστυχώς πολλοί ιστότοποι εξακολουθούν να τις υποστηρίζουν, παρέχοντας έτσι πολλές φορές μία μάλλον «επίφαση» ασφάλειας και όχι πραγματική ασφάλεια.
2) Η αναγνώριση μίας ασφαλούς σύνδεσης με ιστοσελίδα μέσω του πρωτοκόλλου TLS επαφίεται σε μεγάλο βαθμό στο χρήστη, δηλαδή στην ικανότητά του εξετάζοντας κατάλληλο το λογισμικό πλοήγησής του να αναγνωρίζει μία TLS σύνδεση. Δυστυχώς, πολλοί χρήστες δεν έχουν τις βασικές έστω γνώσεις αναγνώρισης των ιστοσελίδων που δεν παρέχουν ασφάλεια και, άρα, η σύνδεση σε αυτές θέτει σε κίνδυνο τα προσωπικά τους δεδομένα.

Η μεταπτυχιακή διατριβή αυτή εκπονήθηκε ορμώμενη από την επιθυμία να διερευνηθεί η κατάσταση σχετική με την ασφάλεια που επικρατεί στις δημοφιλέστερες ελληνικές ιστοσελίδες και παράλληλα να καταγραφούν βασικά στοιχεία σχετικά με τις γνώσεις, τις απαιτήσεις και την συμπεριφορά των χρηστών κατά την πλοήγηση τους στο διαδίκτυο. Ειδικότερα, τα ερευνητικά ερωτήματα που εξετάστηκαν είναι τα εξής:

1) Τι επιπέδου ασφάλεια, αναφορικά με τις υλοποιήσεις του TLS, παρέχουν οι πλέον δημοφιλείς ιστοσελίδες στην Ελλάδα,
2) Σε τι βαθμό οι χρήστες μπορούν και αντιλαμβάνονται πότε μία ιστοσελίδα είναι ασφαλής και πότε όχι.

Η μεταπτυχιακή διατριβή χωρίζεται σε 4 κεφάλαια. Στο κεφάλαιο 2 γίνεται η ανασκόπηση της βιβλιογραφίας εστιάζοντας σε μια σύντομη εισαγωγή στην κρυπτογραφία, μια ιστορική αναδρομή των πρωτοκόλλων SSL/TLS καθώς και παρουσίαση των σημαντικότερων ευπαθειών και συμβάντων. Η αξιολόγηση των πιο δημοφιλών ιστοτόπων παρουσιάζεται στο κεφάλαιο 3, με αναλυτική περιγραφή της μεθοδολογίας και των ευρημάτων της έρευνας. Στο κεφάλαιο 4 καταγράφεται η διαδικασία με την οποία δημιουργήθηκε το ερωτηματολόγιο για τους χρήστες, γίνεται περιγραφή των βασικών αποτελεσμάτων και αποτιμώνται τα ευρήματα της έρευνας. Τέλος, τα συνολικά συμπεράσματα της διατριβής συνοψίζονται στο κεφάλαιο 5.

Κεφάλαιο 2

Βιβλιογραφική ανασκόπηση

2.1 Είδη κρυπτογραφίας

Κρυπτογραφία (cryptography) είναι η μελέτη μαθηματικών τεχνικών με σκοπό την εξασφάλιση της ασφάλειας (εμπιστευτικότητα, ακεραιότητα, αυθεντικότητα) των δεδομένων. Κρυπτανάλυση (cryptanalysis) είναι η μελέτη μαθηματικών τεχνικών για την προσβολή κρυπτογραφικών τεχνικών ή υπηρεσιών ασφάλειας και κρυπτολογία (cryptology) είναι ο συνδυασμός της κρυπτογραφίας και κρυπτανάλυσης σε ένα ενιαίο επιστημονικό κλάδο. Εφαρμογή της κρυπτογραφίας είναι η κρυπτογράφηση. Κρυπτογράφηση είναι ο μετασχηματισμός δεδομένων σε μορφή που να είναι αδύνατον να διαβαστεί (που ονομάζεται κρυπτοκείμενο ή κρυπτογράφημα) χωρίς τη γνώση της σωστής ακολουθίας bit. Η ακολουθία bit καλείται "κλειδί" και χρησιμοποιείται σε συνδυασμό με κατάλληλο αλγόριθμο-συνάρτηση. Η αντίστροφη διαδικασία είναι η αποκρυπτογράφηση και απαιτεί γνώση του κλειδιού. Σκοπός της κρυπτογράφησης είναι να εξασφαλίσει το απόρρητο των δεδομένων κρατώντας τα κρυφά από όλους όσους έχουν πρόσβαση σε αυτά. Η κρυπτογράφηση και η αποκρυπτογράφηση απαιτούν τη χρήση κάποιας μυστικής πληροφορίας, το κλειδί. Για μερικούς μηχανισμούς χρησιμοποιείται το ίδιο κλειδί και για την κρυπτογράφηση και για την αποκρυπτογράφηση, για άλλους τα κλειδιά που χρησιμοποιούνται διαφέρουν [1,2].

2.1.1 Συμμετρική κρυπτογραφία

Στην περίπτωση των συμμετρικών αλγορίθμων ο πομπός και ο δέκτης χρησιμοποιούν το ίδιο κλειδί για κρυπτογράφηση και αποκρυπτογράφηση. Υλοποιούνται τόσο με υλικό όσο και με λογισμικό. Αναφέρονται και ως αλγόριθμοι μοναδικού κλειδιού ή μυστικού κλειδιού ή συμβατικής κρυπτογραφίας.

Η συμμετρική κρυπτογραφία εγγυάται την εμπιστευτικότητα (confidentiality) των δεδομένων αφού κρυπτογραφεί το μήνυμα με το μυστικό κλειδί. Το μήνυμα που παράγεται αποκρυπτογραφείται από τον παραλήπτη με τη βοήθεια του ίδιου κλειδιού, το οποίο πρέπει να μείνει μυστικό μεταξύ των δύο.

Η ασφάλειά τους βασίζεται στην μυστικότητα του κλειδιού. Τα συμμετρικά κρυπτοσυστήματα προϋποθέτουν την ανταλλαγή του κλειδιού μέσα από ένα ασφαλές κανάλι επικοινωνίας ή μέσα από τη φυσική παρουσία των προσώπων. Αυτό το χαρακτηριστικό καθιστά δύσκολη την επικοινωνία μεταξύ απομακρυσμένων ατόμων.

Για την ασφαλή χρήση της συμβατικής κρυπτογραφίας πρέπει να πληρούνται οι ακόλουθες προϋποθέσεις [1,3]:

- Απαιτείται η ύπαρξη ενός ισχυρού (strong) αλγορίθμου κρυπτογράφησης. Ως ελάχιστη απαίτηση αναφέρεται η ύπαρξη αλγορίθμου για τον οποίο ο επιτιθέμενος πρέπει να είναι αδύνατο να κρυπταναλύσει το κρυπτογράφημα ή να ανακαλύψει το κλειδί, ακόμη και αν κατέχει κάποια κρυπτογραφήματα μαζί με τα αντίστοιχα αρχικά μηνύματα, από τα οποία παράχθηκε καθένα από αυτά τα κρυπτογραφήματα.
- Ο πομπός και ο δέκτης πρέπει να έχουν παραλάβει τα αντίγραφα του μυστικού κλειδιού με ασφαλή τρόπο και να διαφυλάσσουν αυτό το μυστικό κλειδί σε ασφαλές μέρος. Εάν κάποιος γνωρίζει τον αλγόριθμο και ανακαλύψει το κλειδί, τότε όλη η επικοινωνία που χρησιμοποιεί αυτό το κλειδί είναι αναγνώσιμη, συνεπώς παραβιάζεται η εμπιστευτικότητα.

Σημειώνεται ότι αδύναμο κρίκο στην ασφάλεια της συμβατικής κρυπτογραφίας αποτελεί μόνον η μυστικότητα του κλειδιού και όχι η μυστικότητα του αλγορίθμου που χρησιμοποιείται. Αυτός θεωρείται δεδομένος, εάν υποτεθεί, ότι για τον επιλεγέντα αλγόριθμο ισχύει η προφανής σχεδιαστική απαίτηση να είναι αδύνατο να αποκρυπτογραφηθεί ένα μήνυμα μόνο με γνώση του κρυπτογραφήματος και του αλγορίθμου κρυπτογράφησης. Συνεπώς, δε χρειάζεται να παραμένει μυστικός ο αλγόριθμος, αλλά μόνο το μυστικό κλειδί. Το χαρακτηριστικό αυτό γνώρισμα της συμβατικής κρυπτογραφίας την καθιστά κατάλληλη για ευρεία χρήση. Το γεγονός ότι δε χρειάζεται να παραμένει μυστικός ο αλγόριθμος επιτρέπει στους κατασκευαστές να αναπτύσσουν χαμηλού κόστους υλοποιήσεις, τόσο σε λογισμικό όσο και σε υλικό, για εφαρμογές κρυπτογράφησης δεδομένων.

Οι κατηγορίες των συμμετρικών αλγορίθμων περιλαμβάνουν:

2.1.2 Ασύμμετρη κρυπτογραφία

Στα μέσα της δεκαετίας του ‘70 οι Whitfield Diffie και Martin Hellman [4] πρότειναν μια νέα τεχνική για τον περιορισμό των προβλημάτων της συμμετρικής κρυπτογραφίας. Η τεχνική αυτή, γνωστή ως κρυπτογραφία δημοσίου κλειδιού ή ασύμμετρη κρυπτογραφία, βασίζεται στην ύπαρξη ενός ζεύγους κλειδιών (key pair). Σε αυτό το ζεύγος, τα κλειδιά, αν και σχετίζονται μεταξύ τους με κάποια μαθηματική σχέση, είναι επαρκώς διαφορετικά έτσι ώστε η γνώση του ενός να μην επιτρέπει την παραγωγή ή τον υπολογισμό του άλλου. Αυτό σημαίνει ότι το ένα από τα κλειδιά μπορεί να είναι δημόσια γνωστό και διαθέσιμο. Το κλειδί αυτό ονομάζεται δημόσιο κλειδί (public key) και χρησιμοποιείται για την κρυπτογράφηση των δεδομένων. Το δεύτερο κλειδί είναι απαραίτητο να μένει ιδιωτικό, γι’ αυτό και ονομάζεται ιδιωτικό κλειδί (private key) και χρησιμοποιείται για την αποκρυπτογράφηση των δεδομένων.

Το ασύμμετρο κρυπτοσύστημα ή κρυπτοσύστημα δημοσίου κλειδιού (Κρυπτογράφηση Δημόσιου Κλειδιού) δημιουργήθηκε για να καλύψει την αδυναμία μεταφοράς κλειδιών που παρουσίαζαν τα συμμετρικά συστήματα. Χαρακτηριστικό του είναι ότι έχει δυο είδη κλειδιών ένα ιδιωτικό και ένα δημόσιο. Το δημόσιο είναι διαθέσιμο σε όλους ενώ το ιδιωτικό είναι μυστικό. Η βασική σχέση μεταξύ τους είναι: ότι κρυπτογραφεί το ένα, μπορεί να το αποκρυπτογραφήσει μόνο το άλλο. Οι δυνατότητες της ασύμμετρης κρυπτογραφίας οδήγησαν στη δημιουργία των ψηφιακών υπογραφών και ακολούθως στην ανάπτυξη της Υποδομής Δημόσιου Κλειδιού (Public Key Infrastructure) και στα Ψηφιακά πιστοποιητικά.

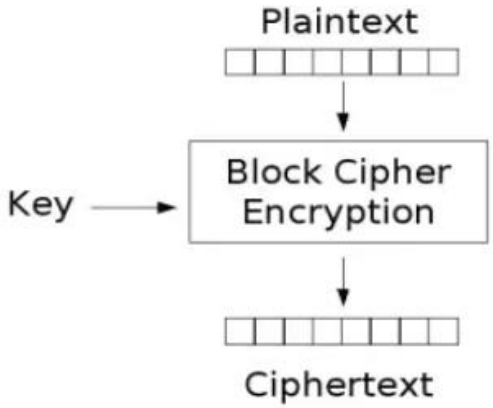
2.1.3 Κρυπτογραφικά Εργαλεία

Μέχρι τώρα αναφερθήκαμε στα δύο σημαντικότερα κρυπτοσυστήματα που ευρέως εφαρμόζονται σήμερα. Περιγράψαμε τις αρχές που τα διέπουν και το είδος των κλειδιών που χρησιμοποιούν (συμμετρικά ή ασύμμετρα). Στις ακόλουθες παραγράφους θα

ασχοληθούμε με τους μηχανισμούς με τους οποίους εφαρμόζεται η κρυπτογραφία γενικότερα.

2.1.3.1 Block Ciphers

Block cipher είναι ένας τύπος αλγόριθμου συμμετρικής κρυπτογράφησης που μετατρέπει ένα τμήμα (block) μη κρυπτογραφημένου καθορισμένου μήκους κειμένου (plaintext), σε block κρυπτογραφημένου του ίδιου μήκους κειμένου (ciphertext). Αυτός ο μετασχηματισμός πραγματοποιείται με την βοήθεια ενός μυστικού κλειδιού που χορηγείται από τον χρήστη. Η αποκρυπτογράφηση γίνεται με την εφαρμογή του αντίστροφου μετασχηματισμού στο κρυπτογραφημένο κείμενο χρησιμοποιώντας το ίδιο μυστικό κλειδί. Κάθε κείμενο δίνει διαφορετικό ciphertext.



Εικόνα 2.1: Η διαδικασία κρυπτογράφησης με Block Ciphers

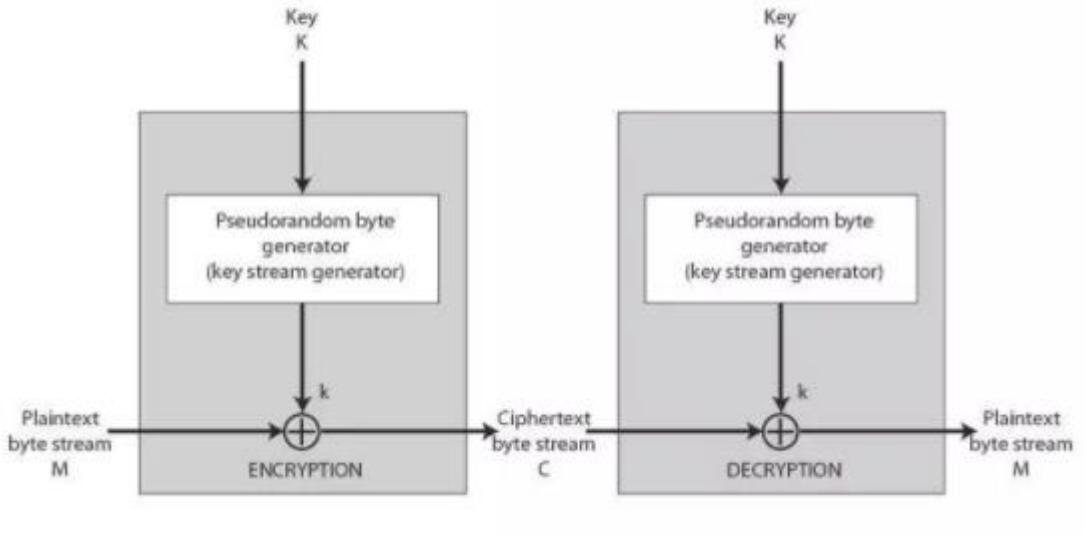
Οι block ciphers λειτουργούν επαναληπτικά, κρυπτογραφώντας ένα block διαδοχικά αρκετές φορές. Σε κάθε γύρο, ο ίδιος μετασχηματισμός εφαρμόζεται στα δεδομένα χρησιμοποιώντας ένα υπο-κλειδί (subkey). Το σύνολο των subkeys προέρχεται από το μυστικό κλειδί που χορήγησε ο χρήστης, με ειδική συνάρτηση.

Ο αριθμός των επαναλήψεων του επαναληπτικού cipher εξαρτάται από το επίπεδο της επιθυμητής ασφάλειας και την απόδοση του συστήματος. Στις περισσότερες περιπτώσεις, ο αυξημένος αριθμός επαναλήψεων βελτιώνει την προσφερόμενη ασφάλεια, αλλά για μερικούς ciphers ο αριθμός των επαναλήψεων θα πρέπει να είναι πολύ μεγάλος για να επιτευχθεί ικανοποιητική ασφάλεια. Οι πιο συνηθισμένοι αλγόριθμοι αυτής της κατηγορίας είναι οι DES, IDEA, AES (Rijndael), Blowfish, Twofish.

2.1.3.2 Stream Ciphers

Ο Stream cipher είναι ένας τύπος αλγόριθμου συμμετρικής κρυπτογράφησης. Είναι εξαιρετικά ταχείς αλγόριθμοι, πολύ ταχύτεροι από τους block ciphers. Σε αντίθεση με τους block ciphers που λειτουργούν με μεγάλα κομμάτια δεδομένων (blocks), οι stream ciphers τυπικά λειτουργούν με μικρότερες μονάδες απλού κειμένου, συνήθως με bits. Η κρυπτογράφηση ενός συγκεκριμένου κειμένου με έναν block cipher θα καταλήγει πάντα στο ίδιο αποτέλεσμα όταν χρησιμοποιείται το ίδιο κλειδί. Με έναν stream cipher, ο μετασχηματισμός των μικρότερων αυτών μονάδων θα ποικίλει, ανάλογα με πότε υλοποιούνται κατά την διάρκεια της κρυπτογράφησης.

Ένας stream ciphers παράγει μια ακολουθία από bits που χρησιμοποιείται σαν κλειδί και καλείται keystream. Η κρυπτογράφηση επιτυγχάνεται με τον συνδυασμό του keystream με το plaintext, συνήθως μέσω πράξης X-OR.



Εικόνα 2.2: Η διαδικασία κρυπτογράφησης με Stream Ciphers

Οι stream ciphers βασίζονται στις θεωρητικές ιδιότητες ενός κρυπτοσυστήματος γνωστού με το όνομα σημειωματάριο μιας χρήσης (one-time pad). One-time pads είναι ciphers που χρησιμοποιούν μια ακολουθία bits που ονομάζεται κλειδοροή (keystream) που παράγεται στην τύχη. Το keystream είναι του ίδιου μήκους με το μη

κρυπτογραφημένο κείμενο και συνδυάζεται μέσω μιας X-OR πράξης με το αυτό για την παραγωγή του ciphertext. Επειδή το keystream είναι τελείως τυχαίο και είναι του ίδιου μήκους με το plaintext, η εύρεση του κειμένου είναι αδύνατη ακόμα και με την διάθεση τεράστιας υπολογιστικής ισχύς. Ένας τέτοιος cipher προσφέρει τέλεια μυστικότητα και ασφάλεια και έχει χρησιμοποιηθεί σε μεγάλη κλίμακα σε καιρό πολέμου για την διασφάλιση διπλωματικών καναλιών. Το γεγονός, όμως, ότι το μυστικό κλειδί (δηλαδή το keystream), που χρησιμοποιείται μόνο μία φορά, είναι του ίδιου μήκους με του μήνυμα, εισάγει σημαντικό πρόβλημα στην διαχείριση του κλειδιού. Κατά συνέπεια, παρόλη την ασφάλεια που προσφέρει, ο one-time pad δεν μπορεί να εφαρμοστεί στην πράξη.

Οι stream ciphers αναπτύχθηκαν σαν μια προσέγγιση της λειτουργίας ενός one-time pad. Ο πιο ευρέως χρησιμοποιούμενος stream cipher είναι ο RC4, ο οποίος ωστόσο πολύ πρόσφατα κρίθηκε ότι πρέπει να αποφεύγεται. Ενδιαφέρον παρουσιάζει το γεγονός ότι συγκεκριμένοι τρόποι λειτουργίας ενός block cipher προσομοιάζουν ένα stream cipher όπως για παράδειγμα ο DES σε CFB και OFB modes. Οι ποιο συνηθισμένοι αλγόριθμοι αυτής της κατηγορίας είναι οι RC4, LFSRs, A5, SEAL

2.1.3.3 Hash Functions

Ο όρος hash function υποδηλώνει ένα μετασχηματισμό που δέχεται σαν είσοδο ένα μήνυμα m οποιουδήποτε μήκους και επιστρέφει στην έξοδο μία ακολουθία χαρακτήρων h περιορισμένου αλλά πάντα σταθερού μήκους που καλείται hash value, δηλαδή είναι h = H(m). Οι hash functions είναι συναρτήσεις της μορφής H(x)=y, με τις εξής ιδιότητες:

- η είσοδος είναι οποιουδήποτε μήκους,
- η έξοδος έχει περιορισμένο μήκος,
- δεδομένου του x, ο υπολογισμός του y είναι εύκολος,
- η H(x) είναι μη αντιστρέψιμη,
- η H(x) είναι αμφιμονοσήμαντη (ένα προς ένα συνάρτηση).

Η hash value παρουσιάζει συνοπτικά το μεγαλύτερο μήνυμα ή έγγραφο, για αυτό καλείται και σύνοψη μηνύματος (message digest). Μπορούμε να φανταστούμε την

σύνοψη του μηνύματος σαν "ψηφιακό αποτύπωμα" ("digital fingerprint") του εγγράφου. Παραδείγματα γνωστών hash functions είναι οι MD2, MD5,SHA2 και SHA3.

Μια επίθεση σύγκρουσης Hash είναι μια προσπάθεια να βρεθούν δύο συμβολοσειρές εισόδου μιας συνάρτησης κατακερματισμού που παράγουν το ίδιο αποτέλεσμα κατακερματισμού. Επειδή οι λειτουργίες κατακερματισμού έχουν άπειρο μήκος εισόδου και προκαθορισμένο μήκος εξόδου, υπάρχει αναπόφευκτα η πιθανότητα δύο διαφορετικών εισόδων που παράγουν την ίδια κατακερματισμό εξόδου. Εάν δύο ξεχωριστές εισόδους παράγουν την ίδια έξοδο κατακερματισμού, ονομάζεται σύγκρουση (collision). Αυτή η σύγκρουση μπορεί στη συνέχεια να αξιοποιηθεί από οποιαδήποτε εφαρμογή που συγκρίνει δύο Hashes, όπως hashes κωδικών πρόσβασης, ελέγχους ακεραιότητας αρχείων κλπ.

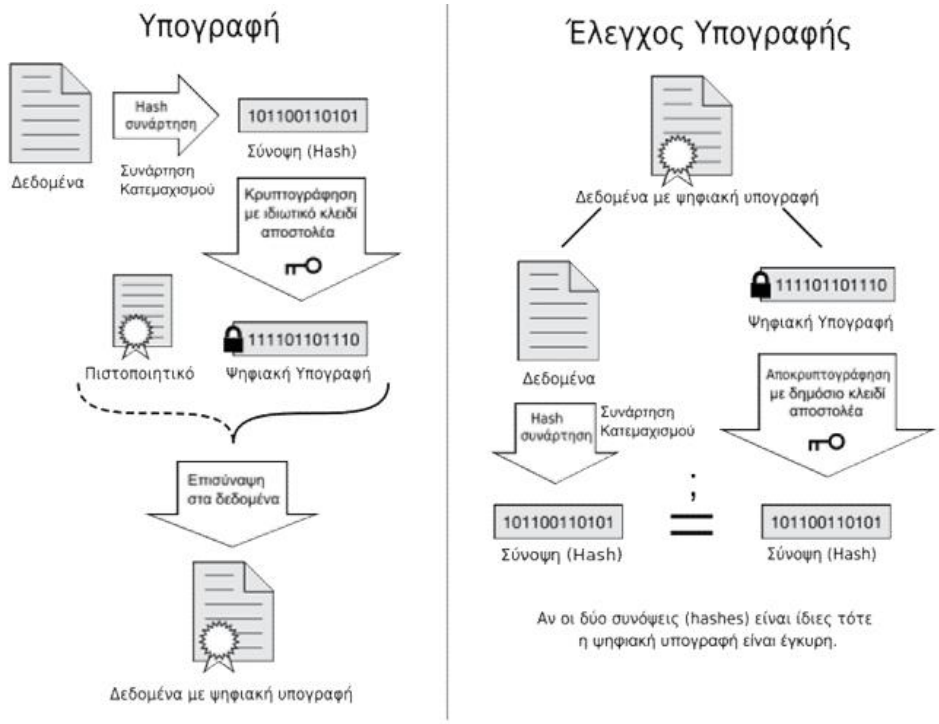
2.1.3.4 Ψηφιακές υπογραφές

Με την κρυπτογράφηση εξασφαλίζουμε την εμπιστευτικότητα της επικοινωνίας μεταξύ δύο οντοτήτων. Με την χρήση των ψηφιακών υπογραφών μπορούμε να διασφαλίσουμε την ακεραιότητα των μηνυμάτων, δηλαδή ότι δεν αλλοιώθηκαν κατά την μεταφορά. Επιπλέον γίνεται πιστοποίηση ότι το μήνυμα ανήκει στον αποστολέα και την αποτροπή της άρνησης παραδοχής συμμετοχής (non reputation).

Για να υπογράψει ένα μήνυμα ο αποστολέας πρέπει να δημιουργήσει μια σύνοψη του μηνύματος με μια συνάρτηση hash. Οποιαδήποτε αλλοίωση του αρχικού μηνύματος θα επιφέρει και αλλαγή στην σύνοψη του μηνύματος. Στην συνέχεια θα κρυπτογραφήσει την σύνοψη με το ιδιωτικό κλειδί ώστε να μπορεί να αποκρυπτογραφηθεί μόνο με το δικό του δημόσιο κλειδί. Η κρυπτογραφημένη αυτή σύνοψη αποτελεί την ψηφιακή υπογραφή. Στην συνέχεια γίνεται κρυπτογράφηση του μηνύματος και της ψηφιακής υπογραφής με το δημόσιο κλειδί του παραλήπτη και πραγματοποιείται η αποστολή.

Ο παραλήπτης πρέπει να επιβεβαιώσει ότι δεν έχει γίνει αλλοίωση του μηνύματος και ότι ο αποστολέας είναι αυτός που δηλώνει. Για να πραγματοποιηθεί αυτό, αρχικά αποκρυπτογραφείται ολόκληρο το μήνυμα. Στην συνέχεια αποκρυπτογραφείται η ψηφιακή υπογραφή με το δημόσιο κλειδί του αποστολέα και δημιουργεί μια σύνοψη του μηνύματος

με σκοπό να την συγκρίνει με αυτή που έλαβε. Αν η σύγκριση είναι επιτυχής τότε το μήνυμα είναι αναλλοίωτο. Η διαδικασία φαίνεται σχηματικά στην Εικόνα 2.3.

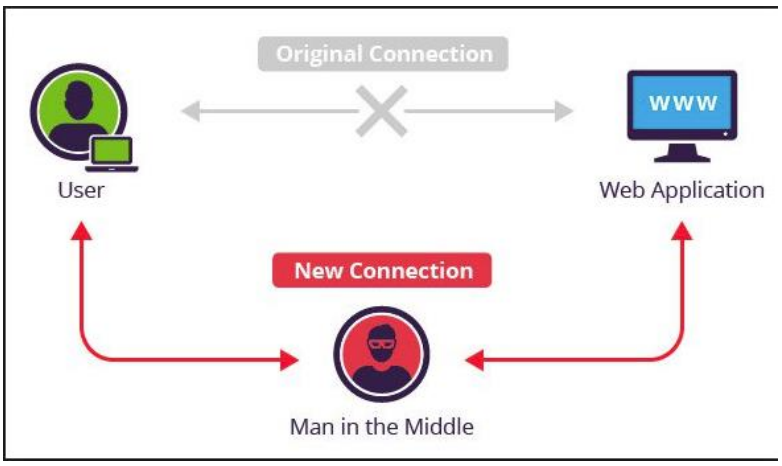


Εικόνα 2.3: Η διαδικασία της ψηφιακής υπογραφής

2.1.3.5 Επιθέσεις man-in-the-middle

Μια επίθεση ενδιάμεσου (MITM) είναι μια μορφή υποκλοπής όπου η επικοινωνία μεταξύ δύο χρηστών παρακολουθείται και τροποποιείται από ένα μη εξουσιοδοτημένο άτομο. Συνήθως, ο επιτιθέμενος παρακολουθεί ενεργά υποκλέπτοντας τα μηνύματα δημόσιου κλειδιού και αναμεταδίδοντας τα αντικαθιστώντας το κλειδί με το δικό του.

Στη διαδικασία, οι δύο αρχικά συμμετέχοντες φαίνεται να επικοινωνούν κανονικά. Ο αποστολέας μηνυμάτων δεν αναγνωρίζει ότι ο δέκτης είναι ένας άγνωστος εισβολέας που προσπαθεί να έχει πρόσβαση ή να τροποποιήσει το μήνυμα πριν από την αναμετάδοση στον δέκτη. Έτσι, ο επιτιθέμενος ελέγχει ολόκληρη την επικοινωνία. Στην Εικόνα 2.4 φαίνεται η διαδικασία αυτή.



Εικόνα 2.4: Σχηματική απεικόνιση της επίθεσης man in the middle attack

2.1.3.6 Ψηφιακά πιστοποιητικά

Το Ψηφιακό πιστοποιητικό είναι ένα ηλεκτρονικό έγγραφο που χρησιμοποιείται για την αναγνώριση μίας οντότητας (φυσικό πρόσωπο, εξυπηρετητής, οργανισμός κοκ) και την ανάκτηση του δημοσίου κλειδιού αυτής. Η έκδοση ενός ψηφιακού πιστοποιητικού γίνεται μετά από αίτηση του ενδιαφερομένου σε μία Αρχή Πιστοποίησης. Η Αρχή Πιστοποίησης επιβεβαιώνει την ταυτότητα του αιτούντος και εκδίδει το πιστοποιητικό, το οποίο συνοπτικά περιλαμβάνει τα εξής στοιχεία:

- Το ονοματεπώνυμο και διάφορες άλλες πληροφορίες σχετικά με τον κάτοχο του πιστοποιητικού.
- Το δημόσιο κλειδί του κατόχου του πιστοποιητικού.
- Την ημερομηνία λήξης του πιστοποιητικού.
- Το όνομα και την ψηφιακή υπογραφή της Αρχής Πιστοποίησης που το εξέδωσε.

Το πιο διαδεδομένο πρότυπο ψηφιακών πιστοποιητικών είναι το X.509. Τα ψηφιακά πιστοποιητικά χρησιμοποιούνται ευρέως για διάφορες κρυπτογραφημένες ηλεκτρονικές συναλλαγές μέσω του διαδικτύου. Παραδείγματα τέτοιων συναλλαγών είναι: Σύνοδοι με βάση το πρωτόκολλο SSL (Client/Server SSL Certificates), κρυπτογραφημένο και υπογεγραμμένο ηλεκτρονικό ταχυδρομείο (S/MIME Certificates), υπογραφή αντικειμένων (Object-signing Certificates) κοκ. Με τα ψηφιακά πιστοποιητικά αντιμετωπίζονται οι επιθέσεις τύπου Man-in-the-middle, υπό την έννοια ότι υπάρχει πάντα αυθεντικοποίηση του άλλου μέλους της επικοινωνίας

2.1.3.7 Message Authentication Code

Message Authentication Code είναι ένα κώδικας (καλείται και checksum) που συνοδεύει το μήνυμα και πιστοποιεί την ταυτότητα του αποστολέα και την ακεραιότητα του μηνύματος. Για την παραγωγή τους εφαρμόζεται στο μήνυμα ένα από τα προαναφερθέντα κρυπτογραφικά εργαλεία σε συνδυασμό με ένα μυστικό κλειδί. Σε αντίθεση με τις ψηφιακές υπογραφές, τα MACs υπολογίζονται και επαληθεύονται με το ίδιο κλειδί, έτσι ώστε να μπορούν να επαληθευθούν μόνο από τον προοριζόμενο παραλήπτη. Υπάρχουν τέσσερις τύποι MAC: (1) τα άνευ όρων ασφαλή, (2) τα βασιζόμενα σε hash functions, (3) τα βασιζόμενα σε stream ciphers και (4) τα βασιζόμενα σε block ciphers.

Οι Simmons και Stinson [5] πρότειναν των άνευ όρων ασφαλή MAC που βασίζεται στην κρυπτογράφηση με ένα one-time pad. Όπως είπαμε, όμως, επειδή το κλειδί ενός one-time pad είναι πολύ μεγάλο, δεν χρησιμοποιούνται στην πράξη.

Τα MACs που βασίζονται σε hash functions χρησιμοποιούν ένα μυστικό κλειδί σε συνδυασμό με ένα hash function για να παράγουν το checksum που συνοδεύει το μήνυμα. Το κλειδί χρησιμοποιείται για να κρυπτογραφήσει το message digest του μηνύματος. Ο παραλήπτης του μηνύματος, που μοιράζεται με τον αποστολέα το ίδιο κλειδί, αποκρυπτογραφεί το message digest και έπειτα το συγκρίνει με ένα message digest που παράγει ο ίδιος από το μήνυμα. Εάν η σύγκριση είναι επιτυχής, τότε ο παραλήπτης σιγουρεύεται ότι τα δεδομένα δεν έχουν αλλοιωθεί. Ένα παράδειγμα είναι ο αλγόριθμος HMAC.

Τα MACs που βασίζονται σε stream ciphers αναπτύχθηκαν από τους Lai, Rueppel και Woolven [6]. Στο αλγόριθμο που ανέπτυξαν, ένας δοκιμασμένος για την ασφάλειά του stream cipher, εφαρμόζεται στα δύο μισά ενός μηνύματος. Τα δύο μισά τροφοδοτούν διαδοχικά το LFSR και η τελική κατάσταση του καταχωρητή αντιπροσωπεύει το checksum. Το μυστικό κλειδί που απαιτείται λειτουργεί σαν διάνυσμα αρχικοποίησης (Initialization Vector) του LFSR.

Τέλος, τα MAC μπορούν να δημιουργηθούν από block ciphers, με έναν ειδικό τρόπο λειτουργίας αυτών, αυτόν τον αλυσιδωτού τμήματος (Cipher Block Chaining Mode – CBC). Σε αυτήν την μέθοδο, το μήνυμα κρυπτογραφείται με εφαρμογή του αλγόριθμου block cipher σε τρόπο λειτουργίας CBC, οπότε και η κρυπτογράφηση ενός τμήματος

εξαρτάται από το προηγούμενο κρυπτογραφημένο τμήμα. Το τελευταίο ciphertext block που δίνει ο αλγόριθμος αποτελεί το checksum του μηνύματος.

2.1.3.8 Μηχανισμοί Διαχείρισης και Ανταλλαγής Κλειδιών

Οι μηχανισμοί διαχείρισης κλειδιών *(key management)* και ανταλλαγής κλειδιών *(key exchange)*, ασχολούνται με την ασφαλή παραγωγή, διανομή και αποθήκευση των κλειδιών κρυπτογράφησης. Η εύρεση απρόσβλητων μεθόδων διαχείρισης και ανταλλαγής κλειδιών είναι πολύ σημαντική στη διατήρηση της ασφάλειας της επικοινωνίας.

Στα ασύμμετρα κρυπτοσυστήματα, τα χαρακτηριστικά που πρέπει να έχει ένας μηχανισμός διαχείρισης κλειδιών είναι τα ακόλουθα. Οι χρήστες πρέπει να είναι σε θέση να μπορούν να αποκτήσουν με ασφάλεια ένα ζεύγος δημόσιας – ιδιωτικής κλείδας που θα ικανοποιεί τις ανάγκες τους για προστατευμένη επικοινωνία. Πρέπει να υπάρχει τρόπος αποθήκευσης και δημοσιοποίησης των δημόσιων κλειδιών, ενώ παράλληλα να είναι δυνατή η ανάκτησή τους όποτε χρειάζεται. Επίσης οι δημόσιες κλείδες θα πρέπει να συσχετίζονται με σίγουρο τρόπο με την ταυτότητα του νόμιμου κατόχου. Έτσι, δεν θα μπορεί κάποιος να παρουσιάζεται σαν κάποιος άλλος, επιδεικνύοντας μία ψεύτικη δημόσια κλείδα. Τέλος οι χρήστες πρέπει να έχουν την δυνατότητα να φυλάσσουν τις ιδιωτικές τους κλείδες με ασφάλεια, οι οποίες θα είναι έγκυρες μόνο για συγκεκριμένο χρονικό διάστημα.

Η ανταλλαγή κλειδιών εφαρμόζεται στα συμμετρικά κρυπτοσυστήματα, όπου οι δύο επικοινωνούντες χρήστες πρέπει να αποφασίσουν για το κοινό μυστικό κλειδί και έπειτα να αποκτήσουν από ένα αντίγραφο αυτού, χωρίς κανένας άλλος να μάθει για αυτό.

2.2 Ιστορική αναδρομή του SSL/TLS

Κατά την διάρκεια του ψυχρού πολέμου, την δεκαετία του 1960, το αμερικανικό Υπουργείο Άμυνας δημιούργησε ένα ερευνητικό πρόγραμμα το ARPANET. Ο σκοπός του προγράμματος ήταν να δημιουργήσει ένα αξιόπιστο και αποκεντρωμένο δίκτυο για τον διαμοιρασμό πληροφοριών μεταξύ του Υπουργείου Άμυνας, των Ενόπλων Δυνάμεων και των αμερικανικών πανεπιστημίων. Η δημιουργία του δικτύου ARPANET βασίζονταν στην υπόθεση ότι θα συνέχιζε να λειτουργεί ακόμη και αν ένας ή περισσότεροι από τους κόμβους του δικτύου δεν λειτουργούσε. Οι χρήστες του δικτύου ARPANET αποτελούνταν από έναν μικρό αριθμό ατόμων οι οποίοι γνωρίζονταν μεταξύ τους και γενικά υπήρχε αμοιβαία εμπιστοσύνη. Έτσι το βασικό μέλημα στην δημιουργία του δικτύου ήταν η ευελιξία και η επεκτασιμότητα, αλλά όχι η ασφάλεια. Τις επόμενες δεκαετίες περισσότερα πανεπιστήμια και ερευνητικά κέντρα συνδέθηκαν στο ARPANET. Μέχρι τις αρχές του 1980 είχαν συνδεθεί πάνω από 200 κόμβοι από όλον τον κόσμο, αλλάζοντας έτσι τον ρόλο του από ένα στρατιωτικό δίκτυο σε αυτό που σήμερα περιγράφουμε σαν διαδίκτυο. Καθώς το δίκτυο εξελίσσονταν, με την δημιουργία καινούργιων υπηρεσιών όπως το ηλεκτρονικό ταχυδρομείο αλλά και το World Wide Web, η ασφάλειά του έδειχνε να μην παίζει σημαντικό ρόλο.

Σε εκείνη την περίοδο η εταιρεία που κυριαρχούσε στους φυλλομετρητές και στους διακομιστές ιστού ήταν η Netscape Communications. Ανταποκρινόμενη στην απαίτηση της αγοράς για ασφαλείς επικοινωνίες, που άρχισε σιγά σιγά να εμφανίζεται, δημιούργησαν το 1994 το πρωτόκολλο Secure Socket Layer (SSL). Στην αρχή το πρωτόκολλο δημιουργήθηκε για την ασφαλή επικοινωνία μεταξύ του φυλλομετρητή της Netscape και του διακομιστή. Στις προδιαγραφές του όμως ήταν σαφές ότι μπορούσε να χρησιμοποιηθεί και από άλλες εφαρμογές. Η έκδοση 1 του πρωτοκόλλου SSL δεν εκδόθηκε ποτέ δημόσια, παρόλα αυτά τράβηξε γρήγορα την προσοχή των εταιρειών και των ερευνητών. Τον επόμενο χρόνο η Netscape εξέδωσε την δεύτερη έκδοση του πρωτοκόλλου. Η έκδοση αυτή αναλύθηκε εξονυχιστικά και βρέθηκαν πολλές ευπάθειες. Ο σκοπός της έκδοσης 2 ήταν να διορθώσει τις ευπάθειες του πρωτοκόλλου και τα μειονεκτήματα του, οδηγώντας έτσι την επόμενη χρονιά σε ένα εκ βαθέων τροποποιημένο πρωτόκολλο.

Παράλληλα με την Netscape, άλλες εταιρίες προσπαθούσαν να φτιάξουν την δική τους λύση ασφαλείας. Για τον λόγο αυτό και για να μην υπάρχει πολυτυπία πρωτοκόλλων, η Microsoft και η Netscape, ζήτησαν από την Internet Engineering Task Force (IETF), να καθορίσει ένα στάνταρ (τυποποιημένο) πρωτόκολλο. Η IETF είναι μία ανοικτή κοινότητα η οποία δημιουργεί πρότυπα, κυρίως για την τεχνολογική επανάσταση που λαμβάνει χώρα στο πεδίο του διαδικτύου. Η IETF συνεργάζεται με τον οργανισμό W3C ώστε μαζί να δημιουργήσουν πρότυπα για το διαδίκτυο και για να προτείνουν καινούργιες λύσεις και εφαρμογές. Το πιο γνωστό προϊόν που παράγει η IETF είναι τα έγγραφα Request For Comments (RFC). Το RFC είναι ένα επίσημο δημόσιο κανάλι, μέσω του οποίου γίνονται προτάσεις για πρότυπα, διαμέσου πολλών γύρων αναθεωρήσεων και προτάσεων, μπορεί να καταλήξει σε ένα Internet Standard (STD). Το 1999 η IETF έκδωσε την πρώτη πρόταση της για ένα καινούργιο πρότυπο: το RFC22461. Η πρόταση της βασίστηκε στην έκδοση 3 του Secure Socket Layer, αλλά επιπλέον έλαβαν υπόψη τους παρατηρήσεις και προτάσεις από πολλούς άλλους ειδικούς. Το αποτέλεσμα της πρότασης αυτής ήταν η δημιουργία της πρώτης έκδοσης του πρωτοκόλλου Transport Layer Security (TLS). Οι αλλαγές από το SSL 3.0 δεν ήταν δραματικές, ήταν όμως αρκετές για να μην είναι συμβατά.

Μετά από 7 χρόνια το πρωτόκολλο αναβαθμίζεται στην έκδοση TLS 1.1. Οι διαφορές από την πρώτη έκδοση δεν ήταν μεγάλες, κυρίως επικεντρώθηκαν στην επιδιόρθωση των ευπαθειών που είχαν ανακαλυφθεί και στην υποστήριξη καινούργιων αλγορίθμων κρυπτογράφησης. Το 2008 το πρωτόκολλο αναβαθμίστηκε ξανά στην έκδοση TLS 1.2. Κατά την περίοδο εκπόνησης της παρούσας μεταπτυχιακής διατριβής βρισκόταν σε φάση δημόσιας συζήτησης η έκδοση TLS 1.3 του πρωτοκόλλου, η οποία τελικά οριστικοποιήθηκε το Μάρτιο του 2018.

Παρακάτω έχουν καταγραφεί αναλυτικά οι διάφορες εκδόσεις του SSL/TLS με τις κυριότερες βελτιώσεις και ευπάθειές τους.

2.2.1 Secure Network Programming API

Πρώιμες ερευνητικές προσπάθειες στην ασφάλεια επιπέδου μεταφοράς (Transport Layer Security) περιλάμβαναν το Secure Network Programming (SNP) API [7], που το 1994 διερεύνησε την προσέγγιση ενός ασφαλούς επιπέδου μεταφοράς. Ήταν μία προσπάθεια για τη δημιουργία ενός υψηλού επιπέδου πλαισίου για ασφαλείς

επικοινωνίες δικτύου από άκρο σε άκρο. Υποστήριζε τόσο τη ροή και στοιχεία που ενισχύουν την ασφάλεια (όπως π.χ. η γνησιότητα της προέλευσης δεδομένων, η ακεραιότητα και εμπιστευτικότητα των δεδομένων). Είχε σχεδιαστεί για να μοιάζει με τη διασύνδεση των υποδοχών Berkeley έτσι ώστε η ασφάλεια να μπορεί εύκολα να ενσωματωθεί σε υπάρχοντα socket programs με μικρές μόνο τροποποιήσεις. Το SNP είναι χτισμένο πάνω από το GSS-API, καθιστώντας το σχετικά συμβατό σε διαφορετικούς μηχανισμούς ελέγχου ταυτότητας που συμμορφώνονται με το GSS-API. Το SNP αποκρύπτει τις λεπτομέρειες του GSS-API (π.χ. διαχείριση διαπιστευτηρίων και πλαισίων), το υποεπίδεδο επικοινωνίας καθώς και το υποεπίδεδο κρυπτογραφίας από τους προγραμματιστές. Ενσωματώνει επίσης ευαίσθητες πληροφορίες ασφαλείας, αποτρέποντας έτσι τυχαία ή σκόπιμη αποκάλυψη από ένα πρόγραμμα εφαρμογής.

2.2.2 SSL 1.0, 2.0 & 3.0

Η ευρεία διάδοση το διαδικτύου, δημιούργησε την ανάγκη για την δημιουργία ασφαλούς πρωτοκόλλου στο επίπεδο μεταφοράς. Το πρωτόκολλο SSL αναπτύχτηκε αρχικά από την Netscape και κατά κύριο λόγο από τον μηχανικό Kipp Hickman. Η έκδοση 1.0 δε δημοσιεύτηκε ποτέ καθώς είχε πολλά προβλήματα ασφαλείας. Η έκδοση 2.0 κυκλοφόρησε το Φεβρουάριο του 1995 αλλά είχε μια σειρά από προβλήματα ασφαλείας που τελικά οδήγησαν στη σχεδίαση του SSL 3.0. Το SSL 3.0 κυκλοφόρησε το 1996 και ήταν ένας πλήρης ανασχεδιασμός του πρωτοκόλλου που έγινε από τον Paul Kocher σε συνεργασία με τους μηχανικούς της Netscape, Phil Karlton & Alan Freir. Οι επόμενες εκδόσεις του SSL/TLS βασίζονται στο SSL v3.0.

Το 2011 SSL V2.0 θεωρήθηκε από την IETF σαν παρωχημένο και ζητήθηκε από τους χρήστες να σταματήσουν να το χρησιμοποιούν καθώς στην δημοσίευση που είχαν κάνει [8]περιέγραφαν τις παρακάτω αδυναμίες:

- Η αυθεντικοποίηση του μηνύματος χρησιμοποιούσε τον αλγόριθμο MD5. Οι ευαισθητοποιημένοι με την ασφάλεια χρήστες, είχαν ήδη σταματήσει κάθε χρήση του αλγόριθμου MD5.
- Τα μηνύματα χειραψίας δεν ήταν προστατευμένα. Αυτό επιτρέπει επιθέσεις τύπου man-in-the-middle με σκοπό να οδηγήσει το θύμα να επιλέξει μία ποιο αδύναμη cipher suite, σε σχέση με αυτή που επέλεγε συνήθως.

- Το κλειδί για την ακεραιότητα του μηνύματος αλλά και για το κρυπτογραφημένο μήνυμα ήταν το ίδιο. Αυτό αποτελούσε πρόβλημα αν η επικοινωνία κατά την διαπραγμάτευση client - server χρησιμοποιούσε αδύναμο αλγόριθμο.
- Σε μία επίθεση man-in-the-middle μπορούσε πολύ εύκολα να εισαχθεί ένα TCP FIN για να κλείσει η σύνοδος, με αποτέλεσμα να υπάρχει σύγχυση αν ο τερματισμός της συνόδου είχε γίνει σωστά.

