ΧΑΡΟΚΟΠΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ

ΣΧΟΛΗ ΨΗΦΙΑΚΗΣ ΤΕΧΝΟΛΟΓΙΑΣ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΜΑΤΙΚΗΣ
ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΜΑΤΙΚΗΣ
ΚΑΤΕΥΘΥΝΣΗ ΤΕΧΝΟΛΟΓΙΕΣ ΚΑΙ ΕΦΑΡΜΟΓΕΣ ΙΣΤΟΥ

Τίτλος Εργασίας Κατά πόσο το FOAF ενισχύει τα κενά Ιδιωτικότητας στα Κοινωνικά δίκτυα

Διπλωματική Εργασία

Νικόλαος Υφαντόπουλος

Αθήνα, 2017

ΧΑΡΟΚΟΠΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ

ΣΧΟΛΗ ΨΗΦΙΑΚΗΣ ΤΕΧΝΟΛΟΓΙΑΣ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΜΑΤΙΚΗΣ
ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΜΑΤΙΚΗΣ
ΚΑΤΕΥΘΥΝΣΗ ΤΕΧΝΟΛΟΓΙΕΣ ΚΑΙ ΕΦΑΡΜΟΓΕΣ ΙΣΤΟΥ

Τριμελής Εξεταστική Επιτροπή

Ηρακλής Βαρλάμης
Επίκουρος Καθηγητής, Τμήμα Πληροφορικής και Τηλεματικής,
Χαροκόπειο Πανεπιστήμιο

Δημήτριος Μιχαήλ
Επίκουρος Καθηγητής, Τμήμα Πληροφορικής και Τηλεματικής,
Χαροκόπειο Πανεπιστήμιο

Κωνσταντίνος Τσερπές
Επίκουρος Καθηγητής, Τμήμα Πληροφορικής και Τηλεματικής,
Χαροκόπειο Πανεπιστήμιο

Ο Νικόλαος Υφαντόπουλος

δηλώνω υπεύθυνα ότι:

1) Είμαι ο κάτοχος των πνευματικών δικαιωμάτων της πρωτότυπης αυτής εργασίας και από όσο γνωρίζω η εργασία μου δε συκοφαντεί πρόσωπα, ούτε προσβάλει τα πνευματικά δικαιώματα τρίτων.

2) Αποδέχομαι ότι η ΒΚΠ μπορεί, χωρίς να αλλάξει το περιεχόμενο της εργασίας μου, να τη διαθέσει σε ηλεκτρονική μορφή μέσα από τη ψηφιακή Βιβλιοθήκη της, να την αντιγράψει σε οποιοδήποτε μέσο ή/και σε οποιοδήποτε μορφότυπο καθώς και να κρατά περισσότερα από ένα αντίγραφα για λόγους συντήρησης και ασφάλειας.

ΕΥΧΑΡΙΣΤΙΕΣ

Αρχικά θα ήθελα να ευχαριστήσω θερμά τον επιβλέποντα της διπλωματικής μου, κ. Βαρλάμη Ηρακλή για την εμπιστοσύνη που μου έδειξε δίνοντάς μου τη δυνατότητα να την εκπονήσω στο συγκεκριμένο επιστημονικό τομέα.

Τέλος, θέλω να εκφράσω ένα τεράστιο ευχαριστώ στην οικογένεια μου, για την στήριξη και την εμπιστοσύνη που μου έδειξε όλα αυτά τα χρόνια των σπουδών μου.

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

Περίληψη στα Ελληνικά

Η έρευνα των κοινωνικών δικτύων και των συναφή θεμάτων, όπως η προστασία της ιδιωτικότητας στα κοινωνικά δίκτυα είναι ένας τομέας ο οποίος έχει απασχολήσει αρκετούς ερευνητές σήμερα, λόγω της ραγδαίας ανάπτυξης των σελίδων κοινωνικής δικτύωσης. Η ραγδαία αυτή ανάπτυξη, αποτυπώνεται σε αριθμούς ως εξής: το MySpace έχει πάνω από 125 εκατομμύρια χρήστες, το Facebook πάνω από 1 δισεκατομμύρια, το Twitter πάνω από 255 εκατομμύρια και το LinkedIn πάνω από 187 εκατομμύρια χρήστες. Ωστόσο, οι περισσότερες από τις σελίδες κοινωνικής δικτύωσης παρουσιάζουν δύο βασικά θέματα. Το πρώτο θέμα είναι ότι οι πληροφορίες που περιέχονται σε αυτές δεν είναι διαθέσιμες σε άλλες ιστοσελίδες ή τεχνολογίες του διαδικτύου και το δεύτερο είναι ότι έχουν τον αποκλειστικό έλεγχο των δεδομένων των χρηστών. Αυτό έχει πολλές φορές ως αποτέλεσμα, να εγείρονται θέματα προστασίας των προσωπικών δεδομένων των χρηστών και κατ' επέκταση και της ιδιωτικότητάς τους.

Μία αναδυόμενη λύση, η οποία μπορεί να προσφέρει τη δημιουργία ενός αποκεντρωμένου κοινωνικού δικτύου, είναι με τη χρήση της οντολογίας FOAF. Η οντολογία αυτή στηρίζεται στο μοντέλο RDF και μπορεί να εμπλουτιστεί από άλλες οντολογίες με σκοπό τη σύνδεση απομακρυσμένων πληροφοριών και τη δημιουργία ενός κοινωνικού δικτύου, στο οποίο κανένας χρήστης δεν θα χρειάζεται να δημιουργήσει λογαριασμό και επιπλέον θα διαλέγει τον εξυπηρετητή (Server) της εμπιστοσύνης του.

Σκοπός της εν λόγω διπλωματικής εργασίας είναι να εξετάσει κατά πόσο το λεξιλόγιο της FOAF (και κατ' επέκταση τα FOAF έγγραφα) μπορεί να συντελέσει στη δημιουργία ενός αποκεντρωμένου δικτύου και να αναλύσει αν το δίκτυο αυτό μεταφέρει τα προβλήματα ιδιωτικότητας που παρουσιάζονται στις σελίδες κοινωνικής δικτύωσης, εγείρει καινούργια ή δρα τελείως απομονωνόμενα και ασφαλή.

Αναλυτικότερα, η εργασία είναι δομημένη σε τέσσερα κεφάλαια. Στο πρώτο κεφάλαιο παρουσιάζεται η έννοια της ιδιωτικότητας και γίνεται αναφορά στο απόρρητο των επικοινωνιών καθώς επίσης και στην οδηγία 94/46 του Ευρωπαϊκού Κοινοβουλίου για τη διασφάλιση της προστασίας των φυσικών προσώπων έναντι της

επεξεργασίας δεδομένων προσωπικού χαρακτήρα και την ελεύθερη κυκλοφορία των δεδομένων αυτών. Στο δεύτερο κεφάλαιο παρουσιάζεται η οντολογία FOAF (Friend-Of-A-Friend) και τα πλεονεκτήματά της και γίνεται συγκριτική ανάλυση των εγγράφων της FOAF με άλλες οντολογίες. Στο τρίτο κεφάλαιο αναφέρονται αρχικά οι κίνδυνοι και οι απειλές κατά της ιδιωτικότητας στις σελίδες κοινωνικής δικτύωσης και μετέπειτα αναλύονται οι απειλές κατά της ιδιωτικότητας στα FOAF έγγραφα. Τέλος, στο τέταρτο κεφάλαιο περιγράφονται μερικές ενδεικτικές λύσεις ασφάλειας για τα FOAF έγγραφα, ενώ στο πέμπτο γίνεται αξιολόγηση των αποτελεσμάτων και εξαγωγή συμπερασμάτων.

Λέξεις κλειδιά: Ιδιωτικότητα, Κοινωνικά δίκτυα, Friend-of-a-friend-Foaf, Κίνδυνοι, Απειλές, Ασφάλεια

Abstract

Researching social networks and related issues such as privacy in social networks is a vibrant field today, cause of the rapid growth of social networking. This rapid growth, was reflected in the pyramid of numbers as follows: Myspace has over 125 million users, Facebook more than 1 billion, Twitter over 255 million and LinkedIn more than 187 million users. Meanwhile, the most of the social networking sites present some issues. One of the two issue is that the information collected in them are not available on other websites or web technologies. The second one is that these sites have the sole control of user data and therefore is raised some issues of personal data protection and privacy issues.

An emerging solution that can provide a decentralized social network can be achieved by adopting the FOAF ontology. FOAF ontology is based on RDF model and can be enriched by other ontologies, in order to link information from different networking sites and also help the creation of a social network, in which each user no need to create an account and also choose his own web server depending of the level of confidence.

The purpose of this thesis is to examine how the vocabulary of FOAF (and so on the FOAF documents) could contribute to the creation of a decentralized network.

The rest of this thesis is structured as follows: Section I introduces the concept of privacy, reference the confidentiality of communications and also state the European Parliament and Council Directive 94/46 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Section II describe the FOAF (Friend-Of-A-Friend) ontology, its advantages and was performed a comparative analysis on which is the best populated ontologies (Docs. populated). Section III mention the privacy-related threats and risks in social networking sites and also state the privacy threats in FOAF documents. Finally, section IV discusses indicatively some security solutions for FOAF documents, while section V evaluate the results of this effort and conclude the thesis.

Keywords: Privacy, Social networking site, Foaf, Risk, Threats, Security

ΚΑΤΑΛΟΓΟΣ ΕΙΚΟΝΩΝ

ΚΑΤΑΛΟΓΟΣ ΠΙΝΑΚΩΝ

ΕΙΣΑΓΩΓΗ

Τα κοινωνικά δίκτυα έχουν ενταχθεί και αποτελούν πλέον αναπόσπαστο κομμάτι στην καθημερινότητα ενός μεγάλου συνόλου ανθρώπων. Ένα μικρό δείγμα του αριθμού των χρηστών των κοινωνικών δικτύων αντικατοπτρίζεται στον κάτωθι πίνακα:

Κοινωνικό δίκτυο	Αριθμός ενεργών χρηστών (2014)
Facebook	1.280.000.000
Google Plus	540.000.000
Twitter	255.000.000
Instagram	200.000.000
LinkedIn	187.000.000

ΠΙΝΑΚΑΣ 1 Αριθμός ενεργών χρηστών ανά κοινωνικό δίκτυο (socialmedialife.gr)

Σύμφωνα με τον Barnes (1972) «*Κοινωνικό δίκτυο είναι μια κοινωνική δομή, στην οποία τα άτομα ή οι οργανισμοί αναπαρίστανται από κόμβους. Οι συνδέσεις μεταξύ των κόμβων αναπαριστούν τις σχέσεις και τις ροές μεταξύ ανθρώπων, ομάδων, οργανισμών ή άλλων οντοτήτων ικανών να επεξεργάζονται δεδομένα και να παράγουν γνώση*».

Επίσης, σύμφωνα με τον ορισμό των Raad και Chbeir (2013) «*Ένα κοινωνικό δίκτυο αποτελείται από κόμβους, οι οποίοι αναπαριστούν άτομα και οι συνδέσεις μεταξύ των κόμβων αναπαριστούν φιλίες*».

Αρχικά για να κατανοηθεί η έννοια του κόμβου και οι συνδέσεις μεταξύ αυτών, θα πρέπει να ορισθεί η έννοια του γράφου. Γράφος είναι η αναπαράσταση ενός συνόλου στοιχείων, όπου μερικά ζευγάρια στοιχείων συνδέονται μεταξύ τους με δεσμούς. Ένας γράφος αποτελείται από ένα σύνολο V κορυφών ή κόμβων και ένα σύνολο από E ακμές. Η θεωρία των γράφων χρησιμοποιείται για τη γραφική αναπαράσταση των δικτύων επικοινωνιών και της ανάλυσή τους. Ένα δίκτυο

υπολογιστών μπορεί να αναπαρασταθεί ως ένα σύνολο κόμβων, οι οποίοι συνδέονται μεταξύ τους μέσω συνδέσμων, που είτε δεν έχουν κατεύθυνση (μη κατευθυνόμενος γράφος), είτε έχουν (κατευθυνόμενος γράφος) (Μπουντουρίδης, 2013).

Σύμφωνα με τους Raad και Chbeir (2013), οι βασικές ιδιότητες των κοινωνικών δικτύων και οι διάφοροι τύποι δεδομένων μπορούν να αναπαρασταθούν με ένα σύνολο γράφων που είτε είναι κατευθυνόμενοι ή μη, είτε προσημασμένοι ή μη είτε με βάρη ή χωρίς. Οι κόμβοι απεικονίζουν τους χρήστες ή τις ομάδες, ενώ οι ακμές δείχνουν τις σχέσεις ή τις ροές μεταξύ των κόμβων.

Λαμβάνοντας υπόψη την πρώτη αναφερόμενη περίπτωση γράφων, η χρήση μη κατευθυνόμενων γράφων σε ένα κοινωνικό δίκτυο, δηλώνει αμοιβαίες σχέσεις, όπως η σχέση φιλίας μεταξύ δύο χρηστών του Facebook. Από την άλλη πλευρά, οι κατευθυνόμενοι γράφοι, όπως είναι στη περίπτωση του Twitter, δεν ορίζουν την αμοιβαία σχέση μεταξύ δύο χρηστών, δηλαδή ένα μέλος στο Twitter μπορεί να ακολουθεί ένα άλλο, χωρίς απαραίτητα να συμβαίνει και το αντίστροφο.

Η σήμανση ενός γράφου, στα κοινωνικά δίκτυα, σε προσημασμένο ή μη προσδιορίζει την σχέση μεταξύ δύο οντοτήτων του δικτύου και μπορεί να βοηθήσει τον χρήστη στην καλύτερη οργάνωση των επαφών του, ανάλογα με το είδος σχέσης (οικογενειακή, φιλική, συναδελφική) που έχει με άλλους χρήστες.

Σε ένα κοινωνικό δίκτυο, τα βάρη στις ακμές σύνδεσης των χρηστών μπορεί να υποδηλώνουν διαφορετικά επίπεδα φιλίας ή επικοινωνίας μεταξύ των χρηστών.

Η ανάλυση των κοινωνικών δικτύων, μέσω της χρήσης γράφων, δίνει τη δυνατότητα της καλύτερης κατανόησης των σχέσεων που αναπτύσσονται μεταξύ των χρηστών του δικτύου, καθώς και των δραστηριότητας τους. Συγκεκριμένα, μπορεί να απεικονιστεί ο αριθμός των συνδέσεων ενός χρήστη, το είδος των σχέσεων που αναπτύσσει, αλλά και η επιρροή που ασκεί ή όχι μέσα στο δίκτυο.

ΚΕΦ.1: Ιδιωτικότητα

Στο κεφάλαιο αυτό θα οριστεί η έννοια της ιδιωτικότητας, θα αναφερθούν τα είδη της, θα γίνει αναφορά στο απόρρητο των επικοινωνιών καθώς επίσης και στην οδηγία 94/46 του Ευρωπαϊκού Κοινοβουλίου για τη διασφάλιση της προστασίας των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και την ελεύθερη κυκλοφορία των δεδομένων αυτών.

1.1. Η έννοια της Ιδιωτικότητας

Κατά το πέρασμα των χρόνων η έννοια της ιδιωτικότητας έχει μελετηθεί από πολλές διαφορετικές σκοπιές. Κοινωνικοί επιστήμονες, φιλόσοφοι αλλά και νομικοί έχουν μελετήσει κατά καιρούς την έννοια της ιδιωτικότητας και έχουν προσπαθήσει να την ορίσουν, χωρίς ωστόσο πολύ θετικά αποτελέσματα, αφού δεν έχουν καταφέρει ακόμη και στις μέρες μας να καταλήξουν σε έναν κοινά αποδεκτό ορισμό. Έτσι, στην διεθνή βιβλιογραφία υπάρχει ένα μεγάλο πλήθος ορισμών για την έννοια της ιδιωτικότητα, οι οποίοι ωστόσο διαφέρουν ως προς το περιεχόμενο, ανάλογα με την εποχή κατά την οποία συντάχθηκαν και με το επιστημονικό πεδίο που αναφέρονται.

Ένας από τους παλαιότερους και τους πλέον φημισμένους ορισμούς για την ιδιωτικότητα είναι αυτός των Αμερικανών δικαστών Warren και Brandeis (1890), οι οποίοι το 1890 μέσω του άρθρου τους "The Right to Privacy", όρισαν την ιδιωτικότητα ως «*Το δικαίωμα του να μένει κανείς μόνος*» (the right to be alone). Σχεδόν έναν αιώνα μετά, ο καθηγητής Alan Westin του Πανεπιστημίου Columbia έδωσε έναν πιο σύγχρονο και πιο πλήρη ορισμό της ιδιωτικότητας στο βιβλίο του "Privacy and Freedom". Σύμφωνα με τον Westin, «*Ιδιωτικότητα είναι η αξίωση των ατόμων, ομάδων και οργανισμών να καθορίζουν το χρόνο, τον τρόπο και την έκταση αναφορικά με τη συλλογή και την επεξεργασία των προσωπικών τους δεδομένων*».

Επιπλέον αξίζει να σημειωθεί η συμπερίληψη της ιδιωτικότητας στην Οικουμενική Διακήρυξη για τα Ανθρώπινα Δικαιώματα από τον Οργανισμό των Ηνωμένων Εθνών το 1948. Σύμφωνα λοιπόν με το κάτωθι άρθρο της Διακήρυξης:

Άρθρο 12

Κανείς δεν επιτρέπεται να υποστεί αυθαίρετες επεμβάσεις στην ιδιωτική του ζωή, την οικογένεια, την κατοικία ή την αλληλογραφία του, ούτε προσβολές της τιμής και της υπόληψης του. Καθένας έχει το δικαίωμα να τον προστατεύουν οι νόμοι από επεμβάσεις και προσβολές αυτού του είδους.

Τέλος, στον Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης και συγκεκριμένα στα άρθρα 7 και 8 γίνεται μια ακόμη αναφορά στην έννοια της ιδιωτικότητας:

Άρθρο 7

Σεβασμός της ιδιωτικής και οικογενειακής ζωής

Κάθε πρόσωπο έχει δικαίωμα στο σεβασμό της ιδιωτικής και οικογενειακής ζωής του, της κατοικίας του και των επικοινωνιών του.

Άρθρο 8

Προστασία των δεδομένων προσωπικού χαρακτήρα

1. Κάθε πρόσωπο έχει δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα που το αφορούν.
2. Η επεξεργασία αυτών των δεδομένων πρέπει να γίνεται νομίμως, για καθορισμένους σκοπούς και με βάση τη συγκατάθεση του ενδιαφερομένου ή για άλλους θεμιτούς λόγους που προβλέπονται από το νόμο. Κάθε πρόσωπο δικαιούται να έχει πρόσβαση στα συλλεγμένα δεδομένα που το αφορούν και να επιτυγχάνει τη διόρθωσή τους.
3. Ο σεβασμός των κανόνων αυτών υπόκειται στον έλεγχο της ανεξάρτητης αρχής.

1.2. Τα είδη της Ιδιωτικότητας

Όπως και με τους ορισμούς της συγκεκριμένης έννοιας, έτσι και με τα είδη της ιδιωτικότητας υπάρχουν πολλές κατηγοριοποιήσεις. Συγκεκριμένα, σύμφωνα με τον Clarke το 1997 έχουμε τις εξής κατηγορίες:

- Ιδιωτικότητα του ατόμου.
- Ιδιωτικότητα των προσωπικών δεδομένων.

- Ιδιωτικότητα της προσωπικής συμπεριφοράς.
- Ιδιωτικότητα των επικοινωνιών.

Επίσης λίγο νωρίτερα και συγκεκριμένα το 1992 ο Rosenberg υποστήριξε ότι η ιδιωτικότητα μπορεί να χωριστεί σε τρεις κατηγορίες:

- Την εδαφική ιδιωτικότητα , η οποία περιλαμβάνει την προστασία του φυσικού χώρου που περιβάλλει ένα άτομο (territorial privacy).
- Την ιδιωτικότητα του ατόμου , η οποία περιλαμβάνει την προστασία του ατόμου από αδικαιολόγητες παρεμβάσεις (privacy of the person.
- Την πληροφοριακή ιδιωτικότητα, η οποία περιλαμβάνει τον έλεγχο του αν και πώς τα προσωπικά δεδομένα ενός ατόμου μπορούν να συλλέγονται, να αποθηκεύονται, να υφίστανται επεξεργασία ή να διαδίδονται επιλεκτικά (information privacy).

