Πανεπιστήμιο Πειραιώς – Τμήμα Πληροφορικής
Πρόγραμμα Μεταπτυχιακών Σπουδών
«Πληροφορική»

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	**Τεχνολογίες προστασίας απορρήτου και ιδιωτικότητας στο διαδίκτυο .**
Ονοματεπώνυμο Φοιτητή	**Μαθιουδάκη Ελένη**
Πατρώνυμο	**Ιωάννης**
Αριθμός Μητρώου	**ΜΠΠΛ**/ 08055
Επιβλέπων	**Παναγιώτης Κοτζανικολάου, Λέκτορας**

Οκτώβριος 2012

Τριμελής Εξεταστική Επιτροπή

(υπογραφή)	(υπογραφή)	(υπογραφή)
Παναγιώτης Κοτζανικολάου Λέκτορας	Δέσποινα Πολέμη Επίκουρος Καθηγήτρια	Χρήστος Δουληγέρης Καθηγητής

Πίνακας Περιεχομένων

Πίνακας εικόνων

Περίληψη

Η προέλευση του όρου ιδιωτικότητα ανάγεται ήδη από την εποχή του Αριστοτέλη με την διάκριση του δημοσίου και ιδιωτικού βίου και φτάνει μέχρι τις μέρες μας δίνοντας στον όρο μια επιπλέον διάσταση: της πληροφορίας που "φέρει" το άτομο. Η διάσταση αυτή αφορά τη δυνατότητα συλλογής, αποθήκευσης και επεξεργασίας των προσωπικών δεδομένων, όπου προσωπικά δεδομένα αποτελούν οι πληροφορίες που αναφέρονται σε και περιγράφουν ένα άτομο (π.χ. ονοματεπώνυμο, ηλικία, εκπαίδευση κτλ). Η ανάπτυξη των τεχνολογιών κατέστησε αντιληπτή την μετατροπή της κοινωνίας σε κοινωνία της πληροφορίας και το ρόλο που διαδραματίζει αυτή στην ενιαία αγορά ώστε να τεθεί πλέον το ζήτημα της προστασίας των προσωπικών δεδομένων. Επειδή, όμως, τα νομοθετικά μέτρα δεν επαρκούν θα πρέπει να χρησιμοποιηθούν και οι κατάλληλες τεχνολογίες ενίσχυσης της ιδιωτικότητας στο διαδίκτυο ανάλογα πάντα με τα τεχνολογικά ζητήματα που προκύπτουν και τις απαιτήσεις του χρήστη.

Η προσπάθειά μας στην παρούσα διατριβή εστιάζεται στην μελέτη τεχνικών προστασίας της ιδιωτικότητας με τη χρήση εικονικού εργαστηριακού περιβάλλοντος. Πιο συγκεκριμένα, οι τεχνολογίες που εφαρμόζονται αφορούν την πλοήγηση μέσω TOR browser, την κρυπτογράφηση με το πρωτόκολλο SSL και την εφαρμογή της πλατφόρμας προστασίας προσωπικών δεδομένων P3P. Για το σκοπό αυτό χρησιμοποιήθηκε ένα λογισμικό καταγραφής πακέτων (packet sniffer), το Wireshark, προκειμένου να εξετάσουμε την αποτελεσματική άμυνα ενός συστήματος απέναντι στην πιο σημαντική επίθεση ενάντια στην ανωνυμία και στην διασφάλιση της ιδιωτικότητας στο Διαδίκτυο. Την επίθεση ενός ωτακουστή.

Στο τέλος γίνεται μια αξιολόγηση των αποτελεσμάτων της μελέτης μας καθώς και διατύπωση προτάσεων για την κατεύθυνση στην οποία θα μπορούσαν να στραφούν μελλοντικές έρευνες.

Λέξεις κλειδιά:privacy, privacy enhancing technologies, SSL, PGP,P3P, LPWA,TOR

Abstract

The origin of the term privacy comes from the times of Aristotle with the distinction between the public and private life and reaches nowdays giving the term an additional dimension: the dimension of the information the person carries. This dimension is related to the collection, storing and processing of personal data, where personal data are all the information which refer to and describe one person (name, age, education etc). The development of the technology made perceptible the transformation of our society to information society and its role in the market and as a result the issue for the protection of personal data is now set. As the legislative measures are not sufficient, the appropriate technologies of privacy enhancing technologies must be used, always accordingly to the technological issues that arise and the demands of the user.

Our effort in this thesis focuses on the study of privacy enhancing technologies using virtual lab environment. More specifically, the technologies refer to anonymous browsing with TOR, encryption with SSL protocoll and deploy of Platform of Privacy Preferences (P3P). For this purpose we used a packet sniffer (Wireshark) for capturing packets in order to examine the effective defence of a system towards the attack of an eavesdropper.

Summarizing, an evaluation of the results of our study takes place and proposals for the direction in which future researches can take place.

Keywords: privacy, privacy enhancing technologies, SSL, PGP,P3P, LPWA,TOR

''*the right to be let alone*''

Warren and Brandeis,1890

ΚΕΦΑΛΑΙΟ 1ο

Εισαγωγή

Ο όρος *ιδιωτικότητα* αναγνωρίστηκε ως θεμελιώδες ανθρώπινο δικαίωμα ήδη από το 1890 με την πραγματεία των δικαστών Warren και Brandeis. Η προέλευση, όμως του όρου ανάγεται σε πολύ παλαιότερα χρόνια, ήδη από την εποχή του Αριστοτέλη με τη διάκριση μεταξύ του δημόσιου βίου (όπως αυτός εκφράζεται μέσω της πολιτικής δραστηριοποίησης του ατόμου) και του ιδιωτικού (που διάγεται στα πλαίσια της οικογένειας και της οικίας).

Κατά τη διάρκεια του Μεσαίωνα, οι κοινωνικές τάξεις ήταν σαφώς διαχωρισμένες, με προεξάρχουσες τον κλήρο και την αριστοκρατία, και την κατώτερη να μην απολαμβάνει ουσιωδών δικαιωμάτων, πόσο μάλλον αυτό της ιδιωτικότητας. Ούτε, βέβαια, και οι ανώτερες τάξεις ήταν απόλυτα προστατευμένες, αφού κάθε τους κίνηση εκτελούταν υπό το άγρυπνο μάτι του περιβάλλοντός τους. Η στροφή άρχισε να παρατηρείται από την εποχή του Διαφωτισμού. Ο Καντ ήταν ο πρώτος που κατέληξε στο συμπέρασμα ότι το άτομο έχει την ικανότητα να επικοινωνεί και να δημιουργεί και η ικανότητα του αυτή διαταρασσόταν αν κάποιος διατάρασσε την ιδιωτικότητά του. Το άτομο, ον λογικό και αυτόνομο, θα πρέπει να έχει όλο τον απαιτούμενο χώρο ώστε να αποφασίζει για τον εαυτό του, να ορίζει ποια είναι η αλήθεια και να εκπληρώνει τους στόχους και τις επιθυμίες του. Γι' αυτό το λόγο, οι ανώτερες τάξεις θα πρέπει να αντιμετωπίζουν τις κατώτερες σαν μεμονωμένα άτομα και όχι σαν μια μάζα, στην οποία αφαιρούν το δικαίωμα να αποφασίζει ο καθένας για τον εαυτό του και την οποία σταδιακά οδηγούν στην υποδούλωση. Ο Λοκ, αν και προγενέστερος του Καντ, ωστόσο προχώρησε ένα βήμα παραπέρα συγκρίνοντας την υπεράσπιση της ιδιοκτησίας με το δικαίωμα του ατόμου πάνω στο ίδιο του το σώμα. Δικαιολογεί εκείνον που οδηγείται στο φόνο προκειμένου να υπερασπιστεί τη ζωή του όταν απειλείται η ιδιοκτησία του και παράλληλα επεκτείνει την υπεράσπιση της ιδιοκτησίας και στον τομέα της ιδιωτικότητας των επικοινωνιών και της ελευθερίας του λόγου.

Αν και η νομική κατοχύρωση της προστασίας της ιδιωτικότητας στη Δύση υπάρχει εδώ και περίπου 100 χρόνια, οι πρωτες προσπάθειες είχαν γίνει πολύ νωρίτερα. Οι πρώτες υποθέσεις που έφτασαν στα δικαστήρια ήταν το 1361 στην Αγγλία και αφορούσαν ωτακουστές. Ακολούθως, αναφορές από τον 17ο αιώνα καθιστούν σαφές ότι η προσωπική αλληλογραφία αποτελεί μέρος της ιδιωτικής ζωής και χρήζει προστασίας. Το 1776, το κοινοβούλιο της Σουηδίας θέσπισε νομοσχέδιο για το δικαίωμα πρόσβασης στα δημόσια έγγραφα. Σύμφωνα με αυτό, όλα οι πληροφορίες που συλλέγονται από την κυβέρνηση και αφορούν πολίτες θα πρέπει να χρησιμοποιούνται για νόμιμους σκοπούς ενώ ταυτόχρονα θα μπορεί ο κάθε πολίτης να έχει πρόσβαση σε αυτές. Το 1858, η Γαλλία απαγόρευσε τη δημοσιοποίηση προσωπικών δεδομένων και θέσπισε ποινές για τους παραβάτες. Το 1889, ο ποινικός κώδικας της Νορβηγίας απαγόρευσε τη δημοσίευση πληροφοριών σχετικές με προσωπικές ή ιδιωτικές υποθέσεις.

Και φτάνουμε στο 1890 όπου οι δικαστές του Ανώτατου Δικαστηρίου των ΗΠΑ, Louis Brandeis και Samuel Warren εκδίδουν το διάσημο πλέον σύγγραμμά τους και στο οποίο χαρακτηρίζουν το δικαίωμα στην ιδιωτικότητα σαν το πιο σημαντικό απ' όλα τα δικαιώματα και τις ελευθερίες που προσφέρει η δημοκρατία [1]. Αναγνωρίζουν ότι οι πολιτικές, οικονομικές και κοινωνικές αλλαγές συνεπάγονται την θέσπιση και νομική κατοχύρωση νέων δικαιωμάτων. Έτσι, ενώ μέχρι τότε ο νόμος προστάτευε την ιδιοκτησία (και κατ' επέκταση την ίδια τη ζωή) από φυσικούς εισβολείς, οι ζυμώσεις και εξελίξεις που συμβαίνουν στους κόλπους μιας κοινωνίας επεκτείνουν το θεσμό της ιδιοκτησίας ώστε να καλύπτει τόσο τα υλικά όσο και τα άυλα αγαθά. Η

ιδιωτικότητα γι' αυτούς είναι το δικαίωμα του κάθε ατόμου στην ηρεμία και στην ''απαραβίαστη προσωπικότητα'', όρος ευρύτερος που καλύπτει τις σκέψεις, τα συναισθήματα και τα πνευματικά επιτεύγματα του ατόμου καθώς, επίσης, και το δικαίωμα του ατόμου να καθορίσει το ίδιο τι πληροφορίες και σε ποιο βαθμό θα κοινοποιηθούν στους άλλους. Και αν ο νόμος μέχρι τότε προστάτευε την υλική ιδιοκτησία του ατόμου, η εξέλιξη της τεχνολογίας κατέστησε σαφές ότι θα πρέπει ο νόμος να αναγνωρίσει την προστασία της προσωπικότητας υπό τον όρο ''προστασία της ιδιωτικότητας''.

Μετά το 2ο Παγκόσμιο Πόλεμο ξεκίνησε στις ΗΠΑ μια συζήτηση σχετικά με την ιδιωτικότητα. Αν και ο ορισμός της ιδιωτικότητας δεν διαφέρει και πολύ από την εποχή των Warren και Brandeis, ωστόσο όλοι συγκλίνουν στο γεγονός ότι λόγω της ανάπτυξης της τεχνολογίας, η ιδιωτικότητα και η προστασία της αποκτά ολοένα και αυξανόμενο ενδιαφέρον. Από τις εκδόσεις εκείνης της εποχής διαπιστώνουμε ότι υπάρχουν κάποιες λέξεις, τις οποίες οι συγγραφείς χρησιμοποιούν κατά κόρον προκειμένου να ορίσουν την ιδιωτικότητα. Οι λέξεις αυτές είναι η ελευθερία, ο έλεγχος και η αυτοδιάθεση του ατόμου.

Το 1967 ο Alan Westin στο έργο του ''Privacy and Freedom'', συνοψίζει και καταλήγει στην εξής διατύπωση για τη ιδιωτικότητα:

> *''Privacy is the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.*

Τη διατύπωση του αυτή μπορούμε να την εκλάβουμε ως αποδοχή αλλά και επέκταση του ορισμού των Warren και Bandeis, αφού διατυπώνει μια πιο ξεκάθαρη άποψη για το τι σημαίνει ''το δικαίωμα να αφήνεται κάποιος μόνος του''. Αμέσως μετά, ο Westin συνεχίζει

> *''Viewed in terms of the relation of the individual to social participation, privacy is the voluntary and temporary withdrawal of a person from the general society through physical or psychological mean, either in a state of solitude or small-group intimacy or, when among larger groups, in a condition of anonymity or reserve. ''*

Το άτομο, λοιπόν, έχει τη δυνατότητα, όχι μόνο να καθορίζει τις πληροφορίες που θα γνωστοποιηθούν, αλλά και ενίοτε να κινείται ανώνυμα μέσα στους κόλπους της κοινωνίας όπου ζει. Θα μπορούσε κάποιος να επισημάνει ότι δεν είναι το άτομο καθεαυτό που ενδιαφέρει αλλά η πληροφορία που μεταφέρει. Η διάσταση αυτή της ιδιωτικότητας αφορά τη δυνατότητα συλλογής, αποθήκευσης και επεξεργασίας των προσωπικών δεδομένων.

Όπως διαπιστώνουν και οι Fischer-Hubner, η έννοια της ιδιωτικότητας μπορεί να εφαρμοστεί σε τρεις διαφορετικούς τομείς:

- Εδαφική προστασία της προσωπικής ζωής. Περιλαμβάνει την προστασία της στενής φυσικής περιοχής που περιβάλλει ένα πρόσωπο.
- Προστασία της ιδιωτικότητας του ίδιου του ατόμου ενάντια σε αδικαιολόγητες παρεισφρύσεις.
- Προστασία της πληροφορίας. Περιλαμβάνει τον έλεγχο του αν και πώς θα γίνει η επεξεργασία των προσωπικών δεδομένων.

1.2 Εννοιολογική θεμελίωση

Γενικά, η «ιδιωτικότητα» μπορεί να γίνει αντιληπτή και ως «περιουσία», υπό την έννοια ότι κάποιος μπορεί να αποδεχθεί να μεταφέρει μέρος του ελέγχου των προσωπικών δεδομένων του σε κάποιο τρίτο για κάποιο αντίτιμο. Επίσης, μπορεί να θεωρηθεί ως «αυτονομία» υπό την έννοια ότι κάθε άτομο είναι ελεύθερο να εξουσιοδοτήσει μερικά ή συνολικά κάποιον τρίτο να συγκεντρώνει, επεξεργάζεται, διαχέει, αξιοποιεί τα προσωπικά δεδομένα του για κάποιο

συγκεκριμένο σκοπό. Τέλος η ιδιωτικότητα μπορεί να θεωρηθεί ως «απομόνωση» υπό την έννοια ότι καθένας έχει το δικαίωνα να απαιτεί να μην τον ενοχλούν.

- **Προσωπικά δεδομένα** είναι κάθε πληροφορία που αναφέρεται σε και περιγράφει ένα άτομο, όπως: στοιχεία αναγνώρισης (ονοματεπώνυμο, ηλικία, κατοικία, επάγγελμα, οικογενειακή κατάσταση κλπ.), φυσικά χαρακτηριστικά, εκπαίδευση, εργασία (προϋπηρεσία, εργασιακή συμπεριφορά κλπ), οικονομική κατάσταση (έσοδα, περιουσιακά στοιχεία, οικονομική συμπεριφορά), ενδιαφέροντα, δραστηριότητες, συνήθειες. Το άτομο (φυσικό πρόσωπο) στο οποίο αναφέρονται τα δεδομένα ονομάζεται υποκείμενο των δεδομένων.
- **Ευαίσθητα δεδομένα** χαρακτηρίζονται τα προσωπικά δεδομένα ενός ατόμου που αναφέρονται στη φυλετική ή εθνική του προέλευση, στα πολιτικά του φρονήματα, στις θρησκευτικές ή φιλοσοφικές του πεποιθήσεις, στη συμμετοχή του σε συνδικαλιστική οργάνωση, στην υγεία του, στην κοινωνική του πρόνοια, στην ερωτική του ζωή, τις ποινικές διώξεις και καταδίκες του, καθώς και στη συμμετοχή του σε συναφείς με τα ανωτέρω ενώσεις προσώπων. Τα ευαίσθητα δεδομένα προστατεύονται από τον Νόμο με αυστηρότερες ρυθμίσεις από ότι τα απλά προσωπικά δεδομένα.
- **Επεξεργασία προσωπικών δεδομένων** είναι κάθε εργασία που πραγματοποιείται σε δεδομένα προσωπικού χαρακτήρα, όπως: συλλογή, καταχώριση, οργάνωση, διατήρηση ή αποθήκευση, τροποποίηση, εξαγωγή, χρήση, διαβίβαση, διάδοση, συσχέτιση ή συνδυασμός, διασύνδεση, δέσμευση, διαγραφή, καταστροφή. Η προστασία των προσωπικών αυτών δεδομένων (ή αλλιώς ασφάλεια δεδομένων) είναι αυτή που εγγυάται ουσιαστικά την ιδιωτικότητα.

Οι δύο όροι της ιδιωτικότητας και της ασφάλειας είναι τόσο στενά συνδεδεμένοι που συχνά υπερκαλύπτει ο ένας τον άλλο αν και υπάρχουν κάποιες διαφορές που αξίζει να αναφερθούν.

- Ως **ιδιωτικότητα** ορίζεται το δικαίωμα του ατόμου να προστατέψει τις πληροφορίες που το αφορούν και να μην προβεί σε αποκάλυψή τους.
- Ως **ασφάλεια** ορίζεται η προστασία της επικοινωνίας από άτομα που δεν έχουν δικαίωμα πρόσβασης σε αυτήν.

Η ιδιωτικότητα δεν αφορά μόνο την πληροφορία και τον κίνδυνο απώλειας του ελέγχου της-αφορά και τον προσωπικό χώρο και τα προσωπικά αντικείμενα που αποτελούν σημαντική πτυχή της προσωπικής ακεραιότητας. Διάσταση υπάρχει ακόμα και στους όρους ‘’προστασία της ιδιωτικότητας’’ και ‘’προστασία των προσωπικών δεδομένων’’ με τον πρώτο να είναι προσανατολισμένος στην προστασία της οικίας, της οικογενειακής ζωής και της επικοινωνίας σε αντιδιαστολή με τον δεύτερο να επικεντρώνει την ανάλυσή του στις ατομικές ελευθερίες και τις σχέσεις επικοινωνίας σε μια κοινωνία.

Σύμφωνα με το Electronic Privacy Information Centre (EPIC) [2] οι βασικοί πυλώνες πάνω στους οποίους στηρίζεται η προστασία της ιδιωτικότητας, είναι οι ακόλουθοι:

1. Νομοθεσία: η ύπαρξη νόμων που διέπουν τη συλλογή, χρήση και διάδοση των προσωπικών πληροφοριών τόσο στο δημόσιο όσο και στον ιδιωτικό τομέα.
2. Διατάξεις, οι οποίες λειτουργούν συμπληρωματικά σε ορισμένους νόμους ή σε συγκεκριμένους τομείς.
3. Οι κανόνες, τους οποίους καθιερώνουν οι εταιρείες και οι οργανισμοί προκειμένου να διασφαλίσουν την ακεραιότητα των δεδομένων τους.
4. Τεχνολογίες ενίσχυσης της ιδιωτικότητας με την ανάπτυξη των οποίων καθίσταται εφικτό στα μεμονωμένα άτομα να προστατεύουν την ιδιωτικότητά τους.

1.3 **Δομή και στόχοι της διατριβής**

Στο 1^{ο} και 2^{ο} κεφάλαιο της παρούσας διατριβής παρουσιάζεται η ιστορική εξέλιξη της προστασίας των προσωπικών δεδομένων σε ευρωπαϊκό, παγκόσμιο αλλά και εθνικό επίπεδο.

Στο 3^{ο} κεφάλαιο θα αναφερθούμε στις απειλές ασφάλειας και ιδιωτικότητας, καθώς και στις απαιτήσεις που ανακύπτουν προκειμένου τα πληροφοριακά συστήματα να αποτρέψουν την παραβίαση της ιδιωτικότητας.

Το 4^{ο} κεφάλαιο αναφέρεται στα μέτρα ενίσχυσης της ιδιωτικότητας που μπορούν να ληφθούν α) στην πλευρά του χρήστη (client-side) β) στην πλευρά του εξυπηρετητή (server-side) και γ) στα κοινά μέτρα προστασίας.

Στο 5^{ο} κεφάλαιο παρουσιάζεται μία μελέτη περίπτωσης, μέσω της πρακτικής εφαρμογής τεχνολογιών ενίσχυσης της ιδιωτικότητας. Εξετάζουμε το επίπεδο ασφαλείας που προσφέρει ο συνδυασμός της εφαρμογής μέτρων ασφάλειας και ιδιωτικότητας, στο επίπεδο της δρομολόγησης (μέσω της εφαρμογής Onion Routing – TOR browser), της κρυπτογράφησης (εφαρμογή πρωτοκόλλου SSL), καθώς και γλωσσών προστασίας της ιδιωτικότητας (πλατφόρμα P3P).

Τέλος στο 6^{ο} κεφάλαιο συνοψίζονται τα βασικά συμπεράσματα και τα ανοικτά προβλήματα που προκύπτουν από την παρούσα διατριβή.

ΚΕΦΑΛΑΙΟ 2°

Νομοθετικό πλαίσιο της προστασίας προσωπικών δεδομένων

2.1 Προστασία των προσωπικών δεδομένων στην Ευρώπη

Το 1950 συνέρχεται το Ευρωπαϊκό Συμβούλιο και στις 5 Νοεμβρίου υπογράφει τη Σύμβαση της Ρώμης για την Προάσπιση των Ανθρωπίνων Δικαιωμάτων και των θεμελιωδών ελευθεριών, της οποίας το άρθρο 8 αποτελεί μέχρι και σήμερα μία από τις πιο σημαντικές διεθνείς συμφωνίες για την προστασία της ιδιωτικότητας.

''Παν πρόσωπον δικαιούται εις σεβασμόν της ιδιωτικής και οικογενειακής ζωής του, της κατοικίας του και της αλληλογραφίας του.''

Το δικαίωμα, βέβαια, αυτό μπορεί να περιοριστεί εφόσον συντρέχουν συγκεκριμένοι λόγοι. Συγκεκριμένα, συνεχίζει στη 2η παράγραφο

'' Δεν επιτρέπεται να υπάρξη επέμβασις δημοσίας αρχής εν τη ασκήσει του δικαιώματος τούτου, εκτός εάν η επέμβασις αύτη προβλέπεται υπό του νόμου και αποτελεί μέτρον το οποίον, εις μίαν δημοκρατικήν κοινωνίαν, είναι αναγκαίον δια την εθνικήν ασφάλειαν, την δημοσίαν ασφάλειαν, την οικονομικήν ευημερίαν της χώρας, την προάσπισιν της τάξεως και την πρόληψιν ποινικών παραβάσεων, την προστασίαν της υγείας ή της ηθικής, ή την προστασίαν των δικαιωμάτων και ελευθεριών άλλων.''

Το Συμβούλιο, μάλιστα,

'' Προκειμένου να διασφαλισθεί ο σεβασμός των υποχρεώσεων που απορρέουν για τα Υψηλά Συμβαλλόμενα Μέρη από την παρούσα Σύμβαση και τα Πρωτόκολλα αυτής, συστήνεται Ευρωπαϊκό Δικαστήριο των Δικαιωμάτων του Ανθρώπου, εφεξής αποκαλούμενο «το Δικαστήριο». Το Δικαστήριο λειτουργεί σε μόνιμη βάση.''

Με τον τρόπο αυτό δεσμεύει την κάθε χώρα να εκτελέσει τη Σύμβαση ενσωματώνοντας τη στο εθνικό της δίκαιο.

Στις 19.12.1968 η Γενική Συνέλευση του Οργανισμού Ηνωμένων Εθνών, στα πλαίσια των δραστηριοτήτων της υιοθέτησε την παραπάνω Σύμβαση με την απόφαση 2450/19.12.1966. Στη Διεθνή Χάρτα των Δικαιωμάτων του Ανθρώπου που εξέδωσε προστατεύεται το δικαίωμα της ιδιοκτησίας (άρθρο 17, παράγραφος 1 & 2), το δικαίωμα της ελευθερίας, της σκέψης και της θρησκείας (άρθρο 18, παράγραφος 1 & 2) και το δικαίωμα της ελευθερίας της γνώμης και της έκφρασης (άρθρο 19, παράγραφος 1 & 2). Συγκεκριμένα το δικαίωμα της έκφρασης περιλαμβάνει ''.. την ελευθερία της αναζήτησης, της λήψης και της μετάδοσης πληροφοριών και απόψεων κάθε είδους, ανεξαρτήτως συνόρων, προφορικά, γραπτά, σε έντυπα, σε κάθε μορφή τέχνης ή με κάθε άλλο μέσο της επιλογής του.'' Και φυσικά υπόκειται σε περιορισμούς ''Για το σεβασμό των δικαιωμάτων ή της υπόληψης των άλλων και για την προστασία της εθνικής ασφάλειας, της δημόσιας τάξης, της δημόσιας υγείας ή των χρηστών ηθών.''

Το 1980, ο Οργανισμός Οικονομικής Συνεργασίας και Ανάπτυξης (ΟΟΣΑ) εξέδωσε τις ''Κατευθυντήριες Αρχές που διέπουν την προστασία της ιδιωτικότητας και τις διασυνοριακές ροές των προσωπικών δεδομένων''. Πρόκειται για κείμενο μη δεσμευτικού χαρακτήρα (soft law) με το οποίο ο ΟΟΣΑ θέλησε και να επιδοκιμάσει την προστασία της ιδιωτικότητας αλλά και να προάγει τις αρχές αυτές γιατί η ύπαρξη πιθανών ανισοτήτων στις εθνικές νομοθεσίες θα μπορούσε να παρεμποδίσει την απρόσκοπτη ροή προσωπικών δεδομένων πέραν των

συνόρων. Κάτι τέτοιο θα μπορούσε να προκαλέσει αποδιοργάνωση σε σημαντικούς τομείς της οικονομίας, όπως ο τραπεζικός τομέας και ο τομέας της ασφάλειας. Οι αρχές αυτές είναι:

1. ***Η αρχή της περιορισμένης συγκέντρωσης και συλλογής δεδομένων (collection limitation principle):*** Θα πρέπει να υπάρχουν όρια στη συλλογή των προσωπικών δεδομένων καθώς και αυτή να γίνεται με νόμιμα μέσα και ανάλογα με την περίπτωση με τη γνώση ή συγκατάθεση του υποκειμένου των δεδομένων.
2. ***Η αρχή της ποιότητας των δεδομένων (data quality principle):*** Τα δεδομένα πρέπει να είναι σχετικά με τους σκοπούς για τους οποίους πρόκειται να χρησιμοποιηθούν και στο βαθμό που απαιτείται να είναι ακριβή, πλήρη και διαρκώς ενημερωμένα.
3. ***Η αρχή του προσδιορισμένου σκοπού (purpose specification principle):*** Θα πρέπει να προσδιορίζονται επακριβώς οι σκοποί για τους οποίους συλλέγονται τα προσωπικά δεδομένα και η χρήση τους να συνάδει με τους σκοπούς αυτούς. Κάθε αλλαγή στους σκοπούς θα πρέπει να αναφέρεται.
4. ***Η αρχή της περιορισμένης χρήσης των προσωπικών δεδομένων (use limitation principle):*** Τα προσωπικά δεδομένα δεν θα πρέπει να αποκαλύπτονται ή να χρησιμοποιούνται για σκοπούς άλλους από αυτούς για τους οποίους έχει συμφωνηθεί εκτός εάν α) υπάρχει η συναίνεση του χρήστη ή β) επιβάλλεται από το νόμο.
5. ***Η αρχή μέτρων ασφαλείας των προσωπικών δεδομένων (security safeguards principle):*** Μέτρα ασφαλείας θα πρέπει να λαμβάνονται ώστε να αποφεύγονται κίνδυνοι όπως απώλεια δεδομένων ή πρόσβαση άνευ αδείας, καταστροφή, τροποποίηση ή αποκάλυψη.
6. ***Η αρχή της διαφάνειας (openness principle):*** Θα πρέπει να υπάρχει μια γενική αρχή διαφάνειας σχετικά με τις εξελίξεις, τις πρακτικές και τις πολιτικές που ακολουθούνται σχετικά με τα προσωπικά δεδομένα.
7. ***Η αρχή της συμμετοχής του ατόμου (individual participation principle):*** Το άτομο θα πρέπει να έχει το δικαίωμα α) να ζητά επιβεβαίωση για το αν ο κάτοχος των δεδομένων (data controller) έχει στη διάθεσή του στοιχεία που το αφορούν β) να ζητά να του κοινοποιηθούν τα στοιχεία που έχει στην κατοχή του ο data controller i) σε εύλογο χρονικό διάστημα ii) αντί λογικού χρηματικού ποσού iii) με εύλογο τρόπο και iv) με εύληπτο τρόπο. γ)Αν τα αιτήματα του απορριφθούν, θα πρέπει να του κοινοποιηθούν οι λόγοι ώστε να μπορέσει να αντιδράσει και δ) να αμφισβητήσει τα στοιχεία που τον αφορούν ώστε αν έχει δίκιο, να πετύχει τη διόρθωση, συμπλήρωση, τροποποίηση ή και διαγραφή των δεδομένων.
8. ***Η αρχή της ευθύνης (accountability principle:*** Ο data controller θα πρέπει να συμμορφώνεται με τα μέτρα που θέτουν σε ισχύ τις προαναφερθείσες αρχές.

Το πρώτο νομικά δεσμευτικό κείμενο αποτελεί η Σύμβαση 108/28.1.1981 του Συμβουλίου της Ευρώπης ‘’για την προστασία των ατόμων από την αυτοματοποιημένη επεξεργασία δεδομένων προσωπικού χαρακτήρα’’. Αποτελεί ήδη σημείο αναφοράς για 43 κράτη στην Ευρώπη, ενώ οποιαδήποτε χώρα στον κόσμο διαθέτει την απαιτούμενη νομοθεσία για την προστασία των δεδομένων μπορεί να γίνει συμβαλλόμενο μέρος της σύμβασης αυτής. Δεν ήταν, βέβαια, αμέσου εφαρμογής. Η ισχύς της, εξαρτιόταν όχι μόνο από την κύρωσή της αλλά και από τη θέσπιση εσωτερικών ρυθμίσεων σε κάθε χώρα (άρθρο 4, ‘’ Each Party shall take the necessary measures in its domestic law to give effect to the basic principles for data protection set out in this chapter’’). Με το άρθρο 12 έθεσε κανόνες για την προστασία των προσωπικών δεδομένων στην περίπτωση της διασυνοριακής ροής πληροφοριών (συγκεκριμένα αναφέρεται ότι η διασυνοριακή ροή δεδομένων δεν θα πρέπει να απαγορεύεται με μοναδικό γνώμονα την προστασία της ιδιωτικότητας-σαφέστατα η αρχή αυτή δεν είναι απόλυτη αλλά υπόκειται σε κάποιες εξαιρέσεις) ενώ με το άρθρο 13 τα μέλη υποχρεούνται στην αμοιβαία συνδρομή για την εφαρμογή της σύμβασης. Αυτό που έλειπε, όμως, από τη συγκεκριμένη σύμβαση ήταν η καθιέρωση ανεξάρτητων μηχανισμών ελέγχου, στοιχείο που προστέθηκε με το Πρόσθετο Πρωτόκολλο του 2001. Όσον αφορά την Ελλάδα η σύμβαση επικυρώθηκε με το νόμο 2068/1992 χωρίς να έχουν ληφθεί τα αναγκαία μέτρα ενώ άρχισε να

ισχύει από την 1.1.1995 και κατέστη αναπόσπαστο μέρος του ελληνικού δικαίου σύμφωνα με τη συνταγματική διάταξη του άρθρου 28, παρ.1 του Συντάγματος.

2.1.1 Κοινοτική Οδηγία 95/46/ΕΚ

Η κοινοτική οδηγία 95/46/ΕΚ [3] του Ευρωπαϊκού Κοινοβουλίου καθιερώνει δύο από τους πιο παλιούς στόχους της ευρωπαϊκής κοινότητας: α) την ελεύθερη και απρόσκοπτη ροή προσωπικών δεδομένων και β) την προστασία θεμελιωδών δικαιωμάτων και ελευθεριών των ατόμων.

Σύμφωνα με το άρθρο 2 της οδηγίας ως δεδομένα προσωπικού χαρακτήρα νοείται ‘’κάθε πληροφορία που αναφέρεται σε φυσικό πρόσωπο του οποίου η ταυτότητα είναι γνωστή ή μπορεί να εξακριβωθεί «το πρόσωπο στο οποίο αναφέρονται τα δεδομένα» ως πρόσωπο του οποίου η ταυτότητα μπορεί να εξακριβωθεί λογίζεται το πρόσωπο εκείνο που μπορεί να προσδιοριστεί, άμεσα ή έμμεσα, ιδίως βάσει αριθμού ταυτότητας ή βάσει ενός ή περισσοτέρων συγκεκριμένων στοιχείων που χαρακτηρίζουν την υπόστασή του από φυσική, βιολογική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική άποψη’’ ενώ ως επεξεργασία δεδομένων προσωπικού χαρακτήρα νοείται ‘’ κάθε εργασία ή σειρά εργασιών που πραγματοποιούνται με ή χωρίς τη βοήθεια αυτοματοποιημένων διαδικασιών και εφαρμόζονται σε δεδομένα προσωπικού χαρακτήρα, όπως η συλλογή, η καταχώρηση, η οργάνωση, η αποθήκευση, η προσαρμογή ή η τροποποίηση, η ανάκτηση, η αναζήτηση πληροφοριών, η χρήση, η ανακοίνωση με διαβίβαση, η διάδοση ή κάθε άλλη μορφή διάθεσης, η εναρμόνιση ή ο συνδυασμός, καθώς και το κλείδωμα, η διαγραφή ή η καταστροφή’’.

Η οδηγία αποτελεί το κείμενο αναφοράς, σε ευρωπαϊκό επίπεδο, στα θέματα προστασίας των δεδομένων προσωπικού χαρακτήρα και θεσπίζει ένα κανονιστικό πλαίσιο που αποσκοπεί στην εγκαθίδρυση μιας ισορροπίας μεταξύ των δύο αυτών στόχων της. Για το σκοπό αυτό ορίζει τα όρια για τη συλλογή και τη χρησιμοποίηση των δεδομένων προσωπικού χαρακτήρα και ζητά τη δημιουργία σε κάθε κράτος-μέλος ενός ανεξάρτητου εθνικού οργανισμού επιφορτισμένου με την προστασία των δεδομένων αυτών. Η οδηγία εφαρμόζεται τόσο στα δεδομένα που αποτελούν αντικείμενο επεξεργασίας με αυτοματοποιημένες διαδικασίες (π.χ. πληροφορική βάση δεδομένων πελατών) καθώς και στη μη αυτοματοποιημένη επεξεργασία δεδομένων προσωπικού χαρακτήρα που περιλαμβάνονται ή πρόκειται να περιληφθούν σε αρχείο (παραδοσιακά αρχεία σε χαρτί).

Αρχικά, πάντως, το θέμα της προστασίας προσωπικών δεδομένων δεν αποτελούσε μείζων ζήτημα για την Ευρωπαϊκή κοινότητα. Αυτό που ενδιέφερε κυρίως ήταν η ανάπτυξη των τεχνολογιών και η κοινωνία της πληροφορίας. Όταν, όμως, έγινε αντιληπτό ότι η υιοθέτηση των νέων τεχνολογιών από την κοινωνία την μετέτρεψαν σταδιακά σε κοινωνία της πληροφορίας και το ρόλο που παίζει αυτή στην ενιαία αγορά, τότε η κοινότητα αναγκάστηκε να επανεξετάσει το ζήτημα της προστασίας των προσωπικών δεδομένων. Συγκεκριμένα, συνετέλεσαν 3 παράγοντες προς αυτήν την κατεύθυνση :

Α) η αύξηση της διασυνοριακής ροής προσωπικών δεδομένων μεταξύ των κρατών-μελών κατέστησε σαφές, ότι το διαφορετικό επίπεδο προστασίας στις εθνικές νομοθεσίες, θα μπορούσε να αποβεί ανασταλτικό στις οικονομικές συναλλαγές μεταξύ τους (Προοίμιο 7 της οδηγίας).

Β) Η συνειδητοποίηση ότι ‘’ για την εγκαθίδρυση και τη λειτουργία της εσωτερικής αγοράς στην οποία, σύμφωνα με το άρθρο 7 Α της συνθήκης, εξασφαλίζεται η ελεύθερη κυκλοφορία εμπορευμάτων, προσώπων, υπηρεσιών και κεφαλαίων, απαιτείται όχι μόνο η δυνατότητα κυκλοφορίας των δεδομένων προσωπικού χαρακτήρα μεταξύ κρατών μελών αλλά και η προστασία των θεμελιωδών δικαιωμάτων του ατόμου ‘’ προκειμένου να ενισχυθεί η εμπιστοσύνη των πολιτών στην Κοινωνία της Πληροφορίας.

Γ) Η εν γένει αλλαγή στη σκέψη της Ευρωπαϊκής Κοινότητας και η στροφή της από μια καθαρά οικονομική ένωση σε μια πολιτική ένωση.