Ομοίως το 2015 το SSL V3.0 θεωρήθηκε από την IETF σαν παρωχημένο. Ενώ το TLS 1.0 είχε ήδη 16 χρόνια που είχε κυκλοφορήσει, παρόλα αυτά το πρωτόκολλο SSL V3.0 ήταν ακόμη σε χρήση. Στο έγγραφο που συνέταξε η IETF όλες οι εκδόσεις του TLS είναι πιο ασφαλείς από το SSL 3.0 για τους εξής λόγους:

- Ανταλλαγή κλειδιών. Η ανταλλαγή κλειδιών στο SSL V3.0 είναι ευάλωτη σε επιθέσεις man-in-the-middle attacks κατά την διαπραγμάτευση ή την επανάληψη συνόδου [TRIPLE-HS].
- Δομικά στοιχεία στην κρυπτογράφηση. Το SSL V3.0 καθορίζει προσαρμοσμένες δομές για τις συναρτήσεις ψευδοτυχαίων αριθμών (PRF), Hashed Message Authentication Code (HMAC), και στις ψηφιακές υπογραφές τα οποία στερούνται την βαθιά και εξονυχιστική κρυπτογραφική εξέταση η οποία είναι δομική στο TLS. Επιπλέον, όλα τα δομικά στοιχεία του SSL V3.0 στηρίζονται στους αλγορίθμους SHA-1 και MD5, οι οποίοι θεωρούνται και οι δύο αδύναμοι.
- Περιορισμένες δυνατότητες. Το SSL V3.0 δεν μπορεί να εκμεταλλευτεί νέες δυνατότητες, οι οποίες αντίθετα έχουν προστεθεί στις εκδόσεις TLS, όπως:
    - Λειτουργίες Authenticated Encryption with Additional Data (AEAD)
    - Elliptic Curve Diffie-Hellman (ECDH) και Digital Signature Algorithm (ECDSA)
    - Stateless session tickets
    - A datagram mode of operation, DTLS Application-layer protocol negotiation

2.2.3 TLS 1.0 (SSL 3.1)

Το TLS 1.0 ορίστηκε καταρχήν στο RFC 2246 τον Ιανουάριο του 1999 σαν μια αναβάθμιση του SSL Version 3.0. Οι αλλαγές ανάμεσα στο TLS 1.0 και το SSL 3.0 δεν είναι

μεγάλες, αλλά είναι αρκετές ώστε μην υπάρχει διαλειτουργικότητα ανάμεσα στα δύο πρωτόκολλα. Το TLS 1.0 περιλαμβάνει ένα μηχανισμό για την υποβάθμιση του πρωτοκόλλου επικοινωνίας σε SSL 3.0.

- Η υλοποίηση που υπήρχε για το διάνυσμα αρχικοποίησης (Initialization Vector), αντικαταστάθηκε με μία πιο συγκεκριμένη και ασφαλή υλοποίηση για να αντιμετωπίσει τις επιθέσεις CBC.
- Η ειδοποίηση bad_record_mac αντικαταστάθηκε από την ειδοποίηση decryption_failed για να προστατευθεί από επιθέσεις που εκμεταλλεύονται κατάλληλα ιδιότητες του CBC τρόπου λειτουργίας.
- Οι καταχωρήσεις της IANA καθορίζονται σαν παράμετροι του πρωτοκόλλου.
- Το πρόωρο κλείσιμο μιας συνεδρίας δεν συνεπάγεται πλέον τη μη επανάληψή της.
- Πρόσθετες ενημερωτικές σημειώσεις προστέθηκαν για διάφορες νέες επιθέσεις στο TLS.

2.2.4 TLS 1.1 (SSL 3.2)

Το TLS 1.1 ορίστηκε στο RFC 4346 τον Απρίλη του 2006. Είναι μια αναβάθμιση από την έκδοση 1.0. Οι βασικές αλλαγές σε αυτή την έκδοση είναι οι παρακάτω:

- Προσθήκη προστασίας ενάντια σε επιθέσεις που εκμεταλλεύονται κατάλληλα κάποιες ιδιότητες του CBC τρόπου λειτουργίας.
- Ο υπονοούμενος Πίνακας Αρχικοποίησης (Initialization Vector) αντικαταστάθηκε από ένα ρητό IV.
- Αλλαγές στη διαχείριση padding errors.
- Υποστήριξη για καταχώρηση παραμέτρου στο IANA.

2.2.5 TLS 1.2 (SSL 3.3)

Το TLS 1.2 ορίστηκε στο RFC 5246 τον Αύγουστο του 2008. Βασίζεται στο TLS 1.1 με κύριες διαφορές τις παρακάτω:

- Ο συνδυασμός MD5-SHA-1 στην ψευδοτυχαία συνάρτηση (PRF) αντικαταστάθηκε από τον SHA-256, με δυνατότητα χρήσης PRF οριζόμενο από την cipher-suite.
- Ο συνδυασμός MD5-SHA-1 στο hash του μηνύματος Finished αντικαταστάθηκε από τον SHA-256, με δυνατότητα χρήσης διαφορετικών αλγορίθμων ανάλογα με το cipher-suite.
- Ο συνδυασμός MD5-SHA-1 στο ψηφιακά υπογεγραμμένο στοιχείο αντικαταστάθηκε με ένα μοναδικό hash που ορίζεται κατά τη διάρκεια της χειραψίας με προεπιλογή το SHA- 1.
- Βελτιώσεις στις δυνατότητες του πελάτη και του εξυπηρετητή να ορίζουν ποιους αλγορίθμους αποδέχονται για hashing και ψηφιακές υπογραφές.
- Επέκταση της υποστήριξης κρυπταλγορίθμων για αυθεντικοποιημένη κρυπτογραφία
- Προστέθηκε ορισμός των επεκτάσεων του TLS, καθώς και Advanced Encryption Standard cipher suites.
- Αυστηρότερος έλεγχος στις εκδόσεις του EncryptedPreMasterSecret.
- Η χρήση του TLS_RSA_WITH_AES_128_CBC_SHA είναι τώρα υποχρεωτική για την υλοποίηση cipher suite.
- Προστέθηκαν HMAC-SHA256 cipher suites.
- Αφαιρέθηκαν IDEA and DES cipher suites.

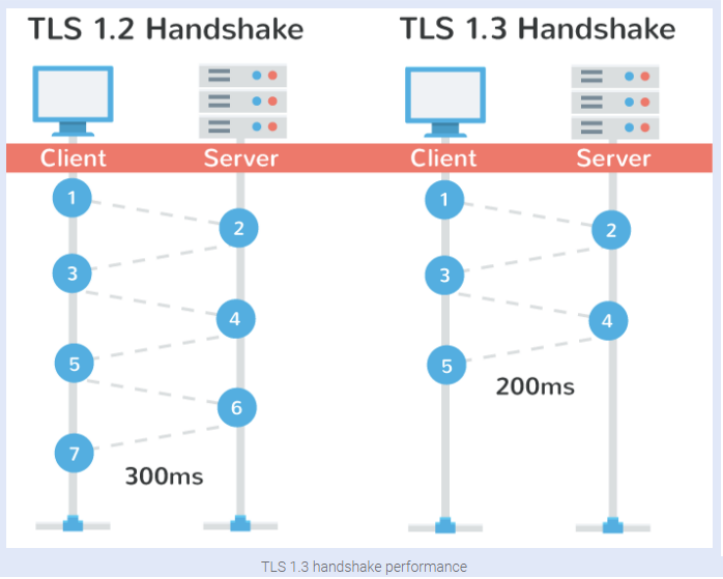
Το TLS 1.2 βελτιώθηκε περαιτέρω στο RFC 6176, το Μάρτιο του 2011, με την αφαίρεση της προς τα πίσω συμβατότητας που επιτρέπει την υποβάθμιση του πρωτοκόλλου στο SSL 2.0.

2.2.6 TLS 1.3

Η ομάδα δράσης IETF αναπτύσσει αυτήν την περίοδο την επόμενη έκδοση του πρωτόκολλου ασφάλειας TLS, την έκδοση 1.3. Η διαφάνεια αυτής της διαδικασίας τυποποίησης επιτρέπει την ολοκληρωμένη κρυπτογραφική ανάλυση των πρωτοκόλλων πριν από την υιοθέτηση, ενώ στις προηγούμενες εκδόσεις του TLS εξετάστηκαν λεπτομερώς από την ερευνητική κοινότητα μόνο μετά την τυποποίηση. Οι

σημαντικότερες αλλαγές που προτείνονται στοχεύουν στην βελτίωση της ταχύτητας και της ασφάλειας σε σχέση με την έκδοση TLS 1.2.

Για παράδειγμα στον τομέα της ταχύτητας, η μέχρι τώρα διαδικασία για την υλοποίηση κρυπτογραφημένης επικοινωνίας απαιτούσε δύο round-trip για την εκτέλεση της χειραψίας του TLS. Στην έκδοση TLS 1.3 αυτό προτείνεται να γίνεται σε ένα round-trip, οπότε και θα υπάρχει κέρδος σε ταχύτητα. Επιπλέον εισάγεται ο όρος του zero round trip. Δηλαδή σε ιστοσελίδες που είχε επισκεφτεί ο χρήστης σε προηγούμενη στιγμή, δεν χρειάζεται να γίνει πάλι εγκαθίδρυση ασφαλούς σύνδεσης με αποτέλεσμα να βελτιώνεται η ταχύτητα.



Εικόνα 2.5:Διαφορές στην χειραψία του πρωτοκόλλου TLS στις εκδόσεις 1.2 και 1.3 [9]

Ένα από τα πιο σημαντικά μειονεκτήματα του πρωτοκόλλου TLS 1.2 είναι ότι, αν δεν έχει ρυθμιστεί σωστά αφήνει τις ιστοσελίδες ανασφαλείς. Η έκδοση TLS 1.3 αφαιρεί παρωχημένους και ανασφαλείς αλγόριθμους που περιέχονται στην έκδοση TLS 1.2 όπως για παράδειγμα:

- SHA-1
- RC4
- DES
- 3DES

- AES-CBC
- MD5
- Arbitrary Diffie-Hellman groups — CVE-2016-0701
- EXPORT-strength ciphers – Responsible for FREAK and LogJam

Στις 26/3/2018, και ενώ είχε ολοκληρωθεί η παρούσα μεταπτυχιακή διατριβή, ανακοινώθηκε η οριστικοποίηση του TLS 1.3. Κάποια εκ των χαρακτηριστικών του, σε σχέση με τις προηγούμενες εκδόσεις είναι:

- Η λίστα με τους συμμετρικούς αλγορίθμους που υποστηρίζονται δεν περιέχει πλέον αυτούς που θεωρούνται παρωχημένοι. Όσοι παρέμειναν υποστηρίζουν Authenticated Encryption with Associated Data (AEAD). Η έννοια της cipher suite έχει αλλάξει για να διαχωρίσει τους μηχανισμούς επαλήθευσης ταυτότητας και κλειδιών από τον αλγόριθμο προστασίας εγγραφής (συμπεριλαμβανομένου του μυστικού μήκους κλειδιού) και έναν hash που θα χρησιμοποιηθεί με τη συνάρτηση παραγωγής κλειδιών και HMAC.
- Προστέθηκε μια λειτουργία 0-RTT, εξοικονομώντας ένα βήμα στη ρύθμιση σύνδεσης για ορισμένα δεδομένα εφαρμογών.
- Έχουν αφαιρεθεί οι στατικές μονάδες κρυπτογράφησης RSA και Diffie-Hellman. όλοι οι μηχανισμοί ανταλλαγής κλειδιών βασισμένοι στο δημόσιο κλειδί παρέχουν τώρα εμπιστευτική μυστικότητα (forward secrecy).
- Όλα τα μηνύματα χειραψίας μετά το ServerHello είναι τώρα κρυπτογραφημένα. Το νεοεισερχόμενο μήνυμα EncryptedExtension επιτρέπει σε διάφορες επεκτάσεις που έχουν αποσταλεί προηγουμένως το ClearHello να απολαμβάνουν επίσης προστασία εμπιστευτικότητας από ενεργούς επιτιθέμενους
- Οι λειτουργίες εξαγωγής κλειδιών έχουν επανασχεδιαστεί. Ο νέος σχεδιασμός επιτρέπει ευκολότερη ανάλυση από τους κρυπτογράφους λόγω των βελτιωμένων ιδιοτήτων τους διαχωρισμού κλειδιών.
- Η διαδικασία χειραψίας έχει αναδιαρθρωθεί σημαντικά ώστε να είναι πιο συνεπής και να αφαιρεί περιττά μηνύματα όπως το ChangeCipherSpec (εκτός εάν απαιτείται για συμβατότητα στο μεσαίο πλαίσιο)
- Οι αλγόριθμοι ελλειπτικής καμπύλης είναι τώρα στις βασικές προδιαγραφές και συμπεριλαμβάνονται νέοι αλγόριθμοι, όπως οι ed25519 και ed448.

- Άλλες βελτιώσεις στην κρυπτογράφηση, συμπεριλαμβάνεται η απομάκρυνση της συμπίεσης και προσαρμοσμένων ομάδων DHE, αλλαγή του padding RSA για χρήση του RSASSA-PSS και αφαίρεση του DSA.
- Η επανάληψη της περιόδου σύνδεσης με και χωρίς την κατάσταση διακομιστή καθώς και οι κρυπτογραφικές μονάδες βασισμένες σε PSK παλαιότερων εκδόσεων TLS έχουν αντικατασταθεί από μία καινούργια ανταλλαγή PSK.

Στο υπόλοιπο τμήμα της μεταπτυχιακής διατριβής δεν γίνεται ειδικότερη μνεία στο TLS 1.3, λόγω του ότι η έκδοση αυτή δεν είχε οριστικοποιηθεί για όσο η διατριβή ήταν σε εξέλιξη. Παρόλα αυτά, στην αξιολόγηση των δικτυακών τόπων που πραγματοποιήθηκε στο Κεφάλαιο 3, λήφθηκε μέριμνα στο να εξεταστεί κατά πόσον μία ιστοσελίδα υποστηρίζει του αλγορίθμους εκείνους που απαιτούσε το σχέδιο προτύπου για το TLS 1.3.

2.3 Δομή του πρωτοκόλλου

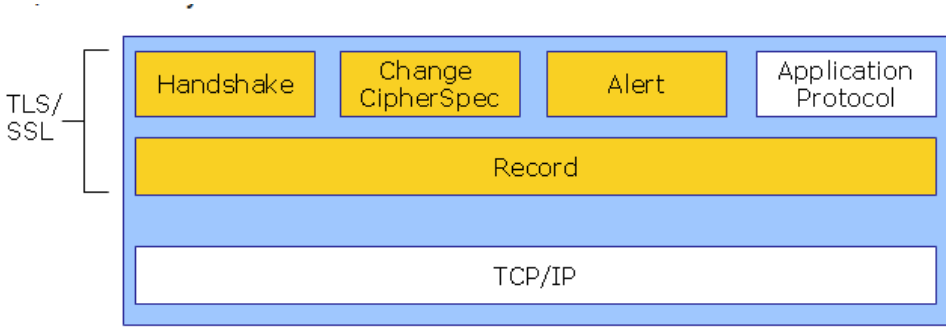
Το πρωτόκολλο ασφαλείας TLS/SSL τοποθετείται μεταξύ του επιπέδου εφαρμογής και του επιπέδου TCP/IP, όπου μπορεί να ασφαλίσει και να στείλει δεδομένα εφαρμογών στο επίπεδο μεταφοράς. Επειδή λειτουργεί μεταξύ του επιπέδου εφαρμογής και του επιπέδου μεταφοράς, το TLS/SSL μπορεί να υποστηρίζει πολλαπλά πρωτόκολλα επιπέδου εφαρμογής [10].

Το TLS/SSL προϋποθέτει ότι χρησιμοποιείται μια connection-oriented transport, συνήθως TCP. Το πρωτόκολλο επιτρέπει σε εφαρμογές πελάτη-διακομιστή να εντοπίζουν τους ακόλουθους κινδύνους ασφαλείας:

- Αλλοιωμένο μήνυμα
- Υποκλοπή μηνυμάτων
- Πλαστά μηνύματα

Το πρωτόκολλο TLS/SSL μπορεί να χωριστεί σε δύο υποεπίπεδα. Το πρώτο επίπεδο αποτελείται από το πρωτόκολλο εφαρμογής και τα τρία υπο-πρωτόκολλα χειραψίας: το πρωτόκολλο Handshake, το πρωτόκολλο Change Cipher Spec και το πρωτόκολλο Alert.

Το δεύτερο επίπεδο είναι το πρωτόκολλο εγγραφής. Η παρακάτω εικόνα απεικονίζει τα διάφορα επίπεδα και τα περιεχόμενα τους.



Εικόνα 2.6: Τα επίπεδα του πρωτοκόλλου TLS/SSL

2.4 Χειραψία TLS

Τα πρωτόκολλα Handshake του TLS/SSL είναι υπεύθυνα για τη δημιουργία ή την επανασύνδεση ασφαλών συνεδριών. Οι κύριοι στόχοι αυτού του επιπέδου είναι:

- Διαπραγματεύεται τις σουίτες κρυπτογράφησης και τους αλγόριθμους συμπίεσης.
- Επαληθεύει τον διακομιστή στον πελάτη και, προαιρετικά, πιστοποιεί τον πελάτη στο διακομιστή μέσω πιστοποιητικών και δημόσιων ή ιδιωτικών κλειδιών.
- Ανταλλάζει τυχαίους αριθμούς και pre-master κλειδιά. Μαζί με ορισμένα άλλα δεδομένα, αυτές οι τιμές θα χρησιμοποιηθούν για τη δημιουργία του κοινόχρηστου μυστικού κλειδιού που θα χρησιμοποιήσει το επίπεδο εγγραφής για την κατακερματισμό και την κρυπτογράφηση των δεδομένων εφαρμογής. Το κοινόχρηστο μυστικό κλειδί καλείται Master Secret.

Τα τρία υπο-πρωτόκολλα χειραψίας είναι:

- Χειραψία (Handshake). Αυτό το δευτερεύον πρωτόκολλο χρησιμοποιείται για τη διαπραγμάτευση των πληροφοριών περιόδου σύνδεσης μεταξύ του πελάτη και του διακομιστή. Οι πληροφορίες περιόδου λειτουργίας αποτελούνται από ένα αναγνωριστικό περιόδου σύνδεσης, τα πιστοποιητικά ομότιμων προσώπων, τις προδιαγραφές κρυπτογράφησης που πρόκειται να χρησιμοποιηθούν, τον

αλγόριθμο συμπίεσης που πρόκειται να χρησιμοποιηθεί και ένα κοινόχρηστο μυστικό που χρησιμοποιείται για την παραγωγή κλειδιών.

- Αλλαγή χαρακτηριστικών κρυπτογράφησης (Change Cipher Spec). Αυτό το υπο-πρωτόκολλο αλλάζει το υλικό κλειδώματος (master-key) που χρησιμοποιείται για την κρυπτογράφηση μεταξύ του πελάτη και του διακομιστή. Το υλικό κλειδώματος είναι ακατέργαστα δεδομένα που χρησιμοποιούνται για τη δημιουργία κλειδιών για κρυπτογραφική χρήση. Το υπο-πρωτόκολλο Change Cipher Spec αποτελείται από ένα μόνο μήνυμα για να πει σε άλλο συμβαλλόμενο μέρος στη σύνοδο TLS/SSL, ο οποίος είναι γνωστός ως ομότιμος, ότι ο αποστολέας θέλει να αλλάξει σε ένα νέο σύνολο κλειδιών. Το κλειδί υπολογίζεται από τις πληροφορίες που ανταλλάσσονται από το υπο-πρωτόκολλο Handshake.
- Συναγερμός (Alert). Αυτό το δευτερεύον πρωτόκολλο χρησιμοποιεί μηνύματα για να υποδείξει μια αλλαγή στην κατάσταση ή μια κατάσταση σφάλματος στο ένα μέλος της επικοινωνίας. Υπάρχει μια μεγάλη ποικιλία ειδοποιήσεων για την ειδοποίηση του ομότιμου χρήστη τόσο για τις κανονικές όσο και για τις συνθήκες σφάλματος. Ένας πλήρης κατάλογος μπορεί να βρεθεί στο RFC 2246 [11]. Οι ειδοποιήσεις αποστέλλονται συνήθως όταν η σύνδεση είναι κλειστή, λαμβάνεται ένα μη έγκυρο μήνυμα, ένα μήνυμα δεν μπορεί να αποκρυπτογραφηθεί ή ο χρήστης ακυρώνει τη λειτουργία.

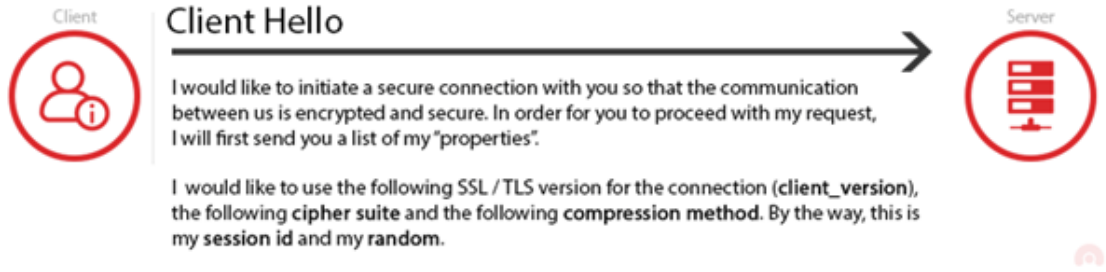
Η χειραψία του πρωτοκόλλου TLS περιλαμβάνει τα παρακάτω βήματα:

2.4.1 Client hello

Η συνηθισμένη εκκίνηση επικοινωνίας σε ένα πρωτόκολλο client-server, ξεκινάει την χειραψία με το μήνυμα Client Hello. Στο πρωτόκολλο SSL/TLS ο πελάτης στέλνει την λίστα με τις εκδόσεις του πρωτοκόλλου που υποστηρίζει καθώς και την επιθυμητή έκδοση (που συνήθως είναι η τελευταία). Για να εκμεταλλευτεί καλύτερα το εύρος ζώνης, ενημερώνει τον διακομιστή ότι χρησιμοποιεί την συγκεκριμένη μέθοδο συμπίεσης. Τέλος αποστέλλονται οι Cipher suites που χρησιμοποιούνται και συγκεκριμένα ο κρυπτογραφικός αλγόριθμος για Key Exchange, Authentication, Bulk (data) Encryption και Message Authentication [12].

Για να γνωρίζει ο διακομιστής αν έχει ξαναμιλήσει με τον πελάτη, αυτός του στέλνει το session_id. Αν το πεδίο αυτό δεν είναι άδειο, τότε έχει υπάρξει μια παλαιότερη επικοινωνία. Τέλος τυχαία δεδομένα μήκους 32-byte από τα οποία τα 4 bytes αναπαριστούν την ημερομηνία και ώρα. Τα υπόλοιπα 28 bytes θα χρησιμοποιηθούν για την δημιουργία του κλειδιού κρυπτογράφησης.

Ο πελάτης έχει την δυνατότητα να ζητήσει επιπλέον λειτουργικότητες από τον διακομιστή. Αυτό γίνεται με την χρήση των επεκτάσεων του πρωτοκόλλου. Αν ο διακομιστής δεν μπορεί να υλοποιήσει τις απαιτήσεις του πελάτη, τότε η διαδικασία της χειραψίας μπορεί να ακυρωθεί από τον πελάτη.



Εικόνα 2.7: Χειραψία με το μήνυμα Client Hello

2.4.2 Server hello

Αφού ο διακομιστής λάβει το μήνυμα Client Hello, το επόμενο βήμα είναι η απάντηση με ένα μήνυμα Server Hello. Εξετάζοντας το μήνυμα που έχει λάβει, αν βρει ένα συμβατό σετ αλγορίθμων που επιθυμεί ο πελάτης, θα απαντήσει δεχόμενος αυτές τις παραμέτρους και στέλνοντας το ψηφιακό πιστοποιητικό του. Αν ο διακομιστής δεν καλύπτει τις απαιτήσεις που του ζητήθηκαν θα απαντήσει στην χειραψία με ένα μήνυμα λάθους.

Στην απάντηση Server Hello που στέλνει περιλαμβάνονται και οι εξής πληροφορίες [13]:

- Server_Version. Ο διακομιστής θα επιλέξει την έκδοση του πρωτοκόλλου SSL/TLS που προτιμάει ο πελάτης.

- Random. Τυχαία δεδομένα μήκους 32-byte από τα οποία τα 4 bytes αναπαριστούν την ημερομηνία και ώρα του διακομιστή. Τα υπόλοιπα 28 bytes θα χρησιμοποιηθούν για την δημιουργία του κλειδιού κρυπτογράφησης.
- Session_Id. Αυτό είναι το αναγνωριστικό για την τρέχουσα σύνοδο. Αν η παράμετρος που έχει στείλει ο πελάτης δεν είναι άδεια, ο διακομιστής θα ψάξει για προηγούμενες αποθηκευμένες για να την συνεχίσει ή θα την καταχωρήσει για μία καινούργια σύνοδο.
- Compression_Methods. Αν υποστηρίζει τις μεθόδους συμπίεσης που ζήτησε ο πελάτης, θα συμφωνήσει στην προτεινόμενη μέθοδο.
- Cipher_Suites. Αν υποστηρίζει τις cipher suite που ζήτησε ο πελάτης, θα συμφωνήσει στην προτεινόμενη μέθοδο.
- Certificate. Το πιστοποιητικό του διακομιστή, το οποίο αποδεικνύει την ταυτότητα του στον πελάτη, μαζί με το δημόσιο κλειδί του.

2.4.3 Server hello done

Αυτό αποστέλλεται στον πελάτη ως επιβεβαίωση ότι ολοκληρώθηκε το μήνυμα Server Hello.

2.4.4 Client Key Exchange

Το μήνυμα Client Key Exchange αποστέλλεται αμέσως μετά τη λήψη του Hello Done από τον διακομιστή. Εάν ο διακομιστής ζητήσει ένα Πιστοποιητικό πελάτη, τότε το Client Key Exchange θα σταλεί μετά από αυτό.

Κατά την διάρκεια αυτού του μηνύματος, ο πελάτης δημιουργεί και το Pre-Master Secret. Αυτό δημιουργείται με βάση την cipher suite που έχει επιλεγεί για να χρησιμοποιηθεί στην συνομιλία. Η αποστολή του Pre-Master Secret, βασίζεται στην ασύμμετρη κρυπτογραφία. Έτσι ο πελάτης το κρυπτογραφεί με το δημόσιο κλειδί του διακομιστή.

2.4.5 Server receives the Pre-Master Secret

Ο διακομιστής λαμβάνει το Pre-Master Secret και χρησιμοποιώντας το ιδιωτικό του κλειδί το αποκωδικοποιεί. Ο εξυπηρετητής και ο πελάτης παράγουν ο καθένας το Master Secret και τα κλειδιά της συνόδου βασισμένα στο Pre-Master Secret και στις τυχαίες τιμές που είχαν ανταλλάξει στα προηγούμενα βήματα με την χρήση μιας ψευδοτυχαίας συνάρτησης [14].

```
master_secret = PRF(pre_master_secret, "master secret", ClientHello.random + ServerHello.random) [0
..47];
```

Εικόνα 2.8: Δημιουργία του Pre-Master Secret

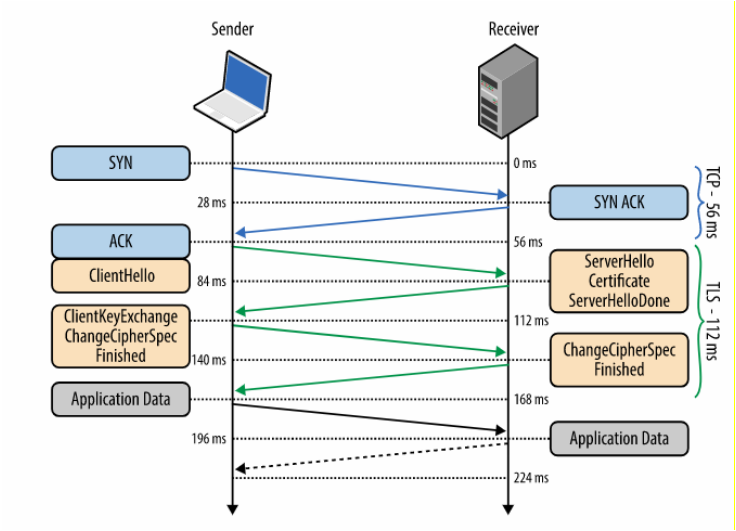
Στην συνέχεια το κύριο κλειδί μήκους 48 bytes που παράχθηκε θα χρησιμοποιηθεί για να πραγματοποιηθεί η συμμετρική κρυπτογράφηση της επικοινωνίας.

2.4.6 Client sends "Change cipher spec

Σε αυτό το σημείο, τόσο ο Πελάτης όσο και ο Διακομιστής είναι έτοιμοι να μεταβούν σε ένα ασφαλές, κρυπτογραφημένο περιβάλλον. Το πρωτόκολλο Change Cipher Spec χρησιμοποιείται για την αλλαγή της κρυπτογράφησης που χρησιμοποιείται από τον πελάτη και τον διακομιστή. Όλα τα δεδομένα που ανταλλάσσονται μεταξύ των δύο πλευρών θα κρυπτογραφηθούν με το συμμετρικό κλειδί που διαθέτουν.

2.4.7 Connection established

Το τελευταίο μήνυμα της διαδικασίας χειραψίας και το πρώτο κρυπτογραφημένο στην ασφαλή σύνδεση είναι το Finished, το οποίο ανταλλάσσεται και από τα δύο μέρη.



Εικόνα 2.9: Σχηματική απεικόνιση της διαδικασίας χειραψίας [15]

2.5 Εφαρμογές

Κατά τη σχεδίαση εφαρμογών, το TLS συνήθως υλοποιείται πάνω από οποιοδήποτε πρωτόκολλο επιπέδου μεταφοράς (OSI level 4), ενθυλακώνοντας πρωτόκολλα εφαρμογών όπως τα HTTP, FTP, SMTP, NNMP & XMMP. Κατά κύριο λόγο έχει χρησιμοποιηθεί πάνω από αξιόπιστα πρωτόκολλα μεταφοράς όπως το TCP, αλλά υπάρχουν και υλοποιήσεις με datagram oriented πρωτόκολλα όπως τα UDP & DCCP/DTLS.

Εξέχουσα εφαρμογή του TLS είναι η χρήση του για την διασφάλιση επικοινωνιών στον παγκόσμιο ιστό με το πρωτόκολλο HTTPS που είναι η ενθυλάκωση του πρωτοκόλλου HTTP από το TLS. Το HTTPS είναι απαραίτητο σε εφαρμογές ηλεκτρονικού εμπορίου και ηλεκτρονικής τραπεζικής. Το πρωτόκολλο SMTP για την αποστολή ηλεκτρονικού ταχυδρομείου προστατεύεται όλο και συχνότερα από το TLS. Οι εφαρμογές αυτές χρησιμοποιούν ψηφιακά πιστοποιητικά για να ταυτοποιήσουν τα εμπλεκόμενα μέλη. Το TLS μπορεί επίσης να χρησιμοποιηθεί για την ενθυλάκωση μιας ολόκληρης στοίβας δικτυακών πρωτοκόλλων, επιτρέποντας έτσι τη δημιουργία ιδεατών εικονικών δικτύων (VPN), με παράδειγμα την περίπτωση του OpenVPN. Σε σύγκριση με παραδοσιακές τεχνολογίες VPN με βάση το IPsec, το TLS προσφέρει πλεονεκτήματα στη διάσχιση firewall και δικτύων με NAT. Το TLS είναι ο κύριος τρόπος προστασίας για το πρωτόκολλο SIP που χρησιμοποιείται σε εφαρμογές δικτυακής τηλεφωνίας VoIP.

2.6 Ευπάθειες-Συμβάντα

Στα χρόνια που υπάρχει η οικογένεια των πρωτοκόλλων SSL/TLS, έχουν ανιχνευτεί διάφορες ευπάθειες και προβλήματα του πρωτοκόλλου, οι οποίες οδήγησαν συνήθως σε επιτυχείς επιθέσεις. Σε παλιότερες υλοποιήσεις, κάποιες αρχές πιστοποίησης δεν όριζαν ρητά την παράμετρο basicConstraints CA = FALSE στα πιστοποιητικά που υπέγραφαν για κόμβους-φύλλα. Σαν αποτέλεσμα τα πιστοποιητικά αυτά μπορούσαν να χρησιμοποιηθούν για να υπογράφουν πλαστά πιστοποιητικά. Επιπλέον, κάποιες πρώιμες εφαρμογές πελάτη (π.χ. Microsoft Internet Explorer 6) δεν έλεγχαν καν το σχετικό πεδίο, πράγμα που μπορεί να χρησιμοποιηθεί για επιθέσεις ενδιάμεσου (man-in-the-middle) σε όλες τις πιθανές συνδέσεις SSL.

Κάποιες υλοποιήσεις, ανάμεσα στις οποίες παλιότερες εκδόσεις του Microsoft Cryptographic API, του Network Security Services και του GnuTLS, σταματούν την ανάγνωση χαρακτήρων μετά τον χαρακτήρα null στο πεδίο ονόματος του πιστοποιητικού, πράγμα που μπορεί να χρησιμοποιηθεί για να ξεγελαστεί η εφαρμογή πελάτη, πιστεύοντας ότι το πιστοποιητικό προήλθε από τον πραγματικό εξυπηρετητή. π.χ. το paypal.com\0.badguy.com θα θεωρούσαν ότι προέρχεται από το paypal.com αντί για το badguy.com.

Οι εφαρμογές πελάτη (π.χ. web browsers) υλοποίησαν μηχανισμούς υποβάθμισης της έκδοσης του πρωτοκόλλου SSL/TLS σε προηγούμενες εκδόσεις για λόγους συμβατότητας. Η προστασία που προσφέρει το SSL/TLS ενάντια στην υποβάθμιση της έκδοσης του πρωτοκόλλου από μία ενεργή επίθεση ενδιάμεσου μπορεί να καταστεί άχρηστη από τέτοιους μηχανισμούς.

Στην έκδοση SSL 2.0 υπάρχουν τα εξής «αδύναμα» σημεία:

- Τα ίδια κρυπτογραφικά κλειδιά χρησιμοποιούνται για την αυθεντικοποίηση των μηνυμάτων και την κρυπτογράφηση.
- Το SSL 2.0 έχει μια αδύναμη κατασκευή MAC που χρησιμοποιεί τη συνάρτηση κατακερματισμού MD5 με ένα μυστικό πρόθεμα, που το καθιστά ευάλωτο σε συγκεκριμένες επιθέσεις (επιθέσεις επέκτασης μήκους).

- Το SSL 2.0 δεν προστατεύει την χειραψία, πράγμα που σημαίνει ότι μια επίθεση υποβάθμισης της έκδοσης μπορεί να μη γίνει καν αντιληπτή.
- Το SSL 2.0 κλείνει την TCP σύνδεση για να σηματοδοτήσει το τέλος των δεδομένων. Αυτό σημαίνει ότι είναι εφικτές επιθέσεις περικοπής. Ο επιτιθέμενος απλά πλαστογραφεί ένα TCP FIN και ο παραλήπτης δεν μπορεί να ξέρει ότι το μήνυμα δεδομένων δε μεταφέρθηκε ολόκληρο. Το SSL 3.0 διορθώνει αυτό το πρόβλημα με μια ρητή προειδοποίηση κλεισίματος.
- Το SSL 2.0 υποθέτει μια μόνο υπηρεσία και ένα πιστοποιητικό για συγκεκριμένο όνομα δικτυακού τόπου, πράγμα που συγκρούεται με το στάνταρ του virtual hosting στου web servers. Αυτό σημαίνει ότι πολλές ιστοσελίδες είναι πρακτικά αδύνατο να χρησιμοποιήσουν SSL.
- Το SSL 2.0 είναι απενεργοποιημένο στους Internet Explorer 7 ή μεγαλύτερο, Mozilla Firefox 2 ή μεγαλύτερο, Opera 9.5 ή μεγαλύτερο και Safari. Ο Mozilla Firefox, αν στείλει ένα TLS ClientHello και δει ότι ο εξυπηρετητής δε μπορεί να ολοκληρώσει τη χειραψία, τότε θα προσπαθήσει να υποβαθμίσει το πρωτόκολλο σε SSL 3.0 με ένα ClientHello σε διαμόρφωση SSL 2.0 προκειμένου να μεγιστοποιήσει την πιθανότητα επιτυχούς χειραψίας με παλιότερους εξυπηρετητές.
- Τροποποιήσεις του αρχικού πρωτοκόλλου όπως το False Start που υιοθετεί ο Google Chrome ή το Snap Start, έχει αναφερθεί ότι εισάγουν περιορισμένες επιθέσεις υποβάθμισης της έκδοσης του πρωτοκόλλου, ή ότι επιτρέπουν παρεμβάσεις στη λίστα με τα cipher suite που στέλνονται από τον πελάτη στον εξυπηρετητή. Ένας επιτιθέμενος μπορεί να επηρεάσει την επιλογή του cipher suite προκειμένου να υποβαθμίσει την ασφάλειά του, επιλέγοντας είτε ένα πιο αδύναμο συμμετρικό αλγόριθμο κρυπτογράφησης ή μια πιο αδύναμη ανταλλαγή κλειδιών.

Τα τελευταία χρόνια με την διαδεδομένη χρήση των πρωτοκόλλων SSL/TLS έχει υπάρξει ένας σημαντικός αριθμός σοβαρών περιστατικών που έχουν αναδείξει ευπάθειες του πρωτοκόλλου ή κακής χρήσης του. Παρακάτω παρουσιάζονται οι σημαντικότερες από αυτές με χρονολογική σειρά [16].

2.6.1 2001

Πλαστά πιστοποιητικά της Microsoft

Το 2001 ένας άγνωστος, παριστάνοντας ότι είναι υπάλληλος της Microsoft, απευθύνθηκε στην VeriSign, εταιρία η οποία εκδίδει ψηφιακά πιστοποιητικά, καταφέρνοντας να αποκτήσει δύο πιστοποιητικά τα οποία είχαν σαν όνομα του ιδιοκτήτη το Microsoft Corporation [17]. Με τον τρόπο αυτό θα μπορούσε να παραπλανήσει κάποιο θύμα, πείθοντας τον ότι το περιεχόμενο που προσπαθεί να τρέξει προέρχεται από την Microsoft.

2.6.2 2008

- Debian RNG Flaw

Οι ερευνητές ανακάλυψαν ότι εξαιτίας ενός σφάλματος στον προγραμματισμό στην δημοφιλή διανομή Linux Debian, το οποίο είχε ενσωματωθεί στην επίσημη έκδοση του λειτουργικού, τα ιδιωτικά κλειδιά που αποθηκεύονταν σε ενημερωμένα συστήματα ήταν ανασφαλή [18].

- Λανθασμένη έκδοση πιστοποιητικού για το login.live.com

Ο Mike Zusman καταχωρεί τη διεύθυνση ηλεκτρονικού ταχυδρομείου sslcertificates@live.com και την χρησιμοποιεί για να αποκτήσει ένα πιστοποιητικό SSL από τον πάροχο Thawte για το live.com της Microsoft.

Η Thawte επέτρεψε την αποστολή μηνυμάτων επικύρωσης για έναν τομέα σε μια διεύθυνση ηλεκτρονικού ταχυδρομείου (sslcertificates@live.com), η οποία δεν προοριζόταν συνήθως ως διεύθυνση διαχειριστή.

- Λανθασμένη έκδοση πιστοποιητικού για την StartCom

Ο Mike Zusman εκμεταλλεύεται ένα ελάττωμα στο web interface της StartCom για να αποκτήσει πιστοποιητικά για τομείς χωρίς κατάλληλη εξουσιοδότηση. Η διεπαφή ιστού της StartCom είχε τυφλή εμπιστοσύνη στους χρήστες, επιτρέποντας την αποστολή ηλεκτρονικών μηνυμάτων επικύρωσης τομέα σε αυθαίρετες διευθύνσεις ηλεκτρονικού ταχυδρομείου για άσχετους τομείς.

- Λανθασμένη έκδοση πιστοποιητικού για την CertStar

Ο Eddy Nigg, διευθυντής τεχνολογίας της StartCom, ανακαλύπτει ότι η CertStar (συνεργάτης της Comodo) εκδίδει πιστοποιητικά χωρίς να επαληθεύει την ιδιοκτησία του τομέα. Επαληθεύοντας την υπόθεσή του, κατάφερε να αποκτήσει πιστοποιητικό για το mozilla.org.

- Ψεύτικη CA

Μια ομάδα ερευνητών με επικεφαλής τον Alex Sotirov και τον Marc Stevens εκμεταλλεύονται τις αδυναμίες MD5 για να εξαπατήσουν το RapidSSL ώστε να τους δώσει το δικό του πιστοποιητικό CA, το οποίο θα μπορούσαν να χρησιμοποιήσουν για την έκδοση πιστοποιητικών για οποιοδήποτε δικτυακό τόπο στον κόσμο. Αναβαθμίστηκε το πιστοποιητικό CA για να αποτραπεί η κατάχρηση του. Το MD5 αποσύρθηκε αμέσως. Οι πλήρεις αδυναμίες του MD5 (συγκρούσεις) ανακαλύφθηκαν αρκετά χρόνια νωρίτερα, το 2004, αλλά οι περισσότεροι στον κόσμο αγνόησαν το εύρημα, γεγονός που ώθησε τους ερευνητές να αναλάβουν δράση [19].

2.6.3 2009

- Ανασφαλής διαπραγμάτευση

Ο Marsh Ray ανακαλύπτει ότι, μέσω επαναδιαπραγμάτευσης, μπορεί να χρησιμοποιηθεί μία σύνδεση TCP για δύο ξεχωριστά κανάλια TLS. Από τη σκοπιά του διακομιστή, υπάρχει μια μόνο ροή δεδομένων. Η εκμετάλλευση είναι δυνατή όταν η μία ροή ανήκει στον χρήστη και η άλλη ανήκει στο θύμα.

- Sslstrip

Ο Moxie Marlinspike κυκλοφορεί το sslstrip για να καταδείξει τον τρόπο με τον οποίο γίνεται παράκαμψη της κρυπτογράφησης, με την παράνομη πρόσβαση στην επικοινωνία του και την εξαπάτηση των τελικών χρηστών πιστεύοντας ότι είναι ασφαλείς [20].

- Επίθεση NUL byte

Στο συνέδριο Black Hat στις ΗΠΑ, ο Dan Kaminsky και ο Moxie Marlinspike επιδεικνύουν, ανεξάρτητα, σιωπηλές επιθέσεις ενδιάμεσων (MITM) που έγιναν δυνατές λόγω λανθασμένου χειρισμού του byte των NUL στις μεγάλες στοίβες SSL / TLS [21].

2.6.4 2010

- Firesheep

Παρόλο που είναι πάντα γνωστό ότι η επικοινωνία απλού κειμένου είναι εγγενώς ανασφαλής, ένα πρόσθετο του Firefox που ονομάζεται Firesheep κέρδισε την προσοχή των ειδικών, αφού έκανε το sidejacking πάρα πολύ εύκολο. Το εργαλείο κατέδειξε την σημασία της ασφάλειας με αποτέλεσμα πολλές εταιρείες να υιοθετούν την κρυπτογράφηση από προεπιλογή [22].

2.6.5 2011

- Comodo

Εννέα πλαστά πιστοποιητικά για επτά πολύ δημοφιλείς τομείς αποκτώνται από κάποιον Hacker που αποκαλείται ComodoHacker. Η επίθεση εντοπίστηκε γρήγορα και τα πιστοποιητικά ανακλήθηκαν μέσα σε λίγες ώρες.

- BEAST

Η επίθεση BEAST χρησιμοποιήθηκε για να εκμεταλλευτεί προβλέψιμα διανύσματα αρχικοποίησης (IVs) στο πρωτόκολλο TLS 1.0. Παρόλο που το πρόβλημα αυτό είχε επιλυθεί στην έκδοση TLS 1.1 που κυκλοφόρησε το 2006 και στο TLS 1.2 το 2008, δεν χρησιμοποιούνται αυτές οι εκδόσεις νεότερων πρωτοκόλλων από όλους. Τα προγράμματα περιήγησης θα υιοθετήσουν το TLS 1.2 περίπου 2 χρόνια μετά από την ανάπτυξή του, ενώ οι εξυπηρετητές πολλά χρόνια μετά. Το BEAST είναι η πρώτη επίθεση που δείχνει πώς η πλούσια λειτουργικότητα του προγράμματος περιήγησης μπορεί να καταχραστεί για να γίνει επίθεση στην κρυπτογράφηση. Πολλές παρόμοιες επιθέσεις θα ακολουθήσουν [23].

- DigiNotar

Μια ελάχιστα γνωστή ολλανδική CA κατέρρευσε θεαματικά, αφού ο ComodoHacker απόκτησε πρόσβαση σε όλα τα συστήματα τους και δημιούργησε εκατοντάδες πλαστά πιστοποιητικά. Η DigiNotar προσπάθησε να το καλύψει, αλλά το περιστατικό αποκαλύφθηκε όταν το δημόσιο κλειδί του Chrome, ήταν ενσωματωμένο σε ένα ψεύτικο πιστοποιητικό Gmail.

2.6.6 2012

- Ανεπαρκής εντροπία ενσωματωμένων συσκευών

Οι ερευνητές μελετούν την ποιότητα των ιδιωτικών κλειδιών στο δημόσιο Διαδίκτυο και ανακαλύπτουν ότι περίπου το 0,5% των κλειδιών RSA και το 1% των κλειδιών DSA μπορούν να εκτεθούν εξαιτίας της ανεπαρκούς εντροπίας κατά τη στιγμή της δημιουργίας. Οι περισσότερες ενσωματωμένες συσκευές επηρεάζονται [24].

- Παύση ανάκλησης πιστοποιητικών από το Chrome

Μετά από πολλά χρόνια στα οποία οι browsers δεν ελέγχουν σωστά για την ανάκληση πιστοποιητικών, η Google τελικά αποφασίζει να απαλλαγεί από τους ελέγχους εντελώς, ακολουθώντας και άλλα προγράμματα περιήγησης. Το αποτέλεσμα είναι ότι είναι πλέον σχεδόν αδύνατο να ανακληθούν τα πιστοποιητικά. Παρόλο που οι προμηθευτές αναπτύσσουν τους δικούς τους μηχανισμούς ανάκλησης, μπορούν να τις χρησιμοποιήσουν μόνο για ένα μικρό αριθμό πιστοποιητικών υψηλού προφίλ [25].

- Flame

Το ιρανικό CERT αποκαλύπτει την ύπαρξη του Flame, ενός κακόβουλου λογισμικού που χρησιμοποιείται σε στοχευμένες επιθέσεις στον κυβερνοχώρο ενάντια στο Ιράν. Το Flame είναι πιθανώς το πρώτο κυβερνο-όπλο που θα μπορούσε να λειτουργήσει ήδη από το 2007. Ύστερα από μία σειρά μελετών και αναλύσεων, διαπιστώθηκε ότι η Flame εκμεταλλεύτηκε μια δική του σύγκρουση MD5 για να αποκτήσει ένα ψεύτικο πιστοποιητικό CA [26].

- CRIME

Οι Duong και Rizzo ανακαλύπτουν μία λειτουργική ευπάθεια η οποία εκμεταλλεύεται τη συμπίεση TLS, ακριβώς όταν κάποια προγράμματα περιήγησης άρχιζαν να την υποστηρίζουν. Η ευπάθεια αυτή διορθώθηκε πολύ γρήγορα [27].

