ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

Τεχνοοικονομική Διοίκηση & Ασφάλεια Ψηφιακών Συστημάτων

Μεταπτυχιακές Σπουδές

ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Μεταπτυχιακή Διπλωματική Εργασία

Ασφάλεια στο Διαδίκτυο για όλους

Υπεύθυνος Καθηγητής: ΞΕΝΑΚΗΣ ΧΡΗΣΤΟΣ

ΒΑΒΟΥΣΗΣ ΚΩΝΣΤΑΝΤΙΝΟΣ ΜΤΕ 14002

ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Πειραιάς, Φεβρουάριος 2016

ΠΕΡΙΕΧΟΜΕΝΑ

Εισαγωγή **3**

Κεφάλαιο 1: Προστασία συστήματος **7**
Ο υπολογιστής σας 7
Αγοράζοντας το κατάλληλο laptop 9
Παραμετροποίηση hardware 13
Ανώνυμη αγορά laptop 15
Επιτήρηση laptop 16
Μέτρα ανιχνευσιμότητας 17

Κεφάλαιο 2: Λειτουργικό σύστημα **18**
Linux 19
Tails 20
Οδηγίες εγκατάστασης 22
Εκκίνηση από USB 23
Ρυθμίσεις ιδιωτικότητας Ubuntu 24
Εγκατάσταση των Tails 24
Εκκαθάριση και προετοιμασία του USB stick σας 25
Κλωνοποίηση ενός Tails USB stick 27
Χειροκίνητη εγκατάσταση των Tails μέσω UNetbootin 29
Χειροκίνητη εγκατάσταση των Tails μέσω Linux 31
Επίλυση προβλημάτων 33
Αναβάθμιση των Tails 34
Χρήση των Tails 34
Χρήση των Tails μέσω bridges (γεφυρών)/ Παράκαμψη λογοκρισίας 35
Δημιουργία μόνιμου αποθηκευτικού όγκου στα Tails 37
KeePassX 38
Email στα Tails 39

Κεφάλαιο 3: Ασφαλής πλοήγηση **44**
Browser γενικής χρήσης 45
Tor 46

Κεφάλαιο 4: Δεδομένα **50**
TrueCrypt 51
Προβλήματα στην εγκατάσταση του TrueCrypt 52
Κρυπτογράφηση αρχείων με το TrueCrypt 53
Μυστικά Κρυπτογραφημένα Σύνολα Δεδομένων 54
Κρυπτογράφηση σκληρών δίσκων 55
Ασφαλής διαμοιρασμός δεδομένων 56
Ασφαλής διαγραφή αρχείων 57
Φυσική διαγραφή 59
Μεταδεδομένα 61

Κεφάλαιο 5: Email **63**
Μεταδεδομένα Email 63
Κρυπτογράφηση Email 64
Ζεύγη κλειδιών 65
Επιβεβαίωση κλειδιών 66
Προστασία ταυτότητας και τοποθεσίας κατά την αποστολή email 66
Βασικές σημειώσεις για την κρυπτογράφηση των email 67
Οδηγίες εγκατάστασης για την κρυπτογράφηση email 68
Ρυθμίσεις Thunderbird 70

Κεφάλαιο 6: Άμεση αποστολή μηνυμάτων (Instant Messaging) **76**
Οδηγίες για το Adium των Mac: 77
Οδηγίες για το Pidgin των Linux 77
Ξεκινήστε το OTR chat 78

Κεφάλαιο 7: Κλήσεις/ Βιντεοκλήσεις μέσω Internet **81**
Ασφάλεια κινητών τηλεφώνων 83
Κλήσεις και βιντεοκλήσεις μέσω Internet 84

Κεφάλαιο 8: Κωδικοί /Passwords **86**
Παραβίαση κωδικών (Password cracking): κατανοώντας τον κίνδυνο 87
Πως να δημιουργήσετε έναν ισχυρό κωδικό 89

Κεφάλαιο 9: Επίλογος **91**

Γλωσσάριο 92
Βιβλιογραφία 93

Εισαγωγή

Το παρόν εγχειρίδιο σχεδιάστηκε για να καθοδηγήσει τους δημοσιογράφους, τα μέσα μαζικής ενημέρωσης αλλά και κάθε χρήστη του διαδικτύου, στην υιοθέτηση και εφαρμογή τεχνολογιών ασφάλειας πληροφοριών στη ψηφιακή εποχή, με σκοπό την καθημερινή προστασία της εργασίας, των πηγών και των επικοινωνιών απέναντι στο σύνολο των σύγχρονων διαδικτυακών κινδύνων.

Η ασφάλεια πληροφοριών, (αγγλική ορολογία: Information security, ή σε συντομία InfoSec), είναι η πρακτική της υπεράσπισης των πληροφοριών από μη εξουσιοδοτημένη πρόσβαση σε αυτές. Οι πληροφορίες που μπορεί να τεθούν σε κίνδυνο περιλαμβάνουν είτε μια απλή έκθεση ειδήσεων στην οποία εργάζετε κάποιος δημοσιογράφος και οποιαδήποτε σχετικά με αυτήν αρχεία ή έγγραφα, η ταυτότητα ενός έμπιστου συνεργάτη, η επικοινωνία με αυτόν, και κατά περιόδους, η ίδια η ταυτότητά των χρηστών που συμμετέχουν στο εκάστοτε έργο.

Δεν είναι απαραίτητο να είναι κάποιος ειδικός σε θέματα πληροφορικής για να διασφαλίσει τις πληροφορίες που διεχειρίζεται. Χρησιμοποιώντας το παρόν εγχειρίδιο, ο αναγνώστης θα είναι σε θέση να μάθει να αποστέλει κρυπτογραφημένα ηλεκτρονικά μηνύματα και έγγραφα από ασφαλές υπολογιστικό σύστημα σε σύντομο χρονικό διάστημα.

Απειλές: Ποιός θέτει μια απειλή;

Στοχευμένες απειλές

Οι αποκαλύψεις του E. Snowden[1] σχετικά με αμερικανούς κατά κύριο λόγο αλλά και ευρωπαίους αξιωματούχους, εξέθεσαν τις εξαιρετικές δυνατότητες ορισμένων κρατικών υπηρεσιών πληροφοριών να παρεμποδίσουν τις επικοινωνίες και να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση σε στοιχεία σχεδόν οποιουδήποτε προσωπικού υπολογιστή ή συσκευής ηλεκτρονικής επικοινωνίας ανά τον κόσμο. Πολλά κράτη στερούνται αυτές τις περίπλοκες τεχνολογίες επιτήρησης – αλλά σχεδόν όλα τα κράτη κατέχουν ορισμένες ικανότητες επιτήρησης και ελέγχου, μερικές από τις οποίες μπορούν να στραφούν, και κατά περιόδους αυτό συμβαίνει, εναντίονδημοσιογραφικών πηγών και όχι μόνο, με ενδεχομένως σοβαρές συνέπειες, οι οποίες μπορεί να αποβούν μοιραίες για την ασφάλεια των πληροφοριών των συγκεκριμένων πηγών. Για παράδειγμα, η Αιθιοπία, ένα λιγότερο τεχνολογικά προηγμένο κράτος, υποστηρίζεται ότι έχει υποστηρίξει επιθέσεις ενάντια σε δημοσιογράφους που εργάζονται σε αμερικανικά πρακτορεία[2].

[1] http://mashable.com/2014/06/05/edward-snowden-revelations/#SNq8ERbziiqI
[2] http://www.cbsnews.com/videos/ethiopian-journalists-jailed-for-government-criticisms/

Ωστόσο, δεν είναι μόνο οι επίσημες κυβερνήσεις ενός κράτους που έχει αποδειχτεί οτι μπορούν να προβούν σε τέτοιες ενέργειες αλλά και μια πληθώρα άλλων οργανισμών και εταιρειών καθώς και εγκληματικών οργανώσεων, οι οποίες διαθέτουν προηγμένες τεχνολογίες και δυνατότητες ελέγχου και επιτήρησης. Δεν είναι λίγες οι φορές που μέσω αυτών των τεχνολογιών έχουν καταφέρει εγκληματικές οργανώσεις να συγκαλύψουν τις παραβατικές τους δραστηριότητες. Επίσης, σύμφωνα με υπάρχουσες πληροφορίες, ο μεξικάνικος στρατός ξόδεψε 350 εκατομμύρια δολάρια σε εργαλεία επιτήρησης μεταξύ των ετών 2011-2012[3], και πλέον κατέχει τις απαραίτητες τεχνολογίες για να συλλέξει μηνύματα κειμένου, τηλεφωνικές κλήσεις και μηνύματα ηλεκτρονικού ταχυδρομείου, για να αυτοματοποιήσει την καταγραφή συνομιλιών σε κινητά τηλέφωνα, ακόμη και για να ανιχνεύσει κίνηση μέσα από τοίχους χρησιμοποιώντας προηγμένες τεχνολογίες ραντάρ. Αξίζει να αναφερθεί οτι μεταξύ των ετών 2011-2012, εννέα δημοσιογράφοι σκοτώθηκαν στο Μεξικό σε υποθέσεις σχετικές με την εργασία τους[4].

Η μη εξουσιοδοτημένη πρόσβαση στα στοιχεία οποιασδήποτε πηγής μπορεί να συνεπάγεται τη χρήση, την κοινοποίησή, την παραποίηση, την τροποποίηση, την επιθεώρηση, την καταγραφή ή ακόμα και την καταστροφή τους. Σε καταστάσεις υψηλού κινδύνου, η ασφάλεια των πληροφοριών (InfoSec) που κατέχει κάποιος μπορεί να είναι εξίσου σημαντική όσο το να φοράει αλεξίσφαιρο γιλέκο και να περιφέρεται υπό την συνοδεία σωματοφυλάκων. Εντούτοις, επειδή οι ψηφιακές απειλές είναι αόρατες, σύνθετες και συχνά μη ανιχνεύσιμες μπορεί να υποτιμηθούν ή να αγνοηθούν.

Απειλές Dragnet

Τα συγκεκριμένα προγράμματα σαρώνουν και συλλέγουν πληροφορίες από τον παγκόσμιο ιστό καθώς και πληροφορίες τηλεπικοινωνιών - ενδεχομένως επιτρέποντας την αναδρομική έρευνα (retroactive investigation) και χρησιμοποιούνται κατα κόρον απο την Αμερικανική Υπηρεσία Εθνικής Ασφαλείας (NSA) και την Κρατική Υπηρεσία Πληροφοριών της Βρετανίας (GCHQ). Σε περίπτωση που κάποιος ή κάποια ενέργεια κινήσει το ενδιαφέρον κάποιας κυβέρνησης, παραδείγματος χάριν λόγω αμφισβητούμενων δραστηριοτήτων, τα προγράμματα αυτά επιτρέπουν να δημιουργηθεί ένας φάκελος ο οποίος θα ενημερώνεται για την καθημερινή δραστηριότητα του εκάστοτε υποκειμένου υπό έρευνα επί παντός επιστητού, με αναδρομική αναφορά πολλών ετών.