Στόχος της οδηγίας είναι η προστασία των δικαιωμάτων και των ελευθεριών των προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα, μέσω του

καθορισμού κατευθυντήριων αρχών που προσδιορίζουν τη νομιμότητα της επεξεργασίας αυτής. Οι αρχές αυτές αφορούν [4]:

i. **την ποιότητα των δεδομένων**. Τα δεδομένα προσωπικού χαρακτήρα πρέπει συγκεκριμένα να αποτελούν αντικείμενο θεμιτής και ρητής επεξεργασίας και να συλλέγονται για καθορισμένους, σαφείς και νόμιμους σκοπούς. Θα πρέπει εξάλλου να είναι ακριβή και, αν χρειάζεται, ενημερωμένα. Εισάγεται ‘’η αρχή της αναλογικότητας’’ ως προς την επεξεργασία με βάση την οποία τα δεδομένα που συλλέγονται πρέπει να είναι συναφή, πρόσφορα και όχι περισσότερα από ότι κάθε φορά είναι απαραίτητο για την εκπλήρωση του σκοπού της επεξεργασίας. Τέλος, η επεξεργασία των δεδομένων θα πρέπει να περιορίζεται στο ελάχιστο επιτρεπτό χρονικό διάστημα που απαιτείται.

ii. **τη νόμιμη επεξεργασία των δεδομένων**. Η επεξεργασία δεδομένων προσωπικού χαρακτήρα δεν μπορεί να γίνεται παρά αν το υποκείμενο των δεδομένων έχει κατά τρόπο αναμφισβήτητο δώσει τη συναίνεσή του ή αν η επεξεργασία είναι απαραίτητη.
   - για την εκτέλεση σύμβασης της οποίας το υποκείμενο των δεδομένων αποτελεί συμβαλλόμενο μέρος,
   - για την τήρηση νομικής υποχρέωσης στην οποία υπόκειται ο υπεύθυνος της επεξεργασίας,
   - για τη διαφύλαξη ζωτικού συμφέροντος του υποκείμενου των δεδομένων,
   - για την εκτέλεση αποστολής δημόσιου συμφέροντος,
   - για την υλοποίηση του θεμιτού συμφέροντος που επιδιώκεται από τον υπεύθυνο της επεξεργασίας.

iii. **την ενημέρωση** των ενδιαφερόμενων προσώπων σχετικά με την επεξεργασία δεδομένων: ορισμένες πληροφορίες (ταυτότητα του υπεύθυνου της επεξεργασίας, σκοπιμότητες της επεξεργασίας, παραλήπτες των δεδομένων ή οποιαδήποτε πληροφορία όπως τους αποδέκτες των πληροφοριών, το κατά πόσο η συλλογή είναι υποχρεωτική ή όχι καθώς και τις συνέπειες της άρνησης παροχής των δεδομένων) θα πρέπει να παρέχονται από τον υπεύθυνο της επεξεργασίας στο πρόσωπο για το οποίο συλλέγει δεδομένα που το αφορούν (άρθρο 10)

iv. **το δικαίωμα πρόσβασης** των προσώπων αυτών στα δεδομένα που τα αφορούν. Κάθε σχετικό πρόσωπο θα πρέπει να έχει το δικαίωμα να επιτύχει από τον υπεύθυνο της επεξεργασίας:
   - την επιβεβαίωση ότι υπάρχει ή όχι επεξεργασία δεδομένων που τα αφορούν καθώς και πληροφορίες, σχετικά τουλάχιστον με τους σκοπούς της επεξεργασίας, τις κατηγορίες δεδομένων υπό επεξεργασία, τους αποδέκτες ή τις κατηγορίες αποδεκτών στις οποίες ανακοινώνονται τα δεδομένα αυτά,
   - τη γνωστοποίηση, με εύληπτο τρόπο, των δεδομένων υπό επεξεργασία καθώς και των διαθέσιμων πληροφοριών σχετικά με την προέλευσή των,
   - την ενημέρωση σχετικά με τη λογική στην οποία στηρίζεται κάθε αυτοματοποιημένη επεξεργασία των δεδομένων τα οποία αναφέρονται στα πρόσωπα αυτά, τουλάχιστον στην περίπτωση των αυτοματοποιημένων αποφάσεων του άρθρου 15,
   - τη διόρθωση, τη διαγραφή ή το κλείδωμα των δεδομένων των οποίων η επεξεργασία δεν είναι σύμφωνη προς τις διατάξεις της παρούσας οδηγίας, ιδίως λόγω ελλιπούς ή ανακριβούς χαρακτήρα των δεδομένων, την κοινοποίηση σε τρίτους, στους οποίους δεν έχουν ανακοινωθεί τα δεδομένα. Κάθε διόρθωσης, διαγραφής ή κλειδώματος που διενεργείται εφόσον τούτο δεν είναι αδύνατον ή δεν προϋποθέτει δυσανάλογες προσπάθειες (άρθρο 12).

v. **τις εξαιρέσεις και τους περιορισμούς**: Η πληροφόρηση του υποκειμένου των δεδομένων, το δικαίωμα πρόσβασης και τη δημοσιότητα των επεξεργασιών μπορούν να έχουν περιορισμένη εμβέλεια ώστε να διαφυλαχθεί, μεταξύ άλλων, η κρατική ασφάλεια, η άμυνα, η δημόσια ασφάλεια, η επιδίωξη ποινικών παραβάσεων, ένα οικονομικό ή δημοσιονομικό σημαντικό συμφέρον ενός κράτους μέλους ή της ΕΕ ή η προστασία του εν λόγω

προσώπου. Τις εξαιρέσεις αυτές μπορούν τα κράτη-μέλη να τις εισάγουν με νομοθετικά μέτρα.

vi. **το δικαίωμα αντίταξης** στην επεξεργασία δεδομένων: Σύμφωνα με το άρθρο 14, το υποκείμενο των δεδομένων θα πρέπει να έχει το δικαίωμα να αντιταχθεί στην επεξεργασία δεδομένων που το αφορούν ‘’ για επιτακτικούς και νόμιμους λόγους σχετικούς με την προσωπική του κατάσταση... Σε περίπτωση αιτιολογημένης αντίταξης, η επεξεργασία δεν μπορεί πλέον να αφορά τα δεδομένα αυτά ’’. Θα πρέπει επίσης να δύναται να αντιταχθεί, εφόσον το ζητήσει και δωρεάν, στην επεξεργασία των δεδομένων προσωπικού χαρακτήρα την οποία προτίθεται να πραγματοποιήσει ο υπεύθυνος επεξεργασίας και σχετίζεται με δραστηριότητες για την προώθηση προϊόντων ή να ενημερώνεται πριν από την πρώτη ανακοίνωση των δεδομένων προσωπικού χαρακτήρα σε τρίτους ή τη χρησιμοποίησή τους για λογαριασμό τρίτων με σκοπό τη διεξαγωγή έρευνας μέσω του ταχυδρομείου και να του παρέχεται ρητά το δικαίωμα να αντιταχθεί δωρεάν πριν από την ανακοίνωση ή τη χρησιμοποίηση.

vii. **την εμπιστευτικότητα και την ασφάλεια της επεξεργασίας**: Κάθε πρόσωπο που ενεργεί υπό την εξουσία του υπευθύνου της επεξεργασίας ή εκείνη υπεργολάβου, καθώς και ο ίδιος ο υπεργολάβος, που έχει πρόσβαση σε προσωπικά δεδομένα, δεν δύναται να τα επεξεργαστεί παρά κατόπιν εντολής του υπευθύνου επεξεργασίας. Εξάλλου, ο υπεύθυνος της επεξεργασίας θα πρέπει να εφαρμόζει τα ενδεδειγμένα μέτρα για την προστασία των δεδομένων προσωπικού χαρακτήρα έναντι τυχαίας ή παράνομης καταστροφής, τυχαίας απώλειας, αλλοίωσης, διάδοσης ή πρόσβασης χωρίς άδεια.

viii. **την κοινοποίηση των αποτελεσμάτων της επεξεργασίας σε ελεγκτική αρχή**: Ο υπεύθυνος επεξεργασίας οφείλει να απευθύνει κοινοποίηση στην αρμόδια ελεγκτική αρχή πριν από την εκτέλεση μιας επεξεργασίας. Προηγούμενες εξετάσεις ως προς τους ενδεχόμενους κινδύνους έναντι των δικαιωμάτων και ελευθεριών των υπόψη προσώπων θα πρέπει να γίνονται από την ελεγκτική αρχή μέχρι τη λήψη της κοινοποίησης. Η δημοσιότητα των αποτελεσμάτων της επεξεργασίας θα πρέπει να διασφαλίζεται και οι ελεγκτικές αρχές οφείλουν να τηρούν μητρώο των κοινοποιημένων αποτελεσμάτων επεξεργασίας. Από την υποχρέωση κοινοποίησης εξαιρούνται α) οι κατηγορίες των επεξεργασιών που δεν δύνανται να θίξουν δικαιώματα και ελευθερίες και β) εφόσον ο υπεύθυνος της επεξεργασίας ορίζει, σύμφωνα με το εθνικό δίκαιο στο οποίο υπόκειται, έναν υπεύθυνο για την προστασία των δεδομένων προσωπικού χαρακτήρα ο οποίος έχει κυρίως ως αποστολή να διασφαλίζει κατ’ ανεξάρτητο τρόπο, την εσωτερική εφαρμογή των εθνικών διατάξεων που θεσπίζονται κατ' εφαρμογή της οδηγίας και να τηρεί μητρώο των επεξεργασιών που εκτελούνται από τον υπεύθυνο της επεξεργασίας.

Κάθε πρόσωπο θα πρέπει να έχει τη δυνατότητα νομικής προσφυγής στην περίπτωση παραβίασης των δικαιωμάτων που εγγυώνται οι εθνικές διατάξεις οι οποίες ισχύουν για τη σχετική επεξεργασία δεδομένων. Εξάλλου, τα άτομα που έχουν υποστεί βλάβη λόγω μιας παράνομης επεξεργασίας των προσωπικών τους δεδομένων έχουν το δικαίωμα να επιτύχουν αποκατάσταση της ζημίας που υπέστησαν (κεφ. 3, άρθρα 22,23,24).

Επιτρέπονται οι μεταβιβάσεις δεδομένων προσωπικού χαρακτήρα από κράτος μέλος σε τρίτη χώρα, υπό την προϋπόθεση ότι η εν λόγω τρίτη χώρα διαθέτει το κατάλληλο επίπεδο προστασίας. Αντίθετα, οι εν λόγω μεταβιβάσεις δεν μπορούν να πραγματοποιηθούν προς τρίτες χώρες οι οποίες δεν διαθέτουν το κατάλληλο επίπεδο προστασίας, εκτός από συγκεκριμένες περιπτώσεις παρέκκλισης οι οποίες απαριθμούνται περιοριστικά (άρθρα 25,26).

Η οδηγία αποσκοπεί στο να διευκολύνει την εκπόνηση κωδίκων εθνικής και κοινοτικής συμπεριφοράς, οι οποίοι θα συμβάλουν στην ομαλή εφαρμογή των κοινοτικών και εθνικών διατάξεων (άρθρο 27).

Κάθε κράτος μέλος υποχρεούται στην ίδρυση μίας ή περισσότερων ανεξάρτητων κρατικών αρχών οι οποίες επιφορτίζονται με την εποπτεία της εφαρμογής, στο εθνικό έδαφος, των ληφθέντων από τα κράτη μέλη μέτρων κατ' εφαρμογή της οδηγίας και ‘’με πλήρη ανεξαρτησία’’ (άρθρο 28).Δημιουργείται, επίσης, μια ομάδα προστασίας των προσώπων έναντι

της επεξεργασίας δεδομένων προσωπικού χαρακτήρα, στην οποία συμμετέχουν εκπρόσωποι των εθνικών αρχών ελέγχου, εκπρόσωποι των ελεγκτικών αρχών των κοινοτικών θεσμικών οργάνων και οργανισμών και ένας εκπρόσωπος της Επιτροπής. Η ομάδα αυτή έχει ευρείες ελεγκτικές αρμοδιότητες (‘’ δικαίωμα να έχει πρόσβαση στα δεδομένα που αποτελούν αντικείμενο επεξεργασίας και το δικαίωμα να συλλέγει κάθε αναγκαία πληροφορία για την εκπλήρωση της αποστολής ελέγχου’’), έχει αποτελεσματικές εξουσίες παρέμβασης (‘’ την εξουσία να διατυπώνει γνώμες πριν από την εκτέλεση των επεξεργασιών... να διασφαλίζει την κατάλληλη δημοσιότητα των γνωμών αυτών, την εξουσία να επιτάσσει τη δέσμευση, διαγραφή ή την καταστροφή δεδομένων, να απαγορεύει επίσης προσωρινά ή οριστικά την επεξεργασία, να απευθύνει προειδοποίηση ή επίπληξη προς τον υπεύθυνο για την επεξεργασία ή να προσφεύγει στα εθνικά κοινοβούλια ή άλλα εθνικά πολιτικά όργανα) και τέλος, έχει την εξουσία να παρίσταται ενώπιον του δικαστηρίου σε περίπτωση παράβασης των εθνικών διατάξεων.

2.1.**2 Κοινοτική Οδηγία 97/66/ΕΚ**

Οι νέες ψηφιακές τεχνολογίες που εισάγονται στα δημόσια τηλεπικοινωνιακά δίκτυα και οι οποίες δημιουργούν ειδικές απαιτήσεις όσον αφορά την προστασία των δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής του χρήστη, ωθούν την Ευρωπαϊκή Κοινότητα να εκδώσει την οδηγία 97/66 [4] προκειμένου να εναρμονίσει τις διατάξεις των κρατών-μελών και να διασφαλίσει ένα ισοδύναμο επίπεδο προστασίας των θεμελιωδών δικαιωμάτων και ελευθεριών όσον αφορά την επεξεργασία δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα. Η οδηγία αυτή εγκρίθηκε από το Ευρωπαϊκό κοινοβούλιο στις 15 Δεκεμβρίου 1997 και έπρεπε να μεταφερθεί στο εθνικό δίκαιο των κρατών-μελών το αργότερο μέχρι τις 24 Οκτωβρίου 1998. Είναι συμπληρωματική της οδηγίας 95/46 και αρχικά αφορούσε την εγκατάσταση ψηφιακού δικτύου ενοποιημένων υπηρεσιών (ISDN). Συγκεκριμένα, οι βασικές της διατάξεις αφορούσαν τους ακόλουθους θεματικούς τομείς:

- την ασφάλεια των υπηρεσιών και των δικτύων
- το απόρρητο των επικοινωνιών
- τα δεδομένα σχετικά με την κίνηση και τη χρέωση
- το δικαίωμα της μη αναλυτικής χρέωσης, την αναγραφή ταυτότητας της καλούσας και της συνδεδεμένης κλήσης καθώς και τον περιορισμό αυτής της δυνατότητας.
- την αυτόματη προώθηση κλήσεων
- αναγραφή των στοιχείων στους τηλεφωνικούς καταλόγους των συνδρομητών τις μη ζητηθείσες κλήσεις που έχοθν σκοπό την απευθείας εμπορική προώθηση.

Κάτι που θα πρέπει επίσης να επισημανθεί είναι ότι στο προστατευτικό πεδίο της οδηγίας , εντάσσονταν, επιπλέον των θεμελιωδών δικαιωμάτων των φυσικών προσώπων, και τα έννομα συμφέροντα των νομικών προσώπων ‘’ ιδίως έναντι των αυξανομένων κινδύνων που απορρέουν από την αυτόματη αποθήκευση και επεξεργασία δεδομένων που αφορούν συνδρομητές και χρήστες’’ και αυτό γιατί κρίθηκε, ότι προϋπόθεση για την εύρυθμη λειτουργία αρκετών νομικών προσώπων, ιδίως εμπορικών, είναι η ασφάλεια και το απόρρητο των επικοινωνιών τους.

Η οδηγία αυτή σύντομα αντικαταστάθηκε από την οδηγία 2002/58/ΕΚ που εγκρίθηκε στις 12 Ιουλίου 2002 και αφορούσε την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών.

2.1.**3 Κοινοτική Οδηγία 2002/58/ΕΚ**

Είναι ενδεικτικό ότι στο προοίμιο της συγκεκριμένης οδηγίας [4] αναφέρεται ρητώς ότι ‘’η οδηγία 97/66/ΕΚ πρέπει να προσαρμοστεί στις εξελίξεις των αγορών και των τεχνολογιών των υπηρεσιών των ηλεκτρονικών επικοινωνιών, προκειμένου να παρέχει το ίδιο επίπεδο προστασίας των προσωπικών δεδομένων και της ιδιωτικής ζωής σε όλους τους χρήστες υπηρεσιών επικοινωνιών διαθέσιμων στο κοινό, ανεξάρτητα από τις χρησιμοποιούμενες τεχνολογίες. Η εν λόγω οδηγία θα πρέπει, ως εκ τούτου, να καταργηθεί και να αντικατασταθεί από την παρούσα.’’ Σκοπός της είναι η διασφάλιση ενός ισοδύναμου επιπέδου προστασίας των θεμελιωδών δικαιωμάτων και ελευθεριών , έτσι ώστε να διασφαλίζεται η ελεύθερη ροή δεδομένων στην κοινότητα. (προοίμιο, άρθρο 5).

Έχει γίνει αντιληπτό, ότι για την διασυνοριακή ανάπτυξη νέων ψηφιακών τεχνολογιών, θα πρέπει να παρέχεται η ασφάλεια στους χρήστες ότι δεν τίθεται εν κινδύνω η ασφάλεια των δεδομένων τους. Τα ενδιαφερόμενα, λοιπόν, κράτη-μέλη, οι χρήστες και οι προμηθευτές, καθώς και οι κοινοτικοί οργανισμοί θα πρέπει να συνεργάζονται ώστε να ελαχιστοποιούν την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και όπου είναι δυνατόν να κάνουν χρήση ανώνυμων ή ψευδώνυμων δεδομένων. Στον τομέα των ηλεκτρονικών επικοινωνιών εφαρμόζονται οι διατάξεις της οδηγίας 95/46/ΕΚ ενώ και οι δύο οδηγίες δεν υπεισέρχονται σε θέματα προστασίας θεμελιωδών δικαιωμάτων που δεν διέπονται από το κοινοτικό δίκαιο. Δεν θίγουν, λοιπόν, τη δυνατότητα των κρατών-μελών να προβαίνουν σε νόμιμη παρακολούθηση όταν αυτό είναι αναγκαίο για λόγους δημόσιας ασφάλειας, εθνικής άμυνας και της ασφάλειας του κράτους (συμπεριλαμβανομένης και της οικονομικής ευμάρειας).

Η νέα αυτή οδηγία εκδόθηκε κυρίως για την αντιμετώπιση 2 παραγόντων. Ο πρώτος αφορούσε την ανάπτυξη κατασκοπευτικού λογισμικού, το οποίο μπορεί να εισέλθει στο τερματικό του χρήστη εν αγνοία του με σκοπό την πρόσβαση σε πληροφορίες και συνιστά ενδεχόμενη σοβαρή παραβίαση της προσωπικής ζωής του χρήστη. Η χρησιμοποίηση τέτοιων λογισμικών θα πρέπει να επιτρέπεται μόνο για θεμιτούς σκοπούς και πάντα με τη σύμφωνη γνώμη του υποκειμένου των δεδομένων. Λογισμικά που μπορούν να χρησιμοποιηθούν για θεμιτούς σκοπούς αποτελούν και τα λεγόμενα ‘’cookies’’, τα οποία χρησιμοποιούνται για παράδειγμα για την ανάλυση της αποτελεσματικότητας του σχεδιασμού και της παρουσίασης μιας ιστοσελίδας και τον έλεγχο της ταυτότητας των χρηστών που πραγματοποιούν συναλλαγές on-line. Ακόμα και σ’ αυτήν την περίπτωση, όμως, οι χρήστες πρέπει να έχουν τη δυνατότητα να αρνηθούν την εγκατάσταση ενός cookie στο τερματικό τους.

Ο δεύτερος παράγοντας αφορούσε τις αυτόκλητες κλήσεις με σκοπό την εμπορική προώθηση μέσω αυτοματοποιημένων συστημάτων κλήσης, fax, ηλεκτρονικού ταχυδρομείου και σύντομων μηνυμάτων (SMS). Επειδή σε ορισμένες περιπτώσεις μπορεί να επιβάλλουν κάποια δαπάνη στο χρήστη ή να προξενήσουν δυσχέρειες στα δίκτυα και στον τερματικό εξοπλισμό, είναι απαραίτητη η εκ των προτέρων ρητή συγκατάθεση των αποδεκτών. Η ενιαία αγορά απαιτεί εναρμονισμένη προσέγγιση ώστε να εξασφαλίζονται απλοί κανόνες για επιχειρηματίες και χρήστες σε όλη την Κοινότητα.

- Επεξεργασία δεδομένων κίνησης (άρθρο 6):

Ως δεδομένα κίνησης νοούνται τα δεδομένα που υποβάλλονται σε επεξεργασία για τους σκοπούς της διαβίβασης μιας επικοινωνίας σε δίκτυο ηλεκτρονικών επικοινωνιών ή της χρέωσής της. Τα δεδομένα αυτά που αφορούν συνδρομητές και χρήστες θα πρέπει να απαλείφονται ή να καθίστανται ανώνυμα όταν δεν είναι πλέον απαραίτητα για το σκοπό μετάδοσης της επικοινωνίας. Τα δεδομένα που είναι απαραίτητα για την χρέωση των συνδρομητών μπορούν να υποβάλλονται σε επεξεργασία αφού πρώτα ο πάροχος έχει ενημερώσει το χρήστη σχετικά με τον τύπο των δεδομένων που υποβάλλονται σε επεξεργασία και μόνον όμως ως το τέλος της χρονικής περιόδου εντός της οποίας μπορεί να αμφισβητηθεί νομίμως ο λογαριασμός ή να επιδιωχθεί η πληρωμή. Όσον αφορά την εμπορική προώθηση των προϊόντων ή την παροχή υπηρεσιών προστιθέμενης αξίας, ο πάροχος δεν μπορεί να επεξεργάζεται τα δεδομένα χωρίς την συγκατάθεση του χρήστη. Τέλος, η επεξεργασία των δεδομένων κίνησης θα πρέπει να περιορίζεται σε πρόσωπα που ενεργούν υπό την εποπτεία του φορέα παροχής του δημοσίου δικτύου και της διαθέσιμης στο κοινό υπηρεσίας ηλεκτρονικών επικοινωνιών και ασχολούνται με τη διαχείριση της χρέωσης ή της κίνησης, τις απαντήσεις σε ερωτήσεις πελατών, την ανίχνευση της απάτης, την εμπορική προώθηση υπηρεσιών ηλεκτρονικών επικοινωνιών και φυσικά να περιορίζεται στα απολύτων αναγκαία για την εξυπηρέτηση των σκοπών αυτών.

- Επεξεργασία δεδομένων θέσης (άρθρο 9):

Ως δεδομένα θέσης νοούνται τα δεδομένα που υποβάλλονται σε επεξεργασία σε δίκτυο ηλεκτρονικών επικοινωνιών και που υποδεικνύουν τη γεωγραφική θέση του τερματικού εξοπλισμού του χρήστη μιας διαθέσιμης στο κοινό υπηρεσίας ηλεκτρονικών επικοινωνιών. Σε δίκτυα κινητής επικοινωνίας, τα δεδομένα θέσης μπορεί να μην χαρακτηρίζονται από μεγάλη

ακρίβεια, ενώ ακόμη μικρότερη είναι η ακρίβεια των δεδομένων θέσης στα δορυφορικά δίκτυα. Με την ανάπτυξη της τεχνολογίας υπάρχουν, πλέον, πολλοί τρόποι εντοπισμού της θέσης των ατόμων: αυτόματες μηχανές εισιτηρίων στον τομέα των μεταφορών, GPS, τραπεζικές κάρτες, κινητά τηλέφωνα. Σε αυτήν την περίπτωση τα δεδομένα είναι πολύ πιο ακριβή και υποβάλλονται σε ειδική επεξεργασία από το δίκτυο για το σκοπό της παροχής υπηρεσιών προστιθέμενης αξίας. Επειδή, όμως, τα δεδομένα αυτά σχετίζονται με ένα εντοπισθέν ή υπό εντοπισμό φυσικό πρόσωπο, η επεξεργασία τους αποτελεί ένα ιδιαίτερα ευαίσθητο θέμα που άπτεται του ζητήματος της ελευθερίας της ανώνυμης μετακίνησης. Υπό αυτό, λοιπόν, το πρίσμα, ορίζεται με σαφήνεια ότι η επεξεργασία επιτρέπεται μόνον με την ρητή συγκατάθεση των χρηστών/συνδρομητών για την απαιτούμενη έκταση και διάρκεια για την παροχή μιας υπηρεσίας προστιθέμενης αξίας. Ο φορέας θα ενημερώνει τους χρήστες/συνδρομητές σχετικά με τον τύπο των δεδομένων που υποβάλλονται σε επεξεργασία καθώς και τους σκοπούς και τη χρονική διάρκεια αυτής. Φυσικά, πρέπει να δίνεται στους χρήστες η δυνατότητα να ανακαλούν οποτεδήποτε τη συγκατάθεσή τους.

- Τηλεφωνικοί κατάλογοι συνδρομητών (άρθρο 12):

Τα δεδομένα προσωπικού χαρακτήρα που συλλέγονται εμπεριέχονται σε καταλόγους, έντυπους ή ηλεκτρονικούς, που διατίθενται στο κοινό ή μπορούν να αποκτηθούν μέσω υπηρεσιών πληροφοριών καταλόγου. Τα κράτη-μέλη, βέβαια, εξασφαλίζουν ότι οι συνδρομητές θα έχουν ενημερωθεί σχετικά με τους σκοπούς των καταλόγων προτού συμπεριληφθούν στους καταλόγους και φυσικά δωρεάν. Παράλληλα θα έχουν τη δυνατότητα να καθορίζουν ποια από τα δεδομένα τους θα περιλαμβάνονται σε αυτούς καθώς και τη δυνατότητα να επαληθεύουν, να διορθώνουν ή να αποσύρουν τα εν λόγω δεδομένα. Τέλος, τα κράτη έχουν τη δυνατότητα να απαιτήσουν πρόσθετη συγκατάθεση των συνδρομητών για χρήση για άλλο σκοπό δημοσίου καταλόγου πέραν της αναζήτησης των στοιχείων της επαφής.

- Αυτόκλητες κλήσεις (άρθρο 13):

Η αυτόκλητη επικοινωνία, κοινώς το spam, μπορεί να έχει τη μορφή αυτόκλητων τηλεφωνικών μηνυμάτων (voicemail), πολυμεσικών μηνυμάτων (MMS), μηνυμάτων τύπου pop-up διαφημιστικών πινακίδων σε δικτυακούς τόπους και τηλεοπτικές εκπομπές, μηνυμάτων τύπου spim (instant messages). Η χρησιμοποίηση αυτόματων συστημάτων κλήσης και επικοινωνίας για σκοπούς εμπορικής προώθησης, επιτρέπεται μόνο στην περίπτωση που οι συνδρομητές έχουν δώσει την συγκατάθεσή τους και εφόσον δεν συγκαλύπτουν ή αποκρύπτουν την ταυτότητα του αποστολέα ή αν παρέχουν έγκυρη διεύθυνση για αποστολή αιτήματος τερματισμού.

Η οδηγία 2002/58/ΕΚ επεκτείνει την ισχύ των διατάξεων της γενικής οδηγίας 95/46/ΕΚ, οι οποίες αφορούν την ένδικη προστασία και συμπεριλαμβάνει τα αποτελέσματα των εργασιών της ειδικής ομάδας εργασίας για την προστασία των προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα (που συστάθηκε δυνάμει του άρθρου 29 της οδηγίας 95/46/ΕΚ). Τέλος, ορίζει τη καταληκτική ημερομηνία κατά την οποία τα κράτη-μέλη θα πρέπει να ενσωματώσουν στο εθνικό τους δίκαιο τις αναγκαίες διατάξεις ώστε να συμμορφωθούν με την οδηγία (31 Οκτωβρίου 2003).

2.2 **Προστασία προσωπικών δεδομένων στην Ελλάδα**

Το ελληνικό σύνταγμα, καινοτομώντας σε σχέση με παλαιότερα συνταγματικά κείμενα, ενέταξε διάταξη για την προστασία του ιδιωτικού βίου (άρθρο 9 παρ.1) όπου ορίζεται ότι ‘’η οικογενειακή και ιδιωτική ζωή είναι απαραβίαστη’’. Δεν προβλέπει κανένα περιορισμό του απαραβίαστου, πάρα μόνο της κατοικίας και μόνο με παρουσία εκπροσώπων της δικαστικής εξουσίας. Φορέας του δικαιώματος είναι κάθε φυσικό πρόσωπο χωρίς να γίνεται διάκριση μεταξύ αλλοδαπών και Ελλήνων πολιτών. Η διάταξη δημιουργεί ένα τείχος προστασίας γύρω από το άτομο

απαγορεύοντας τις επεμβάσεις στον προσωπικό του χώρο είτε με παραδοσιακά είτε με σύγχρονα μέσα καταγραφής και επεξεργασίας των δεδομένων του (άρθρο 9Α).[1]

Το ελληνικό νομοθετικό πλαίσιο συμπληρώνεται, εκτός από τη συνταγματική ρύθμιση, και από το νόμο 2472/97 [6] για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Ο νόμος αυτός ενσωματώνει τις διατάξεις της οδηγίας 95/46/ΕΚ για την προστασία των ατόμων από την επεξεργασία των δεδομένων τους. Για τους σκοπούς του νόμου, νοούνται ως "Δεδομένα προσωπικού χαρακτήρα", κάθε πληροφορία που αναφέρεται στο υποκείμενο των δεδομένων. Δεν λογίζονται ως δεδομένα προσωπικού χαρακτήρα τα στατιστικής φύσεως συγκεντρωτικά στοιχεία, από τα οποία δεν μπορούν πλέον να προσδιορισθούν τα υποκείμενα των δεδομένων και ως "Ευαίσθητα δεδομένα", τα δεδομένα που αφορούν στη φυλετική ή εθνική προέλευση, στα πολιτικά φρονήματα, στις θρησκευτικές ή φιλοσοφικές πεποιθήσεις, στη συμμετοχή σε συνδικαλιστική οργάνωση, στην υγεία, στην κοινωνική πρόνοια και στην ερωτική ζωή, στα σχετικά με ποινικές διώξεις ή καταδίκες, καθώς και στη συμμετοχή σε συναφείς με τα ανωτέρω ενώσεις προσώπων.

Επεξεργασία δεδομένων προσωπικού επιτρέπεται μόνο όταν:

- Το υποκείμενο των δεδομένων έχει δώσει τη συγκατάθεσή του.
- Ο υπεύθυνος της επεξεργασίας οφείλει να συλλέγει τα δεδομένα κατά τρόπο θεμιτό και νόμιμο και για σαφώς καθορισμένους σκοπούς. Τα δεδομένα πρέπει να είναι ακριβή και όχι περισσότερα απ' όσα κάθε φορά χρειάζονται ενώ , επίσης, θα πρέπει να υποβάλλονται σε ενημέρωση και να διατηρούνται σε μορφή που επιτρέπει τον προσδιορισμό της ταυτότητας των υποκειμένων τους.
- Απαγορεύεται η συλλογή και η επεξεργασία ευαίσθητων δεδομένων.
- Αναγνωρίζονται δικαιώματα του υποκειμένου όπως το δικαίωμα ενημέρωσης, το δικαίωμα πρόσβασης στα δεδομένα που το αφορούν, το δικαίωμα αντίρρησης στην επεξεργασία των δεδομένων καθώς και το δικαίωμα δικαστικής προστασίας από αποφάσεις ή πράξεις που το θίγουν.

Το υποκείμενο των δεδομένων απολαμβάνει τα εξής δικαιώματα :

- Δικαίωμα ενημέρωσης (άρθρο 11):

Ο υπεύθυνος επεξεργασίας οφείλει να ενημερώνει το υποκείμενο της επεξεργασίας σχετικά με την ταυτότητά του, τους σκοπούς της επεξεργασίας, τους αποδέκτες και την ύπαρξη του δικαιώματος πρόσβασης. Επίσης, εάν τα δεδομένα πρόκειται να ανακοινωθούν σε τρίτους, το υποκείμενο πρέπει να ενημερωθεί πριν από αυτούς. Εξαίρεση αποτελεί η επεξεργασία που γίνεται για λόγους εθνικής ασφάλειας ή διακρίβωσης σοβαρών εγκλημάτων καθώς και όταν η συλλογή γίνεται αποκλειστικά για δημοσιογραφικούς σκοπούς και αφορά δημόσια πρόσωπα.

- Δικαίωμα πρόσβασης (άρθρο 12):

Το υποκείμενο έχει δικαίωμα να γνωρίζει τα δεδομένα που τον αφορούν και αποτέλεσαν αντικείμενο επεξεργασίας καθώς και να λαμβάνει από τον υπεύθυνο επεξεργασίας με τρόπο σαφή και εύληπτο πληροφορίες όπως τους σκοπούς της επεξεργασίας, την εξέλιξη της και τους αποδέκτες των αποτελεσμάτων της. Το δικαίωμα αυτό ασκείται με καταβολή χρηματικού ποσού, το οποίο επιστρέφεται στον αιτούντα αν το αίτημα της διαγραφής ή διόρθωσης των δεδομένων κριθεί βάσιμο. Σε αυτήν την περίπτωση, ο υπεύθυνος επεξεργασίας υποχρεούται να αποστείλει στον αιτούντα αντίγραφο του διορθωμένου μέρους της επεξεργασίας που τον αφορά.

- Δικαίωμα αντίρρησης (άρθρο 13):

Το υποκείμενο έχει δικαίωμα να προβάλλει αντιρρήσεις για την επεξεργασία των δεδομένων που το αφορούν. Οι αντιρρήσεις (οι οποίες πρέπει να περιέχουν αίτημα για συγκεκριμένη ενέργεια- διόρθωση, δέσμευση, διαγραφή, μη διαβίβαση) υποβάλλονται εγγράφως στον υπεύθυνο επεξεργασίας, ο οποίος υποχρεούται να απαντήσει εντός 15 ημερών και σε περίπτωση που δεν απαντήσει εμπρόθεσμα ή η απάντηση δεν ικανοποιήσει το υποκείμενο, τότε το τελευταίο έχει δικαίωμα να προσφύγει στην Αρχή. Τέλος, καθένας έχει δικαίωμα να δηλώσει ότι δεν επιθυμεί τα δεδομένα του να γίνουν αντικείμενα επεξεργασίας για λόγους

[1] Η ισχύς των δύο διατάξεων μπορεί να ανασταλεί κάτω από ειδικές συνθήκες (πόλεμος, επιστράτευση ή απειλή άμεσης εθνικής ασφάλειας) όπως ορίζει το άρθρο 48.

προώθησης αγαθών ή υπηρεσιών εξ αποστάσεως. Η Αρχή τηρεί αρχείο με τα στοιχεία των συγκεκριμένων υποκειμένων, το οποίο οι υπεύθυνοι επεξεργασίας έχουν υποχρέωση να συμβουλεύονται και να διαγράφουν από το αρχείο τους τα υποκείμενα αυτά.

- Δικαίωμα προσωρινής δικαστικής προστασίας (άρθρο 14):

Καθένας έχει δικαίωμα να ζητήσει από το αρμόδιο δικαστήριο την αναστολή ή μη εφαρμογή απόφασης που τον θίγει εφόσον αυτή ελήφθη με αποκλειστικά αυτοματοποιημένη επεξεργασία και εφόσον η επεξεργασία αυτή αποβλέπει στην αξιολόγηση της φερεγγυότητάς, της αξιοπιστίας του και εν γένει της προσωπικότητάς του. Το δικαίωμα αυτό υφίσταται ακόμα και όταν δεν συντρέχουν οι προϋποθέσεις της προσωρινής δικαστικής προστασίας.

2.2.1 **Νόμος** 3471/2006

Τροποποίηση του νόμου 2472 αποτελεί ο νόμος 3471/2006 [7], όπως αυτός ψηφίστηκε από τη Βουλή και εκδόθηκε στις 28.6.2006 (ΦΕΚ Α' 133) και ο οποίος ενσωματώνει στην ελληνική έννομη τάξη την οδηγία 2002/58/ΕΚ σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στο πλαίσιο της παροχής διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών σε δημόσια δίκτυα ηλεκτρονικών επικοινωνιών. Για την επεξεργασία δεδομένων προσωπικού χαρακτήρα που πραγματοποιείται στο πλαίσιο μη διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών, εφαρμόζεται ο ν. 2472/1997.

- Προστασία απορρήτου (άρθρο 4)

Οποιαδήποτε χρήση των υπηρεσιών ηλεκτρονικών επικοινωνιών που παρέχονται μέσω δημοσίου δικτύου επικοινωνιών και των διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών, καθώς και των συναφών δεδομένων κίνησης και θέσης, προστατεύεται από το απόρρητο των επικοινωνιών. Η άρση του απορρήτου είναι επιτρεπτή μόνο υπό τις προϋποθέσεις και τις διαδικασίες που προβλέπονται από το άρθρο 19 του Συντάγματος (λόγοι εθνικής ασφάλειας και διακρίβωση ορισμένων κακουργημάτων ενώ αίτηση για άρση του απορρήτου μπορεί να υποβάλλει μόνο δικαστική αρχή). Απαγορεύεται η ακρόαση, υποκλοπή, αποθήκευση ή άλλο είδος παρακολούθησης ή επιτήρησης των ηλεκτρονικών επικοινωνιών και των συναφών δεδομένων κίνησης και θέσης, εκτός αν προβλέπεται άλλως από το νόμο ενώ Επιτρέπεται η καταγραφή συνδιαλέξεων και των συναφών δεδομένων κίνησης, όταν πραγματοποιούνται κατά τη διάρκεια νόμιμης επαγγελματικής πρακτικής. Τέλος, επιτρέπεται η τεχνικής φύσεως αποθήκευση, η οποία είναι αναγκαία για τη διαβίβαση της επικοινωνίας (cookies) ενώ απαγορεύεται η εγκατάσταση κατασκοπευτικών λογισμικών (spyware).

- Κανόνες επεξεργασίας (άρθρο 5)

Η επεξεργασία των δεδομένων περιορίζεται στο απολύτως αναγκαίο μέτρο και επιτρέπεται μόνον έπειτα από ενημέρωση του χρήστη για το σκοπό της επεξεργασίας και τους αποδέκτες των αποτελεσμάτων καθώς και στην περίπτωση που η επεξεργασία είναι απαραίτητη για την εκτέλεση σύμβασης στην οποία ο χρήστης είναι μέρος. Η συγκατάθεση του χρήστη δίνεται με εγγράφως (είναι ανά πάσα στιγμή προσβάσιμη και μπορεί να ανακληθεί) και ο πάροχος της υπηρεσίας είναι υποχρεωμένος να εξασφαλίσει ότι ο χρήστης ενεργεί με πλήρη επίγνωση των συνεπειών. Τα δεδομένα κίνησης που υποβάλλονται σε επεξεργασία με τη λήξη της επικοινωνίας πρέπει να καταστρέφονται ή να καθίστανται ανώνυμα. Υποβάλλονται σε επεξεργασία μόνον εφόσον είναι αναγκαίο για την χρέωση των συνδρομητών. Τα δεδομένα θέσης μπορούν να υποστούν επεξεργασία με την παροχή υπηρεσίας προστιθέμενης αξίας μόνον εφόσον καθίστανται ανώνυμα με την κατάλληλη κωδικοποίηση (ή ρητή συγκατάθεση του χρήστη) στην απαιτούμενη έκταση και χρονική διάρκεια.