- Πλαστό πιστοποιητικό από την TurkTrust

Το δημόσιο κλειδί του Chrome, με τους μηχανισμούς άμυνας του, εντόπισε ένα πιστοποιητικό που έχει εκδοθεί εσφαλμένα για μια από τις ιδιοκτησίες του. Αργότερα αποδείχθηκε ότι η TurkTrust είχε παραδώσει λανθασμένα δύο πιστοποιητικά CA στους τελικούς χρήστες, ένα πρόβλημα που παρέμεινε χωρίς να έχει εντοπιστεί για 15 μήνες.

2.6.7 2013

- Lucky 13

Οι AlFardan και Paterson δημοσιεύουν την Lucky 13 [28], την επίθεσή τους στις σουίτες κρυπτογράφησης CBC. Στο TLS, η μπλοκ κρυπτογράφηση έχει σχεδιαστεί για να επαληθεύει το plaintext (και όχι το κρυπτογραφημένο κείμενο), το οποίο δημιουργεί μια ευκαιρία για τον επιτιθέμενο να εκτελέσει επιθέσεις με «τυχαίες προσθήκες» (padding oracle).

- RC4

Εμφανίζονται νέες επιθέσεις εναντίον του RC4. Προηγουμένως, θεωρήθηκε ότι οι αδυναμίες RC4 δεν επηρεάζουν πολύ το TLS, αλλά αυτό αποδείχθηκε ότι ήταν λάθος. Η έρευνα αυτή σηματοδοτεί το «θάνατο» του RC4, παρόλο που θα χρειαστούν μερικά χρόνια πριν συμβεί πραγματικά [29].

- TIME

Ο Tal Be'ery παρουσιάζει το TIME, έναν τρόπο κατάχρησης της διαρροής πληροφοριών που προκύπτει από τη συμπίεση HTTP και στη συνέχεια την κρυπτογράφηση [30].

- BREACH

Η επίθεση BREACH εκμεταλλεύεται επίσης τη συμπίεση HTTP που χρησιμοποιείται πριν από την κρυπτογράφηση. Αυτή η επίθεση εκδηλώνεται με ένα εργαλείο PoC που ανακτά τα tokens CSRF από πραγματικές τοποθεσίες σε λιγότερο από ένα λεπτό. Αν και δεν είναι εύκολο να αξιοποιηθεί, η συμπίεση πριν από την κρυπτογράφηση παραμένει πραγματικό πρόβλημα για όλες τις εφαρμογές ιστού [31].

- Bullrun και Edgehill

Ο κόσμος μαθαίνει για το Bullrun (NSA) και το Edgehill (GCHQ), δύο προγράμματα που αποσκοπούν στην ανατροπή των προτύπων κρυπτογράφησης παγκοσμίως [32].

- Dual EC DRBG

Ο διπλός EC DRBG, ένας ψευδοτυχαίος αριθμός που δημιουργήθηκε, τυποποιήθηκε και προωθήθηκε από το NIST, εμπλέκεται ως πιθανή κερκόπορτα (backdoor). Μια επέκταση TLS που ονομάζεται 'Extended Random', που υποβλήθηκε για τυποποίηση από την NSA, εκθέτει έναν μεγάλο αριθμό τυχαίων αριθμών [33].

- Πλαστό πιστοποιητικό από την ANSSI

Το κλείδωμα του δημόσιου κλειδιού του Chrome ανίχνευσε αριθμό πιστοποιητικών που χρησιμοποιήθηκαν κατά τη διαφανή υποκλοπή κρυπτογραφημένης κίνησης στο ANSSI, το γαλλικό γραφείο ασφάλειας δικτύων και πληροφοριών. Λίγο αργότερα, η CA της ANSSI περιορίστηκε στην έκδοση πιστοποιητικών μόνο για τα γαλλικά εδάφη.

2.6.8 2014

- Triple Handshake Attack

Νέα έρευνα που αποκαλείται Triple Handshake Attack δημοσιεύεται και η επαναδιαπραγμάτευση στο TLS πρέπει να διορθωθεί ξανά. Η επίθεση είναι αρκετά ενδιαφέρουσα, αλλά δεν έχει πολύ πρακτικό αντίκτυπο [34].

- Heartbleed

Μια κρίσιμη ευπάθεια στο OpenSSL, μια ευρέως χρησιμοποιούμενη βιβλιοθήκη TLS, εμφανίζεται. Εάν χρησιμοποιηθεί, το Heartbleed επιτρέπει στους επιτιθέμενους να ανακτήσουν από τη μνήμη διαδικασίες σε ευπαθείς διακομιστές, κάτι που συχνά οδηγεί σε αποκάλυψη του ιδιωτικού κλειδιού [35]. Λόγω της τεράστιας δημοσιότητας που πήρε η επίθεση, οι περισσότεροι δημόσιοι διακομιστές διορθώσαν την ευπάθεια σχεδόν αμέσως. Ωστόσο, παραμένει ένας μεγάλος αριθμός ευάλωτων συσκευών. Η μεγαλύτερη συνεισφορά του Heartbleed ήταν ότι κατέδειξε στον κόσμο πόσο σοβαρά υποβαθμισμένο ήταν το έργο OpenSSL στα 20 χρόνια της ύπαρξής του. Τους επόμενους μήνες, μεγάλοι οργανισμοί άρχισαν να συμβάλλουν στο έργο αυτό.

- Πλαστό πιστοποιητικό από την NIC India

Η Google ανίχνευσε διάφορα πλαστά πιστοποιητικά που εκδόθηκαν εξ ονόματός της. Αυτή τη φορά, ήταν αποτέλεσμα ευπάθειας του NICCA, υπαγόμενου στο Εθνικό Κέντρο Πληροφορικής της Ινδίας. Ως αποτέλεσμα, η Chrome εκδίδει πιστοποιητικά μόνο για ορισμένα ινδικά ονόματα τομέα.

- Νέα επίθεση τύπου Bleichenbacher

Ο Christopher Meyer και οι συνεργάτες του παρουσιάζουν τη νέα τους έρευνα, εφαρμόζοντας το Bleichenbacher attach από το 1998 στις σύγχρονες στοίβες του TLS [36].

- Ευπάθεια BERserk

Το BERserk είναι μια επίθεση πλαστής υπογραφής RSA λόγω εσφαλμένης ανάλυσης του ASN.1 στο Mozilla NSS. Είναι ένα σύγχρονο παράδειγμα της επίθεσης Bleichenbacher [37].

- POODLE

Ανακαλύφθηκε ότι το πρωτόκολλο SSL v3 δεν έχει πραγματική άμυνα εναντίων των επιθέσεων μαντέματος (padding oracle attacks). Ευτυχώς, οι επιθέσεις γενικά δεν είναι τόσο εύκολο να πραγματοποιηθούν και ο περισσότερος κόσμος μπορεί να χρησιμοποιήσει καλύτερα πρωτόκολλα. Οι περισσότεροι ιστότοποι συνειδητοποίησαν ότι μπορούν να απενεργοποιήσουν την παλαιότερη έκδοση πρωτοκόλλου χωρίς να γίνει αντιληπτό. Σε απάντηση στο POODLE, τα προγράμματα περιήγησης σταματούν να γυρίζουν στο SSL v3 σε αποτυχία σύνδεσης TLS [38].

- POODLE TLS

Λίγο αργότερα, ανακαλύφθηκε ότι, παρόλο που το TLS 1.0 έχει ενσωματωμένες άμυνες κατά των επιθέσεων μαντέματος, ορισμένες υλοποιήσεις δεν τις εφαρμόζουν σωστά. Αυτό το νέο πρόβλημα ονομάζεται POODLE TLS. Αυτή η ανακάλυψη τονίζει το γεγονός ότι οι περισσότερες υλοποιήσεις πρωτόκολλου δεν δοκιμάζονται σε ανταγωνιστικές συνθήκες [39].

2.6.9 2015

- Superfish

Αποκαλύφθηκε ότι η Lenovo έστειλε μερικούς φορητούς υπολογιστές προεγκατεστημένους με λογισμικό ικανό να υποκλέψει την κρυπτογραφημένη κίνηση από μία CA. Εκτός αυτού, η Lenovo χρησιμοποίησε την ίδια CA root για όλους τους

φορητούς υπολογιστές, πράγμα που σημαίνει ότι οποιοσδήποτε ιδιοκτήτης θα μπορούσε να εξαγάγει το αντίστοιχο ιδιωτικό κλειδί και να το χρησιμοποιήσει έναντι όλων των άλλων συστημάτων. Το Superfish ήταν το πρώτο ευρέως δημοσιευμένο περιστατικό αυτού του τύπου. εντοπίστηκαν αρκετά παρόμοια προβλήματα, για παράδειγμα σε προϊόντα όπως το Komodia και το PrivDog [40].

- Πλαστό πιστοποιητικό από την CNNIC

Το Κέντρο Πληροφοριών Διαδικτύου της Κίνας (CNNIC) εξέδωσε μια υπο CA για δοκιμαστικούς σκοπούς σε μια εταιρεία που ονομάζεται MCS (Mideast Communication Systems), η οποία τη φόρτωσε αμέσως σε μια συσκευή για διαφανή υποκλοπή δικτύου, δημιουργώντας τουλάχιστον ένα πλαστό πιστοποιητικό. Ως αποτέλεσμα, η Google και το Mozilla ανέτρεψαν την εμπιστοσύνη στις ρίζες του CNNIC.

- Λανθασμένη έκδοση πιστοποιητικού για το live.fi

Επτά χρόνια μετά το αρχικό συμβάν πιστοποιητικού live.com, διαπιστώθηκε ότι η Microsoft ξεχάστηκε να κλείσει όλα τα διαχειριστικά γραμματοκιβώτια στο όνομα του live.fi. Ως αποτέλεσμα, ο κάτοχος του γραμματοκιβωτίου μπορούσε να αποκτήσει ένα έγκυρο πιστοποιητικό για αυτό το όνομα τομέα.

- SMACK

Το SMACK είναι ένα αρκτικόλεξο για τα State Machine AttaCKs. Στοχεύει σε αδυναμίες στις εφαρμογές της μηχανής κατάστασης TLS σε διάφορες βιβλιοθήκες [41].

- FREAK

Οι ερευνητές πίσω από την επίθεση FREAK αποκαλύπτουν ότι οποιοσδήποτε διακομιστής που χρησιμοποιεί εξαγώγιμη κρυπτογραφία μπορεί να χρησιμοποιηθεί μέσω ενός ελαττώματος σε διάφορες υλοποιήσεις TLS πελάτη. Αρχικά θεωρήθηκε ότι το

πρόβλημα υπάρχει μόνο με το OpenSSL, αλλά και ο Schannel και η Secure Transport βρέθηκαν αργότερα επίσης ευάλωτες [42].

- Logjam

https://weakdh.org

Το Logjam είναι μια επίθεση εναντίον αδύναμης ανταλλαγής κλειδιών Diffie-Hellman που χρησιμοποιείται από ορισμένους διακομιστές. Στην ουσία, ένας ενεργός επιτιθέμενος δικτύου αναγκάζει τη χρήση μιας αδύναμης σουίτας κρυπτογράφησης (π.χ. μια σουίτα που χρησιμοποιεί παραμέτρους DH 512 bit) και στη συνέχεια υποκλέπτει τη σύνδεση σε πραγματικό χρόνο [43].

- Επιθέσεις τύπου POODLE

Σε δύο δημοσιεύσεις σε blog, με τίτλο «Υπάρχουν περισσότερες POODLE στο δάσος» [44] και «Το POODLE έχει φίλους» [45], ο ερευνητής και προγραμματιστής του TLS Yngve Nysæter Pettersen δημοσίευσε τα αποτελέσματα της έρευνάς του σε προβλήματα εφαρμογής TLS παρόμοια με την επίθεση POODLE.

2.6.10 2016

- SLOTH

Οι ερευνητές από το INRIA παρουσίασαν το SLOTH (Security Losses from Obsolete and Truncated Transcript Hashes, CVE-2015-7575), γεγονός που εκμεταλλεύεται το γεγονός ότι πολλοί πελάτες και εξυπηρετητές εξακολουθούν να υποστηρίζουν υπογραφές RSA-MD5, παρόλο που θεωρούνται πλέον ανασφαλείς [46].

- DROWN

Οι ερευνητές δημοσιεύουν το DROWN, έναν νέο τρόπο εκμετάλλευσης του πρωτοκόλλου SSL v2. Εκτιμάται ότι περίπου το 33% όλων των εξυπηρετητών HTTPS επηρεάστηκαν κατά τη στιγμή της αποκάλυψης. Μια ενδιαφέρουσα πτυχή αυτής της επίθεσης είναι ότι ακόμη και οι διακομιστές που δεν διαθέτουν SSL v2 μπορούν να επηρεαστούν εάν επαναχρησιμοποιήσουν κλειδιά RSA ή και πιστοποιητικά που χρησιμοποιούνται από διακομιστές SSL v2 αλλού [47].

- SWEET32

Μια νέα επίθεση που ονομάζεται Sweet32 καταδεικνύει τις αδυναμίες των ciphers που χρησιμοποιούν μπλοκ 64 bit, που εκμεταλλεύονται μέσω του παράδοξου των γενεθλίων. Ciphers όπως το 3DES και το Blowfish, προεπιλογή στο OpenVPN, επηρεάζονται.

- WoSign και StartCom

Η Apple, το Chrome και η Mozilla αποφάσισαν ότι δεν είναι πλέον δυνατή η εμπιστοσύνη των WoSign και StartCom. Αυτή η ενέργεια αποτελεί αποκορύφωμα μιας μακράς έρευνας και πολλαπλών παραβιάσεων κανόνων από αυτές τις CA. Ο ριζικός κατάλογος αποθηκεύει όλες τις προσπάθειες που έγιναν για να εξασφαλιστεί η ομαλή μετάβαση σε έμπιστα υπάρχοντα πιστοποιητικά.

2.6.11 2017

- Πιστοποιητικά της Symantec

Τον Μάρτιο του 2017, η Google αποκάλυψε τα σχέδιά της για ανάκληση της εμπιστοσύνης της στα υπάρχοντα πιστοποιητικά της Symantec. Ακολούθησαν πολλοί μήνες συζήτησης. Μέχρι τον Αύγουστο, η Google και η Mozilla συμφώνησαν σε μικρότερες κυρώσεις σε αντάλλαγμα για την έκδοση των πιστοποιητικών της Symantec σε τρίτη εταιρία. Η Symantec όχι μόνο επέλεξε τη DigiCert για την έκδοση, αλλά αποφάσισε επίσης να μεταφέρει όλη την πιστοποίησή τους σε αυτές.

- ROBOT

Το Return of Bleichenbacher's Oracle Threat (ROBOT) Attack είναι μια παραλλαγή της κλασσικής επίθεσης Bleichenbacher εναντίον του RSA - η οποία είναι μία από τις μεθόδους κρυπτογράφησης που χρησιμοποιεί το TLS. Μια επιτυχημένη επίθεση επιτρέπει σε έναν εισβολέα να αποκρυπτογραφήσει την επικοινωνία μεταξύ ενός χρήστη και ενός διακομιστή εάν αυτή η επικοινωνία ήταν κρυπτογραφημένη με έναν αλγόριθμο RSA. Επιπλέον, ο εισβολέας θα μπορούσε να δημιουργήσει και να υπογράψει οποιοδήποτε μήνυμα χρησιμοποιώντας το ιδιωτικό κλειδί του διακομιστή. [48]

- Διαρροή του ιδιωτικού κλειδιού για προγράμματα ERP της Microsoft

Η Microsoft χρησιμοποιούσε το ίδιο ιδιωτικό κλειδί για την απομακρυσμένη σύνδεση μέσω RDP στους διακομιστές του Azure [49], που φιλοξενούσαν το την εφαρμογή ERP [50]. Έτσι όταν ένας ερευνητής κατάφερε να εξάγει το ιδιωτικό κλειδί, μπορούσε ουσιαστικά να συνδεθεί σε όλους τους εικονικούς διακομιστές.

2.6.12 2018

Διαρροή ιδιωτικών κλειδιών της Trustico

Η εταιρία Trustico η οποία εκδίδει πιστοποιητικά SSL/TLS, παραδέχτηκε ότι έχουν εκτεθεί τα ιδιωτικά κλειδιά 23000 πιστοποιητικών [51] ζητώντας την ανάκληση τους.

2.7 Ευρωπαϊκός Κανονισμός για την Προστασία Γενικών Δεδομένων (GDPR)

Ο νέος Ευρωπαϊκός Κανονισμός για την Προστασία Γενικών Δεδομένων (GDPR) τίθεται σε ισχύ με σημαντικές αλλαγές σε σχέση με το προηγούμενο εφαρμοζόμενο πλαίσιο, που με τη σειρά τους θα οδηγήσουν σε λειτουργικές αλλαγές στις επιχειρήσεις/οργανισμούς, σε διαρθρωτικές απαιτήσεις αλλά και σε αλλαγές στην κουλτούρα διαχείρισης πληροφοριών. Βασική στόχευση του νέου πλαισίου που τίθεται σε ισχύ την 25η Μάϊου του 2018, συνιστά η συμμόρφωση με τους κανόνες και τη δεοντολογία διαχείρισης της πληροφορίας και των προσωπικών δεδομένων ανάλογα με το σκοπό τήρησης, το

πρόσωπο που αφορούν, και το αποτέλεσμα της επεξεργασίας τους. Μεταξύ των απαιτούμενων μέτρων προς την κατεύθυνση αυτή είναι ο καθορισμός των εμπλεκόμενων ανθρώπινων και φυσικών πόρων/ μέσων για την ασφαλή διαχείριση, επεξεργασία και τήρηση των δεδομένων, η διασφάλιση της αποφυγής κατάχρησης των δεδομένων πέραν της ενδεδειγμένης και προκαθορισμένης χρήσης τους και κυρίως η λήψη αποτελεσματικών τεχνικών, λειτουργικών, και κανονιστικών μέτρων για τον περιορισμό του κινδύνου παραβιάσεων του Κανονισμού.

Όλα αυτά, υπό την ευθύνη κατάλληλα εκπαιδευμένων επαγγελματιών που θα μπορούν να συνεισφέρουν στην αναπροσαρμογή των διαδικασιών του οργανισμού τους προς την κατεύθυνση αυτή και να εποπτεύουν τη διαρκή εναρμόνιση του οργανισμού με τα απαιτούμενα. Ειδικότερα, σύμφωνα με τα προβλεπόμενα από τον Κανονισμό, ο Υπεύθυνος Προστασίας Δεδομένων (Data Protection Officer – DPO) έχει κρίσιμο συμβουλευτικό ρόλο στον τομέα της ασφάλειας και της διαχείρισης των πληροφοριών αλλά και για το σχεδιασμό της στρατηγικής και την εφαρμογής των διαδικασιών για την προστασία προσωπικών δεδομένων, αναφορικά με τις νέες απαιτήσεις. Ο DPO είναι, τέλος, το σημείο επαφής μεταξύ της εταιρείας/ Οργανισμού και των εποπτικών αρχών.

Μία εκ των σημαντικών αλλαγών που επιφέρει ο GDPR είναι η ανάγκη εκτέλεσης συγκεκριμένων ενεργειών σε περίπτωση που λάβει χώρα περιστατικό παραβίασης προσωπικών δεδομένων. Αυτό με τη σειρά του θέτει πρόσθετες υποχρεώσεις και ως προς την ασφάλεια των διαδικτυακών τόπων.

Κεφάλαιο 3

Ανάλυση επιπέδου ασφάλειας Ιστοτόπων

3.1 Εισαγωγή

Πρώτος στόχος της παρούσας μεταπτυχιακής διατριβής είναι να ερευνήσει και να καταγράψει την πραγματική κατάσταση που επικρατεί στον ελληνικό κυβερνοχώρο. Για το σκοπό αυτό επιλέχθηκαν οι σημαντικότερες κατηγορίες ιστοσελίδων με τις αντίστοιχες δημοφιλέστερες ιστοσελίδες. Για τις ιστοσελίδες αυτές έγινε ανάλυση με δύο διαφορετικά εργαλεία, για επιβεβαίωση των αποτελεσμάτων και για ολοκληρωμένη έρευνα, και ερευνήθηκαν οι πιο σημαντικές ευπάθειες αλλά και άλλες πληροφορίες που έχουν ερευνητική αξία. Στην συνέχεια παρουσιάζονται αναλυτικά τα ευρήματα και αναδεικνύονται τα σημαντικότερα συμπεράσματα.

3.2 Μεθοδολογία

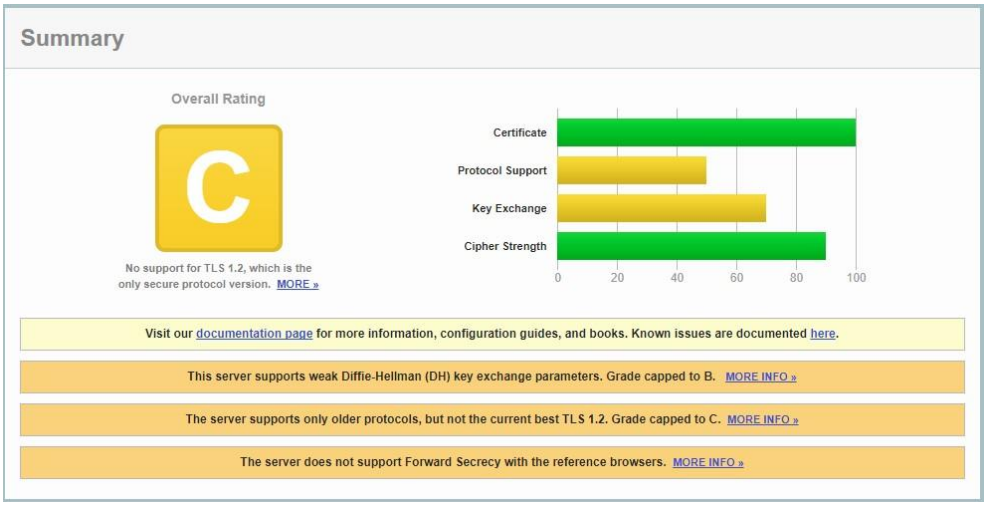
Για την καταγραφή της κατάστασης, σχετικά με τις υλοποιήσεις ασφαλείας και ειδικότερα των πρωτοκόλλων SSL/TLS, στην Ελλάδα, έγινε έλεγχος στις πιο δημοφιλείς ελληνικές ιστοσελίδες. Συγκεκριμένα έγινε επιλογή 241 ιστοσελίδων (Παράρτημά Α) , με βάση την επισκεψιμότητα τους όπως αυτή εμφανίστηκε το Φεβρουάριο του 2018. Για τον σκοπό αυτό χρησιμοποιήθηκε το εργαλείο Alexa [52], το οποίο αποτελεί ένα από τα πιο έγκυρα εργαλεία μέτρησης της επισκεψιμότητας των ιστοσελίδων διεθνώς. Στην συνέχεια, αφού επιλέχθηκαν επτά κατηγορίες, έγινε ανάλυση και αξιολόγηση της διαμόρφωσης των πρωτοκόλλων SSL/TLS με την χρήση δύο εργαλείων. Η μεθοδολογία

που ακολουθήσαμε είναι ανάλογη με αυτή που έχει ακολουθηθεί και από άλλους ερευνητές [53], για να αξιολογηθούν ιστότοποι ως προς το SSL/TLS που υλοποιούν.

3.2.1 Εργαλείο A (SSL Labs)

Το πρώτο εργαλείο που χρησιμοποιήθηκε δημιουργήθηκε από την Qualys SSL Labs [54]. Αποτελεί ένα από τα δημοφιλέστερα εργαλεία ελέγχου του SSL για τις τελευταίες ευπάθειες και συνήθη λάθη ρυθμίσεων. Έχει παρουσιαστεί σε σημαντικά παγκόσμια συνέδρια ασφαλείας [55] και έχει χρησιμοποιηθεί σε ανάλογες μελέτες [56–58]. Μερικές από τις παραμέτρους που ελέγχονται είναι ο εκδότης του πιστοποιητικού, η εγκυρότητά του, ο αλγόριθμος που χρησιμοποιείται για την υπογραφή του πιστοποιητικού, τα πρωτόκολλα και οι κρυπτογραφικές σουίτες (cipher suites) που υποστηρίζει, οι ενεργοποιημένες δυνατότητες, οι γνωστές αδυναμίες και άλλα.

Τα αποτελέσματα του ελέγχου παρέχουν λεπτομερείς τεχνικές πληροφορίες οι οποίες μπορούν να αποτελέσουν πολύτιμο εργαλείο στα χέρια διαχειριστών συστημάτων, μηχανικών ασφαλείας και ελεγκτών για να ενημερωθούν και να επιλύσουν πιθανές αδυναμίες. Στην Εικόνα 3.10 φαίνεται η μορφή της αναφοράς που παράγεται.



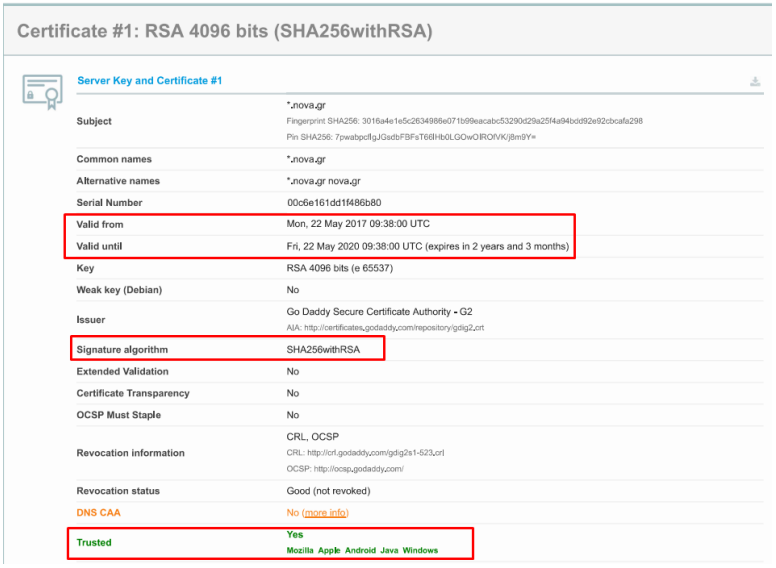
Εικόνα 3.10 Αναφορά αξιολόγησης ιστοτόπου με το εργαλείο A (SSL Labs)

Παρατηρούμε ότι κατά την δημιουργία της αναφοράς, η ιστοσελίδα έχει βαθμολογηθεί. Η βαθμολόγηση, η οποία περιγράφεται λεπτομερώς από τα ssllabs [59], υπολογίζει μία βαθμολογία για κάθε κατηγορία όπως τα υποστηριζόμενα πρωτόκολλα, τους αλγορίθμους, τη διαδικασία ανταλλαγής κλειδιού κλπ. Στην συνέχεια υπολογίζει το συνολικό σκορ, που αντιπροσωπεύεται με ένα γράμμα εντός μίας συγκεκριμένης κλίμακας, όπως φαίνεται στην Εικόνα 3.11, με τις + και – διακυμάνσεις τους. Υπάρχουν σαφείς οδηγίες, για να μπορέσει μια ιστοσελίδα να καταφέρει τον μέγιστο βαθμό αξιολόγησης, με την χρήση του συγκριμένου εργαλείου [60].

Numerical Score	Grade
score >= 80	A
score >= 65	B
score >= 50	C
score >= 35	D
score >= 20	E
score < 20	F

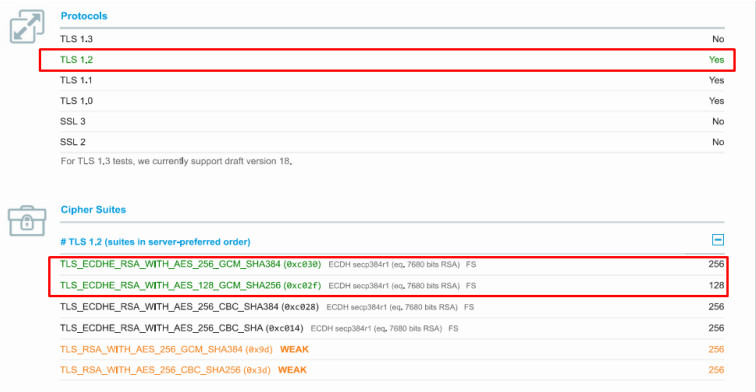
Εικόνα 3.11 Βαθμολογική κλίμακα αξιολόγησης ιστοτόπου με το εργαλείο A (SSL Labs)

Στην συνέχεια παρουσιάζονται πληροφορίες για το πιστοποιητικό της ιστοσελίδας, όπως η ημερομηνία δημιουργίας και λήξης, το μήκος του κλειδιού, αν είναι έγκυρο κλπ. (Εικόνα 3.12).



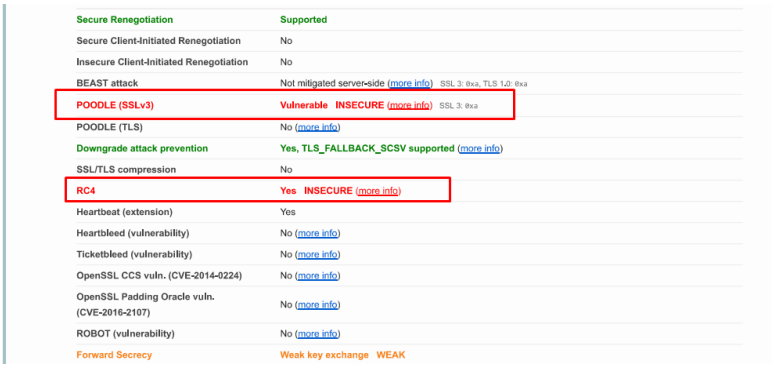
Εικόνα 3.12 Αναφορά του εργαλείου A σχετικά με το πιστοποιητικό της ιστοσελίδας

Πολύ σημαντικό σε έναν έλεγχο είναι η καταγραφή των εκδόσεων SSL/TLS που υποστηρίζονται, καθώς και των αντίστοιχων αλγόριθμων κρυπτογράφησης (Εικόνα 3.13).



Εικόνα 3.13 Αναφορά του εργαλείου A σχετικά με τους αλγόριθμους κρυπτογράφησης

Στο τέλος της αναφοράς καταγράφονται οι σημαντικότερες ευπάθειες της οικογένειας των πρωτοκόλλων και το αντίστοιχο αποτέλεσμα του ελέγχου που διενεργήθηκε (Εικόνα 3.14).



Εικόνα 3.14 Συνοπτική αναφορά των ευπαθειών που εντοπίστηκαν σύμφωνα με το εργαλείο A

3.2.2 Εργαλείο Β (High-Tech Bridge)

Για καλύτερη θεμελίωση των αποτελεσμάτων της μεταπτυχιακής διατριβής αλλά και για πληρέστερη συλλογή στοιχείων, έγινε έλεγχος όλων των ιστοσελίδων και με ένα δεύτερο εργαλείο. Το δεύτερο εργαλείο που χρησιμοποιήθηκε ήταν αυτό που παρέχει η High-Tech Bridge [61]. Οι πληροφορίες που συλλέγονται είναι ενδελεχείς και περιλαμβάνουν τα υποστηριζόμενα πρωτόκολλα, τους αλγόριθμους κρυπτογράφησης που υποστηρίζονται, καθώς επίσης τους προτιμώμενους αλγόριθμους κρυπτογράφησης. Επιπλέον η ιστοσελίδα αξιολογείται στο αν καλύπτει τα κριτήρια τριών διεθνών προτύπων: PCI DSS [62], NIST [63] και HIPAA [64]. Το εργαλείο αυτό έχει χρησιμοποιηθεί και σε παρόμοιες μελέτες [53,65,66] και μάλιστα συγκριτικά και με το πρώτο που επιλέξαμε.

Η φιλοσοφία του εργαλείου είναι ανάλογη με το πρώτο, καθώς βαθμολογεί τις ιστοσελίδες όπως φαίνεται στην Εικόνα 3.15.

Grade	Score
A+	Score greater than 99
A	Score between 90 and 99
A-	Score between 80 and 89

Grade	Score
B+	Score between 70 and 79
B	Score between 60 and 69
B-	Score between 50 and 59

Grade	Score
C+	Score between 35 and 49
C	Score between 20 and 34
F	Score lower than 20

Εικόνα 3.15 Βαθμολογική κλίμακα εργαλείου Β (High-Tech Bridge)

Η βαθμολογία παράγεται από μία προκαθορισμένη λίστα [61], η οποία περιέχει θετικές και αρνητικές βαθμολογίες (Εικόνα 3.16). Έτσι η αξιολόγηση μιας ιστοσελίδας ξεκινάει από το 100 και αναλόγως τις αδυναμίες που εντοπίζονται ή τις σωστές πρακτικές που εφαρμόζονται προκύπτει η τελική βαθμολογία (Εικόνα 3.17).

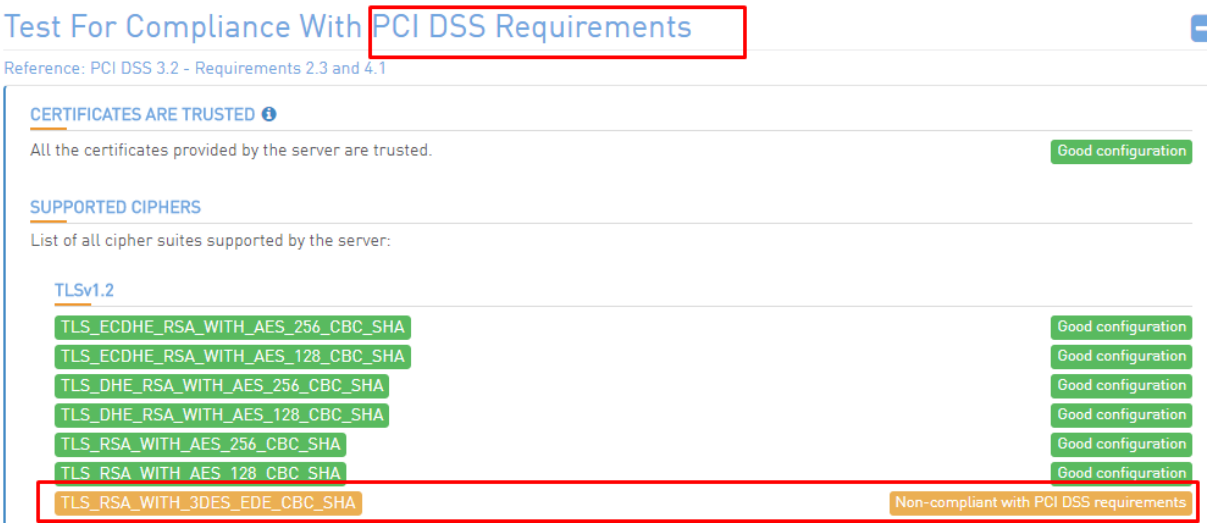
Scoring

Description	Score
Certificate is an Extended Validation (EV) certificate	+10 points
HTTP website redirects to HTTPS (Always-On SSL)	+10 points
Server prefers cipher suites providing strong Perfect Forward Secrecy (PFS)	+10 points
Server provides TLS_Fallback_SCSV extension	+10 points
Server implements HTTP Strict Transport Security (HSTS) with long duration	+10 points
Server implements HTTP Public Key Pinning (HPKP) with long duration	+10 points
Server X509 certificate is prior to version 3	-5 points
Server certificate has been issued for more than 3 year period	-5 points

Εικόνα 3.16 Δείγμα από σημεία αξιολόγησης του εργαλείου B (High-Tech Bridge)

Εικόνα 3.17 Αναφορά αξιολόγησης ιστοτόπου με το εργαλείο B (High-Tech Bridge)

Στην συνέχεια καταγράφονται οι πληροφορίες που ελέγχονται για να καθοριστεί αν είναι συμβατή η ιστοσελίδα με τα πρότυπα PCI DSS, NIST και HIPAA (Εικόνα 3.18).



Εικόνα 3.18 Παράδειγμα ελέγχου συμμόρφωσης με το πρότυπο PCI DSS.

3.2.3 Πληροφορίες που καταγράφηκαν

Όπως αναφέρθηκε παραπάνω, οι πληροφορίες που καταγράφονται στις αναφορές από τα δύο εργαλεία είναι λεπτομερείς και σε βάθος. Για να καταστεί εφικτό να σχηματιστεί μία αντιπροσωπευτική εικόνα των ελληνικών ιστοσελίδων, έγινε μια επιλογή των πληροφοριών που θα αναλυθούν στις παρακάτω ενότητες. Συνεπώς έχουν επιλεγεί οι παρακάτω πληροφορίες:

- Χρήση του RC4. Από την έκδοση 1.1 του TLS ο αλγόριθμος RC4 δεν προτείνεται η χρήση του, λόγω των αδυναμιών του.
- Χρήση αδύναμων παραμέτρων Diffie-Hellman (Weak DH). Είναι πολύ σημαντικό το ιδιωτικό κλειδί του διακομιστή να είναι αρκετά ισχυρό, για να καθιστά την επικοινωνία πιο ασφαλή και πιο δύσκολη την ανάκτηση του από τους επιτιθέμενους.
- Error Forward Secrecy. Στην κρυπτογραφία είναι πολύ σημαντικό, αν κάποια στιγμή αποκαλυφθούν τα μακροπρόθεσμα κλειδιά που χρησιμοποιούνται σε μία επικοινωνία, να μην μπορούν να ανακτηθούν τα προηγούμενα κλειδιά της συνόδου. Η δυνατότητα αυτή ονομάζεται Forward Secrecy (FS) ή Perfect Forward Secrecy (PFS) [67,68].
- Error Authenticated Encryption. Η Authenticated Encryption With Associated Data είναι μια μορφή κρυπτογράφησης που παρέχει συγχρόνως

εμπιστευτικότητα, ακεραιότητα και διαβεβαιώσεις γνησιότητας στα δεδομένα. Αυτά τα χαρακτηριστικά παρέχονται σε μια ενιαία, εύχρηστη διεπαφή προγραμματισμού [69].

- Υποστήριξη στα πρωτόκολλα SSL V3 και SSL V2. Είναι γνωστή η αδυναμία των δύο εκδόσεων του πρωτοκόλλου και η χρήση τους καθιστά τους ιστοτόπους ιδιαίτερα ανασφαλείς.
- Untrust. Σε διάφορες ιστοσελίδες ενώ υλοποιείται το πρωτόκολλο SSL/TLS, σε κάποιες περιπτώσεις αυτό είναι αναξιόπιστο, όταν για παράδειγμα έχει λήξει, δεν επαληθεύεται η ακολουθία των αρχών πιστοποίησης κλπ.
- Mismatch. Τέλος ενώ κάποιο πιστοποιητικό έχει εκδοθεί για έναν ιστότοπο, χρησιμοποιείται σε έναν άλλο, καθιστώντας το αναντίστοιχο.
- Συμβατότητα με την έκδοση TLS 1.3. Για να καθοριστεί αν η ιστοσελίδα είναι συμβατή με την καινούργια έκδοση 1.3 του TLS [70], καταγράφτηκε αν στους αλγόριθμους κρυπτογράφησης που υποστηρίζει, περιλαμβάνονται αυτοί που μέχρι τώρα είναι γνωστό ότι θα υποστηρίζονται:
    - TLS13-AES128-GCM-SHA256
    - TLS13-AES256-GCM-SHA384
    - TLS13-CHACHA20-POLY1305-SHA256
    - TLS13-AES128-CCM-SHA256
    - TLS13-AES128-CCM-8-SHA256

Επιπλέον καταγράφηκε η ύπαρξη ή μη των σημαντικότερων και πιο διαδεδομένων ευπαθειών του πρωτοκόλλου ή υλοποιήσεων αυτού:

- Poodle
- Drown
- ROBOT
- FREAK
- OpenSSL padding-oracle flaw
- HeartBleed

Τέλος καταγράφηκε η συμβατότητα με τρία διεθνή πρότυπα ασφαλείας - οδηγιών, από διάφορους τομείς:

- PCI DSS. Η πιστοποίηση αυτή είναι μία από τις μεγαλύτερες στον χώρο της ασφάλειας πληροφοριών και κυρίως σε ιστοσελίδες που κάνουν χρήση πιστωτικών καρτών [71,72].
- NIST. Το Εθνικό Ινστιτούτο Πρότυπων και Τεχνολογίας (NIST) των Ηνωμένων Πολιτειών της Αμερικής, παρέχει μία σειρά οδηγιών για τον τρόπο που πρέπει να υλοποιηθεί το πρωτόκολλο TLS σε μια ιστοσελίδα για να παρέχει την μέγιστη ασφάλεια [73].
- HIPAA. Το Αμερικανικό Υπουργείο Υγείας εξέδωσε το 1996 έναν νόμο, στο δεύτερος μέρος του οποίου καθορίζονται οι προδιαγραφές και οι απαιτήσεις για τις ηλεκτρονικές υπηρεσίες υγείας [74].

3.3 Κατηγορίες

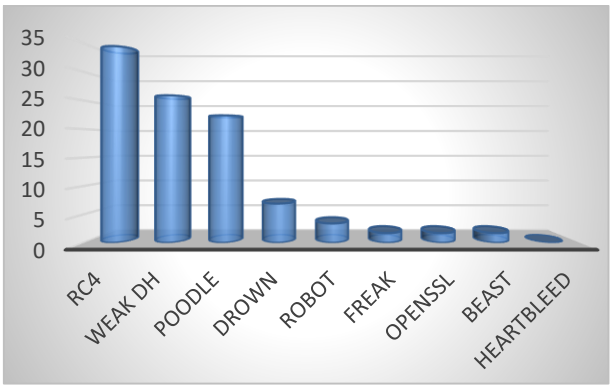
Εξαιτίας του μεγάλου αριθμού ελληνικών ιστοσελίδων, προέκυψε η ανάγκη να γίνει επιλογή των κατηγοριών που θα γίνονταν ανάλυση. Οι κατηγορίες που επιλέχθηκαν είναι:

- Ηλεκτρονικά καταστήματα (E-shops). Η κατηγορία αυτή είναι από τις πιο σημαντικές που ελέγχθηκαν, καθώς το σύνολό τους παρέχει τη δυνατότητα σύνδεσης (login) για την καταχώρηση της παραγγελίας.
- Εταιρείες. Εδώ βρίσκονται οι ιστοσελίδες των μεγαλύτερων εταιριών της Ελλάδας.
- Ενημερωτικά. Οι ιστοσελίδες της κατηγορίες αυτής, παρόλο που δεν γίνονται συναλλαγές, αποτελούν τις πιο δημοφιλείς ιστοσελίδες, με την μεγαλύτερη επισκεψιμότητα.
- Τηλεπικοινωνίες. Λόγω του ειδικού νομικού καθεστώτος που τις διέπει αλλά και της επικείμενης εφαρμογής του νέου Γενικού Κανονισμού Προστασίας Δεδομένων [75], έγινε επιλογή των τηλεπικοινωνιακών οργανισμών.
- Εκπαίδευση. Σχεδόν όλα τα εκπαιδευτικά ιδρύματα παρέχουν ηλεκτρονικές υπηρεσίες, οι οποίες προϋποθέτουν την σύνδεση του χρήστη.

- Οικονομικές υπηρεσίες. Η πιο σημαντική κατηγορία καθώς οι οικονομικές συναλλαγές μπορούν να οδηγήσουν σε επικίνδυνες καταστάσεις, αν δεν παρέχονται οι απαραίτητες προϋποθέσεις ασφαλείας.
- Δημόσιοι οργανισμοί. Τέλος αναλύθηκαν οι ιστοσελίδες των μεγαλύτερων δημοσίων οργανισμών.

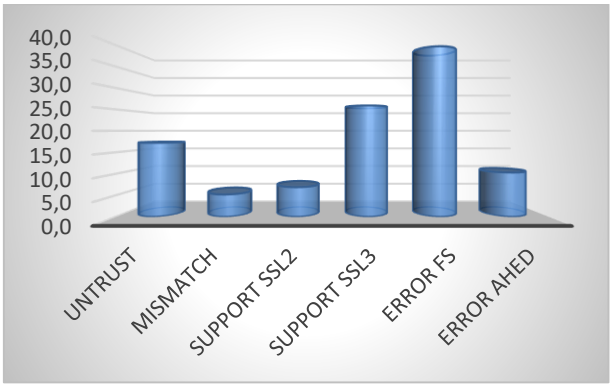
3.3.1 E-Shop

Στην κατηγορία ιστοτόπων "e-shop" αναλύθηκαν συνολικά 58 ιστότοποι. Συγκεκριμένα, οι ευπάθειες του πρωτοκόλλου TLS με φθίνουσα σειρά είναι: RC4 (34,5%), weak DH (25,9%), Poodle (22,4%), Drown(6,9%) και ROBOT (3,4%). Ακόμη όσον αφορά τις ευπάθειες FREAK, OpenSSL padding-oracle flaw και HeartBleed εμφανίστηκαν σε ποσοστό 1,7 % των ιστοτόπων, εκ των οποίων δεν εντοπίστηκε σε καμία περίπτωση η ευπάθεια HeartBleed (Διάγραμμα 3.1).



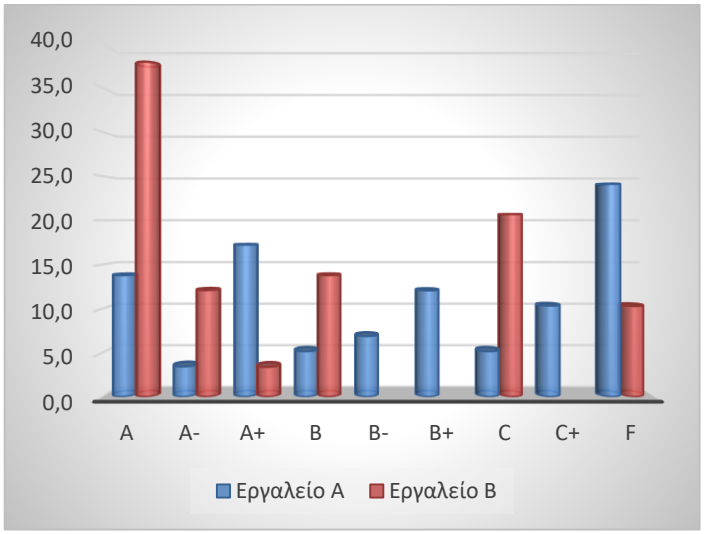
Διάγραμμα 3.1 Ποσοστό (%) των ευπαθειών του πρωτοκόλλου TLS (RC4, Weak DH, Poodle, Drown, ROBOT, Freak, OpenSSL, HeartBleed, Beast) στην κατηγορία ιστοτόπων "e-shop".

Όσον αφορά το ποσοστό εμφάνισης αδυναμιών στη διαμόρφωση του https, είναι με φθίνουσα σειρά Error Forward Secrecy (39,7%), Support SSL V3 (25,9%), Untrust (17,2%), Error Authenticated Encryption (10,3%), Support SSL V2 (6,9%) και Mismatch (5,2%) (Διάγραμμα 3.2).