[3] http://www.slate.com/blogs/future_tense/2012/08/03/surveillance_technology_in_mexico_s_drug_war_.html
[4] https://en.wikipedia.org/wiki/List_of_journalists_and_media_workers_killed_in_Mexico

Η ασφάλεια πληροφοριών στην πράξη

Ένας αποτελεσματικός δημοσιογράφος, σίγουρα στην πορεία της καριέρας του θα έχει βρεθεί να «σκαλίζει σε ξένα χωράφια». Υιοθετώντας, λοιπόν, στην πράξη μια ολοκληρωμένη στρατηγική ασφάλειας πληροφοριών (InfoSec Strategy) και κατα συνέπεια συγκεκριμένες μεθόδους και στρατηγικές, ουσιαστικά μεταλάσσει τον τρόπο με τον οποίο δουλεύει, ειδικότερα όταν διαχειρίζεται ευαίσθητα θέματα σε συνδυασμό με ευπαθείς πηγές. Το πρώτο βήμα στην άσκηση μιας αποδοτικής στρατηγικής InfoSec έγκειται στην ικανότητα της αναγνώρισης των απειλών, και το δεύτερο στην αναγνώριση των ευπαθειών του hardware και του software που χρησιμοποιεί κάποιος. Η κατανόηση του πώς και του γιατί η μη εξουσιοδοτημένη πρόσβαση συμβαίνει, είναι το πρώτο βήμα στην εκμάθηση του τρόπου για να προστατευθεί από αυτήν.

Νομιμότητα

Παρά το γεγονός ότι η επιτήρηση και ο έλεγχος των δεδομένων νομοταγών πολιτών έχει χαρακτηριστεί απο πολλούς[5] ως καταπάτηση των διεθνών ανθρωπίνων δικαιωμάτων περι ιδιωτικότητας, αντίστοιχα και η χρήση ορισμένων εργαλείων ιδιωτικότητας μπορεί να θεωρηθεί παράνομη.

Αρκετά από τα εργαλεία ιδιωτικότητας που αναφέρονται και αναλύονται σε αυτό το εγχειρίδιο είναι κρυπτογραφικά εργαλεία. Ορισμένα συστήματα κρυπτογράφησης μπορεί να είναι παράνομα, ή να απαιτούν την έκδοση άδειας, σε διάφορες χώρες συμπεριλαμβανομένης της Κίνας, της Κούβας, του Ιράν, της Λιβύης, της Μαλαισίας, της Βόρειας Κορέας, της Σιγκαπούρης, του Σουδάν, και της Συρίας[6]. Κατα συνέπεια, η είσοδος σε μια απο τις παραπάνω χώρες θα πρέπει να προυποθέτει και την δήλωση χρήσης οποιασδήποτε τεχνολογίας κρυπτογράφησης. Σε κάθε περίπτωση, θα πρέπει να εξεταστούν προσεκτικά όλες οι νομικές επιπτώσεις της χρήσης ενός συστήματος κρυπτογράφησης ώστε κάποιος με ασφάλεια να μπορεί να αποφασίσει πότε και που μπορεί να το χρησιμοποιήσει.

Μοντελοποίηση Απειλών

Το παρόν εγχειρίδιο περιέχει πολλές πληροφορίες για τις διάφορες πιθανές διαδικτυακές απειλές, καθώς και για τα μέτρα που μπορούν να ληφθούν για την προστασία από αυτές. Αξίζει ωστόσο να σημειωθεί οτι οι τεχνολογίες που χρησιμοποιούνται στις διαδικτυακές επιθέσεις συνεχώς μεταλάσσονται και τις

[5] http://www.nytimes.com/2015/05/08/us/nsa-phone-records-collection-ruled-illegal-by-appeals-court.html?_r=0
[6] Σχετικά με τη νομοθεσία γύρω από την ισχύουσα κρυπτογράφηση σε κάθε χώρα: http://www.cryptolaw.org

περισσότερες φορές παραμένουν μυστικές. Οπότε σπάνια μπορεί κάποιος με βεβαιότητα να πιστοποιήσει την προέλευση ή τον προορισμό κάποιας απειλής και συνεπώς και την αποτελεσματικότητα της άμυνας απέναντι σε αυτήν. Επομένως, το ρίσκο της προσωπικής αξιολόγησης ενός κινδύνου και ο σχεδιασμός της άμυνας είναι προσωπική υπόθεση του καθενός. Κάποιοι αποφασίζουν να παρακάμψουν μεθόδους ασφάλειας, παρόλο που είναι ενήμεροι για τους κινδύνους, γιατί το θεωρούν μη πρακτικό και ταυτόχρονα χρονοβόρο θέτοντας σε κίνδυνο την ασφάλεια των δεδομένων τους.. Άλλοι χρήστες πειραματίζονται με πολύπλοκες InfoSec συμβουλές, οι οποίες δεν ανταποκρίνονται στις πραγματικές τους ανάγκες, επειδή απλά μπορούν να το κάνουν.

Το παρόν εγχειρίδιο έχει εντοπίσει τις βασικές ερωτήσεις, οι οποίες θα πρέπει να διαμορφώνουν το κάθε μοντέλο ασφάλειας που κάποιος αποφασίζει να υιοθετήσει και παρατίθενται παρακάτω:

1. Ποιοι θα μπορούσαν να είναι οι πιθανοί επιτιθέμενοι που θα απειλήσουν;
2. Ποια είναι τα πιθανά εργαλεία που έχουν στην διάθεσή τους οι επιτιθέμενοι;
3. Ποιά η πιθανότητα που έχει ο επιτιθέμενος να διαθέσει τα εργαλεία που διαθέτει για να πραγματοποιήσει μια επίθεση;
4. Ποιοί είναι οι κίνδυνοι που θα υπάρξουν μέσω μιας στοχευμένης επίθεσης;
5. Ποιοι κίνδυνοι προκύπτουν από την παθητική επιτήρηση (passive surveillance); Πόσο εκτενή είναι τα εργαλεία που χρησιμοποιούνται στην παθητική επιτήρηση;
6. Ποιες αμυντικές στρατηγικές είναι πρακτικές, ασφαλείς και αποτελεσματικές;
7. Ποιες αμυντικές στρατηγικές είναι πρακτικές, ασφαλείς, αποτελεσματικές για τις πηγές και τους συναδέλφους, λαμβάνοντας υπόψη τους κινδύνους που υφίστανται από την επικοινωνία μαζί τους;

Στην εποχή της παγκοσμιοποίησης, οι απειλές μεταβάλλονται συνεχώς και μαζί με αυτές αλλάζουν και οι τεχνολογίες που είναι διαθέσιμες για την προστασία των πολιτών αλλά και στην περίπτωση αυτού του εγχειριδίου των δημοσιογράφων. Τα στοιχεία που αναφέρθηκαν παραπάνω και η ανάλυση που θα ακολουθήσει αποδεικνύουν την σημασία της κατανόησης, του InfoSec εις βάθος τόσο σε θεωρητικό όσο και σε πρακτικό επίπεδο.

Κεφάλαιο 1: Προστασία συστήματος

Οι μέθοδοι ασφάλειας ή/και κρυπτογράφησης που χρησιμοποιούνται θα είναι αποτελεσματικές, μόνο εάν και τα επιμέρους στοιχεία ενός συστήματός είναι ασφαλή. Ακόμα κι αν γίνεται αποστολή email χρησιμοποιώντας ισχυρή κρυπτογράφηση, ή ακόμα κι αν υπάρχουν πολύ ισχυροί κωδικοί πρόσβασης, εάν το σύστημά «παρακολουθείται», έχει πέσει θύμα χάκινγκ, ή είναι ευάλωτο σε διαδικτυακές επιθέσεις, τότε κάθε προσπάθεια θα είναι ανώφελη.

Οι στρατηγικές προστασίας μπορεί να ποικίλουν, απο την πιο απλή μέχρι την πιο σύνθετη, ανάλογα με το επίπεδο του κινδύνου και της πολυπλοκότητας των μεθόδων που υιοθετούν εκείνοι που ενδεχομένως μας έχουν στοχοποιήσει (επιτιθέμενοι-κακόβουλοι χρήστες), Σε όλες τις περιπτώσεις, όμως, η λογική που ακολουθείται είναι παρόμοια με το χτίσιμο ενός σπιτιού από τραπουλόχαρτα – για να πετύχει, πρέπει το σπίτι να χτιστεί με ασφάλεια από τα θεμέλια. Είναι αρκετά σημαντικό όλοι οι χρήστες να γνωρίζουν τις ευπάθειες του ίδιου τους του συστήματος, ακόμα κι αν δεν έχουν την ικανότητα ή την ανάγκη να τις διορθώσουν. Το πρώτο αυτό κεφάλαιο θα μελετήσει τις βάσεις που χρειάζεται το εκάστοτε σύστημα για την μέγιστηασφάλεια του hardware και του firmware οπότε είναι στο σύνολο του αρκετά τεχνικό και περιέχει πολύτιμες πληροφορίες για όσους ενδιαφέρονται να διασφαλίσουν στο μέγιστο βαθμό τα δεδομένα τους Στο σημείο αυτό, θα εξεταστεί η οδυνηρή πραγματικότητα της έκτασης των ευπαθειών του hardware, και ο αναγνώστης θα μπορεί να αποφασίσει μόνος του ποια είναι τα κατάλληλα μέτρα ασφάλειας για εκείνον. Για αρκετές από τις λύσεις που περιγράφονται (όπως είναι οι ειδικές τροποποιήσεις στο hardware, και η αντικατάσταση του firmware) ίσως είναι αναγκαία η βοηθεία εξειδικευμένων τεχνικών.

Οι λύσεις που είναι διαθέσιμες είναι αρκετές, αλλά η επίτευξη του μέγιστου επιπέδου ασφάλειας είναι το αποτέλεσμα μόνο μίας.

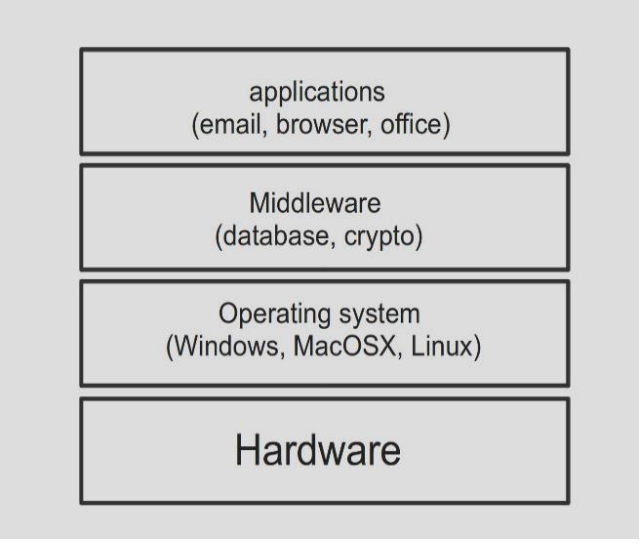
<u>*Ο υπολογιστής*</u>

Interface – οθόνη.

Applications (Εφαρμογές)–Software

λογισμικό/προγράμματά.

Middleware – λογισμικό που συνενώνει δύο ξεχωριστά και ήδη υπάρχοντα προγράμματα: π.χ. επιτρέπει σε προγράμματα να έχουν πρόσβαση σε βάσεις δεδομένων κλπ.