- Ασφάλεια (άρθρο 12)

Ο πάροχος των υπηρεσιών είναι υποχρεωμένος να λαμβάνει όλα τα απαραίτητα μέτρα για την ασφάλεια των υπηρεσιών του καθώς και του δημόσιου δικτύου και αν υπάρχει κίνδυνος παραβίασης της ασφάλειας θα πρέπει να ενημερώνει τους συνδρομητές.

2.2.2 Η Αρχή Προστασίας Προσωπικών Δεδομένων

Το 1997 με το νόμο 2472 ιδρύεται στην Ελλάδα η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ). Αποστολή της Αρχής αποτελεί η προστασία των δικαιωμάτων της προσωπικότητας και της ιδιωτικής ζωής του ατόμου στην Ελλάδα, σύμφωνα με τις διατάξεις των Ν. 2472/1997 και 3471/2006.Πρωταρχικός σκοπός της Αρχής είναι η προστασία του πολίτη από την παράνομη επεξεργασία των προσωπικών του δεδομένων αλλά και η συνδρομή προς αυτόν σε κάθε περίπτωση που διαπιστώνεται παραβίαση των σχετικών δικαιωμάτων του σε κάθε επιχειρησιακό τομέα (χρηματοπιστωτικά, υγεία, ασφάλιση, εκπαίδευση, δημόσια διοίκηση, μεταφορές, ΜΜΕ, κοκ). Επίσης, σκοπός της Αρχής είναι η υποστήριξη και καθοδήγηση των υπεύθυνων επεξεργασίας στην εκπλήρωση των υποχρεώσεων τους απέναντι στο νόμο, λαμβάνοντας υπόψη τις νέες ανάγκες υπηρεσιών της ελληνικής κοινωνίας, καθώς και την διείσδυση των σύγχρονων ψηφιακών επικοινωνιών και δικτύων. Ως εκ τούτου, η Αρχή στρέφει ιδιαίτερα την προσοχή της μεταξύ άλλων στην παρατήρηση και αντιμετώπιση ζητημάτων που προκύπτουν με την εξέλιξη των νέων τεχνολογιών και εφαρμογών.

Οι αρμοδιότητές της μπορούν να ομαδοποιηθούν σε 3 τομείς:

- Διοιητικές-ελεγκτικές

Οι υπεύθυνοι επεξεργασίας υποχρεούνται να υποβάλλουν γνωστοποίηση προς την Αρχή όσον αφορά στη σύσταση και λειτουργία αρχείου και η Αρχή εκδίδει άδειες για τη συλλογή και επεξεργασία δεδομένων προσωπικού χαρακτήρα, για τη διαβίβαση δεδομένων σε χώρες εκτός Ε.Ε. ή/και για τη διασύνδεση δεδομένων, οι οποίες χορηγούνται με συγκεκριμένους όρους και προϋποθέσεις. Η Αρχή ενεργεί αυτεπαγγέλτως ή κατόπιν καταγγελίας διοικητικούς ελέγχους σε αρχεία, τόσο του δημόσιου όσο και του ιδιωτικού τομέα με δικαίωμα πρόσβασης σε κάθε αρχείο χωρίς να μπορεί να αντιταχθεί κανενός είδους απόρρητο. Τέλος, εξετάζει παράπονα και ερωτήματα σχετικά με την εφαρμογή του νόμου και την προστασία των δικαιωμάτων των αιτούντων όταν αυτά θίγονται από την επεξεργασία δεδομένων και εκδίδει σχετικές Αποφάσεις. Επίσης, επιβάλλει στους υπεύθυνους επεξεργασίας ή στους τυχόν εκπροσώπους τους διοικητικές κυρώσεις, για παράβαση των υποχρεώσεών τους που απορρέουν από τον νόμο 2472/97 και από κάθε άλλη ρύθμιση που αφορά την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Τέλος, η Αρχή μπορεί να καταγγέλλει τις παραβάσεις των διατάξεων του νόμου στις αρμόδιες διοικητικές και δικαστικές αρχές.

- Κανονιστικές-συμβουλευτικές.

Η Αρχή εκδίδει Κανονιστικές πράξεις για τη ρύθμιση ειδικών, τεχνικών και λεπτομερειακών θεμάτων. Επίσης, απευθύνει συστάσεις και υποδείξεις στους υπεύθυνους επεξεργασίας ή τους τυχόν εκπροσώπους τους και δίδει κατά την κρίση της δημοσιότητα σε αυτές, και υποστηρίζει τα επαγγελματικά σωματεία και λοιπές ενώσεις φυσικών ή νομικών προσώπων που διατηρούν αρχεία στην κατάρτιση κωδίκων δεοντολογίας σχετικά με την προστασία δεδομένων προσωπικού χαρακτήρα. Τέλος, η Αρχή γνωμοδοτεί για κάθε ρύθμιση που αφορά στην επεξεργασία και προστασία δεδομένων προσωπικού χαρακτήρα.

- Απολογισμού δημοσιοποίησης συνεργασιών.

Οι κύριοι επικοινωνιακοί της στόχοι αφορούν την ενημέρωση και την ευαισθητοποίηση των υποκειμένων των δεδομένων καθώς και των υπεύθυνων επεξεργασίας ως προς τα δικαιώματα και τις υποχρεώσεις τους. Προς τούτο η Αρχή:

- Συντάσσει κάθε χρόνο έκθεση για την εκτέλεση της αποστολής της κατά το προηγούμενο ημερολογιακό έτος.
- Ανακοινώνει στη Βουλή παραβάσεις των ρυθμίσεων που αφορούν στην προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα.

- Συνεργάζεται με αντίστοιχες αρχές άλλων κρατών μελών της Ευρωπαϊκής Ένωσης και του Συμβουλίου της Ευρώπης σε ζητήματα σχετικά με την άσκηση των αρμοδιοτήτων της.

2.3 Προστασία προσωπικών δεδομένων σε άλλες χώρες

2.3.1 ΗΠΑ

Η ιδιωτικότητα δεν αναφέρεται ρητά στην Διακήρυξη των Δικαιωμάτων του Αμερικανικού Συντάγματος, αλλά στην Πρώτη και Τέταρτη Τροποποίηση. Στην Πρώτη Τροποποίηση εξασφαλίζεται η ελευθερία της θρησκείας, του λόγου, του τύπου και του συνέρχεσθαι, ενώ στην Τέταρτη αναφέρεται ότι το δικαίωμα του ατόμου να αισθάνεται ασφαλές στην προσωπική του ζωή και στο σπίτι του καθώς και η προστασία του έναντι αναίτιων ερευνών και κατασχέσεων, θα πρέπει να εξασφαλίζεται. Ο όρος ''προσωπικές πληροφορίες'' δεν αναφέρεται και γι' αυτό αυτές δεν προστατεύονται από τη Διακήρυξη των Δικαιωμάτων. Η Ένατη Τροποποίηση δηλώνει ότι ακόμα και αν ένα δικαίωμα δεν αναφέρεται ρητά στο Σύνταγμα δεν σημαίνει ότι η κυβέρνηση μπορεί να παραβιάζει το δικαίωμα αυτό.

Η προστασία της ιδιωτικής ζωής ρυθμίζεται από την Πράξη για τη Ιδιωτικότητα (Privacy Act) [8] το 1974. Η πράξη αυτή ψηφίστηκε από το Κογκρέσο ως απάντηση στη βάση δεδομένων που διατηρούσε κρυφά το FBI για αντιπάλους στον πόλεμο του Βιετνάμ. Τα αρχεία αυτά περιείχαν πληροφορίες για ακτιβιστές, διασημότητες ακόμα και πολίτες που δεν είχαν διαπράξει κανένα αδίκημα. Σκοπός, λοιπόν, της πράξης ήταν να περιορίσει τα δεδομένα των κυβερνητικών αρχείων. Το κοινό είχε το δικαίωμα να μάθει τι πληροφορίες περιείχαν τα αρχεία καθώς και να έχει τη δυνατότητα να διορθώσει ανακριβείς πληροφορίες καθώς επίσης και κανένα στοιχείο δεν επιτρέπεται να αποκαλύπτεται σε τρίτους χωρίς τη συγκατάθεση του υποκειμένου των δεδομένων. Η πράξη του 1974 περιείχε αδυναμίες, οι οποίες προκειμένου να ξεπεραστούν, ψηφίστηκε από το κογκρέσο το 1988 νόμος σύμφωνα με τον οποίο οι κυβερνητικές υπηρεσίες είναι υποχρεωμένες να επανεξετάζουν την διαδικασία που ακολουθήθηκε προτού προβούν σε οποιαδήποτε διασταύρωση στοιχείων.

Η επίθεση της 11ης Σεπτεμβρίου άλλαξε εντελώς τις ιδέες περί κρυπτογραφίας και οδήγησε στην Πράξη Πατριωτισμού (Patriot Act), η οποία αποδυνάμωσε την προστασία των πολιτών απέναντι στις υποκλοπές. Οι υπηρεσίες επιβολής του νόμου έχουν πλέον τη δυνατότητα να καταγράφουν τους υπόπτους με μία μόνο δικαστική εντολή και η οποία ισχύει σε όλες της πολιτείες της χώρας.

Τέλος, άλλα νομοθετήματα σχετικά με την προστασία της ιδιωτικότητας είναι και το Family Educational Right and Privacy Act του 1974 (εγγυάται στους σπουδαστές και στους γονείς τους πρόσβαση στα αρχεία σπουδαστών), το Right to Financial Privacy Act του 1978 (σχετικά με την προστασία της ιδιωτικότητας στα τραπεζικά αρχεία) και τέλος το Electronic Funds Transfer Act του 1980 (που ορίζει ότι οι πελάτες θα πρέπει να ειδοποιούνται σε περίπτωση πρόσβασης του λογαριασμού τους από τρίτους).

2.3.2 Κίνα

Από το 1980, σύμφωνα με το κινεζικό Σύνταγμα και άλλα νομοθετήματα, οι κινέζοι πολίτες απολαμβάνουν το δικαίωμα της προστασίας της ιδιωτικότητας. Παρόλα αυτά, όμως, λόγω της εξουσίας της κυβέρνησης αλλά και της γενικής απροθυμίας για δικαστικές αντιπαραθέσεις οι νόμοι δεν έχουν εφαρμοστεί σε μεγάλο βαθμό.

Το άρθρο 38 του Συντάγματος αναγνωρίζει το δικαίωμα στην αξιοπρέπεια στους κατοίκους της Λαϊκής Δημοκρατίας της Κίνας και το άρθρο 40 ορίζει τους περιορισμούς αυτού του δικαιώματος: η προστασία κρατικών μυστικών και η έρευνα για κακουργήματα δίνει το δικαίωμα στις κυβερνητικές υπηρεσίες να υποκλέψουν συνομιλίες, αν αυτό κριθεί απαραίτητο. Ειδικά ο όρος ''κρατικά μυστικά'' μπορεί να επεκταθεί και να δώσει στην κυβέρνηση τη δυνατότητα υποκλοπής συνομιλιών.

Πρέπει να επισημανθεί ότι αναγνωρίζεται το δικαίωμα της αξιοπρέπειας και της προστασίας της φήμης. Το Ανώτατο, όμως, δικαστήριο δεν αναγνωρίζει την ιδιωτικότητα σαν ξεχωριστό δικαίωμα. Αυτό σημαίνει, ότι μια δράση μπορεί να θεωρηθεί σαν παραβίαση της ιδιωτικής ζωής μόνον εάν η φήμη του ενάγοντος έχει επίσης παραβιαστεί ή επηρεαστεί.

Οι Αρχές μπορούν, χωρίς καμία δικαστική εντολή, να υποκλέπτουν συνομιλίες (τηλεφωνικές και διαδικτυακές) καθώς και e-mails, εγχώρια και διεθνή, τα οποία έχουν το δικαίωμα να ανοίγουν, να διαβάζουν και να λογοκρίνουν. Οι υπηρεσίες ασφαλείας ελέγχουν την επικοινωνία στη χώρα (εισερχόμενη και εξερχόμενη) σε βαθμό που η επικοινωνία μεταξύ των κατοίκων της χώρας και του υπόλοιπου κόσμου να περιορίζεται. Η κίνηση αυτή, περνά μέσα από φίλτρα, τα οποία ενημερώνονται δυναμικά, καταγράφουν και παρακολουθούν forums ακόμα και σε πραγματικό χρόνο. Όλες οι διεθνείς συνδέσεις περνάνε μέσα από proxy servers, το οποίο ονομάζεται ‘’Great Firewall’’. Βέβαια, η αυξανόμενη χρήση του Internet στην Κίνα το καθιστά ανεπαρκές να ελέγξει όλη την κίνηση. Η σκέψη, λοιπόν, είναι να αναπτυχθεί μια έξυπνη τεχνική παρακολούθησης (Golden Shield) [8] μέσα στο δίκτυο της χώρας και η οποία θα παρακολουθεί όλη την επικοινωνία και αντί να την φιλτράρει, θα εγκατασταθεί σε ιδιωτικούς και δημόσιους χώρους. Αυτή η τεχνολογία είναι παρόμοια με το σύστημα Carnivore με τη διαφορά ότι αντί να συνδέεται με έναν διακομιστή, θα συλλέγει τις πληροφορίες απευθείας από τους ιδιωτικούς χώρους των ατόμων.

Το 2000 κατατέθηκε η διάταξη σχετικά με τις υπηρεσίες Διαδικτύου και σύμφωνα με την οποία απαιτείται από όλους τους παρόχους η καταγραφή των περιεχομένων των chat rooms, forums και ιστοσελίδων. Τα περιεχόμενα αυτά καθώς και οι πληροφορίες για το άτομο που ανήρτησε ένα μήνυμα θα πρέπει να φυλάσσονται το λιγότερο για 60 μέρες. Αν λάβεις mail εναντίον της κινεζικής κυβέρνησης δεν στοιχειοθετεί έγκλημα. Αν, όμως, προωθήσεις το μήνυμα τότε διαπράττεται έγκλημα και το άτομο απειλείται με έως και 10 χρόνια φυλάκιση.

Για να διευκολυνθεί η κατασκοπεία σε βάρος των πολιτών το 1999 προτάθηκε νόμος σύμφωνα με τον οποίο όλες οι εταιρείες και οι οργανισμοί, εκτός των πρεσβειών, θα πρέπει να καταχωρούν τα λογισμικά τους στην κυβέρνηση χρησιμοποιώντας τεχνολογίες κρυπτογράφησης. Επειδή, όμως, αντιτάχθηκαν οι πολυεθνικές, η κυβέρνηση υποχρεώθηκε να αναθεωρήσει και να αλλάξει το νόμο. Έτσι, απαιτεί τα κλειδιά, τα οποία χρησιμοποιούνται στην κρυπτογράφηση του λογισμικού και μόνο συγκεκριμένα λογισμικά καταχωρούνται.

Τέλος να αναφέρουμε πως η Κίνα έχει περίπου 60 κανονισμούς σχετικά με το Internet, οι οποίοι ακολουθούν τον κανόνα ότι κάτι πρέπει να είναι ανοιχτό αλλά πολύ καλά φυλασσόμενο. Αυτό σημαίνει, ότι οι συσκευές επικοινωνίας καταγράφονται για να προστατευτεί η οικονομία και η ασφάλεια του κράτους.

ΚΕΦΑΛΑΙΟ 3°

Ασφάλεια και Ιδιωτικότητα στο Διαδίκτυο

Η ραγδαία αύξηση του αριθμού των χρηστών του διαδικτύου με τον αριθμό τους να έχει 5πλασιαστεί μέσα στην πρώτη δεκαετία του 2000 και η εξάπλωση του Internet σε κάθε πτυχή της κοινωνικής και οικονομικής μας ζωής, είχε σαν αποτέλεσμα να αποδειχθεί αυτό πραγματικός θησαυρός και πηγή πολύτιμων πληροφοριών για τους κυβερνοεγκληματίες. Εντελώς ξαφνικά, τα τραπεζικά και παντός άλλου είδους προσωπικά δεδομένα εκατομμυρίων χρηστών έγιναν προσβάσιμα σε όσους κατέχουν τους κατάλληλους τρόπους εξαπάτησης. Πρόσφατο παράδειγμα αποτελεί η παραβίαση του Playstation Network της Sony που πραγματοποιήθηκε τον Απρίλιο του 2011 με τη διαρροή στοιχείων 100 εκατομμυρίων χρηστών παγκοσμίως. Πρόκειται για μια από τις μεγαλύτερες κλοπές δεδομένων στην ιστορία του Internet και της πληροφορικής. Στα στοιχεία που η Sony εκτιμά πως εκλάπησαν συμπεριλαμβάνονται ονόματα, διευθύνσεις, χώρες προέλευσης, email, ημερομηνίες γέννησης, κωδικοί πρόσβασης σε Playstation Network και Qriocity και Handle/ PSN online ID's. Άλλο ένα αντίστοιχο περιστατικό, τον Απρίλιο του 2011 ήταν η μαζική κλοπή δεδομένων από τις βάσεις δεδομένων της αμερικανικής εταιρείας online marketing, Epsilon (δεκάδες εκατομμύρια ονόματα και διευθύνσεις email - η εταιρεία εξυπηρετεί 2.500 εταιρείες σε όλο τον κόσμο), κατά την οποία αποκτήθηκαν στοιχεία μεγάλων αμερικανικών τραπεζών, ξενοδοχείων και καταστημάτων, τα οποία θεωρείται πως σύντομα θα αρχίσουν (αν δεν έχουν αρχίσει ήδη) να χρησιμοποιούνται σε κυβερνοεγκληματικές δραστηριότητες. Επίσης, ανάλογης έκτασης περιστατικό είχε απασχολήσει και το 2006 τη Citibank, με μαζική κλοπή αριθμών PIN [25]. Επίσης,η έλευση των ιστοσελίδων κοινωνικής δικτύωσης προσέθεσε μια ακόμη απροσδόκητη ευκαιρία σε όσους είχαν βάλει στο μάτι προσωπικά δεδομένα. Οι κακόβουλοι χρήστες συνειδητοποίησαν ότι θα μπορούσαν να έχουν πρόσβαση σε πληθώρα πληροφοριών, αν βέβαια κατάφερναν έξυπνα να εκμεταλλευτούν τις ευκαιρίες που τους δίνονταν. Και αυτές ήταν πολλές αν αναλογιστούμε ότι οι χρήστες άρχισαν να δημοσιοποιούν προσωπικές τους πληροφορίες χωρίς να υπολογίζουν το κόστος που μπορεί να έχει αυτή τους η ενέργεια. Αυτό έχει σαν αποτέλεσμα διάφοροι επιτήδειοι, αλλά και ολόκληρες εταιρείες, να αντλούν σημαντικά έσοδα από τις προσωπικές πληροφορίες που συλλέγουν από το διαδίκτυο.

Οι επιθέσεις που εξαπολύονται απέναντι σε ανυποψίαστους χρήστες πηγάζουν από κάποιον (ή κάποιους επιτιθέμενους) και αποτελούνται από μια ακολουθία βημάτων [26]. Ο επιτιθέμενος, χρησιμοποιώντας κάποια τεχνική (κάποια εντολή ή πρόγραμμα, ακόμα και το social engineering) εκμεταλλεύεται τις αδυναμίες (σχεδιαστικές, λειτουργικές, τεχνικές, ανθρώπινες) του συστήματος ενός αντικειμένου (λογαριασμός χρήστη, δίκτυο υπολογιστών, διεργασίες συστήματος) προκειμένου οι ενέργειές του (συλλογή πληροφοριών, απόκτηση πρόσβασης, υποκλοπή στοιχείων κτλ) να αποφέρουν το προσδοκώμενο αποτέλεσμα (διακύβευση ασφάλειας συστήματος, απόκτηση προνομίων, κλοπή).

Τα αποτελέσματα των ενεργειών τους είναι αυτά που έχουν αναδείξει την ασφάλεια των πληροφοριών και την προστασία της ιδιωτικότητας σε μείζονα θέματα της χρήσης του διαδικτύου προκειμένου αυτό να αναπτυχθεί σε ένα έμπιστο, ευρέως αποδεκτό μέσο ανταλλαγής προϊόντων και υπηρεσιών. Οι στόχοι που θα πρέπει να εκπληρωθούν προκειμένου να επιτευχθεί αυτό είναι [27] :

- Ακεραιότητα δεδομένων (integrity). Αναφέρεται στη διατήρηση των δεδομένων χωρίς ανεπιθύμητες τροποποιήσεις,αφαιρέσεις ή προσθήκες από μη εξουσιοδοτημένα άτομα.
- Διαθεσιμότητα δεδομένων (availability). Αφορά στην εξασφάλιση ότι τα δεδομένα θα είναι στη διάθεση των χρηστών όποτε απαιτείται η χρήση τους.
- Εμπιστευτικότητα (confidentiality). Δηλώνει ότι οι ευαίσθητες πληροφορίες δεν θα πρέπει να αποκαλύπτονται σε μη εξουσιοδοτημένα άτομα.
- Μη αποποίηση ευθύνης (non-repudation). Πιστοποίηση ότι όντως η επικοινωνία μεταξύ των δύο οντοτήτων έχει πραγματοποιηθεί.

- Αυθεντικοποίηση (authentication). Εξασφάλιση ότι η οντότητα με την οποία επικοινωνούμε είναι αυτή που ισχυρίζεται ότι είναι.

3.1 **Απειλές ασφάλειας στο διαδίκτυο**

Η ασφάλεια του Παγκόσμιου Ιστού (Internet) και του Διαδικτύου (Web) γενικότερα είναι ένα πολύπλοκο ζήτημα που περιλαμβάνει πολλές όψεις της παραδοσιακής πληροφοριακής ασφάλειας, της αρχιτεκτονικής των υπολογιστών, του σχεδιασμού συστημάτων, της μηχανικής λογισμικού, της τεχνολογίας του Διαδικτύου, των μαθηματικών και του νόμου [28]. Ο αριθμός των χρηστών που έρχεται σε επαφή με νέα παραδείγματα της πληροφορικής όχι μόνο αυξάνεται αλλά και ενημερώνεται όλο και περισσότερο για τους κινδύνους ασφάλειας και παραβίασης της ιδιωτικότητας που ελλοχεύουν. Παρακάτω εστιάζουμε σε τρεις επιθέσεις ασφάλειας, οι οποίες οδηγούν στην υποκλοπή των προσωπικών δεδομένων των χρηστών και η έννοια της προστασίας της ιδιωτικότητας τίθεται εν αμφιβόλω.

3.1.1 **Επίθεση από Ωτακουστές (**Eavesdroppers)

Ο ωτακουστής είναι ένας επιτιθέμενος ικανός να παρακολουθεί όλες τις πληροφορίες που είτε αποστέλλονται, είτε λαμβάνονται από κάποιο συγκεκριμένο συμμετέχοντα, με σκοπό να ανιχνευτεί είτε ο αποστολέας είτε ο παραλήπτης για κάθε επικοινωνία. Είναι δύσκολο να αντιμετωπιστούν αποτελεσματικά γιατί μπορούν να καταγράφουν και να συγκρίνουν όλα τα εισερχόμενα και εξερχόμενα μηνύματα [30].

Η καταγραφή και η παρακολούθηση δεδομένων που μεταφέρονται μέσω ενός δικτύου μπορεί να γίνει με λογισμικά καταγραφής πακέτων (packet sniffers), τα οποία παρακολουθούν τα μηνύματα που στέλνονται και λαμβάνονται από τις εφαρμογές και τα πρωτόκολλα που τρέχουν στον υπολογιστή μας αλλά τα ίδια δεν στέλνουν ποτέ πακέτα. Παρόμοια, τα λαμβανόμενα πακέτα δεν απευθύνονται ποτέ με ρητό τρόπο στο sniffer. Λαμβάνει μόνο τα αντίγραφά τους. Βέβαια, θα πρέπει η κάρτα δικτύου να λειτουργεί σε κατάσταση ‘’promiscuous mode’’ δηλαδή με τρόπο που της δίνει τη δυνατότητα να λαμβάνει όλα τα πακέτα που περνάνε από το μέσο μετάδοσης (ανεξάρτητα του αποδέκτη).

Συχνά χρησιμοποιούνται περισσότεροι του ενός σε κομβικά σημεία του δικτύου (π.χ. Gateways) ώστε να εντοπίζουν εστίες προβλημάτων και προσπάθειες εισβολής (Intrusion Detection System-IDS).

Αυτά, όμως, τα προτερήματα των λογισμικών αυτών μπορούν να εκμεταλλευτούν διάφοροι επιτήδειοι προκειμένου να υποκλέψουν passwords, αριθμούς πιστωτικών καρτών και άλλα προσωπικά στοιχεία των χρηστών [31].

3**.1.2 Επίθεση κακόβουλων συνεργατών (Malicious collaborators)**

Κακόβουλος συνεργάτης σ’ ένα πρωτόκολλο είναι ένας δικτυακός κόμβος που συνεργάζεται για την υποστήριξη της επικοινωνίας με άλλους κόμβους με σκοπό να ανακαλύψει την ταυτότητα του αποστολέα ενός ή περισσοτέρων μηνυμάτων. Στη χειρότερη περίπτωση όπου όλοι οι διακομιστές πλην ενός είναι εχθρικοί συνεργάτες, κάθε πακέτο που αποστέλλεται από τον αποστολέα αναγνωρίζεται αμέσως [30].

3**.1.3 Επίθεση Αντίστροφης Πορείας (**Trace Back Attack):

Στην επίθεση αντίστροφης πορείας, ο επιτιθέμενος ξεκινά από έναν γνωστό ανταποκριτή και ανιχνεύει το μονοπάτι προς τον αποστολέα κατά το μονοπάτι προώθησης ή το αντίστροφο μονοπάτι. Τα είδη των επιθέσεων αυτών είναι δύο [29].

- Ενεργή επίθεση αντίστροφης πορείας (active trace back attack), όπου ο επιτιθέμενος διατηρεί τον έλεγχο της δικτυακής δομής και είναι ικανός να ακολουθήσει ένα ενεργό και συνεχές ρεύμα πακέτων που διαπερνά το δίκτυο προς το σημείο προέλευσής τους. Εάν το ρεύμα είναι μόνο ένα τότε είναι εύκολο. Εάν, όμως, ποικίλα ρεύματα πακέτων διαπερνούν έναν συγκεκριμένο διακομιστή ίσως είναι δυσκολότερο, ιδιαίτερα αν τα πακέτα αλλάζουν μορφή στο διακομιστή (αν π.χ. κρυπτογραφούνται ή αποκρυπτογραφούνται με διαφορετικό κλειδί.)

- Παθητική επίθεση αντίστροφης πορείας (passive trace back attack), όπου ο επιτιθέμενος είναι κατά κάποιο τρόπο σε θέση να εξετάσει την κατάσταση δρομολόγησης των μελών που συμμετέχουν και να ανιχνεύσει αντίστροφα τη σύνδεση μέσω της αποθηκευμένης πορείας.

Η διαφορά των δύο είναι ότι κατά τη διάρκεια της ενεργής επίθεσης, ο επιτιθέμενος μπορεί να πάρει τον έλεγχο του δικτύου με την έννοια ότι μπορεί να εντοπίσει την προέλευση των πακέτων, ενώ στην παθητική επίθεση ο επιτιθέμενος με κάποιο τρόπο συλλέγει τις πληροφορίες σχετικά με τις ιδιότητες δρομολόγησης του πρωτοκόλλου και οι κόμβοι του δικτύου του επιτρέπουν να εντοπίσει τον αποστολέα του μηνύματος με στατικό τρόπο.

3.2 **Απειλές ιδιωτικότητας στο διαδίκτυο**

Οι παραπάνω απειλές ασφάλειας μπορούν να οδηγήσουν στην αποκάλυψη εσωτερικών δεδομένων της επικοινωνίας παραβιάζοντας έτσι το απόρρητο της επικοινωνίας και την ιδιωτικότητα των χρηστών. Παρακάτω αναφέρονται επιθέσεις (cookies, προσωποποιημένες υπηρεσίες αλλά και συγκέντρωση δεδομένων από τους παρόχους πρόσβασης στο διαδίκτυο) οι οποίες οδηγούν σε παρακολούθηση των δεδομένων των χρηστών και παράνομη χρήση των δεδομένων τους.

3.2.1 **Συλλογή Δεδομένων (**data aggregation)

Ο όρος ομαδοποίηση δεδομένων (data aggregation) αναφέρεται στην τάση για συσσώρευση, διατήρηση και χρήση μεγάλου όγκου ηλεκτρονικών πληροφοριών βασισμένων σε συγκεκριμένες μεταβλητές (όπως η ηλικία, το επάγγελμα ή το εισόδημα) και για διάφορους λόγους, όπως η αρχειοθέτηση και η ανάλυση. Τα συγκεντρωτικά αυτά δεδομένα περιλαμβάνουν και τα μεταδεδομένα που απαιτούνται για τη δημιουργία ευρετηρίου, σήμανσης (flag), ορισμού ή πρόσβασης στις πληροφορίες [31]. Όλος αυτός ο όγκος δεδομένων συγκεντρώνεται σε μια ηλεκτρονική αποθήκη και όταν συνδυαστούν δημιουργούν ένα πορτραίτο του ατόμου, μια ‘’ψηφιακή βιογραφία‘’ [32].

Στο βαθμό που η βιογραφία αυτή είναι ακριβής, τότε η ζωή του ατόμου όχι μόνο αποκαλύπτεται αλλά καταγράφεται και είναι πρόσφορη για έρευνα και ανάλυση, η οποία στην εποχή της πληροφορικής γίνεται σε κλάσματα δευτερολέπτου. Το γεγονός αυτό καθιστά ικανή την έρευνα (τόσο σε κυβερνητικό όσο και σε ιδιωτικό επίπεδο) όχι μόνο υπόπτων αλλά και αθώων πολιτών χωρίς καμία επίβλεψη από ουδέτερο παρατηρητή. Επηρεάζουν τη ζωή μας και μας εκθέτουν σε πλειάδα κινδύνων όπως κλοπή ταυτότητας και παρακολούθηση. Τις περισσότερες, όμως, φορές οι βιογραφίες αυτές είναι ανακριβείς μιας και αποκαλύπτουν πτυχές της προσωπικότητάς μας βασιζόμενες κυρίως σε τυποποιημένες κατηγορίες και συλλογισμούς και όσο ο ρόλος που διαδραματίζουν στη λήψη σημαντικών αποφάσεων μεγαλώνει, τόσο θα αυξάνεται και ο κίνδυνος λανθασμένων εκτιμήσεων.

3.2.2 **Αλλοίωση Δεδομένων (**Data Distortion)

Σύμφωνα με τον Solove, η αλλοίωση δεδομένων συνίσταται στον λανθασμένο τρόπο με τον οποίο ένα άτομο κρίνεται από τους συνανθρώπους του εξαιτίας διάδοσης ανακριβών πληροφοριών σχετικά με την προσωπικότητα και τη ζωή του. Η αλλοίωση, όπως και η αποκάλυψη των δεδομένων, μπορεί να οδηγήσει σε στιγματισμό και να καταφέρει σημαντικό πλήγμα στη φήμη ενός ανθρώπου. Και η φήμη είναι το μέσο με το οποίο αλληλεπιδρούμε με τους άλλους σε μια κοινωνία [33].

Για το σκοπό αυτό, η Ευρωπαϊκή Οδηγία σαφέστατα ορίζει ότι τα δεδομένα ενός ατόμου πρέπει να είναι ακριβή και ενημερωμένα, όσο αυτό είναι εφικτό ενώ παράλληλα πρέπει να παρέχεται, χωρίς καθυστέρηση και με λογικό κόστος, στα άτομα το δικαίωμα να επεμβαίνουν στα στοιχεία αυτά και να τα διορθώνουν ή ακόμα και να τα μπλοκάρουν σε περίπτωση που αυτά δεν ανταποκρίνονται στην πραγματικότητα [34].

3.2.3 **Αποκλεισμός των χρηστών από τη δυνατότητα πρόσβασης στα προσωπικά τους δεδομένα (exclusion)**

Το πρόβλημα του αποκλεισμού δημιουργείται όταν στα υποκείμενα των δεδομένων δεν παρέχεται η δυνατότητα πρόσβασης, διόρθωσης και ελέγχου της ψηφιακής τους βιογραφίας και γενικότερα των προσωπικών τους δεδομένων. Η αιτιολόγηση γι' αυτό εστιάζει τόσο στο κόστος μιας τέτοιας ενέργειας όσο και στο γεγονός ότι οι κυβερνητικές υπηρεσίες πιθανόν να θέλουν να κρατήσουν κρυφά κάποια αρχεία που αφορούν την κρατική ασφάλεια και την επιβολή του νόμου. Ο αποκλεισμός όμως των χρηστών δημιουργεί προβλήματα, τα οποία σχετίζονται με τα αισθήματα ανασφάλειας που προκαλούνται από τα συχνά ανεπαρκή επίπεδα ασφάλειας των δεδομένων. Το άτομο αισθάνεται ότι δεν ενημερώνεται για τη χρήση των δεδομένων του και θεωρεί ότι είναι εντελώς ανίκανο να κάνει κάτι ώστε να την επηρεάσει. Η αδυναμία αυτή του ατόμου αποτελεί έναν ευαίσθητο τομέα, ο οποίος χρήζει ιδιαίτερης προσοχής σε μια εποχή όπου οι προσωπικές πληροφορίες παίζουν σημαντικό ρόλο στη λήψη αποφάσεων σχετικών με τη ζωή του ατόμου.

3.2.4 **Χρήση των προσωπικών δεδομένων των χρηστών για σκοπούς άλλους για τους οποίους συλλέχθηκαν (secondary use)**

Ήδη από το 1980 όποτε και ο ΟΟΣΑ εξέδωσε τις ''Κατευθυντήριες Αρχές που διέπουν την προστασία της ιδιωτικότητας και τις διασυνοριακές ροές των προσωπικών δεδομένων'' γίνεται αναφορά στην αρχή του προσδιορισμένου σκοπού (purpose specification principle), σύμφωνα με την οποία θα πρέπει να προσδιορίζονται επακριβώς οι σκοποί για τους οποίους συλλέγονται τα προσωπικά δεδομένα και η χρήση τους να συνάδει με τους σκοπούς αυτούς ενώ κάθε αλλαγή στους σκοπούς θα πρέπει να αναφέρεται. Στην ευρωπαϊκή κοινοτική οδηγία 95/46 αναφέρεται στο δικαίωμα αντίταξης στην επεξεργασία των δεδομένων, όπου σύμφωνα με το άρθρο 14 το υποκείμενο των δεδομένων θα πρέπει να έχει το δικαίωμα να αντιταχθεί στην επεξεργασία δεδομένων που το αφορούν '' για επιτακτικούς και νόμιμους λόγους σχετικούς με την προσωπική του κατάσταση.Σε περίπτωση αιτιολογημένης αντίταξης, η επεξεργασία δεν μπορεί πλέον να αφορά τα δεδομένα αυτά . Θα πρέπει επίσης να δύναται να αντιταχθεί, εφόσον το ζητήσει και δωρεάν, στην επεξεργασία των δεδομένων προσωπικού χαρακτήρα την οποία προτίθεται να πραγματοποιήσει ο υπεύθυνος επεξεργασίας και σχετίζεται με δραστηριότητες για την προώθηση προϊόντων ή να ενημερώνεται πριν από την πρώτη ανακοίνωση των δεδομένων προσωπικού χαρακτήρα σε τρίτους ή τη χρησιμοποίησή τους για λογαριασμό τρίτων με σκοπό τη διεξαγωγή έρευνας μέσω του ταχυδρομείου και να του παρέχεται ρητά το δικαίωμα να αντιταχθεί δωρεάν πριν από την ανακοίνωση ή τη χρησιμοποίηση.

Ο λόγος για τον οποίο υπάρχει τόσο μεγάλο ενδιαφέρον για την μη εξουσιοδοτημένη χρήση των δεδομένων από τρίτους, είναι γιατί δημιουργεί αισθήματα φόβου στο υποκείμενο των δεδομένων για τη μελλοντική τους χρήση καθώς δεν μπορεί να γνωρίζει τις επιπτώσεις που θα έχει αυτό στη ζωή τους.

3.2.5 **Παραβίαση απορρήτου** (breach of confidentiality)

Στη νομική ορολογία, το ζήτημα της εμπιστευτικότητας έρχεται στο προσκήνιο όταν προκύπτει μια σχέση εμπιστοσύνης μεταξύ του ατόμου που συλλέγει τα δεδομένα και του υποκειμένου των δεδομένων [35]. Αυτή η εμπιστοσύνη μπορεί να προέρχεται από μια ποικιλία συνθηκών ή ακόμα και από το είδος των πληροφοριών που συλλέγονται, οι οποίες μπορεί να αφορούν την απασχόληση, οικονομικές ή ιατρικές πληροφορίες και δίνει το δικαίωμα στο υποκείμενο να απαιτήσει τη μη χρησιμοποίηση των πληροφοριών που παρέχει για σκοπούς άλλους από αυτούς που αρχικώς του ανακοινώθηκαν αλλά και τη μη αποκάλυψη των πληροφοριών χωρίς την άδεια του, εκτός αν υπάρχουν επιτακτικοί λόγοι γενικού συμφέροντος. Βέβαια, θα πρέπει εδώ να επισημάνουμε ότι μεταξύ της αποκάλυψης των πληροφοριών και της παραβίασης απορρήτου υπάρχει μια βασική διαφορά, καθώς η πιο σημαντική πτυχή της δεύτερης είναι η διατάραξη της σχέσης εμπιστοσύνης που έχει αναπτυχθεί και το αίσθημα προδοσίας που αισθάνεται το άτομο.

3.2.6 **Δεδομένα που συγκεντρώνουν οι πάροχοι πρόσβασης στο Διαδίκτυο** (ISPs)

Ο πάροχος διαδικτυακών υπηρεσιών μπορεί να συγκεντρώνει πληροφορίες σχετικές με τις σελίδες που επισκέπτεται ο χρήστης, την ακριβή ώρα, τη διάρκεια πρόσβασης κ.α. Μη εξουσιοδοτημένα άτομα που μπορεί να έχουν πρόσβαση στη βάση δεδομένων του παροχου, όπου εκτός όλων των άλλων μπορεί να περιέχει και προσωπικά/ ευαίσθητα δεδομένα των πελατών του, αποτελούν σοβαρή απειλή παραβίασης της ιδιωτικότητας των χρηστών.