Τέλος στηριζόμενοι στο ότι η ιδιωτικότητα είναι μια έννοια ρευστή αλλά και συνεχώς μεταβαλλόμενη ανάλογα με τις κοινωνικές και τεχνολογικές εξελίξεις, το έτος 2013 οι Finn et al. διέκριναν ακόμη 7 τύπους ιδιωτικότητας. Αυτό κυρίως συνέβη λόγω του ότι είχαν προκύψει νέοι τύποι ιδιωτικότητας, τους οποίους στο παρελθόν κανείς δεν μπορούσε να προβλέψει. Οι τύποι αυτοί είναι:

- Η ιδιωτικότητα του ατόμου (privacy of the person).
- Η ιδιωτικότητα της συμπεριφοράς και της δράσης (privacy of behavior and action).
- Η ιδιωτικότητα των επικοινωνιών (privacy of communication).
- Η ιδιωτικότητα δεδομένων και εικόνων (privacy of data and image).
- Η ιδιωτικότητα της σκέψης και των συναισθημάτων (privacy of thoughts and feelings).
- Η ιδιωτικότητα ομίλων και ομάδων (privacy of association and group privacy).
- Η ιδιωτικότητα του χώρου και της τοποθεσίας (privacy of space and location).

1.3. Ιδιωτικότητα και απόρρητο

Όλα τα προηγούμενα χρόνια αλλά κυρίως στη σύγχρονη εποχή η έννοια της ιδιωτικότητας έχει συνδεθεί άμεσα με την έννοια του απορρήτου. Στη περισσότερες φορές μάλιστα η ιδιωτικότητα έχει ταυτιστεί με το απόρρητο της πληροφορίας. Γενικότερα, το απόρρητο (εκτός από την περίπτωση όπου ο νόμος επιτρέπει την άρση απορρήτου) αποκλείει τους τρίτους από τη γνώση, τη χρήση και την αξιοποίηση των πληροφοριών. Ωστόσο η έννοια της ιδιωτικότητας ταυτίζεται ακόμη και με δύο άλλες θεμελιώδεις έννοιες όπως είναι η μυστικότητα και η εμπιστευτικότητα. Στο σημείο αυτό αξίζει να αναφερθούμε στον διαχωρισμό που υπάρχει ανάμεσα σε αυτές τις δύο έννοιες, μιας και συχνά συγχέονται και θεωρούνται ταυτόσημες.

Η έννοια της εμπιστευτικότητας σχετίζεται με το απόρρητο, από την πλευρά ασφάλειας των πληροφοριών, αλλά ωστόσο, δεν ταυτίζεται με αυτό. Η ασφάλεια της πληροφορίας δεν εξυπηρετείται μόνο από την εγγύηση της εμπιστευτικότητας, καθώς αυτή αποτελεί μία μόνο παράμετρο. Είναι απαραίτητο να συμπεριληφθούν και οι έννοιες της εγκυρότητας, της αυθεντικότητας, της ακεραιότητας και της διαθεσιμότητας. Η ασφάλεια προϋποθέτει ένα οργανωμένο πλαίσιο από έννοιες, αντιλήψεις, αρχές, πολιτικές, διαδικασίες, τεχνικές και μέτρα, τα οποία απαιτούνται, για να προστατέψουν τα στοιχεία ενός πληροφοριακού συστήματος.

Σχετικά με την έννοια της μυστικότητας, η συγκεκριμένη έννοια αναφέρεται είτε στη μη προσπελασιμότητα των πληροφοριών, που εμπίπτουν στην σφαίρα της επιρροής ενός ατόμου είτε στο καθήκον ή στην υποχρέωση των ανθρώπων ή οργανισμών να διαφυλάσσουν πληροφορίες, όπου ένα άτομο έχει εμπιστευτεί σ' αυτά, μέσα φυσικά σε ένα πλαίσιο γενικής εμπιστοσύνης. Παράδειγμα των παραπάνω αποτελεί το ιατρικό και το τραπεζικό απόρρητο.

Στα πλαίσια των γενικών κανόνων καθώς και στη νομοθεσία που υπάρχει για την προστασία της ιδιωτικότητας, παρατηρούνται κάποιες διαφορές ανάμεσα σε διάφορα κράτη του κόσμου ή ακόμη και σε διάφορες ηπείρους. Για παράδειγμα στις Ηνωμένες Πολιτείες Αμερικής, το γεγονός ότι ένα πρόσωπο εμπιστεύεται μια πληροφορία, που το αφορά σε ένα άλλο πρόσωπο ή οργανισμό, οδηγεί στην στέρηση της προστασίας της ιδιωτικότητας. Όταν ένα άτομο αποκαλύπτει εθελοντικά σε ένα τρίτο άτομο ή οργανισμό προσωπικά του στοιχεία και στην συνέχεια αυτά διαβιβάζονται σε μια

δημόσια αρχή, τότε το άτομο αυτό παραιτείται από το δικαίωμα της ιδιωτικότητας, ακόμα και αν αρχικά, έδωσε τα στοιχεία του για ένα περιορισμένο σκοπό.

Στην Ευρώπη ο νόμος υποστηρίζει την διαφύλαξη του απορρήτου μέσα στο σχετικό κανονιστικό πλαίσιο. Συγκεκριμένα, το άρθρο 16 της Οδηγίας 95/46/ΕΚ, που αφορά την προστασία προσωπικών δεδομένων, περιέχει μια ιδιότυπη ρύθμιση για το απόρρητο. Σε αυτήν αναφέρεται ότι όποιος επεξεργάζεται δεδομένα για λογαριασμό του υπεύθυνου επεξεργασίας ή του εκτελούντος επεξεργασία, το πράττει μόνο κατ' εντολή του υπεύθυνου επεξεργασίας. Τέλος, στην Ελλάδα η προστασία του απορρήτου διατυπώνεται στο ν. 2472/97 στο άρθρο 10, παρ.1, ο οποίος ορίζει ότι η επεξεργασία προσωπικών δεδομένων θεωρείται απόρρητη.

1.4. Οδηγία 95/461995

Η Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 24ης Οκτωβρίου 1995, έχει ως σκοπός τη διασφάλιση της προστασίας των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και την ελεύθερη κυκλοφορία των δεδομένων αυτών.

Η συγκεκριμένη οδηγία θεσπίζει ένα κανονιστικό πλαίσιο, το οποίο αποσκοπεί στην εγκαθίδρυση μιας ισορροπίας μεταξύ ενός υψηλού επιπέδου προστασίας της ιδιωτικής ζωής των προσώπων και της ελεύθερης κυκλοφορίας των δεδομένων προσωπικού χαρακτήρα σε όλη την Ευρωπαϊκή Ένωση (ΕΕ). Για το σκοπό αυτό, η Οδηγία ορίζει τα όρια της συλλογής και της χρησιμοποίησης των δεδομένων προσωπικού χαρακτήρα και ζητά τη δημιουργία, σε κάθε κράτος μέλος, ενός ανεξάρτητου εθνικού οργανισμού επιφορτισμένου με την προστασία των δεδομένων αυτών.

Στο σημείο αυτό αξίζει να σημειωθεί ότι η συγκεκριμένη οδηγία δεν εφαρμόζεται στην επεξεργασία δεδομένων η οποία πραγματοποιείται από φυσικό πρόσωπο στο πλαίσιο αποκλειστικά προσωπικών ή οικιακών δραστηριοτήτων, καθώς και στην επεξεργασία δεδομένων όπου πραγματοποιείται για την άσκηση δραστηριοτήτων, που δεν διέπονται από το κοινοτικό δίκαιο, όπως η δημόσια ασφάλεια, η άμυνα ή η ασφάλεια του κράτους.

Αντιθέτως, στόχος της συγκεκριμένης οδηγίας είναι η προστασία των ελευθεριών και των δικαιωμάτων των προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα, μέσω του καθορισμού κατευθυντήριων αρχών, που προσδιορίζουν τη νομιμότητα της συγκεκριμένης επεξεργασίας. Οι αρχές αυτές αφορούν:

Α) Τη νόμιμη επεξεργασία των δεδομένων : Η επεξεργασία δεδομένων προσωπικού χαρακτήρα δεν μπορεί να γίνεται παρά εάν το συγκεκριμένο άτομο έχει δώσει τη συναίνεσή του ή αν η επεξεργασία είναι απαραίτητη:

- Για την τήρηση νομικής υποχρέωσης, στην οποία υπόκειται ο υπεύθυνος της επεξεργασίας.
- Για τη διαφύλαξη ζωτικού συμφέροντος του υπόψη προσώπου.
- Για την εκτέλεση σύμβασης της οποίας το υπόψιν πρόσωπο αποτελεί συμβαλλόμενο μέρος.
- Για την εκτέλεση αποστολής δημόσιου συμφέροντος.
- Για την υλοποίηση του θεμιτού συμφέροντος, που επιδιώκεται από τον υπεύθυνο της επεξεργασίας.

Β) 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.

Γ) Τις ειδικές κατηγορίες επεξεργασίας: Θα πρέπει να απαγορεύεται η επεξεργασία δεδομένων προσωπικού χαρακτήρα, που αποκαλύπτουν τη φυλετική ή εθνολογική καταγωγή, τις δημόσιες απόψεις, τις φιλοσοφικές ή θρησκευτικές πεποιθήσεις, τη συνδικαλιστική τοποθέτηση, καθώς και την επεξεργασία δεδομένων σχετικά με την υγεία και την ερωτική ζωή. Φυσικά υπάρχουν και εξαιρέσεις, όπως για την περίπτωση όπου η επεξεργασία είναι απαραίτητη για σκοπούς προληπτικής ιατρικής ή ιατρικής διάγνωσης καθώς και για τη περίπτωση όπου είναι απαραίτητη για την υπεράσπιση των ζωτικών συμφερόντων του προσώπου.

Δ) Την ενημέρωση των ενδιαφερόμενων προσώπων σχετικά με την επεξεργασία δεδομένων: Ο υπεύθυνος επεξεργασίας θα πρέπει να παρέχει στο πρόσωπο, για το

οποίο συλλέγει δεδομένα που το αφορούν, ορισμένες πληροφορίες, όπως η ταυτότητά του και ποιοι είναι οι παραλήπτες των δεδομένων.

Ε) Το δικαίωμα πρόσβασης των προσώπων αυτών στα δεδομένα : Κάθε σχετικό πρόσωπο θα πρέπει να έχει το δικαίωμα από τον υπεύθυνο της επεξεργασίας για:

- Τη διόρθωση, τη διαγραφή ή την απαγόρευση της πρόσβασης στα δεδομένα, των οποίων η επεξεργασία δεν είναι σύμφωνη προς την τρέχουσα επεξεργασία καθώς και την κοινοποίηση των τροποποιήσεων αυτών προς τρίτους, στους οποίους τα δεδομένα αυτά έχουν διαβιβασθεί.

- Τη διαβεβαίωση ότι τα δεδομένα του ατόμου που υπόκεινται σε επεξεργασία, γίνονται ή όχι αντικείμενο επεξεργασίας και την κοινοποίηση των δεδομένων, που αποτελούν το αντικείμενο επεξεργασίας.

Ζ) Τις εξαιρέσεις και τους περιορισμούς: Οι Αρχές σχετικά με την ποιότητα των δεδομένων, την πληροφόρηση του συγκεκριμένου προσώπου, 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 καθώς και η προστασία του εν λόγω προσώπου.

Η) Το δικαίωμα αντίταξης στην επεξεργασία δεδομένων: Το υπόψιν πρόσωπο θα πρέπει να έχει το δικαίωμα να αντιταχθεί, για θεμιτούς λόγους, στην επεξεργασία δεδομένων, που το αφορούν. Θα πρέπει επίσης να δύναται να αντιταχθεί, εφόσον το ζητήσει και δωρεάν, στην επεξεργασία δεδομένων που προβλέπεται για σκοπούς διερεύνησης. Επίσης θα πρέπει να ενημερώνεται πριν από τη διαβίβαση των δεδομένων σε τρίτους για σκοπούς έρευνας και θα πρέπει να του παρέχεται το δικαίωμα αντίταξης στη διαβίβαση αυτή.

Θ) Την εμπιστευτικότητα και την ασφάλεια της επεξεργασίας: Κάθε πρόσωπο, που ενεργεί κάτω από την εξουσία του υπευθύνου της επεξεργασίας ή εκείνη του υπεργολάβου, καθώς και ο ίδιος ο υπεργολάβος, που έχει πρόσβαση σε προσωπικά δεδομένα, δεν έχει τη δυνατότητα επεξεργασίας παρά μόνο κατόπιν εντολής του υπευθύνου επεξεργασίας. Εξάλλου, ο τελευταίος θα πρέπει να εφαρμόζει τα ενδεδειγμένα μέτρα για την προστασία των δεδομένων προσωπικού χαρακτήρα ως προς τυχαία ή παράνομη καταστροφή, τυχαία απώλεια, αλλοίωση, διάδοση ή πρόσβαση χωρίς άδεια.

I) 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, στα δικαιώματα και ελευθερίες των εν λόγω 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 επιπλέον οι Ελεγκτικές Αρχές οφείλουν να τηρούν μητρώο των κοινοποιημένων αποτελεσμάτων 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. 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. Η Οδηγία αποσκοπεί στο να διευκολύνει την εκπόνηση κωδικών εθνικής και κοινοτικής συμπεριφοράς, οι οποίοι θα συμβάλουν στην ομαλή εφαρμογή των κοινοτικών και εθνικών διατάξεων. Κάθε κράτος μέλος προβλέπει μία ή περισσότερες ανεξάρτητες κρατικές Αρχές, οι οποίες επιφορτίζονται με την εποπτεία της εφαρμογής, στο εθνικό έδαφος, των ληφθέντων από τα κράτη μέλη μέτρων κατ' εφαρμογή της παρούσας Οδηγίας. Τέλος αξίζει να σημειωθεί ότι δημιουργείται 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 των οργανισμών και ένας εκπρόσωπος της Επιτροπής.

1.5. Αρχή διασφάλισης του απορρήτου των επικοινωνιών

Η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ) είναι μια από τις συνταγματικά καθιερωμένες Ανεξάρτητες Αρχές με διοικητική αυτοτέλεια, η οποία συστάθηκε ως ειδικός εποπτεύων φορέας για να προστατεύει το απόρρητο της επικοινωνίας (http://www.adae.gr/fileadmin/docs/pepragmena/2008/Kefalaio_3.pdf).

Συγκεκριμένα η ΑΔΑΕ έχει τις εξής αρμοδιότητες:

- Διενεργεί, αυτεπαγγέλτως ή κατόπιν καταγγελίας, τακτικούς και έκτακτους ελέγχους σε εγκαταστάσεις, τεχνικό εξοπλισμό, αρχεία, τράπεζες δεδομένων και έγγραφα της ΕΥΠ, άλλων δημοσίων υπηρεσιών, οργανισμών, επιχειρήσεων του ευρύτερου δημοσίου τομέα, καθώς και ιδιωτικών επιχειρήσεων που ασχολούνται με ταχυδρομικές, τηλεπικοινωνιακές ή άλλες υπηρεσίες σχετικές με την ανταπόκριση και την επικοινωνία. Οι έλεγχοι διενεργούνται από τα μέλη και το προσωπικό της ΑΔΑΕ προκειμένου να διαπιστωθεί η σωστή εφαρμογή των πολιτικών ασφάλειας που επιβάλλεται να εφαρμόζουν οι πάροχοι ή για τη διαπίστωση παραβίασης του απορρήτου της επικοινωνίας.

- Λαμβάνει πληροφορίες σχετικές με την αποστολή της από τις προαναφερθείσες υπηρεσίες, οργανισμούς και επιχειρήσεις, καθώς και από τους εποπτεύοντες Υπουργούς.

- Καλεί σε ακρόαση τις παραπάνω υπηρεσίες, οργανισμούς, νομικά πρόσωπα και επιχειρήσεις και κάθε άλλο πρόσωπο, που κρίνει ότι μπορεί να συμβάλει στην εκπλήρωση της αποστολής της.

- Προβαίνει σε κατάσχεση των μέσων παραβίασης του απορρήτου που υποπίπτουν στην αντίληψή της κατά την ενάσκηση του έργου της και ορίζεται μεσεγγυούχος αυτών μέχρι να αποφανθούν τα αρμόδια δικαστήρια. Προβαίνει επίσης στην καταστροφή πληροφοριών ή στοιχείων ή δεδομένων, τα οποία αποκτήθηκαν με παράνομη παραβίαση του απορρήτου των επικοινωνιών.

- Εξετάζει καταγγελίες σχετικά με την προστασία των δικαιωμάτων των αιτούντων, όταν θίγονται από τον τρόπο και τη διαδικασία άρσης του απορρήτου.

- Συνεργάζεται με άλλες αρχές της χώρας, με αντίστοιχες αρχές άλλων κρατών, καθώς και με ευρωπαϊκούς και διεθνείς οργανισμούς, για θέματα της αρμοδιότητάς της.

- Γνωμοδοτεί και απευθύνει συστάσεις και υποδείξεις για τη λήψη μέτρων διασφάλισης του απορρήτου των επικοινωνιών, καθώς και τη διαδικασία άρσης του.

- Εκδίδει κανονιστικές πράξεις που δημοσιεύονται στην Εφημερίδα της Κυβερνήσεως με τις οποίες ρυθμίζεται κάθε διαδικασία και λεπτομέρεια σε σχέση με τις ανωτέρω αρμοδιότητές της καθώς και με την εν γένει διασφάλιση του απορρήτου των επικοινωνιών.

Σύμφωνα με την ΑΔΑΕ , στις ηλεκτρονικές επικοινωνίες, απόρρητα θεωρούνται:

- Η ταυτότητα του καλούντος και του καλούμενου.

- Η ταυτότητα του αποστολέα και του παραλήπτη του ηλεκτρονικού ταχυδρομείου.

- Το περιεχόμενο της επικοινωνίας (περιεχόμενο τηλεφωνικών κλήσεων, ηλεκτρονικού ταχυδρομείου και γενικά οποιασδήποτε επικοινωνίας φωνής, εικόνας και δεδομένων).

- Τα δεδομένα θέσης της τερματικής συσκευής, δηλαδή ο γεωγραφικός εντοπισμός.

Στις ταχυδρομικές υπηρεσίες, απόρρητα θεωρούνται:

- Το περιεχόμενο της αλληλογραφίας

- Ο αποστολέας

- Ο παραλήπτης

Τέλος αξίζει να αναφέρουμε, ότι η ΑΔΑΕ το 2004 πρότεινε την εκπόνηση μιας ολοκληρωμένης Εθνικής Στρατηγικής Ασφάλειας Δικτύων και Πληροφοριών, επισημαίνοντας με αυτό τον τρόπο τη σπουδαιότητα και την αναγκαιότητα ύπαρξης σχεδιασμού πολιτικής σχετικά με την ασφάλεια ηλεκτρονικών δικτύων και πληροφοριακών συστημάτων που είναι στρατηγικής σημασίας για τη χώρα μας (http://www.adae.gr/fileadmin/docs/pepragmena/2008/Kefalaio_3.pdf). Επίσης, έχει

τονίσει αρκετές φορές, την απουσία θεσμικού πλαισίου για τον έλεγχο της ασφάλειας των δικτύων, των κρίσιμων υποδομών, των δικτύων των επιχειρήσεων, των οργανισμών και των δικτύων των υπουργείων. Έτσι με το νόμο 3674/2008 ελήφθησαν κάποια νομοθετικά μέτρα για την ενίσχυση του θεσμικού πλαισίου διασφάλισης του απορρήτου της τηλεφωνικής μόνο επικοινωνίας. Ο ίδιος νόμος προβλέπει και την εκπόνηση Εθνικού Σχεδίου Ασφάλειας των Επικοινωνιών (ΕΣΑΕ).