Λειτουργικό σύστημα – Windows XP/7/8/10, Mac OS X, Linux, κ.λπ.

Firmware – θεμελιώδες software προγραμματισμένο πάνω στο hardware, το οποίο παρέχει οδηγίες για το πώς η συσκευή επικοινωνεί με το Hardware του υπολογιστή.

Hardware – τα φυσικά μέρη που περιλαμβάνει ένα υπολογιστικό σύστημα.

Σε αυτό το κεφάλαιο, θα αναλυθεί πρωτίστως η ασφάλεια του θεμελιώδους επιπέδου ενός υπολογιστή: του hardware και του firmware.

Hardware και firmware

«Το Hardware» αναφέρεται στο μηχάνημα αυτό καθαυτό. Καθώς οι υπολογιστές Desktop (γραφείου) δεν συνίστανται για οποιαδήποτε δημοσιογραφική εργασία, επειδή όχι μόνο δεν είναι πρακτικοί, αλλά και ευάλωτοι σε φυσικές παρεμβάσεις, το παρόν κεφάλαιο θα έχει ως βασικό σημείο αναφοράς τα laptops.

Για λόγους ευκολίας, η λέξη laptop θα αναφέρεται σε όλα τα φυσικά μέρη, συμπεριλαμβανομένης της μπαταρίας, του σκληρό δίσκου (hard disk drive), της οπτικής μονάδας CD-DVD (CD-DVD drive), της κάρτας δικτύου, του μικροφώνου, και της κάμερας. Επίσης, θα θεωρηθεί μέρος αυτού και το πρόσθετο hardware: οποιοδήποτε πληκτρολόγιο, ποντίκι, σαρωτή-εκτυπωτή, εξωτερική κάμερα, κ.ο.κ.

Οι κυριότεροι κίνδυνοι για ένα hardware είναι η κλοπή ή η φθορά, η τεχνητή ή φυσική αλλοίωση καθώς και οποιαδήποτε εικονική η απομακρυσμένη επίθεση με στοχο το πλήθος των δεδομένων ενός συστήματος. Τα πέντε σημαντικά μέτρα για την προστασία του hardware είναι:

> Αποτροπή των εικονικών και φυσικών επιθέσεων στο hardware

1. Αγορά του σωστού laptop
2. Τροποποίηση του hardware

> Αποτροπή των φυσικών επιθέσεων στο hardware

3. Ανώνυμη αγορά του laptop
4. Φύλαξη του laptop
5. Μέτρα ανίχνευσης (εάν απομακρύνεστε από το laptop σας)

Παρόλο που αυτά τα πέντε μέτρα μπορεί να φαίνονται περίπλοκα και ίσως να προκαλούν σύγχυση, ή ακόμα και να αποθαρρύνουν τον αναγνώστη εξαρχής, είναι όλα εξ' ολοκλήρου πραγματοποιήσιμα για όλους τους ενδιαφερόμενους δημοσιογράφους, αλλά και για όλους τους χρήστες που είναι άπειροι σε θέματα πληροφορικής και ασφάλειας. Επομένως ανάλογα με το επίπεδο του κινδύνου για το οποίο επιθυμεί κάποιος να προετοιμάσει τον εαυτό του, υπάρχουν και τα κατάλληλα μέτρα για να διατηρηθεί ασφαλές το hardware.

1. Αγοράζοντας το κατάλληλο laptop

Το επίπεδο ασφάλειας καθόριζεται πρωτίστως από την επιλογή και αγορά του laptop. Τη δεδομένη στιγμή, πολύ λίγα laptops είναι επαρκώς ασφαλή ενάντια στις σύγχρονες απειλές. Πράγματι, όσο περισσότερα μαθαίνουμε από τα αρχεία του Snowden για τις ικανότητες εκτενούς επιτήρησης, τόσο καλύτερα κατανοούμε πως όλα τα μηχανήματα είναι επισφαλή. Ενδεχομένως, με την πάροδο του χρόνου, θα είμαστε σε θέση να αναπτύξουμε ασφαλέστερες λύσεις.

Αυτό μπορεί να μην είναι πρόβλημα για όλους τους χρήστες, αλλά εξαρτάται απο το ποιος είναι ο κακόβουλος χρήστης που επιθυμεί να αποσπάσει τα δεδομένα, είτε δηλαδή είναι αρχές ασφαλείας κυβερνήσεων και μεγάλων εταιρειών είτε πρόκειται για πολιτικές, στρατιωτικές, τρομοκρατικές, ή επαναστατικές ομάδες. Κάθε φορά θα πρέπει να υπολογιστεί πόσο περίπλοκα είναι τα εργαλεία που έχει στην διάθεσή του ο εκάστοτε αντίπαλός, πόσο εύκολο είναι αυτά τα εργαλεία να τα διαθέσει εναντίον των δεδομένων που έχει στην κατοχή του κάποιος χρήστης, με ποιούς τρόπους μπορεί να το κάνει, πόσο σημαντικά είναι τα δεδομένα ως στόχος, και επιπλέον ποια μέτρα προστασίας είναι κατάλληλα ανάλογα με την απειλή.

Υπάρχουν 4 ζητήματα που πρέπει να εξετάζονται τη στιγμή της αγοράς ενός laptop και τα οποία θα καθορίσουν το επίπεδο ασφαλείας ενός συστήματός.

Συντήρηση Hardware

Πλέον, πολλές εταιρείες, όπως η IBM/Lenovo, HP, και Dell δίνουν την δυνατότητα ιδιωτικής παραμετροποίησης του hardware του υπολογιστή (DIY hardware modification), παρέχοντας πρόσβαση στο εσωτερικό του, κάτι που πολλοί χρήστες επιλέγουν για την ενίσχυση του επιπέδου ασφάλειας. Κάτι τέτοιο καθίσταται δυσκολότερο με τα MacBooks, τα οποία δεν ανοίγουν εύκολα με αποτέλεσμα πιθανή διακοπή της παρεχόμενης εγγύησης.

Firmware

Το firmware (ελληνικός όρος: υλικολογισμικό) είναι ένα λογισμικό προγραμματισμένο επάνω στο hardware του laptop. Πιο συγκεκριμένα, πρόκειται για ένα είδος λογισμικού το οποίο είναι γραμμένο σε γλώσσα μηχανής (ή σε συμβολική γλώσσα). Με απλά λόγια, το firmware παρέχει οδηγίες για το πώς τα μέρη του laptop πρέπει να επικοινωνήσουν μεταξύ τους. Το firmware αποτελεί άλλον έναν πιθανό στόχο επίθεσης, καθώς οι ιδιαίτερα περίπλοκες διαδικτυακές επιθέσεις μπορεί να είναι σε θέση να αποκτήσουν απομακρυσμένο έλεγχο ενός υπολογιστή.

Το firmware σε ένα MacBook μπορεί να «κλειδωθεί», κάνοντας το firmware προσπελάσιμο μόνο μέσω κωδικού πρόσβασης που θα θέσει ο ίδιος ο χρήστης. Η δυνατότητα να κλειδωθεί το firmware, παρέχει στα Mac ένα συγκεκριμένο πλεονέκτημα ασφάλειας έναντι των υπολοίπων laptops, από τα οποία μόνο ένας περιορισμένος

αριθμός προτύπων μπορεί να εξασφαλιστεί, μέσω μιας ιδιαίτερα τεχνικής διαδικασίας για την αντικατάσταση του firmware κλειστού πηγαίου κώδικα (ο οποίος είναι ιδιόχρηστος και όχι δημόσια διαθέσιμος ή ελέγξιμος) με firmware ανοιχτού πηγιαίου κώδικα (ο οποίος ονομάζεται «coreboot» και είναι διαθέσιμος και ελέγξιμος για όλους δημόσια). Φυσικά, η εμπιστοσύνη στην ασφάλεια που παρέχεται από το κλείδωμα του MacBook εξαρτάται από την εμπιστοσύνη κάποιου στην Apple. Παρόλο αυτά, δεν υπάρχουν προς στιγμήν άγνωστες ευπάθειες (zero-days), και η χρήση του κλειδώματος θα μπορούσε αν μη τι άλλο, να αποτελέσει ένα επιπλέον εμπόδιο για τον επιτιθέμενο.

Κλειδώστε το Mac Firmware

Η ενεργοποίηση της συγκεκριμένης λειτουργίας είναι αρκετά απλή προσφέροντας ένα ικανοποιητικό επίπεδο ασφάλειας στις επιθέσεις σε firmware. Επομένως, οι χρήστες των Mac ίσως επιθυμήσουν να χρησιμοποιήσουν το χαρακτηριστικό αυτό σε κάθε περίπτωση.

Για να ενεργοποιηθεί η πρόσβαση στο firmware με ειδικό κωδικό πρόσβασης για το Mac (OS X), πρέπει να επανεκκινηθεί το laptop, κατά την εκκίνηση ο χρήστης να πατήσει τα πλήκτρα 'cmd' και 'R' για να μπεί στο Recovery mode. Στο top menu bar, ακολουθείται η εξής διαδρομή: 'Utilities' > 'Firmware Password Utility' > 'Turn On Firmware Password'. Κατόπιν της επιλογής ενός ισχυρού κωδικού πρόσβασης (δείτε το κεφάλαιο 8) κάνετε click στο 'Set Password'. Είναι πολύ σημαντικό να θυμάται ο χρήστης τον κωδικό πρόσβασης που έθεσε, αλλιώς υπάρχει η πιθανότητα να χάσει την πρόσβαση στο Mac του.

- **Chipsets**

Τα chipsets είναι τσιπ που λειτουργούν στις μητρικές των laptop. Περίπου από το 2006, η Intel άρχισε να προσθέτει ειδικά στοιχεία στα chipsets της για να επιτραπεί η αυτοματοποιημένη διαχείριση των συστημάτων της πέρα από ένα δίκτυο. Αυτό ονομάζεται 'Intel Active Management Technology', και με απλά λόγια σημαίνει ότι ένας τεχνικός πληροφορικής μπορεί να ενημερώσει το λογισμικό, ή να κάνει άλλες ενέργειες στα μηχανήματα, χωρίς να χρειάζεται να έχει φυσική πρόσβαση στην ίδια τη συσκευή. Το πρόβλημα, φυσικά, είναι ότι την ίδια διαδικασία μπορεί να εκμεταλλευθεί κάποιος για να εγκαταστήσει spyware ή να χειριστεί τα συστήματα με άλλους τρόπους. Όλα τα laptops που κατασκευάσθηκαν μετά το 2008 περιέχουν αυτά τα chipsets, και είναι επομένως ευάλωτα σε αυτού τους είδους των επιθέσεων όταν βρίσκονται εντός δικτύου.

Το chipset «Intel 945» είναι το πιο πρόσφατο chipset χωρίς αυτό το αυτοματοποιημένο χαρακτηριστικό γνώρισμα, και ως εκ τούτου είναι το πλέον κατάλληλο για μια ασφαλέστερη μητρική κάρτα. Κατά την επιλογή του laptop, κάθε χρήστης μπορεί να δει το chipset που περιέχει η μητρική στις προδιαγραφές του.