3.2.7 **Επιθέσεις προσωποποιημένων υπηρεσιών**

Αρκετές ιστοσελίδες προσφέρουν ένα εύρος προσωποποιημένων υπηρεσιών για την προσέλκυση νέων χρηστών. Πάντα, όμως, υπάρχει η απειλή της αποκάλυψης των προσωπικών στοιχείων κατά τη διαδικασία της εγγραφής, γι αυτό και η αυξανόμενη χρήση τέτοιων υπηρεσιών έχει οδηγήσει τους μηχανισμούς ενίσχυσης της ιδιωτικότητας στο διαδίκτυο στην εξεύρεση τρόπων ελαχιστοποίησης αυτής της απειλής.

3.2.8 **Επιθέσεις μέσω αρχείων cookies**

Τα cookies είναι μικρά αρχεία δεδομένων που αποθηκεύονται στους υπολογιστές των χρηστών και σκοπός τους είναι να παρέχουν πληροφορίες για τους ιστοτόπους που επισκέπτονται. Μπορούν να απειλήσουν την ιδιωτικότητα του χρήστη αφού τα προσωπικά του δεδομένα μπορούν να συλλεχθούν από τους διάφορους ιστοτόπους, να επεξεργαστούν και να δημιουργηθεί το προφίλ του χρήστη (web profile). Ένα cookie είναι ένα κομμάτι κειμένου το οποίο στέλνεται από έναν εξυπηρετητή διαδικτύου (web server) στον υπολογιστή του χρήστη (web client) μέσω του προγράμματος πλοήγησης που αυτός χρησιμοποιεί. Μόλις ληφθεί, το πρόγραμμα πλοήγησης (ή φυλλομετρητής) στέλνει αυτό το cookie κάθε φορά που ο χρήστης ζητάει κάποιο καινούργιο έγγραφο από τον web server.

Τα cookies μπορούν να χρησιμοποιηθούν για να παραβιάσουν την ανωνυμία από τους χρήστες ή να την ενισχύσουν. Δυστυχώς η επιλογή δεν είναι στα χέρια του χρήστη, αλλά βρίσκεται υπό τον έλεγχο του web server.

3.3 **Απαιτήσεις ιδιωτικότητας**

Σε μια δικτυακή κοινωνία, όπως η σημερινή, η ιδιωτικότητα, ως βασικό ανθρώπινο δικαίωμα, δεν προστατεύεται μόνο από νόμους και κανονισμούς. Τα πληροφοριακά συστήματα που συλλέγουν προσωπικά δεδομένα θα πρέπει να αποτρέπουν την παραβίαση της ιδιωτικότητας και για το λόγο αυτό θα πρέπει να λαμβάνεται υπόψη σαν μια βασική παράμετρος που θα πρέπει να υλοποιηθεί. Για να επιτευχθεί ο στόχος αυτός θα πρέπει να ικανοποιούνται κάποιες απαιτήσεις, οι λεγόμενες απαιτήσεις ιδιωτικότητας, οι οποίες περιλαμβάνουν την ***ανωνυμία*** (anonymity),την ***ψευδωνυμία*** (pseudonymity), τη ***μη συνδεσιμότητα*** (unlinkability) και τη ***μη παρατηρησιμότητα*** (unobservability). Στη συνέχεια αναλύονται οι παραπάνω ιδιότητες.

3**.3.1 Ανωνυμία (anonymity)**

Η ανωνυμία διασφαλίζει ότι ο χρήστης μπορεί να χρησιμοποιήσει μια υπηρεσία ή να επικοινωνήσει με μια άλλη οντότητα χωρίς να αποκαλύψει την ταυτότητά του [36]. Ανάλογα με το ρόλο που έχει ο χρήστης στην επικοινωνία, έχουν καθοριστεί δύο μορφές ανωνυμίας: η ανωνυμία του αποστολέα (sender anonymity) και η ανωνυμία του παραλήπτη (receiver anonymity). Η ανωνυμία του αποστολέα σημαίνει ότι σε μια επικοινωνία ο χρήστης που έχει το ρόλο του αποστολέα παραμένει ανώνυμος ενώ ο παραλήπτης όχι. Το αντίστοιχο συμβαίνει στην ανωνυμία του παραλήπτη.

Ανωνυμία από την πλευρά του επιτιθέμενου σημαίνει ότι ο επιτιθέμενος δεν μπορεί επακριβώς να αναγνωρίσει το χρήστη μέσα σ' ένα σύνολο ανώνυμων χρηστών [37].Για το χρήστη που στέλνει/λαμβάνει σε μία επικοινωνία υπάρχει ο όρος της τέλειας ανωνυμίας αποστολέα/παραλήπτη (perfect sender/receiver anonymity), που σημαίνει ότι ο επιτιθέμενος

δεν μπορεί να ξεχωρίσει πότε ο αποστολέας/παραλήπτης συμμετέχει σε μια επικοινωνία και πότε όχι. Σε ένα σύστημα η καθολική ανωνυμία (δηλ. η ανωνυμία που προσφέρεται από το σύστημα σε όλους τους χρήστες συνολικά) είναι ισχυρότερη όσο μεγαλύτερο είναι το αντίστοιχο σύνολο ανωνύμων οντοτήτων αλλά και όσο περισσότερο ομοιόμορφα κατανεμημένη είναι η αποστολή και παραλαβή μηνυμάτων από τις οντότητες εντός του συνόλου.

Αντιλαμβανόμαστε ότι η ανωνυμία γενικά είναι ένας όρος που εξαρτάται πολύ από το πλαίσιο μέσα στα οποίο υπάρχει (αριθμός χρηστών, χαρακτηριστικά τους κοκ). Προκειμένου, λοιπόν, να ποσοτικοποιήσουμε την ανωνυμία, θα πρέπει να περιγράψουμε το σύστημα με ικανοποιητική λεπτομέρεια, κάτι το οποίο δεν είναι πάντα δυνατό σε μεγάλα συστήματα. Εκτός, όμως, από την ποσοτικοποίηση της ανωνυμίας, υπάρχει και μια άλλη πλευρά της: η ευρωστία της. Η ευρωστία της ανωνυμίας μέσα σ' ένα συγκεκριμένο περιβάλλον δηλώνει κατά πόσο παραμένει σταθερή στις διάφορες αλλαγές του συγκεκριμένου περιβάλλοντος (π.χ. ισχυρότερος επιτιθέμενος ή διαφορετική κατανομή).

Όλοι οι παραπάνω ορισμοί της ανωνυμίας είναι κατάλληλοι όταν πρόκειται να την περιγράψουμε σ' ένα στατικό περιβάλλον. Σ' ένα περιβάλλον, όμως, δυναμικό, που υφίσταται συνεχώς αλλαγές, χρειαζόμαστε έναν ορισμό που να μπορεί να τις αντικατοπτρίζει. Ο απλούστερος τρόπος είναι να ιδωθεί η διαφοροποίηση από την πλευρά του επιτιθέμενου. Μια διαφοροποίηση της ανωνυμίας από την πλευρά του επιτιθέμενου δηλώνει τη διαφορά ανάμεσα στην ανωνυμία του χρήστη λαμβάνοντας υπόψη τις παρατηρήσεις του επιτιθέμενου (δηλ. την εκ των υστέρων γνώση του) και την ανωνυμία του χρήστη λαμβάνοντας υπόψη του την εκ των προτέρων (δηλ. την αρχική) γνώση του. Για να μιλήσουμε με ποσοτικούς όρους,

Ποσότητα (διαφοροποίηση της ανωνυμίας)=ποσότητα (ανωνυμία a posteriori)- ποσότητα (ανωνυμία a priori)

Καθώς η ποσότητα της ανωνυμίας δεν μπορεί να αυξηθεί, η διαφοροποίηση της δεν μπορεί να έχει θετική τιμή. Αντίθετα, όταν πάρει αρνητική τιμή σημαίνει ότι η ανωνυμία έχει μειωθεί. Τέλεια διατήρηση της ανωνυμίας ενός χρήστη έχουμε όταν η διαφοροποίηση της ανωνυμίας παίρνει την τιμή μηδέν, πράγμα που σημαίνει ότι η ανωνυμία παραμένει σταθερή.

3.3.2 Ψευδωνυμία (pseudonymity)

Η ψευδωνυμία καλύπτει το φάσμα μεταξύ ανωνυμίας και πλήρους αναγνωρισιμότητας και αφορά τη χρήση ψευδωνύμων σαν αναγνωριστικά των χρηστών ενώ η χρήση τους μπορεί να είναι σπάνια, περιστασιακή ή συχνή [39].

Όταν ο χρήστης είναι ο αποστολέας μιλάμε για ψευδωνυμία αποστολέα (sender pseudonymity) ενώ όταν ο χρήστης είναι ο παραλήπτης μιλάμε για ψευδωνυμία παραλήπτη (recipient pseudonymity). Επεκτείνοντας τους ορισμούς αυτούς, μπορούμε να μιλήσουμε και για ομαδικό ψευδώνυμο (group pseudonym), το οποίο αναφέρεται σε πολλούς κατόχους του ψευδωνύμου, αλλά και για το μεταβιβάσιμο ψευδώνυμο (transferable pseudonym), το οποίο μπορεί να μεταφερθεί από τον έναν χρήστη σε κάποιον άλλο. Το ομαδικό ψευδώνυμο μπορεί να επηρεάσει το σύνολο ανωνύμων οντοτήτων, αφού ο επιτιθέμενος, αξιοποιώντας μόνο τις πληροφορίες που εξάγει από το ψευδώνυμο, δεν μπορεί να προσδιορίσει ποιος χρήστης εκτέλεσε ποια πράξη.

3.3.3 Μη συνδεσιμότητα (unlinkability)

Η μη συνδεσιμότητα προστατεύει την ιδιωτικότητα του χρήστη από πιθανούς επιτιθέμενους απαγορεύοντάς τους να συνδέσουν τμήματα πληροφοριών ή διαφορετικές συνόδους (sessions) ενός ανώνυμου χρήστη που θα τους επιτρέψει να ανακαλύψουν την ταυτότητα του χρήστη.

Μη συνδεσιμότητα από την πλευρά του επιτιθέμενου, σημαίνει ότι δεν είναι σε θέση να διακρίνει αν τα στοιχεία που τον ενδιαφέρουν μέσα σ' ένα σύστημα (χρήστες, μηνύματα που εστάλησαν ή/και παραλήφθηκαν κ.α.), σχετίζονται μεταξύ τους ή όχι [38]. Ενώ είναι σε θέση να κάνει πολλές φορές χρήση των πόρων του συστήματος, εντούτοις του είναι αδύνατον να συνδέσει τα γεγονότα με κάποιον τρόπο. Αν θέλουμε να εκφράσουμε τη μη-συνδεσιμότητα με ποσοτικούς όρους (πάντοτε απ' την οπτική του επιτιθέμενου), μπορούμε να πούμε ότι πρόκειται για την διαφορά ανάμεσα στη μη-συνδεσιμότητα δύο ή περισσοτέρων στοιχείων του

συστήματος λαμβάνοντας υπόψη τις παρατηρήσεις του επιτιθέμενου και τη μη-συνδεσιμότητα εκείνων των στοιχείων λαμβάνοντας υπόψη μόνο την εκ των προτέρων γνώση του επιτιθέμενου. Όταν η διαφορά αυτή είναι μηδέν, σημαίνει ότι η πιθανότητα να σχετίζονται τα στοιχεία παραμένει μηδέν τόσο εκ των προτέρων όσο και εκ των υστέρων βάσει των παρατηρήσεων του επιτιθέμενου. Με απλά λόγια, σημαίνει ότι η ικανότητα του επιτιθέμενου να συσχετίσει τα στοιχεία μεταξύ τους δεν αυξάνεται ούτε με την απλή παρατήρηση του συστήματος αλλά ούτε και με την πιθανή αλληλεπίδρασή του με αυτό.

Περιγράφοντας τους όρους της ανωνυμίας λαμβάνοντας υπόψη τον ορισμό της μη-συνδεσιμότητας, μπορούμε να πούμε τα εξής: Καταρχήν, αυτό που ενδιαφέρει είναι το ποιος έχει αποστείλει και ποιος έχει λάβει. Έτσι, λοιπόν, ανωνυμία ενός χρήστη είναι η αδυναμία σύνδεσης του συγκεκριμένου χρήστη και του συγκεκριμένου μηνύματος. Για παράδειγμα, ανωνυμία αποστολέα σημαίνει ότι κανένα μήνυμα δεν μπορεί να συνδεθεί σε έναν εν δυνάμει αποστολέα. Ανάλογος είναι και ο ορισμός για την ανωνυμία παραλήπτη. Επίσης, όταν ανάμεσα σε έναν αποστολέα και έναν παραλήπτη δεν είναι δυνατή η ανίχνευση της μεταξύ τους επικοινωνίας, μιλάμε για μη-συνδεσιμότητα επικοινωνίας.

3.3.4 Μη παρατηρησιμότητα (unobservability)

Η μη-παρατηρησιμότητα προστατεύει την ιδιωτικότητα των χρηστών από πιθανούς επιτιθέμενους απαγορεύοντάς τους να παρατηρήσουν ή να εντοπίσουν τα ίχνη των πρώτων τη στιγμή που περιηγούνται στο διαδίκτυο ή χρησιμοποιούν μια υπηρεσία.

Μη-παρατηρησιμότητα ενός στοιχείου που μας ενδιαφέρει (είτε είναι ο χρήστης είτε το μήνυμα) σημαίνει αφενός ότι δεν υπάρχει δυνατότητα ανίχνευσης του στοιχείου από τους χρήστες που δεν σχετίζονται με αυτό και αφετέρου δηλώνει την ανωνυμία της οντότητας που σχετίζεται με το στοιχείο απέναντι σε οποιαδήποτε οντότητα που σχετίζεται και εκείνη με το στοιχείο [38].

Μη παρατηρησιμότητα αποστολέα δηλώνει ότι μέσα σ' ένα σύνολο μη-παρατηρήσιμων οντοτήτων δεν είναι δυνατόν να ανιχνευθεί κατά πόσο κάποιος αποστολέας στέλνει ένα μήνυμα. Αντίστοιχος είναι και ο ορισμός για την μη-παρατηρησιμότητα παραλήπτη, ενώ όταν δεν είναι επαρκώς παρατηρήσιμη η επικοινωνία ανάμεσα σε ένα σύνολο εν δυνάμει αποστολέων και ένα σύνολο εν δυνάμει παραληπτών, μιλάμε για μη-παρατηρησιμότητα σχέσης.

Φυσικά, η μη-παρατηρησιμότητα μπορεί να περιγραφεί με ποσοτικούς όρους. Έτσι, σχετίζεται με τη διαφορά της μη ανιχνευσιμότητας του στοιχείου από τις οντότητες που δεν σχετίζονται με αυτό και με τη διαφορά της ανωνυμίας της οντότητας που σχετίζεται με το στοιχείο απέναντι σε οποιαδήποτε οντότητα που σχετίζεται και εκείνη με την οντότητα.

ΚΕΦΑΛΑΙΟ 4ο

Τεχνολογίες προστασίας της ιδιωτικότητας (Privacy Enhancing Technologies - PETs)

Το 1995 η Αρχή Προστασίας Δεδομένων της Δανίας εξέδωσε μία μελέτη με τον τίτλο ‘’Privacy Enhancing Technologies – A path to anonymity’’ όπου κατεδείκνυε πώς η τεχνολογία θα μπορούσε να χρησιμοποιηθεί για τη προστασία των χρηστών ενάντια στην κακόβουλη χρήση των προσωπικών τους δεδομένων. Το λογισμικό που θα μπορούσε να κατηγοριοποιηθεί ως PET (Privacy Enhancing Technologies) είναι προγενέστερο από αυτόν τον όρο κατά τουλάχιστον μία δεκαετία. Το πρώτο PET είναι γνωστό ως ‘’Mix networks’’ [40] και επινοήθηκε από το David Chaum μέσα από την επίτευξη ανώνυμων και μη παρατηρήσιμων επικοινωνιών σ’ ένα δίκτυο. Πράγματι, η έρευνά του αποτελεί τη βάση για κάποια ανώνυμα συστήματα επικοινωνίας και e-mail που είναι ακόμα σε χρήση [41]. Σήμερα είναι γενική η πεποίθηση ότι οι τεχνολογίες αυτές είναι σύμφυτες με τον καλό σχεδιασμό οποιουδήποτε συστήματος και προσφέρουν προφανή οφέλη και ανταγωνιστικά πλεονεκτήματα για τις εταιρείες που τα υιοθετούν.

Ουσιαστικά, οι τεχνολογίες ενίσχυσης της ιδιωτικότητας αφορούν μια σειρά μέτρων που προστατεύουν την ιδιωτικότητα εξαλείφοντας ή εμποδίζοντας την περιττή ή/και ανεπιθύμητη επεξεργασία προσωπικών δεδομένων χωρίς να υπάρξει απώλεια της λειτουργικότητας του συστήματος πληροφοριών. Πολλές φορές λανθασμένα θεωρούνται ως υποκατάστατα άλλων μέσων προστασίας των προσωπικών δεδομένων (όπως οι νόμοι και οι φορείς που επιβάλλουν και εφαρμόζουν τη νομοθεσία). Στην πραγματικότητα, όμως, οι τεχνολογίες αυτές δρουν συμπληρωματικά με τους υφιστάμενους νόμους ώστε να εξασφαλίζεται η όσο το δυνατόν μεγαλύτερη ασφάλεια των δεδομένων.

Δεν υπάρχει κάποιος συγκεκριμένος ορισμός για τον όρο Τεχνολογίες Ενίσχυσης της Ιδιωτικότητας, αν και σχεδόν όλοι ενσωματώνουν παρόμοιες αρχές:

- Οι τεχνολογίες αυτές μειώνουν ή εξαλείφουν τον κίνδυνο παραβίασης των αρχών της ιδιωτικής ζωής και της νομοθεσίας.
- Ελαχιστοποιούν τον όγκο των δεδομένων που συλλέγονται για τα άτομα.
- Ενθαρρύνουν τα άτομα πάντοτε να διατηρούν τον έλεγχο των στοιχείων που τα αφορούν.

Παράλληλα, πρέπει να γίνει κατανοητό ότι οι τεχνολογίες αυτές ούτε μπορούν, αλλά ούτε και είναι σχεδιασμένες για να εξετάσουν τις ανησυχίες των καταναλωτών ή τις πολιτικές του κατασκευαστή για τη συλλογή δεδομένων. Είναι, απλώς, ένα χρήσιμο εργαλείο στα χέρια των χρηστών και το οποίο θα πρέπει να ενθαρρύνονται να χρησιμοποιούν αν και εφόσον έχουν αμφιβολίες για τη συλλογή των δεδομένων τους.

Οι τεχνολογίες αυτές μπορούν να ταξινομηθούν ως εξής:

- Προστασία της ιδιωτικότητας στην πλευρά του χρήστη (client-side):
  - Στην παρούσα εργασία θα εξετάσουμε τις τεχνολογίες TOR [46]και το LPWA [43].
- Προστασία της ιδιωτικότητας στην πλευρά του εξυπηρετητή (server-side):
  - Τέτοια μέτρα είναι η κρυπτογράφηση της βάσης των δεδομένων και η κρυπτογράφηση της επικοινωνίας, όπως αυτά μπορούν να πραγματοποιηθούν μέσω του πρωτοκόλλου SSL ή ενός εικονικού δικτύου VPN.
- Κοινά μέτρα προστασίας της ιδιωτικότητας. Στην παρούσα εργασία θα εξετάσουμε την τεχνολογία P3P.

4.1 **Προστασία της ιδιωτικότητας στην πλευρά του χρήστη** (client-side)

4.1.1 **Ανωνυμία χρήστη μέσω ψευδωνύμων** (Lucent Personalized Web Assistant LPWA)

Πολλές ιστοσελίδες, προκειμένου να επιτρέψουν στο χρήστη την πρόσβαση, απαιτούν τη δημιουργία ενός λογαριασμού. Η διαδικασία αυτή ονομάζεται ''εξατομικευμένη περιήγηση στο διαδίκτυο'' (personalized web browsing) και δεν είναι και τόσο απλή μιας και ο χρήστης θα πρέπει να παρέχει ένα μοναδικό username και password για κάθε ιστοσελίδα , τέτοια ώστε να μην μπορούν να συνδεθούν με την ταυτότητά του. Εκτός, όμως, από τις πληροφορίες που ο ίδιος εθελοντικά δίνει σε μια ιστοσελίδα, πολλές άλλες παραχωρούνται σε αυτήν χωρίς ο ίδιος να το γνωρίζει εξαιτίας της αρχιτεκτονικής του HTTP αλλά και της χρήσης των cookies [42].

Έτσι, λοιπόν, αναπτύχθηκε το LPWA [43], το οποίο ουσιαστικά είναι ένας agent (ένας ενδιάμεσος) που αλληλεπιδρά με τις ιστοσελίδες εκ μέρους του χρήστη δημιουργώντας ψευδώνυμα για κάθε site που επισκέπτεται. Τα ψευδώνυμα αυτά αποτελούνται από ένα όνομα χρήστη, έναν μυστικό κωδικό και ένα e-mail. Να σημειωθεί ότι για κάθε ζεύγος χρήστη-ιστοσελίδα δημιουργούνται διαφορετικά ψευδώνυμα, αλλά το ίδιο ψευδώνυμο όταν ο χρήστης επισκέπτεται ξανά την ίδια ιστοσελίδα.

Ουσιαστικά, το LPWA συμβάλλει ώστε ο χρήστης να μην χρειάζεται κάθε φορά να επινοεί ψευδώνυμα και κωδικούς για κάθε ιστοσελίδα που επισκέπτεται ενώ παράλληλα εγγυάται ότι τα ψευδώνυμα που δημιουργεί δεν αποκαλύπτουν την ταυτότητα του χρήστη. Επίσης, παρέχει υποστήριξη στην ιστοσελίδα ώστε να απαντήσει στα ανώνυμα e-mails που στέλνει ο χρήστης ενώ τέλος, μπορεί να φιλτράρει τη ροή δεδομένων στο HTTP ώστε να διατηρήσει την ανωνυμία του χρήστη.

Το LPWA, μπορεί να ρυθμιστεί ως remote server (central proxy), σαν τοπικός εξυπηρετητής ή ακόμα και σαν firewall proxy με διάφορους συμβιβασμούς όσον αφορά την ασφάλεια, την εμπιστοσύνη και την ευκολία.

Αποτελείται από 3 λειτουργικά μέρη:

- Τη γεννήτρια προσωπικοτήτων (persona generator). Παράγει μοναδικά ψεύτικα στοιχεία (e-mail, συνθηματικό και ταυτότητα χρήστη) για κάθε ιστοσελίδα που ο χρήστης επιθυμεί να επισκεφθεί.
- Έναν πληρεξούσιο περιήγησης στον ιστό (HTTP proxy). Αυξάνει την προστασία του χρήστη ανακατευθύνοντας τη σύνδεση στο επίπεδο του TCP και φιλτράροντας τις επικεφαλίδες στο επίπεδο του HTTP.
- Έναν προωθητή μηνυμάτων ηλεκτρονικού ταχυδρομείου (e-mail forwarder), ο οποίος προωθεί τα μηνύματα στον σωστό χρήστη [43]

Κάθε ένα από τα μέρη αυτά μπορεί να βρίσκονται σε διάφορα σημεία. Η γεννήτρια μπορεί να υλοποιείται κατευθείαν στον browser του χρήστη ή και στον πληρεξούσιο περιήγησης στον ιστό (HTTP proxy). Ο HTTP proxy μπορεί να βρίσκεται στο firewall ή και σ' ένα ουδέτερο σημείο στο διαδίκτυο. Ο δε προωθητής πρέπει να βρίσκεται μακριά από το μηχάνημα του χρήστη αφού στόχος είναι τα διάφορα ψευδώνυμα να μην μπορούν να σχετιστούν με τον χρήστη.

Η γεννήτρια χρησιμοποιεί τη συνάρτηση Janus [44], η οποία είναι ένας συνδυασμός κρυπτογραφικών συναρτήσεων. Η συνάρτηση αυτή παίρνει ως δεδομένα ένα όνομα χρήστη, ένα συνθηματικό και μια ιστοσελίδα και παράγει σαν έξοδο ένα ψευδώνυμο και ένα συνθηματικό. Όταν, λοιπόν, ο χρήστης επισκεφθεί μια ιστοσελίδα που του ζητάει να δώσει κάποια στοιχεία, εκείνος πληκτρολογεί στα αντίστοιχα πεδία \u, \p, \@, οι οποίοι είναι χαρακτήρες διαφυγής. Αυτούς το LPWA τους αντιλαμβάνεται και δημιουργεί στον πληρεξούσιο εξυπηρετητή τα ψεύτικα στοιχεία εκ μέρους του χρήστη. Όταν ο χρήστης πληκτρολογεί \@, τότε η γεννήτρια παράγει μία ψεύτικη διεύθυνση αλληλογραφίας το σύστημα αποθηκεύει όλα τα εισερχόμενα μηνύματα και ένας user agent παραλαμβάνει τα μηνύματα για όλα τα ψευδώνυμα που ανήκουν σε έναν συγκεκριμένο χρήστη. Αυτός ο σχεδιασμός έχει το πλεονέκτημα ότι καμία

πληροφορία που μπορεί να απειλήσει την ιδιωτικότητα του χρήστη δεν αποθηκεύεται στο σύστημα e-mail. Η γεννήτρια παράγει διαφορετικές διευθύνσεις αλληλογραφίας για κάθε ιστοσελίδα που επισκέπτεται ο χρήστης, με αποτέλεσμα να επιτρέπει το αποτελεσματικό φιλτράρισμα των spam e-mails (smtp server).

Ο προωθητής των ηλεκτρονικών μηνυμάτων προωθεί τα μη spam μηνύματα στην πραγματική διεύθυνση του χρήστη. Ένα σημείο που θα πρέπει να προσεχθεί, είναι ότι επειδή η ψεύτικη διεύθυνση e-mail παράγεται από την κρυπτογράφηση της πραγματικής, ο προωθητής θα πρέπει να αποθηκεύει με ασφάλεια το μυστικό κλειδί της αποκρυπτογράφησης.

Υπάρχουν, βέβαια, και σοβαρά μειονεκτήματα στη χρήση του LPWA. Καταρχήν ο χρήστης θα πρέπει να εμπιστεύεται τον κεντρικό πληρεξούσιο. Άλλο μειονέκτημα είναι ότι επειδή στο συγκεκριμένο σχεδιασμό, η σύνδεση μεταξύ του περιηγητή του χρήστη και του πληρεξούσιου είναι δημόσια, συνεπάγεται ότι είναι και εύκολα παραβιάσιμη. Επίσης, ο χρόνος ανάκτησης των πληροφοριών από το διαδίκτυο μπορεί να είναι αρκετός, αφού κάθε αίτημα θα πρέπει να μεταφέρεται στο www.lpwa.com. Τέλος, το LPWA δεν φιλτράρει εφαρμογές Java και JavaScript από τις οποίες μπορεί να διαρρέουν πληροφορίες από τον περιηγητή στον εξυπηρετητή [45]

4.1.2 **Δυνατότητα ανωνυμίας στο διαδίκτυο (The onion router** – TOR)

Το Onion Routing είναι ένα κατανεμημένο σύστημα που έχει σχεδιαστεί ώστε να προσφέρει ανωνυμία σε εφαρμογές που βασίζονται σε συνδέσεις TCP, όπως η περιήγηση στο διαδίκτυο, η σύνδεση secure shell και το Instant messaging [46] και λειτουργεί στο επίπεδο της στρατολόγησης (routing). Ο client διαλέγει μία διαδρομή μέσα στο δίκτυο και ‘’χτίζει’’ ένα κύκλωμα, στο οποίο κάθε κόμβος γνωρίζει τον προηγούμενο και τον επόμενο, αλλά κανέναν άλλο. Πρόκειται για ένα πρόγραμμα λογισμικού σχεδιασμένο ώστε να εμποδίζει την ανάλυση της κίνησης, μέσω ενός δικτύου υπολογιστών που χρησιμοποιούν κρυπτογράφηση.Η πρόσβαση στο δίκτυο γίνεται δυνατή μέσω διακομιστών (proxies).

Μία αρχική εφαρμογή δημιουργεί μία σύνδεση (socket) σε έναν application proxy (πρόκειται για το σημείο εισόδου στο onion rooting). Ο proxy μετατρέπει τη μορφή του μηνύματος σύνδεσης σε μια γενική μορφή, η οποία να μπορεί να περάσει μέσα από το δίκτυο [47]. Στη συνέχεια συνδέεται με έναν onion proxy που ορίζει τη διαδρομή που θα ακολουθηθεί μέσα στο δίκτυο δημιουργώντας ένα πολυστρωματικό δίκτυο δεδομένων μέσω μιας σειράς onion δρομολογητών. Πριν την αποστολή των δεδομένων ο onion proxy εφοδιάζει κάθε onion δρομολογητή τόσο με την πληροφορία του ποιος θα είναι ο επόμενος δρομολογητής, όσο και με συμμετρικά κλειδιά κρυπτογράφησης για την αποκρυπτογράφηση των δεδομένων. Όσο το πακέτο μεταδίδεται μέσω της ανώνυμης σύνδεσης, κάθε δρομολογητής αποκωδικοποιεί το μήνυμα που προορίζεται γι αυτόν και μαθαίνει σε ποιον δρομολογητή να στείλει το πακέτο. Ο τελευταίος δρομολογητής οδηγεί το πακέτο προς την έξοδο της διαδρομής και στον παραλήπτη. Όταν ο παραλήπτης απαντήσει, ο τελευταίος δρομολογητής παραλαμβάνει το μήνυμα, το κρυπτογραφεί και το στέλνει πίσω με την ίδια διαδρομή. Κάθε κόμβος κρυπτογραφεί το μήνυμα με τον ίδιο τρόπο και το στέλνει πίσω. Μόλις το πακέτο φτάσει στον onion proxy αποκρυπτογραφείται.

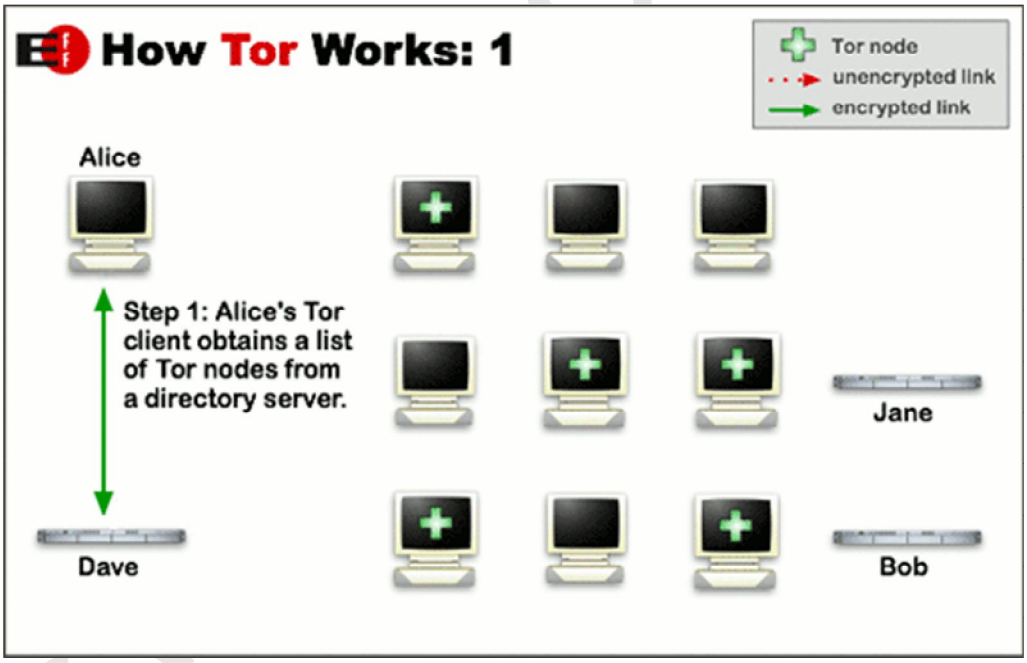
Το TOR [46] είναι ένα δίκτυο από εικονικά τούνελ που δίνει τη δυνατότητα βελτίωσης της ασφάλειας και της προστασίας της ιδιωτικότητας στο διαδίκτυο. Παρέχει τη βάση για ένα ευρύ φάσμα εφαρμογών που επιτρέπουν σε οργανισμούς και άτομα να μοιράζονται πληροφορίες μέσω δημοσίων δικτύων χωρίς να διακυβεύεται η ιδιωτικότητά τους.

Η χρήση του TOR προστατεύει από ένα γνωστό είδος διαδικτυακής παρακολούθησης, γνωστό ως ‘’traffic analysis’’, το οποίο χρησιμοποιείται για να συμπεράνει ποιος μιλάει με ποιον σε ένα δημόσιο δίκτυο. Η γνώση της προέλευσης και του προορισμού της διαδικτυακής μας κίνησης δίνει την δυνατότητα σε επιτήδειους να παρακολουθήσουν τη συμπεριφορά και τα ενδιαφέροντά μας. Πώς λειτουργεί, όμως, η ανάλυση της κίνησης; Τα πακέτα δεδομένων στο διαδίκτυο αποτελούνται από δύο μέρη: το φορτίο των δεδομένων (data payload) και μια κεφαλίδα (header) που χρησιμοποείται για την δρομολόγηση. Ακόμα και να έχουμε κρυπτογραφήσει το φορτίο των δεδομένων μας, η ανάλυση κίνησης μπορεί να αποκαλύψει

πολλά γι αυτά που κάνουμε και ενδεχομένως και για αυτά που λέμε. Και αυτό γιατί το ενδιαφέρον εστιάζεται στην κεφαλίδα, η οποία αποκαλύπτει την πηγή, τον προορισμό, το μέγεθος, το χρονοδιάγραμμα κοκ.

Το βασικό πρόβλημα για την προστασία της ιδιωτικότητας εστιάζεται στο ότι ο παραλήπτης της επικοινωνίας μπορεί να δει τι στείλαμε απλώς κοιτάζοντας τις κεφαλίδες. Το ίδιο, όμως, μπορεί να κάνει και ο πάροχος των υπηρεσιών διαδικτύου όπως και μη εξουσιοδοτημένες τρίτες οντότητες. Μπορεί, λοιπόν, κάποιος πολύ απλά να εγκατασταθεί ανάμεσα στον αποστολέα και τον παραλήπτη και να παρακολουθεί απλώς τις κεφαλίδες. Υπάρχουν, βέβαια, και πιο εξελιγμένες μορφές ανάλυσης κίνησης όπου ο επιτιθέμενος χρησιμοποιεί στατιστικές μεθόδους για να εντοπίσει τα πρότυπα (patterns) επικοινωνίας ατόμων και οργανισμών. Η κρυπτογράφηση, δυστυχώς, σε αυτήν την περίπτωση δεν μπορεί να συμβάλλει στην προστασία από τους επιτιθέμενους αφού αποκρύπτει μόνο το περιεχόμενο της επικοινωνίας και όχι τις κεφαλίδες.

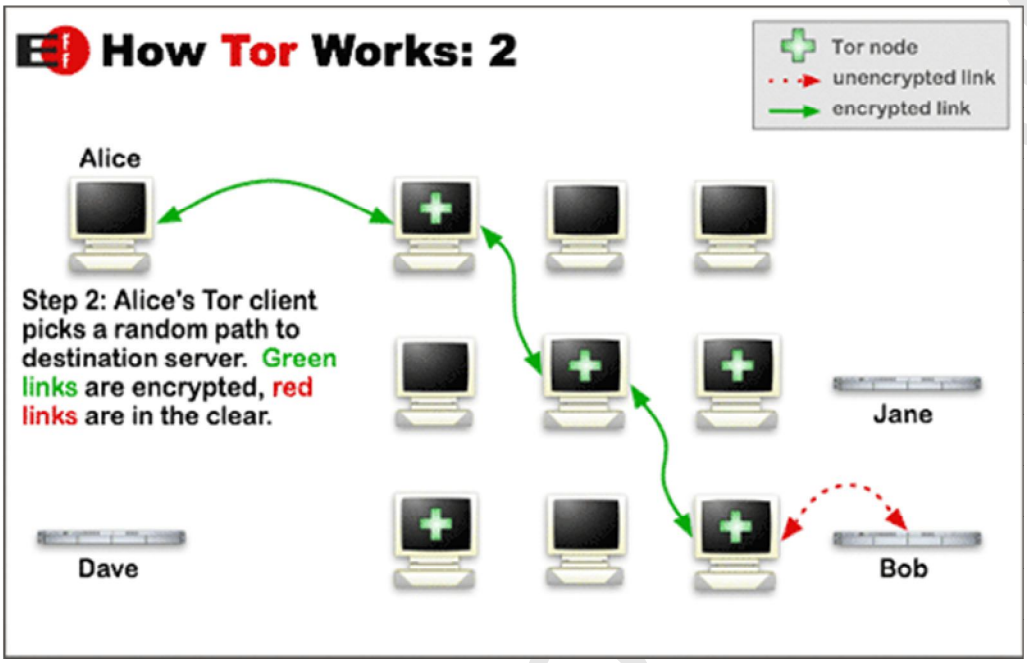
Το TOR μειώνει τους κινδύνους τόσο από την απλή όσο και την πιο εξειδικευμένη ανάλυση κίνησης με το να ‘‘κατανέμει’’ την επικοινωνία σε διάφορα σημεία του διαδικτύου έτσι ώστε κανένα μεμονωμένο σημείο να μην μπορεί να συνδέσει την προέλευση με τον προορισμό. Για να δημιουργηθεί ένα ιδιωτικό μονοπάτι με το TOR, το λογισμικό του χρήστη ‘‘χτίζει’’ σταδιακά ένα κύκλωμα κρυπτογραφημένων συνδέσεων μέσω μεταβιβαστών (relays) στο δίκτυο. Το κύκλωμα επεκτείνεται έναν κόμβο κάθε φορά και ο κάθε μεταβιβαστής γνωρίζει μόνο τον προηγούμενο και τον επόμενο από αυτόν. Κανένας μεταβιβαστής δεν γνωρίζει την πλήρη διαδρομή που θα ακολουθήσει το πακέτο δεδομένων. Ο χρήστης απ’ τη μεριά του διαπραγματεύεται κάθε φορά με κάθε κόμβο ένα διαφορετικό σύνολο κλειδιών κρυπτογράφησης ώστε να εξασφαλίσει ότι κανένας κόμβος δεν θα μπορέσει να εντοπίσει τις κρυπτογραφημένες αυτές συνδέσεις.