1.6. Απαιτήσεις Ιδιωτικότητας στα Κοινωνικά δίκτυα

Με την ολοένα αύξηση των κοινωνικών δικτύων και την έκθεση προσωπικών δεδομένων στο διαδίκτυο, είναι εμφανές ότι πρέπει να υιοθετηθούν οι ελάχιστες απαιτήσεις ιδιωτικότητας, ώστε να μετριαστεί ο κίνδυνος εκδήλωσης απειλών. Με αυτόν τον τρόπο, ο χρήστης θα είναι σε θέση να χρησιμοποιήσει τα κοινωνικά δίκτυα, ενώ παράλληλα θα μπορεί να διατηρεί την ιδιωτικότητά του (Raad and Chbeir 2013). Τα κύρια χαρακτηριστικά των απαιτήσεων ιδιωτικότητας είναι τα εξής:

- Ανωνυμία (Anonymity)
- Ψευδωνυμία (Pseudonymity)
- Μη συνδεσιμότητα (Unlinkability)
- Μη ανιχνευσιμότητα (Undectability)
- Μη παρατηρησιμότητα (Unobservability)

Αναλυτικότερα, ανωνυμία μιας οντότητας (λ.χ χρήστης, διεργασία), σημαίνει ότι η οντότητα αυτή δεν είναι αναγνωρίσιμη σε ένα σύνολο ανώνυμων οντοτήτων. Η κατάσταση της μη αναγνωρισιμότητας εκφράζεται από το γεγονός, ότι μια οντότητα δεν έχει μοναδικά χαρακτηριστικά. Ως εκ τούτου, κατά την πρόσβαση του χρήστη σε μια σελίδα κοινωνικής δικτύωσης δεν πρέπει να παρουσιάζεται ή να προκύπτει η αποκάλυψη της ταυτότητάς του. Ο βαθμός ανωνυμίας μεταξύ ενός συνόλου χρηστών μπορεί να μεταβάλλεται, αφού εξαρτάται από την συμπεριφορά των υπόλοιπων χρηστών-μελών ενός κοινωνικού δικτύου, που ωστόσο καθορίζεται από την εκάστοτε πολιτική προστασίας και πολιτική προσπέλασης κάθε κοινωνικού δικτύου.

Το δεύτερο χαρακτηριστικό είναι η ψευδωνυμία, η οποία ορίζει ότι κάθε χρήστης χρησιμοποιεί κάποιο ψευδώνυμο αντί του πραγματικού του ονόματος με σκοπό να

προστατέψει την αποκάλυψη της ταυτότητάς του. Με αυτόν τον τρόπο, στα πλαίσια μιας επικοινωνίας, προστατεύεται η αναγνώριση των χρηστών από τρίτες οντότητες. Η κύρια χρήση της ψευδωνυμίας είναι σε περιπτώσεις κοινωνικών δικτύων, που δεν μπορεί να υλοποιηθεί η ανωνυμία. Η ψευδωνυμία επιτρέπει στους χρήστες να έχουν πρόσβαση σε δεδομένα χωρίς να αποκαλύπτεται η ταυτότητά τους και συγχρόνως παραμένουν υπόλογοι για τις ενέργειές τους. Η ψευδωνυμία χωρίζεται στα εξής είδη:

- **Αποκλειστικό ψευδώνυμο**: ψευδώνυμο με έναν και μοναδικό κάτοχο, το οποίο δεν μεταβάλλεται και δεν μεταβιβάζεται σε άλλες οντότητες του κοινωνικού δικτύου.
- **Μεταβιβάσιμο ψευδώνυμο**: ψευδώνυμο που μπορεί να μεταβιβαστεί από μία οντότητα σε μια άλλη οντότητα μέσα στο κοινωνικό δίκτυο.
- **Ομαδικό ψευδώνυμο**: ψευδώνυμο που αναφέρεται σε ένα σύνολο οντοτήτων, οι οποίες δεν είναι τυχαίες μεταξύ τους.

Η έννοια της ανωνυμίας διαφέρει από την έννοια της ψευδωνυμίας, αφού η πρώτη προσδιορίζει μια ιδιότητα σε σχέση με την αναγνωρισιμότητα, ενώ η δεύτερη αναφέρεται στην χρήση ενός μηχανισμού.

Το τρίτο χαρακτηριστικό είναι η μη συνδεσιμότητα, κατά την οποία δύο ή περισσότερες οντότητες έχουν μη συνδεσιμότητα, όταν μέσα στο ίδιο κοινωνικό δίκτυο, ο επιτιθέμενος δεν μπορεί να ξεχωρίσει αν αυτές οι οντότητες σχετίζονται μεταξύ τους ή όχι. Αναλυτικότερα, η μη συνδεσιμότητα αποκλείει έναν επιτιθέμενο να συνδέσει τμήματα σχετικών πληροφοριών μεταξύ τους, το οποίο θα οδηγούσε στην αποκάλυψη της ταυτότητας των χρηστών.

Η μη ανιχνευσιμότητα μιας οντότητας σε ένα κοινωνικό δίκτυο, σημαίνει ότι ο επιτιθέμενος δεν είναι σε θέση να προσδιορίσει επακριβώς αν η οντότητα υφίσταται ή όχι. Ο μέγιστος βαθμός της μη ανιχνευσιμότητας επιτυγχάνεται όταν μια οντότητα είναι τελείως δυσδιάκριτη.

Το πέμπτο χαρακτηριστικό είναι η μη παρατηρησιμότητα, κατά την οποία μια οντότητα είναι μη παρατηρήσιμη σε ένα σύνολο οντοτήτων, δηλαδή ένας χρήστης παραμένει ανώνυμος σε σχέση με τους υπόλοιπους χρήστες και έτσι ο επιτιθέμενος δεν μπορεί να εντοπίσει την ταυτότητά του. Αναλυτικότερα, η συγκεκριμένη

απαίτηση αποκλείει έναν επιτιθέμενο να παρατηρήσει ή να εντοπίσει τα ίχνη των χρηστών τη στιγμή που χρησιμοποιούν μια διαδικτυακή υπηρεσία (Raad and Chbeir 2013).

ΚΕΦ.2: Friend of A Friend (FOAF)

Στο κεφάλαιο αυτό θα οριστεί η έννοια του λεξιλογίου Friend-Of-A-Friend (FOAF), θα χαρακτηρισθεί η δομή ενός εγγράφου FOAF και τα πλεονεκτήματά του καθώς επίσης θα δοθούν κατευθυντήριες γραμμές στο πώς να δημιουργήσει κανείς μια συλλογή FOAF εγγράφων.

2.1. Εισαγωγή στην έννοια του λεξιλογίου FOAF

Ο σημασιολογικός ιστός υπόσχεται να προσφέρει νέες εφαρμογές για τους χρήστες του Διαδικτύου, μέσω της χρήσης μεταδεδομένων βασισμένα σε RDF, τα οποία συνδέονται με διάφορες πηγές πληροφόρησης στο διαδίκτυο. Ένας από τους πρωταρχικούς στόχους του σημασιολογικού ιστού, είναι να αποθηκεύει δεδομένα σε κατανεμημένες τοποθεσίες καθώς και να χρησιμοποιεί και να αιτιολογεί τις οντολογίες, ώστε να συναθροίζει (aggregate) και να χρησιμοποιεί τα δεδομένα αυτά. Οι οντολογίες που είναι φτιαγμένες από μεγάλες ομάδες μηχανικών λογισμικού ή αυτοδύναμες εφαρμογές είναι χαρακτηριστικά παραδείγματα των τεχνολογιών του σημασιολογικού ιστού, χωρίς ωστόσο, να απεικονίζουν πλήρως τις δυνατότητές του. Τα ελλιπή στοιχεία είναι μια ακόμα μεγάλη ομάδα από δεδομένα περίπτωσης τα οποία είναι διανεμημένα σε ανεξάρτητους ιστότοπους, και μόνο με τη χρήση της αιτιολόγησης (reasoning) μπορούν να συγχωνευθούν. Σε αντίθετη περίπτωση θεωρούνται ως ξεχωριστά δεδομένα (Golbeck and Rothstein 2008).

Το FOAF (Friends Of A Friends) είναι ένα από τα μεγαλύτερα project του σημασιολογικού ιστού, το οποίο ξεκίνησε το 1999 και πρόσφατα έχει γίνει ένα ευρέως αποδεκτό λεξιλόγιο για την αναπαράσταση των κοινωνικών δικτύων. Αναλυτικότερα, είναι μια οντολογία κατανοητή από τις μηχανές-υπολογιστές, η οποία χρησιμοποιεί το πρότυπο RDF (Resource Description Framework) και τη γλώσσα OWL (Web Ontology language) για να περιγράψει τα άτομα, τις δραστηριότητές τους και τις σχέσεις τους με άλλα άτομα ή αντικείμενα. Το λεξιλόγιο FOAF επιτρέπει σε ομάδες ανθρώπων, να περιγράφουν τα κοινωνικά δίκτυα, χωρίς την ανάγκη χρήσης μια κεντρικοποιημένης Βάσης Δεδομένων (ΒΔ). Παράλληλα, επιτρέπει στους υπολογιστές να βρίσκουν πληροφορίες για μια ομάδα ατόμων, όπως για παράδειγμα, όλα τα άτομα που ζουν στην Ευρώπη. Αυτό επιτυγχάνεται με τον καθορισμό των σχέσεων ανάμεσα στους ανθρώπους. Κάθε προφίλ έχει ένα μοναδικό

αναγνωριστικό, όπως η ηλεκτρονική διεύθυνση του χρήστη ή το URI (Unique Resource Identifier) της προσωπικής του σελίδας, το οποίο χρησιμοποιείται για να οριστεί η σχέση του με άλλα άτομα (Brickley και Miller 2003).

Σήμερα, πολλοί ιστότοποι κοινωνικής δικτύωσης χρησιμοποιούν το λεξιλόγιο foaf, για να παράγουν προφίλ για τους χρήστες τους. Υπάρχουν εκατομμύρια foaf προφίλ, που φιλοξενούνται σε ένα μεγάλο εύρος ιστοτόπων. Επειδή είναι αρκετά επιτυχημένο στη χρήση του, το λεξιλόγιο foaf συχνά χρησιμοποιείται ως ένα παράδειγμα επιτυχίας του σημασιολογικού ιστού. Ο τρόπος με τον οποίο χρησιμοποιείται, ικανοποιεί τους στόχους της χρήσης οντολογιών στην αναπαράσταση υπολογίσιμου πλήθους από κατανεμημένα δεδομένα, σε κανονική μορφή. Ωστόσο, για να αποτελέσει το foaf ένα παράδειγμα πλήρους δυνατοτήτων του σημασιολογικού ιστού, η αιτιολόγηση των δεδομένων πρέπει να οδηγεί στην ανακάλυψη των συνδέσεων μεταξύ στο τι παρουσιάζεται ως διακριτή ομάδα δεδομένων. Αυτό πρακτικά σημαίνει ότι πρέπει να γίνει συγχώνευση των προφίλ που ανήκουν στο ίδιο άτομο από πολλούς ιστότοπους κοινωνικής δικτύωσης και συγχρόνως τη δημιουργία ενός μεγάλου και ταυτόχρονα ενοποιημένου κοινωνικού δικτύου αποτελούμενο από υποδίκτυα τα οποία εμπλέκονται ανεξαρτήτως.

2.2. Λεξιλόγιο FOAF και δομή ενός εγγράφου FOAF

Το ερευνητικό πεδίο του εγγράφου FOAF ξεκίνησε από τον Dan Brickley και τον Libby Miller. Ένα έγγραφο FOAF δημοσιεύει διαδικτυακές ιστοσελίδες για χρήστες, ομάδες, επιχειρήσεις και κάθε άλλου είδους οντότητα, είναι γραμμένο σε XML, και υιοθετεί τις συμβάσεις του προτύπου Resource Description Framework (RDF) (Foaf-project.org 2014). Εμπλουτίζει την έκφραση των προσωπικών πληροφοριών και των σχέσεων και ως εκ τούτου είναι ένα χρήσιμο δομικό στοιχείο για τη δημιουργία πληροφοριακών συστημάτων, τα οποία υποστηρίζουν διαδικτυακές κοινότητες.

Το πιο σημαντικό στοιχείο ενός εγγράφου FOAF είναι το λεξιλόγιο, το οποίο αναγνωρίζεται από την ονοματοδοσία URI: http://xmlns.com/foaf/0.1/. Το λεξιλόγιο FOAF καθορίζει τόσο τις κλάσεις (π.χ., foaf: Agent, foaf: Person και foaf: Document) όσο και τις ιδιότητες (π.χ., foaf: name, foaf: knows, foaf: interest, και foaf: mbox) στηριζόμενες σε σημασιολογία RDF. Σε αντίθεση με ένα σταθερό πρότυπο (όπως

είναι το ISO), το λεξιλόγιο του FOAF είναι *ανοιχτού κώδικα*, δηλαδή, δεν είναι σταθερό αλλά είναι ανοικτό για επέκταση (Foaf-project.org 2014). Ως εκ τούτου, η χρήση του λεξιλογίου FOAF ανάμεσα σε διαφορετικά έγγραφα μπορεί να διαφέρει. Ωστόσο, ένα έγγραφο FOAF πρέπει να είναι ένα ορθώς δομημένο RDF έγγραφο και ένα μεγάλο ποσοστό εγγράφων FOAF προέρχεται από μεγάλα και αναπτυσσόμενα ιστολόγια και παρέχει ένα μεγάλο σύνολο διαφορετικών όρων, το οποίο περιγράφει, όπως αναφέρθηκε και παραπάνω, χρήστες, ομάδες, επιχειρήσεις και κάθε άλλου είδους οντότητα. Οι όροι αυτοί κατηγοριοποιούνται σύμφωνα με το (Foaf-project.org, 2014) στις εξής κατηγορίες:

Πυρήνας (Core): Τον πυρήνα της FOAF αποτελούν οι κλάσεις και οι ιδιότητες. Οι τελευταίες περιγράφουν τα χαρακτηριστικά των ανθρώπων και των κοινωνικών ομάδων, οι οποίες είναι ανεξάρτητες από το χρόνο και τη τεχνολογία και γι' αυτό μπορούν να χρησιμοποιηθούν για να περιγράψουν βασικές πληροφορίες για τους ανθρώπους που αφορούν το παρόν και το παρελθόν, την πολιτιστική τους κληρονομιά καθώς και το περιεχόμενο της ψηφιακής βιβλιοθήκης. Επιπροσθέτως, η FOAF ορίζει κλάσεις για εργασίες, οργανισμούς και ομάδες.

Κοινωνικός ιστότοπος (Social Web): Εκτός από τους βασικούς όρους της FOAF, υπάρχει μια σειρά από όρους που προορίζονται για την χρήση και την περιγραφή των διαδικτυακών λογαριασμών, των βιβλίων διευθύνσεων και άλλων διαδικτυακών δραστηριοτήτων.

Χρησιμότητες διασυνδεδεμένων δεδομένων (Linked Data Utilities): Η FOAF είναι ένας σημαντικός λίθος στην ραγδαία αναπτυσσομένη κοινότητα των διασυνδεδεμένων δεδομένων. Επίσης, η FOAF αποτελεί, μια προσπάθεια για την χρησιμοποίηση του διαδικτύου στην ενσωμάτωση πραγματικών πληροφοριών, με πληροφορίες που έχουν ανθρωποκεντρικό χαρακτήρα, όπως είναι τα βίντεο και τα βιβλία, καθώς και πληροφορίες που βρίσκονται στο μυαλό των ανθρώπων. Ως εκ τούτου, η FOAF περιλαμβάνει ορισμένους όρους που εξυπηρετούν σε μεγάλο βαθμό εκπαιδευτικούς σκοπούς (geekcode), παράλληλα με κάποιους τεχνικούς όρους (focus, LabelProperty), οι οποίοι υποστηρίζουν ευρέως τη διασύνδεση πληροφοριών.

Ενδεικτικά, κάποιοι από τους όρους που χρησιμοποιούνται ευρέως στη διαδικτυακή κοινότητα παρατίθενται ανά κατηγορία (Core και Social Web) στο κάτωθι πίνακα.

Πυρήνας (Core) FOAF	Κοινωνικός ιστότοπος (Social Web) FOAF
• Agent Person name title img depiction (depicts) familyName givenName knows based_near age made (maker) primaryTopic (primaryTopicOf) • Project Organization Group member • Document Image	• nick • mbox • homepage • weblog • openid • jabberID • mbox_sha1sum • interest • topic_interest • topic (page) • workplaceHomepage • workInfoHomepage • schoolHomepage • publications • currentProject • pastProject • account • OnlineAccount • accountName • accountServiceHomepage • PersonalProfileDocument • tipjar • sha1 • thumbnail • logo

ΠΙΝΑΚΑΣ 2 *Βασικό λεξιλόγιο FOAF* (Foaf-project.org 2014)

Επίσης, πρέπει να προστεθεί ότι η εξέλιξη της FOAF έχει να κάνει πολύ περισσότερο με τη σταθερότητα των επιμέρους όρων του λεξιλογίου της, παρά από το specification ως σύνολο. Γι' αυτό το λόγο, στις ιδιότητες και στις κλάσεις προσδιορίζεται και η κατάστασή τους ως «μη σταθερή», «υπό δοκιμή» και «σταθερή». Στο **Error! Reference source not found.** παρατίθενται ενδεικτικά ορισμένες ιδιότητες και κλάσεις, οι οποίες παρέχουν κάποιες βασικές έννοιες που είναι χρήσιμες για τη δημιουργία μιας περιγραφής FOAF.

2.3. Πλεονεκτήματα χρήσης εγγράφων FOAF

Η πρακτική σημασία των εγγράφων FOAF για τους δημιουργούς πληροφορίων και για τους καταναλωτές μπορεί να χαρακτηρισθεί με μια ποικιλία εφαρμογών (Dumbill 2003), οι οποίες συνοψίζονται ως εξής:

Για τους δημιουργούς, το FOAF είναι χρήσιμο για:

- Τη διαχείριση κοινοτήτων, προσφέροντας μια βασική έκφραση για τις σχέσεις φιλίας στην κοινότητα. Πολλές κοινότητες έχουν πολλαπλασιαστεί στο Διαδίκτυο και κυμαίνονται από επιχειρήσεις επαγγελματικών οργανώσεων μέχρι κοινωνικές ομάδες.

- Την έκφραση της ταυτότητας επιτρέποντας την χρήση των μοναδικών χαρακτηριστικών χρήστη μεταξύ των εφαρμογών και των υπηρεσιών, χωρίς να εξασφαλίζεται η ιδιωτικότητα. Για παράδειγμα, η ιδιότητα *foaf:mbox_sha1sum* περιέχει την ASCII κωδικοποίηση της συνάρτησης κατακερματισμού SHA1 ενός URI ηλεκτρονικού ταχυδρομείου (π.χ., mailto: yfantopoulos@hua.gr). Προκειμένου να αποτρέψει κάποιους επιτιθέμενους να κάνουν πλαστοπροσωπία, η κωδικοποίηση έχει σχεδιαστεί ως μια μονόδρομη χαρτογράφηση και δεν μπορεί να δεχτεί επίθεση αντίστροφης μηχανικής (Reverse Engeeniring) με την οποία αποκαλύπτεται η αρχική διεύθυνση του ηλεκτρονικού ταχυδρομείου.

- Την εμφάνιση της ιδιότητας του εκδότη. Τα FOAF εργαλεία χρησιμοποιούν ψηφιακές υπογραφές για να συσχετίσουν μια διεύθυνση ηλεκτρονικού ταχυδρομείου με ένα έγγραφο. Ειδικότερα, χρησιμοποιείται το πρωτόκολλο OpenPGP, μαζί με τη νέα ονοματοδοσία http://xmlns.com/wot/0.1/ για να

υποδηλώσει έννοιες που αποτελούν ένα "Δίκτυο εμπιστοσύνης". Αυτό συσχετίζει μια υπογραφή με το ίδιο το αρχείο και στη συνέχεια προσδιορίζει μια υπογραφή για το συνδεδεμένο έγγραφο, ως ένα μέρος συνδέσμου rdfs:seeAlso. Έτσι, οι πληροφορίες του εκδότη μπορούν να εκφραστούν τόσο εντός όσο και εκτός των σχετικών εγγράφων.