- **Λειτουργικό Σύστημα**

Γενικά προτείνεται η αγορά laptop που θα επιτρέπει στον χρήστη να εγκαταστήσει το λειτουργικό σύστημα της επιλογής του (ιδανικά να είναι open source, του οποίου ο πηγαίος κώδικας είναι δημοσίως διαθέσιμος). Κάτι τέτοιο μπορεί να γίνει αρκετά εύκολα στα περισσότερα laptops, εκτός από τα MacBooks.

Ενώ τα περισσότερα laptops επιτρέπουν στους χρήστες εύκολα να διαγράψουν το λειτουργικό σύστημα Windows, η διαγραφή του λειτουργικού ενός MacBook δεν συνίσταται, καθώς μπορεί να θέσει σε κίνδυνο τη γενική λειτουργία του συστήματος.Τα ιδιόκτητα λειτουργικά συστήματα (Windows, Mac) είναι κλειστού κώδικα και μπορεί να διαθέτουν ορισμένα ενσωματωμένα backdoors ασφάλειας – έτσι δεν είναι γνωστό το κατά πόσο θα είναι ασφαλές ένα laptop που τρέχει ταυτόχρονα εναλλακτικά λειτουργικά συστήματα. Είναι δυνατό να χρησιμοποιηθούν διάφορα λειτουργικά συστήματα στα Mac, αλλά αυτό απαιτεί τη γνώση του τρόπου με τον οποίο μπορεί να τρέξει ένα «μηχάνημα εικονικής πραγματικότητας», ένα θέμα το οποίο δεν θα εξετάσουμε σε αυτό το σημείο. (δείτε το κεφάλαιο 2).

Πώς μπορούμε, όμως, να ερμηνεύσουμε αυτά τα τέσσερα θεμελιώδη θέματα ασφαλείας για τη μοντελοποίηση απειλών; Η πρόσβαση στα απομακρυσμένα hardware, firmware, και στα chipset είναι πολύ πιθανό να είναι δυνατή μόνο από τις επίσημες υπηρεσίες πληροφοριών των τεχνολογικά προηγμένων και πλούσιων χωρών. Ακόμα, όμως κι αν δεν αντιμετωπίζεται ένας κίνδυνο τέτοιου επιπέδου, μπορεί ένας χρήστης να θελήσει να εξετάσεις τις ευπάθειες των ανωτέρω παραγόντων και να λάβει μερικές επιπλέον προφυλάξεις ως μέτρα ασφαλείας. (Ιδιαίτερα εκείνα που απαιτούν λιγότερη προσπάθεια, όπως το κλείδωμα του firmware σε ένα Mac).

Είναι πιθανό οι τεχνολογικά προηγμένες υπηρεσίες πληροφοριών να έχουν πρόσβαση στα backdoors των λειτουργικών συστημάτων. Έτσι θα πρέπει να εξεταστούν προσεκτικά τυχόν επιπτώσεις ασφάλειας που μπορεί να προέρχονται από προβλήματα στο λειτουργικό σύστημα.

Η επιλογή του laptop δεν είναι εύκολη υπόθεση, και γι' αυτό θα πρέπει κάθε χρήστης να αφιερώσει χρόνο ώστε επεξεργαστείτε αυτές τις πληροφορίες, αξιολογώντας τα επίπεδα του κινδύνου, ενώ παράλληλα να αποφασίσει πόσο διατεθιμένος είναι να προσπαθήσει να επενδύσει στην ασφάλεια των πληροφοριών και των δεδομένων του.

Παρακάτω παραθέτω ορισμένες προτάσεις για την επιλογή του laptop που μπορείτε να κάνει οποιοσδήποτε σε διάφορα γενικευμένα επίπεδα κινδύνου:

Χαμηλό επίπεδο κινδύνου: dragnet παρακολούθηση, χαμηλού βαθμού μεμονωμένο hacking, κλοπή.

Οποιοδήποτε laptop θεωρείται καλή επιλογή σε αυτή την περίπτωση. Η αποφυγή της κλοπής ή φυσικών παρεμβάσεων μπορεί να αποφευχθεί με το να κρατάει ο χρήστης

το μηχάνημα διαρκώς κοντά του ενώ η αποφυγή του ψηφιακού dragnet επιτυγχάνεται μέσω των επιλογών του λογισμικού και των εφαρμογών.

Μεσαίο επίπεδο κινδύνου: στοχευμένη παρακολούθηση, από έναν αντίπαλο που είναι προετοιμασμένος ή ικανός να επενδύσει σχετικά περιορισμένους πόρους.

Ενδείκνυται η χρήση είτε laptop του οποίου το τρέχον λειτουργικό σύστημα μπορείτε να διαγραφεί ανά πάσα στιγμή και να εγκατασταθεί ένα άλλο (ιδανικά, ένα λειτουργικό σύστημα open source Linux), είτε η χρήση του λειτουργικού συστήματος Tails για να μπορεί κάποιος να εργαστεί από οποιονδήποτε υπολογιστή. Δείτε το κεφάλαιο 2 για περισσότερες πληροφορίες για τα λειτουργικά συστήματα.

Υψηλό επίπεδο κινδύνου: στοχευμένη παρακολούθηση από μια υπηρεσία πληροφοριών.

Υπάρχουν ελάχιστα μηχανήματα που μπορούν με βεβαιότητα να παραμείνουν ασφαλή ενάντια στην απομακρυσμένη πρόσβαση στο hardware, firmware και στα chipset. Την σύγχρονη εποχή το μοντέλο που εξασφαλίζει υψηλότερο επίπεδο προστασίας είναι το IBM ThinkPad X60 (και X60s). Διαθέτει ένα Intel 945 chipset (δηλ. pre-AMT), καθώς επίσης και λειτουργία που εξασφαλίζει την αντικατάσταση του firmware με firmware ανοιχτού κώδικα, 'coreboot'. Έπειτα επιβάλλεται η χρήση του λειτουργικού συστήματος Tails (δείτε το κεφάλαιο 2) για να διατηρηθεί η ασφάλεια των συστημάτων.

Για να πραγματοποιηθούν οι ανωτέρω ενέργειες απο κάποιον ιδιωτικό χρήστη, θα μπορούσε κάποιος να προμηθευτεί ένα οποιοδήποτε laptop με pre-AMT chipset, το οποίο επιτρέπει να ανοιχτεί το περίβλημα και να χρησιμοποιηθούν on-line διαθέσιμοι οδηγοί με όλα τα βασικά βήματα. Για παράδειγμα, θα μπορούσε να αφαιρεθεί ο σκληρός δίσκος από το laptop, και να αφαιρεθεί ή να τεθεί εκτός λειτουργίας το μικρόφωνο, η webcam, η κάρτα δικτύου, η κάρτα Bluetooth, ή το 3G modem, και η θύρα Ethernet (βλέπε το δεύτερο μέρος αυτού του κεφάλαιου). Παρόλο αυτά, χωρίς την κατάλληλη εκπαίδευση, δεν μπορεί κάποιος να είναισε θέση να κάνει τις περισσότερες τροποποιήσεις hardware για την καλύτερη δυνατή ασφάλεια του συστήματός τους, ή να αντικαταστήσει το firmware.

Ανώτατο επίπεδο κινδύνου: στοχευμένη παρακολούθηση από μια υπηρεσία πληροφοριών, ενδεχομένως με σκοπό να εκθέσει σε κίνδυνο την ασφάλεια και την ελευθερία του στόχου /ή των στόχων, και την ακεραιότητα των στοιχείων τους.

Στις καταστάσεις πολύ υψηλού κινδύνου, θα πρέπει κάποιος να έχει τουλάχιστον δύο laptops στα οποία θα εφαρμόζονται όλα τα ανωτέρω μέτρα ασφάλειας. Ένα από αυτά τα laptops δεν θα πρέπει ποτέ να συνδέεται στο Διαδίκτυο με οποιονδήποτε τρόπο καθώς ακόμη και η ασφαλέστερη συσκευή μπορεί να εκτεθεί σε κίνδυνο όταν βρίσκεται online, ιδιαίτερα εάν ο χρήστης της αποτελεί το αντικείμενο μιας στοχευμένης επίθεσης. Με άλλα λόγια έναairgapped μηχάνημά. αποτελεί ένα πολύ χρήσιμο μηχάνημα για να αποθηκεύονται τα αρχεία , να γράφονται τα άρθρα ή να συντάσσονται οι αναφορές. Ο χρήστης ή κάποιος ειδικός, θα πρέπει να αφαιρέσει ή να θέσει εκτός λειτουργίας όλες τις συνδεδεμένες με το laptop συσκευές, για να εξασφαλισθεί η μη συνδεσιμότητά στο

διαδίκτυο ανά πάσα στιγμή, (δείτε το δεύτερο μέρος του κεφαλαίου). Ιδανικά, και τα δύο μηχανήματα, και το airgapped αλλά και το online μηχάνημα, θα πρέπει να ασφαλίζονται με IBM ThinkPad X60s.

Για παράδειγμα, ο Glenn Greenwald[7] *χρησιμοποιεί ένα airgapped laptop για να εργαστεί στα Έγγραφα Snowden.*Αυτό προσθέτει ένα επιπλέον επίπεδο ασφάλειας στα στοιχεία της πηγής /των πηγών κάποιου δημοσιογράφου, επειδή τα σημαντικά έγγραφά αποθηκεύονται όχι μόνο σε ένα ασφαλές μηχάνημα, αλλά σε ένα εξ ολοκλήρου offline μηχάνημα.

2. Παραμετροποίηση hardware

Ας δούμε τώρα όλα τα παραμετροποιήσιμα εσωτερικά μέρη απο τα οποία θα μπορούσε να αποτελείται το hardware:

- Webcam
- Μικρόφωνο
- Σκληρός δίσκος
- Κάρτα δικτύου - WiFi
- Κάρτα Bluetooth
- 3G modem
- Θύρα Ethernet

Κάμερα υπολογιστή:

Οι κάμερες που είτε είναι ενσωματωμένες στον Η/Υ είτε συνδέονται μέσω θύρας USB, όχι μόνο μπορούν απομακρυσμένα να ενεργοποιηθούν για συγκεκριμένους στόχους, αλλά έχει παρατηρηθεί και το φαινόμενο υποκλοπής εικόνων από webcam ως μέρος προγραμμάτων παρακολούθησης dragnet (dragnet surveillance programs - δείτε την αποκάλυψη Snowden από το πρόγραμμα GCHQ's OPTIC NERVE[8]). Μια απλή λύση είναι να τοποθετηθεί μια αυτοκόλλητη ταινία πάνω στην web κάμερά του υπολογιστή.

Μικρόφωνο:

Το μικρόφωνο του laptop μπορεί επίσης απομακρυσμένα να ενεργοποιηθεί και να παρακολουθεί συνομιλίες. Ένας τρόπος προστασίας είναι να τοποθετηθεί κόλλα στην εσοχή του μικροφώνου, για να σταματήσει τον ήχο. Ακόμη πιο αποτελεσματικό θα ήταν να κοπεί το καλώδιο του μικροφώνου.