Εικόνα 1 Πώς λειτουργεί το TOR (Πηγή: www.torproject.org)

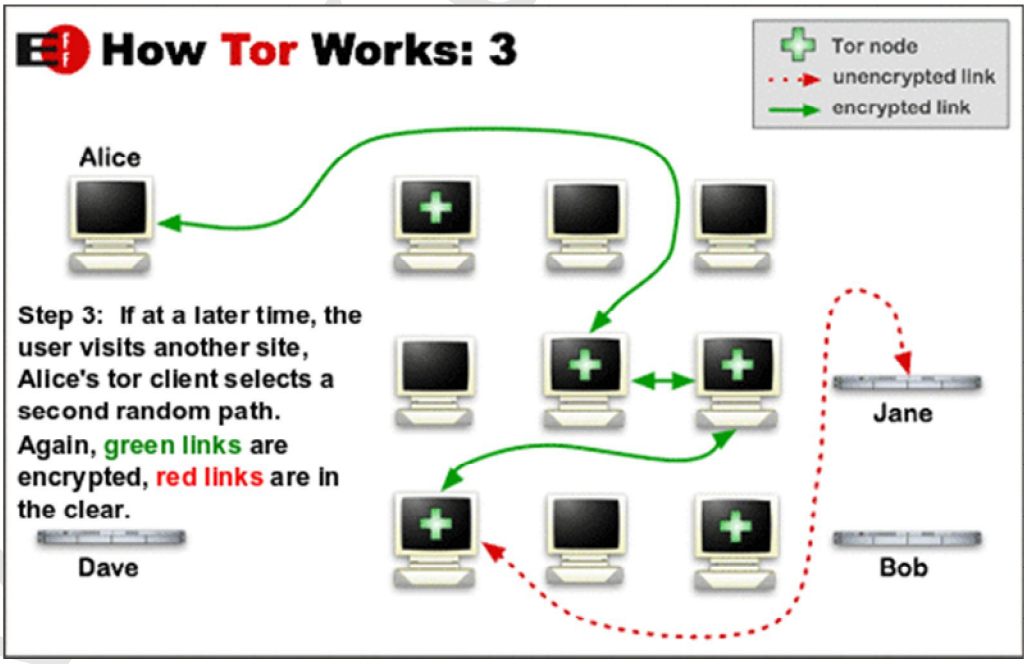
Μόλις ένα κύκλωμα εγκατασταθεί μπορεί να γίνει ανταλλαγή πολλών ειδών δεδομένων καθώς και ανάπτυξη πολλών ειδών εφαρμογών λογισμικού. Επειδή κάθε μεταβιβαστής δεν μπορεί να δει πάνω από έναν κόμβο στο κύκλωμα, αυτό σημαίνει ότι ούτε ένας ωτακουστής αλλά ούτε κι ένας μεταβιβαστής που έχει παραβιαστεί μπορούν να χρησιμοποιήσουν την ανάλυση κίνησης για να συνδέσουν την πηγή της σύνδεσης με τον προορισμό. Το TOR

λειτουργεί μόνο για TCP streams και μπορεί να χρησιμοποιηθεί από οποιαδήποτε εφαρμογή με υποστήριξη SOCKS.



Εικόνα 2 Πώς λειτουργεί το TOR (Πηγή: www.torproject.org)

Για καλύτερη αποτελεσματικότητα, το TOR χρησιμοποιεί το ίδιο κύκλωμα που δημιουργήθηκε τα τελευταία δέκα λεπτά. Δηλαδή, αιτήσεις που θα γίνουν σε μεταγενέστερο χρόνο θα δημιουργήσουν ένα καινούργιο κύκλωμα προκειμένου να αποτρέψουν τη σύνδεση των προηγούμενων ενεργειών μας με τις καινούργιες.



Εικόνα 3 Μία περιγραφή του δικτύου TOR (Πηγή: www.torproject.org)

Η διαφορά, λοιπόν, του TOR από τους άλλους proxy providers είναι ότι ένας κοινός proxy τοποθετεί έναν server κάπου στο διαδίκτυο και επιτρέπει να τον χρησιμοποιήσουμε για να ελέγχει την κίνηση. Αυτό δημιουργεί μια απλή, εύκολη στη συντήρηση αρχιτεκτονική. Όλοι οι χρήστες εισέρχονται και αποχωρούν μέσω του ίδιου server. Ο provider μπορεί να προχωρήσει σε χρεώσεις για τη χρήση του proxy ή να χρηματοδοτεί το κόστος του μέσω διαφημίσεων στο server. Στο πιο απλό configuration δεν χρειάζεται να εγκαταστήσουμε τίποτα. Απλώς να ‘’δείξουμε’’ στον browser τον proxy. Μερικοί απλοί proxy providers χρησιμοποιούν SSL για να προστατέψουν τη σύνδεση σε αυτούς. Άλλοι δημιουργούν ένα ενιαίο σημείο αποτυχίας. Ο provider γνωρίζει ποιος είσαι και πού περιηγείσαι στο Internet. Μπορεί να δει την κίνηση καθώς αυτή περνάει μέσα από τον server του.

Ο TOR περνάει την κίνηση μέσα από τουλάχιστον 3 servers πριν τη στείλει στον προορισμό της. Επειδή υπάρχει ένα διαφορετικό επίπεδο κρυπτογράφησης για κάθε έναν από τους τρεις μεταβίβαστές, ο TOR ούτε τροποποιεί, και ίσως ούτε γνωρίζει τι στέλνουμε.

4.2 **Προστασία της ιδιωτικότητας στην πλευρά του εξυπηρετητή** (server-side)

4.2.1 **Απομακρυσμένη ασφαλής πρόσβαση μέσω ιδιωτικού εικονικού δικτύου** (Virtual Private Network – VPN)

Ένα εικονικό ιδιωτικό δίκτυο (VPN) είναι ένα ιδιωτικό δίκτυο που χρησιμοποιεί τη δημόσια τηλεπικοινωνιακή υποδομή, προκειμένου να παράσχει ασύρματη πρόσβαση στο κεντρικό δίκτυο που επιθυμεί ο χρήστης. Ο όρος ‘’ιδιωτικό δίκτυο’’ σημαίνει ότι πρόσβαση σε αυτό έχουν μόνο οι εξουσιοδοτημένοι χρήστες, ενώ ο όρος ‘’εικονικό’’ σημαίνει ότι τα δεδομένα που αποστέλλονται μπορεί κάθε φορά να ακολουθούν διαφορετική διαδρομή για να φτάσουν στον προορισμό τους.

Τα VPNs κατηγοριοποιούνται ως εξής:

- Αν τα αντιστοιχίσουμε με τα επίπεδα του μοντέλου αναφοράς OSI, τότε έχουμε

i. Τα εικονικά ιδιωτικά δίκτυα επιπέδου 3 (δικτύου). Εδώ ανήκουν τα εικονικά δίκτυα που δομούνται πάνω σε IP δίκτυα και χρησιμοποιούν το πρωτόκολλο IPSec, καθώς και αυτά που δομούνται πάνω σε MPLS δίκτυα.

ii. Τα εικονικά ιδιωτικά δίκτυα επιπέδου 2 (ζεύξης δεδομένων). Τα VPNs αυτής της κατηγορίας χρησιμοποιούν τα πρωτόκολλα L2F, PPTP,L2TP.

iii. Τα εικονικά ιδιωτικά δίκτυα επιπέδου 4 (μεταφοράς). Σ’ αυτήν την κατηγορία χρησιμοποιούν το πρωτόκολλο SSL.

- Με βάση το νοητό κύκλωμα που σχηματίζεται κατά τη μετάδοση των δεδομένων (δίοδος ή tunnel)
  i. Αυθόρμητες δίοδοι (voluntary tunnels)
  ii. Αναγκαστικές δίοδοι (compulsory tunnels ή mandatory tunnels)

- Με βάση ποιοι είναι οι χρήστες του VPN:

i. Το VPN δομής ‘’πελάτης- προς- δίκτυο’’ (client-to-LAN) όπου ένας χρήστης συνδέεται με το τοπικό δίκτυο.

ii. Το VPN δομής ‘’δίκτυο- προς- δίκτυο’’ (LAN-to-LAN), όπου τα δεδομένα ανταλλάσσονται μεταξύ δύο τοπικών δικτύων.

Ένα καλά σχεδιασμένο VPN δίκτυο χρησιμοποιεί διάφορες μεθόδους για να διατηρεί τα δεδομένα ασφαλή [48].

- Firewalls: Αποτελεί ένα σημαντικό εμπόδιο ανάμεσα στο ιδιωτικό δίκτυο και το Internet. Μπορούν να ρυθμιστούν έτσι ώστε να περιορίζουν τον αριθμό των ανοιχτών θυρών, να ελέγχουν το είδος των πακέτων που επιτρέπεται να περάσουν μέσα στο LAN ακόμα και το είδος των επιτρεπόμενων πρωτοκόλλων.

- Κρυπτογράφηση: Χρησιμοποιούν κρυπτογράφηση συμμετρικού κλειδιού (βασίζεται στην ύπαρξη ενός και μόνο κλειδιού τόσο για την κρυπτογράφηση όσο και για την αποκρυπτογράφηση του μηνύματος, το οποίο θα πρέπει να είναι γνωστό μόνο στα συναλλασσόμενα μέρη) ή κρυπτογράφηση δημοσίου κλειδιού (ο αποστολέας και ο παραλήπτης δεν μοιράζονται ένα μυστικό κοινό κλειδί αλλά διαθέτουν διαφορετικά κλειδιά για διαφορετικές λειτουργίες.)
- Internet Protocol Security (IPSec): παρέχει καλύτερους αλγόριθμους κωδικοποίησης και πιο εύκολη πιστοποίηση. Το IPSec έχει δύο μεθόδους πιστοποίησης: το tunnel και το transport. Η πρώτη μέθοδος κρυπτογραφεί μόνο την επικεφαλίδα κάθε πακέτου και το φορτίο του, ενώ η δεύτερη μόνο το φορτίο του. Το πρωτόκολλο αυτό μπορούν να το εκμεταλλευτούν μόνο συσκευές συμβατές με αυτό ενώ όλες οι συσκευές πρέπει να χρησιμοποιούν ένα κοινό κλειδί και τα firewalls να έχουν παρόμοιες πολιτικές ασφαλείας. Το IPSec μπορεί να κρυπτογραφήσει διάφορες συσκευές, όπως:
    - Router προς router
    - Firewall προς router
    - Υπολογιστή προς router
    - Υπολογιστή προς server
- Εξυπηρετητές AAA (authentication, authorization and accounting). Οι εξυπηρετητές αυτοί χρησιμοποιούνται για ακόμα πιο ασφαλή πρόσβαση σε απομακρυσμένα περιβάλλοντα VPN. Όταν λαμβάνεται μία αίτηση από κάποιον πελάτη για δημιουργία καινούργιας συνεδρίας μέσω τηλεφώνου, η αίτηση προωθείται από τον διαμεσολαβητή στον AAA εξυπηρετητή, ο οποίος ελέγχει τα ακόλουθα:
    - Ποιος είναι ο αιτών (αυθεντικοποίηση)
    - Τί δικαιώματα έχει (εξουσιοδότηση)
    - Ποιες είναι οι πραγματικές ενέργειες που θέλει να πραγματοποιήσει (έλεγχος)

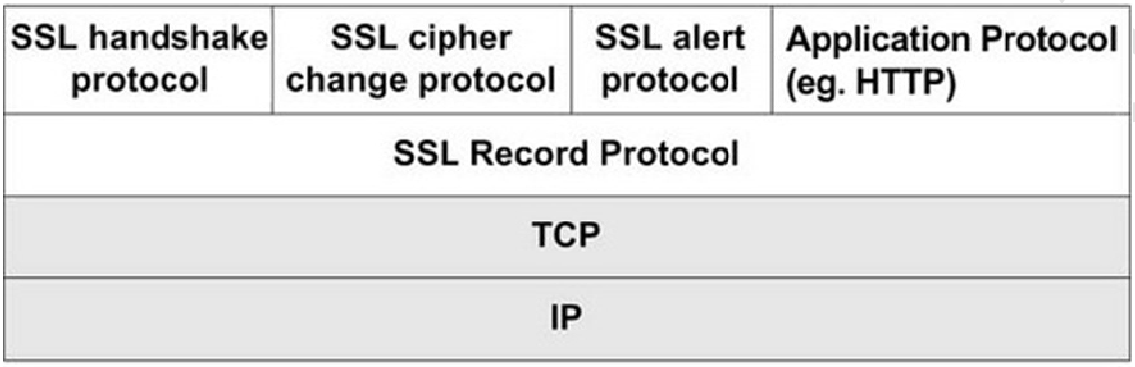
4.2.2 **Κρυπτογράφηση επικοινωνίας – Το πρωτόκολλο SSL (Secure Sockets Layer)**

Το SSL (Secure Socket Layer) είναι ένα κρυπτογραφικό πρωτόκολλο για την προστασία της επικοινωνίας στο Διαδίκτυο μεταξύ δύο συστημάτων εκ των οποίων το ένα λειτουργεί ως client και το άλλο ως server. Πρόκειται για ένα μικρό κομμάτι κώδικα με δύο βασικές λειτουργίες [49]:

Α) Αυθεντικοποίηση και Επαλήθευση χρήστη. Το πρωτόκολλο διαθέτει λεπτομέρειες σχετικά με την αυθεντικότητα συγκεκριμένων πληροφοριών που αφορούν την ταυτότητα του προσώπου, της επιχείρησης ή της ιστοσελίδας, οι οποίες θα εμφανίζονται στους επισκέπτες της ιστοσελίδας κάθε φορά που εκείνοι κάνουν κλικ στο σήμα εμπιστοσύνης του browser.

Β) Κρυπτογράφηση δεδομένων. Οι ευαίσθητες πληροφορίες που μεταδίδονται μέσω διαδικτύου δεν μπορούν να υποκλαπούν και να διαβαστούν από κανέναν άλλο πέραν του αποδέκτη.

Αποτελείται από 2 επίπεδα πρωτοκόλλων.



Εικόνα 4 Η αρχιτεκτονική του πρωτοκόλλου SSL (πηγή www.windowsecurity.com)

Το SSL Record Protocol, το οποίο διασφαλίζει την εμπιστευτικότητα μέσω της κρυπτογράφησης των δεδομένων. Εγκαθιδρύει ένα μοναδικό συμμετρικό κλειδί που χρησιμοποιείται για να παράγει τα κλειδιά για την κρυπτογράφηση και αποκρυπτογράφηση των δεδομένων. Το μήνυμα συμπιέζεται πριν κρυπτογραφηθεί και οι αλγόριθμοι που χρησιμοποιούνται για την κρυπτογράφησή του είναι AES,IDEA,RC2-40, DES-40 κ.α. Για τη διασφάλιση της ακεραιότητας του μηνύματος χρησιμοποιείται ένα πρωτόκολλο MAC με ένα κοινό μυστικό κλειδί. Για να χρησιμοποιηθεί το SSL, πρέπει Server και Client να γνωρίζουν ότι η άλλη πλευρά χρησιμοποιεί υπηρεσίες SSL.

Έχουν καθοριστεί ξεχωριστοί αριθμοί θυρών για κάθε πρωτόκολλο εφαρμογής με υποστήριξη SSL.

Keyword	Port	Description
https	443	HTTP με υποστήριξη SSL
Ssmtp	465	SMTP με υποστήριξη SSL
Snntp (παλιό)	563	NNTP με υποστήριξη SSL
sldap	636	LDAP με υποστήριξη SSL
spop3	995	POP3 με υποστήριξη SSL

Εικόνα 5 Αριθμοί θυρών (Πηγή www.iana.org)

Στο επόμενο επίπεδο, βρίσκεται το SSL Change Cipher Spec Protocol. Πρόκειται για το πιο απλό πρωτόκολλο και αποτελείται από ένα μόνο μήνυμα του ενός byte και σκοπό έχει να επικαιροποιήσει τον κρυπτογραφικό αλγόριθμο που χρησιμοποιείται. Το δεύτερο πρωτόκολλο αυτού του επιπέδου είναι το SSL Alert Protocol, το οποίο μεταφέρει προειδοποιήσεις σχετικές με το SSL στην ομόλογη οντότητα (peer entity). Τέλος, υπάρχει το SSL Handshake Protocol, το οποίο επιτρέπει σε client και server να πιστοποιήσουν ο ένας την ταυτότητα του άλλου (μέσω ψηφιακών πιστοποιητικών που εκδίδονται από τις Αρχές Έκδοσης Πιστοποιητικών-Certificates Authorities-CA), να διαπραγματευτούν ποιοι αλγόριθμοι κρυπτογράφησης και MAC θα χρησιμοποιηθούν καθώς και να διαπραγματευτούν για τα κρυπτογραφικά κλειδιά που θα χρησιμοποιηθούν [50].

Η χρήση του πρωτοκόλλου SSL αυξάνει τα διακινούμενα πακέτα μεταξύ των δύο μηχανών και καθυστερεί την μετάδοση των πληροφοριών επειδή χρησιμοποιεί μεθόδους κρυπτογράφησης και αποκρυπτογράφησης. Ειδικότερα οι διάφορες καθυστερήσεις εντοπίζονται στα εξής σημεία:

- Στην αρχική διαδικασία χειραψίας όπου κανονίζονται οι λεπτομέρειες της σύνδεσης και ανταλλάσσονται τα κλειδιά της συνόδου.
- Στην διαδικασία κρυπτογράφησης και αποκρυπτογράφησης που γίνεται στους δύο υπολογιστές με αποτέλεσμα να δαπανώνται υπολογιστικοί πόροι και χρόνος.
- Στην καθυστέρηση μετάδοσης των κρυπτογραφημένων δεδομένων αφού αυτά αποτελούνται από περισσότερα bytes σε σχέση με την αρχική μη κρυπτογραφημένη πληροφορία.

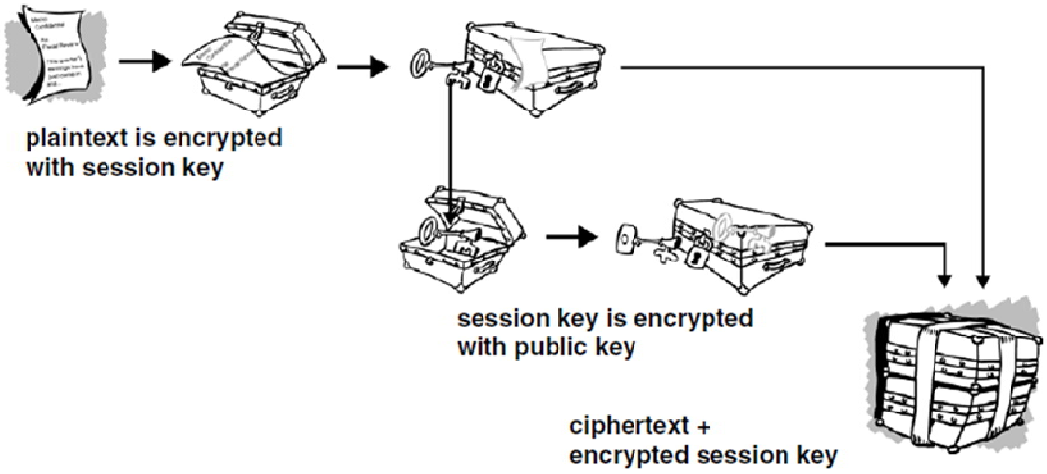
Λόγω αυτών των επιβαρύνσεων που εισάγει το πρωτόκολλο SSL, χρησιμοποιείται πλέον μονάχα σε περιπτώσεις όπου πραγματικά χρειάζεται ασφαλής σύνδεση (πχ μετάδοση κωδικών χρήστη ή αριθμών πιστωτικών καρτών μέσω του διαδικτύου) και όχι σε περιπτώσεις απλής επίσκεψης σε μία ιστοσελίδα.

4.3 Κοινά μέτρα προστασίας της ιδιωτικότητας

4.3.1 Κρυπτογράφηση δεδομένων – Το λογισμικό κρυπτογράφησης PGP (Pretty Good Privacy)

Το PGP (Pretty Good Privacy) [51] δημιουργήθηκε από τον Phillip Zimmerman και πρόκειται για ένα υβριδικό σύστημα κρυπτογράφησης που συνδυάζει μερικά από τα καλύτερα χαρακτηριστικά γνωρίσματα τόσο της κλασικής κρυπτογραφίας όσο και της κρυπτογραφίας δημοσίου κλειδιού [51]. Ο στόχος του Zimmerman ήταν να δημιουργήσει ένα λογισμικό ισχυρής κρυπτογράφησης διαθέσιμο για όλους τους χρήστες, χρησιμοποιώντας ήδη γνωστούς και αναγνωρισμένους αλγορίθμους κρυπτογραφίας. Με αυτό τον τρόπο θα ήταν δυνατή η προστασία της εμπιστευτικότητας των δεδομένων κάθε χρήστη, σε μία εποχή που ακόμη υπήρχαν περιορισμοί στην ανοικτή χρήση του λογισμικού κρυπτογράφησης, Κατά την κρυπτογράφηση ενός αρχικού κειμένου με το PGP, αυτό προχωρά αρχικά στη συμπίεση του αρχείου. Με τον τρόπο αυτό εξοικονομείται και χρόνος μετάδοσης και χώρος στο δίσκο ενώ παράλληλα ενισχύεται η κρυπτογραφική ασφάλεια. Οι περισσότερες τεχνικές κρυπτανάλυσης εκμεταλλεύονται τα πρότυπα που υπάρχουν μέσα στο απλό κείμενο για να σπάσουν τον αλγόριθμο. Η συμπίεση μειώνει αυτά τα πρότυπα ενισχύοντας έτσι σε μεγάλο βαθμό την αντίσταση στην κρυπτανάλυση.

Το PGP τότε δημιουργεί ένα κλειδί κρυπτογράφησης, το οποίο είναι μοναδικό και δημιουργείται μόνο για αυτή τη συνεδρία (session key). Με έναν πολύ ασφαλή αλγόριθμο κρυπτογράφησης χρησιμοποιείται για την κρυπτογράφηση του κειμένου. Το αποτέλεσμα είναι το ciphertext (κρυπτογραφημένο κείμενο). Στη συνέχεια το κλειδί συνόδου κρυπτογραφείται με το δημόσιο κλειδί του παραλήπτη. Τα δύο αυτά κλειδιά, μαζί με το κρυπτοκείμενο αποστέλλονται στον παραλήπτη.Θα πρέπει εδώ να σημειώσουμε ότι τα symmetric block ciphers (τα συμμετρικά δηλ. κρυπτοσυστήματα όπου η κρυπτογράφηση γίνεται ανά block) που χρησιμοποιούνται από το PGP είναι ο CAST, ο 3-DES, ο IDEA και ο Twolfish [51]. Οι τρεις πρώτοι λειτουργούν σε μπλοκ των 64 bits απλού κα κρυπτογραφημένου κειμένου. Ο CAST και ο IDEA έχουν μήκος κλειδιού 128 bits ενώ ο 3-DES χρησιμοποιεί κλειδί 168 bits. Ο Twolfish ανήκει στους πέντε κορυφαίους αλγορίθμους του προγράμματος NIST Advanced Encryption Standard (AES) project.



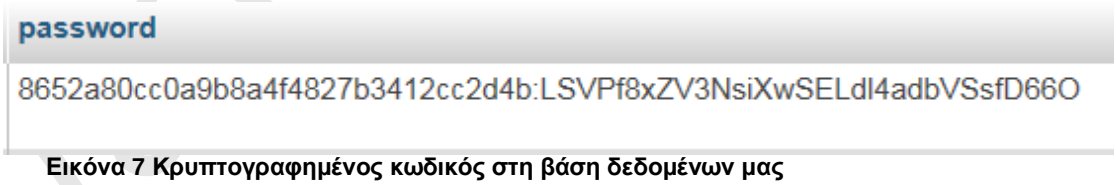
Εικόνα 6 Κρυπτογράφηση με PGP (Πηγή www.pgp.org ''An introduction to cryptography-June 2004'')

Η αποκρυπτογράφηση λειτουργεί αντίστροφα. Το αντίγραφο PGP του παραλήπτη χρησιμοποιεί το ιδιωτικό κλειδί του προκειμένου να αποκτήσει το κλειδί συνόδου με το οποίο θα αποκρυπτογραφήσει το κείμενο.

Οι δύο αυτές μέθοδοι συνδυάζουν την άνεση της κρυπτογραφίας δημοσίου κλειδιού, η οποία δίνει λύσεις σε θέματα μετάδοσης των δεδομένων, με την ταχύτητα της συμβατικής κρυπτογραφίας, η οποία είναι 10000 φορές ταχύτερη.

4.3.2 Κρυπτογράφηση με μηχανισμούς που υποστηρίζει η βάση δεδομένων μας.

Μία άλλη μέθοδος κρυπτογράφησης που μπορεί να εφαρμοστεί, είναι μέσω μηχανισμών που υποστηρίζει η βάση δεδομένων μας. Στην παρούσα εργασία έχουμε εγκαταστήσει το Joomla και χρησιμοποιεί το phpMy Admin.Αν κοιτάξουμε προσεκτικά τους κωδικούς πρόσβασης που αποθηκεύει η βάση, θα διαπιστώσουμε ότι αυτοί είναι κρυπτογραφημένοι με μια συνάρτηση κατακερματισμού (συγκεκριμένα με την MD5). Οι συναρτήσεις αυτές δέχονται ως είσοδο μια αυθαίρετου μεγέθους ομάδα δεδομένων και δίνουν ως έξοδο μια καθορισμένου μεγέθους συμβολοσειρά (string) πολύ μικρότερη από τη είσοδο. Στο Joomla οι κωδικοί πρόσβασης πριν κατατεμαχιστουν αναμειγνύονται (salted) με τυχαία bits που χρησιμεύουν ως μία από τις εισόδους της κρυπτογραφικής συνάρτησης. Η τελική μορφή με την οποία αποθηκεύονται οι κωδικοί είναι {hash}:{salt}.



Εικόνα 7 Κρυπτογραφημένος κωδικός στη βάση δεδομένων μας

4.3.3 **Πλατφόρμα προστασίας ιδιωτικότητας δεδομένων** P3P

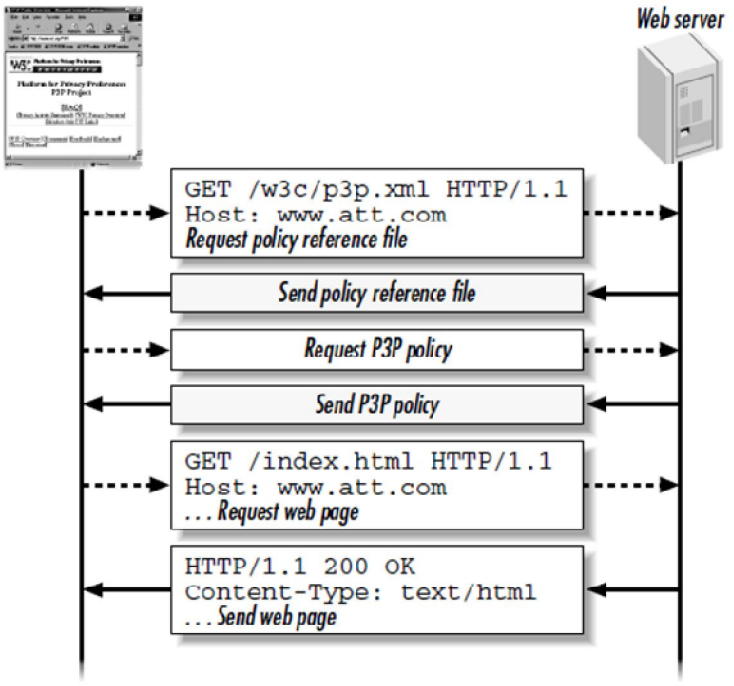
Η κοινοπραξία World Wide Web Consortium, της οποίας στόχος είναι ‘’να οδηγήσει το διαδίκτυο στο μέγιστο των δυνατοτήτων του δημιουργώντας πρωτόκολλα που προάγουν την εξέλιξή του και εξασφαλίζουν την λειτουργικότητά του’’, δημιούργησε το 1997 το πρωτόκολλο για τις προτιμήσεις ασφάλειας ή αλλιώς Platform for Privacy Preferences Project (P3P) [52]. Κύριος στόχος είναι να επιτρέψει στις ιστοσελίδες να παρουσιάσουν τις πρακτικές που ακολουθούν για τη συλλογή δεδομένων με έναν τυποποιημένο τρόπο και αφετέρου να διευκολύνει το χρήστη να κατανοήσει ποια δεδομένα του θα συλλεχθούν από τις ιστοσελίδες τις οποίες επισκέπτεται, πώς αυτά θα χρησιμοποιηθούν καθώς και τη δυνατότητα που έχει να συναινέσει στη συλλογή τους ή όχι [53].

Μπορούμε να το θεωρήσουμε σαν εργαλείο ‘’ενδυνάμωσης’’ του χρήστη, το οποίο δημιουργεί μια αυτόματη ‘’χειραψία που εγγυάται την προστασία της ιδιωτικότητας’’ (privacy handshake) μεταξύ των ιστοσελίδων και των browsers. Αυτοί οι διάλογοι σκοπό έχουν να αντιπαραβάλλουν τις πολιτικές για την προστασία της ιδιωτικότητας που ακολουθεί η ιστοσελίδα με τις απαιτήσεις του χρήστη. Στοιχεία της προδιαγραφής P3P είναι [54]:

- **P3P policies (Πολιτικές P3P):** Πρόκειται για την πολιτική προστασίας της ιδιωτικότητας που ακολουθεί η ιστοσελίδα, γραμμένη σε γλώσσα XML και χρησιμοποιώντας το αντίστοιχο λεξιλόγιο, προκειμένου να προβάλλει τις πρακτικές ιδιωτικότητας που ακολουθεί. Η συγκεκριμένη γλώσσα μπορεί να συλλάβει κοινά στοιχεία στις πολιτικές προστασίας αλλά όχι όλα (οι διάφορες ιστοσελίδες μπορεί να παρέχουν περαιτέρω επεξηγήσεις σε πιο εξειδικευμένη μορφή).
- **P3P clients (P3P πελάτες):** Μπορεί να είναι browsers, proxies, plug-ins, java applets, Java Scripts κα και να βρίσκεται εξ ολοκλήρου σε server side ή να είναι μέρος μιας ενδιάμεσης υπηρεσίας, ενός toolbar κ.α. Οι P3P πελάτες στέλνουν ένα αίτημα HTTP GET request, ελέγχουν την πολιτική και προχωρούν στις απαραίτητες ενέργειες, που μπορεί να περιλαμβάνουν την εμφάνιση ενός συμβόλου, έναν συγκεκριμένο ήχο ή την προτροπή του χρήστη να αναλάβει δράση (π.χ. αποδοχή, απόρριψη κλπ).
- **Προτιμήσεις απορρήτου που καθορίζονται από το χρήστη:** Οι συνομιλητές (browsers, agents) μπορούν να αναλάβουν δράση βασισμένοι στις προτιμήσεις του χρήστη (καλό θα ήταν ο χρήστης να μην εμπιστεύεται τις by default ρυθμίσεις του προμηθευτή). Επιπλέον αν είναι σε θέση να διαβάσουν τα αρχεία APPEL, τότε μπορούν να προσφέρουν μια πλειάδα προκαθορισμένων επιλογών που έχουν αναπτυχθεί από έμπιστες τρίτες οντότητες (TTPs).
- **Το λεξιλόγιο του P3P:** Αποτελείται από 8 βασικά συστατικά (components), αρκετά από τα οποία αποτελούνται από δευτερεύοντα στοιχεία και χαρακτηριστικά [55]:
  - Entity (οντότητα): Περιλαμβάνει πληροφορίες για την επιχείρηση ή το πρόσωπο στο οποίο ανήκει η ιστοσελίδα.
  - Access (πρόσβαση): Καθορίζει το βαθμό πρόσβασης που θα έχει ο χρήστης στα προσωπικά δεδομένα που συλλέγει η ιστοσελίδα και τον αφορούν. Υπάρχουν 6 διαφορετικοί βαθμοί πρόσβασης.
  - Disputes (διαφωνίες): Περιγράφει τον τρόπο επίλυσης των διαφορών μεταξύ της ιστοσελίδας και του χρήστη και περιλαμβάνει το υποστοιχείο remedies που αφορά τα διορθωτικά μέτρα που μπορούν να ληφθούν.
  - Data (δεδομένα): Καταγραφή των δεδομένων που συλλέγονται.
  - Purpose (σκοπός χρήσης): Παρουσιάσει τον τρόπο με τον οποίο χρησιμοποιούνται τα δεδομένα που συλλέγονται και αν οι χρήστες μπορούν να συγκατατεθούν ή όχι στη χρήση τους.
  - Recipient (παραλήπτης): Αναφέρει κατά πόσο και υπό ποιες συνθήκες τα δεδομένα μπορούν να διαμοιραστούν σε τρίτους, καθώς και αν υπάρχει η δυνατότητα συναίνεσης του υποκειμένου.
  - Retention (διατήρηση δεδομένων): Αναφέρει το χρόνο διατήρησης των συλλεχθέντων δεδομένων.

- Consequence (συνέπεια): Παρουσιάζει μία επεξήγηση όλων των πρακτικών που ακολουθούνται σε ευανάγνωστη μορφή.

Η πλατφόρμα συνήθως αποτελείται από απαντήσεις σε ερωτήσεις πολλαπλής επιλογής και έτσι εμπεριέχει πάντοτε λεπτομερείς πληροφορίες, όπως μια πολιτική σε πιο ευανάγνωστη μορφή (σε απλό κείμενο). Περιλαμβάνει επίσης ένα πρωτόκολλο για την υποβολή αίτησης και διαβίβασης των πολιτικών P3P (P3P policies). Το πρωτόκολλο αυτό είναι βασισμένο στο ίδιο πρωτόκολλο HTTP που χρησιμοποιούν οι web browsers για να επικοινωνήσουν με τους web servers.



Εικόνα 8 Βασικό πρωτόκολλο για την εύρεση της P3P Policy (Πηγή www.oreillynet.com)

Όπως φαίνεται από την παραπάνω εικόνα οι user agents στέλνουν HTTP αιτήματα προκειμένου να φέρουν το αρχείο αναφοράς της πολιτικής (policy reference file) που ακολουθείται και βρίσκεται σε γνωστή τοποθεσία στην ιστοσελίδα που γίνεται το αίτημα. Μπορεί για ολόκληρη την ιστοσελίδα να υπάρχει μόνο μία πολιτική ή αρκετές κάθε μία από τις οποίες καλύπτει διαφορετικό τμήμα της ιστοσελίδας. Ο user agent φέρνει την κατάλληλη πολιτική, την αναλύει και δρα ανάλογα με τις προτιμήσεις του χρήστη [56]. Υπάρχει, επίσης, η δυνατότητα να τοποθετηθεί το αρχείο αναφοράς σε άλλη τοποθεσία με την μόνη υποχρέωση να δηλωθεί αυτή χρησιμοποιώντας μια HTTP header ή ενσωματώνοντας ένα link στο HTML αρχείο. Ειδικά HTTP headers χρησιμοποιούνται για τη δήλωση μιας περιεκτικής πολιτικής (compact policy) που περιγράφει συνοπτικά την πρακτική που ακολουθείται σχετικά με τα cookies.

ΚΕΦΑΛΑΙΟ 5ο

Μελέτη περίπτωσης - Εφαρμογή τεχνολογιών PET σε διαδικτυακή εφαρμογή

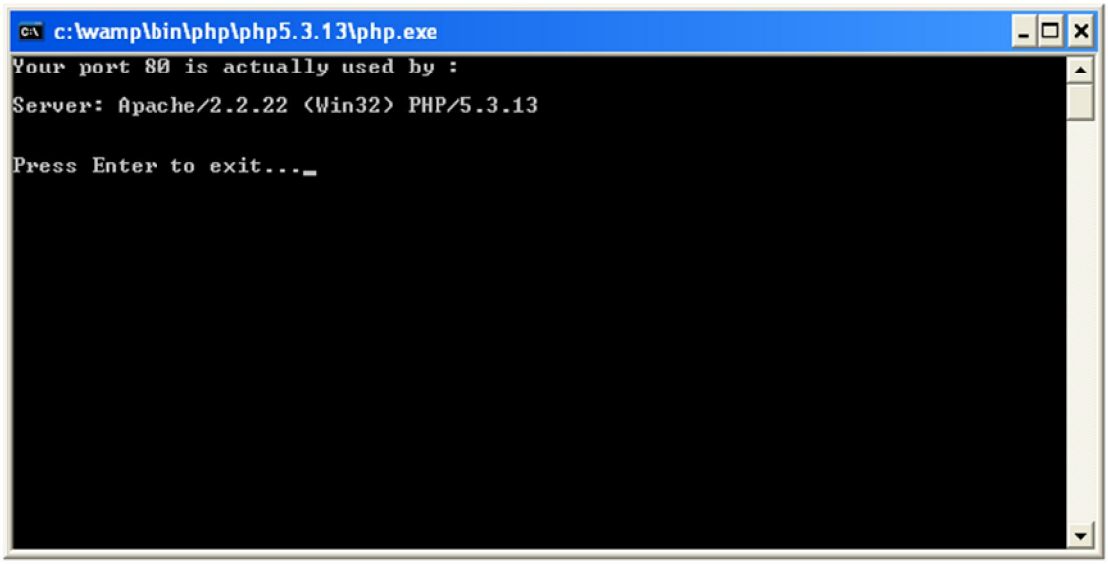
Στην παρούσα εργασία θα επιχειρήσουμε να δημιουργήσουμε μια διαδικτυακή εφαρμογή (μία ιστοσελίδα) στην οποία θα εφαρμόσουμε τεχνολογίες PET προκειμένου να διαπιστώσουμε την ασφάλεια που μας παρέχουν σε μια πιθανή επίθεση ωτακουστή. Τα βήματα, λοιπόν, που θα ακολουθήσουμε αφορούν την εγκατάσταση του server μας, τη δημιουργία της ιστοσελίδας, την εγκατάσταση του SSL certificate Καθώς και την μετατροπή του server μας σε forward proxy.