Η FOAF στηρίζει τους καταναλωτές:

- Επιτρέποντας τον εντοπισμό της προέλευσης και παρέχοντας υπευθυνότητα (Dumbill 2003). Στο διαδίκτυο, η πηγή των πληροφοριών είναι εξίσου σημαντική όσο και η κρίση της αξιοπιστία της ίδιας της πληροφορίας. Τα εργαλεία ανίχνευσης της προέλευσης RDF μπορούν να δείξουν πού και πότε λαμβάνεται ένα κομμάτι πληροφορίας. Μια κοινή πρακτική στην FOAF κοινότητα είναι να συνδεθεί η πηγή URI με κάθε δήλωση RDF.

- Με την παροχή βοήθειας σε νεοεισερχόμενους σε μια κοινότητα. Παραδείγματος χάριν, οι άνθρωποι που δεν είναι εξοικειωμένοι με μια κοινότητα μπορούν να μάθουν τη δομή και την αυθεντία ενός ερευνητικού πεδίου μέσα από τα αρχεία της κοινότητας FOAF.

- Με τον εντοπισμό ανθρώπων με κοινά ενδιαφέροντα. Οι χρήστες τείνουν να έχουν συμφέροντα και αξίες παρόμοιες με εκείνες που επιθυμούν άλλοι άνθρωποι (Adamic 2003). Οι σχέσεις των ομότιμων δικτύων (Peer-to-peer networks) είναι ένα ιδανικό συστατικό για τη συνεργασία, η οποία είναι και η κινητήρια δύναμη της διαδικτυακής κοινότητας.

- Αυξάνοντας το φιλτράρισμα του ηλεκτρονικού ταχυδρομείου και δίνοντας προτεραιότητα σε email που προέρχονται από αξιόπιστους συναδέλφους. Χρησιμοποιώντας το βαθμό εμπιστοσύνης που προέρχεται από τα αρχεία FOAF, οι άνθρωποι μπορούν να δώσουν προτεραιότητα στα εισερχόμενα e-mail που τους ενδιαφέρουν και αντίστοιχα να μπλοκάρουν με τη χρήση φίλτρων άτομα χαμηλής εμπιστοσύνης.

2.4. Σύγκριση του λεξιλογίου FOAF με άλλες οντολογίες

Μεταξύ ενός μεγάλου αριθμού οντολογιών που έχουν δημοσιευθεί στον Παγκόσμιο Ιστό, λίγες μόνο από αυτές είναι συμπληρωμένες, δηλαδή έχουν κάποια σημαντική χρήση. Μια πρόσφατη έρευνα της ομοματοδοσίας των χώρων από καλά συμπληρωμένες οντολογίες (βλέπε *ΠΙΝΑΚΑΣ*) αποκάλυψε ότι, εκτός από τις "meta-level" οντολογίες (π.χ RDF, RDFS, DAML και OWL), μια από τις καλύτερα συμπληρωμένες οντολογίες είναι η FOAF (Foaf-project.org 2014). Εκτός από το να αντιπροσωπεύουν προσωπικές πληροφορίες είναι επίσης και ένα δημοφιλές θέμα στην οντολογική μηχανική (σε περισσότερα από 1.000 έγγραφα RDF έχουν οριστεί όροι που περιέχουν την έννοια «άτομο»). Οι υπόλοιπα καλά συμπληρωμένες οντολογίες (οι οποίες δεν είναι μετα-οντολογίες) είναι το DC (Dublin Core Element Set), το οποίο καθορίζει τις ιδιότητες των μετα-δεδομένων στα έγγραφα, χωρίς να υποστηρίζει τομείς, και το RSS (RDF Site Summary), το οποίο είναι μια ελαφριά, πολλαπλών χρήσεων, περιγραφή των μεταδεδομένων και συγχρόνως αποτελεί πρότυπο σύνδεσης για τον σχολιασμό των ιστοσελίδων.

Ονόματα	Ονοματοδοσία URI	Ενσωματωμένα έγγραφα
RDF	http://www.w3.org/1999/02/22-rdf-syntax-ns#	> 1.129.749
FOAF	http://www.foaf-project.org/	> 1.126.002
DC	http://purl.org/dc/elements/1.1/	> 1.117.433
RDFS	http://www.w3.org/2000/01/rdf-schema#	> 1.129.749
MCVB	http://webns.net/mvcb/	> 8.838
RSS	http://purl.org/rss/1.0/	> 7.560
vCard	http://www.w3.org/2001/vcard-rdf/3.0#	> 6.229
Bio	http://purl.org/vocab/bio/0.1/	> 6.183

ΠΙΝΑΚΑΣ 3 *Οι 8 καλύτερα συμπληρωμένες οντολογίες* (Ding Li και συν. 2005)

Το λεξιλόγιο FOAF παρέχει ένα RDF/XML λεξιλόγιο για να περιγράφει προσωπικές πληροφορίες, συμπεριλαμβανομένου του ονόματος, του ηλεκτρονικού

ταχυδρομείου, της διεύθυνσης της αρχικής σελίδας και τους φίλους (Dumbill 2002). Με αυτόν τον τρόπο, τα έγγραφα FOAF δημιουργούν ένα έμπιστο δίκτυο, το οποίο υποστηρίζει εφαρμογές για εξαγωγή γνώσης και διαδικτυακές κοινότητες.

Οι εξελίξεις στο λεξιλόγιο FOAF και στις εφαρμογές φέρνουν αρκετές προκλήσεις που πρέπει να αντιμετωπιστούν. Για παράδειγμα, το πώς μπορεί κανείς να συγκεντρώσει μια συλλογή εγγράφων FOAF για την υποστήριξη μιας έρευνας σημασιολογικού ιστού, ποια είναι τα κοινά πρότυπα των συνδέσεων μεταξύ εγγράφων FOAF, ποιοι από τους όρους στο λεξιλόγιο FOAF χρησιμοποιούνται πιο συχνά, ποιες είναι οι δυνατότητες του FOAF στη ενίσχυση της νοημοσύνης των διαδικτυακών πληροφοριακών συστημάτων. Μέσα από την βιβλιογραφική ανασκόπηση διαφαίνεται ένα όραμα και διάφορα μοντέλα για το πώς τα έγγραφα FOAF θα μπορούσαν να χρησιμοποιηθούν για την υποστήριξη διαδικτυακών πληροφοριακών συστημάτων, με την προϋπόθεση βέβαια ότι τα έγγραφα αυτά είναι ευρέως διαθέσιμα. Υπάρχει ωστόσο έλλειψη εμπειρικής έρευνας σχετικά με τα χαρακτηριστικά και τη δομή του αυξανόμενου σώματος των εκατομμυρίων εγγράφων του FOAF. Η έρευνα των Ding L. και συν (Ding L και συν. 2005) παρουσιάζει ενδεικτικά εμπειρικά αποτελέσματα που απαντούν στις παραπάνω ερωτήσεις και βασίζονται σε μια μεγάλη συλλογή δεδομένων (πάνω από 1,5 εκατομμύριο) από αληθινά έγγραφα FOAF τα οποία αντλήθηκαν από το διαδίκτυο. Η εν λόγω έρευνα αποτελούνταν από τέσσερα βήματα: τον προσδιορισμό των FOAF εγγράφων, την ανακάλυψη FOAF εγγράφων χρησιμοποιώντας πράκτορες λογισμικού (software agents), την εξαγωγή προσωπικών πληροφοριών, και την συγχώνευση των προσωπικών πληροφοριών με βάση τη σημασιολογία του λεξιλογίου FOAF. Με τη χρήση στατιστικών στοιχείων πάνω σε αυτή τη συλλογή των εγγράφων FOAF, περιγράφεται στην εν λόγω έρευνα, οι κοινές ιδιότητες και οι ονοματοδοσίες που διαμοιράζονται από την κοινότητα του FOAF. Η ανάλυση αυτή, έχει ως απώτερο σκοπό, να βοηθήσει τους προγραμματιστές που δουλεύουν πάνω στο λεξιλόγιο της FOAF, στο σχεδιασμό και στην καλύτερη οικοδόμηση των εργαλείων, καθώς και στην ενημέρωση των βασικών χρηστών που δουλεύουν πάνω στο λεξιλόγιο της FOAF, σχετικά με το πώς να δημιουργήσουν αποτελεσματικά έγγραφα. Οι αναλύσεις των κοινωνικών δικτύων που κωδικοποιούνται στα έγγραφα του λεξιλογίου της FOAF, δίνουν μια πρώτη εικόνα σχετική με τα διαρθρωτικά πρότυπα του Σημασιολογικού Ιστού από την προσωπική προοπτική. Ο "πλούτος" του προφίλ

στα έγγραφα του λεξιλογίου της FOAF, επιτρέπει στους χρήστες να χαρακτηρίσουν τους περαιτέρω κοινωνικούς δεσμούς και να αναγνωρίσουν τα είδη φιλίας.

Ένα άμεσο αποτέλεσμα της εν λόγω μελέτης είναι ένας κατάλογος με σχέσεις φιλίας στον Σημασιολογικό Ιστό. Με βάση αυτόν τον κατάλογο, τη φήμη και τα συστήματα σύστασης, μπορούν να βοηθηθούν οι χρήστες ώστε να επιλέξουν αξιόπιστους παρόχους υπηρεσιών και να αξιολογήσουν την εμπιστοσύνη μέσα από τις σχέσεις φιλίας. Για παράδειγμα, ένας πράκτορας λογισμικού (software agent), μπορεί να βοηθήσει έναν πελάτη να βρει ένα καλό φθηνό εστιατόριο σε μία περιοχή, ταξινομώντας τις προτιμήσεις βάση απόστασης.

Τα δίκτυα φιλίας που συνδέονται με τις σχέσεις του λεξιλογίου FOAF μπορούν να παρέχουν γνώσεις σχετικά με τα χαρακτηριστικά και τα πρότυπα των κοινωνικών δικτύων στο Σημασιολογικό Ιστό και να προωθήσουν τις θεωρίες και τα μοντέλα των κοινωνικών δομών. Τα δίκτυα φιλίας στον φυσικό κόσμο έχουν μελετηθεί αρκετά στην κοινωνική επιστήμη. Ένα πολύ γνωστό παράδειγμα είναι το φαινόμενο του μικρόκοσμου του Μίλγκραμ πάνω στο οποίο ο καθένας μπορεί να αναγνωρισθεί μέσω μιας μικρής αλυσίδας κοινωνικών γνωριμιών. Η έννοια αυτή δίνει μεγάλη έκταση στην περίφημη φράση των έξι βαθμών διαχωρισμού, η οποία έχει πρόσφατα εφαρμοστεί στην ανάλυση των κοινωνικών δικτύων τόσο σε φυσικά όσο σε εικονικά περιβάλλοντα (Xu and Chen 2013). Οι κοινωνικές σχέσεις έχουν προέλθει από «συμφραζόμενες» πληροφορίες ή τομείς γνώσης, με έμμεσο τρόπο μέσω της χρήσης τεχνικών εξόρυξης δεδομένων. Εκτός από τα κοινωνικά δίκτυα, η συλλογή των εγγράφων του λεξιλογίου της FOAF μπορεί να χρησιμεύσει ως πολύτιμος λίθος στον Σημασιολογικό Ιστό αναφορικά με την έρευνα, την ανάπτυξη και τη δοκιμή έμπιστων μοντέλων όπως είναι τα μοντέλα διάδοσης εμπιστοσύνης (Ding et al. 2004).

2.5. Δημιουργία συλλογής FOAF εγγράφων

Για να δημιουργήσεις κανείς μια συλλογή FOAF εγγράφων, θα χρειασθεί να ακολουθήσει τα εξής βήματα: Πρωταρχικά χρειάζεται να αναγνωρίσει τα έγγραφα, στη συνέχεια να ανεύρει τα έγγραφα FOAF και τέλος να τα εξάγει. Στην έρευνα του Ding (Ding et al. 2005) χρησιμοποιήθηκαν είτε ολόκληρα τα “qualified names” είτε συντομογραφία αυτών ως QNames (βλέπε *ΠΙΝΑΚΑΣ*).

rdfs:	http://www.w3.org/2000/01/rdf-schema#
foaf:	http://xmlns.com/foaf/0.1/
dc:	http://purl.org/dc/elements/1.1/
bio:	http://purl.org/vocab/bio/0.1/
daml:	http://www.daml.org/2001/03/daml+oil#

ΠΙΝΑΚΑΣ *4 Τα Qnames και οι ονοματοδοσίες τους* (Ding et al. 2005)`

Α. Αναγνώριση FOAF εγγράφων

Είναι εύκολο να ελεγχθεί εάν ένα έγγραφο RDF χρησιμοποιεί την ονοματοδοσία του FOAF, αλλά επίσης είναι σημαντικό να δοθούν κριτήρια ώστε να αναγνωριστεί εάν είναι ένα έγγραφο FOAF ή όχι. Ένα έγγραφο FOAF δεν έχει μια συγκεκριμένη δομή αφού είναι πιθανό να δημοσιευτεί από διαφορετικούς εκδότες με διαφορετικές προθέσεις. Τα κανονικά έγγραφα FOAF είναι προσωπικά προφίλ σε ιστολόγια και σε καταλόγους συλλεγμένων ατόμων. Παρόλο που το FOAF λεξιλόγιο μπορεί να χρησιμοποιηθεί για την περιγραφή πραγμάτων παρά ανθρώπων, η έρευνα των Ding et al. εστιάζει στην περιγραφή προσωπικών πληροφοριών.

Με σκοπό να δοθεί ένας επίσημος ορισμός ενός εγγράφου FOAF στην εν λόγω έρευνα, αναλύθηκαν τα πρότυπα χαρακτηριστικά τα οποία προέρχονται από τις σημασιολογικές οντολογίες και την εμπειρική χρήση του FOAF λεξιλογίου. Για το λόγο αυτό προσδιορίστηκε ένα αυστηρό D έγγραφο FOAF [1] με τα ακόλουθα τέσσερα πρότυπα χαρακτηριστικά:

1. Το D είναι ένα έγκυρο έγγραφο RDF, το οποίο μπορεί να επαληθευτεί από έναν RDF parser.

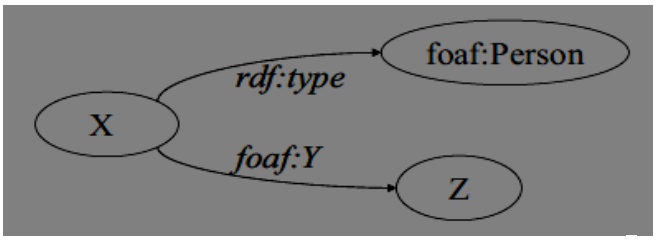
2. Το D χρησιμοποιεί την ονοματοδοσία του FOAF.

3. Το D εμπεριέχει ένα πρότυπο γράφο RDF όπως αναπαρίσταται στην Εικόνα 1. Στην εικόνα αυτή, τα X και Z είναι δύο διαφορετικά instances του

[1] Δομή FOAF Document: # document type
foaf:PersonalProfileDocument a foaf:Document.
#specific instance of document, with indication of its topic
<http://www.example.org/doc/john> a foaf:PersonalProfileDocument;
foaf:primaryTopic <http://www.example.org/doc/john#me>.

rdfs:Resource και το Y είναι ένα rdf:Property που χρησιμοποιεί την ονοματοδοσία (namespace) του FOAF.

4. Το D ορίζει μόνο ένα instance του foaf:Person το οποίο δεν έχει αναφορά ως αντικείμενο (Object) σε κάποια τριπλέτα μέσα στο D. Το D μπορεί να έχει κάποια άλλα επιπρόσθετα instances του FOAF:Person. Ωστόσο, καθένα από αυτά πρέπει να αναφέρεται ως αντικείμενο (Object) σε τουλάχιστον μία τριπλέτα.



ΕΙΚΟΝΑ 1 *Πρότυπο έγγραφο FOAF* (Ding et al. 2005)

Τα παραπάνω πρότυπα χαρακτηριστικά και ειδικότερα το 4ο είναι αρκετά αυστηρά και αποκλείουν πολλά έγγραφα που δεν αναφέρονται σε άτομα. Γι' αυτό το λόγο, αφαιρώντας το 4ο πρότυπο, ορίστηκε ένα γενικό έγγραφο FOAF που περιέχει instances του foaf:Person.

Αφού το RDF/XML χρησιμοποιείται συνήθως για την κωδικοποίηση του RDF, στην εν λόγω περίπτωση χρησιμοποιήθηκε μόνο το RDF/XML για την κωδικοποίηση των αρχείων. Επίσης παρατηρήθηκε ότι σε ένα instance του foaf:Person, ενσαρκώνονται μερικές ιδιότητες του FOAF, όταν περιγράφει ένα άτομο. Με βάση τη σημασιολογία του rdfs:domain, απλοποιήθηκε η λειτουργία του 3^{ου} προτύπου καθώς ελέγχθηκε η ύπαρξη των ιδιοτήτων του FOAF και βρέθηκε ότι το rdfs:domain είναι το foaf:Person.

Β. Ανεύρεση και εξαγωγή FOAF εγγράφου

Με βάση τα παραπάνω πρότυπα, στην έρευνα του Ding (Ding et al. 2005) χρησιμοποιήθηκαν και συμβατικές μηχανές αναζήτησης και Crawlers, για την ανεύρεση FOAF έγγραφων. Η ανεύρεση ενός έγγραφου FOAF είναι μια επαναληπτική διαδικασία που αποτελείται από δύο στάδια: Στο πρώτο στάδιο χρησιμοποιούνται κάποιες μηχανές αναζήτησης για την ανακάλυψη των URL διευθύνσεων των FOAF εγγράφων ενώ στο δεύτερο στάδιο εκτελείται ένας Crawler,

με σκοπό την επικύρωση και την ανακάλυψη νέων συνδέσεων, σύμφωνα με τη σημασιολογία του FOAF λεξιλογίου.

Οι συμβατικές μηχανές αναζήτησης θεωρούνται ένα καλό σημείο εκκίνησης για την ανακάλυψη FOAF έγγραφων στο διαδίκτυο. Επίσης, αφού οι μηχανές αναζήτησης αντιμετωπίζουν τα διαδικτυακά έγγραφα ως ελεύθερο κείμενο, τα τέσσερα μοτίβα ενός FOAF έγγραφου μπορούν να μεταφραστούν ως ερωτήματα (queries). Σύμφωνα με το πρώτο μοτίβο, μπορεί να υποβληθούν ερωτήματα μόνο για τα έγγραφα που είναι δημοφιλή και ακολουθούν τα πρότυπα RDF εγγράφου, συμπεριλαμβανομένων των «rdf», «xrdf», «owl» και ούτω καθεξής. Σύμφωνα με το δεύτερο και το τρίτο μοτίβο, μπορούν να δημιουργηθούν αρκετές αναζητήσεις με λέξεις-κλειδιά. Ο *ΠΙΝΑΚΑΣ* δείχνει την αποτελεσματικότητα των διαφορετικών ερωτημάτων σε διαφορετικές μηχανές αναζήτησης. Επίσης, είναι αξιοσημείωτο ότι στην έρευνα του Ding (Ding et al. 2005), η Google ξεπέρασε άλλες μηχανές αναζήτησης, λόγω της ικανότητάς της στο να ψάχνει τύπους αρχείων. Ωστόσο, πρέπει να αναφερθεί ότι οι μηχανές αναζήτησης δεν υποστηρίζουν πλήρως την αναζήτηση μεταδεδομένων, δηλαδή, θα επιστρέψουν μόνο ένα μικρό μέρος των εγγράφων Web που έχουν ανακαλύψει. Για παράδειγμα, η Google επιστρέφει μόνο τις URL διευθύνσεις των πρώτων 1.000 έγγραφων για οποιαδήποτε ερώτημα.