Σκληρός δίσκος:

Έχει ανακαλυφθεί ότι μερικοί σκληροί δίσκοι περιέχουν «κακό» firmware – δηλαδή θα μπορούσαν ενδεχομένως να ενεργοποιηθούν για να θέσουν σε κίνδυνο την ασφάλειά

[7] https://en.wikipedia.org/wiki/Glenn_Greenwald
[8] http://www.commondreams.org/news/2015/06/01/victory-privacy-vindication-snowden-phone-dragnet-sunsets

κάποιου χρήστη, εάν γινόταν στόχος κακόβουλων χρηστών που είχαν στη διάθεση τους προηγμένα εργαλεία (toolkit).

Σε καταστάσεις υψηλού κινδύνου, ενδείκνυται να αφαιρείται η μονάδα σκληρού δίσκου και αντ' αυτού ο χρήστης να εργάζεται μέσω USB drives. Οι USB drives είναι επίσης ιδανικοί για αποθήκευση του ασφαλισμένου λειτουργικού συστήματος, του Tails (δείτε το κεφάλαιο 2), δηλαδή μπορούν να παρέχουν ένα μικρό, ανώνυμο σύστημα στο οποίο μπορεί κάποιος να εργάζεται. Τα USB sticks είναι φορητά, αντιγράψιμα, και μπορούν εύκολα να προστατευτούν με πολύ ισχυρή κρυπτογράφηση (δείτε το κεφάλαιο 4). Αυτό σημαίνει ότι, εάν ένα laptop κλαπεί ή καταστραφεί, τα δεδομένα που έχουν αποθηκευτεί στο USB σα θα παραμείνουν ασφαλή. Εντούτοις, μπορεί κάποιος αν το επιθυμεί να κρατήσει τη μονάδα σκληρού δίσκου για την καθημερινή του εργασία, και να εργάζεται από τους USB drives μόνο σε ειδικές περιπτώσεις.

Κάρτα Wi-Fi, Κάρτα Bluetooth, 3G modem:

Σε καταστάσεις υψηλού κινδύνου, οποιοδήποτε στοιχείο που επιτρέπει την συνδεσιμότητα του laptop μπορεί εν δυνάμει απομακρυσμένα να ενεργοποιηθεί και να εγκαταστήσει εργαλεία επιτήρησης, ή ακόμη και να στείλει πολύτιμα δεδομένα σε μη εξουσιοδοτημένους χρήστες. Επομένως, ο έλεγχος της συνδεσιμότητας ενός laptop είναι καίριο σημείο στην προστασία των χρηστών.

Ο καλύτερος τρόπος για να επιτευχθεί αυτό είναι να αφαιρεθούν φυσικά τα στοιχεία συνδεσιμότητας. Θα πρέπει να αφαιρεθεί το εξωτερικό περίβλημα του laptop, και να ξεβιδωθεί η κάρτα Wi-Fi, καθώς επίσης και η κάρτα Bluetooth και το 3G modem, εάν φυσικά το laptop τα διαθέτει (οι ενδιαφερόμενοι μπορούν να συμβουλευτούν το εγχειρίδιο του laptop εάν δεν είστε βέβαιοι – υπάρχουν επίσης αντίγραφα εγχειριδιών διαθέσιμα online). Η διαδικασία ίσως φανεί δύσκολη και αποθαρρυντική στην αρχή, αλλά καθένας με σταθερό χέρι και τις σωστές οδηγίες μπορεί να τα καταφέρει.

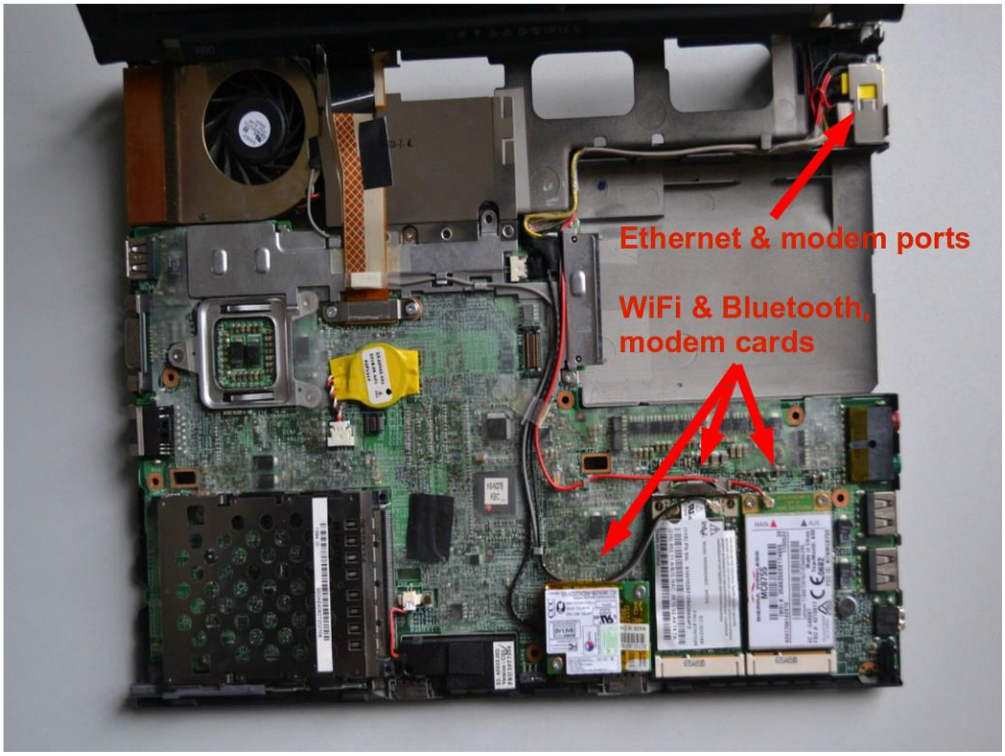
Θα μπορούσατε επίσης κάποιος να αγοράσει έναν αντάπτορα Wi-Fi USB, ο οποίος λειτουργεί με τον ίδιο τρόπο όπως και η κάρτα Wi-Fi –επιτρέπει την σύνδεση στο Διαδίκτυο. Η διαφορά έγκειται στο γεγονός ότι εύκολα μπορεί ο χρήστης να συνδέσει και να αποσυνδέσει τον USB αντάπτορα ανά πάσα στιγμή, κι έτσι ο ίδιος ο χρήστης αποφασίζει πότε θα είναι συνδεδεμένος στο διαδίκτυο και πότε όχι.

Θύρα Ethernet:

Η θύρα Ethernet χρησιμεύει για σύνδεση με φυσικό τρόπο (καλώδιο) σε ένα τοπικό δίκτυο LAN (Local Area Network). Φυσικά, το Wi-Fi χρησιμοποιείται κατά κόρον στην εποχή μας και είναι περισσότερο διαδεδομένο από τις συνδέσεις μέσω καλωδίων Ethernet.

Είναι επίσης γνωστό ότι οι θύρες Ethernet έχουν συγκεκριμένες ευπάθειες ασφαλείας τις οποίες μπορούν να εκμεταλλευθούν τυχόν κακόβουλοι χρήστες. Εάν ο στόχος είναι να

προφυλαχθεί το ένα μηχάνημα ενάντια στην εκμετάλλευση των ευπαθειών της θύρας Ethernet (π.χ. για ένα airgapped μηχάνημα), μπορείτε κάποιος να γεμίσει τη θύρα με κόλλα. Εναλλακτικά, μπορείτε να αποσυνδέσει τα καλώδια της θύρας στο εσωτερικό του laptop.



3. Ανώνυμη αγορά laptop

Μια σοφή απόφαση για τους χρήστες, οι οποίοι συνεργάζονται με πηγές υψηλού κινδύνου ή εργάζονται πάνω σε πολύ ευαίσθητα project είναι η αγορά ενός ή δύο καινούριων laptops. Ωστόσο, δεν πρέπει κανείς να ξεχνάει τους βασικούς κανόνες ασφάλειας πληροφοριακών συστημάτων, οι οποίοι αναλύονται στο παρόν κείμενο. Η διαδικασία της αγοράς ασφαλών laptops πρέπει να είναι όσο το δυνατόν περισσότερο ανώνυμη σε καταστάσεις υψηλού κινδύνου, έτσι ώστε να:

α) αποτραπούν οι εκάστοτε κακόβουλοι χρήστες απο το να προσπαθήσουν να τοποθετήσουν από πριν πιθανά εργαλεία επιτήρησης στο hardware,

β) μη γνωρίζει κανείς στοιχεία για το νέο hardware και

γ) φυσικά κατ' αυτόν τον τρόπο να αποτραπεί η εισβολή στον υπολογιστή μετά την αγορά.

Τα παραπάνω ενισχύονται σαν πιθανότητες αν οι χρήστες συνεργάζονται με πηγές υψηλού κινδύνου (πχ. intelligence whistleblower), οι οποίες ενδέχεται να βρίσκονται ήδη υπό παρακολούθηση.

Τα έγγραφα Snowden αποκάλυψαν[9] ότι οι Υπηρεσίες Πληροφοριών παρακολουθούν συσκευές εμφυτεύοντας εργαλεία παρακολούθησης στο στάδιο προτού το μηχάνημα σφραγιστεί από το εργοστάσιο, και έπειτα διατίθεται στο εμπόριο – έτσι θα πρέπει να αποφεύγεται η αγορά οποιουδήποτε hardware (ακόμη και φορτιστές) online. Τα περισσότερα μέρη του hardware μπορούν να τροποποιηθούν με τέτοιο τρόπο ώστε να λειτουργούν ως εργαλεία παρακολούθησης.

Συνεπώς, πριν απο οποιαδήποτε αγορά θα πρέπει να έχει πραγματοποιηθεί έρευνα αγοράς χρησιμοποιώντας τον ανώνυμο browser Tor (εκτενέστερη αναφορά στο κεφάλαιο 3). Για μεγαλύτερη ασφάλεια συνίσταται η αγορά με μετρητά και η προτίμηση περιοχής μακριά απο την περιοχή που θα ψώνιζε κάποιος υπο κανονικές συνθήκες. Σε καταστάσεις υψηλότερου κινδύνου, συνιστάται η αγορά κάθε εξαρτήματος του laptop ξεχωριστά απο αρκετά διαφορετικά καταστήματα. Παράλληλα ενώ πραγματοποιούνται οι αγορές, καλό θα ήταν οποιαδήποτε συσκευή που θα μπορούσε να χρησιμοποιηθεί για τον εντοπισμό (δηλ. ένα τηλέφωνό) να μπει μέσα σε ένα κουτί Faraday (μεταλλική συσκευή που αποτρέπει τη μετάδοση του σήματος) ή απλώς να μείνει σε ένα ασφαλές μέρος στο σπίτι.

4. **Επιτήρηση laptop**

Για να αποτραπεί η κλοπή, η ζημιά (σκόπιμη ή μη), και οι φυσικές επιθέσεις σε ενα hardware, ειδικά εάν πρόκειται για κίνδυνο στοχευμένης παρακολούθησης, θα πρέπει να υιοθετηθεί μια νέα σημαντική συμπεριφορά: θα πρέπει ο χρήστης να έχει οπτική επαφή με tolaptop ανά πάσα στιγμή. Η υιοθέτηση τέτοιας συμπεριφοράς αποκαλείται μερικές φορές «OpSec», ή «Λειτουργική ασφάλεια».