5.1 Εγκατάσταση Wamp και λήψη αρχειων Joomla

Ο WAMP είναι ένας server, ο οποίος μας επιτρέπει να εγκαταστήσουμε σε έναν υπολογιστή τις τεχνολογίες Apache, PHP, MySQL και PHPAdmin χωρίς ιδιαίτερη δυσκολία. Για να το εγκαταστήσουμε το κατεβάζουμε δωρεάν από την επίσημη ιστοσελίδα http://www.wampserver.com/en/ και ξεκινάμε τον οδηγό εγκατάστασης. Όταν μας ζητηθεί αποθηκεύουμε τον server στο σκληρό, δημιουργούμε μία συντόμευση στην επιφάνεια εργασίας και στο τέλος πατάμε finish. Παρατηρούμε ότι έχει εμφανιστεί ένα καινούργιο εικονίδιο στο taskbar, το οποίο όταν είναι πράσινο σημαίνει ότι λειτουργεί κανονικά (αντιθέτως όταν είναι κόκκινο δεν έχει ενεργοποιηθεί ενώ όταν είναι πορτοκαλί μία μόνο από τις υπηρεσίες είναι εγκατεστημένη).

Θα πρέπει τώρα να ελέγξουμε αν λειτουργεί η θύρα 80, η θύρα δηλ. την οποία ‘’ακούει’’ ο server. Για να γίνει αυτό πατάμε πάνω στο εικονίδιο και στη λίστα που εμφανίζεται επιλέγουμε Apache service και μετά test port 80.

Ο web server ακούει στη θύρα 80, όπως φαίνεται στο παρακάτω σχήμα:

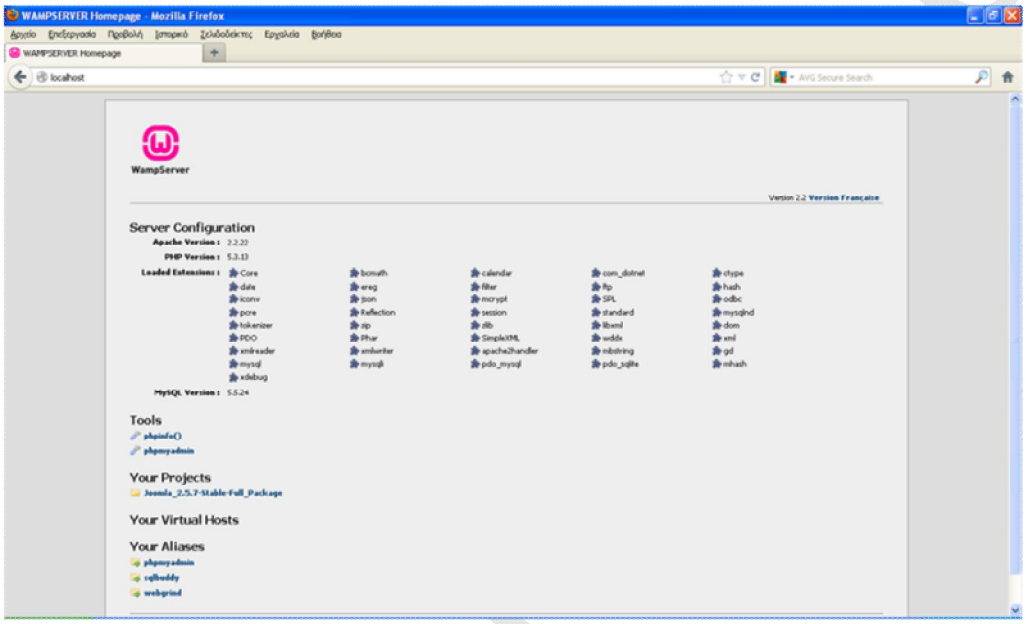


Εικόνα 9 Δοκιμή της θύρας 80

Στη συνέχεια, μπαίνουμε στην επίσημη ιστοσελίδα του joomla http://www.joomla.org/ και πατάμε το κουμπί λήψης. Μόλις ολοκληρωθεί η λήψη κάνουμε αποσυμπίεση στο φάκελο Joomla_2.5.4-Stable-Full_Package\. Μετά την αποσυμπίεση εμφανίζεται ο φάκελος στην επιφάνεια εργασίας, τον οποίο και αντιγράφουμε ή μετακινούμε στη θέση C:\wamp\www.

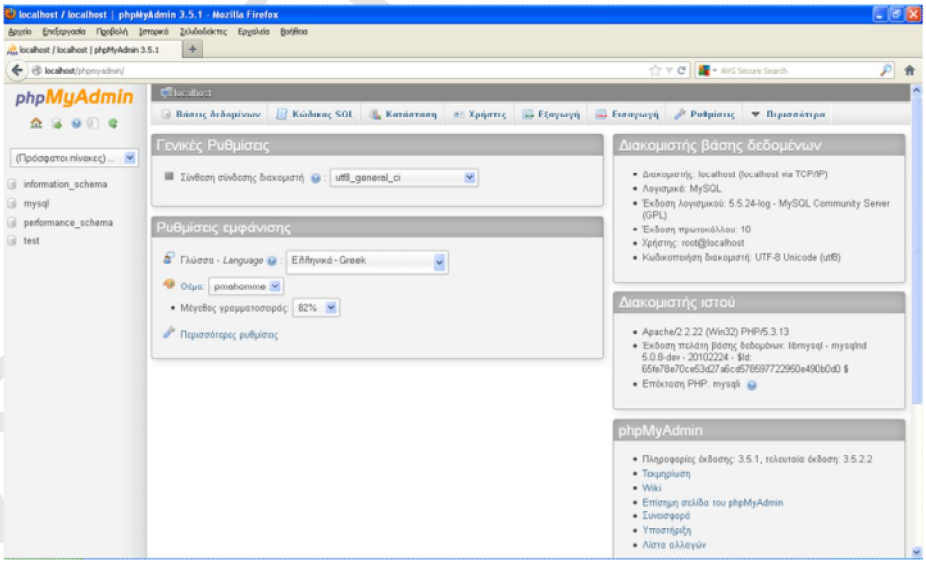
5.2 **Δημιουργία βάσης δεδομένων**

Μετά την εγκατάσταση του joomla θα πρέπει να δημιουργήσουμε τη βάση δεδομένων μας. Ανοίγουμε τον browser (στην προκειμένη περίπτωση τον Mozilla Firefox) και πληκτρολογούμε στη γραμμή διεύθυνσης http://localhost και πατάμε enter και εμφανίζεται η παρακάτω οθόνη.



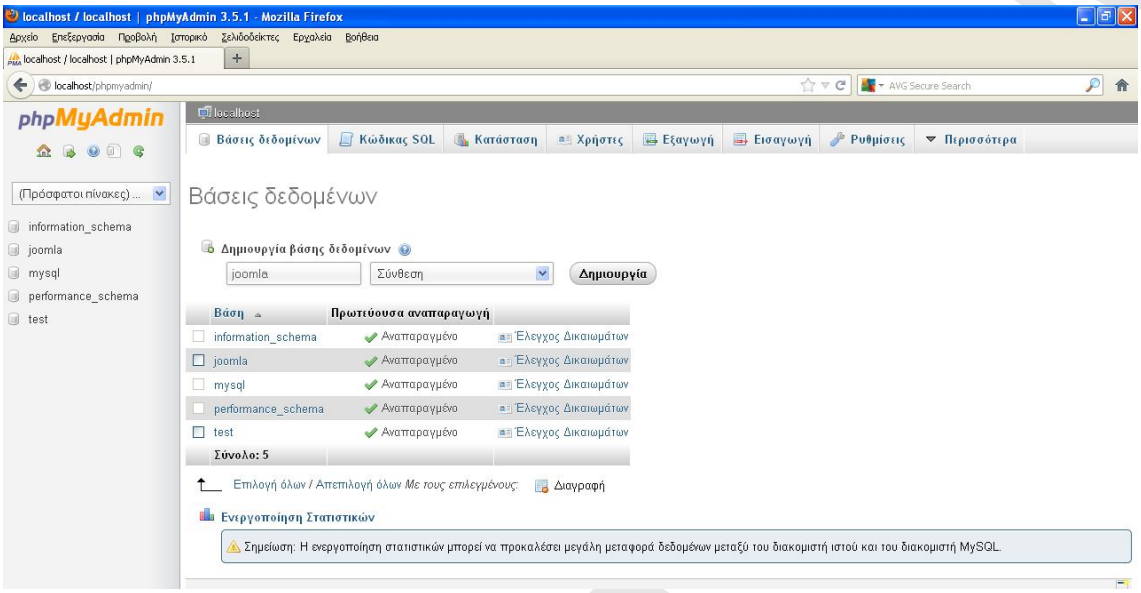
Εικόνα 10 Η σελίδα του Localhost

Στην περιοχή Tools βρίσκεται ο σύνδεσμος phpmyadmin. Κάνουμε κλικ και εμφανίζεται η παρακάτω οθόνη:



Εικόνα 11 Αρχική σελίδα του phpMyAdmin

Στο tab Databases εισάγουμε το όνομα της βάσης (πχ joomla).



Εικόνα 12 Δημιουργία της βάσης δεδομένων

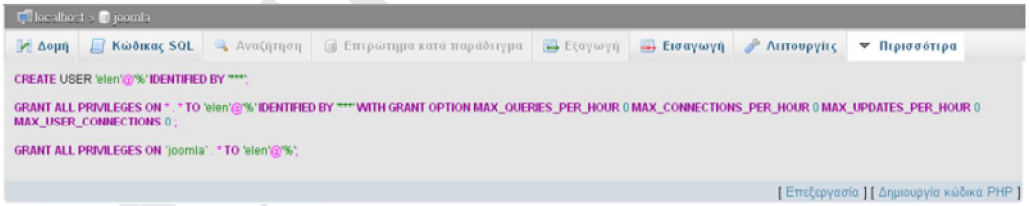
Αφού δημιουργήθεί η βάση,μπαίνουμε μέσα και κάνουμε κλικ στο σύνδεσμο privileges (δικαιώματα) και κάνουμε Προσθήκη χρήστη. Στην οθόνη που εμφανίζεται και στη περιοχή Πληροφορίες Σύνδεσης εισάγουμε τα παρακάτω στοιχεία

Όνομα χρήστη: elen

Κωδικός πρόσβασης: elenelen12

Επαναεισαγωγή: elenelen12

Στη συνέχεια επιλέγουμε το «Επιλογή όλων» για να αποκτήσουμε πλήρη δικαιώματα στη βάση δεδομένων και τέλος επιλέγουμε το «Προσθήκη χρήστη» στο τέλος της σελίδας.

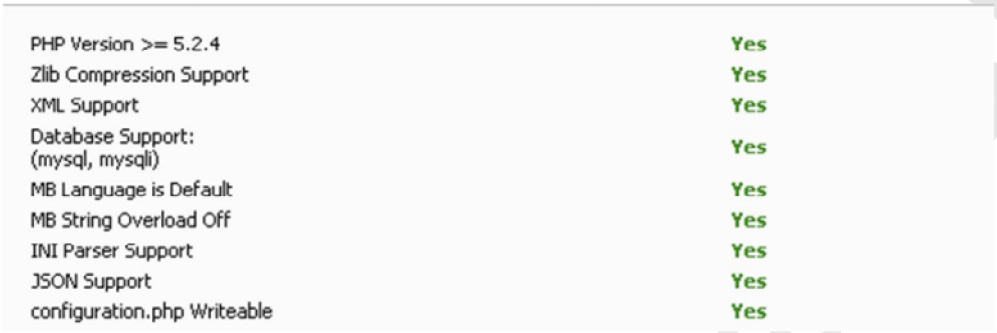


Εικόνα 13 Προσθήκη χρήστη

5.3 **Εγκατάσταση** Joomla

Ανοίγουμε τον browser και εισάγουμε στη γραμμή διευθύνσεων το localhost. Στη σελίδα που εμφανίζεται και κάτω από τον τίτλο “Your projects”, επιλέγουμε το σύνδεσμο Joomla_2.5.7-Stable-Full_Package. Η εγκατάσταση του Joomla ξεκινάει.

Στο Βήμα 1 θα πρέπει να επιλέξουμε τη γλώσσα ενώ στο Βήμα 2 εμφανίζεται γίνεται ο προληπτικός έλεγχος σχετικά με τη συμβατότητα του συστήματος. Εάν κάτι εμφανίζεται με κόκκινο χρώμα, το διορθώνουμε και πατάμε επανέλεγχος.



PHP Version >= 5.2.4	Yes
Zlib Compression Support	Yes
XML Support	Yes
Database Support: (mysql, mysqli)	Yes
MB Language is Default	Yes
MB String Overload Off	Yes
INI Parser Support	Yes
JSON Support	Yes
configuration.php Writeable	Yes

Εικόνα 14 Έλεγχος συμβατότητας συστήματος

Στην παρακάτω ομάδα, άλλες ενδείξεις είναι ενεργές και άλλες ανενεργές ανάλογα με τις ρυθμίσεις του server.

Directive	Recommended	Actual
Safe Mode	Off	Off
Display Errors	Off	On
File Uploads	On	On
Magic Quotes Runtime	Off	Off
Magic Quotes GPC	Off	Off
Register Globals	Off	Off
Output Buffering	Off	On
Session Auto Start	Off	Off
Native ZIP support	On	On

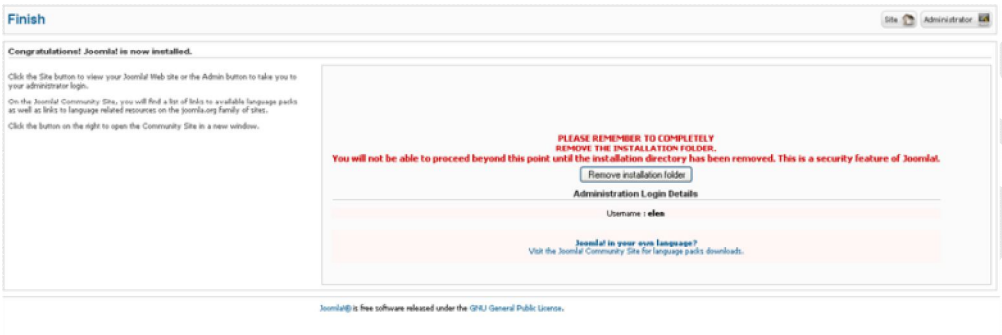
Εικόνα 15 Ρυθμίσεις server

Στο Βήμα 3 εμφανίζεται η άδεια χρήσης GNU και στο τέταρτο βήμα εισάγουμε τα στοιχεία της βάσης δεδομένων με την οποία θα συνεργάζεται το joomla. Εισάγουμε στα πλαίσια κειμένου τα αντίστοιχα δεδομένα.Στο database type επιλέγουμε από την αναδιπλούμενη λίστα το Mysql. Στο host name εισάγουμε localhost, στο username εισάγουμε το όνομα root, το πλαίσιο password το αφήνουμε κενό, και στο database name το όνομα της βάσης που δώσαμε όταν τη δημιουργήσαμε, δηλ. joomla. Όταν ολοκληρώσουμε πατάμε next.

Στο επόμενο βήμα μπορούμε να δημιουργήσουμε έναν FTP (File transfer protocoll). Αν βέβαια το λειτουργικό που χρησιμοποιούμε είναι Windows μπορούμε αυτό το βήμα να το παραλείψουμε.

Το Βήμα 5 είναι οι βασικές ρυθμίσεις (main configuration). Στο πλαίσιο site name εισάγουμε το όνομα της ιστοσελίδας μας, το admin username και password. Επιλέγοντας το Advanced settings-optional εμφανίζεται ένα πλαίσιο κειμένου στο οποίο μπορούμε να εισάγουμε μια περιγραφή του ιστοτόπου προκειμένου να είναι πιο εύκολη η αναζήτησή του από τις μηχανές αναζήτησης.Τέλος, κάνουμε κλικ στην επιλογή Sample Data set και πατάμε next.

Η τελευταία οθόνη μας ενημερώνει ότι η εγκατάσταση ολοκληρώθηκε με επιτυχία και για λόγους ασφαλείας θα πρέπει να διαγράψουμε το φάκελο installation.



Εικόνα 16 Επιτυχής εγκατάσταση του Joomla

Αφού το διαγράψουμε έχουμε 2 επιλογές. Είτε να μεταφερθούμε στο front end (επιλέγοντας το κουμπί site πάνω δεξιά) είτε να μεταφερθούμε στο back end (επιλέγοντας το κουμπί administrator)

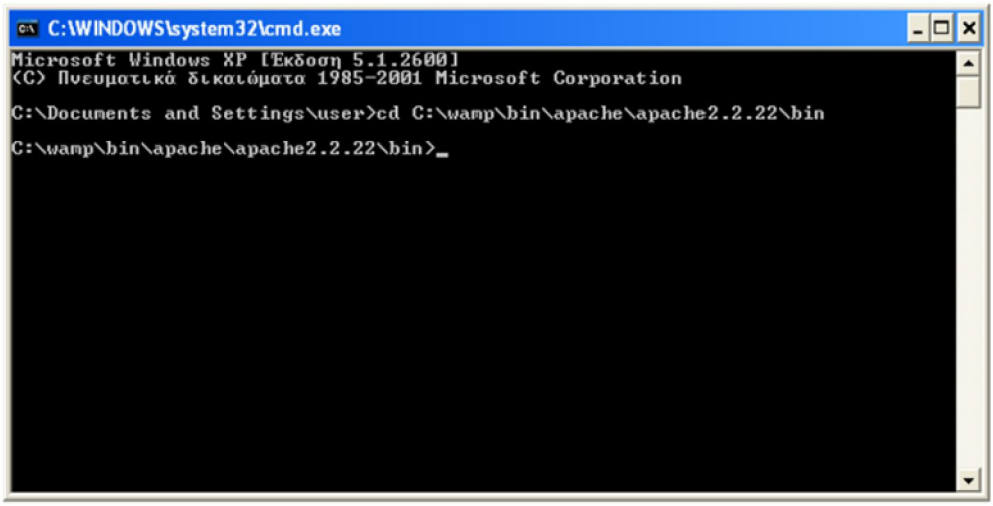
5.4 **Εγκατάσταση SSL**

Το SSL (Secure Socket Layer) είναι ένα πρωτόκολλο, το οποίο δημιουργεί μια ασφαλή σύνδεση μεταξύ του περιηγητή του client και της ιστοσελίδας ώστε όλη η επικοινωνία που μεταδίδεται μέσω αυτής της σύνδεσης να είναι κρυπτογραφημένη και άρα ασφαλής. Παρακάτω θα δούμε πώς γίνεται η εγκατάσταση του SSL certificate.

ΒΗΜΑ 1ο:

Δημιουργία του SSL Certificate και του κλειδιού.

Α) Ανοίγουμε ένα DOS command window και αλλάζουμε το directory ώστε αυτό να «δείχνει» το bin directory του wamp apache, όπως φαίνεται στο παρακάτω σχήμα.



Εικόνα 17 Αλλαγή directory

Β) Δημιουργούμε ένα κλειδί με κρυπτογράφηση 1024 bits. Προκειμένου να γίνει αυτό, θα πρέπει πρώτα να έχουμε εγκαταστήσει στον υπολογιστή μας το openssl (εμείς εγκαταστήσαμε το openssl-0.9.8k_WIN32 [57]) και στη συνέχεια να αντιγράψουμε και να αντικαταστήσουμε τα ακόλουθα 3 αρχεία στο wamp apache bin directory:

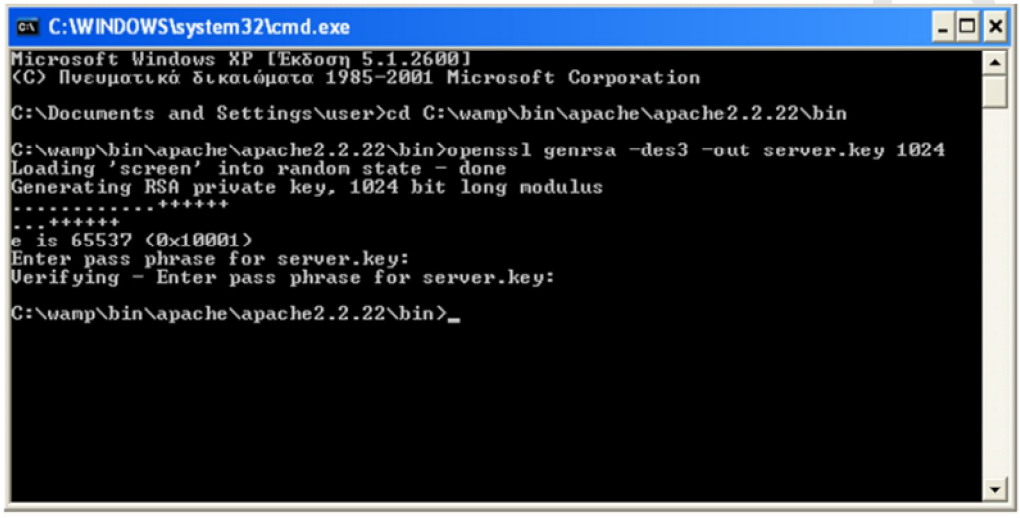
- openssl.exe
- ssleay32.dll

- libeay32.dll

Στη συνέχεια χρησιμοποιούμε την ακόλουθη εντολή:

```
openssl genrsa -des3 -out server.key 1024
```

Θα μας ζητήσει να εισάγουμε ένα passphrase, το οποίο και πληκτρολογούμε. Εν προκειμένω το pass phrase που εισάγαμε ήταν το elen12



Εικόνα 18 Δημιουργία server key

Γ) Θα πρέπει τώρα να αφαιρέσουμε την passphrase από το RSA ιδιωτικό κλειδί (κρατώντας, φυσικά, ένα backup του αρχικού αρχείου). Για να γίνει αυτό, θα πρέπει να εισάγουμε την εντολή:

```
copy server.key server.key.org
```

και στη συνέχεια την εντολή:

```
openssl rsa -in server.key.org -out server.key
```

Θα μας ζητήσει και πάλι το pass phrase, το οποία και εισάγουμε.

Δ) Δημιουργούμε ένα προσωπικό certificate (X509 structure) με το RSA κλειδί που μόλις δημιουργήσαμε. Εισάγουμε την εντολή:

```
openssl req -new -x509 -nodes -sha1 -days 365 -key server.key -out server.crt -config
    C:\wamp\bin\apache\apache2.2.22\conf\openssl.cnf
```

Συμπληρώνουμε τις πληροφορίες που ζητάει μετά από αυτήν τη εντολή.

ΒΗΜΑ 2ο

Στο βήμα αυτό θα αντιγράψουμε το server.key και τα αρχεία server.crt.

Στο conf folder του apache, δημιουργούμε 2 φακέλους και τους ονομάζουμε ssl.key και ssl.crt. Αντιγράφουμε το αρχείο server.key (από το bin) στον φάκελο ssl.key και το αρχείο server.crt (από το bin) στον φάκελο ssl.crt.

ΒΗΜΑ 3ο

Επεξεργαζόμαστε τα αρχεία httpd.conf και php.ini.

Στο httpd.conf file αφαιρούμε το '' # '' στη γραμμή που αναφέρει:

LoadModule ssl_module modules/mod_ssl.so

Καθώς και το '' # '' στη γραμμή που αναφέρει:

Include conf/extra/httpd-ssl.conf

Την τελευταία αυτή γραμμή τη μεταφέρουμε μετά την εντολή:

<IfModule ssl_module>... </IfModule>

Στη συνέχεια, ανοίγουμε το αρχείο php.ini που βρίσκεται στο bin του apache και αφαιρούμε το '' ; '' στη γραμμή που αναφέρει:

extension=php_openssl.dll

ΒΗΜΑ 4ο

Επεξεργασία του αρχείου httpd_ssl.conf που βρίσκεται μέσα στο φάκελο extra του apache.

Βρίσκουμε τη γραμμή που αναφέρει:

SSLMutex ....

και την αλλάζουμε σε:

SSLMutex default

Στη συνέχεια βρίσκουμε τη γραμμή που αναφέρει:

<VirtualHost _default_:443>

Αμέσως μετά από αυτήν, αλλάζουμε το:

DocumentRoot "c:/Apache2/htdocs"

σε *DocumentRoot "C:/wamp/www/"*

Αλλάζουμε το " ErrorLog... " σε Errorlog logs/sslerror_log καθώς και το "TransferLog ...." σε TransferLog logs/sslaccess_log

Εν συνεχεία βρίσκουμε τη γραμμή:

"SSLCertificateFile ...."

σε *SSLCertificateFile conf/ssl.crt/server.crt*

καθώς και το *"SSLCertificateKeyFile ...."* σε *SSLCertificateKeyFile conf/ssl.key/server.key*

Η επόμενη αλλαγή αφορά τη γραμμή:

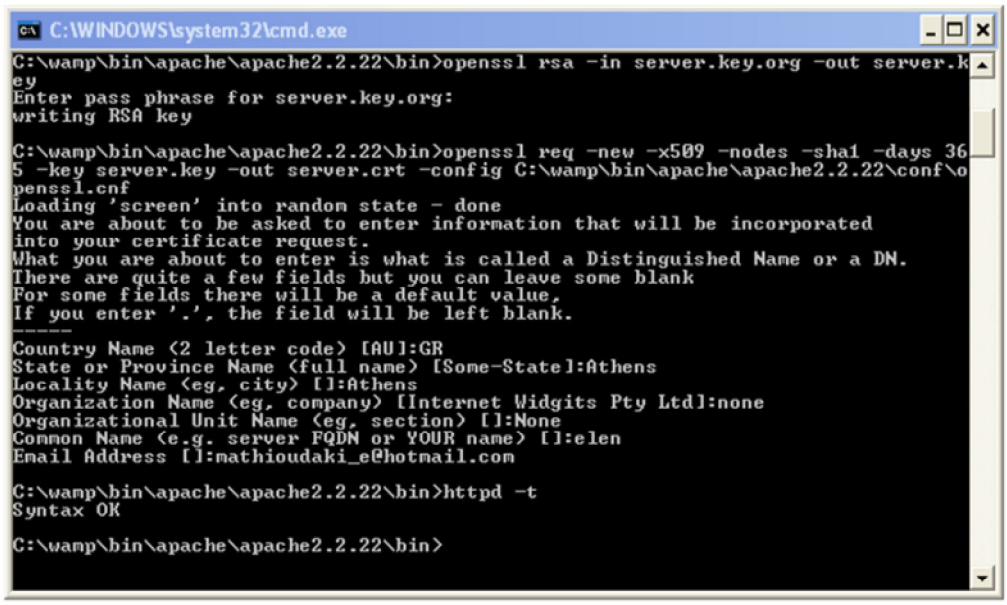
<Directory "c:/Apache2/cgi-bin"> σε *<Directory "C: /wamp/www/">* και ανάμεσα στα tags *<Directory ... >...</Directory>* αφαιρούμε το *SSLOptions* και *StdEnvVars* και προσθέτουμε τις ακόλουθες γραμμές:

Options Indexes FollowSymLinks MultiViews
AllowOverride All
Order allow, deny
allow from all

Επιβεβαιώνουμε ότι στη γραμμή CustomLog *"c:/Apache2/logs/ssl_request.log" \ "%t %h %{SSL_PROTOCOL}x %{SSL_CIPHER}x \"%r\" %b"*

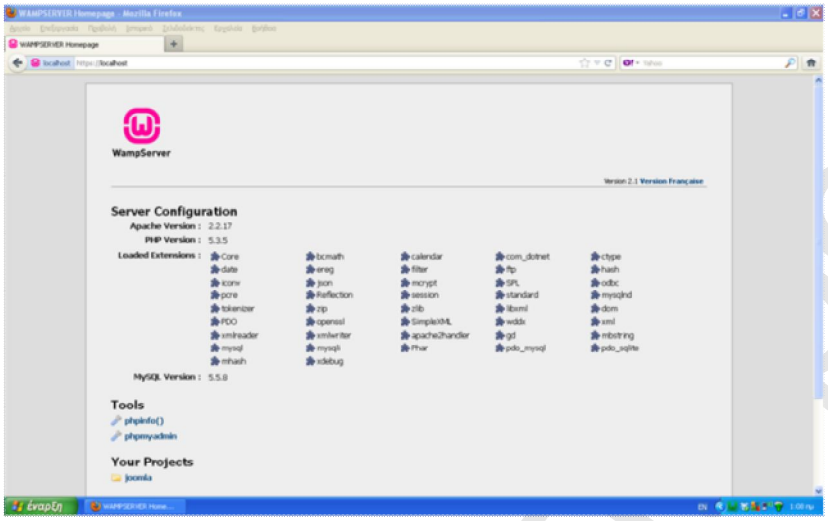
δεν υπάρχει η ένδειξη ‘’ # ‘’και αλλάζουμε τη συνταξη σε *CustomLog logs/ssl_request_log "%h %l %u %t \"%r\" %>s %b".*

Ελέγχουμε την σύνταξη με την εντολή httpd –t. Αν μας εμφανίσει Syntax OK μπορούμε να προχωρήσουμε.



Εικόνα 19 Ολοκλήρωση εγκατάστασης SSL

Κάνουμε επανεκκίνηση του Apache server και αν είναι επιτυχής, γράφουμε στον browser https://localhost



Εικόνα 20 Αρχική εικόνα του localhost μετά την επιτυχή εγκατάσταση του SSL

5.5 **Μετατροπή του** Apache **σε** Forward Proxy

Οι proxy servers λαμβάνουν αιτήματα που προορίζονται για άλλους servers, τα οποία στη συνέχεια προωθούν,ανακατευθύνουν ή απορρίπτουν. Δύο πολύ βασικοί λόγοι χρησιμοποίησής τους είναι η ενίσχυση της δικτυακής ασφάλειας που παρέχουν και η ελάττωση της κίνησης στο δίκτυο. Ο forward proxy είναι η πιο ευρέως χρησιμοποιούμενη μορφή proxy server και γενικά χρησιμοποιείται προκειμένου να στείλει αιτήματα από ένα απομονωμένο, ιδιωτικό δίκτυο στο Διαδίκτυο μέσω ενός firewall. Ο server θα ελέγξει πρώτα αν το αίτημα είναι έγκυρο (αν όχι θα το απορρίψει στέλνοντας μήνυμα λάθους στον client ή θα τον ανακατευθύνει) και στη συνέχεια αν υπάρχει αποθηκευμένο. Αν ναι, θα "φέρει" την αποθηκευμένη πληροφορία. Αν όχι, θα στείλει το αίτημα μέσω του firewall σε άλλον server. Ο forward proxy μόλις λάβει την πληροφορία θα την στείλει στον client και ίσως την αποθηκεύσει για μελλοντικά αιτήματα.

Για να μετατρέψουμε τον Apache σε forward proxy θα πρέπει να επεξεργαστούμε το αρχείο httpd.conf, το οποίο θα το βρούμε στο path C:\wamp\bin\apache\Apache2.2.22\conf

Ανοίγοντας το αρχείο (με κάποιον text editor όπως το Notepad) αφαιρούμε από τις ακόλουθες εντολές το ‘’#’’

LoadModule cache_module modules/mod_cache.so
LoadModule deflate_module modules/mod_deflate.so
LoadModule mem_cache_module modules/mod_mem_cache.so
LoadModule disk_cache_module modules/mod_disk_cache.so
LoadModule proxy_module modules/mod_proxy.so
LoadModule proxy_ajp_module modules/mod_proxy_ajp.so
LoadModule proxy_connect_module modules/mod_proxy_connect.so
LoadModule proxy_ftp_module modules/mod_proxy_ftp.so
LoadModule proxy_http_module modules/mod_proxy_http.so
LoadModule proxy_scgi_module modules/mod_proxy_scgi.so

Επίσης, καλό θα ήταν να χρησιμοποιήσουμε άλλη θύρα από την 80 για τον διακομιστή μας. Για να γίνει αυτό επεξεργαζόμαστε το αρχείο httpd.conf και αλλάζουμε την εντολή Listen. Στην παρούσα εργασία χρησιμοποιήσαμε τη θύρα 8080 (εναλλακτική θύρα για τον Apache).

Στη συνέχεια αλλάζουμε και το ServerName directory ώστε να αντικατοπτρίζει αυτήν την αλλαγή (επίσης μπορούμε απλώς να εισάγουμε την IP διεύθυνσή του αν δεν χρησιμοποιούμε DNS).

ServerName Localhost: 8080

Αποθηκεύουμε το αρχείο και κάνουμε restart τον Apache. Αν ο Apache ξεκινήσει, ανοίγουμε και πάλι και αφαιρούμε το ‘’#’’ από τις ακόλουθες εντολές (οι οποίες αν δεν υπάρχουν φροντίζουμε να τις προσθέσουμε)

Include conf/extra/httpd-mpm.conf
Include conf/extra/httpd-vhosts.conf
Include conf/extra/httpd-deflate.conf
Include conf/extra/httpd-cache.conf

Μέσα, όμως,στο directory conf/extra, θα πρέπει να δημιουργήσουμε τα αρχεία httpd-deflate.conf και httpd-cache.conf, τα οποία προσθέσαμε στο παραπάνω αρχείο. Κατ’αρχάς, δημιουργούμε ένα καινούργιο αρχείο, το οποίο ονομάζουμε httpd-cache.conf και εισάγουμε το παρακάτω κείμενο, όπου οι εντολές Allow from και NoProxy να αντικατοπτρίζουν το τοπικό μας δίκτυο.

 # http://httpd.apache.org/docs/2.2/mod/mod_proxy.html
<IfModule mod_proxy.c>
ProxyRequests On
*<Proxy *>*
Order Deny, Allow
Deny from all
Allow from 192.168..*/255.255.*.**
</Proxy>
ProxyVia On
</IfModule>
<IfModule mod_cache.c>
<IfModule mod_disk_cache.c>
CacheRoot \"C:/temp/proxy\"
CacheEnable disk /
CacheDirLevels 3
CacheDirLength 2
CacheMaxFileSize 100000000
CacheDefaultExpire 259200

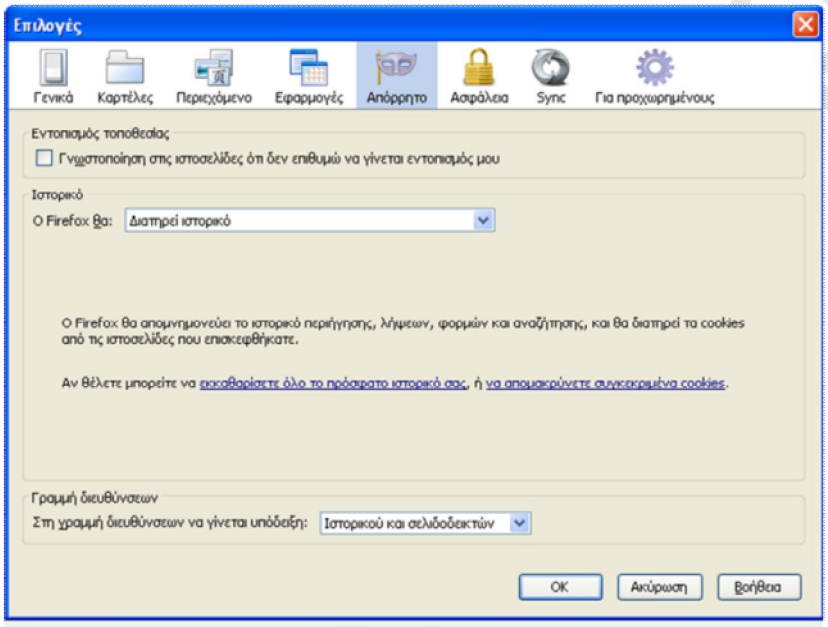
CacheMaxExpire 432000
</IfModule>
ProxyTimeout 60
NoProxy 192.168..*/255.255.*.**
 # When acting as a proxy, don\'t cache the list of security update
CacheDisable http://security.update.server/update-list/
</IfModule>
 # End of proxy directives

Στη συνέχεια δημιουργούμε και ένα δεύτερο αρχείο με το όνομα httpd-deflate.conf και εισάγουμε το παρακάτω κείμενο.

 # http://httpd.apache.org/docs/2.2/mod/mod_deflate.html
<IfModule mod_deflate.c>
AddOutputFilterByType DEFLATE text/html text/plain text/css application/x-javascript
#Highest 9 - Lowest 1
DeflateCompressionLevel 2
SetEnvIfNoCase Request_URI \\.(?:gif|jpe?g|png)$ no-gzip dont-vary
SetEnvIfNoCase Request_URI \\.(?:exe|t?gz|zip|bz2|sit|rar)$ no-gzip dont-vary
SetEnvIfNoCase Request_URI \\.pdf$ no-gzip dont-vary
SetEnvIfNoCase Request_URI \\.wmv$ no-gzip dont-vary
SetEnvIfNoCase Request_URI \\.wma$ no-gzip dont-vary
SetEnvIfNoCase Request_URI \\.swf$ no-gzip dont-vary
SetEnvIfNoCase Request_URI \\.wav$ no-gzip dont-vary
SetEnvIfNoCase Request_URI \\.wmd$ no-gzip dont-vary
SetEnvIfNoCase Request_URI \\.wmz$ no-gzip dont-vary
SetEnvIfNoCase Request_URI \\.mcf$ no-gzip dont-vary
SetEnvIfNoCase Request_URI \\.wmx$ no-gzip dont-vary
SetEnvIfNoCase Request_URI \\.wm$ no-gzip dont-vary
SetEnvIfNoCase Request_URI \\.wax$ no-gzip dont-vary
SetEnvIfNoCase Request_URI \\.asf$ no-gzip dont-vary
SetEnvIfNoCase Request_URI \\.rm$ no-gzip dont-vary
SetEnvIfNoCase Request_URI \\.pls$ no-gzip dont-vary
SetEnvIfNoCase Request_URI \\.asx$ no-gzip dont-vary
SetEnvIfNoCase Request_URI \\.mpg$ no-gzip dont-vary
SetEnvIfNoCase Request_URI \\.mp2$ no-gzip dont-vary
SetEnvIfNoCase Request_URI \\.mp3$ no-gzip dont-vary
SetEnvIfNoCase Request_URI \\.avi$ no-gzip dont-vary
</IfModule>

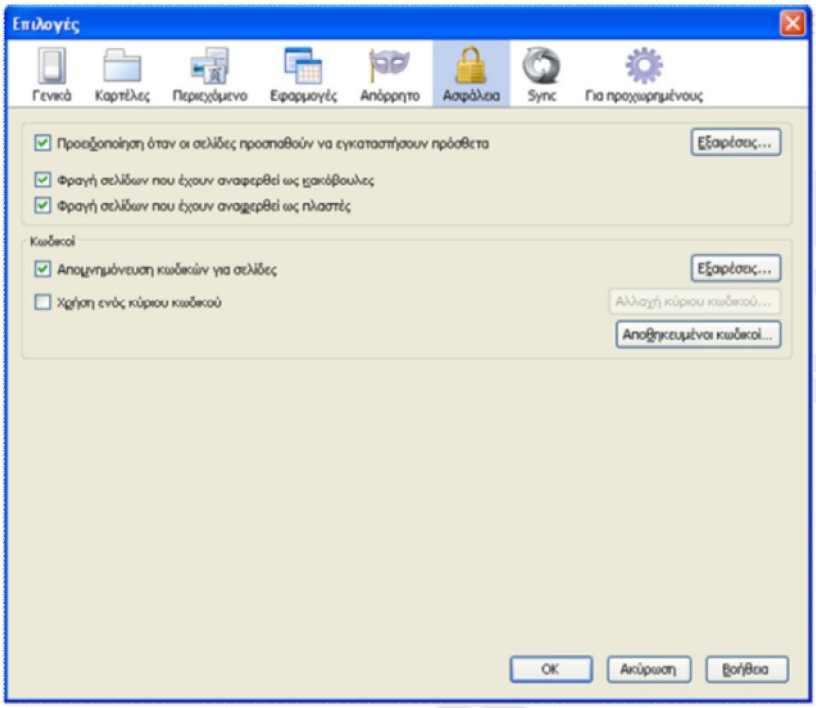
5.6 Διαμόρφωση επιλογών ιδιωτικότητας στον χρήστη

Για την διαμόρφωση των επιλογών ιδιωτικότητας στον χρήστη (web browser), εξετάζουμε την περίπτωση του Mozilla Firefox. Επιλέγουμε Internet options (ή επιλογές στα Ελληνικά) και εμφανίζεται η ακόλουθη οθόνη. Κάτω από το Tab Απόρρητο έχουμε τη δυνατότητα να επιτρέψουμε (ή όχι) στον browser να κρατάει ιστορικό περιήγησης και τα cookies από τις ιστοσελίδες τις οποίες επισκεφθήκαμε.