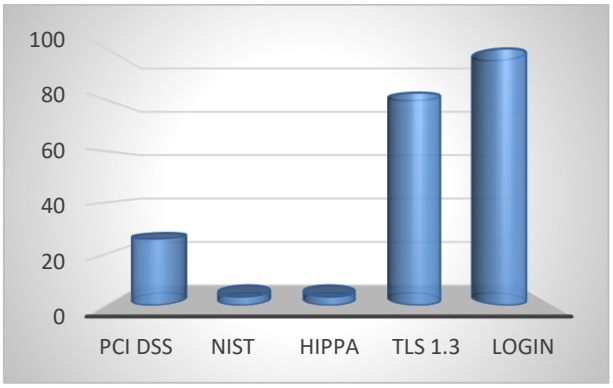
Διάγραμμα 3.2 Ποσοστό (%) των αδυναμιών της διαμόρφωσης του πρωτοκόλλου TLS (Untrust, Mismatch, Support SSL2, Support SSL3, Error FS, Error AHED) στην κατηγορία ιστοτόπων "e-shop".

Από την ανάλυση της βαθμολογίας των ιστοτόπων "e-shop" που χρησιμοποιούν SSL/TLS, προέκυψε ότι με την χρήση του εργαλείου Α, η πλειοψηφία αυτών αξιολογήθηκε με τον βαθμό 'A' (37,9%) και ακολουθούν οι βαθμοί 'C' (20,7%), 'B' (13.8%), 'A-' (12.1%), 'F' (10.3%) και 'A+' (3,4%). Η αντίστοιχη βαθμολογία με την χρήση του εργαλείου Β είναι: 'A+' (17,2%), 'A' (13,8%), 'B+' (12,1%), 'C+' (10,3%), 'B-' (6,9%), 'B' και 'C' (5,2%) και 'A-' (3,4%) (Διάγραμμα 3.3).



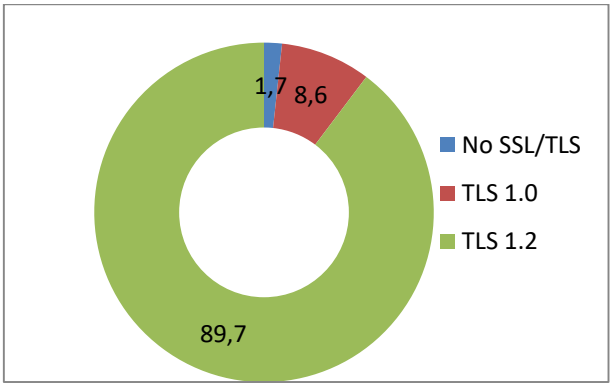
Διάγραμμα 3.3 Ποσοστό (%) της βαθμολογίας που έλαβαν οι ιστότοποι της κατηγορίας "e-shop" μετά την ανάλυσή τους όσον αφορά την ασφάλεια που παρέχουν με τα εργαλεία Α (μπλε μπάρες) και Β (κόκκινες μπάρες).

Το σύνολο των ιστοτόπων της κατηγορίας “e-shop” έδιναν την δυνατότητα στον χρήστη να πραγματοποιήσει σύνδεση (Login) (100%) και η πλειοψηφία αυτών (82,8%) είχε την δυνατότητα να μεταβεί στην έκδοση 1.3 του πρωτοκόλλου TLS. Η συμμόρφωση με τα διεθνή πρότυπα PCI DSS, NIST και HIPAA, καταγράφηκε σε ποσοστά 25,9%, 3.4% και 3,4 αντίστοιχα (Διάγραμμα 3.4).



Διάγραμμα 3.4 Ποσοστό (%) της συμμόρφωσης με διεθνή πρότυπα (PCI, NIST, HIPPA), ετοιμότητας για μετάβαση στην έκδοση του πρωτόκολλου TLS 1.3, καθώς και την δυνατότητα εγγραφής (Login), στην κατηγορία ιστοτόπων “e-shop”.

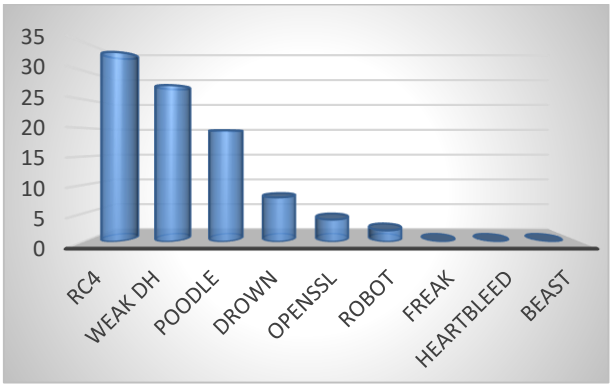
Η πλειοψηφία των ιστοτόπων υποστηρίζουν ως νεότερη έκδοση του πρωτοκόλλου TLS την 1.2 (89,7%), (8,6%) την έκδοση 1.0 ενώ υπήρχε και ένα μικρό ποσοστό (1,7%) το οποίο δεν εφάρμοζε κανένα πρωτόκολλο SSL/TLS (Διάγραμμα 3.5).



Διάγραμμα 3.5 Ποσοστό (%) των ιστοτόπων της κατηγορίας e-shop σύμφωνα με την νεότερη έκδοση του πρωτοκόλλου TLS που υποστηρίζουν και συγκεκριμένα TLS 1.0 (κόκκινο), TLS 1.2 (πράσινο) και καμία έκδοση SSL/TLS (μπλε).

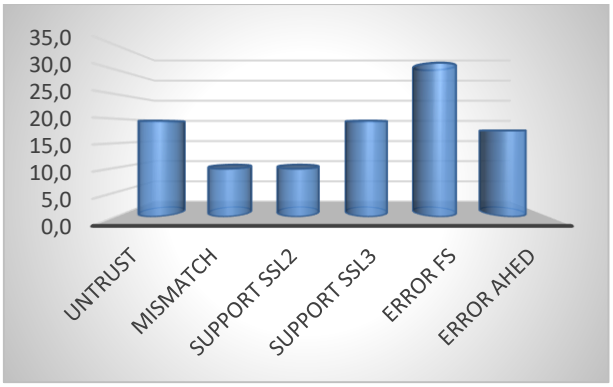
3.3.2 Εταιρείες

Στην κατηγορία ιστοτόπων "εταιρείες" αναλύθηκαν συνολικά 51 ιστότοποι. Συγκεκριμένα, οι ευπάθειες του πρωτοκόλλου TLS με φθίνουσα σειρά είναι RC4 (33,3%), weak DH (27,5%), Poodle (19,6%), Drown(7,8%), OpenSSL padding-oracle flaw (3,9%) και ROBOT (2%). Δεν εντοπίστηκαν οι ευπάθειες FREAK, HeartBleed και Beast (Διάγραμμα 3.6).



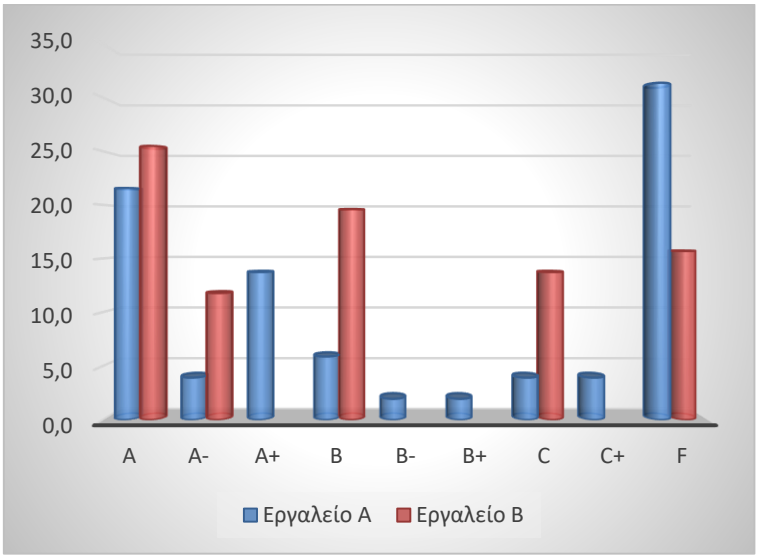
Διάγραμμα 3.6 Ποσοστό (%) των ευπαθειών του πρωτοκόλλου TLS (RC4, Weak DH, Poodle, Drown, ROBOT, Freak, OpenSSL, HeartBleed, Beast) στην κατηγορία ιστοτόπων "εταιρείες".

Όσον αφορά το ποσοστό εμφάνισης αδυναμιών στη διαμόρφωση του https, είναι με φθίνουσα σειρά Error Forward Secrecy (31,4%), Support SSL V3 (19,6%), Untrust (19,6%), Error Authenticated Encryption (17,6%), Support SSL V2 (9,8%) και Mismatch (9,8%) (Διάγραμμα 3.7).



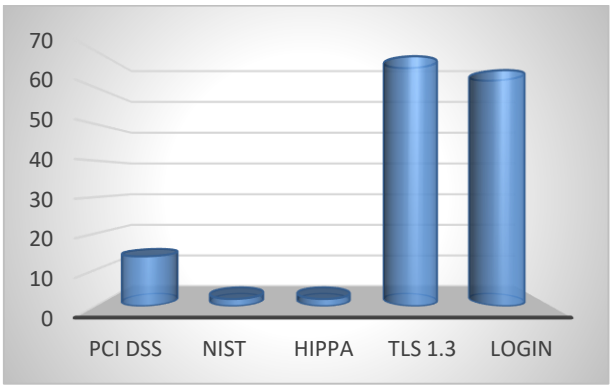
Διάγραμμα 3.7 Ποσοστό (%) των αδυναμιών της διαμόρφωσης του πρωτοκόλλου TLS (Untrust, Mismatch, Support SSL2, Support SSL3, Error FS, Error AHED) στην κατηγορία ιστοτόπων "εταιρίες".

Από την ανάλυση της βαθμολογίας των ιστοτόπων "εταιρείες" που χρησιμοποιούν SSL/TLS, προέκυψε ότι με την χρήση του εργαλείου A, η πλειοψηφία αυτών αξιολογήθηκε με τον βαθμό 'A' (25,5%) και ακολουθούν οι βαθμοί 'B' (19,6%), 'F' (15,7%), 'C' (13,7%), 'A-' (11.8%). Η αντίστοιχη βαθμολογία με την χρήση του εργαλείου B είναι: 'F' (31,4%), 'A' (21,6%), 'A+' (13,7%), 'B' (5,9%), 'A-' , 'C' και 'C+' (3.9%), 'B' και 'B+' (2%) (Διάγραμμα 3.8).



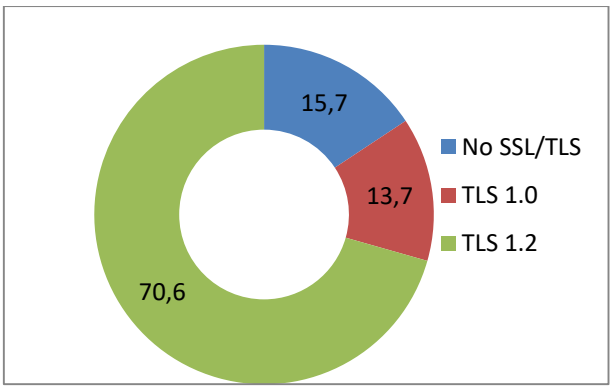
Διάγραμμα 3.8 Ποσοστό (%) της βαθμολογίας που έλαβαν οι ιστότοποι της κατηγορίας "εταιρείες" μετά την ανάλυση τους όσον αφορά την ασφάλεια που παρέχουν με τα εργαλεία A (μπλε μπάρες) και B (κόκκινες μπάρες).

Ποσοστό 64,7% των ιστοτόπων της κατηγορίας “εταιρείες” έδιναν την δυνατότητα στον χρήστη να πραγματοποιήσει σύνδεση (Login) και ενώ 68,5% αυτών είχε την δυνατότητα να μεταβεί στην έκδοση 1.3 του πρωτοκόλλου TLS. Η συμμόρφωση με τα διεθνή πρότυπα PCI DSS, NIST και HIPAA, καταγράφηκε σε ποσοστά 13,7%, 2% και 2% αντίστοιχα (Διάγραμμα 3.9).



Διάγραμμα 3.9 Ποσοστό (%) της συμμόρφωσης με διεθνή πρότυπα (PCI, NIST, HIPPA), ετοιμότητας για μετάβαση στην έκδοση του πρωτόκολλου TLS 1.3, καθώς και την δυνατότητα εγγραφής (Login), στην κατηγορία ιστοτόπων “εταιρίες”.

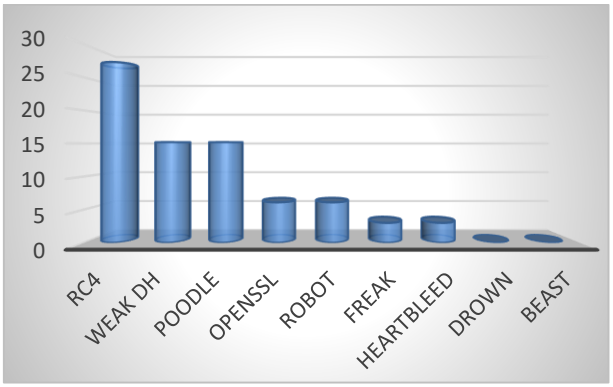
Η πλειοψηφία των ιστοτόπων υποστηρίζουν ως νεότερη έκδοση του πρωτοκόλλου TLS την 1.2 (70,6%), την έκδοση 1.0 (13,7%), ενώ οι ιστότοποι σε ποσοστό (15,7%) δεν εφάρμοζαν κανένα πρωτόκολλο SSL/TLS (Διάγραμμα 3.10).



Διάγραμμα 3.10 Ποσοστό (%) των ιστοτόπων της κατηγορίας "εταιρίες" σύμφωνα με την νεότερη έκδοση του πρωτοκόλλου TLS που υποστηρίζουν και συγκεκριμένα TLS 1.0 (κόκκινο), TLS 1.2 (πράσινο) και καμία έκδοση SSL/TLS (μπλε).

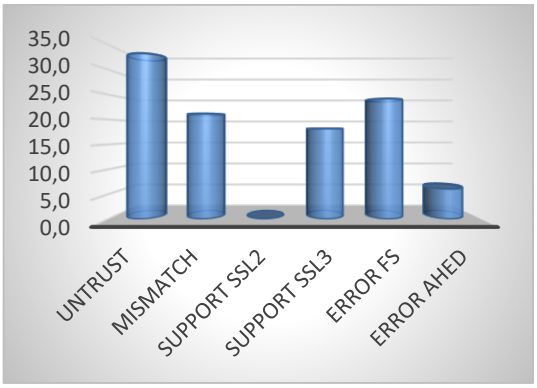
3.3.3 Ενημερωτικά

Στην κατηγορία ιστοτόπων "ενημερωτικά" αναλύθηκαν συνολικά 33 ιστότοποι. Συγκεκριμένα, οι ευπάθειες του πρωτοκόλλου TLS με φθίνουσα σειρά είναι RC4 (27,3%), weak DH (15,2%), Poodle (15,2%), (7,8%), OpenSSL padding-oracle flaw και ROBOT (6,1%) FREAK και HeartBleed (3%). Δεν εντοπίστηκαν οι ευπάθειες Drown και Beast (Διάγραμμα 3.11).



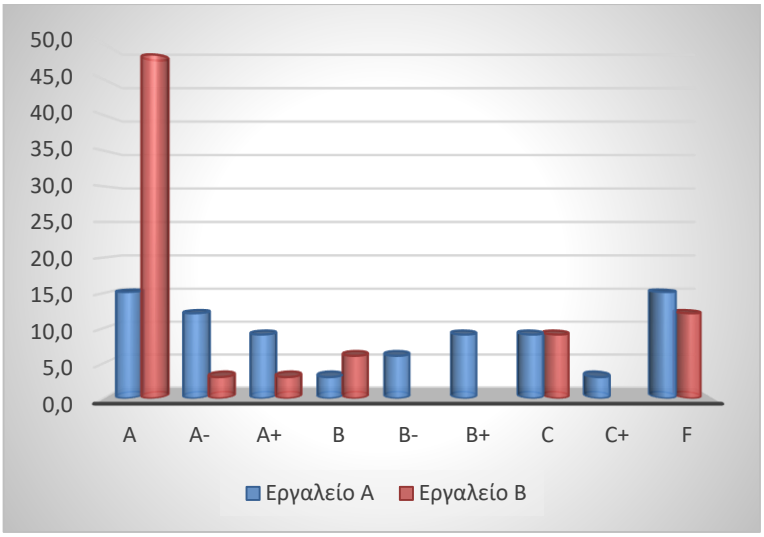
Διάγραμμα 3.11 Ποσοστό (%) των ευπαθειών του πρωτοκόλλου TLS (RC4, Weak DH, Poodle, Drown, ROBOT, Freak, OpenSSL, HeartBleed, Beast) στην κατηγορία ιστοτόπων "ενημερωτικά".

Όσον αφορά το ποσοστό εμφάνισης αδυναμιών στη διαμόρφωση του https, είναι με φθίνουσα σειρά Untrust (33,3%), Error Forward Secrecy (24,2%), Mismatch (21,2%), Support SSL V3 (18,2%) και Error Authenticated Encryption (6,1%). Δεν ανιχνεύθηκε σε κανέναν ιστότοπο της κατηγορίας η αδυναμία Support SSL V2 (Διάγραμμα 3.12).



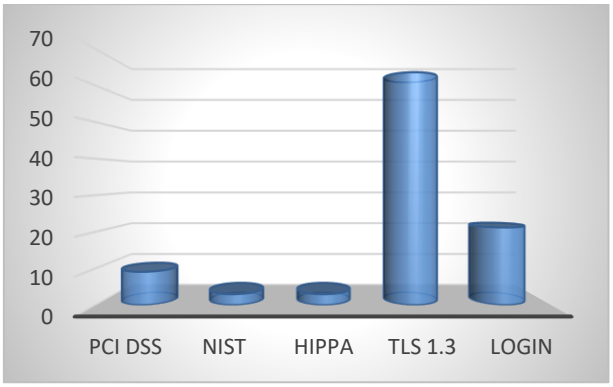
Διάγραμμα 3.12 Ποσοστό (%) των αδυναμιών της διαμόρφωσης του πρωτοκόλλου TLS (Untrust, Mismatch, Support SSL2, Support SSL3, Error FS, Error AHED) στην κατηγορία ιστοτόπων "ενημερωτικά".

Από την ανάλυση της βαθμολογίας των ιστοτόπων "εταιρείες" που χρησιμοποιούν SSL/TLS, προέκυψε ότι με την χρήση του εργαλείου A, η πλειοψηφία αυτών αξιολογήθηκε με τον βαθμό 'A' (48,5%) και ακολουθούν οι βαθμοί 'F' (12,1%), 'C' (9,1%), 'B' (6,1%), 'A-' και 'A+' (3%). Η αντίστοιχη βαθμολογία με την χρήση του εργαλείου B είναι: 'F' και 'A' (15,2%), 'A-' (12,1%), ίδιο ποσοστό για 'A+' 'B+' και 'C' (9,1%), 'B' και 'C+' (3%) (Διάγραμμα 3.13).



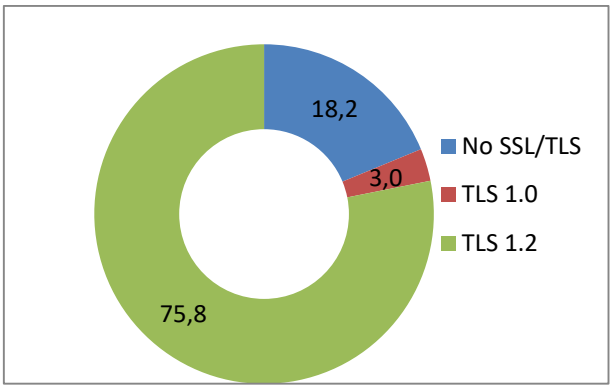
Διάγραμμα 3.13 Ποσοστό (%) της βαθμολογίας που έλαβαν οι ιστότοποι της κατηγορίας "ενημερωτικά" μετά την ανάλυση τους όσον αφορά την ασφάλεια που παρέχουν με τα εργαλεία Α (μπλε μπάρες) και Β (κόκκινες μπάρες).

Ένα μικρό ποσοστό της τάξης του 21,2% των ιστοτόπων της κατηγορίας "ενημερωτικά" έδιναν την δυνατότητα στον χρήστη να πραγματοποιήσει σύνδεση (Login), ενώ 63,6% εξ αυτών είχε την δυνατότητα να μεταβεί στην έκδοση 1.3 του πρωτοκόλλου TLS. Η συμμόρφωση με τα διεθνή πρότυπα PCI DSS, NIST και HIPAA, καταγράφηκε σε ποσοστά 9,1%, 3% και 3% αντίστοιχα (Διάγραμμα 3.14).



Διάγραμμα 3.14 Ποσοστό (%) της συμμόρφωσης με διεθνή πρότυπα (PCI, NIST, HIPPA), ετοιμότητας για μετάβαση στην έκδοση του πρωτόκολλου TLS 1.3, καθώς και την δυνατότητα εγγραφής (Login), στην κατηγορία ιστοτόπων "ενημερωτικά".

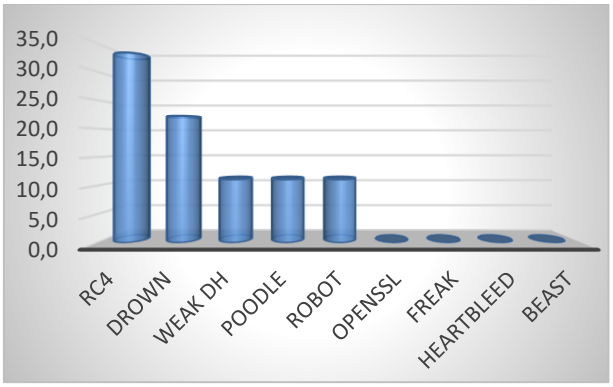
Η πλειοψηφία των ιστοτόπων υποστηρίζουν ως νεότερη έκδοση του πρωτοκόλλου TLS την 1.2 (75,8%), την έκδοση 1.0 (3%), ενώ οι ιστότοποι σε ποσοστό (18,2%) δεν υιοθετούσαν κανένα πρωτόκολλο SSL/TLS (Διάγραμμα 3.15).



Διάγραμμα 3.15 Ποσοστό (%) των ιστοτόπων της κατηγορίας "ενημερωτικά" σύμφωνα με την νεότερη έκδοση του πρωτοκόλλου TLS που υποστηρίζουν και συγκεκριμένα TLS 1.0 (κόκκινο), TLS 1.2 (πράσινο) και καμία έκδοση SSL/TLS (μπλε).

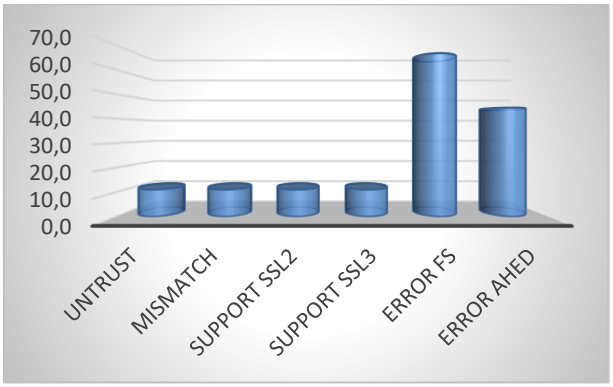
3.3.4 Τηλεπικοινωνίες

Στην κατηγορία ιστοτόπων "τηλεπικοινωνίες" αναλύθηκαν συνολικά 9 ιστότοποι. Συγκεκριμένα, οι ευπάθειες του πρωτοκόλλου TLS με φθίνουσα σειρά είναι RC4 (33,3%), Drown (22,2%), ποσοστό weak DH, Poodle, και ROBOT (11,1%). Δεν ανιχνεύθηκαν οι ευπάθειες OpenSSL padding-oracle flaw, FREAK, Drown και Beast (Διάγραμμα 3.16).



Διάγραμμα 3.16 Ποσοστό (%) των ευπαθειών του πρωτοκόλλου TLS (RC4, Weak DH, Poodle, Drown, ROBOT, Freak, OpenSSL, HeartBleed, Beast) στην κατηγορία ιστοτόπων "τηλεπικοινωνίες".

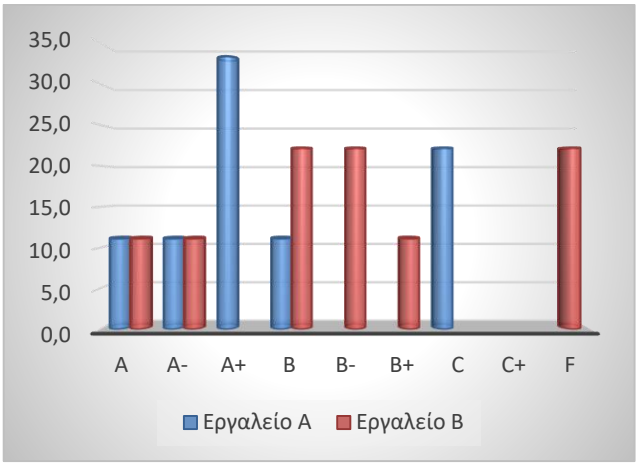
Όσον αφορά το ποσοστό εμφάνισης αδυναμιών στη διαμόρφωση του https, είναι με φθίνουσα σειρά Error Forward Secrecy (66,7%) και Error Authenticated Encryption (44,4%) ενώ ίδια ποσοστά παρατηρήθηκαν στις Untrust (33,3%), Mismatch (21,2%), Support SSL V3 και Support SSL V2 (11,1%) (Διάγραμμα 3.17).



Διάγραμμα 3.17 Ποσοστό (%) των αδυναμιών της διαμόρφωσης του πρωτοκόλλου TLS (Untrust, Mismatch, Support SSL2, Support SSL3, Error FS, Error AHED) στην κατηγορία ιστοτόπων "τηλεπικοινωνίες".

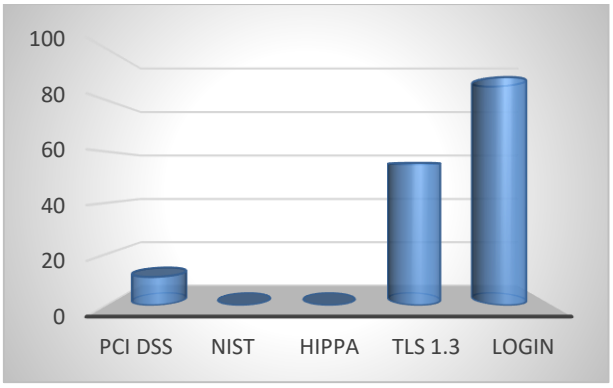
Από την ανάλυση της βαθμολογίας των ιστοτόπων "ενημερωτικά" που χρησιμοποιούν SSL/TLS, προέκυψε ότι με την χρήση του εργαλείου A, η πλειοψηφία αυτών αξιολογήθηκε με τον βαθμό 'A+' (33,3%) και ακολουθούν οι βαθμοί 'C' (22,2%), 'C' (22,2%), και σε ποσοστό 11,1% οι βαθμοί 'A' , 'A-' και 'B'. Η αντίστοιχη βαθμολογία με

την χρήση του εργαλείου Β είναι: ‘Β’, ‘Β-‘ και ‘F’ (22,2%), ‘Α+’, ‘Α-’ και ‘Β+’ (11,1%) (Διάγραμμα 3.18). Παρατηρούμε ότι εμφανίζονται αποκλίσεις οι οποίες εξηγούνται στη συνέχεια.



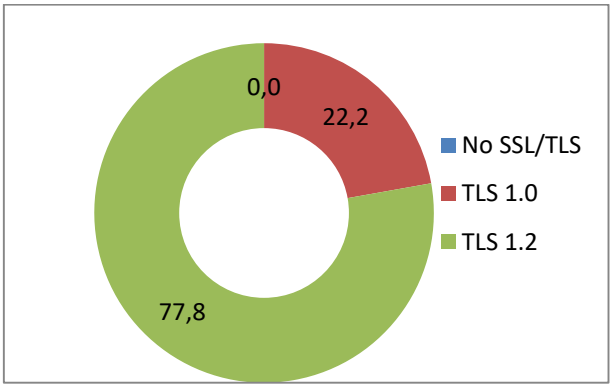
Διάγραμμα 3.18 Ποσοστό (%) της βαθμολογίας που έλαβαν οι ιστότοποι της κατηγορίας “τηλεπικοινωνίες” μετά την ανάλυση τους όσον αφορά την ασφάλεια που παρέχουν με τα εργαλεία Α (μπλε μπάρες) και Β (κόκκινες μπάρες).

Η πλειοψηφία των ιστοτόπων 88,9% της κατηγορίας “τηλεπικοινωνίες” έδιναν την δυνατότητα στον χρήστη να πραγματοποιήσει σύνδεση (Login), ενώ 55,6% εξ αυτών είχε την δυνατότητα να μεταβεί στην έκδοση 1.3 του πρωτοκόλλου TLS. Η συμμόρφωση με το διεθνές πρότυπο PCI DSS καταγράφηκε σε ποσοστό 11,1%, ενώ κανένας ιστότοπος της κατηγορίας δεν ήταν σε συμμόρφωση με τα πρότυπα NIST και HIPPA (Διάγραμμα 3.19).



Διάγραμμα 3.19 Ποσοστό (%) της συμμόρφωσης με διεθνή πρότυπα (PCI, NIST, HIPPA), ετοιμότητας για μετάβαση στην έκδοση του πρωτόκολλου TLS 1.3, καθώς και την δυνατότητα εγγραφής (Login), στην κατηγορία ιστοτόπων "τηλεπικοινωνίες".

Η πλειοψηφία των ιστοτόπων υποστηρίζουν ως νεότερη έκδοση του πρωτοκόλλου TLS την 1.2 (77,8%), κανένας εξ αυτών την έκδοση 1.0, ενώ οι ιστότοποι σε ποσοστό (22,2%) δεν υιοθετούσαν κανένα πρωτόκολλο SSL/TLS (Διάγραμμα 3.20).

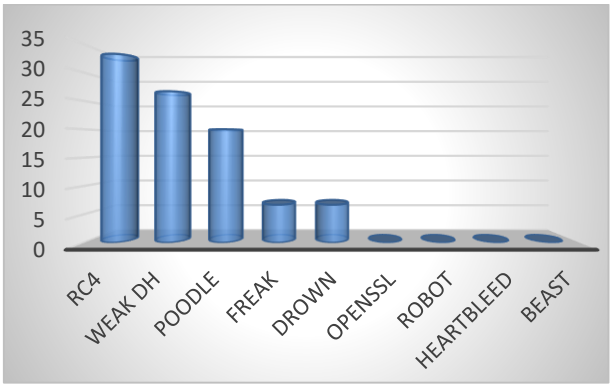


Διάγραμμα 3.20 Ποσοστό (%) των ιστοτόπων της κατηγορίας "τηλεπικοινωνίες" σύμφωνα με την νεότερη έκδοση του πρωτοκόλλου TLS που υποστηρίζουν και συγκεκριμένα TLS 1.0 (κόκκινο), TLS 1.2 (πράσινο) και καμία έκδοση SSL/TLS (μπλε).

3.3.5 Εκπαίδευση

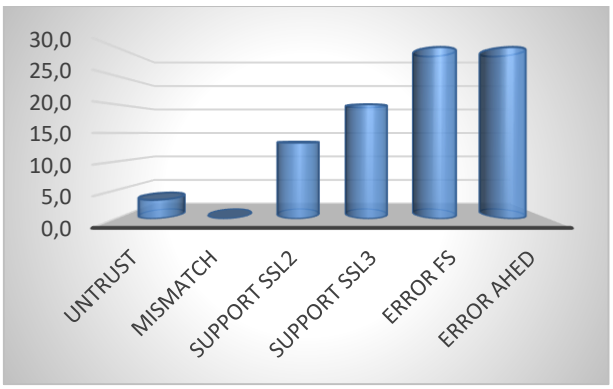
Στην κατηγορία ιστοτόπων "εκπαίδευση" αναλύθηκαν συνολικά 30 ιστότοποι. Συγκεκριμένα, οι ευπάθειες του πρωτοκόλλου TLS με φθίνουσα σειρά είναι RC4 (33,3%),

weak DH (26,7%), Poodle (20%), FREAK και Drown (6,7%). Δεν εντοπίστηκαν οι ευπάθειες OpenSSL padding-oracle flaw, ROBOT, HeartBleed και Beast (Διάγραμμα 3.21).



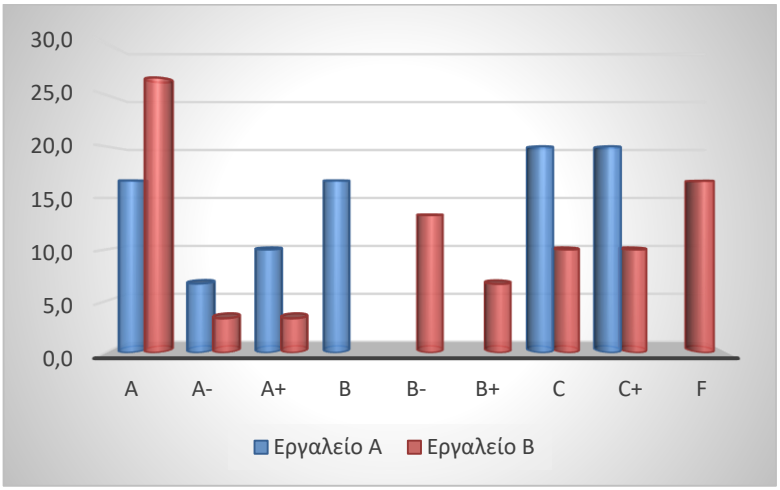
Διάγραμμα 3.21 Ποσοστό (%) των ευπαθειών του πρωτοκόλλου TLS (RC4, Weak DH, Poodle, Drown, ROBOT, Freak, OpenSSL, HeartBleed, Beast) στην κατηγορία ιστοτόπων "εκπαίδευση".

Όσον αφορά το ποσοστό εμφάνισης αδυναμιών στη διαμόρφωση του https, είναι με φθίνουσα σειρά Error Authenticated Encryption και Error Forward Secrecy (30%), Support SSL V3 (20%), Support SSL V2 (13,3%) και Untrust (3,3%). Δεν ανιχνεύθηκε σε κανέναν ιστότοπο της κατηγορίας η αδυναμία Mismatch (Διάγραμμα 3.22).



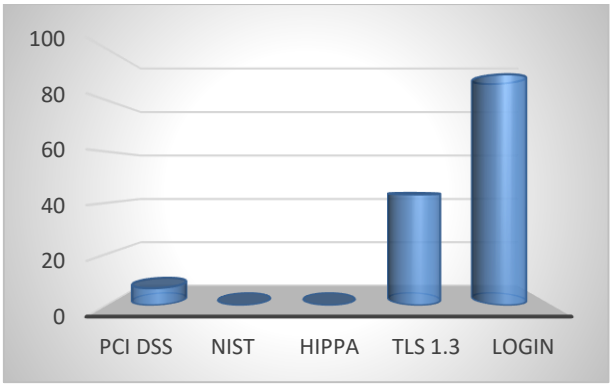
Διάγραμμα 3.22 Ποσοστό (%) των αδυναμιών της διαμόρφωσης του πρωτοκόλλου TLS (Untrust, Mismatch, Support SSL2, Support SSL3, Error FS, Error AHED) στην κατηγορία ιστοτόπων "εκπαίδευση".

Από την ανάλυση της βαθμολογίας των ιστοτόπων “εκπαίδευση” που χρησιμοποιούν SSL/TLS, προέκυψε ότι με την χρήση του εργαλείου A, η πλειοψηφία αυτών αξιολογήθηκε με τον βαθμό ‘C’ και ‘F’ (20%) και ακολουθούν οι βαθμοί ‘A’ και ‘B’ (16,7%),‘A+’ (10%) και ‘A-’ (6,7%). Η αντίστοιχη βαθμολογία με την χρήση του εργαλείου B είναι: ‘A’ (26,7%), ‘F’ (16,7%), ‘B-’ (13,3%), ίδιο ποσοστό για ‘C+’ και ‘C’ (10%), ‘B+’ (6,7%), ίδιο ποσοστό για ‘A+’ και ‘A-‘ (3,3%) (Διάγραμμα 3.23) .



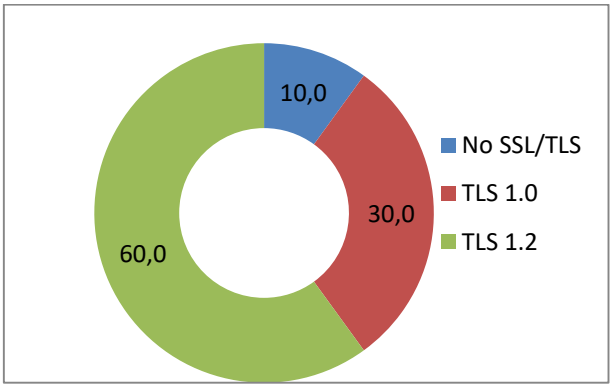
Διάγραμμα 3.23 Ποσοστό (%) της βαθμολογίας που έλαβαν οι ιστότοποι της κατηγορίας “εκπαίδευση” μετά την ανάλυση τους όσον αφορά την ασφάλεια που παρέχουν με τα εργαλεία A (μπλε μπάρες) και B (κόκκινες μπάρες).

Η πλειοψηφία των ιστοτόπων 90% της κατηγορίας “εκπαίδευση” έδιναν την δυνατότητα στον χρήστη να πραγματοποιήσει σύνδεση (Login), ενώ 43,3% εξ αυτών είχε την δυνατότητα να μεταβεί στην έκδοση 1.3 του πρωτοκόλλου TLS. Η συμμόρφωση με το διεθνές πρότυπο PCI DSS καταγράφηκε σε ποσοστό 6,7%, ενώ κανένας ιστότοπος της κατηγορίας δεν ήταν σε συμμόρφωση με τα πρότυπα NIST και HIPPA (Διάγραμμα 3.24).



Διάγραμμα 3.24 Ποσοστό (%) της συμμόρφωσης με διεθνή πρότυπα (PCI, NIST, HIPPA), ετοιμότητας για μετάβαση στην έκδοση του πρωτόκολλου TLS 1.3, καθώς και την δυνατότητα εγγραφής (Login), στην κατηγορία ιστοτόπων "εκπαίδευση".

Η πλειοψηφία των ιστοτόπων υποστηρίζουν ως νεότερη έκδοση του πρωτοκόλλου TLS την 1.2 (60%), την έκδοση 1.0 (30%), ενώ οι ιστότοποι σε ποσοστό (10%) δεν υιοθετούσαν κανένα πρωτόκολλο SSL/TLS (Διάγραμμα 3.25).

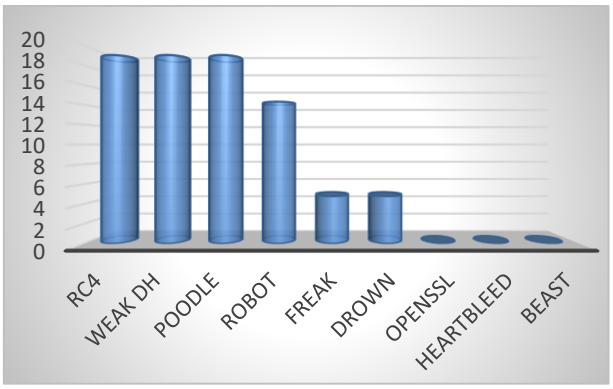


Διάγραμμα 3.25 Ποσοστό (%) των ιστοτόπων της κατηγορίας "εκπαίδευση" σύμφωνα με την νεότερη έκδοση του πρωτοκόλλου TLS που υποστηρίζουν και συγκεκριμένα TLS 1.0 (κόκκινο), TLS 1.2 (πράσινο) και καμία έκδοση SSL/TLS (μπλε).

3.3.6 Οικονομικές Υπηρεσίες

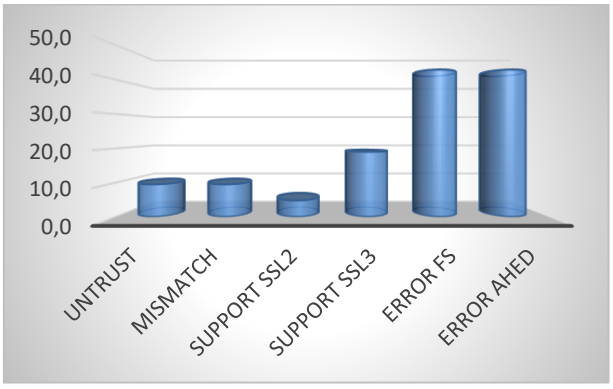
Στην κατηγορία ιστοτόπων "οικονομικές υπηρεσίες" αναλύθηκαν συνολικά 21 ιστότοποι. Συγκεκριμένα σύμφωνα με το Διάγραμμα 1 οι ευπάθειες του πρωτοκόλλου

TLS με φθίνουσα σειρά είναι RC4, weak DH και Poodle (19%), ROBOT (14,3%), FREAK και Drown (4,8%). Δεν εντοπίστηκαν οι ευπάθειες OpenSSL padding-oracle flaw , HeartBleed και Beast (Διάγραμμα 3.26).



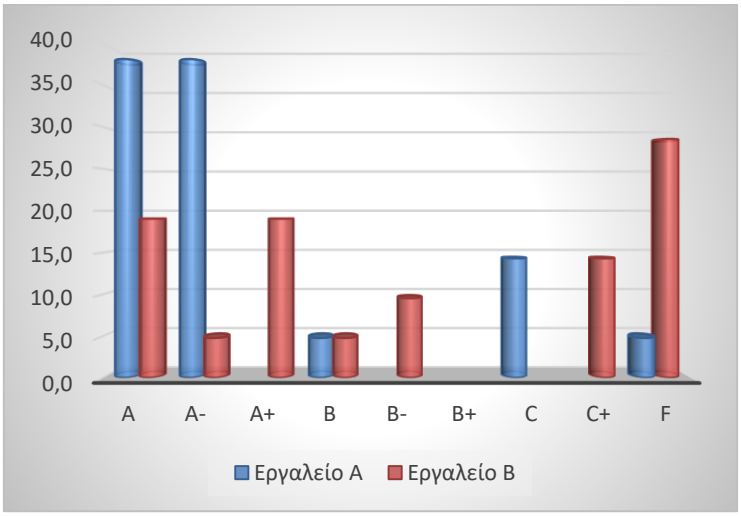
Διάγραμμα 3.26 Ποσοστό (%) των ευπαθειών του πρωτοκόλλου TLS (RC4, Weak DH, Poodle, Drown, ROBOT, Freak, OpenSSL, HeartBleed, Beast) στην κατηγορία ιστοτόπων "οικονομικές υπηρεσίες".

Όσον αφορά το ποσοστό εμφάνισης αδυναμιών στη διαμόρφωση του https, είναι με φθίνουσα σειρά Error Authenticated Encryption και Error Forward Secrecy (42,9%), Support SSL V3 (19%), Untrust και Mismatch (9,5%) και Support SSL V2 (4,8%) (Διάγραμμα 3.27).



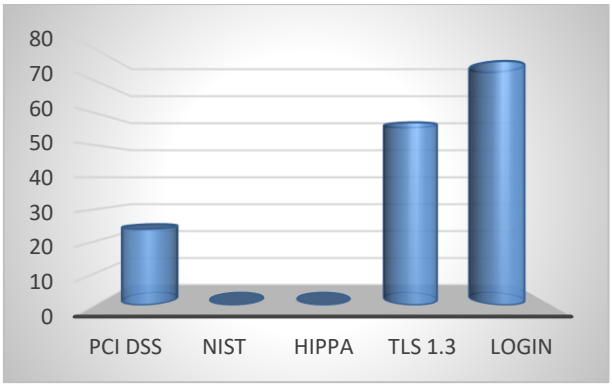
Διάγραμμα 3.27 Ποσοστό (%) των αδυναμιών της διαμόρφωσης του πρωτοκόλλου TLS (Untrust, Mismatch, Support SSL2, Support SSL3, Error FS, Error AHED) στην κατηγορία ιστοτόπων "οικονομικές υπηρεσίες".

Από την ανάλυση της βαθμολογίας των ιστοτόπων "οικονομικές υπηρεσίες" που χρησιμοποιούν SSL/TLS, προέκυψε ότι με την χρήση του εργαλείου Α, η πλειοψηφία αυτών αξιολογήθηκε με τον βαθμό 'Α' και 'Α-' (38,1%) και ακολουθούν οι βαθμοί 'C' (14,3%), 'F' και 'B' (4,8%). Η αντίστοιχη βαθμολογία με την χρήση του εργαλείου Β είναι: 'F' (28,6%), 'Α' και 'Α+' (19%), 'C+' (14,3%), 'B-' (9,5%) και ίδιο ποσοστό για 'Α-' και 'B' (4,8%) (Διάγραμμα 3.28). Παρατηρούμε ότι εμφανίζονται αποκλίσεις οι οποίες εξηγούνται στη συνέχεια.



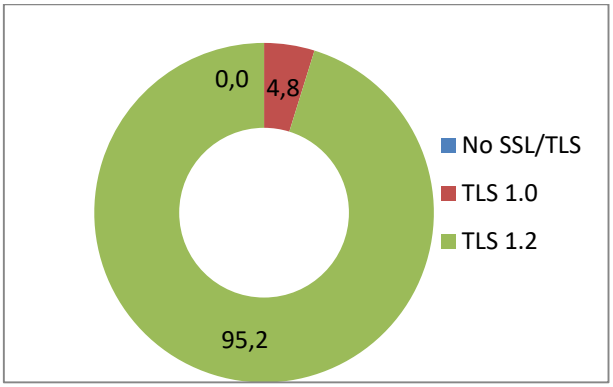
Διάγραμμα 3.28 Ποσοστό (%) της βαθμολογίας που έλαβαν οι ιστότοποι της κατηγορίας "οικονομικές υπηρεσίες" μετά την ανάλυση τους όσον αφορά την ασφάλεια που παρέχουν με τα εργαλεία Α (μπλε μπάρες) και Β (κόκκινες μπάρες).

Η πλειοψηφία των ιστοτόπων 76,2% της κατηγορίας " οικονομικές υπηρεσίες " έδιναν την δυνατότητα στον χρήστη να πραγματοποιήσει σύνδεση (Login), ενώ 57,1% εξ αυτών είχε την δυνατότητα να μεταβεί στην έκδοση 1.3 του πρωτοκόλλου TLS. Η συμμόρφωση με το διεθνές πρότυπο PCI DSS καταγράφηκε σε ποσοστό 23,8%, ενώ κανένας ιστότοπος της κατηγορίας δεν ήταν σε συμμόρφωση με τα πρότυπα NIST και HIPPA (Διάγραμμα 3.29).



Διάγραμμα 3.29 Ποσοστό (%) της συμμόρφωσης με διεθνή πρότυπα (PCI, NIST, HIPPA), ετοιμότητας για μετάβαση στην έκδοση του πρωτόκολλου TLS 1.3, καθώς και την δυνατότητα εγγραφής (Login), στην κατηγορία ιστοτόπων "οικονομικές υπηρεσίες".

Η πλειοψηφία των ιστοτόπων υποστηρίζουν ως νεότερη έκδοση του πρωτοκόλλου TLS την 1.2 (95,2%) και την έκδοση 1.0 (4,8%) (Διάγραμμα 3.30).