Εάν κάποια στιγμή ένα laptop μείνει αφύλακτο (για παράδειγμα, στο σπίτι, σε ένα café, ή στο γραφείο) ή βρίσκεται στην κατοχή τρίτου προσώπου (για παράδειγμα, όταν στην πείπτωση check-in πριν από μια πτήση, το laptop μπορεί να βρίσκεται στην κατοχή της αστυνομίας ή των αρχών του αεροδρομίου), θα πρέπει να εξεταστεί το ενδεχόμενο, ανάλογα με το επίπεδο κινδύνου, το σύστημά να μην είναι πλέον ασφαλές.

το ασφαλισμένο σύστημά πρέπει να παραμείνει όσο πιο απλό, μικρό, και ελαφρύ γίνεται καθώς και να αποφευχθεί η σύνδεση ποντικιού ή πληκτρολογίου, ή εκτυπωτή, ή docking station, ή άλλων συσκευών (που, για τους στόχους υψηλού κινδύνου, θα μπορούσαν πιθανότατα να «παρακολουθούνται») με το laptop . Με αυτό τον τρόπο περιορίζεται το hardware που πρέπει να μεταφερθεί μαζί με το laptop.

Σε κάθε περίπτωση η φυσική ασφάλεια του hardware θα πρέπει να εξετάζεται ανά τακτά χρονικά διαστήματα όχι μόνο προς το παρόν και το μέλλον, αλλά και αναδρομικά. Θα μπορούσε να έχει δεχθεί φυσική επίθεση στο παρελθόν; Πώς κατασκευάσθηκε; Θα μπορούσε το hardware να έχει ήδη εκτεθεί σε κίνδυνο;

[9] http://www.bbc.com/news/world-us-canada-23123964

5. Μέτρα ανιχνευσιμότητας (Detectability measures)

Η ανίχνευση των πιθανών φυσικών επεμβάσεων σε ένα laptop είναι εξαιρετικά δύσκολη. Εάν πρέπει να αποθηκευτεί ασφαλώς ένα laptop για κάποιο λόγο (για παράδειγμα, σε περίπτωση ταξιδιου χωρίς αυτό) πρέπει να γίνει με τέτοιο τρόπο ώστε οποιαδήποτε παραβίαση ασφαλείας να μπορέσει να ανιχνευθεί από τον ιδιοκτήτη. Φυσικά πέρα απο ευφάνταστες λύσεις, το ιδανικότερο θα ήταν να παραμείνει με ένα πρόσωπο εμπιστοσύνης. Ως μέσο άμυνας και μέτρο ασφάλειας σε καταστάσεις χαμηλού επιπέδου κινδύνου, μπορεί να χρησιμοποιηθεί μια open source εφαρμογή που ονομάζεται Prey[10]. Είναι ένα software που βοηθά τους χρήστες να βρούν, να κλειδώσουν και να ανακτήσουν τους υπολογιστές τους. Επιτρέπει επίσης τα screenshots (στιγμιότυπα οθόνης) της κλεμμένης οθόνης του laptop, και να ενεργοποιηθεί η webcam ώστε να ταήτυτοποιηθεί ο καινούριος ιδιοκτήτης του. Δεδομένου ότι η εφαρμογή αυτή είναι open source είναι πολύ πιθανό να είναι αρκετά αξιόπιστη. Παρόλο αυτά, ένας εξειδικευμένος εισβολέας δεν θα «πιαστεί σε αυτήν την παγίδα» τόσο εύκολα. Συνιστάται να χρησιμοποιείται αυτή η εφαρμογή μόνο σε περίπτωση άμυνας απέναντι σε λιγότερο προηγμένους χρήστες.

Σε κάθε περίπτωση πρέπει να όλοι οι χρήστες να είναι ενήμεροι, πως άπαξ και αποτελέσουν στόχο παρακολούθησης κάποιου που έχει στην διάθεσή του τους πόρους, την ικανότητα και το κίνητρο να αποκτήσει τα δεδομένα τους, κατά πάσα πιθανότητα βρίσκονται προ τετελεσμένου γεγονότος.

[10] https://preyproject.com

Κεφάλαιο 2: Λειτουργικό σύστημα

Ας υποθέσουμε οτι έχει πλέον καταστήσει ένας χρήστης ασφαλές το hardware του, είναι εξίσου ζωτικής σημασίας να αποτρέψει την εισαγωγή του software που μπορεί να καταστήσει το σύστημά του ευπαθές. Η χρήση του σωστού λογισμικού, ακόμα κι αν πρόκειται για δραστηριότητες σε επίπεδα χαμηλής επικινδυνότητας μπορεί να βοηθήσει στην διασφάλιση των δεδομένων και των επικοινωνιών από μια αυτοματοποιημένη παρακολούθηση.

Το σημαντικότερο software σε έναν υπολογιστή είναι το λειτουργικό του σύστημα. Πρόκειται για το λογισμικό που παίρνει τον έλεγχο του υπολογιστή καθώς ενεργοποιείται και είναι η διεπαφή μέσω της οποίας ο χρήστης χρησιμοποιεί τον υπολογιστή. Εν ολίγοις, το λειτουργικό σύστημα λέει στον υπολογιστή τι να κάνει, και πώς να το κάνει. Τα δημοφιλέστερα λειτουργικά συστήματα είναι οι εκδόσεις των Windows (π.χ. XP, Vista, 7, 8, 10), τα OS X της Apple για Mac και τα Linux.

Ξέρουμε πλέον ότι οι υπηρεσίες πληροφοριών έχουν πρόσβαση «στα backdoors» των δημοφιλών λειτουργικών συστημάτων, τα οποία τους επιτρέπουν να αποκτήσουν πρόσβαση στα στοιχεία των χρηστών.

Απειλές που σχετίζονται με τα λειτουργικά συστήματα:

- Κακόβουλα λογισμικά, ιοί
- Παρακολούθηση «backdoors» μέσα σε ένα λειτουργικό σύστημα, που είναι προσιτό σε τρίτους

Δύο είναι τα βασικά μέτρα που είναι σημαντικά για την προστασία ενάντια σε απειλές που σχετίζονται με τα λειτουργικά συστήματα:

- Η χρήση open source λειτουργικού συστήματος (για καταστάσεις μέσου κινδύνου).
- Η χρήση του Tails, ένα λειτουργικό σύστημα το οποίο έχει δημιουργηθεί με γνώμονα τη διασφάληση της ανωνυμίας και της ιδιωτικότητας (για καταστάσεις υψηλού – πολύ υψηλού κινδύνου).

Για να βεβαιωθεί κάποιος ότι το λειτουργικό του σύστημα πιθανώς δεν παρακολουθείται θα πρέπει αυτό να είναι «ανοικτού πηγαίου κώδικα». Τα λογισμικά ανοικτού πηγαίου κώδικα διανέμονται ελεύθερα, και ο πηγαίος κώδικάς τους, ο σκελετός του λειτουργικού συστήματος, είναι δημοσίως διαθέσιμος. Αυτό επιτρέπει στους

ανεξάρτητους εμπειρογνώμονες να έχουν πρόσβαση στον πηγαίο κώδικα ανά πάσα στιγμή, και να ελέγξουν αν υπάρχει κάποιο κενό ασφαλείας στο λειτουργικό σύστημα[11].

Επιπλέον, τα λειτουργικά συστήματα ανοικτού πηγαίου κώδικα είναι λιγότερο ευαίσθητα σε κακόβουλα λογισμικά (malware, spyware) και ιούς. Αυτό συμβαίνει επειδή χρησιμοποιούνται πολύ λιγότερο από τα ιδιόκτητα λειτουργικά συστήματα και έχουν αντίστοιχα χαμηλό μερίδιο αγοράς.

Το λογισμικό ανοιχτού κώδικα είναι επίσης γνωστό ως «ελεύθερο λογισμικό» – όχι μόνο για την ελευθερία της πρόσβασης στον πηγαίο κώδικά του, αλλά επίσης επειδή διανέμεται σε μια ελεύθερη βάση.

Πρέπει να σημειωθεί ότι το λογισμικό ανοιχτού κώδικα είναι αξιόπιστο μόνο εάν εξετάζεται από ειδικό αρκετά συχνά ο πηγαίος κώδικας για τυχόν κενά ασφαλείας. Παρόλο αυτά, το ανοικτό λογισμικό που χρησιμοποιείται ευρέως είναι πιθανότερο να εξετάζεται αρκετά συχνά, και να προτιμάται (τουλάχιστον για λόγους ασφάλειας) από τα λογισμικά κλειστού πηγαίου κώδικα.

Τα λειτουργικά συστήματα της Microsoft και της Apple (όπως π.χ τα Windows, και τα OS X) είναι κλειστού πηγαίου κώδικα (closed source), και για αυτό μπορεί να περιέχουν backdoors επιτήρησης που είναι προσιτά σε μυστικές υπηρεσίες και μεγάλες εταιρείες. Τα λειτουργικά συστήματα της Microsoft είναι ιδιαίτερα ακατάλληλα, για σημαντικά δεδομένα και επικοινωνίες, εάν λάβει κανείς υπόψη του ότι κάποιος που επικοινωνεί μαζί του θα μπορούσε να είναι (ή να γίνει) στόχος παρακολούθησης.

Θα πρέπει εδώ να σημειωθεί οτι τα κλειστού τύπου mobile λειτουργικά συστήματα, όπως το iOS και το Android, είναι πανταχού παρόντα στα smart phones, τα οποία είναι επομένως απροστάτευτα ενάντια σε στοχευμένες επιθέσεις – δείτε το κεφάλαιο 7 για την ασφάλεια πληροφοριακών συστημάτων στο κινητό δίκτυο.

Linux

Το Linux αποτελεί την επιτομή των λειτουργικών συστημάτων ανοικτού κώδικα. Υπάρχουν πολλές διαφορετικές εκδόσεις του λειτουργικού Linux που μπορεί να χρησιμοποιηθεί.

Ubuntu-Linux

Ubuntu.com

Το Ubuntu είναι το πιο ευρέως διαδεδομένο και αυτό που χρησιμοποιείται κατά κόρον από όλες τις εκδόσεις του λειτουργικού συστήματος Linux. Είναι εύκολο να εγκατασταθεί, ιδιαίτερα λειτουργικό, και φιλικό προς το χρήστη.