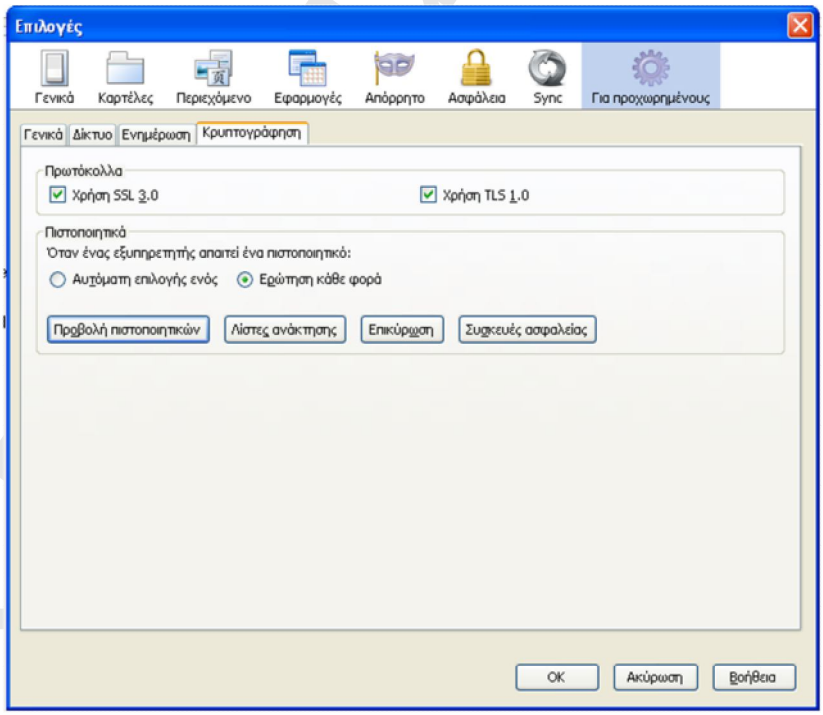
Εικόνα 21 Διαμόρφωση επιλογών ιδιωτικότητας στον χρήστη

Στο tab Ασφάλεια μπορούμε να επιλέξουμε τη φραγή ιστοσελίδων που έχουν χαρακτηριστεί κακόβουλες ή πλαστές καθώς και να μας προειδοποιεί σε περίπτωση που κάποια ιστοσελίδα προσπαθεί να εγκαταστήσει πρόσθετα (add-ons).



Εικόνα 22 Δυνατότητα επιλογών ασφάλειας στον χρήστη

Τέλος, κάτω από την καρτέλα Για Προχωρημένους, μπορούμε να επιλέξουμε τα πρωτόκολλα κρυπτογράφησης που θα χρησιμοποιούμε καθώς και να ενημερωνόμαστε κάθε φορά αν κάποιος server απαιτεί κάποιο πιστοποιητικό.



Εικόνα 23 Δυνατότητα επιλογής πρωτοκόλλων κρυπτογράφησης στον χρήστη

5.7 **Πειραματική επαλήθευση**

Αφού, λοιπόν, εγκαταστήσαμε τον server, δημιουργήσαμε την ιστοσελίδα, παραμετροποιήσαμε τον client και εγκαταστήσαμε και το SSL, θα εξετάσουμε την ασφάλεια που μας παρέχουν μέσω της επίθεσης ενός ωτακουστή.

Οταν ένας υπολογιστής συνδέεται στο Διαδίκτυο, ουσιαστικά συνδέεται στο δίκτυο που έχει δημιουργήσει και συντηρεί ο Πάροχος Διαδικτύου (ISP). Το δίκτυο του ISP είναι συνδεδεμένο με τα δίκτυα των άλλων ISPs κ.ο.κ με αποτέλεσμα να δημιουργείται το παγκόσμιο δίκτυο των δικτύων που αποκαλούμε Διαδίκτυο. Η μεταφορά δεδομένων στα δίκτυα των υπολογιστών (όπως και σε πολλά άλλα δίκτυα) γίνεται με τη μορφή πακέτων (data packets ή απλά packets), έτσι ώστε αφενός να μπορούν να μεταφέρουν όλοι οι υπολογιστές τα δεδομένα σχεδόν ταυτόχρονα και αφετέρου για καλύτερο έλεγχο των λαθών [27]. Σε κάθε πακέτο προστίθεται μια επικεφαλίδα (header) με τα στοιχεία του αποστολέα, του παραλήπτη κ.α. ώστε να μπορέσει να δρομολογηθεί στον σωστό παραλήπτη. Στο Διαδίκτυο, την αποστολή του κάθε πακέτου, ανάλογα με το περιεχόμενό του, την αναλαμβάνει και το αντίστοιχο πρωτόκολλο (το HTTP για μεταφορά σελίδων Web, το SMTP και το POP3 για μεταφορά e-mail κ.α). Κάθε υπολογιστής που είναι συνδεδεμένος στο Διαδίκτυο δέχεται μόνο τα πακέτα που προορίζονται γι αυτόν και αγνοεί όλα τα υπόλοιπα. Η ανταλλαγή των πακέτων μπορεί να παρατηρηθεί από εργαλεία τα οποία ονομάζονται packet sniffers.

Ο packet sniffer συλλαμβάνει τα μηνύματα που στέλνονται ή/και λαμβάνονται από τον υπολογιστή μας ενώ μπορεί και να απεικονίσει τα περιεχόμενα διαφόρων πεδίων πρωτοκόλλων που περιέχονται στα μηνύματα που συλλαμβάνονται. Ο ίδιος, όμως, δεν στέλνει ποτέ πακέτα.

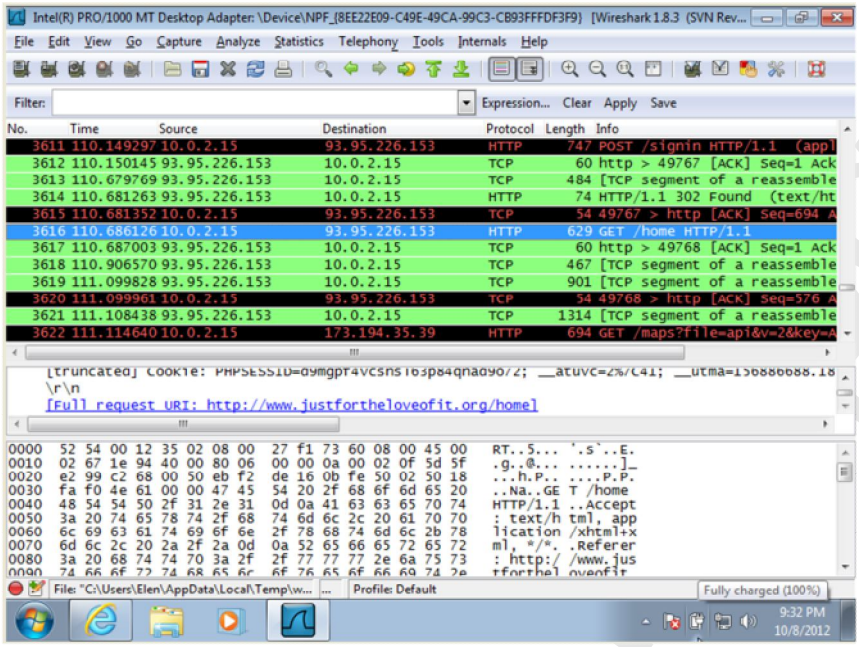
Στην εργασία αυτή θα χρησιμοποιήσουμε τον packet sniffer Wireshark, ο οποίος είναι ελεύθερο και ανοιχτού κώδικα λογισμικό και είναι διαθέσιμος για όλα τα λογισμικά (όπως τα Windows, Linux, Mac OS, Solaris).

Αφού επισκεφτούμε την ιστοσελίδα http://www.wireshark.org/ και φορτώσουμε το απαραίτητο λογισμικό, μπορούμε να ξεκινήσουμε την εκτέλεση του προγράμματος. Κατά την εκτέλεση του προγράμματος εμφανίζεται στην οθόνη η γραφική διεπαφή χρήστη (graphical user interface, GUI). Η διεπαφή του Wireshark περιλαμβάνει πέντε κύρια συστατικά στοιχεία:

- Το μενού των εντολών
- Το παράθυρο καταλόγου πακέτων (packet-listing window)
- Το παράθυρο λεπτομερειών επικεφαλίδας πακέτου (packet-header details window)
- Το παράθυρο περιεχομένων πακέτου (packet-contents window)
- Τέλος, το πεδίο φίλτρου παρουσίασης πακέτων (packet display filter field) στο επάνω μέρος, κάτω ακριβώς από το μενού εντολών.

5.7.1 **Δοκιμαστική εκτέλεση του** Wireshark

Ανοίγουμε το Wireshark και ξεκινάμε την καταγραφή των πακέτων. Πληκτρολογούμε στο πρόγραμμα περιήγησης www.justfortheloveofit.org ,ανοίγουμε την ιστοσελίδα και κάνουμε login χρησιμοποιώντας username και password. Επιστρέφουμε στον ωτακουστή μας και σταματάμε την σύλληψη των πακέτων. Η εικόνα που έχουμε είναι η ακόλουθη



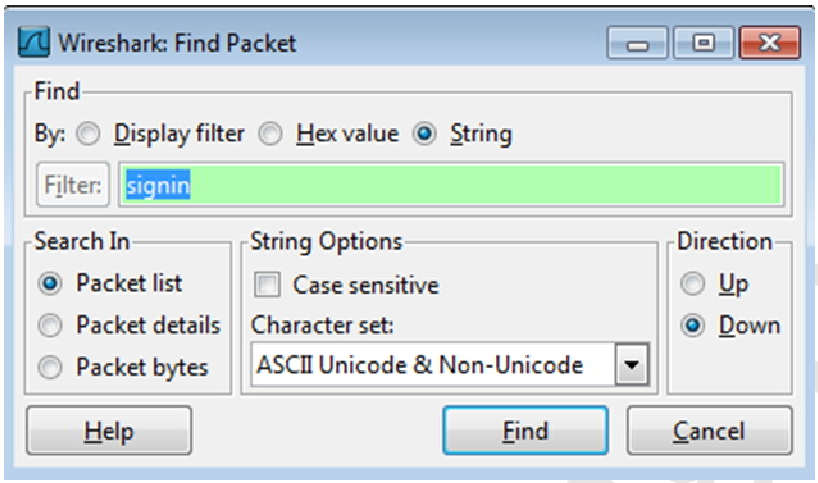
Εικόνα 24 Ακολουθία πακέτων (trace) όπως απεικονίζεται στο Wireshark

Το παράθυρο καταλόγου πακέτων παρουσιάζει μία περίληψη της μιας γραμμής για κάθε πακέτο που συλλαμβάνεται και η οποία περιλαμβάνει τον αριθμό του πακέτου (πρόκειται για αριθμό που απονέμεται από το Wireshark και όχι για έναν αριθμό πακέτου που περιέχεται στην επικεφαλίδα οποιουδήποτε πρωτοκόλλου), τον χρόνο σύλληψης του πακέτου, τις διευθύνσεις πηγής και προορισμού, το είδος του πρωτοκόλλου και πληροφορία σχετική με το πρωτόκολλο η οποία περειέχεται στο πακέτο.

Το παράθυρο λεπτομεριών επικεφαλίδας πακέτου περιλαμβάνει λεπτομέρειες σχετικά με το επιλεγμένο πακέτο στο παράθυρο packet-listing. Οι λεπτομέρειες περιλαμβάνουν πληροφορίες σχετικές με το πλαίσιο Ethernet, το πρωτόκολλο IP, λεπτομέρειες σχετικές με το πρωτόκολλο μεταφοράς κ.α

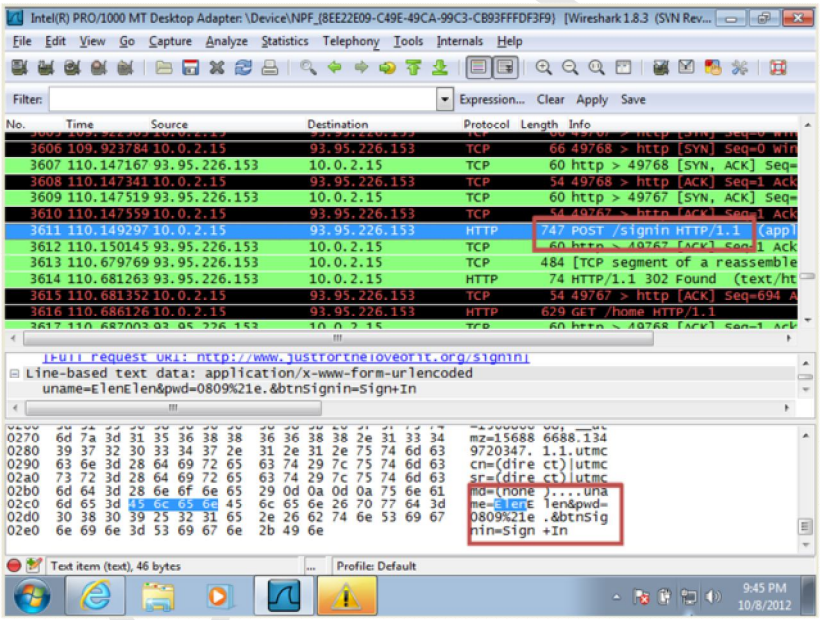
Τέλος, το παράθυρο περιεχομένων πακέτου παρουσιάζει ολόκληρο το περιεχόμενο ενός συλλαμβανόμενου πλαισίου που δεν είναι κρυπτογραφημένο και σε μορφή ASCII και σε δεκαεξαδική μορφή. Το πακέτο 3616 που βλέπουμε παραπάνω μας δίνει την πληροφορία της ιστοσελίδας στην οποία περιηγήθηκε ο χρήστης.

Το Wireshark μας δίνει τη δυνατότητα με την εντολή Find packet να φιλτράρουμε τα δεδομένα μας ανάλογα με το πακέτο που θέλουμε να δούμε. Έτσι, λοιπόν, επιλέγουμε να τα φιλτράρουμε με τον όρο signin προκειμένου να ανιχνεύσουμε username και password.



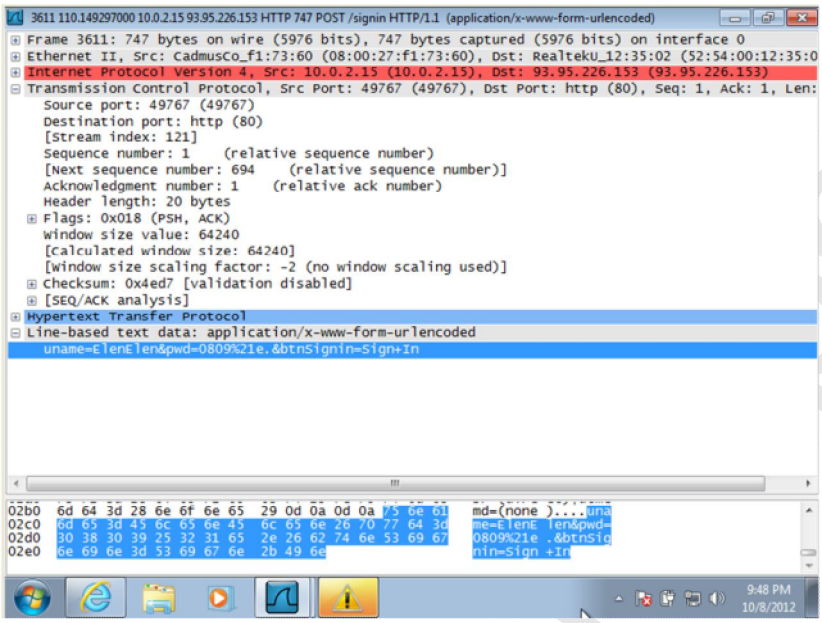
Εικόνα 25 Φιλτράρισμα δεδομένων

Πράγματι, το πακέτο 3611 μας δίνει το όνομα χρήστη και τον κωδικό.



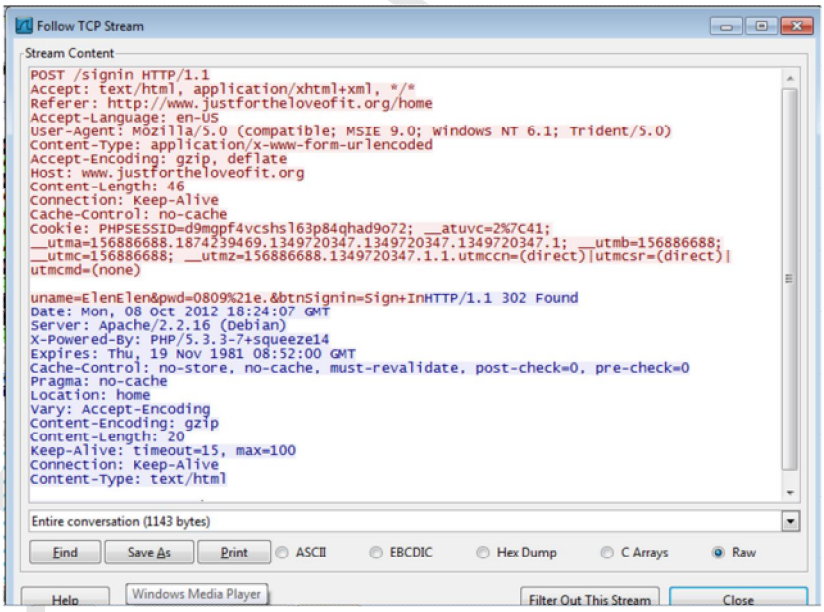
Εικόνα 26 Εύρεση ονόματος χρήστη και συνθηματικού

Αν ανοίξουμε το πακέτο μπορούμε να το δούμε και πιο καθαρά



Εικόνα 27 Λεπτομέρειες πακέτου

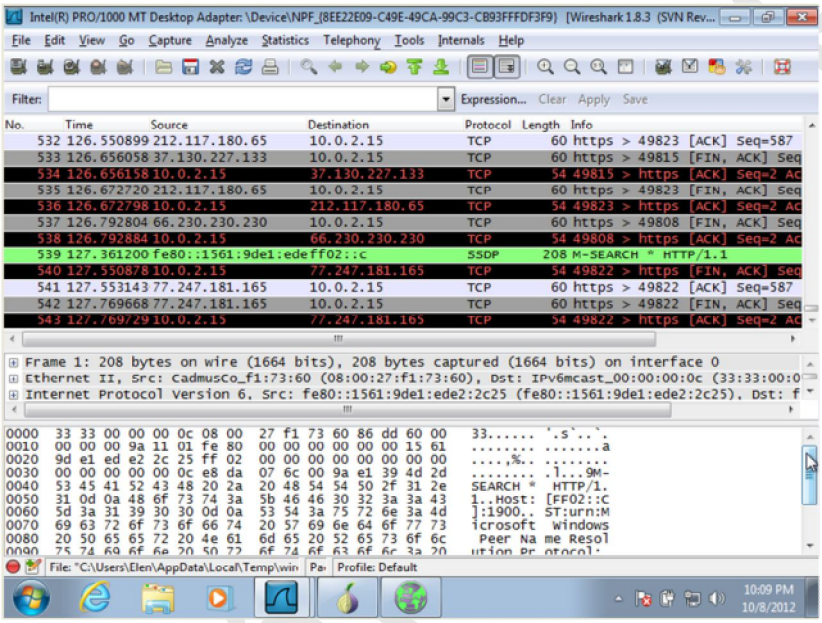
Τέλος, στην παρακάτω εικόνα μπορούμε να δούμε το περιεχόμενο της συγκεκριμένης ροής TCP, δηλαδή την ανταλλαγή μηνυμάτων μεταξύ του πλοηγού και του εξυπηρετητή ιστού. Τα μηνύματα (εντολές) του πλοηγού ιστού εμφανίζονται σε ροζ φόντο ενώ τα μηνύματα (αποκρίσεις) του εξυπηρετητή ιστού σε γαλάζιο.



Εικόνα 28 Ροή TCP (TCP flow)

5.7.2 **Πλοήγηση μέσω** TOR browser **και καταγραφή των πακέτων** (client-side anonymity)

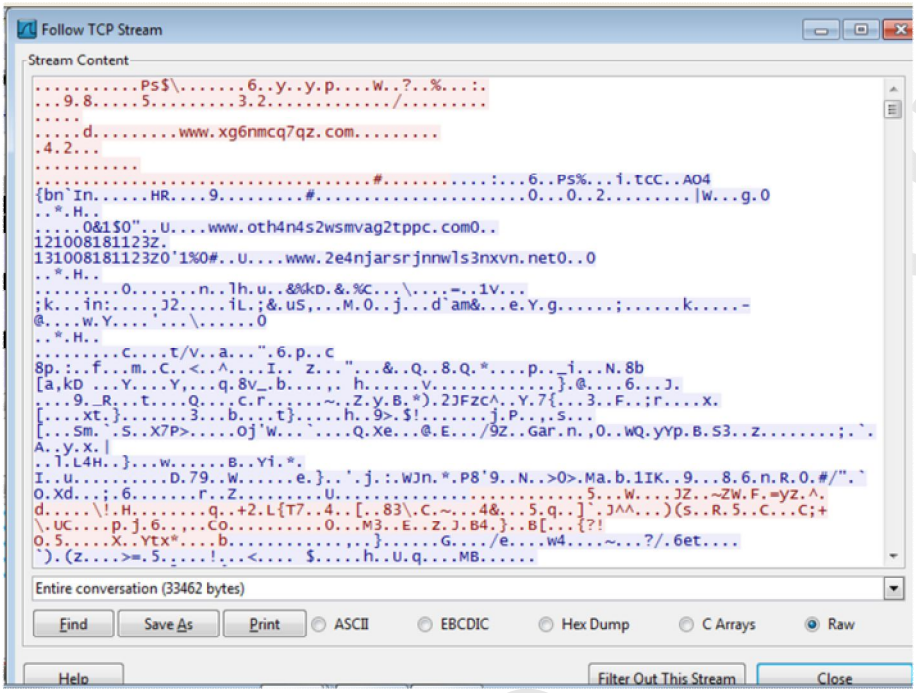
Αφού, λοιπόν, είδαμε πώς λειτουργεί το Wireshark ας πλοηγηθούμε στο Διαδίκτυο μέσω του TOR browser, σύστημα, που όπως είδαμε και παραπάνω, μας προσφέρει ανωνυμία σε εφαρμογές που βασίζονται σε συνδέσεις TCP. Πηγαίνουμε στην ίδια ιστοσελίδα, όπως και προηγουμένως (www.justfortheloveofit.org) και η εικόνα που μας δίνει ο ωτακουστής είναι η ακόλουθη:



Εικόνα 29 Καταγραφή πακέτων μετά την πλοήγησή μας μέσω TOR browser

Παρατηρούμε ότι αν προσπαθήσουμε να φιλτράρουμε, προκειμένου να βρούμε τα signin credentials, αυτό δεν καθιστάται δυνατό καθώς δεν λαμβάνουμε σχετικά αποτελέσματα.

Ανοίγοντας τη ροή TCP για κάποιο πακέτο, έχουμε δεδομένα της παρακάτω μορφής:



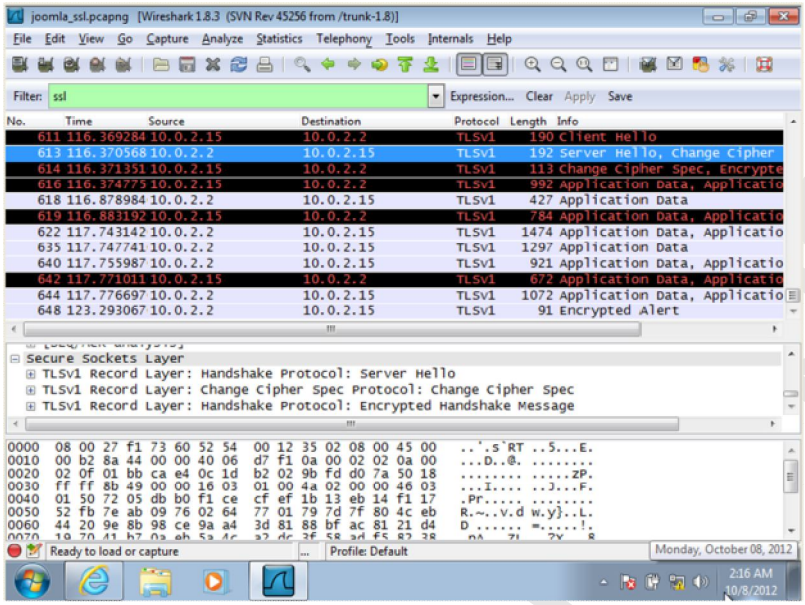
Εικόνα 30 Ροή TCP μετά την πλοήγηση μέσω TOR browser

Όπως βλέπουμε τα δεδομένα είναι κρυπτογραφημένα και δεν είμαστε σε θέση να δούμε ποιες είναι οι εντολές του πελάτη και ποιες οι αποκρίσεις του εξυπηρετητή.Ο TOR περνάει την κίνηση από τρεις διαφορετικούς servers με διαφορετικό επίπεδο κρυπτογράφησης για κάθε έναν από αυτούς.

Βασικό μειονέκτημα του TOR είναι η αργή απόδοση του, εξαιτίας της οποίας πολλοί χρήστες αρνούνται να το χρησιμοποιήσουν. Αυτό, βέβαια, έχει αρνητική επίδραση στην προστασία της ιδιωτικότητας που παρέχεται από τον TOR καθώς αυτή βρίσκεται σε ευθεία εξάρτηση από τον αριθμό των χρηστών και τη διαθεσιμότητα των κοινόχρηστων πόρων [58].

5.7.3 Έλεγχος για κρυπτογράφηση της επικοινωνίας με το πρωτόκολλο SSL και καταγραφή των πακέτων

Όπως είδαμε σε προηγούμενη ενότητα, προχωρήσαμε στην εγκατάσταση του SSL στην ιστοσελίδα που έχουμε δημιουργήσει. Θα πληκτρολογήσουμε στον browser https://10.0.2.2 και θα περιηγηθούμε στη σελίδα.Τέλος, θα εισάγουμε user name και password προκειμένου να δούμε τί θα καταγράψει ο packet sniffer μας. Η εικόνα που μας έδωσε (με φίλτρο ssl) είναι



Εικόνα 31 Το Wireshark μετά την κρυπτογράφηση με SSL

Ο Wireshark εμφανίζει τα πακέτα που μεταφέρουν τα μηνύματα HTTPS ως SSL ή TLS. Το πρωτόκολλο TLSv1 είναι ένα πρωτόκολλο που εγγυάται ότι κατά την επικοινωνία πελάτη-εξυπηρετητή μέσω του Διαδικτύου δεν πρόκειται να μεσολαβήσει κάποιος τρίτος που θα υποκλέψει το περιεχόμενο της επικοινωνίας. Μια σύντομη περιγραφή του TLS είναι η εξής:

Ο πελάτης και εξυπηρετητής TLS διαπραγματεύονται την εγκατάσταση σύνδεσης ακολουθώντας μια διαδικασία χειραψίας. Κατά τη χειραψία ο πελάτης και ο εξυπηρετητής συμφωνούν σε διάφορες παραμέτρους σχετικές με την ασφάλεια της σύνδεσης. Η χειραψία αρχίζει όταν ο πελάτης ζητά μια ασφαλή σύνδεση στέλνοντας στον εξυπηρετητή ένα μήνυμα ClientHello και παρουσιάζοντας μια λίστα των υποστηριζόμενων κωδίκων κρυπτογράφησης (ciphers) και συναρτήσεων κατακερματισμού (hash functions). Ο εξυπηρετητής απαντά με το μήνυμα ServerHello και επιλέγει από τη λίστα τον κώδικα κρυπτογράφησης και τη συνάρτηση κατακερματισμού.

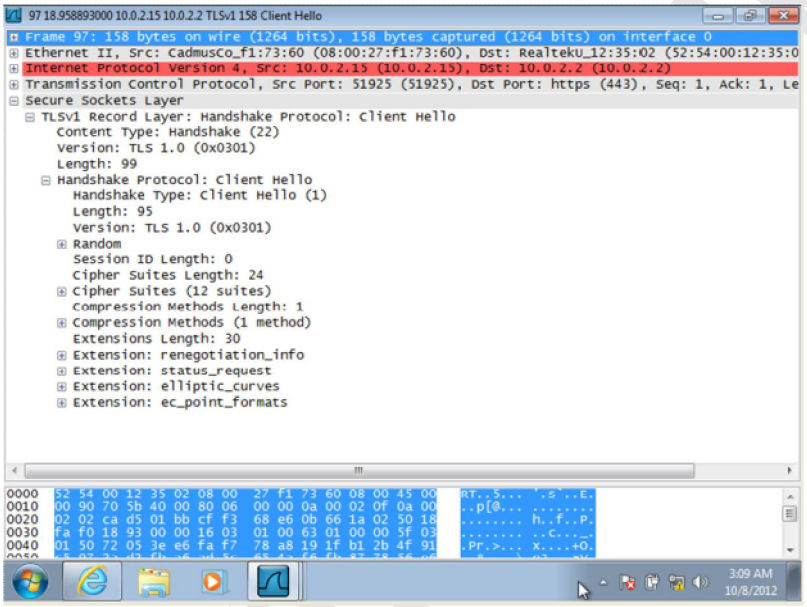
Κατόπιν, ο εξυπηρετητής αποστέλλει στον πελάτη μέσω του μηνύματος Certificate την ταυτότητά του με τη μορφή ενός ψηφιακού πιστοποιητικού (digital certificate). Το πιστοποιητικό συνήθως περιέχει ο όνομα του εξυπηρετητή, την έμπιστη αρχή πιστοποίησης (trusted certificate authority – CA) και το δημόσιο κλειδί κρυπτογράφησης του εξυπηρετητή. Ο πελάτης μπορεί να επικοινωνήσει με τον CA και να επιβεβαιώσει ότι το πιστοποιητικό είναι αυθεντικό προτού προχωρήσει στην εγκατάσταση κλειδιού κρυπτογράφησης για τη σύνοδο. Ο εξυπηρετητής αποστέλλει το μήνυμα ServerHelloDone υποδηλώνοντας ότι ολοκλήρωσε από την πλευρά του τη χειραψία.

Για την παραγωγή του κλειδιού συνόδου, ο πελάτης κρυπτογραφεί ένα τυχαίο αριθμό με το δημόσιο κλειδί του εξυπηρετητή και στέλνει το αποτέλεσμα στον εξυπηρετητή με το μήνυμα ClientKeyExchange. Μόνο ο εξυπηρετητής μπορεί να το αποκρυπτογραφήσει χρησιμοποιώντας το μυστικό του κλειδί. Με τον τρόπο αυτό ο εξυπηρετητής και ο πελάτης μοιράζονται ένα κοινό μυστικό που δεν είναι προσβάσιμο από τρίτους. Με το κοινό αυτό μυστικό και οι δύο πλευρές παράγουν το κλειδί συνόδου για την (από)κρυπτογράφηση των δεδομένων. Ο πελάτης στέλνει το μήνυμα ChangeCipherSpec λέγοντας στον εξυπηρετητή ότι η επικοινωνία από εδώ και πέρα θα είναι κρυπτογραφημένη. Κατόπιν, ο πελάτης στέλνει το κρυπτογραφημένο μήνυμα EncryptedHandshakeMessage που περιέχει το αποτέλεσμα της συνάρτησης κατακερματισμού επί των προηγούμενων μηνυμάτων της χειραψίας. Ο εξυπηρετητής θα προσπαθήσει να το αποκρυπτογραφήσει και να επιβεβαιώσει την ορθότητα του αποτελέσματος της συνάρτησης κατακερματισμού. Εάν αυτό γίνει επιτυχώς, ο εξυπηρετητής στέλνει το δικό του

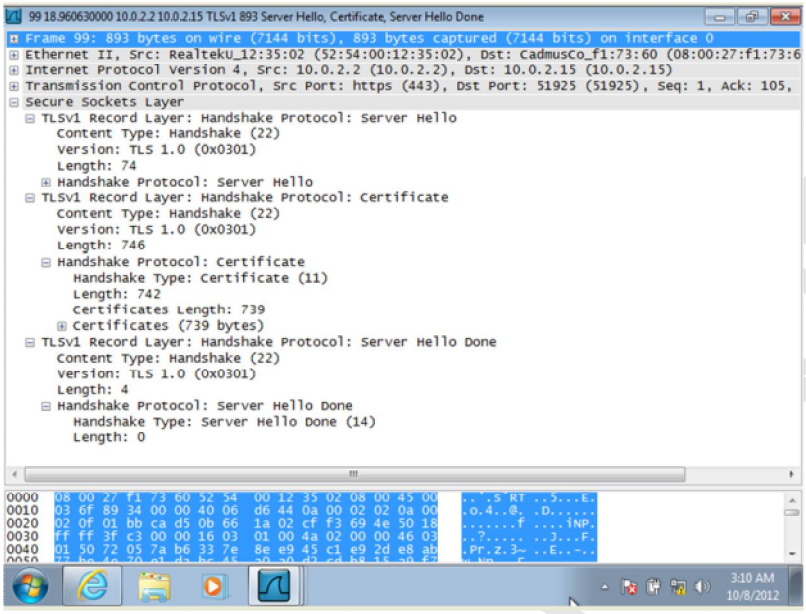
ChangeCipherSpec καθώς και το κρυπτογραφημένο μήνυμα EncryptedHandshakeMessage. Ο πελάτης το αποκρυπτογραφεί και επιβεβαιώνει την ορθότητα του αποτελέσματος της συνάρτησης κατακερματισμού.

Εάν κάποιο από τα προηγούμενα βήματα αποτύχει, η χειραψία αποτυγχάνει και δεν εγκαθίσταται σύνδεση. Από εδώ και πέρα τα μηνύματα εφαρμογής ApplicationData είναι κρυπτογραφημένα. Το μόνο που δεν μπορεί να κρυπτογραφηθεί είναι ότι ένας συγκεκριμένος client μιλάει με έναν συγκεκριμένο server. Αυτό, όμως ,μπορεί να υπερκεραστεί αν χρησιμοποιηθεί το SSL με proxy server.

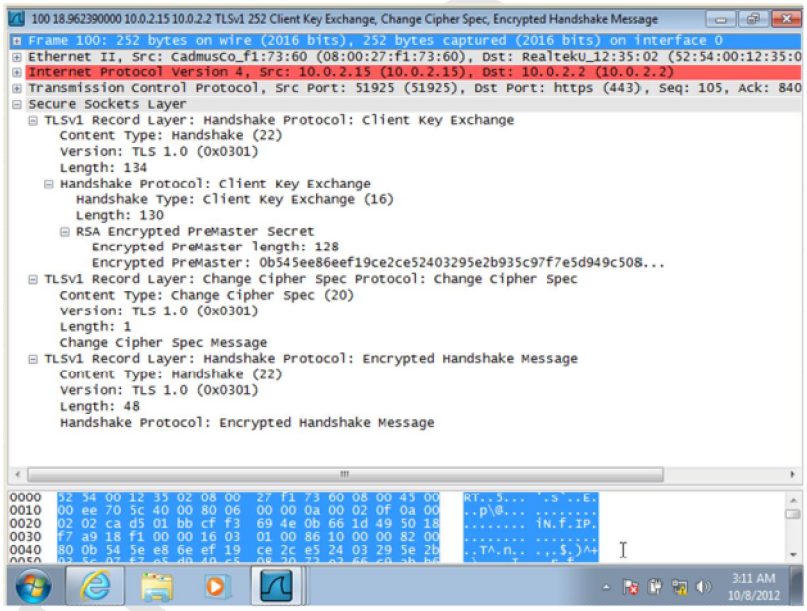
Τα παραπάνω μπορούμε να τα δούμε στα πακέτα 97 (client hello),99 (server hello), 100 (client key exchange), 102 (change cipher spec), 150 (encrypted application data).