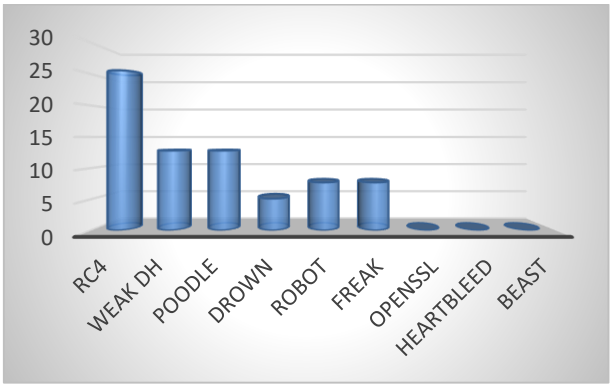


Διάγραμμα 3.30 Ποσοστό (%) των ιστοτόπων της κατηγορίας "οικονομικές υπηρεσίες" σύμφωνα με την νεότερη έκδοση του πρωτοκόλλου TLS που υποστηρίζουν και συγκεκριμένα TLS 1.0 (κόκκινο), TLS 1.2 (πράσινο) και καμία έκδοση SSL/TLS (μπλε).

3.3.7 Δημόσιοι Οργανισμοί

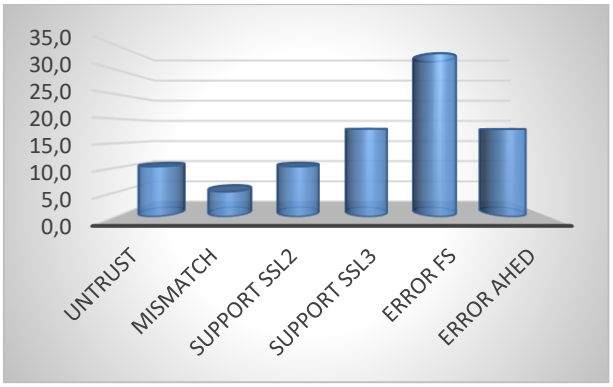
Στην κατηγορία ιστοτόπων "δημόσιοι οργανισμοί" αναλύθηκαν συνολικά 39 ιστότοποι. Συγκεκριμένα, οι ευπάθειες του πρωτοκόλλου TLS με φθίνουσα σειρά είναι RC4 (25,6%), weak DH και Poodle (12,8%), ROBOT και FREAK (7,7%) και Drown (5,1%). Δεν

εντοπίστηκαν οι ευπάθειες OpenSSL padding-oracle flaw, HeartBleed και Beast (Διάγραμμα 3.31).



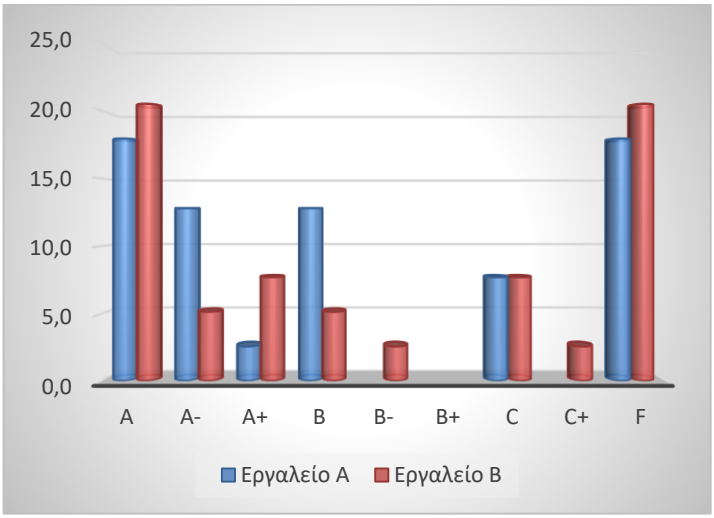
Διάγραμμα 3.31 Ποσοστό (%) των ευπαθειών του πρωτοκόλλου TLS (RC4, Weak DH, Poodle, Drown, ROBOT, Freak, OpenSSL, HeartBleed, Beast) στην κατηγορία ιστοτόπων "δημόσιοι οργανισμοί".

Όσον αφορά το ποσοστό εμφάνισης αδυναμιών στη διαμόρφωση του https, είναι με φθίνουσα σειρά Error Forward Secrecy (33,3%), Error Authenticated Encryption και Support SSL V3 (17,9%), Untrust και Support SSL V2 (10,3%) και Mismatch (5,1%) (Διάγραμμα 3.32).



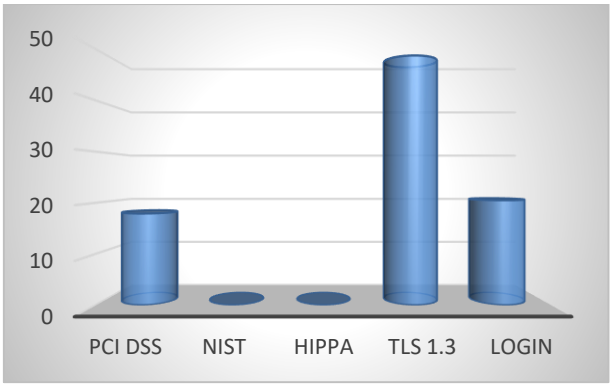
Διάγραμμα 3.32 Ποσοστό (%) των αδυναμιών της διαμόρφωσης του πρωτοκόλλου TLS (Untrust, Mismatch, Support SSL2, Support SSL3, Error FS, Error AHED) στην κατηγορία ιστοτόπων "δημόσιοι οργανισμοί".

Από την ανάλυση της βαθμολογίας των ιστοτόπων " δημόσιοι οργανισμοί " που χρησιμοποιούν SSL/TLS, προέκυψε ότι με την χρήση του εργαλείου Α, η πλειοψηφία αυτών αξιολογήθηκε με τον βαθμό 'Α' και 'F' (17,9%) και ακολουθούν οι βαθμοί 'Α-' και 'Β' (12,8%), 'C' (7,7%) και 'Α+' (2,6%). Η αντίστοιχη βαθμολογία με την χρήση του εργαλείου Β είναι: 'F' και 'Α' (20,5%), 'Α+' και 'C' (7,7%), ίδιο ποσοστό για 'Α-' και 'Β' (5,1%), 'Β-' και 'C+' (2,6%) (Διάγραμμα 3.33).



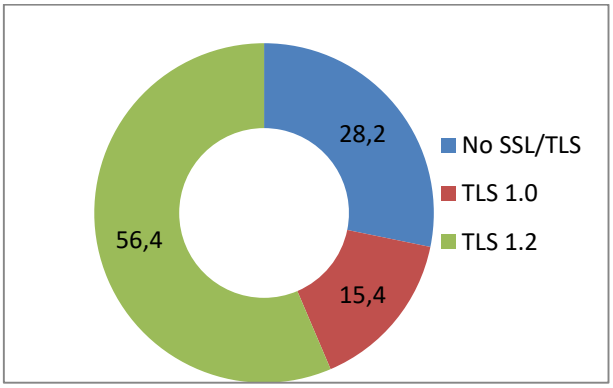
Διάγραμμα 3.33 Ποσοστό (%) της βαθμολογίας που έλαβαν οι ιστότοποι της κατηγορίας "δημόσιοι οργανισμοί" μετά την ανάλυση τους όσον αφορά την ασφάλεια που παρέχουν με τα εργαλεία Α (μπλε μπάρες) και Β (κόκκινες μπάρες).

Ένα μικρό ποσοστό της τάξης του 20,5% των ιστοτόπων της κατηγορίας "δημόσιοι οργανισμοί" έδιναν την δυνατότητα στον χρήστη να πραγματοποιήσει σύνδεση (Login), ενώ 48,7% εξ αυτών είχε την δυνατότητα να μεταβεί στην έκδοση 1.3 του πρωτοκόλλου TLS. Η συμμόρφωση με το διεθνές πρότυπο PCI DSS καταγράφηκε σε ποσοστό 17,9%, ενώ κανένας ιστότοπος της κατηγορίας δεν ήταν σε συμμόρφωση με τα πρότυπα NIST και HIPPA (Διάγραμμα 3.34).



Διάγραμμα 3.34 Ποσοστό (%) της συμμόρφωσης με διεθνή πρότυπα (PCI, NIST, HIPPA), ετοιμότητας για μετάβαση στην έκδοση του πρωτόκολλου TLS 1.3, καθώς και την δυνατότητα εγγραφής (Login), στην κατηγορία ιστοτόπων "δημόσιοι οργανισμοί".

Σχεδόν οι μισοί εκ των ιστοτόπων υποστηρίζουν ως νεότερη έκδοση του πρωτοκόλλου TLS την 1.2 (56,4%), την έκδοση 1.0 (15,4%), ενώ οι ιστότοποι σε ποσοστό (28,2%) δεν υιοθετούσαν κανένα πρωτόκολλο SSL/TLS (Διάγραμμα 3.35).

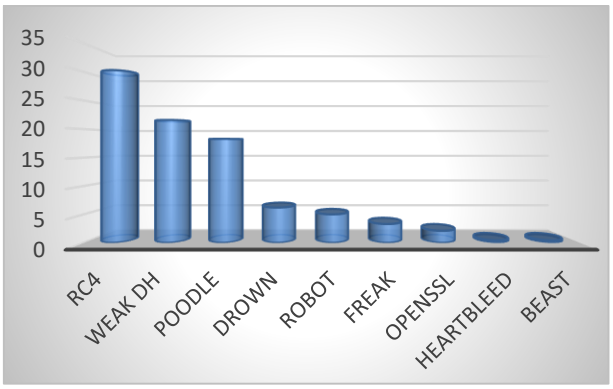


Διάγραμμα 3.35 Ποσοστό (%) των ιστοτόπων της κατηγορίας "δημόσιοι οργανισμοί" σύμφωνα με την νεότερη έκδοση του πρωτοκόλλου TLS που υποστηρίζουν και συγκεκριμένα TLS 1.0 (κόκκινο), TLS 1.2 (πράσινο) και καμία έκδοση SSL/TLS (μπλε).

3.3.8 Συνολικά

Συνολικά σε όλες τις κατηγορίες αναλύθηκαν 241 ιστότοποι. Συγκεκριμένα, οι ευπάθειες του πρωτοκόλλου TLS με φθίνουσα σειρά είναι RC4 (30,3%), weak DH (21,6%), Poodle

(18,3%), Drown(6,2%), ROBOT (5%), Freak (3,3%), OpenSSL padding-oracle flaw (2,1%), HeartBleed και Beast (0,4%) (Διάγραμμα 3.36).

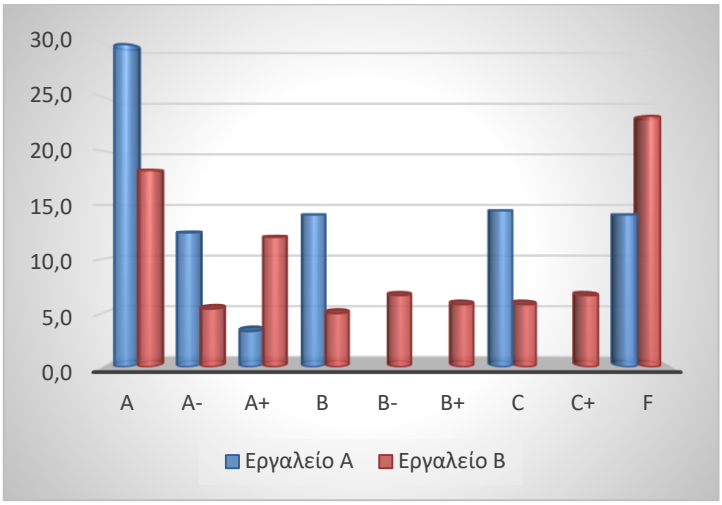


Διάγραμμα 3.36. Ποσοστό (%) των ευπαθειών του πρωτοκόλλου TLS (RC4, Weak DH, Poodle, Drown, ROBOT, Freak, OpenSSL, HeartBleed, Beast) συνολικά σε όλες τις κατηγορίες ιστοτόπων.

Όσον αφορά το ποσοστό εμφάνισης αδυναμιών στη διαμόρφωση του https, είναι με φθίνουσα σειρά Error Forward Secrecy (34,9%), Support SSL V3 (20,3%), Error Authenticated Encryption (19,1%), Untrust (16,2%), Mismatch (8,3%) και Support SSL V2 (7,9%) (Διάγραμμα 3.37).

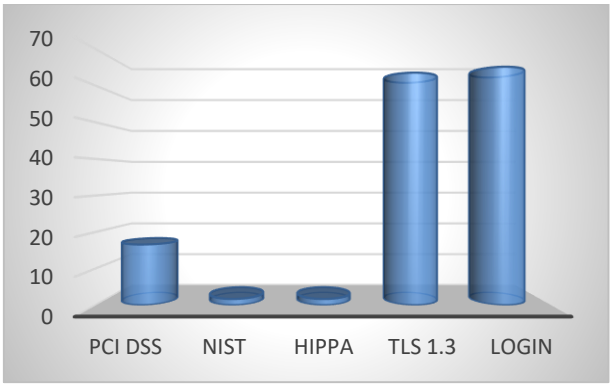
Διάγραμμα 3.37 Ποσοστό (%) των αδυναμιών της διαμόρφωσης του πρωτοκόλλου TLS (Untrust, Mismatch, Support SSL2, Support SSL3, Error FS, Error AHED) συνολικά σε όλες τις κατηγορίες ιστοτόπων.

Από την ανάλυση της βαθμολογίας των ιστοτόπων όλων των κατηγοριών που χρησιμοποιούν SSL/TLS, προέκυψε ότι με την χρήση του εργαλείου Α, η πλειοψηφία αυτών αξιολογήθηκε με τον βαθμό 'A' (29,9%) και ακολουθούν οι βαθμοί 'C' (14,5%), 'B' και 'F' (14,1%), 'A-' (12.4%) και 'A+' (3,3%). Η αντίστοιχη βαθμολογία με την χρήση του εργαλείου Β είναι: 'F' (23,2%), 'A' (18,3%), 'A+' (12%), 'B-' και 'C-' (6,6%), 'B+' και 'C' (5,8%), 'A-' (5,4%) και 'B' (5%) (Διάγραμμα 3.38). Παρατηρούμε ότι εμφανίζονται αποκλίσεις οι οποίες εξηγούνται στη συνέχεια.



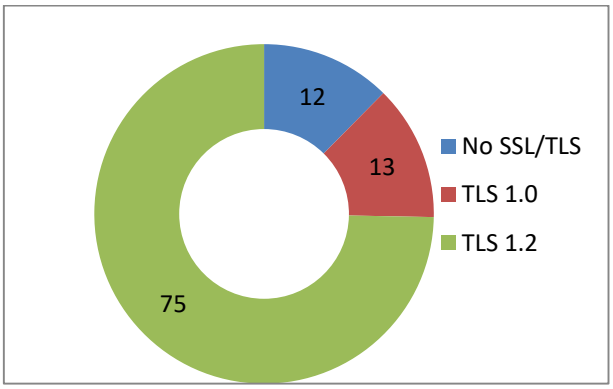
Διάγραμμα 3.38 Ποσοστό (%) της βαθμολογίας που έλαβαν συνολικά όλες οι κατηγορίες ιστοτόπων μετά την ανάλυση τους όσον αφορά την ασφάλεια που παρέχουν με τα εργαλεία Α (μπλε μπάρες) και Β (κόκκινες μπάρες).

Ποσοστό 65,1% των ιστοτόπων όλων των κατηγοριών έδιναν την δυνατότητα στον χρήστη να πραγματοποιήσει σύνδεση (Login) και ενώ 63,5% αυτών είχε την δυνατότητα να μεταβεί στην έκδοση 1.3 του πρωτοκόλλου TLS. Η συμμόρφωση με τα διεθνή πρότυπα PCI DSS, NIST και HIPAA, καταγράφηκε σε ποσοστά 16,6%, 1,7% και 1,7% αντίστοιχα (Διάγραμμα 3.39).



Διάγραμμα 3.39 Ποσοστό (%) της συμμόρφωσης με διεθνή πρότυπα (PCI, NIST, HIPPA), ετοιμότητας για μετάβαση στην έκδοση του πρωτόκολλου TLS 1.3, καθώς και την δυνατότητα εγγραφής (Login), συνολικά σε όλες τις κατηγορίες ιστοτόπων.

Η πλειοψηφία των ιστοτόπων υποστηρίζουν ως νεότερη έκδοση του πρωτοκόλλου TLS την 1.2 (75%), την έκδοση 1.0 (13%), ενώ οι ιστότοποι σε ποσοστό (12%) δεν εφάρμοζαν κανένα πρωτόκολλο SSL/TLS (Διάγραμμα 3.40).

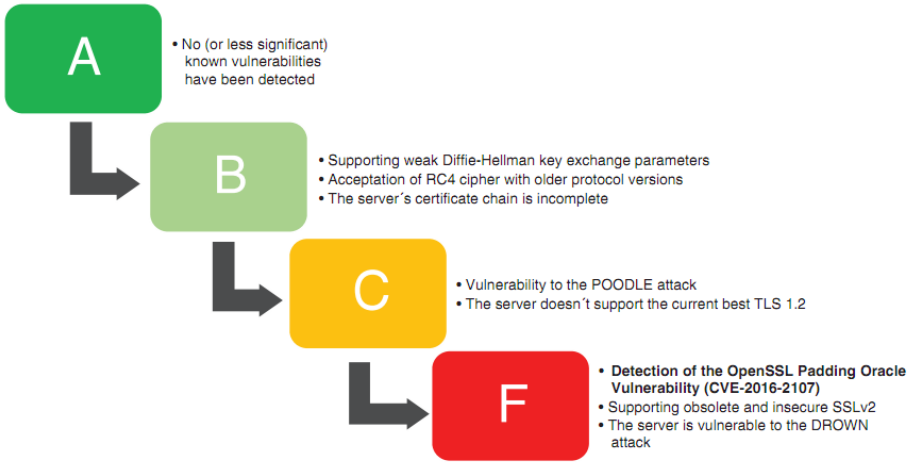


Διάγραμμα 3.40 Ποσοστό (%) των ιστοτόπων σε όλες τις κατηγορίες σύμφωνα με την νεότερη έκδοση του πρωτοκόλλου TLS που υποστηρίζουν και συγκεκριμένα TLS 1.0 (κόκκινο), TLS 1.2 (πράσινο) και καμία έκδοση SSL/TLS (μπλε).

3.4 Συμπεράσματα

Παρατηρούμε στο Διάγραμμα 3.38 Ποσοστό (%) της βαθμολογίας που έλαβαν συνολικά όλες οι κατηγορίες ιστοτόπων μετά την ανάλυση τους όσον αφορά την ασφάλεια που παρέχουν

με τα εργαλεία A (μπλε μπάρες) και B (κόκκινες μπάρες). ότι η αξιολόγηση με τα δύο εργαλεία παρουσιάζει σημαντικές διαφορές. Αυτό συμβαίνει γιατί τα δύο εργαλεία δεν χρησιμοποιούν τα ίδια κριτήρια βαθμολόγησης. Έτσι για παράδειγμα το πρώτο εργαλείο μετρά επιμέρους βαθμολογίες για κάθε κατηγορία που αναλύει και στο τέλος τις συνθέτει για να υπολογίσει την τελική βαθμολογία, ενώ το δεύτερο εργαλείο ξεκινά από τις 100 μονάδες και προσθαφαιρεί πόντους ανάλογα με τα ευρήματα. Αν όμως εντοπίζει κάποια συγκεκριμένα ευρήματα μειώνει σημαντικά την βαθμολογία. Παρακάτω παρουσιάζεται σχηματικά η διαδικασία η οποία κατατάσσει κάθε ιστοσελίδα και οι σημαντικότεροι λόγοι για τον οποίο λαμβάνουν τον ανάλογο βαθμό. Από το Διάγραμμα 3.38 παρατηρούμε ότι μεγάλο ποσοστό από τις ελληνικές ιστοσελίδες που εξετάστηκαν παρουσιάζουν πολύ καλή βαθμολόγηση και με τα δύο εργαλεία που χρησιμοποιήθηκαν. Ωστόσο παρατηρούμε ότι ένα σημαντικό ποσοστό δεν έχει λάβει καλή βαθμολογία, γεγονός που μας οδηγεί στο συμπέρασμα ότι υπάρχουν ακόμα σημαντικά περιθώρια βελτίωσης.



Εικόνα 3.19 Σχηματική αναπαράσταση της διαδικασίας βαθμολόγησης [53]

Στα συγκεντρωτικά αποτελέσματα από το Διάγραμμα 3.36. Ποσοστό (%) των ευπαθειών του πρωτοκόλλου TLS (RC4, Weak DH, Poodle, Drown, ROBOT, Freak, OpenSSL, HeartBleed, Beast) συνολικά σε όλες τις κατηγορίες ιστοτόπων. παρατηρούμε ότι οι τρεις σημαντικότερες ευπάθειες που εντοπίστηκαν είναι οι RC4, Weak DH και Poodle. Οι ευπάθειες αυτές, παρόλο που είναι γνωστές, παρατηρούμε ότι ανιχνεύονται σε σημαντικά ποσοστά,

γεγονός που καταδεικνύει πόσο σημαντική είναι η εκπαίδευση και η ευαισθητοποίηση των διαχειριστών των ιστοσελίδων, καθώς δεν αρκεί η υιοθέτηση των πρωτοκόλλων ασφαλείας, αλλά και σωστή υλοποίηση τους.

Αντίθετα οι ευπάθειες Drown, ROBOT, Freak, OpenSSL, HeartBleed, Beast παρουσιάζονται σε ποσοστό μικρότερο του 10% για το σύνολο των ιστοσελίδων. Οι επιθέσεις αυτές είναι κατά κύριο λόγο επιθέσεις που έλαβαν μεγάλη δημοσιότητα κατά τον εντοπισμό τους και έτσι φαίνεται ότι οι περισσότεροι διαχειριστές ιστοσελίδων ενημερώθηκαν και ευαισθητοποιήθηκαν σύντομα.

Από τις ιστοσελίδες που εξετάστηκαν μόνο το 12% δεν χρησιμοποιεί κάποιο από τα πρωτόκολλα SSL/TLS. Αυτό είναι αναμενόμενο καθώς πολλές από τις ιστοσελίδες δεν έχουν κάποιο μηχανισμό σύνδεσης (Login) (34,9%). Ειδικότερα σε κάποιες κατηγορίες παρατηρούνται μεγάλες διαφορές σύμφωνα με την στατιστική ανάλυση που διενεργήθηκε με την χρήση του SPSS [76] με χρήση chi-square test ($p<0.05$). Η διαδικασία χ^2 είναι από τις πιο διαδεδομένες τεχνικές που χρησιμοποιούνται για την ανάλυση ποιοτικών δεδομένων. Με τη χρήση της πραγματοποιήθηκε έλεγχος της ανεξαρτησίας δυο μεταβλητών και συγκεκριμένα εξετάστηκε εάν οι παρατηρούμενες συχνότητες στις κατηγορίες μιας απλής κατανομής συχνοτήτων στο δείγμα μας συμφωνούν με τις συχνότητες που υποθέτουμε ότι υπάρχουν στις κατηγορίες αυτές στον πληθυσμό (SPSS: Analyze > Descriptive > Crosstab, statistics-x square). Έτσι για τα e-shop παρουσιάζεται στατιστικώς σημαντικά μεγαλύτερη χρήση login, σε σχέση με τις κατηγορίες εταιριών και οικονομικών οργανισμών και στατιστικώς σημαντικά μεγαλύτερη χρήση πρωτοκόλλων SSL/TLS σε σχέση με τους δημόσιους φορείς. Αντίθετα οι δημόσιοι οργανισμοί και οι ενημερωτικές ιστοσελίδες παρουσιάζουν στατιστικά σημαντικά μικρότερη χρήση login, σε σχέση με τα e-shop, εταιριών και οικονομικών οργανισμών. Για τα υπόλοιπα αποτελέσματα, ενώ υπήρχαν κάποιες διαφορές, ωστόσο δεν προέκυπτε κάποια στατιστικώς σημαντική διαφορά.

Στο σύνολο των ιστοσελίδων που εξετάστηκαν, 65,3% είναι έτοιμο για μετάβαση στην έκδοση TLS 1.3, ποσοστό που ανεβαίνει στο 71,85% αν αφαιρεθούν οι ιστοσελίδες που δεν έχουν κάποια υλοποίηση SSL/TLS. Αυτό δείχνει ότι η πλειοψηφία των ιστοσελίδων είναι έτοιμη να λειτουργήσει με την επόμενη έκδοση του πρωτοκόλλου TLS, όταν κυκλοφορήσει η τελική του έκδοση. Σε σχέση με την έκδοση του TLS που υποστηρίζεται, η πλειοψηφία των ιστοσελίδων υποστηρίζει την έκδοση 1.2 (75%) γεγονός που τις καθιστά ενημερωμένες. Υπάρχει όμως και ένα ποσοστό (13%) το οποίο χρησιμοποιεί την

έκδοση 1.0 του πρωτοκόλλου και το οποίο θα πρέπει να πραγματοποιήσει άμεσα την μετάβαση στην νεότερη έκδοση.

Από τα συνολικά αποτελέσματα παρατηρούμε ότι για τα πρότυπα - οδηγίες PCI, NIST και HIPPA τα ποσοστά συμμόρφωσης είναι ιδιαίτερα χαμηλά. Υπενθυμίζεται ότι τα πρότυπα αυτά είναι ιδιαίτερα απαιτητικά αλλά και επικεντρωμένα σε συγκεκριμένες περιπτώσεις (PCI για οικονομικές υπηρεσίες και HIPPA για ιατρικές υπηρεσίες). Επιπλέον τα πρότυπα αυτά χρησιμοποιούνται κυρίως στις Ηνωμένες Πολιτείες Αμερικής και όχι την Ευρωπαϊκή Ένωση. Συνεπώς τα χαμηλά ποσοστά συμμόρφωσης είναι αναμενόμενα καθώς το PCI εφαρμόζεται κυρίως για οικονομικές συναλλαγές, ενώ το HIPPA για δεδομένα υγείας και τέλος το PCI για οικονομικούς φορείς.

Χαρακτηριστικά παραδείγματα κακής ρύθμισης των πιστοποιητικών είναι τα ποσοστά Untrust (16,2%) και Mismatch (8,3%). Ιστοσελίδες οι οποίες πιθανότητα έχουν αξιόπιστο πιστοποιητικό, εξαιτίας κακής ρύθμισης παρουσιάζεται στους φυλλομετρητές σαν αναξιόπιστο. Επιπλέον αυτό αυξάνει την πιθανότητα ένας χρήστης να πέσει θύμα παραπλάνησης, καθώς μπορεί να θεωρεί ότι το μήνυμα που λαμβάνει είναι μικρής σημασίας, ενώ στην πραγματικότητα να συμβαίνει κάτι άλλο (π.χ. Man in the middle attack). Όσον αναφορά στην υποστήριξη ξεπερασμένων εκδόσεων, παρατηρούμε ότι ένα ποσοστό ιστοσελίδων υποστηρίζει ακόμη τις εκδόσεις SSL v3 (20,3%) και SSL v2 (7,9%). Αυτό το ποσοστό (ειδικά για το SSL v3) δεν είναι αμελητέο και αποτελεί ένα εν γένει κίνδυνο για τις ιστοσελίδες. Τέλος παρατηρούμε ότι τα ποσοστά Error FS (34,9%) και Error AHED (19,1%) είναι αυξημένα και παρόλο που δεν αποτελούν ευπάθειες, θα ήταν πρακτικά σημαντικό να υλοποιηθούν για να προσφέρουν ενισχυμένη ασφάλεια.

Κεφάλαιο 4

Ερωτηματολόγιο

4.1 Εισαγωγή

Στην προηγούμενη ενότητα παρουσιάστηκαν τα ευρήματα από την ανάλυση των σημαντικότερων ελληνικών ιστοσελίδων. Όμως ο άλλος πόλος της ασφάλειας είναι οι χρήστες, καθώς αυτοί χρησιμοποιούν τις ιστοσελίδες και διαμορφώνουν τις απαιτήσεις στις οποίες πρέπει να ανταποκριθούν οι διαχειριστές των ιστοσελίδων και οι πάροχοι. Εξάλλου, ακόμα και αν μία ιστοσελίδα υλοποιεί τα βέλτιστα μέτρα ως προς την ασφάλεια, εάν οι χρήστες δεν γνωρίζουν πώς να διαπιστώνουν της ασφάλεια των ιστοσελίδων που επισκέπτονται τότε παραμένουν ευάλωτοι σε επιθέσεις (π.χ. επιθέσεις «phishing»).

Η μελέτη μας σχεδιάστηκε για να απαντήσει ορισμένα ερευνητικά ερωτήματα και συγκεκριμένα:

α) αν είναι οι τυπικοί χρήστες του διαδικτύου είναι γνώστες των κινδύνων που αντιμετωπίζουν on-line, β) αν οι κίνδυνοι αυτοί είναι ξεκάθαροι ως προς το εύρος και το βάθος που καλύπτουν ώστε να υποστηρίξουν την σαφή λήψη αποφάσεων διαχείρισης επικινδυνότητας, γ) αν είναι οι τυπικοί χρήστες του διαδικτύου ενήμεροι για τα πιο διαδεδομένα εργαλεία που βοηθούν στην λήψη αποφάσεων και τα χρησιμοποιούν ώστε να λαμβάνουν τις σωστές αποφάσεις για την διαχείριση κινδύνων ασφαλείας κατά την πλοήγηση τους, δ) πώς κρίνουν την ασφάλεια μιας ιστοσελίδας ανάλογα με την κατηγορία στην οποία ανήκει (π.χ. τράπεζες, ενημερωτικά κλπ.) και ε) ποιες είναι οι απαιτήσεις και η συμπεριφορά των χρηστών από τις ιστοσελίδες τις οποίες επισκέπτονται.

4.2 Σκοπός μελέτης

Η χρήση ερωτηματολογίου για την αποτύπωση της Ελληνικής πραγματικότητας στον τομέα ασφαλούς πλοήγησης στο διαδίκτυο, ως προς τη σκοπιά της αξιοποίησης του πρωτοκόλλου TLS, παρουσιάζει ενδιαφέρον καθώς δεν φαίνεται ότι έχει γίνει παρόμοια μελέτη στο παρελθόν. Αυτή η μελέτη διερεύνησε τις απόψεις, την ευαισθητοποίηση, τις απαιτήσεις, τις γνώσεις και τις αυτό-αναφερόμενες πρακτικές των Ελλήνων χρηστών του διαδικτύου κατά την πλοήγηση τους. Τα δεδομένα συλλέχθηκαν από συνολικά 773 χρήστες με τη χρήση αυτό-διαχειριζόμενου και δομημένου διαδικτυακού ερωτηματολογίου, με συστηματική και τυχαία δειγματοληψία. Μέσω των αποτελεσμάτων που παρείχε η έρευνα αποτιμήθηκαν τα συνηθισμένα λάθη των χρηστών, η έλλειψη τεχνικής γνώσης ή σημεία που δεν είναι επαρκώς κατανοητά κι ενέχουν αβεβαιότητα από τους καταναλωτές.

4.3 Μεθοδολογία

Στις παρακάτω ενότητες περιγράφεται η μεθοδολογία που ακολουθήθηκε και η τεκμηρίωσή της. Επιπλέον καταγράφεται ο τρόπος με τον οποίο κατοχυρώνεται η εγκυρότητα και η αξιοπιστία της έρευνας. Τέλος παρουσιάζεται ο τρόπος με τον οποίο γίνεται η επιστημονική ανάλυση των δεδομένων που προέκυψαν από τις απαντήσεις του ερωτηματολογίου.

4.3.1 Ερευνητικό εργαλείο συλλογής δεδομένων

Στην παρούσα έρευνα επιλέχτηκε η χρήση ερωτηματολογίου καθώς θεωρούνται τα πιο κατάλληλα εργαλεία για τις κοινωνικές επιστήμες, ενώ επίσης καθιστούν εύκολη τη συλλογή δεδομένων από ανθρώπους που βρίσκονται σε μεγάλες αποστάσεις. Το ερωτηματολόγιο διανεμήθηκε και συμπληρώθηκε την περίοδο Φεβρουαρίου – Μαρτίου 2018.

Τα εργαλείο συλλογής δεδομένων ήταν ένα ερωτηματολόγιο που περιείχε δεκαεννέα ερωτήσεις-ισχυρισμούς (statements) της κλίμακας γνώσης, διατυπωμένες ως θετικές (positive) με τιμές μεταβλητής κλίμακας μέτρησης τύπου Likert (1 = διαφωνώ απόλυτα μέχρι 5 = συμφωνώ απόλυτα). Το ερωτηματολόγιο διανεμήθηκε για να απαντηθεί στα μέσα κοινωνικής δικτύωσης (Facebook, Twitter) και μέσω ηλεκτρονικού ταχυδρομείου. Οι χρήστες παροτρύνθηκαν να ακολουθήσουν την παρακάτω ηλεκτρονική διεύθυνση https://goo.gl/Xywy8M και να το συμπληρώσουν (όσο βέβαια το ερωτηματολόγιο είχε καταστεί ως δημόσιο) ώστε να έχουν πρόσβαση όσοι αποτελούσαν το δείγμα του ερωτηματολογίου.

Το διαδίκτυο αποτελεί πλέον ένα εργαλείο που χρησιμοποιείται ολοένα και περισσότερο για τη διεξαγωγή ποσοτικών ερευνών. Στη δεκαετία του ‘30 και του ‘40 οι μοναδικοί τρόποι συλλογής δεδομένων μιας έρευνας ήταν η ταχυδρομική αποστολή των ερωτηματολογίων ή οι συνεντεύξεις με τους ερωτώμενους πηγαίνοντας από πόρτα σε πόρτα. Από τη δεκαετία του ‘70 οι τηλεφωνικές συνεντεύξεις έγιναν μια δημοφιλής εναλλακτική λύση, χάρη στη σχεδόν καθολική υιοθέτηση του τηλεφώνου. Σήμερα, καθώς το διαδίκτυο χρησιμοποιείται όλο και περισσότερο, οι διαδικτυακές έρευνες γίνονται μια όλο και πιο ενδιαφέρουσα επιλογή.

Τα πλεονεκτήματα της διαδικτυακής έρευνας έναντι της συμβατικής έρευνας είναι τα εξής [77,78]:

- Η εξοικονόμηση πόρων (χρημάτων, ανθρώπινου δυναμικού, αναλώσιμων κ.τ.λ.)
- Η εξάλειψη σφαλμάτων κατά την εισαγωγή δεδομένων, αφού γίνεται από τους ίδιους τους ερωτώμενους
- Η αποτελεσματικότητα: γρήγορη συλλογή και αποθήκευση δεδομένων
- Η εύκολη εύρεση ατόμων με συγκεκριμένα χαρακτηριστικά και ενδιαφέροντα, για παράδειγμα άτομα τα οποία συμμετέχουν σε συγκεκριμένα περιβάλλοντα στο ιντερνέτ όπως: forum, ομάδες κοινωνικής δικτύωσης με συγκεκριμένες θεματικές
- Η απουσία μεροληπτικότητας από το πρόσωπο που διενεργεί τη συνέντευξη
- Η επιλογή του τόπου και του χρόνου συμπλήρωσης των ερωτηματολογίων από τους ερωτώμενους
- Η πρόσβαση σε γεωγραφικά κατανεμημένους πληθυσμούς

Τα μειονεκτήματα της διαδικτυακής έρευνας είναι ότι απευθύνεται κυρίως σε νέες ηλικιακές ομάδες (όπου η χρήση του διαδικτύου είναι εκτεταμένη και σε καθημερινή βάση) και η απουσία προσωπικής επαφής με τον ερωτώμενο. Βέβαια, στη συγκεκριμένη περίπτωση, το αντικείμενο της έρευνας ούτως ή άλλως δεν αφορά ανθρώπους οι οποίοι δεν κάνουν καμία χρήση του Διαδικτύου.

4.3.2 Εγκυρότητα και αξιοπιστία της έρευνας

Αξιοπιστία είναι ο βαθμός στον οποίο ένα τεστ ή μια διαδικασία παράγει τα ίδια αποτελέσματα κάτω από σταθερές συνθήκες σε όλες τις περιπτώσεις, με την ίδια μέθοδο συλλογής δεδομένων και με τα ίδια υποκείμενα στις ίδιες συνθήκες. Είναι φανερό πως ο έλεγχος της εγκυρότητας μιας έρευνας είναι δύσκολο να ελεγχθεί πριν αυτή γίνει. Η εγκυρότητα και αξία της έρευνας θα προκύψει από τη μελέτη των αποτελεσμάτων του δείγματος και τη δυνατότητα γενίκευσής τους και θα εξαρτηθεί και από την αντιπροσωπευτικότητα του δείγματος.

4.3.3 Ανάλυση δεδομένων

Για τη διερεύνηση της δομικής εγκυρότητας της κάθε θεματικής ενότητας πραγματοποιήθηκε διερευνητική παραγοντική ανάλυση, η οποία εφαρμόζεται όταν η δομή του μοντέλου δεν είναι γνωστή ή προκαθορισμένη και χρησιμοποιούνται τα δεδομένα για να την αποκαλύψουν [79]. Για την ολοκλήρωση της παραγοντικής ανάλυσης και τον έλεγχο των αποτελεσμάτων, ακολουθήθηκε συγκεκριμένη διαδικασία και εξετάστηκαν οι κατάλληλοι δείκτες. Συγκεκριμένα:

1) Για την εξαγωγή των παραγόντων εφαρμόστηκε η μέθοδος της Ανάλυσης Βασικών Συνιστωσών (Principal Component Analysis) με Ορθογώνια Περιστροφή των αξόνων με τη μέθοδο Varimax, η οποία, κατά τους Sharma και Hair [80,81], αποτελεί μία από τις δημοφιλέστερες μεθόδους ορθογώνιας περιστροφής.

Rotated Component Matrix[a]

	Component			
	1	2	3	4
Γνωρίζω πως ελέγχουμε την ασφάλεια ενός πιστοποιητικού σε συνδέσεις https	,845			
Ελέγχω πάντα αν η ιστοσελίδα που επισκέπτομαι είναι https	,808			
Γνωρίζω την διαφορά του http από το https	,803			
Γνωρίζω τι σημαίνει το λουκέτο στην γραμμή πλοήγησης του φυλλομετρητή	,769			
Γνωρίζω πως μπορώ να προστατευθώ από μία ηλεκτρονική απάτη	,755			
Ελέγχω πάντα αν η ιστοσελίδα που επισκέπτομαι έχει το χαρακτηριστικό λουκέτο	,753			
Ο φυλλομετρητής μου υποστηρίζει τα τελευταία πρωτόκολλα ασφαλείας	,503			
Οι ιστοσελίδες των e-shop έχουν λάβει όλα τα απαραίτητα μέτρα για την ασφαλή πλοήγηση των χρηστών		,772		
Οι ιστοσελίδες των δημοσίων φορέων έχουν λάβει όλα τα απαραίτητα μέτρα για την ασφαλή πλοήγηση των χρηστών		,717		
Οι ιστοσελίδες των τραπεζών έχουν λάβει όλα τα απαραίτητα μέτρα για την ασφαλή πλοήγηση των χρηστών		,693		
Οι ειδησεογραφικές ιστοσελίδες έχουν λάβει όλα τα απαραίτητα μέτρα για την ασφαλή πλοήγηση των χρηστών		,616		
Οι ιστοσελίδες των Social media (Facebook, Twitter κλπ.) έχουν λάβει όλα τα απαραίτητα μέτρα για την ασφαλή πλοήγηση των χρηστών		,588		
Όταν πλοηγούμαι στο Internet ενδιαφέρομαι τα στοιχεία που εισάγω να μην γίνονται γνωστά σε τρίτους			,879	
Όταν πλοηγούμαι στο Internet ενδιαφέρομαι για την ασφάλεια των πληροφοριών μου			,869	
Όταν πλοηγούμαι στο Internet ενδιαφέρομαι για την ιδιωτικότητα μου			,803	
Αν ο φυλλομετρητής μου βγάλει προειδοποίηση ότι η ιστοσελίδα που μπαίνω δεν είναι ασφαλής, θα διέκοπτα την πλοήγηση μου				,882
Αν γνώριζα ότι μία ιστοσελίδα που χρησιμοποιώ συχνά δεν είναι ασφαλής, θα σταματούσα να την χρησιμοποιώ				,854

Πίνακας 4.1: Εξαγωγή παραγόντων με τη μέθοδο της Ανάλυσης Βασικών Συνιστωσών (Principal Component Analysis) και Ορθογώνια Περιστροφή των αξόνων με τη μέθοδο Varimax

2) Για τον έλεγχο της Συνολικής Δειγματικής Καταλληλόλητας χρησιμοποιήθηκε το μέτρο Κ.Μ.Ο. (Kaiser-Mayer-Olkin), το οποίο είναι το πλέον δημοφιλές διαγνωστικό μέτρο και οι τιμές του κυμαίνονται από 0 έως 1. Δεν υπάρχει στατιστικός έλεγχος για τις τιμές του δείκτη, αλλά οι Kaiser και Rice [82] συνιστούν να απορρίπτονται τιμές μικρότερες του 0,5.

KMO and Bartlett's Test

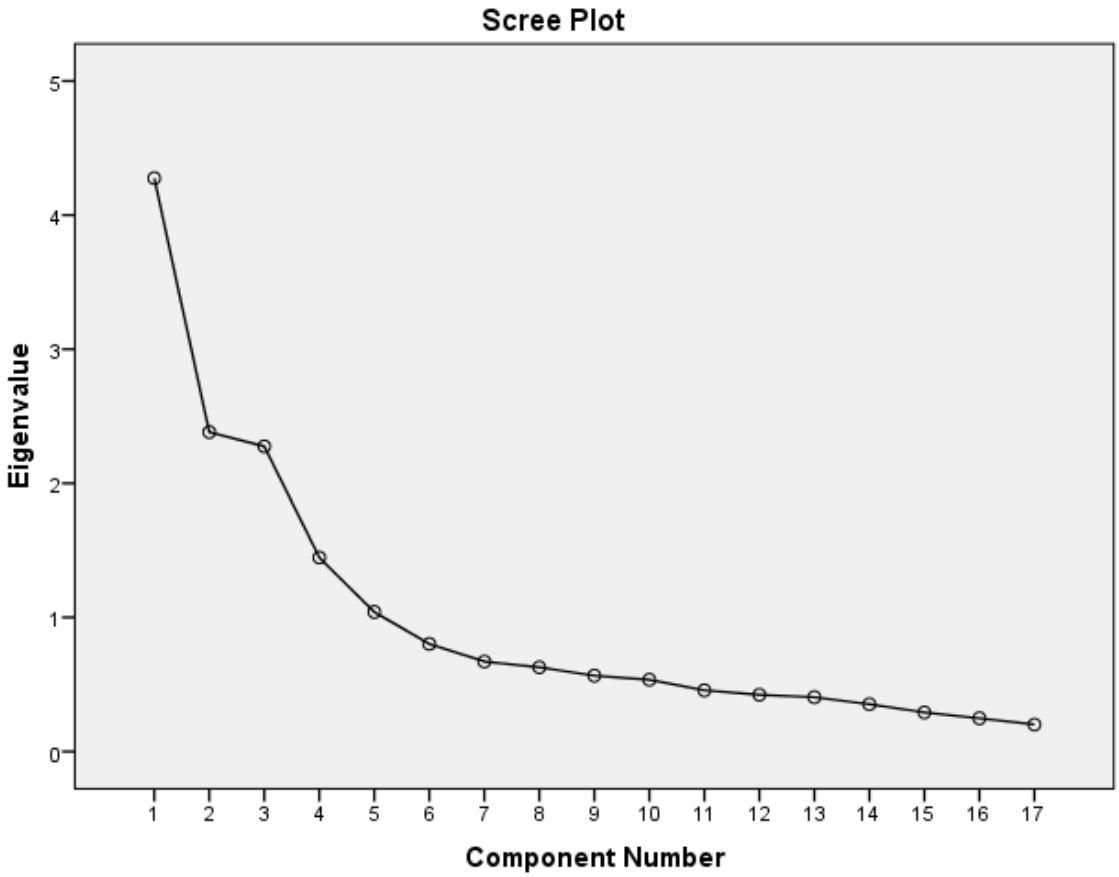
Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		,778
Bartlett's Test of Sphericity	Approx. Chi-Square	5005,900
	df	136
	Sig.	,000

Πίνακας 4.2: Έλεγχος Συνολικής Δειγματικής Καταλληλόλητας με το μέτρο Κ.Μ.Ο. (Kaiser-Mayer-Olkin)

3) Για περαιτέρω και πληρέστερη εξέταση της καταλληλόλητας των δεδομένων για παραγοντική ανάλυση, έγινε ο έλεγχος Σφαιρικότητας του Bartlett (Bartlett's Test of Sphericity). Ο έλεγχος αυτός εξετάζει την ύπαρξη συσχετίσεων μεταξύ των μεταβλητών και στην ουσία παρέχει τη στατιστική πιθανότητα, ο πίνακας συσχετίσεων να περιέχει σημαντικές συσχετίσεις μεταξύ, τουλάχιστον, κάποιων μεταβλητών.

4) Για τον έλεγχο της καταλληλόλητας της κάθε μεταβλητής ξεχωριστά, εξετάστηκαν οι δείκτες M.S.A. (measure of sample adequacy) οι οποίοι πρέπει να είναι μεγαλύτεροι του 0,5 [80].

5) Για τον προσδιορισμό του αριθμού των παραγόντων (Factors) έχουν αναπτυχθεί πολλά κριτήρια. Το πλέον δημοφιλές είναι το κριτήριο της ιδιοτιμής (Eigenvalue), σύμφωνα με το οποίο επιλέγουμε μόνο τους παράγοντες των οποίων η τιμή υπερβαίνει το 1 [81].



Διάγραμμα 4.41: Προσδιορισμός αριθμού των παραγόντων (Factors) με το κριτήριο της ιδιοτιμής (Eigenvalue)

Ένα άλλο σημαντικό κριτήριο, για την επιλογή του πλήθους των παραγόντων, είναι το κριτήριο του ποσοστού της Διακύμανσης, το οποίο ερμηνεύουν οι παράγοντες. Δεν είναι ασυνήθιστο, μία λύση που υπολογίζει το 60% της συνολικής διακύμανσης (και σε κάποιες περιπτώσεις ακόμη λιγότερο) να θεωρείται ικανοποιητική [80].

Total Variance Explained

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	4,275	25,149	25,149	4,275	25,149	25,149	4,125	24,262	24,262
2	2,382	14,012	39,161	2,382	14,012	39,161	2,405	14,145	38,406
3	2,276	13,387	52,547	2,276	13,387	52,547	2,227	13,099	51,505
4	1,446	8,507	61,055	1,446	8,507	61,055	1,623	9,549	61,055
5	1,041	6,121	67,176						
6	,802	4,718	71,894						
7	,671	3,947	75,841						
8	,628	3,692	79,534						
9	,566	3,327	82,860						
10	,535	3,149	86,010						
11	,456	2,684	88,693						
12	,423	2,491	91,184						
13	,405	2,384	93,568						
14	,353	2,075	95,643						
15	,292	1,716	97,359						
16	,248	1,457	98,816						
17	,201	1,184	100,000						

Extraction Method: Principal Component Analysis.