[11] Ένας πλήρης οδηγός δέκα σημείων είναι διαθέσιμος στο: **www.opensource.org/osd**

Μπορείτε να αντικαταστήσετε Τα Windows μπορούν να αντικατασταθούν με Ubuntu, ή μπορούν να τρέχουν και τα δύο στο ίδιο laptop (μια πρακτική που βοηθά τους νέους χρήστες να εξοικειωθούν πρώτα με το Ubuntu προτού το υιοθετήσουν). Το Ubuntu είναι πολύ φιλικό προς το χρήστη και δεν διαφέρει πολύ από άλλα λειτουργικά συστήματα, έτσι συνήθως συστήνεται ως πρώτη επιλογή για σκοπούς ασφάλειας (ειδάλλως, τα πιθανά «backdoors» ίσως παραμείνουν). Ωστόσο επειδή η αφαίρεση του παλαιού λειτουργικού συστήματος θα αφαιρέσει επίσης και όλα τα αρχεία που συνδέονται με αυτό θα πρέπει προτού γίνει κάτι τέτοιο να διασφαλιστεί η αποθήκευση σε ασφαλές μέρος των αρχείων που είναι ακόμα χρήσιμα. Δεν συνιστάται οι άπειροι χρήστες να αφαιρούν από ένα MacBook το ήδη εγκατεστημένο λειτουργικό σύστημά του προκειμένου να εγκαταστήσουν το Ubuntu, αφού κάτι τέτοιο θα μπορούσε να προκαλέσει προβλήματα με τη λειτουργία του υπολογιστή. Επίσης, θα μπορούσε να διερευνηθεί η δυνατότητα χρήσης του Ubuntu μέσω ενός 'virtual machine', αλλά είναι ακόμα ασαφές ποια είναι τα πλεονεκτήματα ασφάλειας που μπορούν να επιτευχθούν τρέχοντας ταυτόχρονα τα δύο λειτουργικά συστήματα.

Πρέπει να σημειωθεί ότι μερικά στοιχεία του Ubuntu είναι προς το παρόν κλειστού τύπου – υποτίθεται ότι αυτά δεν θέτουν σε απειλή το σύστημα. Εντούτοις, άλλες δημοφιλείς παραλλαγές του Linux, συμπεριλαμβανομένων των Debian και Trisquel, είναι εξ ολοκλήρου ανοικτού πηγαίου κώδικα. Να σημειωθεί ότι αυτά μπορεί να είναι λιγότερο φιλικά προς το χρήστη, ειδικότερα για νέους χρήστες των Linux.

Tails-Linux

tails.boum.org

Το Tails[12] αποτελεί ένα λειτουργικό σύστημα το οποίο έχει δημιουργηθεί με γνώμονα τη διασφάλιση της ανωνυμίας και της ιδιωτικότητας, 'The Amnesic Incognito Live System'. Είναι ανοικτού πηγαίου κώδικα, βασισμένο σε Linux, και προστατεύει την ιδιωτικότητα και την ανωνυμία των χρηστών.

Amnesic: χαρακτηρίζεται έτσι επειδή κανένα ίχνος χρήσης του υπολογιστή δεν παραμένει στο σύστημα μετά από την απενεργοποίηση του.

Incognito: επειδή είναι προσανατολισμένο στην μυστικότητα και την ασφάλεια, η πρόσβαση στο Διαδίκτυο γίνεται ανώνυμα από προεπιλογή, και παρακάμπτει έτσι οποιοδήποτε είδος λογοκρισίας.

Το Tails έχει σχεδιαστεί σκόπιμα ως σύστημα αντι-παρακολούθησης, και συνοδεύεται από διάφορες ενσωματωμένες (εξ ολοκλήρου ανοικτού κώδικα) προσανατολισμένες στην ασφάλεια εφαρμογές:

[12] https://tails.boum.org/

- *Ενσωματωμένη online ανωνυμία*

Ο ενσωματωμένος web browser, Iceweasel, χρησιμοποιεί ανώνυμη τεχνολογία web browsing όπως το Tor (δείτε το κεφάλαιο 3). Ο browser περιλαμβάνει επίσης δημοφιλείς επεκτάσεις ασφάλειας, όπως την κρυπτογράφηση HTTP και HTTPS, παντού και κρυπτογραφεί τα στοιχεία του browser, το Adblock Plus για να μπλοκάρει τις διαφημίσεις, και το NoScript για να μπλοκάρει Java και Flash (τα οποία θα μπορούσαν να θέσουν σε κίνδυνο την ανωνυμία κάποιου χρήστη). Αυτό σημαίνει ότι μερικά χαρακτηριστικά γνωρίσματα του Διαδικτύου δεν θα λειτουργούν όταν χρησιμοποιείται το Tails, αλλά αυτό είναι ένας σημαντικός συμβιβασμός που πρέπει να γίνει προκειμένου να είναι εφικτό ένα ικανοποιητικό επίπεδο μυστικότητας κατά την εργασία σε ευαίσθητα projects.

Σε αυτό το σημείο θα πρέπει να διευκρινιστεί οτι εάν κάποιος προσπαθήσει να συνδεθεί σε έναν online λογαριασμό που συνδέεται άμεσα με την πραγματική του ταυτότητα, θα θέσει σε κίνδυνο την ανωνυμία του και ολόκληρο το σύστημά του. Γι'αυτό πρέπει κάθε φορά που χρησιμοποιείται μια νέα ταυτότητα να απενεργοποιείται και να ξεκινάει εκ νέου το Tails. Τα αρχεία και τα έγγραφα μπορούν επίσης να περιέχουν metadata που ίσως προδώσουν την τοποθεσία κάποιου μέσω GPS.

- *Ενσωματωμένα κρυπτογραφημένα email και chat*

Το Tails προσφέρει ενσωματωμένο κρυπτογραφημένο email και συνομιλίες μέσω chat. Το Tails περιλαμβάνει το Claws email client με OpenPGP για κρυπτογράφηση email (δείτε το κεφάλαιο 5) και instant messaging client Pidgin (δείτε το κεφάλαιο 6) το οποίο διασφαλίζει την ιδιωτικότητα και την ανωνυμία των προσωπικών μηνυμάτων.

- *Ενσωματωμένη κρυπτογράφηση αρχείων*

Το λειτουργικό σύστημα Tails συνοδεύεται απο την υπηρεσία LUKS, η οποία μπορεί να κρυπτογραφήσει αρχεία μέσω του USB stick που χρησιμοποιείται για να τρέχει το ίδιο το Tails,. Το Tails θα κρυπτογραφήσει το χώρο αυτό από προεπιλογή, ζητώντας τον κωδικό πρόσβασής για τα αρχεία που αποθηκεύονται εκεί.

Ειδικές πληροφορίες: Ενώ ο μόνιμος αυτός χώρος αποθήκευσης είναι χρήσιμος για σχετικά ασήμαντες πληροφορίες και έγγραφα, δεν θα πρέπει να χρησιμοποιείται για να αποθηκεύονται ή να μεταφέρονται εκεί πιο ευαίσθητα έγγραφα ή δεδομένα. Και αυτό γιατί ο χώρος αυτός δεν είναι «κρυμμένος». Δηλαδή, εάν ο εκάστοτε κακόβουλος χρήστης πάρει το USB stick, θα είναι σε θέση να δει ότι υπάρχει ένας κρυπτογραφημένος όγκος δεδομένων στη συσκευή, και κατά συνέπεια ενδέχεται να καταφέρει να αποσπάσει τον κωδικό. Συνεπώς πρέπει να δημιουργηθεί ένας «κρυμμένος» χώρος για τα πιο ευαίσθητα έγγραφά (ίσως σε ένα διαφορετικό USB stick), που ίσως να φαίνεται ότι δεν έχει καθόλου

μνήμη – και μόνο ο ιδιοκτήτης να γνωρίζει ότι βρίσκονται εκεί. Αυτό μπορεί να γίνει εύκολα με μια εφαρμογή που ονομάζεται TrueCrypt, η οποία θα αναλυθεί στο κεφάλαιο 4.

- *Ενσωματωμένη προστασία κωδικών*

Το Tails έχει προεγκατεστημένο το KeePassX, ένα πρόγραμμα διαχείρισης κωδικών πρόσβασης, το οποίο αποθηκεύει credentials σε κρυπτογραφημένη μορφή σε βάση δεδομένων, προστατευμένη από έναν κύριο κωδικό πρόσβασης. Έχει επίσης εγκατεστημένο το PWGen, έναν αρκετά αποτελεσματικό γεννήτορα κωδικών πρόσβασης (random password generator).

Το Tails έχει σχεδιαστεί να χρησιμοποιείται από ένα USB stick ανεξάρτητα από το αρχικό λειτουργικό σύστημα του υπολογιστή. Αυτό σημαίνει ότι είναι δυνατό ακόμα κι αν έχει αφαιρεθεί ο σκληρός δίσκος ενός laptop εκκινηθεί το laptop μέσω ενός Tails USB stick.

Εναλλακτικά εαν τοποθετηθεί ένα Tails USB stick σε έναν υπολογιστή με άθικτο σκληρό δίσκο και επανεκκινηθεί με Tails, το μηχάνημα θα αγνοήσει τον σκληρό δίσκο καθώς και το λειτουργικό του σύστημα, και αντ' αυτού θα τρέξει από το USB drive στον οποίο είναι εγκατεστήμενα τα Tails.

Η παροχή ενός «μίνι συστήματος» σε ένα USB stick με Tails το καθιστά ιδανικό για όσους διαχειρίζονται ευαίσθητα δεδομένα. Το εκάστοτε σύστημα μπορεί ουσιαστικά να απαλλαγεί από κάθε ίχνος ενεργειών, και τα έγγραφά μπορούν να αποθηκευτούν σε ένα φορητό USB stick. Το Tails διατίθεται και με προεγκατεστημένο ανοικτό λογισμικό επεξεργασίας, όπως για παράδειγμα το OpenOffice για τη δημιουργία, ανάγνωση, και επεξεργασία εγγράφων, το Gimp για την επεξεργασία εικόνων, και το Audacity για την επεξεργασία ήχου.

Το USB stick είναι ιδανικό για ταξίδια, και μπορεί να συνδεθεί σε οποιονδήποτε υπολογιστή. Ενδείκνυται ο διαχωρισμός των USB sticks με το Tails για διαφορετικά projects, για να μη μπορέσουν να ανιχνευθούν τα ίχνη κάποιου και να ελαχιστοποιηθεί το ρίσκο σε περίπτωση που χαθεί ένα USB stick. Εάν κριθεί απαραίτητο, μια καλή τακτική θα ήταν να επικοινωνεί ο ενδιαφερόμενος χρήστης με την πηγή των πληροφοριών του μέσω ενός USB stick με Tails

Η χρήση του Ubuntu είναι μια καλή επιλογή για καθημερινή χρήση . Παρόλο αυτά, η δημιουργία ενός USB stick με Tails για να χρησιμοποιείται σε περιπτώσεις επεξεργασίας ευαίσθητων δεδομένων και σημαντικών εγγράφων η ακόμα και σε περιπτώσεις επικοινωνίας με άτομα υψηλού κινδύνου. Επιπλέον, η λήψη ισχυρών μέτρων ασφάλειας πληροφοριακών συστημάτων μπορεί να παρατείνει τη διατήρηση της ανωνυμίαςκάποιου, και το πιο σημαντικό την ανωνυμία της πηγής του, προτού να γίνουν το επίκεντρο μιας στοχευμένης παρακολούθησης.

Μέχρι στιγμής έχουμε αναλύσει τους τρόπους προστασίας ενός συστήματος. Στη συνέχεια θα προχωρήσουμε με την προστασία των επικοινωνιών και την διατήρηση της ανωνυμίας των δεδομένων ενός browser αλλά και του τρόπου κρυπτογράφησης και αποστολής ευαίσθητων εγγράφων.