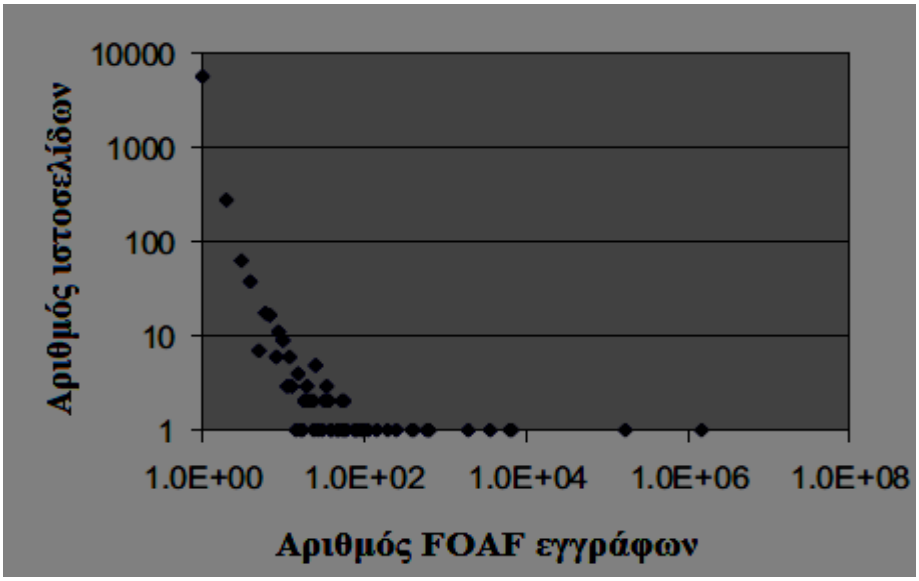
	Google	Yahoo	AskJeeves
filetype:rdf foaf	13.600	5.730	26
xmlns.com/foaf/0.1/	9.390	1	1000+
foaf:Person	5.080	2.820	1000+

ΠΙΝΑΚΑΣ 5 *Αποτελέσματα από μηχανές αναζήτησης (Ding et al. 2005)*

Η σημασιολογία της FOAF οντολογίας υποδηλώνει ότι τα FOAF έγγραφα είναι συνδεδεμένα με τη foaf:knows και επαυξάνονται με την rdfs:seeAlso. Επίσης, προτείνεται στην προδιαγραφή της FOAF ότι, όταν κάποιος χρησιμοποιεί το foaf:knows, τότε πρέπει να εισάγει και την προδιαγραφή rdfs:seeAlso ώστε να συνδέσει έγγραφα FOAF μεταξύ τους

Στην έρευνα του Ding (Ding et al. 2005) ανακαλύφθηκαν αρχικά πάνω από 10.000 έγγραφα FOAF, από συμβατικές μηχανές αναζήτησης. Επίσης, καθώς εξελίσσονται τα ευρετήρια δεδομένων, μπορεί κάποιος να ανακαλύψει περισσότερα

έγγραφα στην πάροδο του χρόνου. Επιπλέον, με τη χρήση Crawler οποίος υποστηρίζει τη σημασιολογία του FOAF λεξιλογίου, είναι δυνατή η ανακάλυψη πάνω από 1,5 εκατομμύριων FOAF έγγραφων. Το *ΔΙΑΓΡΑΜΜΑ 1* δείχνει πώς αυτά τα FOAF έγγραφα, στην εν λόγω έρευνα, βρίσκονται κατανεμημένα σε περισσότερες από 5.400 διαφορετικές ιστοσελίδες.



ΔΙΑΓΡΑΜΜΑ 1 *Διανομή FOAF εγγράφων* (Ding et al. 2005)

Ο ΠΙΝΑΚΑΣ 6 δείχνει ότι τα περισσότερα έγγραφα FOAF προήλθαν από διάφορες ιστοσελίδες και επιπλέον έξι από τις επτά κορυφαίες ιστοσελίδες, είναι ιστοσελίδες blog, όπου τα FOAF έγγραφα δημιουργούνται αυτόματα.

Ιστοσελίδα	Εύρεση από Crawler	Εύρεση από τη μηχανή αναζήτησης της Google
www.livejournal.com	1.508.346	0
www.deadjournal.com	169.546	0
www.ecademy.com	6.208	0
www.meinbild.ch	3.697	0
blog.livedoor.jp	1.914	3.560
www.ilrt.bris.ac.uk	621	651
eikeon.com	403	408

ΠΙΝΑΚΑΣ 6 *Οι 7 ιστοσελίδες με τα περισσότερα FOAF έγγραφα* (Ding et al. 2005)

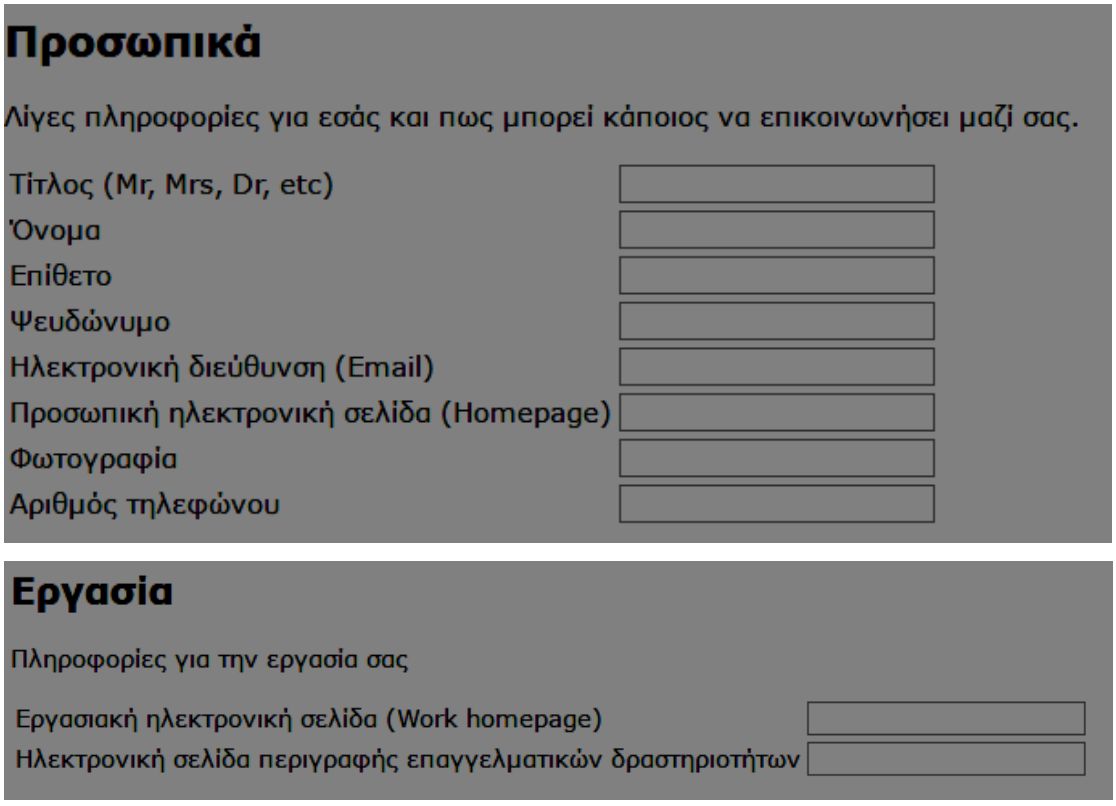
2.6. FOAF-A-Matic

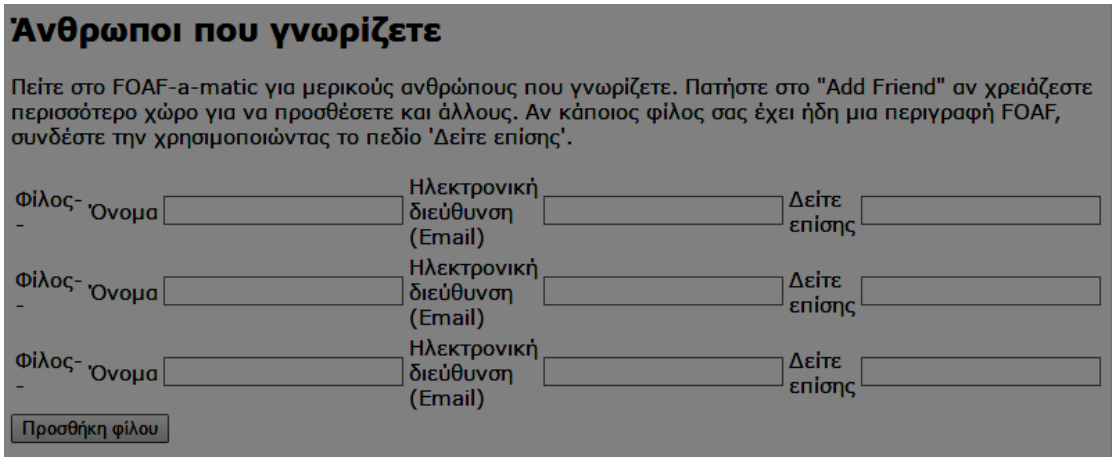
Το FOAF-a-matic είναι μια JavaScript εφαρμογή, η οποία επιτρέπει την δημιουργία περιγραφών FOAF (Friend-of-A-Friend) του εαυτού μας (http://www.ldodds.com/foaf/foaf-a-matic.html).

Αρχικά, πρέπει να συμπληρωθεί μία φόρμα με λεπτομέρειες που αφορούν την περιγραφής μας. Το όνομα και η ηλεκτρονική διεύθυνση (email) είναι απαραίτητα πεδία και προαιρετικά προσθέτουμε τους φίλους μας. Όταν κάποιος επεξεργαστής FOAF διαβάσει και καταλογογραφίσει την περιγραφή, θα μπορέσει να συσχετίσει το άτομο μας σαν ένα δίκτυο ατόμων.

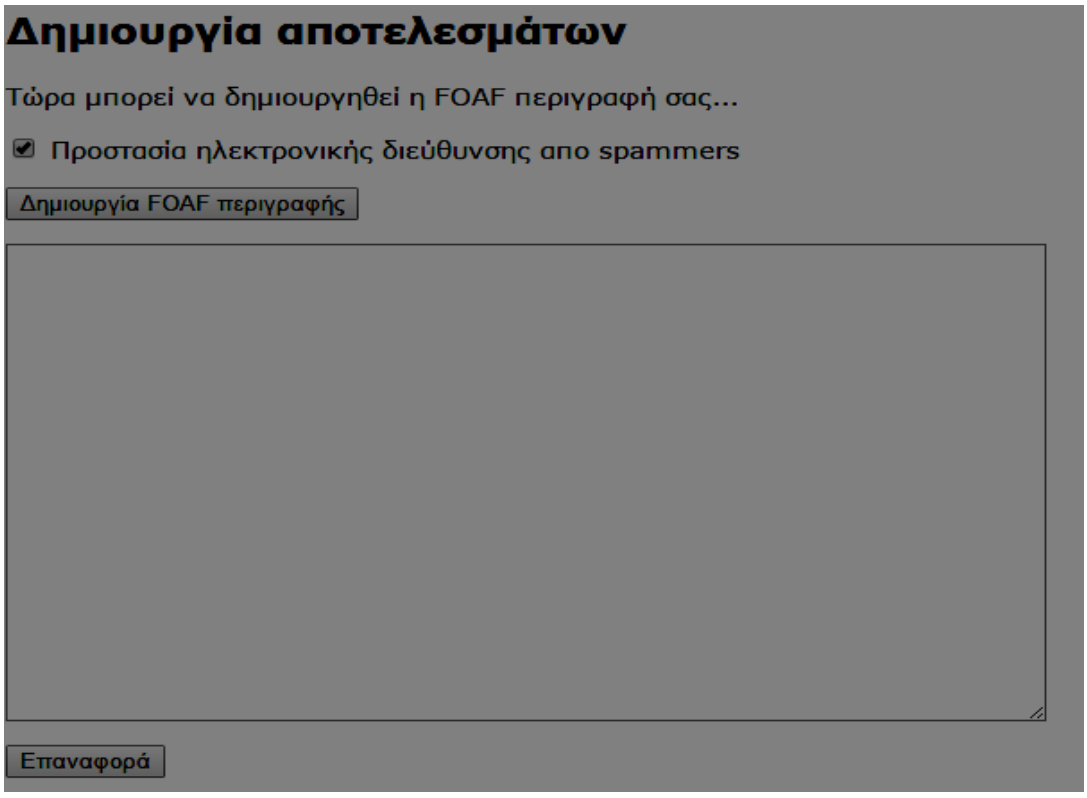
Στη ιστοσελίδα που υποβάλλεται η φόρμα, μας παρέχετε η διαβεβαίωση ότι ουδεμία από τις πληροφορίες που θα υποβάλουμε σε αυτήν την σελίδα δεν αποθηκεύεται με οποιονδήποτε τρόπο και όλη η επεξεργασία της φόρμας γίνεται στον υπολογιστή μας χωρίς να αποστέλλεται οποιαδήποτε πληροφορία σε κάποιο διακομιστή.

Οι φόρμες που πρέπει να συμπληρωθούν ώστε να δημιουργηθεί η FOAF περιγραφή είναι οι εξής:





Στη συνέχεια πατώντας στο κουμπί «Δημιουργία FOAF περιγραφής», δημιουργείται σε XML μορφή, η περιγραφή FOAF του ατόμου που εισάγαμε τα στοιχεία του.



Στη συνέχεια, πρέπει να δημοσιεύσουμε την FOAF περιγραφή στο διαδικτυακό χώρο. Αναλυτικότερα, αντιγράφουμε την FOAF περιγραφή που έχει δημιουργηθεί από το παραπάνω πεδίο και την επικολλούμε σε ένα καινούργιο αρχείο με όνομα foaf.rdf". Στη συνέχεια, τοποθετούμε το αρχείο αυτό στο διαδικτυακό χώρο, έτσι ώστε μηχανές αναζήτησης σαν το google να μπορούν να χρησιμοποιηθούν για ευρέσεις αρχείων FOAF στο δίκτυο.

Για την εύρεση της περιγραφής μας από τις εφαρμογές του FOAF, υπάρχουν τρεις διαδεδομένοι τρόποι.

Ο 1ος τρόπος είναι να χρησιμοποιήσουμε το στοιχείο link της HTML, σαν δείκτη της τοποθεσίας FOAF περιγραφών, όπως το χρησιμοποιούν οι bloggers για να δείχνουν την τοποθεσία των RSS αρχείων τους. Για παράδειγμα:
<link rel="meta" type="application/rdf+xml" title="FOAF" href="foaf.rdf" />

Ο 2ος τρόπος είναι να αναφέρεται σε αυτό κάποιος φίλος μας μέσω ενός άλλου FOAF αρχείου. Ένας καταλογογράφος FOAF μπορεί με αυτόν τον τρόπο να ανακαλύψει όλα τα FOAF αρχεία που συνδέονται με αυτόν τον τρόπο. Επίσης μπορούμε να πραγματοποιήσουμε και εμείς την παραπάνω διαδικασία κάνοντας τις εξής μετατροπές στην FOAF περιγραφή μας:

1. Μετατρέπουμε το στοιχείο rdf:RDF έτσι ώστε να προστεθεί το RDF Schema namespace, ως εξής:

   <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"
   xmlns:foaf="http://xmlns.com/foaf/0.1/"
   xmlns:rdfs="http://www.w3.org/2000/01/rdf-schema#">

2. Προσθέτουμε links που παραπέμπουν σε άλλα FOAF αρχεία προσθέτοντας ένα rdfs:seeAlso στοιχείο για κάθε αρχείο ως εξής:

   <rdfs:seeAlso rdf:resource="http://www.example.com/friends.xrdf"/>
   <rdfs:seeAlso rdf:resource="http://www.ldodds.com/webwho.xrdf"/>

Ο 3ος τρόπος είναι μέσω της χρήσης του πίνακα ανακοινώσεων του FOAF, στην ιστοσελίδα http://www.ldodds.com/foaf/bulletin-board.html, προσθέτοντας το όνομά μας και ένα link με τη FOAF περιγραφή μας

Για να γίνει κατανοητή η παραπάνω διαδικασία, παρατίθενται στο κάτωθι πλαίσιο ένα παράδειγμα δημιουργίας FOAF προφίλ μέσω της εφαρμογής FOAF-a-matic.

```
<rdf:RDF
    xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"
    xmlns:rdfs="http://www.w3.org/2000/01/rdf-schema#"
    xmlns:foaf="http://xmlns.com/foaf/0.1/"
    xmlns:admin="http://webns.net/mvcb/">
<foaf:PersonalProfileDocument rdf:about="">
```

```
  <foaf:maker rdf:resource="#me"/>
  <foaf:primaryTopic rdf:resource="#me"/>
  <admin:generatorAgent rdf:resource="http://www.ldodds.com/foaf/foaf-a-matic"/>
  <admin:errorReportsTo rdf:resource="mailto:leigh@ldodds.com"/>
</foaf:PersonalProfileDocument>
<foaf:Person rdf:ID="me">
<foaf:name>Bill Papadopoulos</foaf:name>
<foaf:title>Mr</foaf:title>
<foaf:givenname>Bill</foaf:givenname>
<foaf:family_name>Papadopoulos</foaf:family_name>
<foaf:nick>billpap</foaf:nick>
<foaf:mbox_sha1sum>7464c18a3c9c144a126024e98f9beb3bbf82753b</foaf:mbox_s
ha1sum>
<foaf:phone rdf:resource="tel:6945023648"/>
<foaf:knows>
<foaf:Person>
<foaf:name>nick papadakis</foaf:name>
<foaf:mbox_sha1sum>cfa8eaf4d950f8b1e36bf21546f32b0a6ac4704e</foaf:mbox_sh
a1sum></foaf:Person></foaf:knows>
<foaf:knows>
<foaf:Person>
<foaf:name>leonidas papadopoulos</foaf:name>
<foaf:mbox_sha1sum>5cb45f1945fb32af9af1fc4e4cd548beb02dd4eb</foaf:mbox_sh
a1sum></foaf:Person></foaf:knows>
<foaf:knows>
<foaf:Person>
<foaf:name>Efthymis Oikonomou</foaf:name>
<foaf:mbox_sha1sum>808768e690045d598bf58c9989438a4526f8d4ad</foaf:mbox_
sha1sum></foaf:Person></foaf:knows></foaf:Person>
</rdf:RDF>
```

ΚΕΦ.3: Κίνδυνοι και απειλές κατά της Ιδιωτικότητας στα Κοινωνικά Δίκτυα και στα FOAF προφίλ

Στο κεφάλαιο αυτό θα παρουσιαστούν οι κίνδυνοι και οι απειλές κατά της ιδιωτικότητας στις σελίδες κοινωνικής δικτύωσης καθώς επίσης και τα ζητήματα ιδιωτικότητας από τη χρήση FOAF προφίλ.

3.1. Κίνδυνοι κατά της Ιδιωτικότητας στις σελίδες Κοινωνικής δικτύωσης

Οι σελίδες κοινωνικής δικτύωσης έχουν δημιουργήσει μια επανάσταση στην κοινωνική συνδεσιμότητα αλλά και στην καθημερινότητα πολλών ανθρώπων. Αρκετοί χρήστες δημοσιεύουν καθημερινά στα προφίλ τους μια πληθώρα πληροφοριών, οι οποίες προέρχονται είτε από κάποια αλλαγή στην κοινωνική τους κατάσταση, είτε αναρτώντας μια φωτογραφία ή βίντεο, είτε σχολιάζοντας μια δημοσίευση ενός φίλου τους, είτε κοινοποιώντας τη παρουσία τους σε κάποιο σημείο είτε άλλες πληροφορίες που αφορούν τον εαυτό του ή τους φίλους του. Ως εκ τούτου, τα κοινωνικά δίκτυα αποτελούν μια τεράστια δεξαμενή δεδομένων και συγχρόνως ένα εύκολο στόχο για τους κακόβουλους χρήστες του διαδικτύου.

Συνήθως υπάρχουν δύο είδη κακόβουλων χρηστών που εκμεταλλεύονται τα κοινωνικά δίκτυα είτε διαμοιράζοντας κάποιο κακόβουλο- ιομορφικό λογισμικό είτε υποκλέπτοντας προσωπικές πληροφορίες από τους χρήστες. Αυτά τα δύο είδη είναι:

1. Επαγγελματίες προγραμματιστές (hackers) ή χομπίστες που ειδικεύονται στον να γράφουν και να τροποποιούν τον κώδικα του υπολογιστή. Με αυτό τον τρόπο μπορούν να αποκτήσουν πρόσβαση στον υπολογιστή ενός χρήστη και να του εγκαταστήσουν οποιοδήποτε ανεπιθύμητο πρόγραμμα επιθυμούν σε αυτόν ή στην κινητή του συσκευή.