Πίνακας 4.3: Επιλογή πλήθους παραγόντων με το κριτήριο του ποσοστού της Διακύμανσης

Για τη διερεύνηση της αξιοπιστίας χρησιμοποιήθηκε ο δείκτης εσωτερικής συνέπειας του Cronbach (Cronbach 's α). Ο δείκτης α είναι ένας δείκτης της εσωτερικής συνέπειας ενός τεστ (Internal consistency) και υπολογίζεται από τη συσχέτιση της κάθε ερώτησης του τεστ με την συνολική κλίμακα. Είναι από τις περισσότερο δημοφιλείς τεχνικές υπολογισμού της αξιοπιστίας [83]. Το συνολικό Cronbach a του ερωτηματολογίου ήταν 0,782, πάνω από το 0,6 όπου είναι το ελάχιστο όριο αξιοπιστίας.

Reliability Statistics

Cronbach's Alpha	N of Items
,782	17

Πίνακας 4.4: Δείκτης εσωτερικής συνέπειας του Cronbach για τη διερεύνηση της αξιοπιστίας

Έτσι προέκυψαν τέσσερις εννοιολογικές κατασκευές με συνολικά 17 ερωτήσεις-ισχυρισμούς, σχετικά με τις γνώσεις σε θέματα ασφάλειας. Η πρώτη ονομάστηκε

«**ευαισθητοποίηση/ πεποιθήσεις σχετικά με την ασφαλή πλοήγηση**» και απαρτίζεται από τις ερωτήσεις 14, 15, 16, 17 και 18. Η δεύτερη καταγράφηκε ως «**απαιτήσεις χρηστών κατά την πλοήγηση**» και αποτελείται από τις ερωτήσεις 19, 20 και 21. Η τρίτη χαρακτηρίστηκε ως «**γνώσεις σε θέματα ασφαλούς πλοήγησης**» και περιλαμβάνει τις ερωτήσεις 24, 27, 28, 29, 30, 32 και 33. Η τέταρτη αναφέρεται ως «**συμπεριφορά χρηστών κατά την πλοήγηση**» και την συνθέτουν οι ερωτήσεις 34 και 35.

4.4 Ερωτηματολόγιο

Παρακάτω παρατίθεται το ερωτηματολόγιο (σύνολο 35 ερωτήσεις) σε έξι διακριτές ενότητες. Η πρώτη περιλαμβάνει δημογραφικά στοιχεία (4 ερωτήσεις), η δεύτερη πληροφορίες σχετικά με την χρήση διαδικτύου (9 ερωτήσεις), η τρίτη ενότητα περιλαμβάνει ερωτήσεις για την ευαισθητοποίηση των χρηστών σχετικά με την ασφαλή πλοήγηση (5 ερωτήσεις), η τέταρτη ενότητα τις απαιτήσεις των χρηστών κατά την πλοήγηση τους (5 ερωτήσεις), η πέμπτη καταγράφει τις γνώσεις σε θέματα ασφαλούς πλοήγησης (8 ερωτήσεις) και η έκτη αποτιμά την συμπεριφορά χρηστών κατά την πλοήγηση τους (4 ερωτήσεις).

4.4.1 Ενότητα Α: Δημογραφικά στοιχεία

1. **Φύλο:**

a. Άνδρας
b. Γυναίκα
c. Δεν απαντώ

2. **Ηλικία**

a. 16-24
b. 25-39
c. 40 -55

d. 55 και άνω

3. Μορφωτικό επίπεδο (Μέγιστη βαθμίδα εκπαίδευσης που έχετε ολοκληρώσει)

a. Απόφοιτος (η) δημοτικού – γυμνασίου
b. Απόφοιτος (η) λυκείου/ΙΕΚ
c. Απόφοιτος (η) ΑΕΙ/ΤΕΙ
d. Κάτοχος μεταπτυχιακού - διδακτορικού τίτλου

4. Έχετε σπουδές σχετικές με την Επιστήμη Υπολογιστών ή την Πληροφορική;

a. Ναι
b. Όχι

4.4.2 Ενότητα Β: Πληροφορίες σχετικά με την χρήση διαδικτύου

5. "Είμαι εξοικειωμένος με την χρήση του Internet".

i. Διαφωνώ απόλυτα
ii. Διαφωνώ
iii. Ούτε διαφωνώ, ούτε συμφωνώ
iv. Συμφωνώ
v. Συμφωνώ απόλυτα

6. Καθημερινά πλοηγούμαι στο Internet για:

a. Λιγότερο από 1 ώρα
b. 2-3 ώρες
c. 3-4 ώρες
d. Περισσότερες από 4

7. **Για ποιους λόγους χρησιμοποιείτε κυρίως το Internet? (επιλέξτε ένα ή περισσότερα)**

a. Έλεγχος e-mail
b. Αγορές αγαθών
c. Τραπεζικές συναλλαγές
d. Κοινωνική δικτύωση
e. Αναζήτηση πληροφοριών

8. **Ποιο φυλλομετρητή (browser) χρησιμοποιείτε κυρίως στον υπολογιστή σας;**

a. Chrome
b. Firefox
c. Safari
d. Microsoft Internet Explorer/ Edge
e. Opera
f. Άλλο

9. **Ποιο φυλλομετρητή (browser) χρησιμοποιείτε κυρίως στο κινητό σας;**

a. Chrome
b. Firefox
c. Safari
d. Microsoft Internet Explorer/ Edge
e. Opera
f. Άλλο

10. **Πόσο συχνά αναβαθμίζετε τον φυλλομετρητή σας;**

a. Αυτόματα
b. Κάθε Εβδομάδα
c. Κάθε Μήνα
d. Κάθε Χρόνο
e. Ποτέ

11. Έχετε πέσει θύμα κάποιας ηλεκτρονικής απάτης (κλοπή συνθηματικών, στοιχεία πιστωτικής κάρτας);

a. Ναι
b. Όχι

12. Πώς αντιλαμβάνεστε τον όρο "Ασφαλή Ιστοσελίδα": (επιλέξτε ένα ή περισσότερα)

a. Τα στοιχεία που εισάγουμε δεν δίνονται σε τρίτους
b. Προστατεύονται οι κωδικοί πρόσβασης και οι συναλλαγές
c. Θα πρέπει να υπάρχει σαφής σχετική δήλωση στην ιστοσελίδα
d. Να είναι καλαίσθητη και σύγχρονη
e. Να ανήκει σε γνωστή εταιρία που εμπιστεύομαι
f. Άλλο (εισαγωγή κειμένου)

13. Πως αντιλαμβάνεστε τον όρο "Ασφαλή σύνδεση": (επιλέξτε ένα ή περισσότερα)

a) Οι πληροφορίες που εισάγω μεταφέρονται με ασφάλεια στο διαδίκτυο, ώστε να μην υποκλέπτονται από τρίτο
b) Οι πληροφορίες που εισάγω κρυπτογραφούνται
c) Οι πληροφορίες που εισάγω αποθηκεύονται με ασφάλεια και δεν μπορεί να έχει πρόσβαση κάποιος τρίτος
d) Άλλο (εισαγωγή κειμένου)

4.4.3 Ενότητα Γ: Ευαισθητοποίηση σχετικά με την ασφαλή πλοήγηση

14. "Οι ιστοσελίδες των τραπεζών έχουν λάβει όλα τα απαραίτητα μέτρα για την ασφαλή πλοήγηση των χρηστών".

i. Διαφωνώ απόλυτα
ii. Διαφωνώ
iii. Ούτε διαφωνώ, ούτε συμφωνώ
iv. Συμφωνώ

v. Συμφωνώ απόλυτα

15. "Οι ιστοσελίδες των e-shop έχουν λάβει όλα τα απαραίτητα μέτρα για την ασφαλή πλοήγηση των χρηστών".

i. Διαφωνώ απόλυτα
ii. Διαφωνώ
iii. Ούτε διαφωνώ, ούτε συμφωνώ
iv. Συμφωνώ
v. Συμφωνώ απόλυτα

16. "Οι ιστοσελίδες των δημοσίων φορέων έχουν λάβει όλα τα απαραίτητα μέτρα για την ασφαλή πλοήγηση των χρηστών".

i. Διαφωνώ απόλυτα
ii. Διαφωνώ
iii. Ούτε διαφωνώ, ούτε συμφωνώ
iv. Συμφωνώ
v. Συμφωνώ απόλυτα

17. "Οι ιστοσελίδες των Social media (Facebook, Twitter κλπ) έχουν λάβει όλα τα απαραίτητα μέτρα για την ασφαλή πλοήγηση των χρηστών".

i. Διαφωνώ απόλυτα
ii. Διαφωνώ
iii. Ούτε διαφωνώ, ούτε συμφωνώ
iv. Συμφωνώ
v. Συμφωνώ απόλυτα

18. "Οι ειδησεογραφικές ιστοσελίδες έχουν λάβει όλα τα απαραίτητα μέτρα για την ασφαλή πλοήγηση των χρηστών".

i. Διαφωνώ απόλυτα
ii. Διαφωνώ
iii. Ούτε διαφωνώ, ούτε συμφωνώ
iv. Συμφωνώ
v. Συμφωνώ απόλυτα

4.4.4 Ενότητα Δ: Απαιτήσεις χρηστών κατά την πλοήγηση

19. "Όταν πλοηγούμαι στο Internet ενδιαφέρομαι για την ιδιωτικότητα μου".

i. Διαφωνώ απόλυτα
ii. Διαφωνώ
iii. Ούτε διαφωνώ, ούτε συμφωνώ
iv. Συμφωνώ
v. Συμφωνώ απόλυτα

20. "Όταν πλοηγούμαι στο Internet ενδιαφέρομαι τα στοιχεία που εισάγω να μην γίνονται γνωστά σε τρίτους".

i. Διαφωνώ απόλυτα
ii. Διαφωνώ
iii. Ούτε διαφωνώ, ούτε συμφωνώ
iv. Συμφωνώ
v. Συμφωνώ απόλυτα

21. "Όταν πλοηγούμαι στο Internet ενδιαφέρομαι για την ασφάλεια των πληροφοριών μου".

i. Διαφωνώ απόλυτα
ii. Διαφωνώ
iii. Ούτε διαφωνώ, ούτε συμφωνώ
iv. Συμφωνώ
v. Συμφωνώ απόλυτα

22. "Θα ήθελα τα δεδομένα που πληκτρολογώ στο Internet (π.χ. κωδικοί, προσωπικές πληροφορίες κλπ) να κρυπτογραφούνται".

i. Διαφωνώ απόλυτα
ii. Διαφωνώ
iii. Ούτε διαφωνώ, ούτε συμφωνώ
iv. Συμφωνώ
v. Συμφωνώ απόλυτα

23. "Όταν πλοηγούμαι σε μία ιστοσελίδα, ενδιαφέρομαι να είναι σύγχρονη, με εύκολη δομή και πρόσβαση".

i. Διαφωνώ απόλυτα
ii. Διαφωνώ
iii. Ούτε διαφωνώ, ούτε συμφωνώ
iv. Συμφωνώ
v. Συμφωνώ απόλυτα

4.4.5 Ενότητα Ε: Γνώσεις σε θέματα ασφαλούς πλοήγησης

24. "Ο φυλλομετρητής μου υποστηρίζει τα τελευταία πρωτόκολλα ασφαλείας".

i. Διαφωνώ απόλυτα
ii. Διαφωνώ
iii. Ούτε διαφωνώ, ούτε συμφωνώ
iv. Συμφωνώ
v. Συμφωνώ απόλυτα

25. "Γνωρίζω την οικογένεια πρωτόκολλων ασφαλείας SSL/TLS".

i. Διαφωνώ απόλυτα
ii. Διαφωνώ
iii. Ούτε διαφωνώ, ούτε συμφωνώ
iv. Συμφωνώ
v. Συμφωνώ απόλυτα

26. Ποια-ές από τις παρακάτω ιστοσελίδες θεωρείτε ασφαλείς; (επιλέξτε ένα η περισσότερα)

a. 

b. 

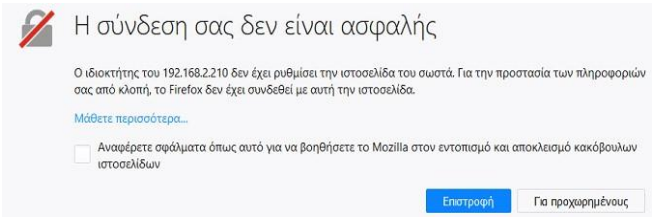
c. 

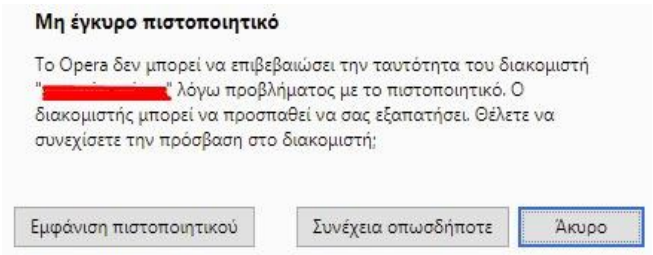
d. 

e. 

f. 

g.

h. 



27. "Γνωρίζω την διαφορά του http από το https".

i. Διαφωνώ απόλυτα
ii. Διαφωνώ
iii. Ούτε διαφωνώ, ούτε συμφωνώ
iv. Συμφωνώ
v. Συμφωνώ απόλυτα

28. "Γνωρίζω πως ελέγχουμε την ασφάλεια ενός πιστοποιητικού σε συνδέσεις https".

i. Διαφωνώ απόλυτα
ii. Διαφωνώ
iii. Ούτε διαφωνώ, ούτε συμφωνώ
iv. Συμφωνώ
v. Συμφωνώ απόλυτα

29. "Γνωρίζω τι σημαίνει το λουκέτο στην γραμμή πλοήγησης του φυλλομετρητή".

i. Διαφωνώ απόλυτα
ii. Διαφωνώ

iii. Ούτε διαφωνώ, ούτε συμφωνώ
iv. Συμφωνώ
v. Συμφωνώ απόλυτα

30. "Γνωρίζω πως μπορώ να προστατευθώ από μία ηλεκτρονική απάτη".

i. Διαφωνώ απόλυτα
ii. Διαφωνώ
iii. Ούτε διαφωνώ, ούτε συμφωνώ
iv. Συμφωνώ
v. Συμφωνώ απόλυτα

31. Ποια-ές από τις παρακάτω επιθέσεις γνωρίζετε (επιλέξτε ένα η περισσότερα)

a) Poodle
b) Freak
c) HeartBleed
d) ROBOT
e) Drown
f) Καμία

4.4.6 Ενότητα ΣΤ: Συμπεριφορά χρηστών κατά την πλοήγηση

32. "Ελέγχω πάντα αν η ιστοσελίδα που επισκέπτομαι είναι https".

i. Διαφωνώ απόλυτα
ii. Διαφωνώ
iii. Ούτε διαφωνώ, ούτε συμφωνώ
iv. Συμφωνώ
v. Συμφωνώ απόλυτα

33. "Ελέγχω πάντα αν η ιστοσελίδα που επισκέπτομαι έχει το χαρακτηριστικό λουκέτο".

i. Διαφωνώ απόλυτα
ii. Διαφωνώ

iii. Ούτε διαφωνώ, ούτε συμφωνώ
iv. Συμφωνώ
v. Συμφωνώ απόλυτα

34. "Αν ο φυλλομετρητής μου βγάλει προειδοποίηση ότι η ιστοσελίδα που μπαίνω δεν είναι ασφαλής, θα διέκοπτα την πλοήγηση μου".

i. Διαφωνώ απόλυτα
ii. Διαφωνώ
iii. Ούτε διαφωνώ, ούτε συμφωνώ
iv. Συμφωνώ
v. Συμφωνώ απόλυτα

35. "Αν γνώριζα ότι μία ιστοσελίδα που χρησιμοποιώ συχνά δεν είναι ασφαλής, θα σταματούσα να την χρησιμοποιώ".

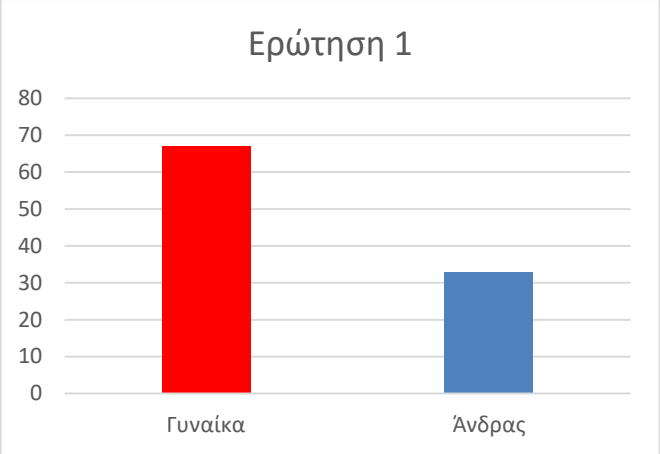
i. Διαφωνώ απόλυτα
ii. Διαφωνώ
iii. Ούτε διαφωνώ, ούτε συμφωνώ
iv. Συμφωνώ
v. Συμφωνώ απόλυτα

4.5 Αποτελέσματα και συζήτηση

Παρακάτω παρουσιάζονται τα δεδομένα που συλλέχθηκαν από το ερωτηματολόγιο, για κάθε μία από τις έξι εννοιολογικές ενότητες.

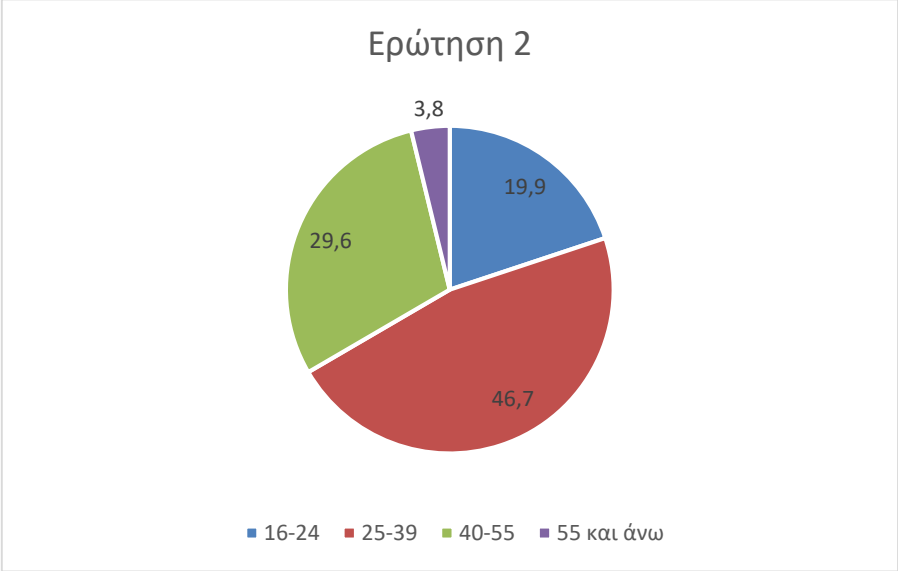
4.5.1 Ενότητα Α: Δημογραφικά στοιχεία

Σύμφωνα με τα δημογραφικά στοιχεία λάβαμε τις εξής απαντήσεις όσον αφορά το φύλο: 67 % γυναίκες, 33% άνδρες. Συνεπώς οι γυναίκες αποτελούν τα 2/3 του δείγματος.



Διάγραμμα 4.42: Απαντήσεις στην ερώτηση 1 «Επιλέξτε φύλο»

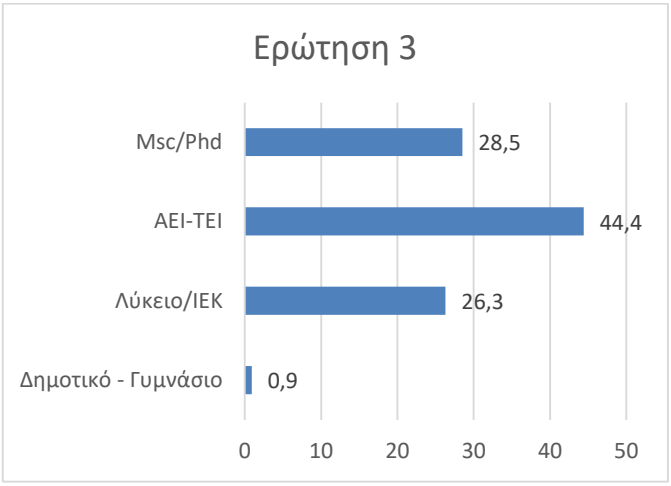
Όσον αφορά την ηλικία των ερωτηθέντων, κατανεμήθηκαν σε τέσσερις κατηγορίες και έλαβαν τα εξής ποσοστά: 20% (16-24), 47% (25-39), 30% (40-55) και 4% (55 και άνω).



Διάγραμμα 4.43: Απαντήσεις στην ερώτηση 2 «Ηλικία»

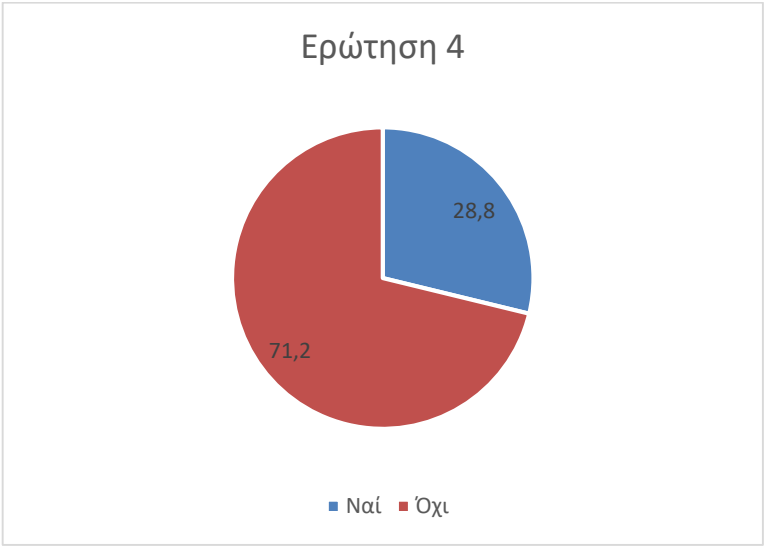
Όσον αφορά το μορφωτικό επίπεδο από τις τέσσερεις κατηγορίες (απόφοιτος δημοτικού, απόφοιτος λυκείου/ΙΕΚ, απόφοιτος ΑΕΙ/ΑΤΕΙ, κάτοχος μεταπτυχιακού-διδακτορικού) επιλέχθηκαν τρεις τελικές κατηγορίες (απόφοιτος γυμνασίου/λυκείου, απόφοιτος ανώτατης εκπαίδευσης (ΑΕΙ/ΑΤΕΙ), απόφοιτος μεταπτυχιακού/διδακτορικού). Σύμφωνα με τα δεδομένα που συλλέχθηκαν εκ των

ερωτηθέντων ποσοστό 27 % έχουν ολοκληρώσει τη μέση εκπαίδευση, 44 % έχουν αποφοιτήσει από ΑΕΙ/ΑΤΕΙ και 28 % είναι κάτοχοι μεταπτυχιακού/διδακτορικού.



Διάγραμμα 4.44: Απαντήσεις στην ερώτηση 3 «Μορφωτικό επίπεδο»

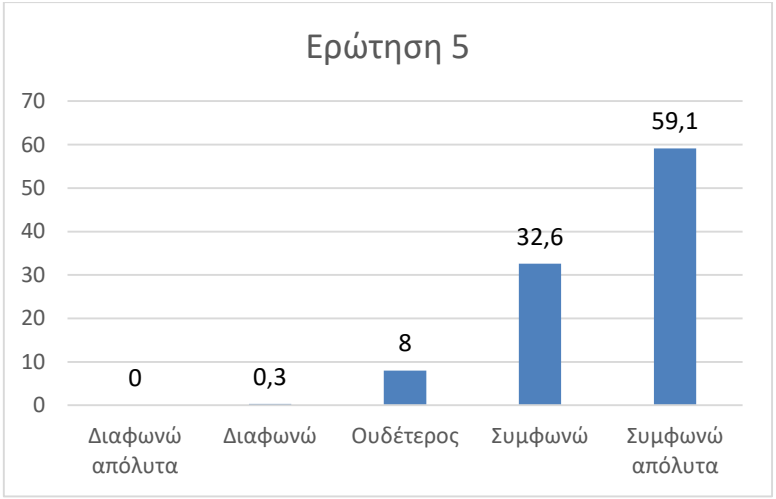
Το 1/3 (29%) των ερωτηθέντων είχε σπουδές σχετικές με την επιστήμη Υπολογιστών ή την Πληροφορική, γεγονός που πιθανόν τους καθιστά πιο εξοικειωμένους με το θέμα του ερωτηματολογίου και ίσως κατέχουν πιο εξειδικευμένες γνώσεις όσον αφορά την ασφάλεια κατά την πλοήγηση στο διαδίκτυο.



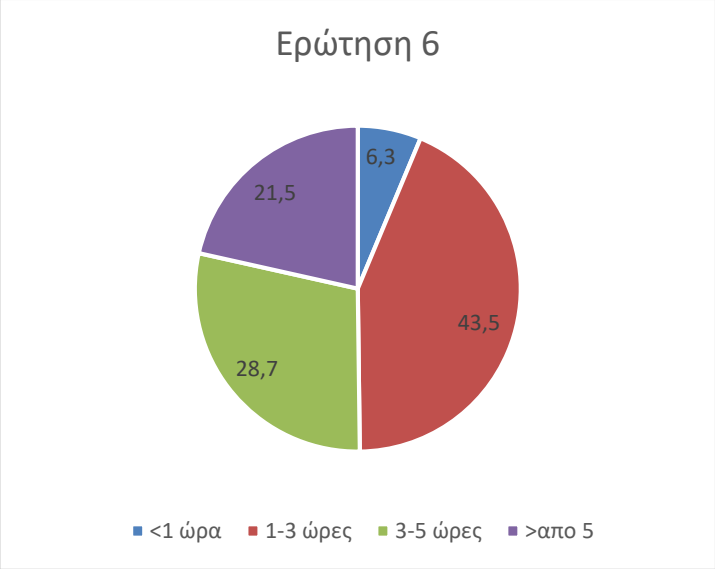
Διάγραμμα 4.45: Απαντήσεις στην ερώτηση 4 «Έχετε σπουδές σχετικές με την Επιστήμη Υπολογιστών ή την Πληροφορική;»

4.5.2 Ενότητα Β: Πληροφορίες σχετικά με την χρήση διαδικτύου

Η πλειοψηφία των χρηστών (91,7%) δήλωσαν εξοικειωμένοι με την χρήση του internet και πλοηγούνται καθημερινά σε αυτό για 1-3 ώρες (43%), ποσοστό 29% για 3-5 ώρες, 1/5 (21%) των χρηστών για περισσότερες από 5 ώρες και μόνο 6% λιγότερο από 1 ώρα. Στην μελέτη των (Furnell and Karweni, 1999) η οποία διεξήχθη το 1999 στο Ηνωμένο Βασίλειο με την μικτή χρήση on-line ερωτηματολογίου και την διανομή έντυπου ερωτηματολογίου σε 64 χρήστες, το 45% των χρηστών χρησιμοποιούσε το Internet για 1 με 4 ώρες την ημέρα, 36% έως οκτώ ώρες και 14% άνω των οκτώ ωρών. Μόνο το 2% από το δείγμα που ελέγχθηκε το χρησιμοποιούσε για λιγότερο από μία ώρα.

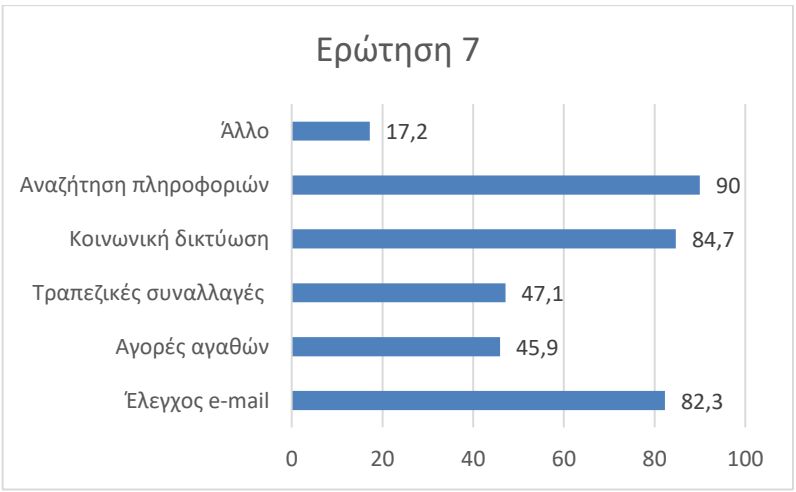


Διάγραμμα 4.46: Απαντήσεις στον ισχυρισμό 5 «Είμαι εξοικειωμένος με την χρήση του Internet».



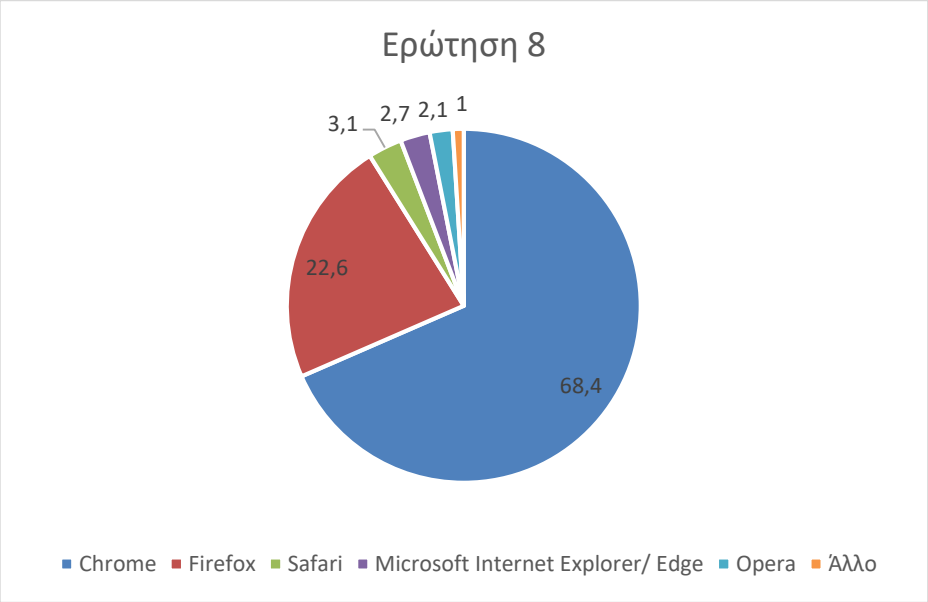
Διάγραμμα 4.47: Απαντήσεις στην ερώτηση 6 «Χρόνος πλοήγησης στο Internet καθημερινά»

Οι κύριοι λόγοι χρήσης του Διαδικτύου ήταν η αναζήτηση πληροφοριών (90%), η κοινωνική δικτύωση (85%) και ο έλεγχος των e-mail (82%). Οι μισοί εκ των ερωτηθέντων πραγματοποιούσαν επίσης τραπεζικές συναλλαγές (47%) και αγορά αγαθών (46%). Η χρήση του διαδικτύου σε αντίστοιχη μελέτη επικεντρώθηκε στην αποστολή e-mail (52%), στην αγορά προϊόντων (22%) και αναζήτηση πληροφοριών (50%) (Furnell and Karweni, 1999). Ας μην ξεχνάμε βέβαια ότι στο χρονικό πλαίσιο στο οποίο διεξήχθη η έρευνα είναι το 1999, περίοδος στην οποία το διαδίκτυο δεν είχε την διάδοση που έχει στις μέρες μας.

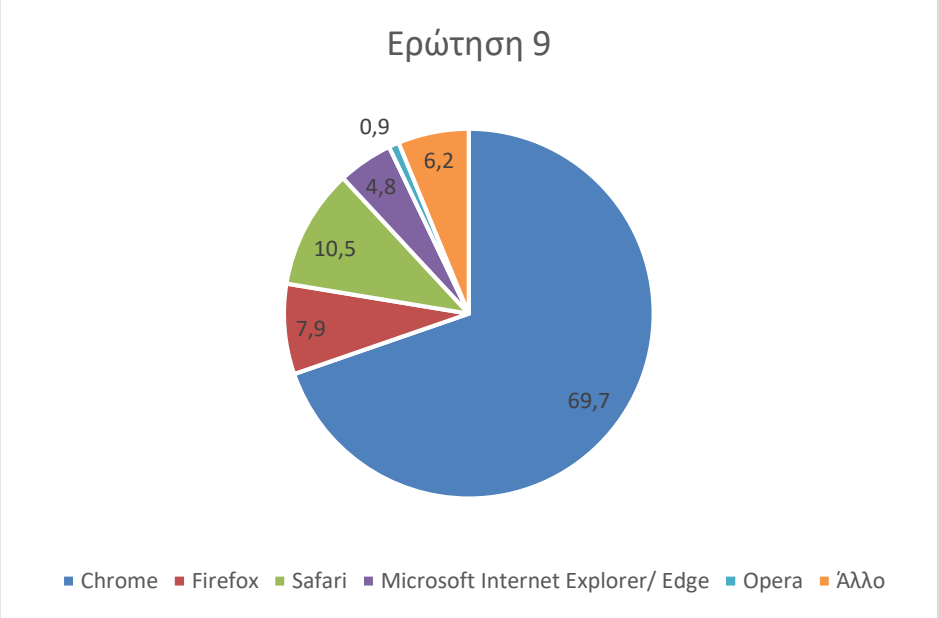


Διάγραμμα 4.48: Απαντήσεις στην ερώτηση 7 «Για ποιους λόγους χρησιμοποιείτε κυρίως το Internet?»

Η πλειοψηφία των ερωτηθέντων χρησιμοποιούν ως φυλλομετρητή (browser) τον Chrome και τα αντίστοιχα ποσοστά στον υπολογιστή και το κινητό είναι 68 και 70%. Η κατανομή των υπόλοιπων φυλλομετρητών (Firefox, Safari, Microsoft Internet Explorer/Edge και Opera αποτυπώνεται στα Διάγραμμα 4.49 και Διάγραμμα 4.50

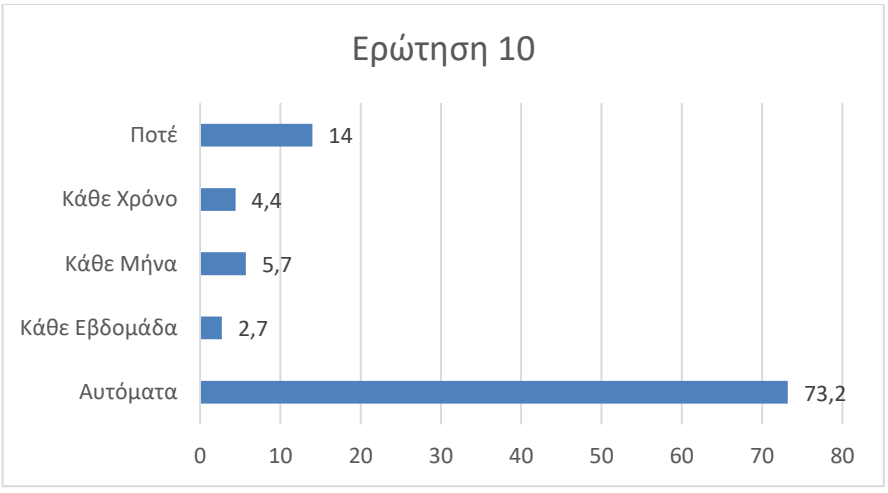


Διάγραμμα 4.49: Απαντήσεις στην ερώτηση 8 «Ποιο φυλλομετρητή (browser) χρησιμοποιείτε κυρίως στον υπολογιστή σας;»



Διάγραμμα 4.50: Απαντήσεις στην ερώτηση 9 «Ποιο φυλλομετρητή (browser) χρησιμοποιείτε κυρίως στο κινητό σας;»

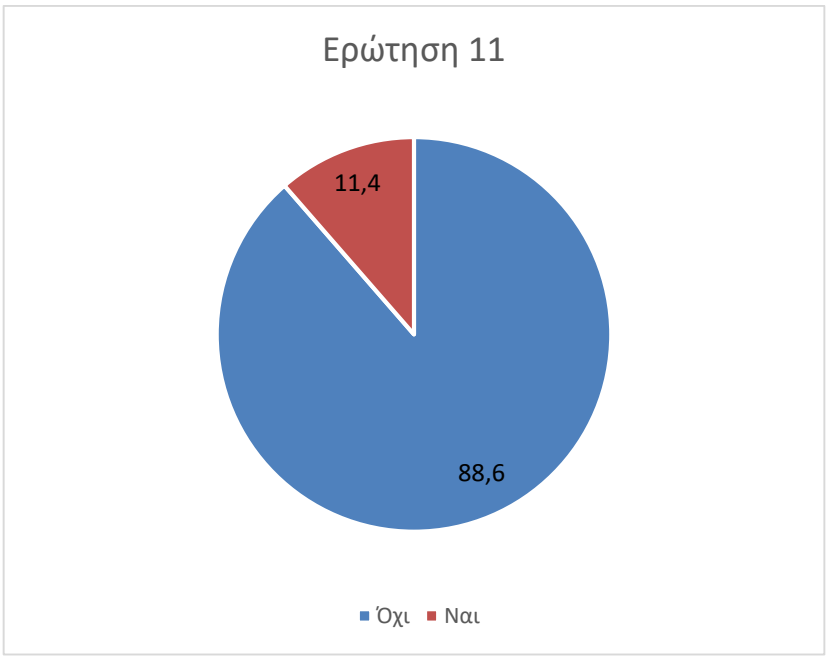
Ο κύριος τρόπος αναβάθμισης του φυλλομετρητή των χρηστών είναι ο αυτόματος (73%), ενώ σε ποσοστό 14% οι χρήστες δεν τον αναβαθμίζουν ποτέ.



Διάγραμμα 4.51: Απαντήσεις στην ερώτηση 10 «Πόσο συχνά αναβαθμίζετε τον φυλλομετρητή σας;»

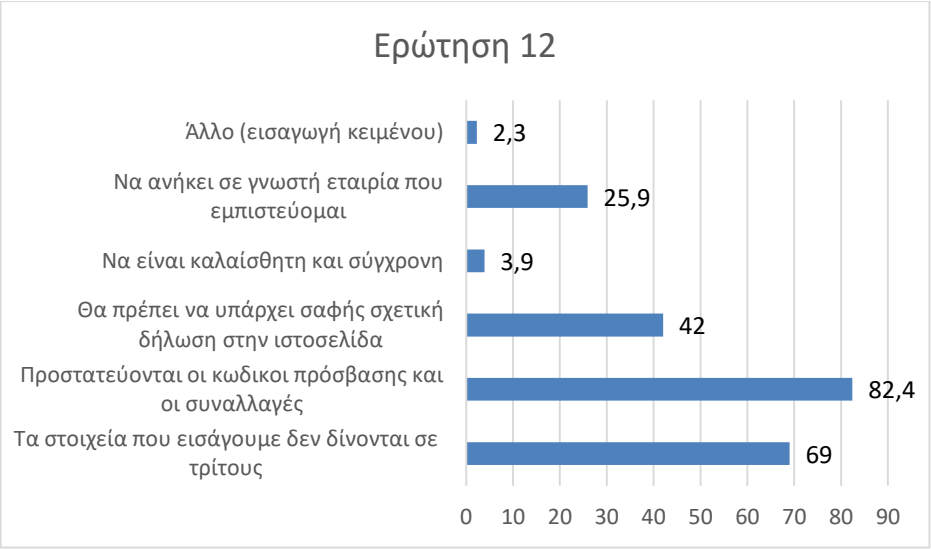
Η πλειοψηφία των χρηστών (88,6%) δεν έχει πέσει θέμα κάποιας ηλεκτρονικής απάτης που αφορούσε κλοπή συνθηματικών ή στοιχεία πιστωτικής κάρτας. Το φύλο, η ηλικία, το μορφωτικό επίπεδο (ανώτατο επίπεδο εκπαίδευσης που έχει συμπληρωθεί), και η

ύπαρξη σπουδών σχετικών με την επιστήμη των υπολογιστών δεν φαίνεται να επηρεάζει την πιθανότητα ηλεκτρονικής απάτης καθώς δεν υπάρχει στατιστικώς σημαντική διαφορά μεταξύ των κατηγοριών (P>0.05).



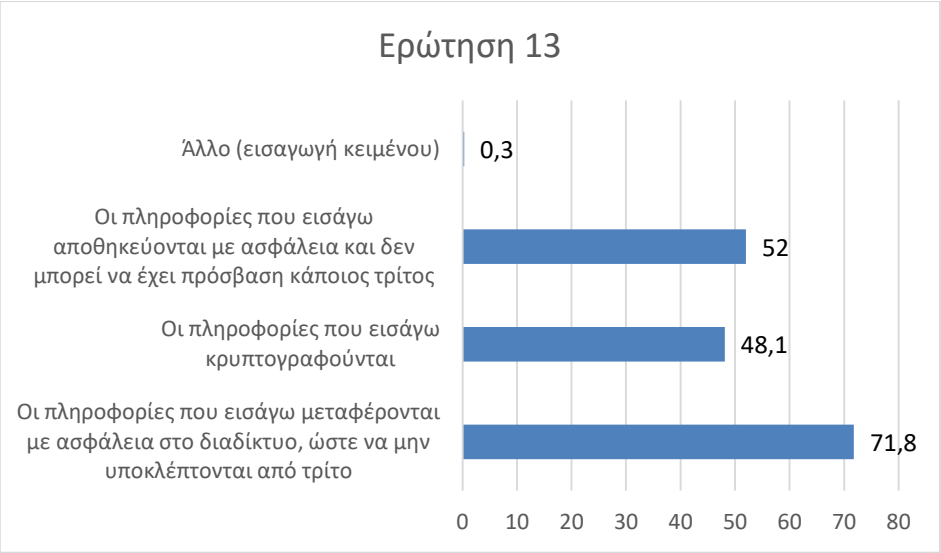
Διάγραμμα 4.52: Απαντήσεις στην ερώτηση 11 «Έχετε πέσει θύμα κάποιας ηλεκτρονικής απάτης (κλοπή συνθηματικών, στοιχεία πιστωτικής κάρτας);»

Στην ερώτηση «πώς αντιλαμβάνεστε τον όρο ασφαλή ιστοσελίδα», 82,4% των ερωτηθέντων επέλεξαν την προστασία των κωδικών πρόσβασης και των συναλλαγών, 69% απαντά με το να μην δίνονται τα στοιχεία που εισάγουν σε τρίτους και 42% απαντά με το να υπάρχει σαφής σχετική δήλωση στην ιστοσελίδα. Επιπλέον, 1 στους 4 χρήστες συνέδεσαν τον όρο ασφαλή ιστοσελίδα με το να ανήκει σε γνωστή εταιρεία που εμπιστεύονται και μόνο 3,9% να είναι σύγχρονη και καλαίσθητη.



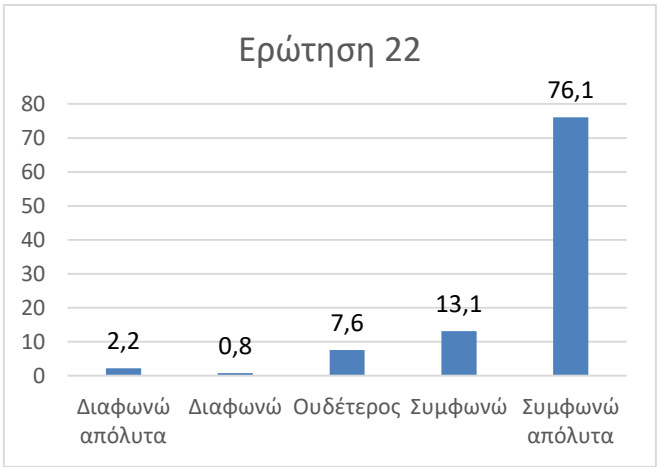
Διάγραμμα 4.53: Απαντήσεις στην ερώτηση 12 «Πώς αντιλαμβάνεστε τον όρο "Ασφαλή Ιστοσελίδα"».

Στην ερώτηση «πώς αντιλαμβάνεστε τον όρο ασφαλή σύνδεση», οι χρήστες είχαν την δυνατότητα για πολλαπλές απαντήσεις και αναφέρθηκαν στην ασφαλή μεταφορά των πληροφορίων (71,8%), στην ασφαλή αποθήκευση των πληροφοριών (52%) και στην κρυπτογράφηση των πληροφοριών (48,1%). Οι (Friedman et al., 2002) στην μελέτη που έκαναν σε τρεις πολιτείες των Ηνωμένων Πολιτειών και σε 72 χρήστες με συνέντευξη, στον κατανόηση του ορισμού της ασφαλούς σύνδεσης το 27% ανέφερε την προστασία των πληροφοριών κατά την μεταφορά τους στο web, το 22% στην κρυπτογράφηση των πληροφοριών και το 8% στη προστασία των πληροφοριών κατά την αποθήκευση.

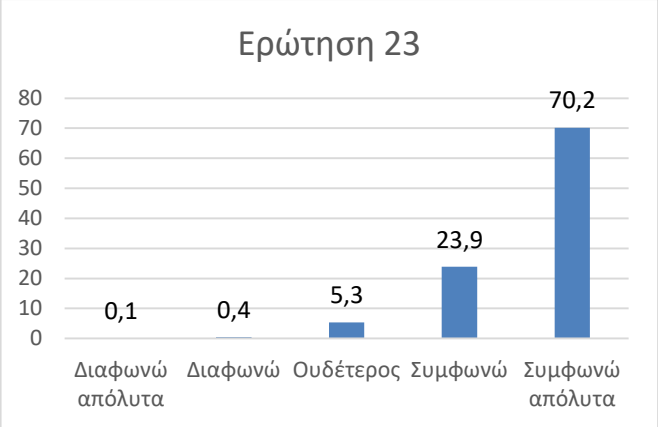


Διάγραμμα 4.54: Απαντήσεις στην ερώτηση 13 «Πως αντιλαμβάνεστε τον όρο "Ασφαλή σύνδεση"».

Ποσοστό 89,2% επιθυμούν τα δεδομένα που πληκτρολογούν στο Internet (π.χ. κωδικοί, προσωπικές πληροφορίες κλπ.) να κρυπτογραφούνται. Ομοίως, μεγάλο ποσοστό των χρηστών (94,1%) ενδιαφέρονται όταν πλοηγούνται σε μία ιστοσελίδα, να είναι σύγχρονη, με εύκολη δομή και πρόσβαση.

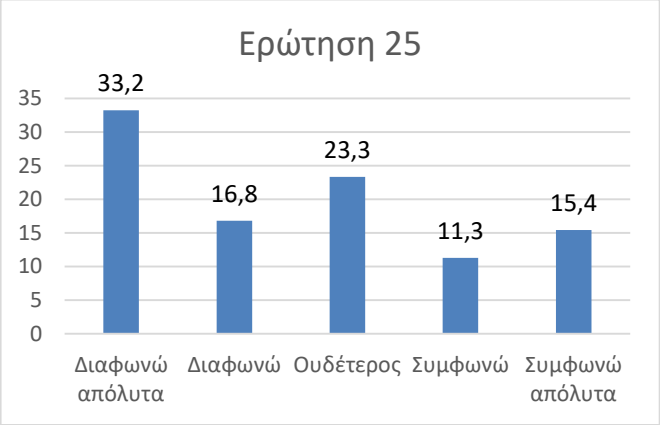


Διάγραμμα 4.55: Απαντήσεις στον ισχυρισμό 22 "Θα ήθελα τα δεδομένα που πληκτρολογώ στο Internet (π.χ. κωδικοί, προσωπικές πληροφορίες κλπ) να κρυπτογραφούνται"



Διάγραμμα 4.56: Απαντήσεις στον ισχυρισμό 23 "Όταν πλοηγούμαι σε μία ιστοσελίδα, ενδιαφέρομαι να είναι σύγχρονη, με εύκολη δομή και πρόσβαση".