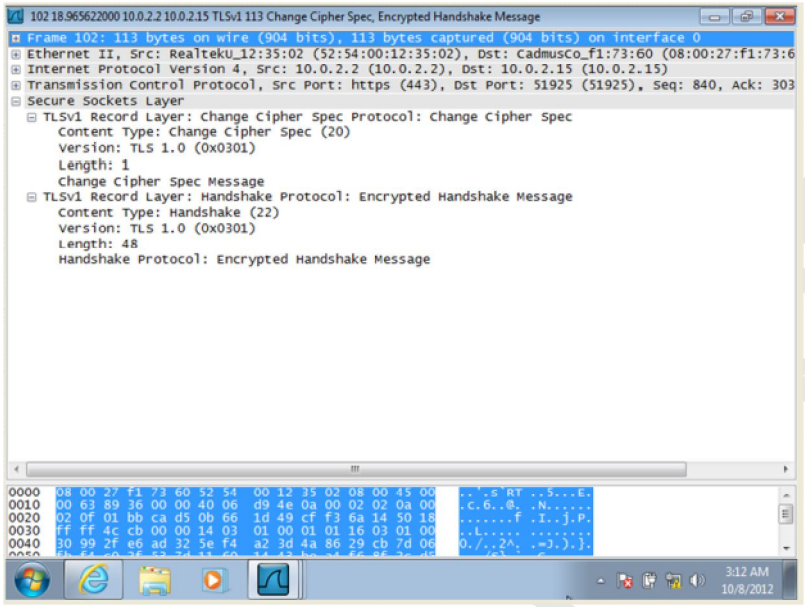
Εικόνα 32 Μύνημα Client Hello



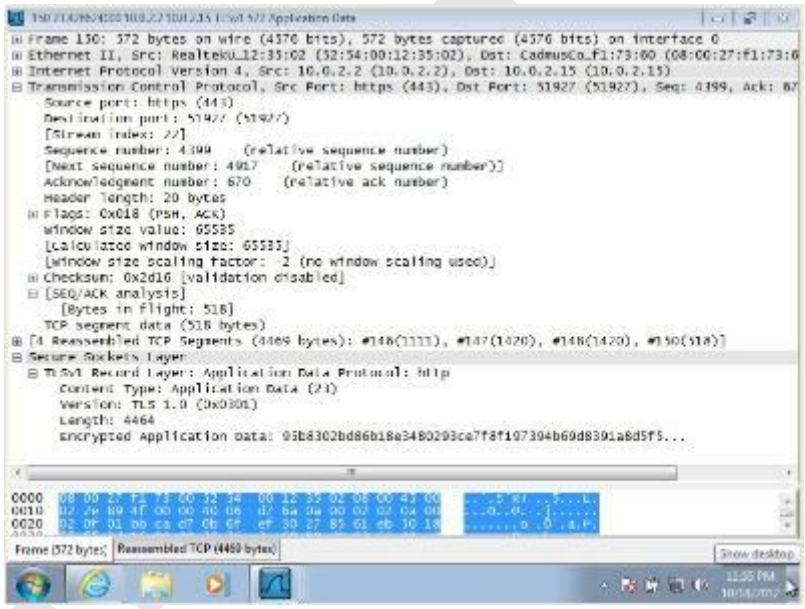
Εικόνα 33 Μήνυμα Server Hello, certificate, Server Hello Done



Εικόνα 34 Client Key Exchange



Εικόνα 35 Change Cipher Spec



Εικόνα 36 Encrypted Application Data

5.7.4 **Πλατφόρμα προστασίας δεδομένων** P3P

Με βάση όσα προαναφέρθηκαν στο κεφάλαιο 3.4 το πρώτο βήμα που θα πρέπει να γίνει, είναι η ενσωμάτωση στην ιστοσελιδα μιας ευανάγνωστης μορφής της πολιτικής που θα ακολουθηθεί ώστε ο επισκέπτης να είναι ενήμερος για τον τρόπο με τον οποίο πρόκειται να χρησιμοποιηθούν τα δεδομένα του. Ένα παράδειγμα πολιτικής σε φυσική γλώσσα μπορούμε να δούμε στο Παράρτημα [73].

Στη συνέχεια δημιουργούμε το P3P Policy reference site σε γλώσσα XML. Το αρχείο αυτό είναι το πρώτο που ψάχνει ένας user agent όταν επισκέπτεται την ιστοσελίδα.Ουσιαστικά

παρέχει έναν “χάρτη” για το πού βρίσκεται η πολιτική (ή οι πολιτικές) καθώς και ποια πολιτική συνδέεται με ποιο directory, ιστοσελίδα ή cookie. Το αρχείο αυτό θα το βρούμε στο /w3c directory του server και ονομάζεται p3p.xml. Αν και αυτή η μέθοδος είναι η προτιμότερη, εντούτοις μπορούμε να στείλουμε στον server μία HTTP header response δίνοντας του τη θέση του reference file ή ακόμα και να παραμετροποιήσουμε το HTML περιεχόμενο της ιστοσελιδας ώστε αυτό να περιέχει συνδέσεις για το reference file [59]. Παρακάτω μπορούμε να δούμε το reference file που φτιάξαμε για την ιστοσελίδα μας www.elentestpage.com

```
<META xmlns="http://www.w3.org/2002/01/P3Pv1">
<POLICY-REFERENCES>
   <POLICY-REF about="http://www.elentestpage.com/Privacy_policy/policy.xml">
    <INCLUDE>/*</INCLUDE>
    <COOKIE-INCLUDE/>
   </POLICY-REF>
</POLICY-REFERENCES>
</META>
```

Διαπιστώνουμε ότι το policy file βρίσκεται στη διεύθυνση www. elentestpage.com αποθηκευμένο στο φάκελο w3c και είναι διαθέσιμο για όλους τους πόρους του elentestpage εφόσον υπάρχει το tag include που περιλαμβάνει το /* χωρίς exclude tag. Τέλος, το reference file είναι βασισμένο στην έκδοση 1 του P3P, όπως βλέπουμε στην δεύτερη γραμμή.

Υπάρχει, επίσης, ένα P3P Policy File σε XML format, το οποίο περιλαμβάνει την πολιτική (ή τις πολιτικές) που ακολουθεί η ιστοσελίδα.

```
<?xml version="1.0"?>
<POLICIES xmlns="http://www.w3.org/2002/01/P3Pv1">
   <!-- Generated by IBM P3P Policy Editor version Beta 1.12 built 2/27/04 1:19 PM -->

   <!-- Expiry information for this policy -->
   <EXPIRY date="Tue, 01 Jan 2013 12:00:00 GMT"/>

<POLICY
   name="privacypolicy"
   discuri="http://www. elentestpage.com/legal.htm"
   opturi="www. elentestpage.com/legal.htm"
   xml:lang="en">
   <!-- Description of the entity making this policy statement. -->
   <ENTITY>
   <DATA-GROUP>
<DATA ref="#business.name">Elen Test Page</DATA>
<DATA ref="#business.contact-info.online.email">info@ elentestpage.com</DATA>
<DATA ref="#business.contact-info.online.uri">http://www. elentestpage.com</DATA>
<DATA ref="#business.contact-info.telecom.telephone.number">0030-210-3245678</DATA>
<DATA ref="#business.contact-info.postal.organization">Elen Test Page</DATA>
<DATA ref="#business.contact-info.postal.street">123 Athens str.        </DATA>
<DATA ref="#business.contact-info.postal.city">Athens</DATA>
```

```
<DATA ref="#business.contact-info.postal.stateprov">Attica</DATA>
<DATA ref="#business.contact-info.postal.postalcode">12345</DATA>
<DATA ref="#business.contact-info.postal.country">Greece</DATA>
  </DATA-GROUP>
  </ENTITY>

  <!-- Disclosure -->
  <ACCESS><none/></ACCESS>


  <!-- Disputes -->
  <DISPUTES-GROUP>
    <DISPUTES resolution-type="law"
  service="http://europa.eu.int/internal_market/privacy/law_en.htm#directive" short-
  description="Directive 95/46/EC">
      <LONG-DESCRIPTION>Published in Official Journal L 281, 23/11/1995 P.0031-0050:
  " Directive 95/46/EC of the European Parliament and of the Council 24 October 1995 on
  the protection of individuals with regard to the processing of personal data and on the free
  movement of such data" </LONG-DESCRIPTION>
      <REMEDIES><law/></REMEDIES>
    </DISPUTES>
  </DISPUTES-GROUP>

  <!-- Statement for group "New Group" -->
  <STATEMENT>
    <EXTENSION optional="yes">
      <GROUP-INFO xmlns="http://www.software.ibm.com/P3P/editor/extension-1.0.html"
  name="New Group"/>
    </EXTENSION>

  <!-- No consequence specified -->

  <!-- Use (purpose) -->
  <PURPOSE><admin/><contact required="opt-in"/><current/><develop/><pseudo-
  analysis/><pseudo-decision/><individual-analysis/><individual-decision/><tailoring
  required="opt-out"/><historical/><telemarketing required="opt-in"/></PURPOSE>

  <!-- Recipients -->
  <RECIPIENT><ours/><same required="opt-in"/><other-recipient required="opt-
  in"/><delivery required="opt-in"/><public/><unrelated required="opt-in"/></RECIPIENT>

  <!-- Retention -->
  <RETENTION><indefinitely/></RETENTION>

  <!-- Base dataschema elements. -->
  <DATA-GROUP>
```

```
    <DATA ref="#dynamic.clickstream"/>
    <DATA ref="#user.name"/>
    <DATA ref="#user.bdate"/>
    <DATA ref="#user.cert"/>
    <DATA ref="#user.home-info"/>
    <DATA ref="#dynamic.miscdata"><CATEGORIES><physical/></CATEGORIES></DATA>
    <DATA ref="#dynamic.miscdata"><CATEGORIES><online/></CATEGORIES></DATA>
    <DATA ref="#dynamic.miscdata"><CATEGORIES><uniqueid/></CATEGORIES></DATA>
    <DATA ref="#dynamic.miscdata"><CATEGORIES><purchase/></CATEGORIES></DATA>
    <DATA ref="#dynamic.miscdata"><CATEGORIES><computer/></CATEGORIES></DATA>
    <DATA
      ref="#dynamic.miscdata"><CATEGORIES><navigation/></CATEGORIES></DATA>
    <DATA ref="#dynamic.miscdata"><CATEGORIES><location/></CATEGORIES></DATA>
    <DATA                                                    ref="#dynamic.cookies"
      optional="yes"><CATEGORIES><computer/><content/><interactive/><location/><navigati
      on/><online/><physical/><preference/><purchase/><uniqueid/></CATEGORIES></DATA
      >
    </DATA-GROUP>
  </STATEMENT>

  <!-- End of policy -->
  </POLICY>
  </POLICIES>
```

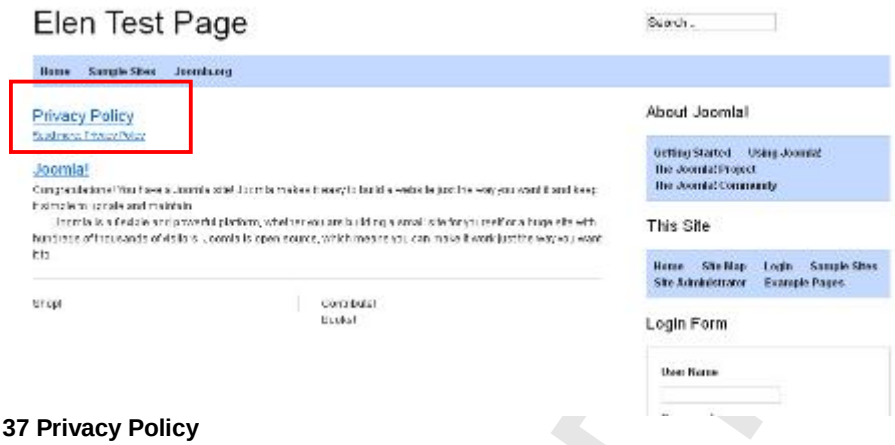
Σύμφωνα με το παραπάνω policy file:

- Μια ευανάγνωστη μορφή της πολιτικής μπορεί να βρεθεί στη θέση legal.htm
- Στο element entity μπορούμε να βρούμε πληροφορίες για την ιστοσελίδα και την εταιρεία.
- Το βαθμό πρόσβασης που έχει ο χρήστης στα δεδομένα που συλλέγει η ιστοσελίδα και αφορούν το πρόσωπό του (στο συγκεκριμένο παράδειγμα δεν έχει καμία πρόσβαση).
- Στη συνέχεια, καθορίζει τον τρόπο επίλυσης πιθανών διαφορών που ίσως ανακύψουν καθώς και με ποια νομοθεσία είναι σύμφωνη η πολιτική που ακολουθείται από την συγκεκριμένη ιστοσελίδα (στο συγκεκριμένο παράδειγμα η ιστοσελίδα είναι σύμφωνη με την Κοινοτική οδηγία 95/46 και όποιες διαφωνίες προκύψουν θα επιλυθούν μέσω δικαστηρίων).
- Δηλώνει, επίσης, τι δεδομένα συλλέγονται και για ποιο σκοπό καθώς και ότι γίνεται χρήση cookies δίνοντας, βέβαια, τη δυνατότητα στον χρήστη να αποφασίσει αν θέλει να τα αποδεχτεί ή όχι.

Τέλος, υπάρχει και η compact policy, η οποία δηλώνει επιγραμματικά όλα τα παραπάνω:

```
CP="NON DSP LAW CURa ADMa DEVa TAIo PSAa PSDa IVAa IVDa CONi HISa TELi
OUR DELi SAMi UNRi PUBa OTRi IND PHY ONL UNI PUR COM NAV INT DEM CNT
PRE LOC"
```

Και τα τρία αυτά αρχεία (.html με την ευανάγνωστη μορφή της πολιτικής που ακολουθείται, p3p.xml, policy.xml) τα τοποθετήσαμε στο root directory του server μας ώστε να βρίσκουν εφαρμογή σε ολόκληρη την ιστοσελίδα.



Εικόνα 37 Privacy Policy

ΚΕΦΑΛΑΙΟ 6ο

Συμπεράσματα και προτάσεις μελλοντικής έρευνας

Όσο το Διαδίκτυο διαπερνά κάθε πτυχή της καθημερινότητας του σύγχρονου ανθρώπου, τόσο καθιστάται πιο επιτακτική η ανάγκη να περιοριστεί η μη εξουσιοδοτημένη συλλογή και χρήση των προσωπικών πληροφοριών του ατόμου, Ορισμένες χώρες,όπως η Σουηδία και ο Καναδάς,έχουν πολύ αυστηρούς νόμους για την προστασία του απορρήτου. Άλλες χώρες δεν έχουν κανένα νόμο. Για να παρακαμφεί το πρόβλημα, η Ευρωπαϊκή Ένωση εκδίδει οδηγία το 1997, η οποία αφορά την προστασία των ανθρωπίνων δικαιωμάτων στον τηλεπικοινωνιακό τομέα. Οι υπολογιστές, όμως, και η τεχνολογία διασύνδεσης αναπτύσσονται εξαιρετικά γρήγορα και σύμφωνα με το νόμο του Moore το υπολογιστικό υλικό διπλασιάζεται σε ισχύ κάθε δύο χρόνια. Έτσι, λοιπόν, καθιστούν όλο και πιο εύκολη τη συλλογή, αποθήκευση και διεξαγωγή αναζητήσεων σε τεράστια ποσά πληροφοριών. Δεν χρειάζεται να είναι κανείς κατάσκοπος για να μπορέσει να έχει πρόσβαση σε αυτές τις πληροφορίες. Το μόνο που χρειάζεται είναι ένας packet sniffer, ο οποίος παγιδεύει την κίνηση που βρίσκεται μέσα στην επικράτειά του. Κάθε συνδεδεμένος υπολογιστής αποτελεί πιθανό στόχο.

Ο ωτακουστής είναι ένας επιτιθέμενος, ο οποίος λαμβάνει ένα αντίγραφο των πακέτων που στέλνονται ή λαμβάνονται από τις εφαρμογές και τα πρωτόκολλα που εκτελούνται στον υπολογιστή μας. Μπορεί, λοιπόν, με αυτόν τον τρόπο να αποκαλύψει τον αποστολέα ή τον παραλήπτη κάθε πακέτου. Αυτή η επίθεση αποτελεί μία από τις σημαντικότερες ενάντια στη διασφάλιση της ιδιωτικότητας και της ανωνυμίας στο διαδίκτυο. Στη συγκεκριμένη εργασία εστιάσαμε στην προστασία της ιδιωτικότητας με δυνατότητα ανωνυμίας στο Διαδίκτυο μέσω του TOR browser, στην κρυπτογράφηση της επικοινωνίας μέσω πρωτοκόλλου SSL καθώς και στην πλατφόρμα προστασίας P3P. Τα συμπεράσματα στα οποία καταλήξαμε καθώς και οι προτάσεις μας για περαιτέρω μελέτη είναι οι εξής:

Το Onion Routing χρησιμοποιεί ισχυρή κρυπτογραφία απέναντι σε επιθέσεις κατά της ανωνυμίας του χρήστη στο επίπεδο του δικτύου (IP layer). Η ανωνυμία παραβιάζεται μόνο αν γίνει παρακολούθηση όλων των κόμβων που συμμετέχουν στο κύκλωμα, αφού κάθε μεταβιβαστής δεν μπορεί να δει πάνω από έναν κόμβο στο κύκλωμα. Βασικό μειονέκτημα του TOR είναι η αργή απόδοσή του και οι μελλοντικές έρευνες θα πρέπει να εστιάσουν στη βελτίωση αυτής προκειμένου το TOR να γίνει ευρέως αποδεκτό. Πιθανή λύση θα ήταν να ερευνήσουμε κατά πόσο αλλάζοντας κάποιες παραμέτρους όπως π.χ. ο αριθμός των κόμβων στο ανώνυμο δίκτυο, θα μπορέσει να οδηγήσει σε μικρότερο χρόνο αναμονής και ταυτόχρονα να έχει θετική επίδραση στην διατήρηση της ανωνυμίας [58]

Το SSL προσφέρει ένα υψηλό επίπεδο προστασίας στο επίπεδο της συνόδου (session layer) καθώς στην κρυπτογράφηση χρησιμοποιεί ένα συνδυασμό συμμετρικού και δημοσίου κλειδιού. Η κρυπτογράφηση συμμετρικού κλειδιού είναι είναι πολύ πιο γρήγορη και αποδοτική σε σχέση με την κρυπτογράφηση του δημοσίου, η οποία, όμως προσφέρει καλύτερες τεχνικές πιστοποίησης. Οι τεχνικές, λοιπόν, κρυπτογράφησης αλλά και αποκρυπτογράφησης που χρησιμοποιούνται εξασφαλίζουν ότι η επικοινωνία προστατεύεται από ωτακουστές.Βέβαια,ένα μειονέκτημά του είναι ότι αυξάνει τα διακινούμενα πακέτα και συνεπώς καθυστερεί την μετάδοση των πληροφοριών επειδή χρησιμοποιεί μεθόδους κρυπτογράφησης και αποκρυπτογράφησης. Λόγω αυτών των επιβαρύνσεων το πρωτόκολλο SSL χρησιμοποιείται πλέον μόνο σε περιπτώσεις όπου πραγματικά απαιτείται ασφαλής σύνδεση (π.χ μετάδοση κωδικών χρήστη ή αριθμών πιστωτικών καρτών μέσω Διαδικτύου) και όχι σε περιπτώσεις απλής επίσκεψης σε μια ιστοσελίδα.

Τέλος, το P3P που εξετάσαμε παραπάνω, επιτρέπει στο χρήστη να εκφράσει τις προτιμήσεις ιδιωτικότητάς του σε όποια ιστοσελίδα επισκέπτεται και να προσδιορίσει ο ίδιος κατά πόσο επιθυμεί ή όχι να συλλεχθούν τα προσωπικά του δεδομένα από τον πάροχο υπηρεσιών. Βέβαια, παρά τις δυνατότητες που έχει πρέπει να αναγνωρίσομε ότι δεν περιέχει καμία δυνατότητα εφαρμογής τεχνικών ανωνυμίας, ψευδωνυμίας, κρυπτογράφησης κ.α. Κύριος στόχος του P3P είναι η διαπραγμάτευση και η αξιολόγηση συγκεκριμένων στοιχείων της

πολιτικής ασφαλείας και όχι η προσφορά μηχανισμών προστασίας. Έτσι, τα μεταδιδόμενα πακέτα δεν προστατεύονται από τις επιθέσεις των ωτακουστών, οι οποίοι έχουν στη διάθεσή τους όλη την απαιτούμενη πληροφορία [37].

Συμπερασματικά,τα μέτρα που είναι δυνατόν να ληφθούν για την προστασία της ανωνυμίας και των δεδομένων είναι πολλά και διάφορα. Προτού, όμως, επιλέξουμε κάποια λύση θα πρέπει να αναρωτηθούμε κατά πόσο εμπιστευόμαστε την εταιρεία που μου παρέχει τη συγκεκριμένη λύση. Από τη στιγμή που η ασφάλεια των προσωπικών μας στοιχείων στηρίζεται σε κάποιον τρίτο, η απάντηση που θα δώσουμε καθορίζει και πόσο σίγουροι μπορούμε να νιώσουμε.

Και φυσικά δεν πρέπει να μας διαφεύγει το γεγονός ότι ό,τι μέτρα και να εγκαταστήσουμε θα πρέπει πάντα να συνδυάζονται με παραδοσιακές αρχές ασφάλειας όπως η φυσική και η ασφάλεια προσωπικού. Η φυσική ασφάλεια γενικά είναι μία από τις συχνότερα παραμελημένες μορφές ασφάλειας λόγω του ότι τα θέματα που περικλείει – οι απειλές, οι πρακτικές και οι διαθέσιμες προφυλάξεις - είναι διαφορετικές για κάθε υπολογιστική εγκατάσταση. Η εκπαίδευση των χρηστών θα πρέπει να περιλαμβάνει διαδικασίες για την επιλογή και χρήση των κωδικών πρόσβασης, πολιτικές για την πρόσβαση του υπολογιστικού συστήματος, πολιτικές για την αποκάλυψη πληροφοριών κ.α.. Ας μην ξεχνάμε ότι όσο οι τεχνολογίες ασφάλειας θα συνεχίζουν να βελτιώνονται, κάνοντας ολοένα και πιο δύσκολη την εκμετάλλευση των τεχνικών ευπαθειών, τόσο οι εισβολείς θα στρέφουν την προσοχή τους στην εκμετάλλευση του ανθρώπινου παράγοντα.

ΠΑΡΑΡΤΗΜΑ

Privacy Policy

About Us

This is a privacy policy for Elen Test Page. Our homepage on the Web is located at http://www.elentestpage.com . The full text of our privacy policy is available on the Web at http://www. elentestpage.com /legal.htm Users may go to www. elentestpage.com /legal.htm for information on how to opt-in or opt-out of use of their information.

We invite you to contact us if you have questions about this policy. You may contact us by mail at the following address:

Elen Test Page
123 Athens str.
Athens, Attica 12345
Greece

You may contact us by e-mail at info@ elentestpage.com. You may call us at 0030-210-3245678.

Dispute Resolution and Privacy Seals

We have the following privacy seals and/or dispute resolution mechanisms. If you think we have not followed our privacy policy in some way, they can help you resolve your concern.

- **Directive 95/46/EC**: Published in Official Journal L 281, 23/11/1995 P.0031-0050: " Directive 95/46/EC of the European Parliament and of the Council 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data"

Additional Information

This policy is valid until 1 Ιαν, 2013 at 12:00:00 EET.

Data Collection

P3P policies declare the data they collect in groups (also referred to as "statements"). This policy contains 1 data group.

Group "New Group"

We collect the following information:

- Click-stream data
- User's Name
- User's Birth Date
- User's Identity certificate

- User's Home Contact Information
- Physical contact information
- Online contact information
- Unique identifiers
- Purchase information
- Computer information
- Navigation and click-stream data
- Current location data

At the user's option, we may also collect the following data:

- HTTP cookies

This data will be used for the following purposes:

- Completion and support of the current activity.
- Web site and system administration.
- Research and development.
- One-time tailoring. The user is allowed to **opt-out** of this usage.
- Anonymous user analysis.
- Anonymous user profiling and decision-making.
- User analysis.
- User profiling and decision-making.
- Contacting visitors for marketing of services or products. The user must **opt-in** to this usage.
- Telemarketing. The user must **opt-in** to this usage.
- Historical preservation.

This data will be used by ourselves and our agents. In addition, the following types of entities will receive this information:

- Delivery services. The user must **opt-in** to this data sharing.
- Others following the same practices. The user must **opt-in** to this data sharing.
- Others following different practices. The user must **opt-in** to this data sharing.
- Unrelated third parties. The user must **opt-in** to this data sharing.
- The general public.

Cookies

Cookies are a technology which can be used to provide you with tailored information from a Web site. A cookie is an element of data that a Web site can send to your browser, which may then store it on your system. You can set your browser to notify you when you receive a cookie, giving you the chance to decide whether to accept it.

Our site makes use of cookies. Cookies are used for the following purposes:

- Site administration
- Contacting users
- Completing the user's current activity
- User targeting

- Pseudononymous analysis
- Pseudonym-based decision-making
- User analysis
- Individual-based decision-making
- Research and development

Compact Policy Summary

The compact policy which corresponds to this policy is:

CP="NON DSP LAW CURa ADMa DEVa TAIo PSAa PSDa IVAa IVDa CONi HISa TELi OUR DELi SAMi UNRi PUBa OTRi IND PHY ONL UNI PUR COM NAV INT DEM CNT PRE LOC"

The following table explains the meaning of each field in the compact policy.

Field	Meaning
CP=	This is the compact policy header; it indicates that what follows is a P3P compact policy.
NON	No access is available to collected information.
DSP	The policy contains at least one dispute-resolution mechanism.
LAW	Privacy law specifies penalties for a violation of this policy.
CURa	The data is used for completion of the current activity.
ADMa	The data is used for site administration.
DEVa	The data is used for research and development.
TAIo	The data is used for tailoring the site, unless the user chooses otherwise.
PSAa	The data is used for pseudononymous analysis.
PSDa	The data is used for pseudononymous decision-making.
IVAa	The data is used for analysis, including knowledge of the visitor's identity.
IVDa	The data is used for decision-making, including knowledge of the visitor's identity.
CONi	The data is used for contacting the user, if the user selects it.
HISa	The data is used for historical archival purposes.
TELi	The data is used for telemarketing, if the user selects it.
OUR	The data is given to ourselves and our agents.
DELi	The data is given to delivery services, if the user selects it.

SAMi	The data is given to other organizations following the same practices, if the user selects it.
UNRi	The data is given to other, unrelated organizations, if the user selects it.
PUBa	The data is made public.
OTRi	The data is given to other organizations with different privacy practices, if the user selects it.
IND	The data will be kept indefinitely.
PHY	Physical contact information is collected.
ONL	Online contact information is collected.
UNI	Unique identifiers are collected.
PUR	Purchase information is collected.
COM	Computer information is collected.
NAV	Navigation and clickstream data is collected.
INT	Interactive data is collected.
DEM	Demographic and socioeconomic data is collected.
CNT	Content data is collected.
PRE	Preference information is collected.
LOC	Current location information is collected.

The compact policy is sent by the Web server along with the cookies it describes. For more information, see the P3P deployment guide at http://www.w3.org/TR/p3pdeployment.

Policy Evaluation

Microsoft Internet Explorer 6 will evaluate this policy's compact policy whenever it is used with a cookie. The actions IE will take depend on what privacy level the user has selected in their browser (Low, Medium, Medium High, or High; the default is Medium. In addition, IE will examine whether the cookie's policy is considered satisfactory or unsatisfactory, whether the cookie is a session cookie or a persistent cookie, and whether the cookie is used in a first-party or third-party context. This section will attempt to evaluate this policy's compact policy against Microsoft's stated behavior for IE6.

Note: this evaluation is currently experimental and should not be considered a substitute for testing with a real Web browser.

Unsatisfactory policy: this compact policy is considered *unsatisfactory* according to the rules defined by Internet Explorer 6. The behavior of Internet Explorer 6 regarding cookies set under this compact policy is as follows:

	First-party usage	Third-party usage
PersistentCookies	• **Low:** Policy satisfactory at this level; cookies will be accepted. • **Medium:** Opt-out is not provided for all unsatisfactory purposes and recipients, so the cookie will be **downgraded** to a session cookie. • **Medium High:** No opt-out is provided, so the cookie will be **blocked**. • **High:** Since opt-in is not required, the cookie will be **blocked**.	• **Low:** Opt-out is not provided for all unsatisfactory purposes and recipients, so the cookie will be **downgraded** to a session cookie. • **Medium:** Opt-out is not provided for all unsatisfactory purposes and recipients, so the cookie will be **blocked**. • **Medium High:** Since opt-in is not required, the cookie will be **blocked**. • **High:** Since opt-in is not required, the cookie will be **blocked**.
Session Cookies	• **Low:** Policy satisfactory at this level; cookies will be accepted. • **Medium:** Policy satisfactory at this level; cookies will be accepted. • **Medium High:** Policy satisfactory at this level; cookies will be accepted. • **High:** Since opt-in is not required, the cookie will be **blocked**.	• **Low:** Policy satisfactory at this level; cookies will be accepted. • **Medium:** Opt-out is not provided for all unsatisfactory purposes and recipients, so the cookie will be **blocked**. • **Medium High:** Since opt-in is not required, the cookie will be **blocked**. • **High:** Since opt-in is not required, the cookie will be **blocked**.

A policy which is considered unsatisfactory by Internet Explorer 6 contains certain categories of data which are used or shared in a particular manner. This policy is placed in the unsatisfactory category, because the following categories of data are associated with this policy's cookies:

- Physical contact information is collected.
- Online contact information is collected.

In addition, the data is used in the following manner, marking the policy as unsatisfactory:

- The data is used for analysis, including knowledge of the visitor's identity.
- The data is used for decision-making, including knowledge of the visitor's identity.
- The data is made public.
- The data is used for contacting the user, if the user selects it.
- The data is given to other organizations with different privacy practices, if the user selects it.
- The data is given to other organizations following the same practices, if the user selects it.
- The data is used for telemarketing, if the user selects it.
- The data is given to other, unrelated organizations, if the user selects it.

Note that allowing an opt-out will make this policy acceptable under the Low and Medium settings, and under Medium High for first-party cookie usage. At the High setting, and at the Medium High setting for third-party cookies, all of these data uses must be opt-in for the policy to be considered satisfactory.

ΒΙΒΛΙΟΓΡΑΦΙΑ

ΚΕΦ.1

1. Warren, Bandeis (posted Febr 8.1999) ''The right to Privacy'', Harvard Law Review
2. Holvast Jan (2007), ''History of Privacy'', Holvast & Partner, Privacy consultants, NL-Landsmeer

Κεφ.2

3. Ευρωπαϊκή νομοθεσία ''Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου 1995 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών'' (http://eur-lex.europa.eu τελευταία πρόσβαση 22.9.2011)
4. Επίσημη ιστοσελίδα της Ευρώπης ''Επεξεργασία δεδομένων προσωπικού χαρακτήρα'' (http://europa.eu/legislation_summaries/information_society/data_protection/l14012_el.htm τελευταία πρόσβαση 22.9.2011)
5. Υπουργείο ανάπτυξης-Ε.Π Κοινωνία της πληροφορίας-E-business forum ''Μελέτη αξιολόγησης και βασικού σχολιασμού αναφορικά με το θεματικό περιεχόμενο της Οδηγίας 2002/58/ΕΚ του Ευρωπαϊκού κοινοβουλίου και του Συμβουλίου σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα και της προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών'' (http://www.ebusinessforum.gr τελευταία πρόσβαση 22.9.2011)
6. Αρχή προστασίας δεδομένων προσωπικού χαρακτήρα (http://www.dpa.gr/portal/page?_pageid=33,19052&_dad=portal&_schema=PORTAL τελευταία πρόσβαση 22.9.2011)
7. Αρχή προστασίας δεδομένων προσωπικού χαρακτήρα (http://www.dpa.gr/portal/page?_pageid=33,123437&_dad=portal&_schema=PORTAL τελευταία πρόσβαση 22.9.2011)
8. Horniak Virginia (2004), ''Privacy of Communication-Ethics and Technology'' Malardalen University
9. Jacobson Andreas (2008), ''Privacy and security in internet-based information systems'' Blekinge Institute of Technology
10. G.W van Blarkom, Borking J.J, Olk J.G.E (2003) ''Handbook of Privacy and Privacy-Enhancing technologies. The case of intelligent software agents'', College bescherming persoonsgegevens
11. Stanford encyclopedia of Philosophy ''Privacy'' 2006
12. Ιγγλεζάκης Δημήτρης ,'' Προστασία προσωπικών δεδομένων στις ηλεκτρονικές επικοινωνίες'' Τμήμα Πληροφορικής και Οικονομικών επιστημών του ΑΠΘ, (http://dpms.csd.auth.gr/)
13. Μήτρου Λίλιαν, ''Αρχές δικαίου και προστασία προσωπικών δεδομένων'' Πανεπιστήμιο Αιγαίου, σημειώσεις μαθήματος.
14. Παπαδόπουλος Μαρίνος, 2ο Πανελλήνιο Συνέδριο για το Ηλεκτρονικό Έγκλημα,2004 (http://www.md5.gr/el/index.php)

Κείμενα από διαδίκτυο

15. http://en.wikipedia.org/wiki/Privacy (τελευταία πρόσβαση 22.9.2011)
16. Privacy International (www.privacyinternational.org τελευταία πρόσβαση 22.9.2011)
17. McDougall Bonnie '' Privacy- The psychological function and philosophical values of privacy'', Science Encyclopedia (http://science.jrank.org/ τελευταία πρόσβαση 22.9.2011
18. Ύπατη αρμοστεία του ΟΗΕ (www.unhcr.gr τελευταία πρόσβαση 22.9.2011

19. Περιφερειακό κέντρο πληροφόρησης των Ηνωμένων Εθνών (http://www.unric.org τελευταία πρόσβαση 22.9.2011)
20. Ενημερωτικός Κόμβος Πανελλήνιου σχολικού δικτύου-Ασφάλεια στο διαδίκτυο (http://blogs.sch.gr/internet-safety/archives/309 τελευταία πρόσβαση 22.9.2011)
21. '' Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data'' Συμβούλιο της Ευρώπης (http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm τελευταία πρόσβαση 22.9.2011)
22. Ευρωπαϊκή επιτροπή, '' Γνώμη της Ομάδας Εργασίας του άρθρου 29 για την χρήση των δεδομένων θέσης με σκοπό την παροχή υπηρεσιών προστιθέμενης αξίας'' (2005) (http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp115_el.pdf τελευταία πρόσβαση 22.9.2011)
23. ''Το απαραβίαστο της ιδιωτικής ζωής και τα ΜΜΕ'' (http://greeklaws.com/pubs/uploads/2113.pdf τελευταία πρόσβαση 22.9.2011)
24. ''Προστασία της ιδιωτικής ζωής, άρθρο 9 του Συντάγματος'' (http://www.greeklaws.com/pubs/uploads/49.pdf τελευταία πρόσβαση 22.9.2011)

ΚΕΦ.3

25. http://portal.kathimerini.gr/4Dcgi/4dcgi/_w_articles_kathworld_7_27/04/2011_388788
26. Πατσός Δημήτρης '' Αποτελεσματική διοικητική υποστήριξη ασφάλειας δικτύων και επικοινωνιών-Αναγνώριση και αντιμετώπιση περιστατικών'', Πανεπιστήμιο Πειραιώς 2009
27. Horniak Virginia ''Privacy of communication-Ethics and technology'' Malardalen University, 2004
28. Γρηγοράτος Βαλάντης ''Εισαγωγή στην ασφάλεια πληροφοριακών συστημάτων και την διαχείρηση της πληροφορίας''
29. Shields Clay, Levine Brian ''A protocol for anonymous communication over the Internet'', 2000
30. Gritzalis Stefanos,''Enhancing web privacy and anonymity in the digital era'', Information management & computer security, vol.12, No 3, 2004, p.255-288
31. Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης (www.caclab.csd.auth.gr τελευταία πρόσβαση 25.10.2011)
32. ''Protecting aggregated data'', US-CERT, Dec 2005.
33. Solove Daniel J. (August 2001) ''Access and aggregation. Public records, privacy and the constitution''
34. Solove Daniel J. (January 2006) ''A taxonomy of Privacy'' University of Pensylvania Law review, vol.154
35. Omer Tene '' What Google knows: Privacy and Internet search engines'' Utah Law review.1434 (2008)
36. Breach of privacy and Confidentiality under information Technology Act, 2000 (http://www.legalserviceindia.com/article/l288-Breach-of-privacy-&-Confidentiality-.html τελευταία πρόσβαση 25.10.2011)
37. Λαμπρινουδάκης Κων., Μήτρου Λίλιαν, Γκρίτζαλης Στέφανος, Κάτσικας Σωκράτης '' Προστασία της ιδιωτικότητας & Τεχνολογίες Πληροφορικής και επικοινωνιών-Τεχνικά και νομικά θέματα'', εκδ. Παπασωτηρίου, Αθήνα 2010
38. Pfitzmann Andreas, Hansen Marit ''Anonymity, unlinkability, undetectability, unobservability, pseudonymity and identity management-a consolidated proposal for terminology'', version v0.31, Feb.15, 2008
39. Von Tilborg Henk C.A ''Encyclopedia of cryptography and security'', Springer

ΚΕΦ.4

40. Enterprise Privacy group '' Privacy by design-an overview of Privacy Enhancing Technologies'' 2008
41. Van Blarkom, G.W , Borking J.J., Olk J.G.E. '' Handbook of Privacy and PET- The case of intelligent software agents'' The Hague, 2003
42. Oppliger R. ''Privacy protection and anonymity services for the World Wide Web '' Elsevier, Future generation computer systems 16 (2000) 379-391
43. Kristol D., Gabber E., Gibbons P. ''Design and implementation of the lucent personalized web assistant (LPWA)'' Information sciences research center, June 1998
44. Gabber E., Gibbons P., Kristol D., ''Consistent yet anonymous web access with LPWA'' Information sciences research center, October 1998
45. Gritzalis St. (No. 3, 2004) '' Enhancing Web privacy and anonymity in the digital era'' Information Management & Computer Security Vol. 12 pp. 255-288 , Emerald Group Publishing Limited
46. Dingledine R., Mathewson N., Syverson P. ''TOR: The second generation onion router'' Published in: Proceedings of the 13th conference on USENIX Security Symposium-Volume 13
47. Reed M., Syverson P. Goldschlag D., '' Anonymous connections and onion routing'' IEE journal on selected areas in communications, vol. 16, No. 4, May 1998
48. Jeff Tyson ''How virtual private networks work'' found at http://www.scribd.com/doc/55172926/How-Virtual-Private-Networks-Work (τελευταία πρόσβαση 15.12.2011)
49. www.verisign.com
50. Stallings William ''Cryptography and Network security'' 5th edition
51. ''An introduction to Cryptography'' released June 8, 2004 by PGP Corporation.
52. Lindskog H., Lindskog S. ''Web site privacy with P3P'' Wiley Publishing, Inc. 2003
53. www.w3c.org
54. Subirana B, Bain M. (2005) ''Integrated series in information systems-Legal programming Designing Legally Compliant RFID and Software Agent Architectures for Retail Processes and Beyond'', Volume 4, 193-244
55. Cranor L. '' P3P: making privacy policies more useful'', IEEE Computer society, 2003
56. Cranor L. ''Web privacy with P3P'' O'Reilly and associates, Sept.2002

ΚΕΦ.5

57. http://www.openssl.org/
58. Muller S., Brecht F., Fabian B., Kunz S., Kunze D. ,'' Distributed performance and Usability assesment of the TOR anonymization Network'' article in Future Internet 2012,4, 488-513, www.mpdi.com/journal/futureinternet
59. http://p3ptoolbox.org/guide/section4.shtml#toc