2. Άνθρωποι που εξειδικεύονται στην κοινωνική μηχανική και μπορούν να αποσπάσουν αρκετές πληροφορίες για έναν χρήστη αρκεί κοιτώντας το κοινωνικό του προφίλ. Με αυτό τον τρόπο προσεγγίζουν ανθρώπους και τους χειραγωγούν έτσι ώστε να αποσπάσουν οποιαδήποτε πληροφορία τους ενδιαφέρει.

Οι χρήστες είναι συνήθως ο πιο αδύναμος κρίκος στην ασφάλεια του διαδικτύου, αφού αρκετοί εξ αυτών νομίζουν ότι οι πληροφορίες που δημοσιεύουν μέσα στο κοινωνικό τους προφίλ παραμένουν ιδιωτικές και πρόσβαση σε αυτές έχουν μόνο οι ίδιοι και οι φίλοι τους. Όσες περισσότερες πληροφορίες δημοσιεύει κάποιος, τόσο πιο ευάλωτος μπορεί να γίνει σε κάποιο είδος επίθεσης. Ακόμα και όταν ο χρήστης χρησιμοποιεί υψηλές ρυθμίσεις ασφαλείας, υπάρχουν παραδείγματα που δημοσιεύτηκαν κατά λάθος πληροφορίες που δεν έπρεπε, διότι εμφανίσθηκε κάποιο σφάλμα κατά την αναβάθμιση της πολιτικής ασφαλείας του κοινωνικού δικτύου.

Οι προσωπικές πληροφορίες που κοινοποιεί ένας χρήστης θα μπορούσαν να χρησιμοποιηθούν εναντίον του ή εναντίον των συνεργατών του. Όσο περισσότερη πληροφορία κοινοποιεί κάποιος, τόσο μεγαλώνει η πιθανότητα να ξεγελάσουν αυτόν ή κάποιον φίλο του έτσι ώστε να του αποσπάσουν προσωπικές πληροφορίες ή να τον οδηγήσουν σε ιστοσελίδες με επιβλαβές για τον υπολογιστή του λογισμικό.

Πολλές φορές ανταγωνιστές επιχειρήσεων χρησιμοποιούν Κοινωνικούς Μηχανικούς για να αποσπάσουν πληροφορίες από τα κοινωνικά προφίλ των εργαζομένων μιας επιχείρησης. Με αυτό τον τρόπο χειραγωγούν τους εργαζομένους και αποκτούν κρίσιμες πληροφορίες για την επιχείρηση, έτσι ώστε αργότερα να οργανώσουν μια επίθεση προς αυτή.

Σύμφωνα με τον Ευρωπαϊκό Οργανισμό Ασφαλείας Πληροφοριακών Συστημάτων (ENISA) οι κύριοι κίνδυνοι που αναδύονται στα κοινωνικά δίκτυα μπορούν να κατηγοριοποιηθούν ως εξής: α) Κίνδυνοι που απειλούν την ιδιωτικότητα των χρηστών (Privacy related threats), β) Παραδοσιακοί κίνδυνοι του διαδικτύου που επεκτείνονται και στο περιβάλλον των κοινωνικών δικτύων (SNS variants of traditional network and information security threats), γ) Κίνδυνοι που σχετίζονται με την ταυτότητα του χρήστη (Identity related threats) και δ) Κοινωνικοί κίνδυνοι (Social threats).

3.2. Απειλές κατά της Ιδιωτικότητας στις σελίδες Κοινωνικής δικτύωσης

Οι κύριες απειλές κατά της ιδιωτικότητας που εμφανίζονται στα κοινωνικά δίκτυα είναι οι ακόλουθες και έχουν να κάνουν κατά κύριο λόγο με την ανεπαρκή

ενημέρωση των χρηστών σε θέματα ασφάλειας και ιδιωτικότητας καθώς επίσης και με την έλλειψη κουλτούρας ασφάλειας και ευαισθητοποίησης των χρηστών.

Δημιουργία ψηφιακού φακέλου (Digital Dossier Aggregation)

Τα κοινωνικά δίκτυα αποτελούν σήμερα μια τεράστια δεξαμενή από ευαίσθητα προσωπικά δεδομένα, που καθιστά δυνατή τη δημιουργία ψηφιακών φακέλων. Οι φάκελοι αυτοί μπορεί να περιέχουν δεδομένα όπως δημογραφικά στοιχεία χρηστών, λίστα φίλων, φωτογραφίες και βίντεο του κάθε χρήστη, τοποθεσίες που έχει κοινοποιήσει ο κάθε χρήστης στο προφίλ του καθώς και μια πληθώρα άλλων πληροφοριών που χαρακτηρίζουν μονοσήμαντα τον κάθε χρήστη.

Μέσα όμως από τη δημιουργία ψηφιακών φακέλων, οι χρήστες μπορεί να αντιμετωπίσουν μια σειρά απειλών κατά της ιδιωτικότητας του χρήστη. Ένα χαρακτηριστικό παράδειγμα είναι η συλλογή των τοποθεσιών που έχει επισημανθεί ο χρήστης. Επιπλέον, μια πιο σύνηθες απειλή, αποτελεί η αποκάλυψη του ονόματος, του επώνυμου, ακόμα και της φωτογραφίας ενός χρήστη, από μία απλή αναζήτηση σε ένα κοινωνικό δίκτυο. Αξίζει να σημειωθεί επίσης ότι ακόμα και αν ο χρήστης διαγράψει κάποια δεδομένα ή ακόμα και το προφίλ του, τα δεδομένα αυτά υπάρχουν και σε άλλες κατανεμημένες τοποθεσίες και ως εκ τούτου δεν διαγράφονται ολοκληρωτικά (ENISA 2007).

Δευτερογενής Συλλογή Δεδομένων (Secondary Data Collection)

Εκτός από τα προσωπικά δεδομένα που αποκαλύπτονται εν γνώσει του χρήστη, υπάρχουν και προσωπικές πληροφορίες που αποκαλύπτονται στο πάροχο του δικτύου, μέσα από το φιλτράρισμα της κίνησης. Τέτοια δεδομένα είναι ο χρόνος και η διάρκεια της σύνδεσης, η τοποθεσία του χρήστη, η οποία προκύπτει την IP διεύθυνση του, το προφίλ άλλων χρηστών που επισκέπτεται καθώς και τα μηνύματα που ανταλλάσσει με άλλους χρήστες. Τα δεδομένα αυτά αποτελούν μια πολύ σημαντική πληροφορία για τους παρόχους των κοινωνικών δικτύων, αφού τους δίνεται τη δυνατότητα δημιουργίας αποθηκών δεδομένων (data warehouses) από τις οποίες μπορούν να αποκομίσουν σημαντικά οικονομικά οφέλη (ENISA 2007).

Αναγνώριση Προσώπου (Face Recognition)

Μια από τις πιο διαδεδομένες δραστηριότητες των χρηστών κοινωνικής δικτύωσης είναι η δημοσίευση πληθώρας φωτογραφιών, τόσο με τους ίδιους, όσο και με φίλους τους. Έμφαση στο γεγονός αυτό έρχεται να δώσει η δημοσίευση μερικών στατιστικών στοιχείων του 2013 αναφορικά με τους χρήστες του Facebook, οι οποίοι είχαν ανεβάσει περισσότερες από 250 δισεκατομμύρια φωτογραφίες και κάθε μέρα «ανεβάζουν» κατά μέσο όρο 350 εκατομμύρια νέες φωτογραφίες. Επίσης, λιγότερο παρηγορητικό είναι το γεγονός ότι πολλές από αυτές τις φωτογραφίες είναι δημόσια διαθέσιμες, τόσο για να τις δει κανείς όσο και για να τις κατεβάσει στον προσωπικό του υπολογιστή. Η εν λόγω απειλή αποτελεί μια εξελιγμένη μέθοδο συλλογής δεδομένων και χρησιμοποιείται για αυτοματοποιημένη αναγνώριση ή επιβεβαίωση της ταυτότητας ενός ατόμου από μία ψηφιακή εικόνα ή ένα καρέ από βίντεο. Επίσης, ένας επιτιθέμενος μπορεί να χρησιμοποιήσει μια "mashup" εφαρμογή (συνδυάζει δεδομένα από περισσότερες από μια πηγές σε ένα ενιαίο εργαλείο) ώστε να συνδυάσει τη φωτογραφία του χρήστη με άλλες του πληροφορίες, που βρίσκονται αναρτημένες σε άλλους ιστότοπους κοινωνικής δικτύωσης. Επιπροσθέτως, θα μπορούσε να συνδέσει τη φωτογραφία του χρήστη με το ψευδώνυμο που χρησιμοποιεί σε ένα Web blog (ENISA 2007).

Ανάκτηση Εικόνας Βάσει Περιεχομένου (Content Based Image Retrieval)

Το σύστημα ανάκτησης εικόνας βάσει περιεχομένου χρησιμοποιήθηκε αρχικά στην ψηφιακή εγκληματολογία (digital forensics). Το εν λόγω σύστημα είναι μια αναδυόμενη τεχνολογία η οποία είναι σε θέση να ταιριάξει χαρακτηριστικά, όπως ο εντοπισμός των πτυχών ενός δωματίου (π.χ. ένας πίνακας ζωγραφικής) και στηρίζεται σε πολύ μεγάλες βάσεις δεδομένων που περιέχουν εικόνες. Επίσης, επιτρέπει την σύνδεση των δεδομένων θέσης μέσω της αναγνώρισης των κοινών αντικειμένων σε εικόνες. Έτσι, δίνει τη δυνατότητα αναγνώρισης τοποθεσιών μέσα από φαινομενικά ανώνυμα προφίλ που περιέχει εικόνες με τα σπίτια των χρηστών. Ωστόσο, αυτή η δυνατότητα μπορεί να οδηγήσει σε ανεπιθύμητα μηνύματα μάρκετινγκ, σε παρακολούθηση, σε εκβιασμό και σε άλλες ενέργειες που μπορεί να σχετίζονται με την αποκάλυψη της τοποθεσίας (ENISA 2007).

Συνδεσιμότητα από Μεταδεδομένα Εικόνων (Linkability from Image Metadata)

Πολλά κοινωνικά δίκτυα επιτρέπουν στους χρήστες τους να επισημάνουν (tag) τις εικόνες που δημοσιοποιούν με μεταδεδομένα. Τα μεταδεδομένα αυτά μπορεί να είναι ονόματα των προσώπων που απεικονίζονται στις φωτογραφίες, σύνδεσμοι (links) προς τα προφίλ τους ή ακόμα και οι διευθύνσεις e-mail τους. Αυτή η δυνατότητα μπορεί να ενέχει αρκετούς κινδύνους ιδιωτικότητας για τους χρήστες, διότι άλλοι χρήστες μπορεί να δημοσιεύσουν αυτές τις εικόνες για λογαριασμό τους. Επίσης, πολλές ψηφιακές μηχανές και ακόμα περισσότερο τα smartphones ενσωματώνουν αυτόματα μεταδεδομένα, τα οποία μπορεί να χρησιμοποιηθούν για συσχετισμό με την τοποθεσία λήψης (ENISA 2007).

Δυσκολία Πλήρους Διαγραφής του Λογαριασμού ενός Χρήστη (Difficulty of Complete Account Deletion)

Όταν οι χρήστες σε ένα κοινωνικό δίκτυο, επιχειρήσουν να διαγράψουν πλήρως το προφίλ τους, θα συνειδητοποιήσουν ότι ενώ διαγράφετε η σελίδα του προφίλ τους, δεν διαγράφονται δευτερογενής πληροφορίες όπως μηνύματα προς άλλους χρήστες και δημόσια σχόλια.

Επίσης υπάρχει ασάφεια για το αν όντως οι πληροφορίες των χρηστών διαγράφονται οριστικά ή αν διατηρούνται αντίγραφα των δεδομένων των χρηστών οι οποίοι επιλέγουν να απενεργοποιήσουν ή να διαγράψουν τον λογαριασμό τους (ENISA 2007).

Ανεπιθύμητη αλληλογραφία (Spam)

Η ανεπιθύμητη αλληλογραφία είναι αυτόκλητα μηνύματα, τα οποία διαδίδονται χρησιμοποιώντας τις σελίδες κοινωνικής δικτύωσης. Πολλοί spammers έχουν προσπαθήσει να επωφεληθούν από την εκθετική αύξηση και από την ελεύθερη κυκλοφορία που παρέχουν τα κοινωνικά δίκτυα. Αυτό είναι ένα πολύ σοβαρό θέμα δεδομένου ότι στατιστικά στοιχεία ερευνών δείχνουν ότι οι ηλεκτρονικές διευθύνσεις (e-mails) αντικαθιστάτε από τα κοινωνικά δίκτυα, ως μέθοδος επικοινωνίας των χρηστών (ENISA 2007).

Απάτη (Scams)

Τα “Scams” είναι ψεύτικες προσφορές με σκοπό να ξεγελάσουν και να εξαπατήσουν τους χρήστες προσφέροντάς τους χρήματα, πληροφορίες ή κάποια επί πληρωμή υπηρεσία, εντελώς δωρεάν.

Αν ακούγεται υπερβολικά καλό για να είναι αληθινό, στο διαδίκτυο σίγουρα είναι απάτη (Scam). Οι εγκληματίες του κυβερνοχώρου χρησιμοποιούν δημοφιλείς εκδηλώσεις και ψεύτικες ειδήσεις ως δόλωμα, έτσι ώστε ο ανυποψίαστος χρήστης να ανοίξει το phishing email που του έχουν στείλει ή να κάνει κλικ σε κάποια σελίδα.

Μια μέρα πριν το παγκόσμιο κύπελλο ποδοσφαίρου του 2010, κάποιοι εγκληματίες του κυβερνοχώρου προσφέρανε δωρεάν εισιτήρια ή εισιτήρια σε πολύ χαμηλές τιμές μέσω phishing emails.

Επίσης μετά τον θάνατο του Οσάμα Μπιν Λάντεν, κυκλοφόρησε ένα βίντεο στο Facebook, το οποίο ισχυριζόταν ότι έδειχνε την σύλληψη του Μπιν Λάντεν. Το συγκεκριμένο βίντεο ήταν πλαστό. Ζητούσε από τους χρήστες να αντιγράψουν ένα κώδικα JavaScript και να το τρέξουν στον περιηγητή τους, ώστε να δουν το βίντεο. Με αυτό τον τρόπο οι εγκληματίες του κυβερνοχώρου έπαιρναν τον απόλυτο έλεγχο στον λογαριασμό Facebook του χρήστη.

Ηλεκτρονικό ψάρεμα (Phishing)

Το Phishing είναι ένα email που μοιάζει ότι στάλθηκε από κάποια νόμιμη εταιρεία ή από κάποιον αξιόπιστο άνθρωπο, δεν είναι όμως και περιέχει ένα σύνδεσμο ή ένα αρχείο που έχει κακόβουλο λογισμικό.

Οι επιθέσεις phishing δεν στοχεύουν κάποιον συγκεκριμένα και συνήθως είναι emails που στέλνονται σε τυχαίες διευθύνσεις ηλεκτρονικού ταχυδρομείου. Από την άλλη όμως οι επιθέσεις spear phishing επικεντρώνονται σε ένα συγκεκριμένο άτομο ή μια συγκεκριμένη επιχείρηση.

Τον Μάρτιο του 2011 μια ομάδα από hackers έστειλε ένα email σε κάποιους εργαζόμενους της εταιρείας παροχής υπηρεσιών ασφαλείας, RSA. Το μόνο που χρειαζόντουσαν ήταν τουλάχιστον ένας εργαζόμενος να πατήσει πάνω στο email, έτσι ώστε να κατέβει το κακόβουλο λογισμικό. Αποτέλεσμα αυτής της επίθεσης είναι οι

περισσότερες άμυνες στο δίκτυο της RSA να έχουν κατάρρευση από ένα μόνο phishing email (ENISA 2007).

Click-jacking (Παρακίνηση για κλικ σε έναν επιβλαβή σύνδεσμο)

Είναι σύνδεσμοι πάνω σε σελίδες και πολλές φορές δεν φαίνονται ύποπτοι, αλλά όταν πατηθούν μπορεί να δημιουργηθούν διάφορα προβλήματα όπως εγκατάσταση κακόβουλου λογισμικού ή αποστολή της ψηφιακής ταυτότητας του χρήστη σε κάποιον υπολογιστή.

Τα τελευταία χρόνια με την ανάπτυξη των κοινωνικών δικτύων πολλοί από αυτούς τους συνδέσμους έχουν την μορφή κουμπιών κοινωνικών δικτύων. Για παράδειγμα οι κακόβουλοι σύνδεσμοι που έχουν τα περισσότερα clicks έχουν την μορφή του Like Button του Facebook.

Προτείνετε για να αποφεύγονται οι παραπάνω σύνδεσμοι, οι χρήστες να απενεργοποιούν το Scripting καθώς και τα iframes. Επίσης καλό θα ήταν να γίνει η εγκατάσταση κάποιου προγράμματος στο περιηγητή του χρήστη, που να απενεργοποιεί αυτούς τους συνδέσμους. Τέλος οι χρήστες πρέπει να τροποποιήσουν την ρυθμίσεις ασφαλείας του περιηγητής τους για μεγαλύτερη ασφάλεια.

3.3. Μελέτη περίπτωσης δημιουργίας ψηφιακού φακέλου από φίλους φίλων στο Facebook

Στην έρευνα του Giannakopoulou (Giannakopoulos, Oikonomou & Varlamis 2012) ελέγχθηκε η ιδιωτικότητα των φωτογραφιών και των φωτογραφικών άλμπουμ των χρηστών στο Facebook. Στην εν λόγω έρευνα διαπιστώθηκε ότι προκειμένου να ελεγχθεί η ιδιωτικότητα, πρέπει να πάρεις σαν δείγμα 3 διαφορετικούς χρήστες, από τους οποίους ο ένας θα είναι λογαριασμός φίλου, ο δεύτερος θα είναι λογαριασμός ενός φίλου του φίλου και ο τρίτος, θα είναι τυχαίος. Προκειμένου να ελεγχθεί το παραπάνω σενάριο, δημιουργήθηκε ένα πρόγραμμα σε Java κώδικα, το οποίο λάμβανε ως είσοδο τα στοιχεία εισόδου του χρήστη (credential) U και προσπαθούσε να αποκτήσει πρόσβαση στη λίστα των φίλων του χρήστη U, καθώς και στις φωτογραφίες και στα άλμπουμ των φίλων του χρήστη U και των φίλων από τους φίλους του χρήστη U. Το πρόγραμμα εκτελέσθηκε σε τέσσερις γύρους. Ο $1^{ος}$ γύρος επεξεργάστηκε και δημιούργησε τη λίστα των φίλων του U. Ο $2^{ος}$ γύρος

επεξεργάστηκε τις σελίδες των φίλων του U και έβγαλε ως αποτέλεσμα τους φίλους του U, τις φωτογραφίες τους και τα άλμπουμ τους. Ο 3ος γύρος εξήγαγε τις φωτογραφίες και τα άλμπουμ από όλους τους φίλους των φίλων του U (Friend-Of-A-Friend of U/FOAFU) καθώς επίσης και τα στατιστικά προσβασιμότητας στα προφίλ των χρηστών. Ο τελευταίος γύρος του προγράμματος προσπάθησε να αποκτήσει πρόσβαση σε όλες τις φωτογραφίες και τα άλμπουμ από τους φίλους και τους φίλους-φίλων του χρήστη U, χωρίς να προσποιηθεί ότι είναι ο χρήστης U.

Τα αποτελέσματα της εν λόγω έρευνας έδειξαν ότι η πλειοψηφία των χρηστών του Facebook παρέχουν στους φίλους τους πρόσβαση στο προφίλ τους, παρέχουν περιορισμένη πρόσβαση στους φίλους των φίλων και πολύ μικρότερη πρόσβαση σε άγνωστους χρήστες. Ωστόσο, αυτοί οι περιορισμοί παρακάμπτονται εύκολα, όταν ζητηθεί πρόσβαση από μια εφαρμογή που χρησιμοποιεί ο χρήστης.