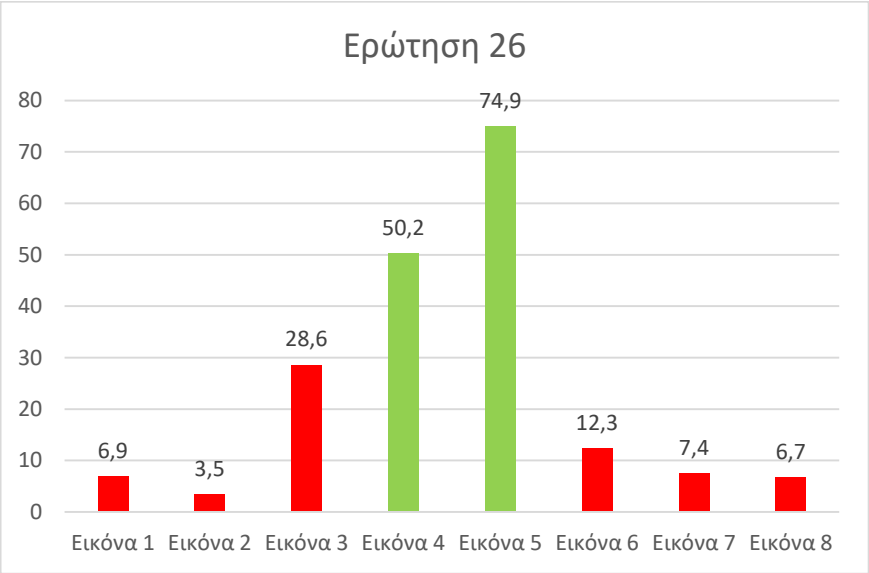
Μόνο η μειοψηφία των συμμετεχόντων στην έρευνα (26,7%) γνωρίζουν την οικογένεια πρωτοκόλλων ασφάλειας SSL/TLS.



Διάγραμμα 4.57: Απαντήσεις στον ισχυρισμό 25 "Γνωρίζω την οικογένεια πρωτόκολλων ασφαλείας SSL/TLS".

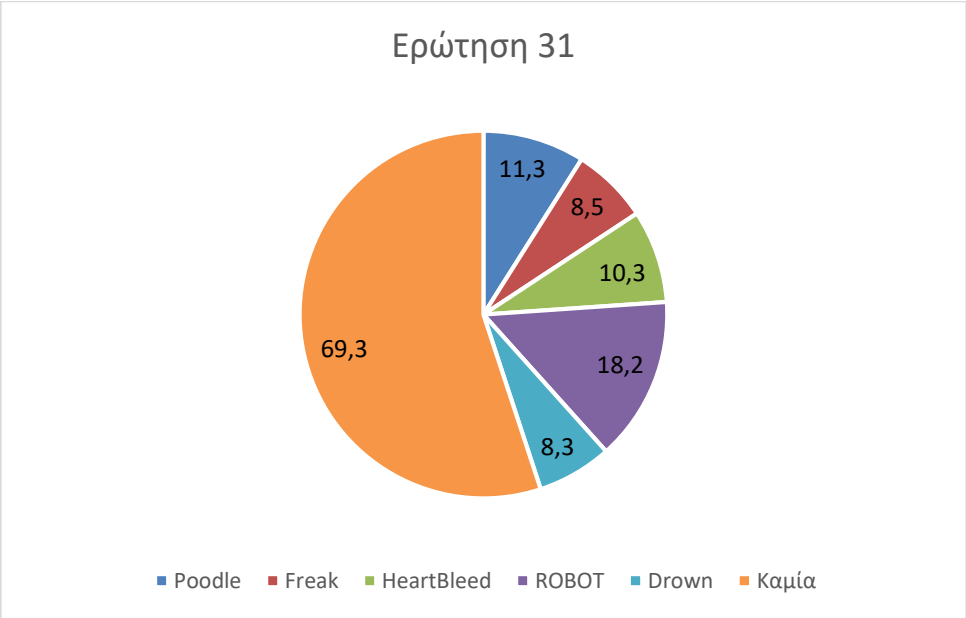
Στην ερώτηση που αφορά την επιλογή ποιες από τις εικόνες που δίνονται είναι ασφαλείς, ποσοστό 74,9% αναγνώρισε σωστά την ιστοσελίδα με το χαρακτηριστικό https (εικόνα 5), ενώ οι μισοί από τους ερωτηθέντες επέλεξαν ως ασφαλή την ιστοσελίδα με το λουκέτο (εικόνα 4). Οι μη ασφαλείς ιστοσελίδες (εικόνα 1, 2, 3, 6, 7, 8) επιλέχθηκαν εσφαλμένα από τους χρήστες σε ποσοστά που κυμαινόταν από 3,5 έως 28,6%. Σε παρόμοια μελέτη και στο ερώτημα κατά πόσο οι χρήστες μπορούν να αναγνωρίσουν μία ασφαλή

ιστοσελίδα το 20% αναγνώρισαν σωστά ως ασφαλείς ιστοσελίδες αυτές που χρησιμοποιούσαν https και 53% αυτές που έφεραν το χαρακτηριστικό λουκέτο [84].



Διάγραμμα 4.58: Απαντήσεις στην ερώτηση 26 για το ποιες ιστοσελίδες θεωρείτε ασφαλείς;

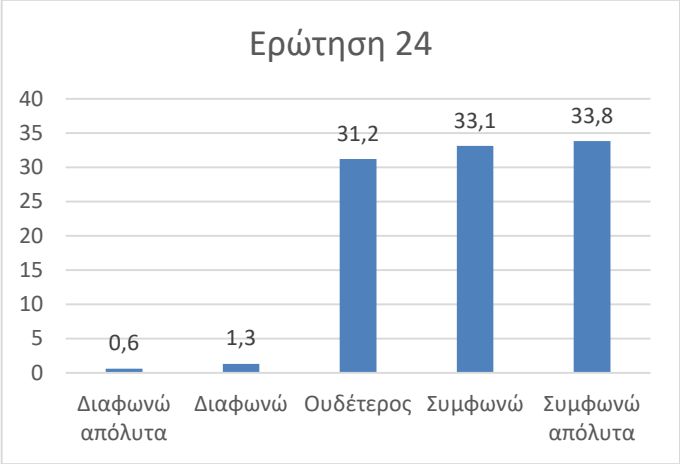
Τα ποσοστά αναγνώρισης επιθέσεων του πρωτοκόλλου TLS από τους ερωτηθέντες είναι τα εξής: Poodle (11,3%), Freak (8,5%), HeartBleed (10,3%), ROBOT (18,2%) και Drown (8,3%). Ωστόσο, το 69,3% των χρηστών δεν γνωρίζουν καμία από τις παραπάνω επιθέσεις.



Διάγραμμα 4.59: Απαντήσεις στην ερώτηση 12 «Ποια-ές από τις παρακάτω επιθέσεις γνωρίζετε».

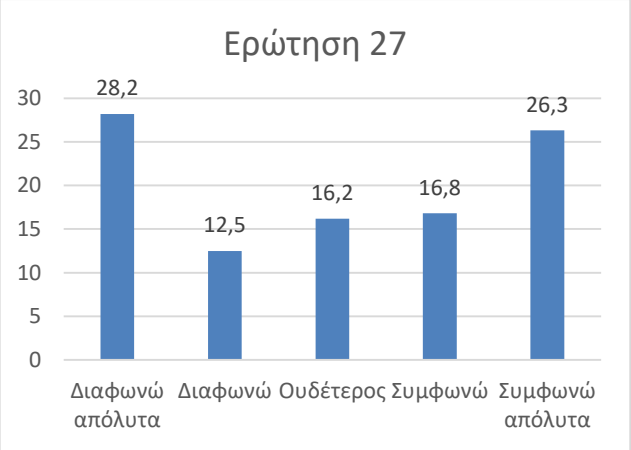
4.5.3 Εννοιολογική κατασκευή Α: «Γνώσεις σε θέματα ασφαλούς πλοήγησης»

Σε αυτή την εννοιολογική κατασκευή οι χρήστες κλήθηκαν να αποτυπώσουν τις γνώσεις τους σε θέματα ασφαλούς πλοήγησης. Συγκεκριμένα μελετήθηκαν οι γνώσεις τους σχετικά με τον έλεγχο πρωτοκόλλων ασφαλείας, του https και του λουκέτου ασφαλείας στην γραμμή του φυλλομετρητή. Ποσοστό 66,9% συμφωνεί/ συμφωνεί απόλυτα στον ισχυρισμό ότι φυλλομετρητής τους υποστηρίζει τα τελευταία πρωτόκολλα ασφαλείας, ενώ 1 στους 3 χρήστες δεν διαθέτει αυτή την γνώση.



Διάγραμμα 4.60: Απαντήσεις στον ισχυρισμό 24 «Ο φυλλομετρητής μου υποστηρίζει τα τελευταία πρωτόκολλα ασφαλείας.»

Σημαντικό ποσοστό της τάξης του 4,7% δεν γνωρίζει την διαφορά του http και https, έναντι του 43,1% που είναι γνώστες αυτής της πληροφορίας.

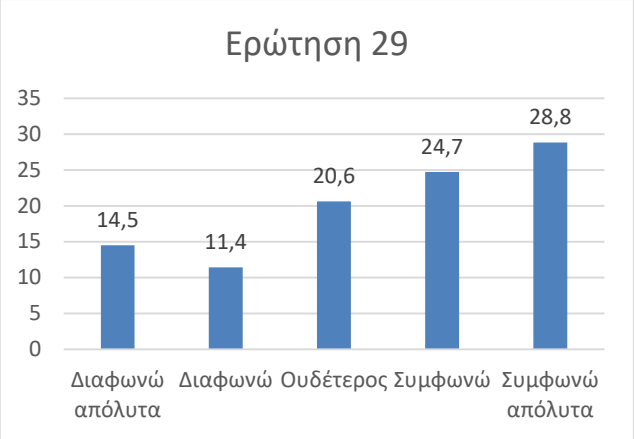


Διάγραμμα 4.61: Απαντήσεις στον ισχυρισμό 27 «Γνωρίζω την διαφορά του http από το https.»

Μόνο 1 στους 3 ερωτηθέντες (27,3%) γνωρίζει πώς να ελέγξει την ασφάλεια ενός πιστοποιητικού σε συνδέσεις https, ποσοστό αντίστοιχο με τους χρήστες που έχουν σπουδές σχετικές με την επιστήμη Υπολογιστών ή την Πληροφορική.

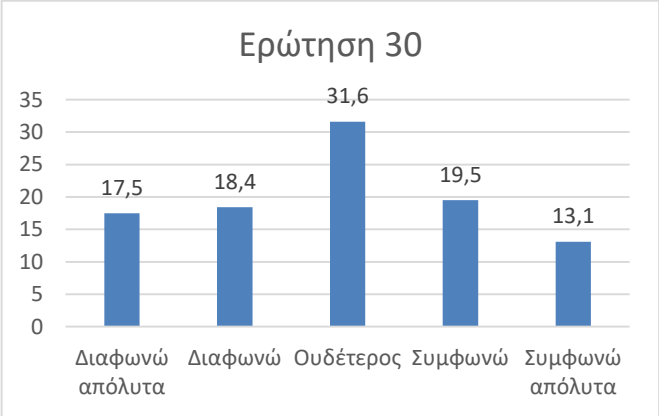
Διάγραμμα 4.62: Απαντήσεις στον ισχυρισμό 28 «Γνωρίζω πως ελέγχουμε την ασφάλεια ενός πιστοποιητικού σε συνδέσεις https.»

Οι μισοί από τους χρήστες (53,5%) γνωρίζουν τι σημαίνει το λουκέτο στην γραμμή πλοήγησης του φυλλομετρητή.



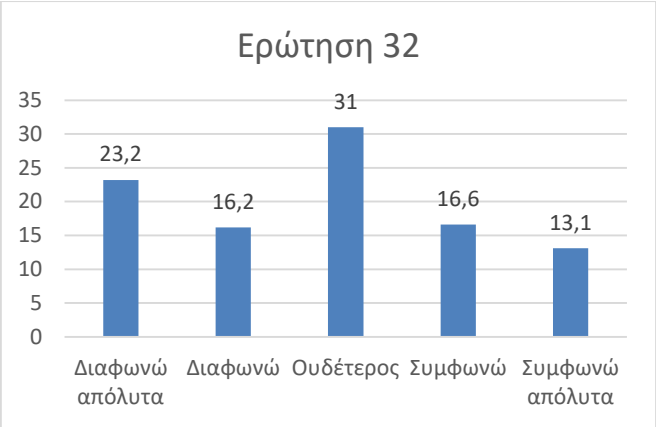
Διάγραμμα 4.63: Απαντήσεις στον ισχυρισμό 29 «Γνωρίζω τι σημαίνει το λουκέτο στην γραμμή πλοήγησης του φυλλομετρητή.»

Ποσοστό 35,9% πιστεύει ότι δεν γνωρίζει πως να προστατευθεί από μια ηλεκτρονική απάτη, ενώ 1 στους 3 χρήστες εκφράζει αβεβαιότητα για το αν μπορεί, σε αντίθεση με το 32,6% που έχει την γνώση αυτή.

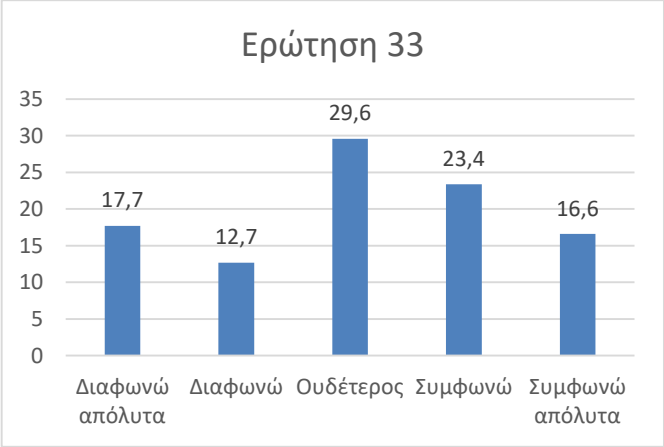


Διάγραμμα 4.64: Απαντήσεις στον ισχυρισμό 30 «Γνωρίζω πως μπορώ να προστατευθώ από μία ηλεκτρονική απάτη.»

Ένα μικρό ποσοστό της τάξης του 29,7% ελέγχουν αν η ιστοσελίδα που επισκέπτονται είναι https και 4 στους 10 χρήστες αν έχει το χαρακτηριστικό λουκέτο αντίστοιχα.



Διάγραμμα 4.65: Απαντήσεις στον ισχυρισμό 32 «Ελέγχω πάντα αν η ιστοσελίδα που επισκέπτομαι είναι https.»

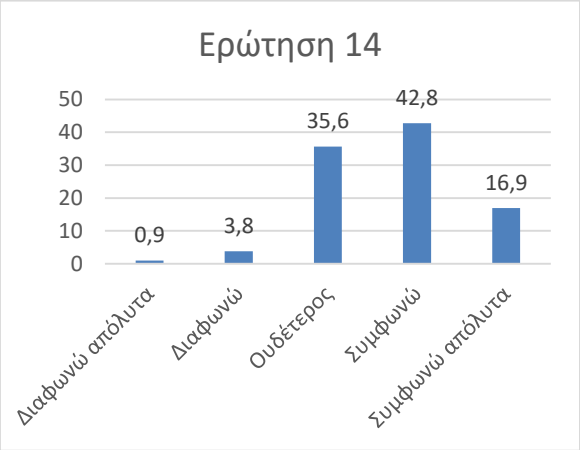


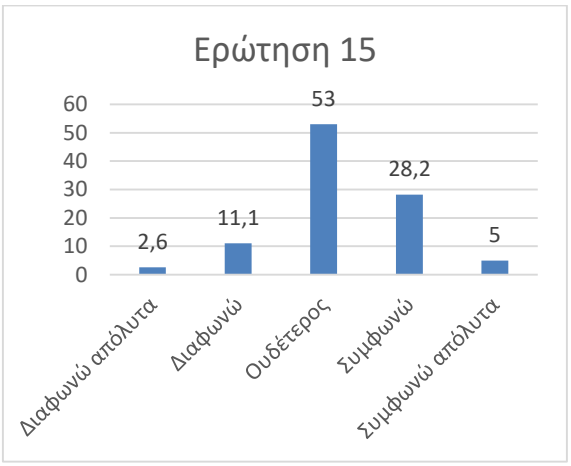
Διάγραμμα 4.66: Απαντήσεις στον ισχυρισμό 33 «Ελέγχω πάντα αν η ιστοσελίδα που επισκέπτομαι έχει το χαρακτηριστικό λουκέτο.»

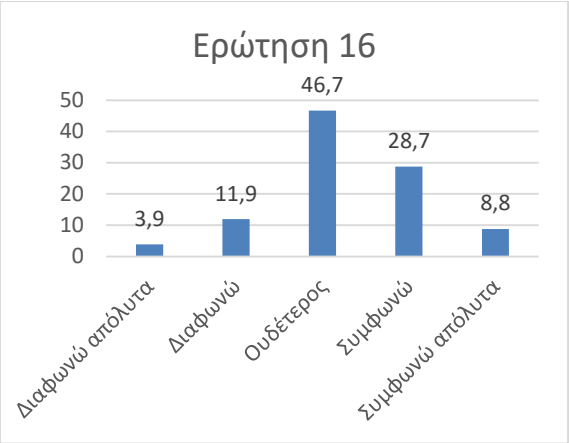
4.5.4 Εννοιολογική κατασκευή Β: «Ευαισθητοποίηση/ πεποιθήσεις σχετικά με την ασφαλή πλοήγηση»

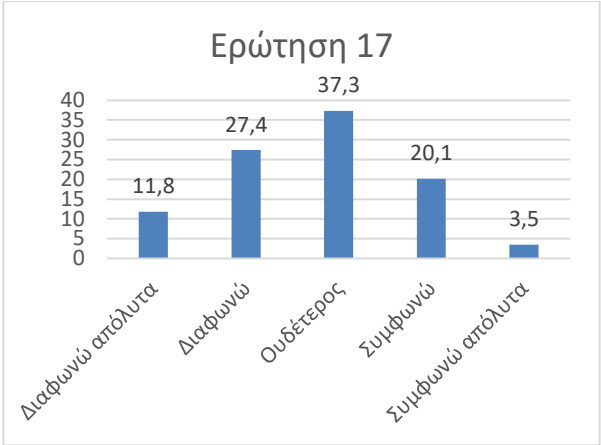
Σε αυτή την εννοιολογική κατασκευή οι χρήστες κλήθηκαν να αποτυπώσουν τις πεποιθήσεις τους στο κατά πόσο συγκεκριμένες κατηγορίες ιστοτόπων λαμβάνουν τα απαραίτητα μέτρα για την ασφαλή πλοήγηση των χρηστών τους. Οι κατηγορίες που επιλέχθηκαν ήταν οι τράπεζες, τα e-shop, οι δημόσιοι φορείς, οι ειδησεογραφικές και τα κοινωνικά δίκτυα (Facebook, twitter κτλ.). Οι τέσσερις πρώτες επιλέχθηκαν λόγω του συσχετισμού τους με το πρώτο πειραματικό μέρος της μεταπτυχιακής διατριβής έτσι

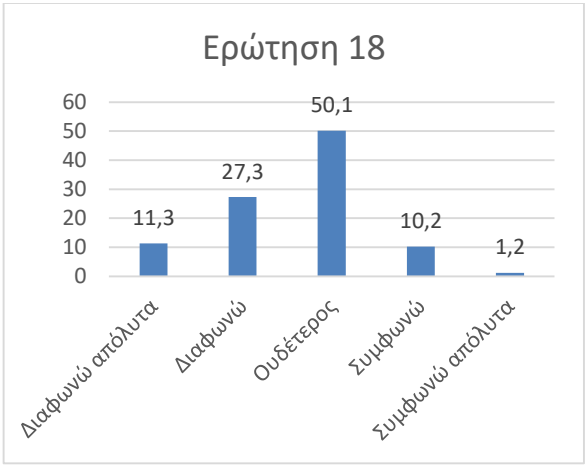
ώστε να σφυγμομετρηθεί η γνώμη του κοινού και η κατηγορία των κοινωνικών δικτύων λόγω της εκτεταμένης χρήσης τους. Σύμφωνα με τα αποτελέσματα των ερωτήσεων 14 έως 18, η σειρά κατάταξης των κατηγοριών ιστοτόπων σε σχέση με την αξιοπιστία με φθίνουσα τάση είναι: τράπεζες, δημόσιοι φορείς, e-shop, κοινωνικά δίκτυα και ειδησεογραφικές. Συγκεκριμένα, 60% των ερωτηθέντων συμφωνούν/ συμφωνούν απόλυτα ότι οι τράπεζες έχουν λάβει όλα τα απαραίτητα μέτρα για την ασφαλή πλοήγηση, ενώ τα ποσοστά για τους δημόσιους φορείς και τα e-shop διαμορφώνονται στο 38% και 33%, αντίστοιχα. Η αρνητική τάση εμπιστοσύνης στις ειδησεογραφικές ιστοσελίδες και τα κοινωνικά δίκτυα φαίνεται από το γεγονός ότι ποσοστά 38 και 39 % αντίστοιχα διαφωνούν/ διαφωνούν απόλυτα ότι οι παραπάνω κατηγορίες ιστοτόπων λαμβάνουν τα απαραίτητα μέτρα. Παρακάτω ακολουθούν τα αναλυτικά διαγράμματα με τις αντίστοιχες απαντήσεις των χρηστών και τα ποσοστά ανά κατηγορία ιστοτόπων.







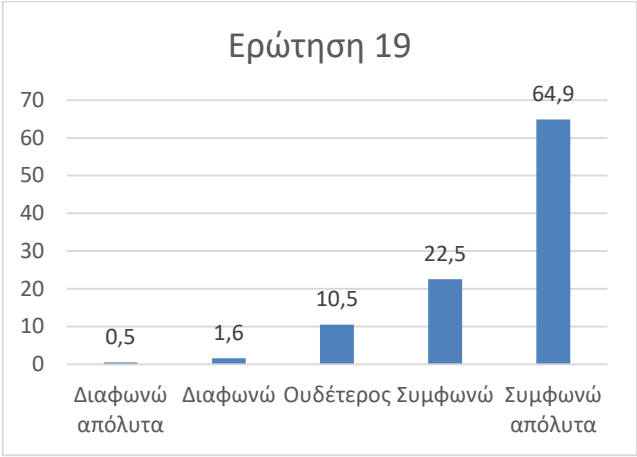




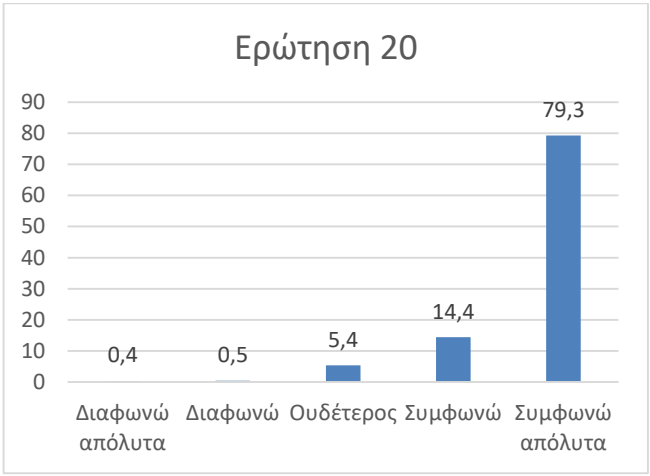
Διάγραμμα 4.67: Απαντήσεις στις ερωτήσεις 14, 15, 16, 17, 18: Οι ιστοσελίδες των τραπεζών (14) , e-shop (15), δημοσίων φορέων (16), ειδησεογραφικών (17) και social media (Facebook, Twitter κτλ.) (18) έχουν λάβει όλα τα απαραίτητα μέτρα για την ασφαλή πλοήγηση των χρηστών.

4.5.5 Εννοιολογική κατασκευή Γ: «Απαιτήσεις χρηστών κατά την πλοήγηση»

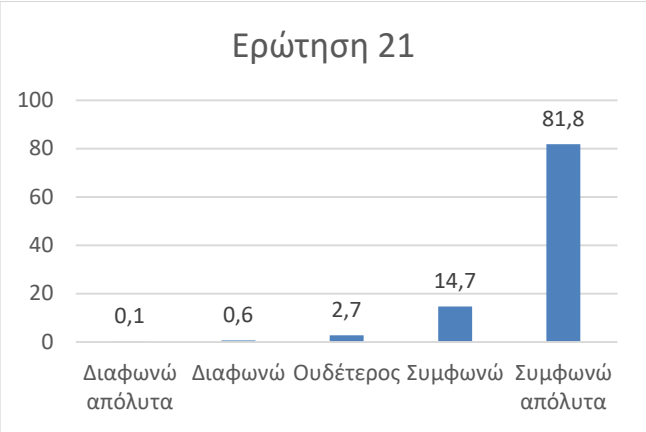
Η πλειοψηφία των χρηστών (87,4%) συμφωνεί/ συμφωνεί απόλυτα ότι ενδιαφέρεται για την ιδιωτικότητα του όταν πλοηγείτε στο Internet. Αντίστοιχα υψηλά ποσοστά χρηστών δεν θέλουν τα στοιχεία που εισάγουν κατά τη χρήση του διαδικτύου να γίνονται γνωστά σε τρίτους (93,7%). Ομοίως σχεδόν όλοι οι ερωτηθέντες (96,5%) ενδιαφέρονται για την ασφάλεια των πληροφοριών τους όταν πλοηγούνται στο διαδίκτυο.



Διάγραμμα 4.68: Απαντήσεις στον ισχυρισμό 19 «Όταν πλοηγούμαι στο Internet ενδιαφέρομαι για την ιδιωτικότητα μου».



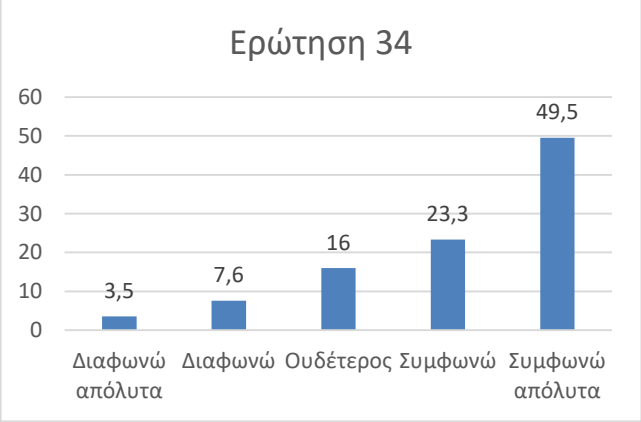
Διάγραμμα 4.69: Απαντήσεις στον ισχυρισμό 20 «Όταν πλοηγούμαι στο Internet ενδιαφέρομαι τα στοιχεία που εισάγω να μην γίνονται γνωστά σε τρίτους».



Διάγραμμα 4.70: Απαντήσεις στον ισχυρισμό 21 «Όταν πλοηγούμαι στο Internet ενδιαφέρομαι για την ασφάλεια των πληροφοριών μου».

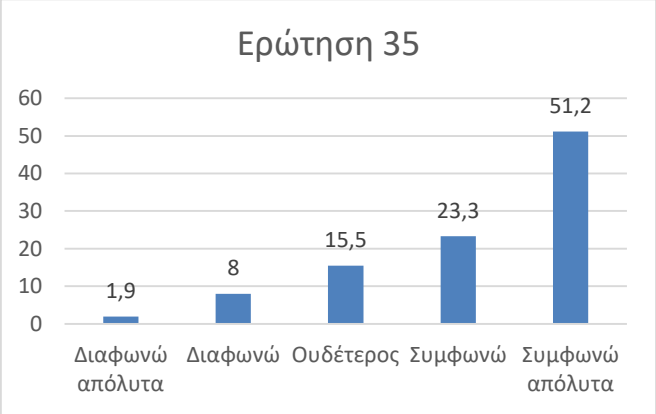
4.5.6 Εννοιολογική κατασκευή Δ: «Συμπεριφορά χρηστών κατά την πλοήγηση»

Ποσοστό 72% των χρηστών συμφωνούν/ συμφωνούν απόλυτα ότι θα διέκοπταν την πλοήγησή τους αν ο φυλλομετρητής τους έβγαζε προειδοποίηση ότι η ιστοσελίδα που εισέρχονται δεν είναι ασφαλής. Ωστόσο, 1 στους 10 χρήστες θα συνέχιζε την πλοήγηση του και ποσοστό 16% είναι αναποφάσιστοι ως προς την συμπεριφορά που θα ακολουθούσαν.



Διάγραμμα 4.71: Απαντήσεις στον ισχυρισμό 34 «Αν ο φυλλομετρητής μου βγάλει προειδοποίηση ότι η ιστοσελίδα που μπαίνω δεν είναι ασφαλής, θα διέκοπτα την πλοήγηση μου».

Ποσοστό 10% των χρηστών θα συνέχιζε να χρησιμοποιεί μια ιστοσελίδα ακόμη κι αν γνώριζε ότι δεν ήταν ασφαλής. Ωστόσο 7 στους 10 χρήστες θα σταματούσαν να μπαίνουν στη μη ασφαλή ιστοσελίδα ακόμη και αν τη χρησιμοποιούσαν συχνά, ενώ 15,5% των χρηστών δεν τους ενδιαφέρει αν θα είναι ασφαλής ή όχι η ιστοσελίδα. Σε on-line μελέτη [85] που έγινε σε 237 χρήστες του Καναδά, του Ηνωμένου Βασιλείου και των Ηνωμένων Πολιτειών το 60% των χρηστών δήλωσε ότι θα σταματούσε να χρησιμοποιεί κάποια ιστοσελίδα αν γνώριζε ότι δεν ήταν ασφαλής.



Διάγραμμα 4.72: Απαντήσεις στον ισχυρισμό 35 «Αν γνώριζα ότι μία ιστοσελίδα που χρησιμοποιώ συχνά δεν είναι ασφαλής, θα σταματούσα να την χρησιμοποιώ».

4.5.7 Συγκρίσεις μεταξύ εννοιολογικών κατασκευών

Οι εννοιολογικές κατασκευές (constructs) δεν ακολουθούν την κανονική κατανομή καθώς το $p<0.05$.

Tests of Normality

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Γνώσεις σε θέματα ασφαλούς πλοήγησης	,052	772	,000	,978	772	,000
Ευαισθητοποίηση/ πεποιθήσεις σχετικά με την ασφαλή πλοήγηση	,050	772	,000	,990	772	,000
Απαιτήσεις χρηστών κατά την πλοήγηση	,270	772	,000	,718	772	,000
Συμπεριφορά χρηστών κατά την πλοήγηση	,124	772	,000	,908	772	,000

a. Lilliefors Significance Correction

Πίνακας 4.5: Έλεγχος κανονικότητας των εννοιολογικών κατασκευών.

Επομένως, για τη διεξαγωγή της διαδικασίας ανάλυσης συσχέτισης δεν χρησιμοποιήθηκε ο συντελεστής συσχέτισης Pearson, αλλά ο αντίστοιχος του Spearman. Είναι συντελεστής γραμμικής συσχέτισης, συμβολίζεται με r και παίρνει τιμές από -1 έως 1 (-1 ≤ rho ≤ 1).

- -1 έως -0,5 θεωρούμε ότι είναι υψηλός αρνητικός συντελεστής συσχέτισης
- -0,5 έως -0,2: θεωρούμε ότι είναι χαμηλός αρνητικός συντελεστής συσχέτισης
- -0,2 έως 0,2: θεωρούμε ότι ο συντελεστής συσχέτισης είναι μηδενικός
- 0,2 έως 0,5: θεωρούμε ότι είναι χαμηλός θετικός συντελεστής συσχέτισης
- 0,5 έως 1: θεωρούμε ότι είναι υψηλός θετικός συντελεστής συσχέτισης

Correlations

			Γνώσεις σε θέματα ασφαλούς πλοήγησης	Ευαισθητοποίηση/ πεποιθήσεις σχετικά με την ασφαλή πλοήγηση	Απαιτήσεις χρηστών κατά την πλοήγηση	Συμπεριφορά χρηστών κατά την πλοήγηση
Spearman's rho	Γνώσεις σε θέματα ασφαλούς πλοήγησης	Correlation Coefficient	1,000	,012	-,152**	-,015
		Sig. (2-tailed)	.	,747	,000	,669
		N	772	772	772	772
	Ευαισθητοποίηση/ πεποιθήσεις σχετικά με την ασφαλή πλοήγηση	Correlation Coefficient	,012	1,000	-,010	,002
		Sig. (2-tailed)	,747	.	,774	,946
		N	772	772	772	772
	Απαιτήσεις χρηστών κατά την πλοήγηση	Correlation Coefficient	-,152**	-,010	1,000	-,195**
		Sig. (2-tailed)	,000	,774	.	,000
		N	772	772	772	772
	Συμπεριφορά χρηστών κατά την πλοήγηση	Correlation Coefficient	-,015	,002	-,195**	1,000
		Sig. (2-tailed)	,669	,946	,000	.
		N	772	772	772	772

**. Correlation is significant at the 0.01 level (2-tailed).

Πίνακας 4.6: Ανάλυση συσχέτισης με το συντελεστή συσχέτισης Spearman

Ανάμεσα στις «γνώσεις σε θέματα ασφαλούς πλοήγησης» και «απαιτήσεις χρηστών κατά την πλοήγηση» υπάρχει μηδενικός συντελεστής συσχέτισης (ρ = -0,152) και στατιστικά σημαντικός σε επίπεδο σημαντικότητας 0,01. Ανάμεσα στις «απαιτήσεις χρηστών κατά την πλοήγηση» και «συμπεριφορά χρηστών κατά την πλοήγηση» υπάρχει μηδενικός συντελεστής συσχέτισης (ρ = -0,195) και στατιστικά σημαντικός σε επίπεδο σημαντικότητας 0,01. Συμπερασματικά από τα παραπάνω προκύπτει ότι δεν υπάρχει σημαντική συσχέτιση μεταξύ των εννοιολογικών κατασκευών που αναλύθηκαν, δηλαδή για παράδειγμα οι γνώσεις των χρηστών δεν φαίνεται να επηρεάζουν στατιστικώς σημαντικά την συμπεριφορά τους κατά την πλοήγηση στο διαδίκτυο.

4.5.8 Συμπεράσματα

Η προστασία των χρηστών κατά την πλοήγηση στο διαδίκτυο εξαρτάται άμεσα από την ανίχνευση λανθασμένων συμπεριφορών με απώτερο σκοπό την ανάπτυξη κατάλληλων στρατηγικών για την μείωση του κινδύνου. Αυτή η μελέτη κατέδειξε ορισμένα κενά ως προς τις γνώσεις και τις πρακτικές που αφορούν την ασφάλεια κατά την πλοήγηση σε ιστοτόπους.

Από τα αποτελέσματα καταδεικνύεται ότι μόνο ένας στους τρεις γνωρίζει την οικογένεια πρωτοκόλλων SSL/TLS, ποσοστό το οποίο είναι παρόμοιο με αυτούς που δήλωσαν ότι έχει σπουδές σχετικές με την Πληροφορική. Ανάλογο ποσοστό γνωρίζει πώς να ελέγχει την ασφάλεια ενός πιστοποιητικού σε συνδέσεις https, ενώ 4 στους 10 δεν γνωρίζει την διαφορά http και https, παρά το γεγονός ότι η πλειοψηφία αναγνώρισε την εικόνα που γίνονταν χρήση του https ως ασφαλή ιστοσελίδα. Επίσης, οι μισοί από το δείγμα ξέρουν την έννοια του λουκέτου στην μπάρα πλοήγησης του φυλλομετρητή και σε ποσοστό παρόμοιο με αυτούς αναγνώρισαν την αντίστοιχη εικόνα ως ασφαλή ιστοσελίδα. Ωστόσο, μόνο η μειοψηφία των χρηστών ελέγχουν αν η ιστοσελίδα είναι https κι αν έχει το χαρακτηριστικό λουκέτο, γεγονός που αναδεικνύει ότι δεν εφαρμόζουν τις γνώσεις τους στην πράξη. Τέλος σε ποσοστό 69,3% δεν γνωρίζουν καμία από τις επιθέσεις που τους παρουσιάστηκαν. Αυτό καταδεικνύει ότι οι τυπικοί χρήστες του διαδικτύου δεν είναι πλήρως γνώστες των κινδύνων που αντιμετωπίζουν on-line και το 25% των ερωτηθέντων έχει πέσει θύμα ηλεκτρονικής απάτης κάποιας στιγμή στο παρελθόν.

Αν και η πλειοψηφία των ερωτηθέντων δήλωσαν εξοικειωμένοι με την χρήση του διαδικτύου, περίπου οι μισοί από αυτούς προβαίνουν σε διαδικτυακές αγορές αγαθών και σε on-line τραπεζικές συναλλαγές, καθώς το χρησιμοποιούν κυρίως για αποστολή email και κοινωνική δικτύωση. Η πλειοψηφία ενδιαφέρεται η ιστοσελίδα να είναι σύγχρονη, με εύκολη δομή και πρόσβαση αλλά ταυτόχρονα να κρυπτογραφούνται τα δεδομένα που εισάγουν και να εξασφαλίζεται η ιδιωτικότητα και η εμπιστευτικότητα των πληροφοριών. Γενικά, οι ερωτηθέντες εμπιστεύονται τις ιστοσελίδες των τραπεζών, των e-shop και των δημόσιων φορέων και θεωρούν ότι λαμβάνουν όλα τα απαραίτητα μέτρα για την ασφαλή πλοήγηση των χρηστών τους, ενώ είναι επιφυλακτικοί με τα κοινωνικά δίκτυα και τις ειδησεογραφικούς ιστοτόπους. Το σημαντικότερο στοιχείο στην συμπεριφορά των χρηστών εντοπίζεται στο γεγονός ότι σε μεγάλο ποσοστό δεν θα επισκεπτόταν ξανά μια ιστοσελίδα μη ασφαλή και θα διέκοπτε την σύνδεση του αν δεν ήταν ασφαλής.

Συμπερασματικά θα μπορούσαμε να πούμε ότι οι χρήστες στην Ελλάδα δεν είναι εξοικειωμένοι με τα πρωτόκολλα ασφαλείας, τις επιθέσεις σε πρωτόκολλα SSL/TLS και τους τρόπους ελέγχου της ασφάλειας των ιστοσελίδων που πλοηγούνται, υπογραμμίζοντας την ανάγκη για την περαιτέρω εκπαίδευση τους. Η βελτίωση της συμπεριφοράς των χρηστών ως προς την προσοχή που δείχνουν για την ασφάλεια των

ιστοσελίδων, μπορεί να οδηγήσει στη μείωση της συχνότητας εμφάνισης φαινομένων διαδικτυακής απάτης.

Κεφάλαιο 5

Επίλογος

Η παρούσα μεταπτυχιακή διατριβή στόχευσε αφενός στην καταγραφή και την ανάλυση της κατάστασης που βρίσκονται οι σημαντικότερες ελληνικές ιστοσελίδες και αφετέρου να καταγράψει τις γνώσεις, τις πρακτικές και την συμπεριφορά των χρηστών, σε σχέση με την ασφάλεια των ιστοσελίδων που πλοηγούνται. Από τα αποτελέσματα της μεταπτυχιακής διατριβής προκύπτει το συμπέρασμα ότι οι ελληνικές ιστοσελίδες βρίσκονται σε αρκετά καλή κατάσταση, ως προς την ασφάλεια που παρέχουν στους χρήστες αν και υπάρχουν σημαντικά περιθώρια βελτίωσης. Συγκεκριμένα ενώ μεγάλο ποσοστό έχει λάβει βαθμολογία και με τα δύο εργαλεία Α ή Β, το οποίο σημαίνει ότι έχουν εφαρμόσει σωστά το SSL/TLS, υπάρχει και ένα αξιομνημόνευτο ποσοστό ιστοσελίδων το οποίο δεν έχει λάβει καλή βαθμολογία. Αυτό μας καταδεικνύει ότι πρέπει να είναι διαρκής η προσπάθεια για την ενημέρωση των υπευθύνων των ιστοσελίδων αλλά και των χρηστών για την σημασία της ασφάλειας των ιστοσελίδων. Στα συγκεντρωτικά αποτελέσματα από το παρατηρούμε ότι οι τρεις σημαντικότερες ευπάθειες που εντοπίστηκαν είναι οι RC4, Weak DH και Poodle. Οι ευπάθειες αυτές, παρόλο που είναι γνωστές, παρατηρούμε ότι ανιχνεύονται σε σημαντικά ποσοστά, γεγονός που καταδεικνύει πόσο σημαντική είναι η εκπαίδευση και η ευαισθητοποίηση των διαχειριστών των ιστοσελίδων. Δεν αρκεί η υιοθέτηση των πρωτοκόλλων ασφαλείας, αλλά και σωστή υλοποίηση τους.

Η στατιστική ανάλυση κατέδειξε ότι σε κάποιες κατηγορίες παρατηρούνται μεγάλες διαφορές στην χρήση του login στις ιστοσελίδες. Έτσι για τα e-shop παρουσιάζεται στατιστικά σημαντικά μεγαλύτερη χρήση login, σε σχέση με τις κατηγορίες εταιριών και οικονομικών οργανισμών και στατιστικά σημαντικά μεγαλύτερη χρήση πρωτοκόλλων SSL/TLS σε σχέση με τους δημόσιους φορείς. Αντίθετα οι δημόσιοι οργανισμοί και οι ενημερωτικές ιστοσελίδες παρουσιάζουν στατιστικά σημαντικά μικρότερη χρήση login, σε σχέση με τα e-shop, εταιριών και οικονομικών οργανισμών. Για τα υπόλοιπα αποτελέσματα, ενώ υπήρχαν κάποιες διαφορές, ωστόσο δεν προέκυπτε κάποια

στατιστικώς σημαντική διαφορά. Η πλειοψηφία των ιστοσελίδων είναι έτοιμη να λειτουργήσει με την επόμενη έκδοση του πρωτοκόλλου TLS 1.3. Σε σχέση με την έκδοση του TLS που υποστηρίζεται, η πλειοψηφία των ιστοσελίδων υποστηρίζει την έκδοση 1.2 γεγονός που τις καθιστά ενημερωμένες. Υπάρχει όμως και ένα μικρό ποσοστό το οποίο χρησιμοποιεί την έκδοση 1.0 του πρωτοκόλλου και το οποίο θα πρέπει να πραγματοποιήσει άμεσα την μετάβαση στην νεότερη έκδοση. Σε ένα σημαντικό ποσοστό παρατηρείται η ύπαρξη γνωστών αδυναμιών όπως RC4, Weak DH .

Η μελέτη κατέδειξε επίσης ορισμένα κενά ως προς τις γνώσεις των χρηστών και τις πρακτικές που ακολουθούν αναφορικά με την ασφάλεια των ιστοτόπων. Από τα αποτελέσματα καταδεικνύεται ότι μόνο ένας στους τρεις γνωρίζει την οικογένεια πρωτοκόλλων SSL/TLS. Ανάλογο ποσοστό γνωρίζει πώς να ελέγχει την ασφάλεια ενός πιστοποιητικού σε συνδέσεις https, ενώ 4 στους 10 δεν γνωρίζει την διαφορά http και https, παρά το γεγονός ότι η πλειοψηφία αναγνώρισε την εικόνα που γίνονταν χρήση του https ως ασφαλή ιστοσελίδα. Επίσης, οι μισοί από το δείγμα ξέρουν την έννοια του λουκέτου στην μπάρα πλοήγησης του φυλλομετρητή και σε ποσοστό παρόμοιο με αυτούς αναγνώρισαν την αντίστοιχη εικόνα ως ασφαλή ιστοσελίδα. Ωστόσο, μόνο η μειοψηφία των χρηστών ελέγχουν αν η ιστοσελίδα είναι https κι αν έχει το χαρακτηριστικό λουκέτο, γεγονός που αναδεικνύει ότι δεν εφαρμόζουν τις γνώσεις τους στην πράξη. Τέλος σε ποσοστό 69,3% δεν γνωρίζουν καμία από τις επιθέσεις που τους παρουσιάστηκαν. Αυτό καταδεικνύει ότι οι τυπικοί χρήστες του διαδικτύου δεν είναι πλήρως γνώστες των κινδύνων που αντιμετωπίζουν on-line και το 25% των ερωτηθέντων έχει πέσει θύμα ηλεκτρονικής απάτης κάποιας στιγμή στο παρελθόν.

Γενικά, οι ερωτηθέντες εμπιστεύονται τις ιστοσελίδες των τραπεζών, των e-shop και των δημόσιων φορέων στο ότι λαμβάνουν όλα τα απαραίτητα μέτρα για την ασφάλεια, ενώ είναι επιφυλακτικοί με τα κοινωνικά δίκτυα και τους ειδησεογραφικούς ιστοτόπους. Συμπερασματικά θα μπορούσαμε να πούμε ότι οι χρήστες στην Ελλάδα δεν ήταν εξοικειωμένοι με τα πρωτόκολλα ασφαλείας, τις επιθέσεις σε πρωτόκολλα SSL/TLS και τους τρόπους ελέγχου της ασφάλειας των ιστοσελίδων που πλοηγούνται, υπογραμμίζοντας την ανάγκη για την περαιτέρω εκπαίδευση τους. Η βελτίωση της συμπεριφοράς των χρηστών ως προς την προσοχή που δείχνουν για την ασφάλεια των ιστοσελίδων, μπορεί να οδηγήσει στη μείωση της συχνότητας εμφάνισης φαινομένων διαδικτυακής απάτης.

Βιβλιογραφία

[1] B. Schneier, Applied cryptography : protocols, algorithms, and source code in C, 1996.

[2] A.J. Menezes, P.C. Van Oorschot, S.A. Vanstone, APPLIED CRYPTOGRAPHY, (1997). http://math.fau.edu/bkhadka/Syllabi/A handbook of applied cryptography.pdf (accessed April 6, 2018).

[3] W. Stallings, M. Bauer, M. Hirsch, COMPUTER SECURITY Second Edition, 2013.

[4] W. Diffie, M.E. Hellman, New Directions in Cryptography, IEEE Trans. Inf. Theory. 22 (1976) 644–654. doi:10.1109/TIT.1976.1055638.

[5] D.R. (Douglas R. Stinson, Cryptography : theory and practice, Chapman & Hall/CRC, 2006. https://books.google.gr/books?hl=el&lr=&id=uhl_kYfpgo4C&oi=fnd&pg=PP1&dq=Stinson.+Cryptography++Theory+and+Practice&ots=nwsXjAeiQ1&sig=N9M_a34Bbrh39GMaDdAgnIKOif8&redir_esc=y#v=onepage&q=Stinson. Cryptography Theory and Practice&f=false (accessed December 25, 2017).

[6] X. Lai, R.A. Rueppel, J. Woollven, A fast cryptographic checksum algorithm based on stream ciphers, in: Springer, Berlin, Heidelberg, 1993: pp. 339–348. doi:10.1007/3-540-57220-1_73.