3.4. Απειλές που σχετίζονται με τα FOAF προφίλ στα Κοινωνικά δίκτυα

Μία από τις μεγαλύτερες ανησυχίες ιδιωτικότητας που προκύπτει από τη χρήση FOAF εγγράφων στα κοινωνικά δίκτυα είναι η ανεπιθύμητη αλληλογραφία (Spam). Παρά το γεγονός ότι τα διαγράφουμε ή τα επισημάνουμε ως spam, τα μηνύματα αυτά μερικές φορές φθάνουν στο ηλεκτρονικό μας ταχυδρομείο. Βασικές εταιρείες βιομηχανίας όπως η Microsoft επενδύουν ένα τεράστιο ποσό χρημάτων στην καταπολέμηση των spam και των spammers, αλλά ωστόσο φαίνεται ότι οι τελευταίοι κερδίζουν συνεχώς έδαφος.

Διάφορες τεχνικές έχουν ξεκινήσει και αναπτύσσονται κατά των spam. Ετικέτες που είναι αναγνωρίσιμες από τον άνθρωπο (όπως η τεχνική CAPTCHA) χρησιμοποιούνται σήμερα από μεγάλους παρόχους ηλεκτρονικών ταχυδρομείων ώστε να περιοριστεί η αποστολή των αυτοματοποιημένων spam. Υπηρεσίες όπως το tinymail, το οποίο έχει ως στόχο να κρύψει διευθύνσεις ηλεκτρονικού ταχυδρομείου, ή το Icon Generator, το οποίο δημιουργεί μια εικόνα εκτός ηλεκτρονικής διεύθυνσης, είναι δείγματα αυτών των προσπαθειών για την καταπολέμηση των spam μηνυμάτων. Ωστόσο, μερικοί spammers προσλαμβάνουν άτομα με σκοπό να φτιάξουν προγράμματα που παρακάμπτουν τις προαναφερθείσες τεχνικές. Ο άγραφος κανόνας του παιχνιδιού μεταξύ spammer και "spammee" (το πρόσωπο το οποίο λαμβάνει το

spam) είναι ότι όσες λιγότερες πληροφορίες παρέχονται στο διαδίκτυο σχετικά με τις προσωπικές πληροφορίες μιας επαφής, τόσο μικρότερη είναι η πιθανότητα ότι η επαφή αυτή θα λάβει μήνυμα spam.

Επιπρόσθετα, το context-aware spam, σε αντίθεση με το κοινό spam, έχει ένα υψηλό ποσοστό επισκεψιμότητας, καθώς περιέχει περισσότερες σχετικές πληροφορίες. Αυτή η έκδοση μπορεί να χρησιμοποιηθεί εύκολα από έναν spammer ή από έναν εισβολέα για την ανταλλαγή συνδέσμων διαδικτυακής απάτης ή για κάποιο άλλο κακόβουλο λογισμικό. Ο Brown μελέτησε τα τρωτά σημεία των μεγάλων κοινωνικών δικτύων (π.χ. Facebook) κατά του contextaware spam και υπολόγισε ότι περίπου το 85% των χρηστών του Facebook θα μπορούσε να είναι στο στόχαστρο του context-aware spam (Brown et al. 2008).

Αναφορικά με τα FOAF προφίλ χρησιμοποιούνται από πολλούς ανθρώπους, συμπεριλαμβανομένων των ερευνητών Σημασιολογικού Ιστού και των επαγγελματιών, ως μέσο για να δομήσουν τα στοιχεία επικοινωνίας και τα κοινωνικά δίκτυα. Τα FOAF προφίλ θεωρούνται ως "ερμηνεύσιμες μηχανές», καθώς βασίζονται σε ένα επίσημο μοντέλο και αποτελεί μια εκπροσώπηση των χαρακτηριστικών ενός ατόμου, καθώς ο χρήστης λαμβάνει υπόψη του το γεγονός ότι κατά πάσα πιθανότητα θα χρησιμοποιηθούν μόνο από μηχανές. Σε αντίθεση με τα αυτομάτως παραγόμενα αρχεία FOAF, τα αρχεία FOAF τα οποία παράγονται από τους χρήστες, συνήθως φιλοξενούνται σε προσωπικές ιστοσελίδες. Τα FOAF προφίλ που αναβαθμίζονται από τους χρήστες είναι μια χρονοβόρα και επιρρεπής σε λάθη διαδικασία. Ως εκ τούτου, έχουν αναπτυχθεί ορισμένα εργαλεία ώστε να βοηθήσουν τους χρήστες να δημιουργήσουν και να ενημερώσουν το προφίλ τους όπως η εφαρμογή FOAF-a-Matic, που αναφέρθηκε στο προηγούμενο κεφάλαιο.

Στην έρευνα των Nasirifard, Hausenblas και Decker (Nasirifard, Hausenblas and Decker 2009), περιγράφεται ένα πρόβλημα ιδιωτικότητας που προκύπτει από τη δημόσια διαθεσιμότητα, των διασυνδεδεμένων δεδομένων (linked data) σε FOAF. Συγκεκριμένα, υποστηρίζεται ότι ένας spammer μπορεί δυνητικά να επωφεληθεί από τα FOAF προφίλ στέλνοντας στους ιδιοκτήτες τους, ένα context-aware spam, Πιστεύεται ότι τα FOAF προφίλ παρέχουν μια έτοιμη είσοδο για τους spammers, οι οποίοι μπορούν να τα χρησιμοποιούν για να προσαρμόσουν το μήνυμα spam και να αυξήσουν την επισκεψιμότητα των μηνυμάτων ηλεκτρονικού ταχυδρομείου.

Καθώς τα FOAF προφίλ αποτελούν συνδεδεμένα δεδομένα, θα πρέπει να επιλέγουν μερικά συνδεδεμένα αρχεία. Σαν παράδειγμα της εν λόγω έρευνας χρησιμοποιήθηκε το αρχείο FOAF του «Axel Polleres», το οποίο ήταν είναι πλήρες και χωρίς λάθη. Ο στόχος των ερευνητών ήταν να στείλουν ένα contex-aware spam μήνυμα στον Axel χρησιμοποιώντας το FOAF προφίλ του.

Η ΕΙΚΟΝΑ 2 αναπαριστά όλα τα βήματα της διαδικασίας αποστολής spam μηνυμάτων με την εκμετάλλευση FOAF προφίλ. Το πρώτο βήμα είναι η χρήση της μηχανής αναζήτησης της Google ώστε να βρεθεί το FOAF αρχείο του ατόμου που θέλουμε να στείλουμε το Spam και να χρησιμοποιηθεί ως seed. Ωστόσο, η διαδικασία αυτή μπορεί να αυτοματοποιηθεί με τη χρήση του Google API ή κάνοντας parsing τα αποτελέσματα του HTML κώδικα. Επιπλέον, η χρήση κάποιων διαθέσιμων τεχνικών, όπως είναι η αξιοποίηση της επιλογής του είδους του αρχείου, μπορεί να βοηθήσει τους spammers να φτάσουν το επιθυμητό FOAF προφίλ στις υψηλότερες βαθμίδες (δηλαδή filetype:rdf). Στο πείραμά της εν λόγω έρευνας, θέτοντας το ερώτημα "Axel Polleres FOAF" επέστρεψε το ζητούμενο φάκελο FOAF ως τον πρώτο ανακτηθέν σύνδεσμο. Στη συνέχεια, οι ερευνητές ακολούθησαν τη σύνδεση και απέκτησαν πρόσβαση στο FOAF προφίλ του Axel. Από τη στιγμή που τα συνδεδεμένα δεδομένα είναι καλά δομημένα, μπορούν να αναλυθούν με βάση τις κοινές βιβλιοθήκες επεξεργασίας RDF, όπως η Sesame ή η Jena. Μέσα από την ανάλυση του FOAF προφίλ του Axel, εξάχθηκαν πολύτιμες πληροφορίες για τους φίλους του και τα στοιχεία επικοινωνίας.

Το επόμενο βήμα στην εν λόγω έρευνα ήταν να βρεθεί η διεύθυνση του ηλεκτρονικού ταχυδρομείου του συνδεδεμένου αρχείου. Αρχικά, τα προφίλ FOAF περιλαμβάνουν τον κώδικα κατακερμαστισμού SHA1 των διευθύνσεων ηλεκτρονικού ταχυδρομείου και είναι δύσκολο για έναν επιτιθέμενο να το σπάσει (χρησιμοποιώντας Collision attack) με την τρέχουσα δύναμη των υπολογιστών, γι' αυτό και οι συναρτήσεις κατακερματισμού αποτελούν καλές πηγές για σκοπούς "επαλήθευσης". Ως εκ τούτου, για την εύρεση των διευθύνσεων ηλεκτρονικού ταχυδρομείου, ακολουθήθηκε μια παρόμοια προσέγγιση με εκείνη για την εύρεση των προφίλ FOAF. Πιο συγκεκριμένα, μέσω της αναζήτησης στη Google και χρησιμοποιώντας το ερώτημα "Axel Polleres Email" επιστράφηκε το αιτούμενο e-mail ως τον πρώτο ανακτώμενο σύνδεσμο. Βέβαια, από τη μία μεριά το αποτέλεσμα

που επιστράφηκε είναι μια σελίδα HTML και χρειάζεται περαιτέρω επεξεργασία, αλλά από την άλλη μεριά μπορεί να χρησιμοποιηθεί ο κώδικας κατακερματισμού SHA1 του email, ώστε να βρεθεί η διεύθυνση του "spammee".

Πολλοί άνθρωποι, ως τεχνική αποφυγής ανεπιθύμητης αλληλογραφίας (spam) προσπαθούν να συγκαλύψουν τις διευθύνσεις του ηλεκτρονικού τους ταχυδρομείου χρησιμοποιώντας διάφορες τεχνικές βασισμένες σε κείμενα, όπως η αντικατάσταση του "@" με το "[at]".

Μετά την πρόσβαση του spammer (στην εν λόγω περίπτωση των ερευνητών) σε μια σελίδα HTML που περιέχει τη διεύθυνση ηλεκτρονικού ταχυδρομείου του "spammee", έπεται η αναζήτηση της λέξης κλειδί "e-mail" ή "email" αυτής της σελίδας. Στη συνέχεια εφαρμόζει τα ακόλουθα πρότυπα για την ανάκτηση του email:

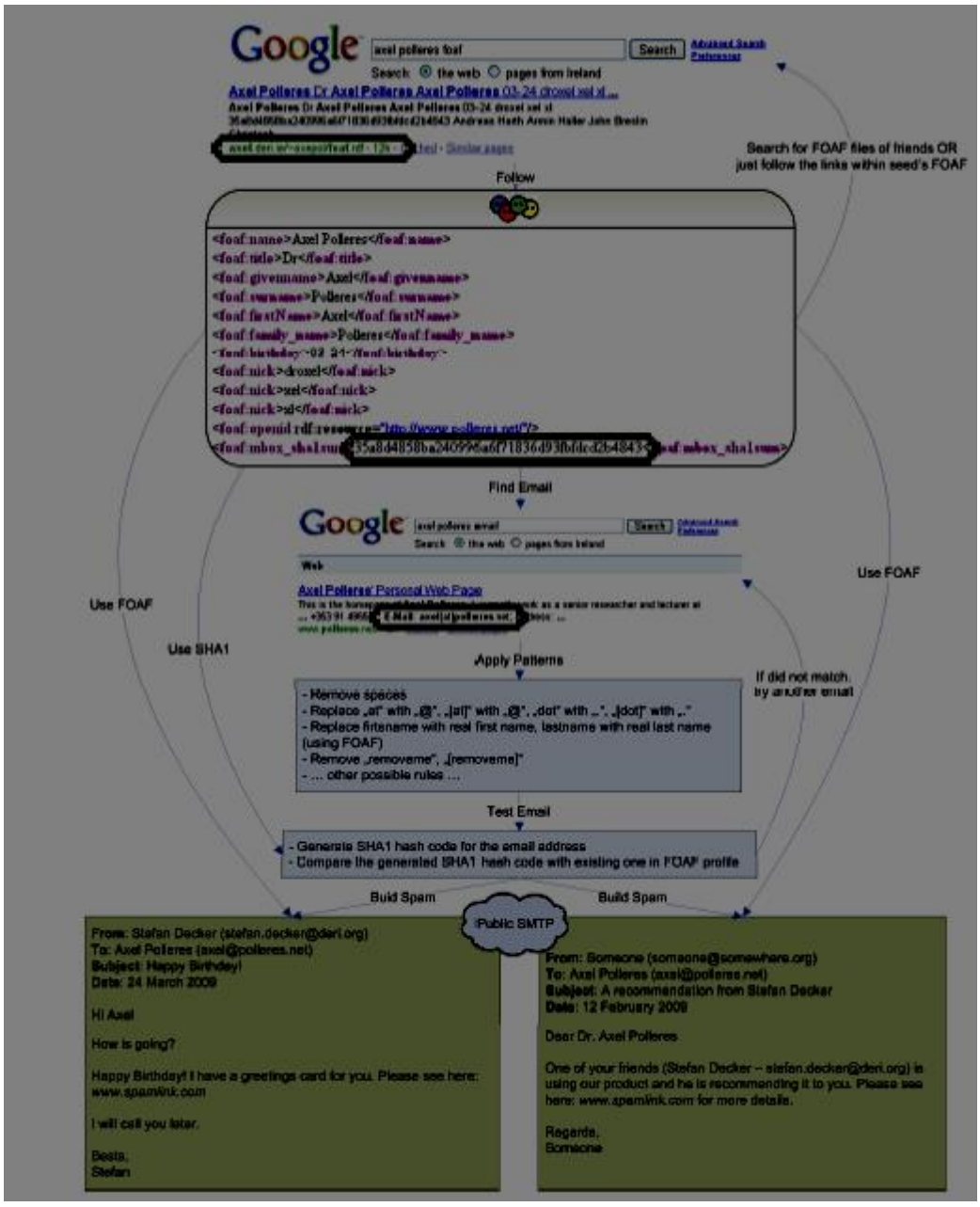
- Κατάργηση των κενών
- Αντικατάσταση του ’at’ ή ‘[at]’ με "@", και του ‘dot’ ή ‘[dot]’, με μια τελεία
- Η αντικατάσταση του «μικρού ονόματος» με το πραγματικό μικρό όνομα του χρήστη, και του «επωνύμου» με το πραγματικό επώνυμο του χρήστη (που αποκτήθηκε από το προφίλ FOAF)
- Κατάργηση των «removeme» και «[removeme]»

Καθώς η δημιουργία ενός κώδικα κατακερματισμού SHA1 είναι γρήγορη, είναι αντίστοιχα δυνατός ο συνεχής έλεγχος της έγκυρης διεύθυνσης του ηλεκτρονικού ταχυδρομείου του "spammee". Αν ο spammer, δεν επιτύχει στον πρώτο ανακτηθέν σύνδεσμο, συνεχίζει να ανατρέχει στα δεύτερα ή στα τρίτα αποτελέσματα των μηχανών αναζήτησης. Θα πρέπει να σημειωθεί ωστόσο, ότι μερικοί χρήστες παράγουν τον κώδικα κατακερματισμού του e-mail τους, χωρίς το πρόθεμα "mailto:".

Χρησιμοποιώντας τις παραπάνω τεχνικές, στην εν λόγω έρευνα προσδιορίστηκε με επιτυχία η διεύθυνση του ηλεκτρονικού ταχυδρομείου του Axel. Τώρα, για να σταλεί ένα μήνυμα ανεπιθύμητης αλληλογραφίας, πρέπει να προσδιοριστούν οι φίλοι του Axel καθώς και τα στοιχεία επικοινωνίας τους. Η εύρεση των φίλων του Axel από το FOAF προφίλ του είναι απλή, αφού παρατίθενται στο προφίλ του. Για την εύρεση των email τους, επαναλαμβάνετε η προηγούμενη μέθοδος (μέσω της μηχανής αναζήτησης της Google και χρησιμοποιώντας τη

συνάρτηση κατακερματισμού SHA1 για την έγκυρη ηλεκτρονική διεύθυνση των φίλων του).

Εφόσον έχουν συλλεχθεί η διεύθυνση ηλεκτρονικού ταχυδρομείου του spammee, μαζί με τις διευθύνσεις ηλεκτρονικού ταχυδρομείου των φίλων του, μπορεί εύκολα ο spammer να σταλεί ένα context-aware spam, χρησιμοποιώντας μερικά προκαθορισμένα πρότυπα, βάση της διασποράς των πληροφοριών που οι άνθρωποι παρέχουν στο FOAF προφίλ τους.



ΕΙΚΟΝΑ 2 *Συνολική εικόνα της διαδικασίας αποστολής Spam μνήματος εκμεταλλευόμενοι τα FOAF προφίλ* (Nasirifard, Hausenblas and Decker 2009)

Έστω στο συγκεκριμένο παράδειγμα, ότι η πληροφορία που παρείχε στο FOAF προφίλ του ο Axel, είναι η ημερομηνία γέννησής του. Ένα context-aware spam μπορεί να σταλεί στην ηλεκτρονική του διεύθυνση τη μέρα των γενεθλίων του από έναν ή περισσότερους φίλους του, που έχει ως σκοπό να τον ενθαρρύνει να επισκεφθεί μια διαδικτυακή κάρτα χαιρετισμών, η οποία περιέχει κάποιες επιβλαβής συνδέσεις (π.χ συνδέσεις που οδηγούν σε κάποιο ιστότοπο ενός επιτιθέμενου ή συνδέσεις που σε οδηγούν σε ιστότοπο με κακόβουλο λογισμικό, με απώτερο σκοπό το harvesting των προσωπικών σου στοιχείων). Επίσης, μπορεί να χρησιμοποιηθεί

ένα άλλο πρότυπο που παραπέμπει σε κάποια διαφημιστική καμπάνια και ο χρήστης να μπει σε πειρασμό να κλικάρει το σύνδεσμο, νομίζοντας ότι του το έχουν στείλει οι φίλοι του και τελικά οδηγώντας τον σε κάποια επιβλαβή ιστοσελίδα. Στην ΕΙΚΟΝΑ , απεικονίζονται δύο δείγματα μηνυμάτων spam που έχουν δημιουργηθεί με τη χρήση κάποιων προτύπων: το ένα για γενέθλια και το άλλο που συστήνει ένα προϊόν. Επιπλέον, μπορούν να υιοθετηθούν τεχνικές και εργαλεία, όπως το URL shortening, τα οποία χρησιμοποιούνται δυνητικά στην απόκρυψη του περαιτέρω περιεχόμενου και του στόχου των συνδέσμων.

Για το εν λόγω πείραμα, δεν χρησιμοποιήθηκε κάποιο πρότυπο. Δημιουργήθηκε ένα απλό email με ένα ενσωματωμένο σύνδεσμο που στάλθηκε μέσω ενός προσαρμοσμένου διακομιστή SMTP για το θύμα. Εκείνος κλίκαρε στο σύνδεσμο, νομίζοντας ότι προέρχεται από έναν από τους φίλους του και οδηγήθηκε σε μια επιβλαβή ιστοσελίδα. Αξίζει να σημειωθεί στο σημείο αυτό, ότι αυτή η προσέγγιση είναι επαναληπτική και μπορεί οι φίλοι του θύματος να χρησιμοποιηθούν ως νέα θύματα (νέοι seed) και η διαδικασία να συνεχίζεται διαρκώς.