[7] T.Y.C. Woo, R. Bindignavle, S. Su, S.S. Lam, SNP: An Interface for Secure Network Programming, in: USTC'94 Proc. USENIX Summer 1994 Tech. Conf. USENIX Summer 1994 Tech. Conf., 1994. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.8.8279&rep=rep1&type=pdf (accessed November 22, 2017).

[8] S. Turner, T. Polk, Prohibiting Secure Sockets Layer (SSL) Version 2.0, 2011. doi:10.17487/rfc6176.

[9] Brian Jackson, An Overview of TLS 1.3 - Faster and More Secure, (2018). https://kinsta.com/blog/tls-1-3/ (accessed April 7, 2018).

[10] Microsoft, How TLS/SSL Works: Logon and Authentication, (2003). https://technet.microsoft.com/en-us/library/cc783349(v=ws.10).aspx (accessed April 7, 2018).

[11] T. Dierks, C. Allen, The TLS Protocol Version 1.0, IETF. (1997). https://www.ietf.org/rfc/rfc2246.txt (accessed October 23, 2017).

[12] IBM, An Overview of the SSL or TLS handshake, IBM Knowl. Cent. (2013). https://www.ibm.com/support/knowledgecenter/SSFKSJ_7.1.0/com.ibm.mq.doc/sy10660_.htm?lang=en (accessed November 9, 2017).

[13] C. Kemmerer, The SSL/TLS Handshake: an Overview - SSL.com, (2015). https://www.ssl.com/article/ssl-tls-handshake-overview/ (accessed November 9, 2017).

[14] Microsoft Developers' Network (MSDN), "TLS Handshake Protocol.," Msdn. (2003). https://msdn.microsoft.com/en-us/library/windows/desktop/aa380516(v=vs.85).aspx (accessed November 9, 2017).

[15] I. Grigorik, Transport Layer Security (TLS), (2003).

[16] I. Ristić, SSL/TLS and PKI History, Feistyduck.Com. (2017). https://www.feistyduck.com/ssl-tls-and-pki-history/ (accessed April 7, 2018).

[17] Microsoft, Microsoft Security Bulletin MS10-046 %93 Critical, Vulnerabilities Wind. Print Spooler Could Allow Remote Code Exec. (2010). https://technet.microsoft.com/en-us/library/security/ms10-046.aspx (accessed December 25, 2017).

[18] B. Schneier, Random Number Bug in Debian Linux - Schneier on Security, (2008). https://www.schneier.com/blog/archives/2008/05/random_number_b.html (accessed December 25, 2017).

[19] A. Sotirov, M. Stevens, J. Appelbaum, A. Lenstra, D. Molnar, D.A. Osvik, B. De Weger, MD5 considered harmful today, Announc. 25th Chaos Commun. Congr. (2008) 1–25. http://www.win.tue.nl/hashclash/rogue-ca/ (accessed April 7, 2018).

[20] Moxie Marlinspike, Sslstrip, (2009). https://moxie.org/software/sslstrip/ (accessed April 7, 2018).

[21] D. Kaminsky, PKI Layer Cake: New Collision Attacks Against The Global X.509 CA Infrastructure, (2009). https://ioactive.com/pdfs/PKILayerCake.pdf (accessed April 7, 2018).

[22] Eric Butler, Firesheep, (2010). http://codebutler.com/firesheep?c=1 (accessed April 7, 2018).

[23] SecureAuth, SSL/TLS Information Disclosure (BEAST), (2016). https://docs.secureauth.com/pages/viewpage.action?pageId=14778519 (accessed April

7, 2018).

[24] N. Heninger, Z. Durumeric, E. Wustrow, J.A. Halderman, Mining your Ps and Qs: detection of widespread weak keys in network devices, USENIX Secur. Symp. (2012) 35. http://dl.acm.org/citation.cfm?id=2362793.2362828 (accessed April 7, 2018).

[25] ImperialViolet, Revocation checking and Chrome's CRL, (2012). https://www.imperialviolet.org/2012/02/05/crlsets.html (accessed April 7, 2018).

[26] K. Zetter, Meet "Flame," The Massive Spy Malware Infiltrating Iranian Computers, Wired. (2012). http://www.wired.com/2012/05/flame/ (accessed April 7, 2018).

[27] J.R. Y, T. Duong, The CRIME attack, Ekoparty Secur. Conf. 8th Ed. (2012). http://www.ekoparty.org/archive/2012/CRIME_ekoparty2012.pdf (accessed April 7, 2018).

[28] N.J. AlFardan, K.G. Paterson, Lucky thirteen: Breaking the TLS and DTLS record protocols, in: Proc. - IEEE Symp. Secur. Priv., 2013: pp. 526–540. doi:10.1109/SP.2013.42.

[29] N. AlFardan, D. Bernstein, On the security of RC4 in TLS and WPA, in: USENIX Secur. …, USENIX Association, 2013: pp. 1–31. http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:On+the+Security+of+RC4+in+TLS+and+WPA+?#0.

[30] T. Be'ery, A. Shulman, A Perfect CRIME? Only TIME Will Tell, BlackHat Eur. 2013. (2013). https://media.blackhat.com/eu-13/briefings/Beery/bh-eu-13-a-perfect-crime-beery-wp.pdf.

[31] O. Santos, BREACH, CRIME and Black Hat, Cisco, 2013. http://blogs.cisco.com/security/breach-crime-and-blackhat/ (accessed April 7, 2018).

[32] GRACE EDEN, BULLRUN, (2015). http://www.dcssproject.net/bullrun/ (accessed April 7, 2018).

[33] S. Checkoway, M. Fredrikson, W. Madison, R. Niederhagen, On the Practical Exploitability of Dual EC in TLS Implementations, USENIX Secur. 2014. (2014) 319–335. http://dualec.org/DualECTLS.pdf (accessed April 7, 2018).

[34] M. Gree, Triple Handshakes Considered Harmful Breaking and Fixing Authentication over TLS, (2014). https://mitls.org/ (accessed April 7, 2018).

[35] Santibanez, Heartbleed Bug, (2015) 1–11. http://heartbleed.com/ (accessed April 7, 2018).

[36] C. Meyer, J. Somorovsky, E. Weiss, J. Schwenk, S. Schinzel, E. Tews, Revisiting SSL/TLS Implementations: New Bleichenbacher Side Channels and Attacks, 23rd USENIX Secur. Symp. (USENIX Secur. 14). (2014) 733–748. https://www.usenix.org/conference/usenixsecurity14/technical-sessions/presentation/meyer (accessed April 7, 2018).

[37] Infosecurity Magazine, BERserk Flaw Opens Door to SSL Spoofing and MiTM, (2014). https://www.infosecurity-magazine.com/news/berserk-flaw-opens-ssl-spoofing/ (accessed April 7, 2018).

[38] B. Möller, T. Duong, K. Kotowicz, This POODLE Bites: Exploiting The SSL 3.0 Fallback, Secur. Advis. (2014) 1–6. doi:10.1145/1629575.1629606.

[39] Qualys Blog, Poodle Bites TLS, (2014). https://blog.qualys.com/ssllabs/2014/12/08/poodle-bites-tls (accessed April 7, 2018).

[40] S. Rosenblatt, Lenovo's Superfish security snafu blows up in its face, Cnet. (2015). http://www.cnet.com/news/superfish-torments-lenovo-owners-with-more-than-adware/ (accessed April 7, 2018).

[41] miTLS Team, SMACK: State Machine AttaCKs, (2015). https://www.smacktls.com/#freak (accessed April 7, 2018).

[42] Censys Team, The FREAK Attack, Censys.io. (2015). https://censys.io/blog/freak (accessed April 7, 2018).

[43] D. Adrian, K. Bhargavan, Z. Durumeric, P. Gaudry, M. Green, A. Halderman, N. Heninger, Weak Diffie-Hellman and the Logjam Attack, Weakdh.Org. (2015). https://weakdh.org/ (accessed April 7, 2018).

[44] Yngve Nysæter, There are more POODLEs in the forest, (2015). https://yngve.vivaldi.net/2015/07/14/there-are-more-poodles-in-the-forest/ (accessed April 7, 2018).

[45] Yngve Nysæter, The POODLE has friends, (2015). https://yngve.vivaldi.net/2015/07/14/the-poodle-has-friends/ (accessed April 7, 2018).

[46] Karthikeyan Bhargavan, G. Leurent, Security Losses from Obsolete and Truncated Transcript Hashes, (2016). https://www.mitls.org/pages/attacks/SLOTH (accessed April 7, 2018).

[47] N. Aviram, S. Schinzel, J. Somorovsky, N. Heninger, M. Dankel, J. Steube, L. Valenta, D. Adrian, J.A. Halderman, V. Dukhovni, E. Käsper, S. Cohney, S. Engels, C. Paar, Y. Shavitt,

DROWN : Breaking TLS using SSLv2, Proc. 25th USENIX Secur. Symp. (2016) 1–18. https://drownattack.com/drown-attack-paper.pdf (accessed April 7, 2018).

[48] J. Somorovsky, C. Young, Return Of Bleichenbacher ' s Oracle Threat (ROBOT), (2017) 1–28. https://eprint.iacr.org/2017/1189.pdf (accessed April 7, 2018).

[49] Microsoft, Microsoft Azure Cloud Computing Platform, Microsoft Website. (2017) 1. https://azure.microsoft.com/en-us/ (accessed April 7, 2018).

[50] Matthias Gliwka, Microsoft leaks TLS private key for cloud ERP product, (2017). https://medium.com/matthias-gliwka/microsoft-leaks-tls-private-key-for-cloud-erp-product-10b56f7d648 (accessed April 7, 2018).

[51] The Register, 23,000 HTTPS certs will be axed in next 24 hours after private keys leak, (2018). https://www.theregister.co.uk/2018/03/01/trustico_digicert_symantec_spat/ (accessed April 7, 2018).

[52] Alexa, Top Sites by Categ. World/Greek. (2018). https://www.alexa.com/topsites/category/Top/World/Greek (accessed March 2, 2018).

[53] M. Formanek, M. Zaborsky, Web interface security vulnerabilities of selected European open-access academic repositories, Lib. Q. 27 (2017) 45–57. doi:10.18352/lq.10178.

[54] S. Labs, Qualy's SSL Lab's SSL Pulse, (2018). https://www.ssllabs.com/ssl-pulse/%0Ahttp://www.webcitation.org/6wepClCQS (accessed March 4, 2018).

[55] I. Ristic, Internet SSL Survey 2010, in: Agenda, Black Hat, Abu Dhabi, 2010: pp. 1–43. http://media.blackhat.com/bh-ad-10/Ristic/BlackHat-AD-2010-Ristic-Qualys-SSL-Survey-HTTP-Rating-Guide-slides.pdf (accessed March 4, 2018).

[56] S.M. Jawi, F.H.M. Ali, Non-intrusive SSL/TLS proxy implementation and issues, 2015 IEEE Student Conf. Res. Dev. SCOReD 2015. (2016) 684–689. doi:10.1109/SCORED.2015.7449426.

[57] W. Mayer, M. Schmiedecker, Turning active TLS scanning to eleven, in: IFIP Adv. Inf. Commun. Technol., Springer, Cham, 2017: pp. 3–16. doi:10.1007/978-3-319-58469-0_1.

[58] K. Krombholz, W. Mayer, M. Schmiedecker, E. Weippl, "I Have No Idea What I'm Doing" – On the Usability of Deploying HTTPS, USENIX Secur. (2017) 1–18. https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/krombholz (accessed March 4, 2018).

[59] Qualys SSL Labs, SSL Server Rating Guide, (2015) 10.

https://www.ssllabs.com/downloads/SSL_Server_Rating_Guide.pdf (accessed March 4, 2018).

[60] Getting an A+ rating on the Qualys SSL Test, (2014). https://scotthelme.co.uk/a-plus-rating-qualys-ssl-test/ (accessed March 4, 2018).

[61] SSL/TLS Server Test, (2018). https://www.htbridge.com/ssl/ (accessed March 4, 2018).

[62] A. Bhargav, Monitoring and Testing, CRC Press, Taylor and Francis, 2007. doi:10.1016/B978-159749165-5/50028-3.

[63] S.R. Material, S.R. Standard, National Institute of Standards and Technology, Measurement. (2005) 1–11. http://webbook.nist.gov/cgi/cbook.cgi?ID=67-63-0&Type=IR-SPEC&Index=QUANT-IR,16 (accessed March 4, 2018).

[64] Office of Civil Rights Department of Health and Human Services, Summary of the HIPAA Security Rule, (2012) 1–4. https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html (accessed March 4, 2018).

[65] M. Maass, P. Wichmann, H. Pridöhl, D. Herrmann, PrivacyScore: Improving privacy and security via crowd-sourced benchmarks of websites, in: Lect. Notes Comput. Sci. (Including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), Springer, Cham, 2017: pp. 178–191. doi:10.1007/978-3-319-67280-9_10.

[66] J. Costa, A. Michalas, Middle Man: An Efficient Two-Factor Authentication Framework, 17 (2017). http://www.westminster.ac.uk/westminsterresearch%0Ahttp://ieeexplore.ieee.org/Xplore/home.jsp (accessed March 6, 2018).

[67] Qualys Blog, SSL Labs: Deploying Forward Secrecy, (2011). https://blog.qualys.com/ssllabs/2013/06/25/ssl-labs-deploying-forward-secrecy (accessed March 8, 2018).

[68] V. Bernat, SSL / TLS & Perfect Forward Secrecy, (2011) 1–10. https://vincent.bernat.im/en/blog/2011-ssl-perfect-forward-secrecy (accessed March 8, 2018).

[69] A. Rastegarnia, A. Sohrabibidar, V. Bagheri, M. Razifard, A. Zolfaghari, Assessment of Relationship Between Grouted Values and Calculated Values in the Bazoft Dam Site, 2017. doi:10.1007/s10706-017-0176-1.

[70] T. Dierks, E. Rescorla, The Transport Layer Security (TLS) Protocol Version 1.3, (2014) 1–143. https://tools.ietf.org/html/draft-ietf-tls-tls13-03.

[71] PCI Security Standard Council, Payment Card Industry Data Security Standard, Card Technol. Today. 21 (2009) 9. doi:10.1016/S0965-2590(09)70094-5.

[72] D.A.A. Chuvakin, B.R. Williams, PCI Compliance: Understanding and Implement Effective PCI Data Security Standard Compliance, 2009.

[73] T. Polk, K. McKay, S. Chokhani, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations, National Institute of Standards and Technology, Gaithersburg, MD, 2014. doi:10.6028/NIST.SP.800-52r1.

[74] L.O. Gostin, Health Information Privacy, Cornell Law Rev. 80 (2013) 451–528. http://www.hhs.gov/ocr/privacy/ (accessed March 8, 2018).

[75] EU, Home Page of EU GDPR, EU GDPR Termin. (2016). https://www.eugdpr.org/ (accessed March 10, 2018).

[76] IBM, IBM SPSS Software, Ibm. (2018) 1. https://www.ibm.com/analytics/data-science/predictive-analytics/spss-statistical-software (accessed March 11, 2018).

[77] M. Van Selm, N.W. Jankowski, Conducting online surveys, Qual. Quant. 40 (2006) 435–456. doi:10.1007/s11135-005-8081-8.

[78] Ε. Λιναρδής, Α., Παπαγιαννόπουλος, Κ. & Καλησπεράτη, Η διαδικτυακή έρευνα. Πλεονεκτήματα, μειονεκτήματα και εργαλεία διεξαγωγής διαδικτυακών ερευνών., (2011). https://www.ekke.gr/publications/wp/wp23.pdf (accessed April 1, 2018).

[79] N.H. Timm, Applied multivariate analysis, Springer, 2002.

[80] J.F. Hair, Multivariate Data Analysis: With Readings, Prentice Hall, 1998.

[81] M. Marcucci, S. Sharma, Applied Multivariate Techniques, Technometrics. 39 (1997) 101. doi:10.2307/1270777.

[82] H.F. Kaiser, J. Rice, Little Jiffy, Mark Iv, Educ. Psychol. Meas. 34 (1974) 111–117. doi:10.1177/001316447403400115.

[83] L.J. Cronbach, Coefficient alpha and the internal structure of tests, Psychometrika. 16 (1951) 297–334. doi:10.1007/BF02310555.

[84] B. Friedman, D. Hurley, D.C. Howe, E. Felten, H. Nissenbaum, Users' conceptions of web security, CHI '02 Ext. Abstr. Hum. Factors Comput. Syst. - CHI '02. (2002) 746. doi:10.1145/506443.506577.

[85] S. Flinn, J. Lumsden, User perceptions of privacy and security on the web, Proc. Third

Annu. Conf. Privacy, Secur. Trust. (2005).

Παράρτημα Α

Ιστοσελίδες

A/A	Site	A/A	Site
1	emarket.gr	122	otenet.gr
2	http://www.admie.gr	123	forth.gr
3	Thermiki.gr	124	mat-security.com
4	patakis.gr	125	mediamarkt.gr
5	toyota.gr	126	Kathimerini.gr
6	oktabit.gr	127	Doktoris.gr
7	ametro.gr	128	https://estudent.aua.gr:8443/estudent/
8	Skai.gr	129	piraeusbank.gr
9	Oneman.gr	130	piraeusbank.gr
10	Nova.gr	131	MYACCOUNT.NOVA.GR
11	Fthis.gr	132	myshoe.gr
12	euro2day.gr	133	apothema.gr
13	kerdos.gr	134	cosmote.gr
14	hau.gr	135	www.uoc.gr
15	pde.gr	136	https://e-secretariat.teiemt.gr/unistudent/login.asp
16	panteion.gr	137	eett.gr
17	https://portal.astynomia.gr/	138	ioannina24.gr
18	ypes.gr	139	Egalaxy.gr
19	pi-schools.gr	140	ikea.gr
20	ypeka.gr	141	Tovima.gr
21	noa.gr	142	Tanea.gr
22	http://www.ilsp.gr	143	in.gr
23	minagric.gr	144	Emimikos.gr
24	yme.gr	145	Telebest.gr

25	demokritos.gr	146	E-gadgets.gr
26	acci.gr	147	Vodafone.gr
27	hri.org	148	esos.gr
28	multirama.gr	149	katerelos.gr
29	vapeland.gr	150	e-click.gr
30	cilek.gr	151	Kokotas.gr
31	kourtakis-lighting.gr	152	https://estudy.teiath.gr/unistudent/login.asp
32	Batteries.gr	153	Novasports.gr
33	www.e-smarteck.gr	154	Kotsovolos.gr
34	praktiker.gr	155	helexpo.gr
35	public.gr	156	greekmoney.gr
36	Oleng.eu	157	volleyball.gr
37	dominos.gr	158	anek.gr
38	dnhost.gr	159	e-forologia.gr
39	ip.gr	160	https://sso.aueb.gr/
40	vapeland.gr	161	https://sso.teipir.gr/login
41	pizzahut.gr	162	greekbooks.gr
42	Parapolitika.gr	163	sportarena.gr
43	Thebest.gr	164	viva.gr
44	taxheaven.gr	165	https://dionysos.teilar.gr/unistudent/
45	eurobank.gr	166	espa.gr
46	capital.gr	167	http://www.evrosbank.gr
47	alfavita.gr	168	nbg.gr
48	sso.sch.gr	169	http://www.helex.gr/el/web/guest/home
49	https://e-students.teiwest.gr/	170	play247.gr
50	tsig.gr	171	laredoute.gr
51	https://www.atticabank.gr	172	Alterego.gr
52	http://www.aegeanbalticbank.com	173	Cityshop.gr
53	minedu.gov.gr	174	villagecinemas.gr
54	bebeosis.army.gr	175	www.ntua.gr
55	hellenicnavy.gr	176	plus4u.gr
56	Demo.gr	177	oroloi.gr
57	winbank.gr	178	sofokleous10.gr
58	aia.gr	179	superfast.com
59	auth.gr	180	studentweb.aegean.gr

60	idp.duth.gr	181	https://websrv.stdnet.tuc.gr/unistudent/
61	https://moodle.teithe.gr	182	ote.gr
62	oaed.gr	183	Jotis.gr
63	Watt-volt.gr	184	eopyy.gov.gr
64	Elpedison.gr	185	Ellinikomeli.gr
65	ab.gr	186	suzuki.gr
66	https://students.unipi.gr/login.asp	187	alpha.gr
67	ika.gr	188	asep.gr
68	tee.gr	189	Vivartia.com
69	olympicair.com	190	opel.gr
70	haf.gr	191	sofokleousin.gr
71	goldenbrands.gr	192	http://www.dramabank.gr
72	volkswagen.gr	193	e-shop.gr
73	Protothema.gr	194	brandsgalaxy.gr
74	Naftemporiki.gr	195	psichogios.gr
75	Pcsteps.gr	196	adorama.gr
76	www.alphatv.gr	197	e-ergaleio.gr
77	bankofgreece.gr	198	kosmima.gr
78	basket.gr	199	livanis.gr
79	Ebw.gr	200	Eaparts.gr
80	Alfawood.gr	201	5050.gr
81	gsis.gr	202	Videosun.gr
82	wind.gr	203	Heron.gr
83	eap.gr	204	odeon.gr
84	delikaris-sport.gr	205	adorama.gr
85	msystems.gr	206	acscourier.gr
86	getitnow.gr	207	forth-crs.gr
87	fashioncity.gr	208	Antenna.gr
88	ideashop.gr	209	uoa.gr
89	Electrostudio.gr	210	https://gmweb.teiep.gr/login.asp
90	Smart-tech.gr	211	http://www.ibg.gr
91	Protergia.gr	212	http://www.chaniabank.gr
92	aegeanair.com	213	http://www.pancretabank.gr
93	papaki.gr	214	statistics.gr
94	mercedes-benz.gr	215	http://www.ermis.gov.gr
95	hyperhosting.gr	216	protoporia.gr

96	Madata.gr	217	e-oro.gr
97	Techblog.gr	218	telemarketing.gr
98	whatsup.gr	219	Cptpapadakisphoto.gr
99	https://e-secretary.uop.gr/classweb/	220	Copperalliance.eu
100	http://www.epirusbank.com	221	Mytilineos.gr
101	http://www.bankofkarditsa.gr	222	pizzafan.gr
102	http://www.pieriabank.gr	223	nakas.gr
103	diavgeia.gov.gr	224	ford.gr
104	mfa.gr	225	minoan.gr
105	Volterra.gr	226	Real.gr
106	http://www.serrescoopbank.gr	227	Amna.gr
107	opap.gr	228	express.gr
108	plaisio.gr	229	cyta.gr
109	You.gr	230	hol.gr
110	902.gr	231	www.upatras.gr
111	Duralstores.gr	232	WWW.uth.gr
112	z-mall.gr	233	https://my.teicrete.gr/el
113	audi.gr	234	http://www.credicom.gr
114	sevenspot.gr	235	elta.gr
115	valentine.gr	236	et.gr
116	Voria.gr	237	oasa.gr
117	http://www.bankofthessaly.gr	238	culture.gr
118	Dei.gr	239	services.uom.gr/unistudent/login.asp
119	Singer.gr	240	Sony.gr
120	Matelcom.gr	241	ecourse.uoi.gr/login/index.php
121	dei.gr		

Παράρτημα Β

Διαγράμματα

Διαγραμμα 3.1 Ποσοστο (%) των ευπαθειων του πρωτοκολλου TLS (RC4, Weak DH, Poodle, Drown, ROBOT, Freak, OpenSSL, HeartBleed, Beast) στην κατηγορια ιστοτοπων "e-shop"..... 63
Διαγραμμα 3.2 Ποσοστο (%) των αδυναμιων της διαμορφωσης του πρωτοκολλου TLS (Untrust, Mismatch, Support SSL2, Support SSL3, Error FS, Error AHED) στην κατηγορια ιστοτοπων "e-shop"..... 64
Διαγραμμα 3.3 Ποσοστο (%) της βαθμολογιας που ελαβαν οι ιστοτοποι της κατηγοριας "e-shop" μετα την αναλυση τους οσον αφορα την ασφαλεια που παρεχουν με τα εργαλεια A (μπλε μπαρες) και B (κοκκινες μπαρες)..... 64
Διαγραμμα 3.4 Ποσοστο (%) της συμμορφωσης με διεθνη προτυπα (PCI, NIST, HIPPA), ετοιμοτητας για μεταβαση στην εκδοση του πρωτοκολλου TLS 1.3, καθως και την δυνατοτητα εγγραφης (Login), στην κατηγορια ιστοτοπων "e-shop". 65
Διαγραμμα 3.5 Ποσοστο (%) των ιστοτοπων της κατηγοριας e-shop συμφωνα με την νεοτερη εκδοση του πρωτοκολλου TLS που υποστηριζουν και συγκεκριμενα TLS 1.0 (κοκκινο), TLS 1.2 (πρασινο) και καμια εκδοση SSL/TLS (μπλε). 66
Διαγραμμα 3.6 Ποσοστο (%) των ευπαθειων του πρωτοκολλου TLS (RC4, Weak DH, Poodle, Drown, ROBOT, Freak, OpenSSL, HeartBleed, Beast) στην κατηγορια ιστοτοπων "εταιρειες". 66
Διαγραμμα 3.7 Ποσοστο (%) των αδυναμιων της διαμορφωσης του πρωτοκολλου TLS (Untrust, Mismatch, Support SSL2, Support SSL3, Error FS, Error AHED) στην κατηγορια ιστοτοπων "εταιριες". 67
Διαγραμμα 3.8 Ποσοστο (%) της βαθμολογιας που ελαβαν οι ιστοτοποι της κατηγοριας "εταιρειες" μετα την αναλυση τους οσον αφορα την ασφαλεια που παρεχουν με τα εργαλεια A (μπλε μπαρες) και B (κοκκινες μπαρες)..... 67
Διαγραμμα 3.9 Ποσοστο (%) της συμμορφωσης με διεθνη προτυπα (PCI, NIST, HIPPA), ετοιμοτητας για μεταβαση στην εκδοση του πρωτοκολλου TLS 1.3, καθως και την δυνατοτητα εγγραφης (Login), στην κατηγορια ιστοτοπων "εταιριες". 68
Διαγραμμα 3.10 Ποσοστο (%) των ιστοτοπων της κατηγοριας "εταιριες" συμφωνα με την νεοτερη εκδοση του πρωτοκολλου TLS που υποστηριζουν και συγκεκριμενα TLS 1.0 (κοκκινο), TLS 1.2 (πρασινο) και καμια εκδοση SSL/TLS (μπλε). 69
Διαγραμμα 3.11 Ποσοστο (%) των ευπαθειων του πρωτοκολλου TLS (RC4, Weak DH, Poodle, Drown, ROBOT, Freak, OpenSSL, HeartBleed, Beast) στην κατηγορια ιστοτοπων "ενημερωτικα". 69
Διαγραμμα 3.12 Ποσοστο (%) των αδυναμιων της διαμορφωσης του πρωτοκολλου TLS (Untrust, Mismatch, Support SSL2, Support SSL3, Error FS, Error AHED) στην κατηγορια ιστοτοπων "ενημερωτικα". 70
Διαγραμμα 3.13 Ποσοστο (%) της βαθμολογιας που ελαβαν οι ιστοτοποι της κατηγοριας "ενημερωτικα" μετα την αναλυση τους οσον αφορα την ασφαλεια που παρεχουν με τα εργαλεια A (μπλε μπαρες) και B (κοκκινες μπαρες)..... 71
Διαγραμμα 3.14 Ποσοστο (%) της συμμορφωσης με διεθνη προτυπα (PCI, NIST, HIPPA), ετοιμοτητας για μεταβαση στην εκδοση του πρωτοκολλου TLS 1.3, καθως και την δυνατοτητα εγγραφης (Login), στην κατηγορια ιστοτοπων "ενημερωτικα"..... 71
Διαγραμμα 3.15 Ποσοστο (%) των ιστοτοπων της κατηγοριας "ενημερωτικα" συμφωνα με την νεοτερη εκδοση του πρωτοκολλου TLS που υποστηριζουν και συγκεκριμενα TLS 1.0 (κοκκινο), TLS 1.2 (πρασινο) και καμια εκδοση SSL/TLS (μπλε). 72

Διαγραμμα 3.16 Ποσοστο (%) των ευπαθειων του πρωτοκολλου TLS (RC4, Weak DH, Poodle, Drown, ROBOT, Freak, OpenSSL, HeartBleed, Beast) στην κατηγορια ιστοτοπων "τηλεπικοινωνιες". 73
Διαγραμμα 3.17 Ποσοστο (%) των αδυναμιων της διαμορφωσης του πρωτοκολλου TLS (Untrust, Mismatch, Support SSL2, Support SSL3, Error FS, Error AHED) στην κατηγορια ιστοτοπων "τηλεπικοινωνιες". ... 73
Διαγραμμα 3.18 Ποσοστο (%) της βαθμολογιας που ελαβαν οι ιστοτοποι της κατηγοριας "τηλεπικοινωνιες" μετα την αναλυση τους οσον αφορα την ασφαλεια που παρεχουν με τα εργαλεια A (μπλε μπαρες) και B (κοκκινες μπαρες)..... 74
Διαγραμμα 3.19 Ποσοστο (%) της συμμορφωσης με διεθνη προτυπα (PCI, NIST, HIPPA), ετοιμοτητας για μεταβαση στην εκδοση του πρωτοκολλου TLS 1.3, καθως και την δυνατοτητα εγγραφης (Login), στην κατηγορια ιστοτοπων "τηλεπικοινωνιες". 75
Διαγραμμα 3.20 Ποσοστο (%) των ιστοτοπων της κατηγοριας "τηλεπικοινωνιες" συμφωνα με την νεοτερη εκδοση του πρωτοκολλου TLS που υποστηριζουν και συγκεκριμενα TLS 1.0 (κοκκινο), TLS 1.2 (πρασινο) και καμια εκδοση SSL/TLS (μπλε). 75
Διαγραμμα 3.21 Ποσοστο (%) των ευπαθειων του πρωτοκολλου TLS (RC4, Weak DH, Poodle, Drown, ROBOT, Freak, OpenSSL, HeartBleed, Beast) στην κατηγορια ιστοτοπων "εκπαιδευση". 76
Διαγραμμα 3.22 Ποσοστο (%) των αδυναμιων της διαμορφωσης του πρωτοκολλου TLS (Untrust, Mismatch, Support SSL2, Support SSL3, Error FS, Error AHED) στην κατηγορια ιστοτοπων "εκπαιδευση". 76
Διαγραμμα 3.23 Ποσοστο (%) της βαθμολογιας που ελαβαν οι ιστοτοποι της κατηγοριας "εκπαιδευση" μετα την αναλυση τους οσον αφορα την ασφαλεια που παρεχουν με τα εργαλεια A (μπλε μπαρες) και B (κοκκινες μπαρες)..... 77
Διαγραμμα 3.24 Ποσοστο (%) της συμμορφωσης με διεθνη προτυπα (PCI, NIST, HIPPA), ετοιμοτητας για μεταβαση στην εκδοση του πρωτοκολλου TLS 1.3, καθως και την δυνατοτητα εγγραφης (Login), στην κατηγορια ιστοτοπων "εκπαιδευση". 78
Διαγραμμα 3.25 Ποσοστο (%) των ιστοτοπων της κατηγοριας "εκπαιδευση" συμφωνα με την νεοτερη εκδοση του πρωτοκολλου TLS που υποστηριζουν και συγκεκριμενα TLS 1.0 (κοκκινο), TLS 1.2 (πρασινο) και καμια εκδοση SSL/TLS (μπλε). 78
Διαγραμμα 3.26 Ποσοστο (%) των ευπαθειων του πρωτοκολλου TLS (RC4, Weak DH, Poodle, Drown, ROBOT, Freak, OpenSSL, HeartBleed, Beast) στην κατηγορια ιστοτοπων "οικονομικες υπηρεσιες". 79
Διαγραμμα 3.27 Ποσοστο (%) των αδυναμιων της διαμορφωσης του πρωτοκολλου TLS (Untrust, Mismatch, Support SSL2, Support SSL3, Error FS, Error AHED) στην κατηγορια ιστοτοπων "οικονομικες υπηρεσιες". 79
Διαγραμμα 3.28 Ποσοστο (%) της βαθμολογιας που ελαβαν οι ιστοτοποι της κατηγοριας "οικονομικες υπηρεσιες" μετα την αναλυση τους οσον αφορα την ασφαλεια που παρεχουν με τα εργαλεια A (μπλε μπαρες) και B (κοκκινες μπαρες). 80
Διαγραμμα 3.29 Ποσοστο (%) της συμμορφωσης με διεθνη προτυπα (PCI, NIST, HIPPA), ετοιμοτητας για μεταβαση στην εκδοση του πρωτοκολλου TLS 1.3, καθως και την δυνατοτητα εγγραφης (Login), στην κατηγορια ιστοτοπων "οικονομικες υπηρεσιες". 81
Διαγραμμα 3.30 Ποσοστο (%) των ιστοτοπων της κατηγοριας "οικονομικες υπηρεσιες" συμφωνα με την νεοτερη εκδοση του πρωτοκολλου TLS που υποστηριζουν και συγκεκριμενα TLS 1.0 (κοκκινο), TLS 1.2 (πρασινο) και καμια εκδοση SSL/TLS (μπλε)..... 81
Διαγραμμα 3.31 Ποσοστο (%) των ευπαθειων του πρωτοκολλου TLS (RC4, Weak DH, Poodle, Drown, ROBOT, Freak, OpenSSL, HeartBleed, Beast) στην κατηγορια ιστοτοπων "δημοσιοι οργανισμοι". 82
Διαγραμμα 3.32 Ποσοστο (%) των αδυναμιων της διαμορφωσης του πρωτοκολλου TLS (Untrust, Mismatch, Support SSL2, Support SSL3, Error FS, Error AHED) στην κατηγορια ιστοτοπων "δημοσιοι οργανισμοι". 82
Διαγραμμα 3.33 Ποσοστο (%) της βαθμολογιας που ελαβαν οι ιστοτοποι της κατηγοριας "δημοσιοι οργανισμοι" μετα την αναλυση τους οσον αφορα την ασφαλεια που παρεχουν με τα εργαλεια A (μπλε μπαρες) και B (κοκκινες μπαρες)..... 83
Διαγραμμα 3.34 Ποσοστο (%) της συμμορφωσης με διεθνη προτυπα (PCI, NIST, HIPPA), ετοιμοτητας για μεταβαση στην εκδοση του πρωτοκολλου TLS 1.3, καθως και την δυνατοτητα εγγραφης (Login), στην κατηγορια ιστοτοπων "δημοσιοι οργανισμοι"..... 84

Διαγραμμα 3.35 Ποσοστο (%) των ιστοτοπων της κατηγοριας “δημοσιοι οργανισμοι” συμφωνα με την νεοτερη εκδοση του πρωτοκολλου TLS που υποστηριζουν και συγκεκριμενα TLS 1.0 (κοκκινο), TLS 1.2 (πρασινο) και καμια εκδοση SSL/TLS (μπλε). 84
Διαγραμμα 3.36. Ποσοστο (%) των ευπαθειων του πρωτοκολλου TLS (RC4, Weak DH, Poodle, Drown, ROBOT, Freak, OpenSSL, HeartBleed, Beast) συνολικα σε ολες τις κατηγοριες ιστοτοπων. 85
Διαγραμμα 3.37 Ποσοστο (%) των αδυναμιων της διαμορφωσης του πρωτοκολλου TLS (Untrust, Mismatch, Support SSL2, Support SSL3, Error FS, Error AHED) συνολικα σε ολες τις κατηγοριες ιστοτοπων. 85
Διαγραμμα 3.38 Ποσοστο (%) της βαθμολογιας που ελαβαν συνολικα ολες οι κατηγοριες ιστοτοπων μετα την αναλυση τους οσον αφορα την ασφαλεια που παρεχουν με τα εργαλεια A (μπλε μπαρες) και B (κοκκινες μπαρες). 86
Διαγραμμα 3.39 Ποσοστο (%) της συμμορφωσης με διεθνη προτυπα (PCI, NIST, HIPPA), ετοιμοτητας για μεταβαση στην εκδοση του πρωτοκολλου TLS 1.3, καθως και την δυνατοτητα εγγραφης (Login), συνολικα σε ολες τις κατηγοριες ιστοτοπων. 87
Διαγραμμα 3.40 Ποσοστο (%) των ιστοτοπων σε ολες τις κατηγοριες συμφωνα με την νεοτερη εκδοση του πρωτοκολλου TLS που υποστηριζουν και συγκεκριμενα TLS 1.0 (κοκκινο), TLS 1.2 (πρασινο) και καμια εκδοση SSL/TLS (μπλε). 87
Διαγραμμα 4.41: Προσδιορισμος αριθμου των παραγοντων (Factors) με το κριτηριο της ιδιοτιμης (Eigenvalue) 97
Διαγραμμα 4.42: Απαντησεις στην ερωτηση 1 «Επιλεξτε φυλο» 109
Διαγραμμα 4.43: Απαντησεις στην ερωτηση 2 «Ηλικια» 109
Διαγραμμα 4.44: Απαντησεις στην ερωτηση 3 «Μορφωτικο επιπεδο» 110
Διαγραμμα 4.45: Απαντησεις στην ερωτηση 4 «Έχετε σπουδες σχετικες με την Επιστημη Υπολογιστων η την Πληροφορικη;» 110
Διαγραμμα 4.46: Απαντησεις στον ισχυρισμο 5 «Ειμαι εξοικειωμενος με την χρηση του Internet». 111
Διαγραμμα 4.47: Απαντησεις στην ερωτηση 6 «Χρονος πλοηγησης στο Internet καθημερινα» 112
Διαγραμμα 4.48: Απαντησεις στην ερωτηση 7 «Για ποιους λογους χρησιμοποιειτε κυριως το Internet?» 113
Διαγραμμα 4.49: Απαντησεις στην ερωτηση 8 «Ποιο φυλλομετρητη (browser) χρησιμοποιειτε κυριως στον υπολογιστη σας;» 113
Διαγραμμα 4.50: Απαντησεις στην ερωτηση 9 «Ποιο φυλλομετρητη (browser) χρησιμοποιειτε κυριως στο κινητο σας;» 114
Διαγραμμα 4.51: Απαντησεις στην ερωτηση 10 «Ποσο συχνα αναβαθμιζετε τον φυλλομετρητη σας;» 114
Διαγραμμα 4.52: Απαντησεις στην ερωτηση 11 «Έχετε πεσει θυμα καποιας ηλεκτρονικης απατης (κλοπη συνθηματικων, στοιχεια πιστωτικης καρτας);» 115
Διαγραμμα 4.53: Απαντησεις στην ερωτηση 12 «Πως αντιλαμβανεστε τον ορο "Ασφαλη Ιστοσελιδα"». 116
Διαγραμμα 4.54: Απαντησεις στην ερωτηση 13 «Πως αντιλαμβανεστε τον ορο "Ασφαλη συνδεση"». 117
Διαγραμμα 4.55: Απαντησεις στον ισχυρισμο 22 “Θα ηθελα τα δεδομενα που πληκτρολογω στο Internet (π.χ. κωδικοι, προσωπικες πληροφοριες κλπ) να κρυπτογραφουνται” 117
Διαγραμμα 4.56: Απαντησεις στον ισχυρισμο 23 “Οταν πλοηγουμαι σε μια ιστοσελιδα, ενδιαφερομαι να ειναι συγχρονη, με ευκολη δομη και προσβαση”. 118
Διαγραμμα 4.57: Απαντησεις στον ισχυρισμο 25 “Γνωριζω την οικογενεια πρωτοκολλων ασφαλειας SSL/TLS”. 118
Διαγραμμα 4.58: Απαντησεις στην ερωτηση 26 για το ποιες ιστοσελιδες θεωρειτε ασφαλεις; 119
Διαγραμμα 4.59: Απαντησεις στην ερωτηση 12 «Ποια-ες απο τις παρακατω επιθεσεις γνωριζετε». 120
Διαγραμμα 4.60: Απαντησεις στον ισχυρισμο 24 «Ο φυλλομετρητης μου υποστηριζει τα τελευταια πρωτοκολλα ασφαλειας.» 120
Διαγραμμα 4.61: Απαντησεις στον ισχυρισμο 27 «Γνωριζω την διαφορα του http απο το https.» 121
Διαγραμμα 4.62: Απαντησεις στον ισχυρισμο 28 «Γνωριζω πως ελεγχουμε την ασφαλεια ενος πιστοποιητικου σε συνδεσεις https.» 121
Διαγραμμα 4.63: Απαντησεις στον ισχυρισμο 29 «Γνωριζω τι σημαινει το λουκετο στην γραμμη πλοηγησης του φυλλομετρητη.» 122
Διαγραμμα 4.64: Απαντησεις στον ισχυρισμο 30 «Γνωριζω πως μπορω να προστατευθω απο μια ηλεκτρονικη απατη.» 122

Διαγραμμα 4.65: Απαντησεις στον ισχυρισμο 32 «Ελεγχω παντα αν η ιστοσελιδα που επισκεπτομαι ειναι https.» 123
Διαγραμμα 4.66: Απαντησεις στον ισχυρισμο 33 «Ελεγχω παντα αν η ιστοσελιδα που επισκεπτομαι εχει το χαρακτηριστικο λουκετο.» 123
Διαγραμμα 4.67: Απαντησεις στις ερωτησεις 14, 15, 16, 17, 18: Οι ιστοσελιδες των τραπεζων (14) , e-shop (15), δημοσιων φορεων (16), ειδησεογραφικων (17) και social media (Facebook, Twitter κτλ.) (18) εχουν λαβει ολα τα απαραιτητα μετρα για την ασφαλη πλοηγηση των χρηστων 125
Διαγραμμα 4.68: Απαντησεις στον ισχυρισμο 19 «Όταν πλοηγουμαι στο Internet ενδιαφερομαι για την ιδιωτικοτητα μου». 126
Διαγραμμα 4.69: Απαντησεις στον ισχυρισμο 20 «Όταν πλοηγουμαι στο Internet ενδιαφερομαι τα στοιχεια που εισαγω να μην γινονται γνωστα σε τριτους». 126
Διαγραμμα 4.70: Απαντησεις στον ισχυρισμο 21 «Όταν πλοηγουμαι στο Internet ενδιαφερομαι για την ασφαλεια των πληροφοριων μου» 127
Διαγραμμα 4.71: Απαντησεις στον ισχυρισμο 34 «Αν ο φυλλομετρητης μου βγαλει προειδοποιηση οτι η ιστοσελιδα που μπαινω δεν ειναι ασφαλης, θα διεκοπτα την πλοηγηση μου». 127
Διαγραμμα 4.72: Απαντησεις στον ισχυρισμο 35 «Αν γνωριζα οτι μια ιστοσελιδα που χρησιμοποιω συχνα δεν ειναι ασφαλης, θα σταματουσα να την χρησιμοποιω». 128

Παράρτημα Γ

Εικόνες

Εικονα 2.1: Η διαδικασια κρυπτογραφησης με Block Ciphers 16
Εικονα 2.2: Η διαδικασια κρυπτογραφησης με Stream Ciphers 17
Εικονα 2.3: Η διαδικασια της ψηφιακης υπογραφης 20
Εικονα 2.4: Σχηματικη απεικονιση της επιθεσης man in the middle attack 21
Εικονα 2.5:Διαφορες στην χειραψια του πρωτοκολλου TLS στις εκδοσεις 1.2 και 1.3 [9] 30
Εικονα 2.6: Τα επιπεδα του πρωτοκολλου TLS/SSL 33
Εικονα 2.7: Χειραψια με το μηνυμα Client Hello 35
Εικονα 2.8: Δημιουργια του Pre-Master Secret 37
Εικονα 2.9: Σχηματικη απεικονιση της διαδικασιας χειραψιας [15] 38
Εικονα 3.10 Αναφορα αξιολογησης ιστοτοπου με το εργαλειο A (SSL Labs) 55
Εικονα 3.11 Βαθμολογικη κλιμακα αξιολογησης ιστοτοπου με το εργαλειο A (SSL Labs) 56
Εικονα 3.12 Αναφορα του εργαλειου A σχετικα με το πιστοποιητικο της ιστοσελιδας 56
Εικονα 3.13 Αναφορα του εργαλειου A σχετικα με τους αλγοριθμους κρυπτογραφησης 57
Εικονα 3.14 Συνοπτικη αναφορα των ευπαθειων που εντοπιστηκαν συμφωνα με το εργαλειο A 57
Εικονα 3.15 Βαθμολογικη κλιμακα εργαλειου B (High-Tech Bridge) 58
Εικονα 3.16 Δειγμα απο σημεια αξιολογησης του εργαλειου B (High-Tech Bridge) 59
Εικονα 3.17 Αναφορα αξιολογησης ιστοτοπου με το εργαλειο B (High-Tech Bridge) 59
Εικονα 3.18 Παραδειγμα ελεγχου συμμορφωσης με το προτυπο PCI DSS 60
Εικονα 3.19 Σχηματικη αναπαρασταση της διαδικασιας βαθμολογησης [53] 88

Παράρτημα Δ

Πίνακες

ΠΙΝΑΚΑΣ 4.1: ΕΞΑΓΩΓΗ ΠΑΡΑΓΟΝΤΩΝ ΜΕ ΤΗ ΜΕΘΟΔΟ ΤΗΣ ΑΝΑΛΥΣΗΣ ΒΑΣΙΚΩΝ ΣΥΝΙΣΤΩΣΩΝ (PRINCIPAL COMPONENT ANALYSIS) ΚΑΙ ΟΡΘΟΓΩΝΙΑ ΠΕΡΙΣΤΡΟΦΗ ΤΩΝ ΑΞΟΝΩΝ ΜΕ ΤΗ ΜΕΘΟΔΟ VARIMAX..... 95
ΠΙΝΑΚΑΣ 4.2: ΈΛΕΓΧΟΣ ΣΥΝΟΛΙΚΗΣ ΔΕΙΓΜΑΤΙΚΗΣ ΚΑΤΑΛΛΗΛΟΛΗΤΑΣ ΜΕ ΤΟ ΜΕΤΡΟ K.M.O. (KAISER-MAYER-OLKIN).. 96
ΠΙΝΑΚΑΣ 4.3: ΕΠΙΛΟΓΗ ΠΛΗΘΟΥΣ ΠΑΡΑΓΟΝΤΩΝ ΜΕ ΤΟ ΚΡΙΤΗΡΙΟ ΤΟΥ ΠΟΣΟΣΤΟΥ ΤΗΣ ΔΙΑΚΥΜΑΝΣΗΣ..... 98
ΠΙΝΑΚΑΣ 4.4: ΔΕΙΚΤΗΣ ΕΣΩΤΕΡΙΚΗΣ ΣΥΝΕΠΕΙΑΣ ΤΟΥ CRONBACH ΓΙΑ ΤΗ ΔΙΕΡΕΥΝΗΣΗ ΤΗΣ ΑΞΙΟΠΙΣΤΙΑΣ..... 98
ΠΙΝΑΚΑΣ 4.5: ΈΛΕΓΧΟΣ ΚΑΝΟΝΙΚΟΤΗΤΑΣ ΤΩΝ ΕΝΝΟΙΟΛΟΓΙΚΩΝ ΚΑΤΑΣΚΕΥΩΝ..... 129
ΠΙΝΑΚΑΣ 4.6: ΑΝΑΛΥΣΗ ΣΥΣΧΕΤΙΣΗΣ ΜΕ ΤΟ ΣΥΝΤΕΛΕΣΤΗ ΣΥΣΧΕΤΙΣΗΣ SPEARMAN..... 130