ΚΕΦ.4: Ασφάλεια στα FOAF προφίλ

Η προστασία της ιδιωτικότητας των FOAF προφίλ έχει γίνει θέμα συζήτησης από αρκετούς ερευνητές. Συγκεκριμένα, ο Reagle (Reagle 2003) πρότεινε την κρυπτογράφηση των τμημάτων του αρχείου FOAF με σκοπό τον περιορισμό τον προσβάσεων άνευ άδειας. Επίσης, οι Frivolt και Bielikovά (2007) πρότειναν το διαχωρισμό των FOAF αρχείων, όπου το κάθε ένα θα έχει μια συγκεκριμένη προβολή. Ωστόσο, αυτές οι λύσεις δεν χρησιμοποιούνται ευρέως και ιδιαίτερα από απλούς χρήστες με αποτέλεσμα τα αρχεία FOAF να είναι προσβάσιμα σε όλους και να ανιχνεύονται από μεγάλες σημασιολογικές μηχανές αναζήτησης. Επιπλέον, φαίνεται ότι η απόκρυψη των FOAF προφίλ μπορεί να είναι αντιφατική με την άποψη περί ανοικτών δεδομένων.

Σε σύγκριση με τις κοινές ιστοσελίδες κοινωνικής δικτύωσης, η χρήση των FOAF προφίλ είναι πιο επιρρεπής σε αποστολή μηνυμάτων ανεπιθύμητης αλληλογραφίας μέσω της τεχνικής "context-aware spam". Αυτό οφείλετε στους εξής λόγους:

1. Η εύρεση του ηλεκτρονικού ταχυδρομείου των χρηστών από τα κοινωνικά δίκτυα μπορεί να είναι πολύ δύσκολη, καθώς οι περισσότεροι δικτυακοί τόποι κρύβουν τις διευθύνσεις του ηλεκτρονικού ταχυδρομείου των χρηστών. Σε αντίθεση, ο κώδικας κατακερματισμού SHA1 των email των FOAF προφίλ μπορεί να χρησιμοποιηθεί ως μέσο για την εξακρίβωση της έγκυρης διεύθυνσης του ηλεκτρονικού ταχυδρομείου των χρηστών.

2. Η ανίχνευση, μέσω Crawling, των ετερογενών και των άκρως προσαρμόσιμων κοινωνικών δικτύων (π.χ. MySpace) αποτελεί μια τεράστια διαδικτυακή επιβάρυνση (overhead) για τους spammers, ενώ τα FOAF προφίλ αποτελεί ένα μοναδικά δομημένο δεδομένο και είναι εύκολο στην ανίχνευσή του.

3. Κάποιος μπορεί να δημιουργήσει ένα ψεύτικο προφίλ χρήστη με ελλιπή ονόματα στα κοινωνικά δίκτυα, ενώ τα FOAF προφίλ θεωρούνται ότι είναι αξιόπιστα, διότι φιλοξενούνται στις προσωπικές σελίδες των χρηστών και μπορούν να παράγονται αυτόματα από μοναδικά αξιόπιστα δεδομένα.

Οι ψηφιακές υπογραφές μπορούν ενδεχομένως να εμποδίσουν την ανεπιθύμητη αλληλογραφία που βασίζεται στην εξακρίβωση της έγκυρης διεύθυνσης του ηλεκτρονικού ταχυδρομείου μέσω της συνάρτησης κατακερματισμού SHA1, αλλά

δεν είναι ευρέως χρησιμοποιημένες. Το αποτέλεσμα μιας έρευνας που πραγματοποιήθηκε από τους Nasirifard, Hausenblas και Stefan (2009), έδειξε ότι μόνο ένας στους εκατό ερευνητές και είκοσι άτομα από το προσωπικό χρησιμοποιεί μόνιμα τις ψηφιακές υπογραφές. Τρεις ερευνητές ισχυρίστηκαν ότι τις χρησιμοποιούν μόνο όποτε θέλουν να φαίνονται σοβαροί είτε όταν θέλουν να επικοινωνήσουν με κάποιον επίσημα. Ένας συμμετέχοντας υποστήριξε ότι διέθετε ψηφιακή υπογραφή, αλλά επειδή οι φίλοι του δεν την χρησιμοποιούσαν, τη θεώρησε άχρηστη και διέκοψε τη χρήση της. Ένας άλλος συμμετέχοντας ισχυρίστηκε ότι πάντα ήθελε να διαθέτει μια, αλλά λόγω των περιορισμών του χρόνου, δεν είχε διερευνήσει πώς μπορεί να την εγκαταστήσει στο ηλεκτρονικό του ταχυδρομείου. Ένας συμμετέχοντας ισχυρίστηκε ότι η διαχείριση του ζεύγους δημόσιου-ιδιωτικού κλειδιού είναι πολύ χρονοβόρα. Είπε, ωστόσο, ότι υπάρχουν κάποια εργαλεία που μπορούν να βοηθήσουν στη διαχείριση των κλειδιών αλλά απαιτούν επαλήθευση του χρήστη (human-in-the-loop) η οποία στο τέλος δημιουργεί μεγάλη επιβάρυνση για εκείνους. Ένας από τους συμμετέχοντες με επαρκή τεχνικό υπόβαθρο προσπάθησε να εγκαταστήσει ένα πιστοποιητικό στο ηλεκτρονικό του ταχυδρομείου, αλλά μετά από μισή ώρα προσπάθειας, σταμάτησε και διαμαρτυρήθηκε για την πολυπλοκότητά του υποστηρίζοντας ότι η διαδικασία είναι πολύ χρονοβόρα για ένα κοινό χρήστη χωρίς καθόλου ή με μικρό τεχνικό υπόβαθρο. Το αποτέλεσμα της έρευνας έδειξε ότι 114 από 120 συμμετέχοντες δεν έχουν χρησιμοποιήσει ποτέ ψηφιακή υπογραφή. Το γεγονός ότι πολλοί άνθρωποι δεν χρησιμοποιούν ψηφιακές υπογραφές υποδηλώνει τη χρησιμότητα των ψηφιακών υπογραφών για εκείνους, οι οποίοι τις χρησιμοποιούν επί μονίμου βάσεως.

Μια άλλη πιθανή λύση για να εμποδίσουν την ανεπιθύμητη αλληλογραφία που βασίζεται στην εξακρίβωση της έγκυρης διεύθυνσης του ηλεκτρονικού ταχυδρομείου μέσω της συνάρτησης κατακερματισμού SHA1, βασίζεται στις λεπτομερείς κεφαλίδες των μηνυμάτων του ηλεκτρονικού ταχυδρομείου. Αυτό θα δείξει την "αντιστροφή" της πορείας ενός email κατά το ταξίδι του για να φτάσει στο άτομο-στόχο. Ωστόσο, είναι ένα τεχνικό σημείο, το οποίο πολλοί χρήστες δεν γνωρίζουν ακόμη ενώ και για τους έμπειρους χρήστες, αποτελεί μια χρονοβόρα διαδικασία. Επιπλέον, υπάρχουν κάποια RFCs (π.χ. RFC 4408 - Πλαίσιο πολιτικής αποστολέα (SPF)) που βοηθούν προς αυτή την κατεύθυνση, αλλά δεν χρησιμοποιούνται ευρέως.

Μερικές ακόμα λύσεις οι οποίες μπορούν να θεωρηθούν ικανές όσον αφορά την αύξηση της προστασίας της ιδιωτικότητας των FOAF προφίλ είναι:

- Η αφαίρεση του κώδικα της συνάρτησης κατακερματισμού SHA1
- Η χρήση διάφορων λειτουργιών κατακερματισμού μέσα στη FOAF, πέρα από τη SHA1
- Η χρήση ψευδώνυμου στα άτομα και στα ονόματα των φίλων του μέσα στο FOAF προφίλ

ΚΕΦ.5: Συμπεράσματα

Η οντολογία FOAF περιγράφει κάθε οντότητα του διαδικτύου, η οποία μπορεί να είναι είτε κλάση είτε ιδιότητα. Γενικότερα, μπορεί να ειπωθεί ότι είναι ένας τρόπος για να περιγράψει κάποιος τον εαυτό του στο διαδίκτυο μέσω του ονόματός του, της ηλεκτρονικής του διεύθυνσης και των φίλων του.

Το αποτέλεσμα του Project της FOAF είναι ένα σύνολο εγγράφων, τα οποία περιγράφουν ένα δίκτυο ανθρώπων και κάθε έγγραφο με τη σειρά του, είναι μια κωδικοποιημένη περιγραφή της δομής του δικτύου.

Μελετώντας στην εν λόγω διπλωματική, το λεξιλόγιο και τη δομή ενός εγγράφου FOAF, θα λέγαμε ότι το Project της FOAF μπορεί να συντελέσει στη δημιουργία ενός αποκεντρωμένου δικτύου, λόγω της συγκεντρωτικής δομής των εγγράφων του και των διασυνδεδεμένων δεδομένων που υποστηρίζουν τα FOAF προφίλ. Ωστόσο, υπάρχουν αρχικά κάποιες προϋποθέσεις, οι οποίες πρέπει να ληφθούν υπόψη.

Η πρώτη είναι η αναγνώριση των διαφορετικών προφίλ που ανήκουν στο ίδιο πρόσωπο (π.χ., μετασχηματισμένα προφίλ από διαφορετικά κοινωνικά δίκτυα), διασφαλίζοντας τη συνοχή του δικτύου και συγχρόνως τον σχεδιασμό της αρχιτεκτονικής ενός ελεύθερου διασυνδεόμενου λογισμικού εξυπηρέτησης κοινωνικών δικτύων.

Η δεύτερη και πιο σημαντική προϋπόθεση είναι η διασφάλιση της ιδιωτικότητας ενός FOAF προφίλ. Παρά το γεγονός ότι τα διασυνδεδεμένα δεδομένα βασισμένα στο λεξιλόγιο της FOAF διαθέτουν πολλά πλεονεκτήματα για την διαδικτυακή κοινότητα, είναι απαραίτητο να γίνεται γνωστή και η κακόβουλη χρήση των εν λόγω δεδομένων (π.χ ανεπιθύμητα μηνύματα μέσω της τεχνικής context-aware spam). Επίσης, οι σημερινές επιμέρους λύσεις, όπως οι ψηφιακές υπογραφές, δεν είναι αρκετές ώστε να προστατέψουν την ιδιωτικότητα των χρηστών που έχουν δημιουργήσει τα FOAF προφίλ.

Εν κατακλείδι, θα λέγαμε ότι τα FOAF προφίλ, δεν υιοθετούν τα ζητήματα ιδιωτικότητας των κοινωνικών δικτύων, αλλά ωστόσο σε αυτά εγείρονται νέα ζητήματα, τα οποία έχουν να κάνουν με την συγκεντρωτική δομή των αρχείων FOAF.

Εάν δηλαδή κάποιος κακόβουλος χρήστης χρησιμοποιήσει ένα Crawler ή κάποια μηχανή αναζήτησης και βρει το FOAF προφίλ ενός χρήστη, μπορεί με κατάλληλες τεχνικές να αναγνωρίσει τα πραγματικά στοιχεία του χρήστη (ονοματεπώνυμο), την διεύθυνση email του, τους φίλους του και κατ' επέκταση τα κοινωνικά δίκτυα που έχει λογαριασμό ο χρήστης-στόχος.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Ξενόγλωσση βιβλιογραφία

- Buyukkokten, O., Adar, E., & Adamic, L. (2005). A social network caught in the Web. First Monday.no. 6.
- Barnes, J. A. (1972). Social networks (Vol. 26).
- Brickley, D., & Miller, L. (2004). Foaf vocabulary specification, namespace document. FOAF project.
- Brown, G., Howe, T., Ihbe, M., Prakash, A., & Borders, K. (2008, November). Social networks and context-aware spam. In Proceedings of the 2008 ACM conference on Computer supported cooperative work (pp. 403-412). ACM.
- Ding, L., Kolari, P., Ganjugunte, S., Finin, T., & Joshi, A. (2005). Modeling and evaluating trust network inference. MARYLAND UNIV BALTIMORE DEPT OF COMPUTER SCIENCE AND ELECTRICAL ENGINEERING.
- Ding, L., Zhou, L., Finin, T., & Joshi, A. (2005, January). How the semantic web is being used: An analysis of foaf documents. In System Sciences, 2005. HICSS'05. Proceedings of the 38th Annual Hawaii International Conference on (pp. 113c-113c). IEEE.
- Frivolt, G., & Bieliková, M. (2007). Ensuring privacy in FOAF profiles. In Znalosti 2007, 6th Conference on Knowledge (pp. 304-307).
- Giannakoulopoulos, A., Oikonomou, S., & Varlamis, I. Photo Sharing and Privacy on Facebook.
- Golbeck, J., & Rothstein, M. (2008, July). Linking Social Networks on the Web with FOAF: A Semantic Web Case Study. In AAAI (Vol. 8, pp. 1138-1143).
- Nasirifard, P., Hausenblas, M., & Decker, S. (2009, June). Privacy concerns of FOAF-based linked data. In Trust and Privacy on the Social and Semantic Web Workshop (SPOT 09) at ESWC09, Heraklion, Greece.
- Raad, E., & Chbeir, R. (2013). Privacy in online social networks. In Security and Privacy Preserving in Social Networks (pp. 3-45). Springer Vienna.
- Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. Harvard law review, 193-220.
- Xu, J., & Chen, H. (2003, June). Untangling criminal networks: A case study. In International Conference on Intelligence and Security Informatics (pp. 232-248). Springer Berlin Heidelberg.

Διαδικτυακές Πηγές

- Dodds, L. (2013). FOAF-a-Matic. Retrieved 5 February 2017, from http://www.ldodds.com/foaf/foaf-a-matic.html
- Dumbill, E. (2002). Finding friends with xml and rdf, IBM's XML Watch. Retrieved 5 February 2017, from http://www-106.ibm.com/developerworks/xml/library/x-foaf.html
- Dumbill, E. (2003). Tracking provenance of rdf data, IBM's XML Watch, Retrieved 5 February 2017, from http://www-106.ibm.com/developerworks/xml/library/x-rdfprov.html

- ENISA (2007). Security issues and recommendations for online social networks. Retrieved 5 February 2017, from http://www.enisa_pp_social_networks.pdf
- Foaf-project.org. (2014). The FOAF Project. Retrieved 1 February 2017, from http://www.foaf-project.org
- Reagle, J. (2003). FOAF Spheres of Privacy. Retrieved 1 February 2017, from http://reagle.org/joseph/2003/09/foaf-spheres.html
- Social Media Life (2014). Στατιστικά των Social Media Life. Retrieved 5 February 2017, from http://www.socialmedialife.gr/ [Accessed 5 Feb. 2017].
- Μπουντουρίδης, Α. (2013). Η Επιστήμη των Δικτύων: Μια Πολύ Σύντομη Εισαγωγική Παρουσίαση. Τμήμα Μαθηματικών Πανεπιστημίου Πατρών, Σημειώσεις Μαθήματος. Retrieved 4 February 2017, from http://www.slideshare.net/lisupatras/ss-19742844

Παράρτημα

Ενδεικτικές κλάσεις και ιδιότητες των FOAF εγγράφων

Κλάσεις (Class)

Κλάση foaf:Agent

Agent: ένα άτομο, μια ομάδα, ένα λογισμικό ή ένα φυσικό αντικείμενο

Κατάσταση: σταθερή
Ιδιότητες που περιέχει:
gender yahooChatID account birthday icqChatID aimChatID jabberID made mbox interest tipjar skypeID topic_interestage mbox_sha1sum status msnChatID ope nid holdsAccount weblog
Περιγραφή: Η κλάση Agent είναι η κλάση των παραγόντων, δηλαδή των αντικειμένων που ενεργούν. Μια γνωστή υποκλάση της Agent είναι η Person, η οποία αναπαριστά τους ανθρώπους. Άλλοι τύποι παραγόντων είναι οι Organization και Group.

Κλάση foaf:Group

Group: μια κλάση των παραγόντων (Agents)

Κατάσταση: σταθερή
Ιδιότητες που περιέχει: member
Υποκλάση του Agent
Περιγραφή: Η κλάση Group αναπαριστά μια συλλογή από μεμονωμένους πράκτορες, αλλά μπορεί και η ίδια να διαδραματίσει τον ρόλο ενός πράκτορα, καθώς επίσης να συνδεθεί και με άλλους πράκτορες, οι οποίοι αποτελούν την κλάση Group.

Κλάση foaf:Organization

Organization: ένας οργανισμός

Κατάσταση: σταθερή
Υποκλάση του Agent
Δεν έχει κοινά στοιχεία με: Person, Document
Περιγραφή: Η κλάση Organization αποτελεί ένα είδος της κλάσης agent, το οποίο αντιστοιχεί σε κοινωνικούς θεσμούς (π.χ εταιρίες)

Κλάση foaf:Document

Document: ένα έγγραφο

Κατάσταση: υπό δοκιμή
Ιδιότητες που περιέχει: topic, sha1, primaryTopic

Χρησιμοποιείται με:
workInfoHomepage workplaceHomepage page accountServiceHomepage openid tipj ar schoolHomepagepublications isPrimaryTopicOf interest homepage weblog
Υποκλάση του Image, PersonalProfileDocument
Δεν έχει κοινά στοιχεία με: Organization, Project
Περιγραφή: Η κλάση Document περιέχει όλα εκείνα τα αντικείμενα, τα οποία έχουν σχεδιαστεί ως έγγραφα. Η κλάση Image είναι υποκατηγορία της κλάσης Document, δεδομένου ότι όλες οι εικόνες αποτελούν έγγραφα.

Κλάση foaf:Person

Person: ένα άτομο

Κατάσταση: σταθερή
Ιδιότητες που περιέχει:
plan surname geekcode pastProject lastName family_name publications currentProjec t familyName firstNameworkInfoHomepage myersBriggs schoolHomepage img work placeHomepage knows
Χρησιμοποιείται με: knows
Υποκλάση του Agent, Spatial Thing
Δεν έχει κοινά στοιχεία με: Organization, Project
Περιγραφή: Η κλάση Person αναπαριστά ανθρώπους, χωρίς να παίζει κανένα ρόλο αν είναι εν ζωή ή όχι, αν είναι φανταστικοί ή μη. Η κλάση Person είναι υποκλάση της κλάσης Agent, δεδομένου ότι όλοι οι άνθρωποι θεωρούνται πράκτορες.

Ιδιότητες (Properties)

Ιδιότητα foaf:homepage

homepage: μια προσωπική ιστοσελίδα

Κατάσταση: σταθερή
Domain: αντικείμενο (Thing)
Range: κάθε τιμή αυτής της ιδιότητας είναι ένα έγγραφο (Document)
Inverse functional property
Η ιδιότητα homepage σχετίζει ένα αντικείμενο με την προσωπική ιστοσελίδα που υπάρχει για αυτό.
Πολλά είδη αντικειμένων έχουν προσωπικές ιστοσελίδες και κάθε αντικείμενο μπορεί να έχει πολλές προσωπικές ιστοσελίδες, αλλά περιορίζει την προσωπική σελίδα έτσι ώστε να μπορεί να υπάρχει μόνο ένα αντικείμενο που να την έχει.

Ιδιότητα foaf:knows

knows: ένα άτομο που γνωρίζει αυτό το άτομο

Κατάσταση: σταθερή
Domain: άτομο (Person)
Range: κάθε τιμή αυτής της ιδιότητας είναι ένα άτομο (Person)

Inverse functional property
Η ιδιότητα knows σχετίζει ένα άτομο σε ένα άλλο άτομο που γνωρίζει.
Αν κάποιος ξέρει ένα άτομο, είναι συνηθισμένο ότι η σχέση πρέπει να ανταποδίδεται.
Μια σχέση knows δεν σημαίνει φιλία, έγκριση ή ότι έχει γίνει μία συνάντηση πρόσωπο με πρόσωπο

Ιδιότητα foaf:account

account: υποδηλώνει ένα λογαριασμό που κατέχεται από αυτόν τον πράκτορα

Κατάσταση: υπό δοκιμή
Domain: πράκτορας (agent)
Range: κάθε τιμή αυτής της ιδιότητας είναι ένας ηλεκτρονικός λογαριασμός (OnlineAccount)
Η ιδιότητα account σχετίζει ένα πράκτορα (Agent) σε ένα ηλεκτρονικό λογαριασμό (OnlineAccount), του οποίου είναι ο μοναδικός κάτοχος
Αν κάποιος ξέρει ένα άτομο, είναι συνηθισμένο ότι η σχέση πρέπει να ανταποδίδεται.
Μια σχέση knows δεν σημαίνει φιλία, έγκριση ή ότι έχει γίνει μία συνάντηση πρόσωπο με πρόσωπο