Οδηγίες εγκατάστασης βήμα προς βήμα

Ubuntu

Πριν αναλύσουμε τις οδηγίες εγκατάστασης του Ubuntu, θα πρέπει να σημειωθεί οτι όλα τα έγγραφά, τα προγράμματα, τα αρχεία κ.λπ. που είχαν αποθηκευτεί στα Windows θα διαγραφούν εάν αντικατασταθούν με Ubuntu. Ωστόσο, αυτό συστήνεται ανεπιφύλακτα για λόγους ασφάλειας.

1. Μεταφόρτωση του Ubuntu

Προκειμένου να μεταφορτωθεί το Ubuntu[13], θα πρέπει ο κάθε ενδιαφερόμενος να γνωρίζει πόση μνήμη RAM έχει το laptop του, και να μεταφορτώσει είτε την έκδοση των 32-bit (συνιστάται για παλαιότερα μηχανήματα, όπως το ThinkPads, με 2GB ή λιγότερη RAM) είτε την έκδοση των 64-bit (συνιστάται για νεότερα μηχανήματα με μνήμη RAM 4GB ή περισσότερο). Η διάρκεια μεταφόρτωσης (download) ενδέχεται να ποικίλει.

2. Μεταφόρτωση του Linux's USB Installer

Προκειμένου να μεταφορτωθεί ο USB installer, ο οποίος θα επιτρέψει να αποθηκευτεί το Ubuntu στο USB drive, το οποίο στη συνέχεια θα χρησιμοποιηθεί για να εγκατασταθεί το Ubuntu, πρέπει να επισκεφθούμε την σχετική[14] ιστοσελίδα, και να κάνουμε κλικ στο 'Download Pen Drive Linux's USB Installer ›', και στο τέλος της σελίδας στην επιλογή 'Download UUI'.

Σε αυτό το σημείο, θα πρέπει να αναφερθεί οτι κατά τη διάρκεια της εγκατάστασης, ο σκληρός δίσκος δεν μπορεί να τρέξει οποιοδήποτε άλλο λογισμικό – έτσι είναι απαραίτητη μια άλλη πηγή, σε αυτήν την περίπτωση ένα USB stick, για να τρέξει το εγκατεστημένο λογισμικό.

3. Τοποθέτηση του Ubuntu στο USB Installer

Όταν ολοκληρωθούν και οι δύο μεταφορτώσεις, θα πρέπει να εισαχθεί ένα άδειο και καθαρό USB stick ώστε να ανοίξει ο USB Installer. Κατόπιν πρέπει να γίνει:

[13] http://www.ubuntu.com/download/desktop
[14] http://www.ubuntu.com/download/desktop/create-a-usbstick-on-windows

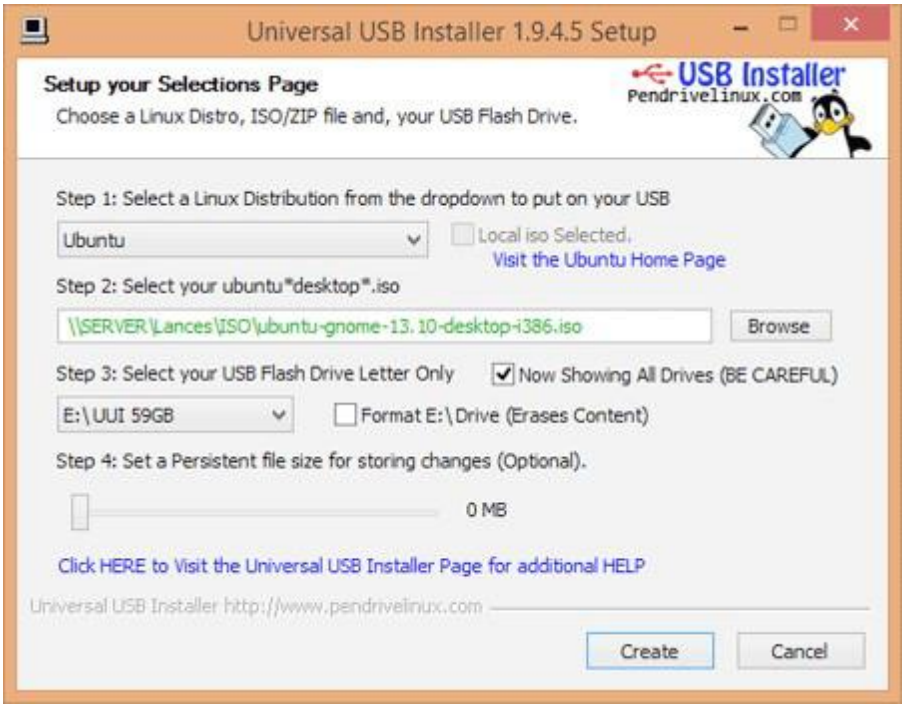
α) επιλογή του Linux Distribution από το μενού (Ubuntu)

β) χρήση του πλήκτρου αναζήτησης για να επιλεχθεί το σημείο που θέλουμε να εγκατασταθεί το Ubuntu

γ) επιλογή του USB Flash Drive (όπου έχει τοποθετήσει αυτόματα ο υπολογιστής το USB stick). Τέλος,

δ) κάνουμε κλικ στο κουμπί 'Δημιουργία'

το, χρησιμοποιήστε το, και επιλέξτε το USB Flash Drive (όπου έχει τοποθετήσει αυτόματα ο υπολογιστής σας το USB stick). Έπειτα κάνετε κλικ.



Όταν ολοκληρωθεί αυτή η διαδικασία, αφαιρούμε με ασφάλεια το USB stick, και απενεργοποιούμε τον υπολογιστή μας.

4. Εγκατάσταση του Ubuntu

<u>Εκκίνηση από USB</u>

Προκειμένου να επανακκινηθεί ένα μηχάνημα απο USB, θα πρέπει να γίνει μια συγκεκριμένη ρύθμιση στο μενού BIOS του laptop, στο οποίο αποκτά κανείς πρόσβαση κατα την εκκίνηση του μηχανήματός του. Ωστόσο, προτού προβούμε σε μια τέτοια ενάργεια, καλό ειναι να αναζητήσουμε online μερικές πληροφορίες σχετικά με τους ειδικούς τρόπους χρήσης του. Σε πολλά μηχανήματα εμφανίζεται ένα setup message όταν γίνεται η επανεκκίνηση, που σας πληροφορεί ότι μπορείτε να πιέσετε το [τάδε] κουμπί για να εισέλθουμε στο BIOS/setup/system configuration. Συνήθως πρόκειται για τα βοηθητικά κουμπιά, όπως το F1, F2, F3, F12 ή το DEL.

. Επιπλέον για την επανεκκίνηση του μηχανήματος απο το USB drive, πρέπει να γίνει εισαγωγή του USB stick στο laptop όσο είναι κλειστό, κι έπειτα να γίνει εκκίνηση και να μεταφερθούμε στο μενού BIOS. Αυτή η ρύθμιση ίσως βρίσκεται στο υπομενού Startup > Boot, ή σε κάποιο tab του μενού όπως για παράδειγμα 'Boot', 'Boot options', ή 'Boot selection menu'.
Στη συνέχεια, πρέπει να γίνει επιλογή του ή να διασφαλίσουμε οτι USB drive, το USB drive είναι στο βασικό μενού η σε κάποιο υπομενού. Η σειρά μπορεί να αλλαχθεί χρησιμοποιώντας τα πλήκτρα + και – για να δοθείπροτεραιότητα ή να απορριφθείκάποια επιλογή. Τέλος, για να σιγουρευτούμε οτι οι προτιμήσεις μας έχουν αποθηκευτεί, πρέπει να επιλέξουμε την επιλογή "Εξοδος/Αποθήκευση αλλαγών' (ή κάποια παρόμοια).
Αφού έχουν πραγματοποιηθεί οι παραπάνω ενέργειες, το μηχάνημα θα κάνει επανεκκίνηση από το USB και επιπλέον θα φορτώσει το Ubuntu installer boot menu. Απο εκεί επιλέγουμε το κουμπί 'Εγκατάσταση Ubuntu στον σκληρό δίσκο' και ο οδηγός αυτόματης εγκατάστασης θα μας οδηγήσει βήμα βήμα για την εγκατάσταση του Ubuntu.
Ίσως χρειασθεί να εγκατασταθεί και το WiFi, αλλά προς το παρόν δεν υπάρχει λόγος ανησυχίας, ειδικά εάν έχει αφαιρεθεί η κάρτα Wi-Fi.

Κάτω από το 'Installation type' πρέπει να πραγματοποιηθούν οι ακόλουθες ενέργειες:

 Επιλογή: Replace Windows with Ubuntu (για να αλλάξουμε τα Windows).

 Επιλογή: Encrypt the new Ubuntu installation for security.

 Επιλογή: Use LVM with the new Ubuntu installation.

Επιλογή ισχυρού κωδικού πρόσβασης και στην συνέχεια επιλογή του 'require my password to log in' και της οδηγίας 'encrypt my home folder' (το κεφάλαιο 8 περέχει τις απαραίτητες οδηγίες).

Στη συνέχεια πρέπει ο χρήστης να διαλέξει ένα όνομα για τον υπολογιστή του και ένα username για να συνδέεται. Το Ubuntu τώρα θα ολοκληρώσει την εγκατάσταση. Εφόσον εγκατασταθεί, απενεργοποιούμε το laptop και αφαιρούμε το USB. Όταν εκκινήσουμε το laptop εκ νέου θα πρέπει να εμφανισθεί το Ubuntu.

Όταν συνδεθούμε στο διαδίκτυο, επιλέγουμε το εικονίδιο που βρίσκεται στην πάνω αριστερή γωνία της επιφάνειας εργασίας σας και κάνουμε αναζήτηση για ενημερώσεις λογισμικού (updates) κάνοντας κλικ στο 'accept any updates'.

Ρυθμίσεις ιδιωτικότητας Ubuntu

 Επιλογή 'System Settings' στην επιφάνεια εργασίας και έπειτα > Security and Privacy.

 Κάτω από το 'Files and Applications' μπορεί να γίνει επιλογή να αποθηκεύονται οι εγγραφές από τα αρχεία ή τις εφαρμογές που χρησιμοποιεί ο χρήστης.

 Κάτω από το 'Search' μπορεί να απενεργοποιηθεί η online αναζήτηση αποτελεσμάτων όταν πραγματοποιείται αναζήτηση στο Dash. Αυτό θα αποτρέψει την επικοινωνία μεταξύ της Amazon, του Ubuntu και του Dash, κι έτσι οι αναζητήσεις δε θα μπορούν να αποστέλλονται πίσω στους servers του Ubuntu και της Amazon. Επίσης το εικονίδιο Amazon μπορεί να αφαιρεθεί από την επιφάνεια εργασίας κάνοντας δεξί κλικ στο εικονόδιο και επιλέγοντας 'Unlock from Launcher'. Κάτω από το 'Diagnostics' μπορείτε να γίνει επιλογή της αποστολής 'error reports' και 'occasional system information' σε canonical.

Tails

Υπάρχουν τρεις τρόποι με τους οποίους συνιστάται να γίνει η εγκατάσταση του Tails:

1. Μέσω ενός προεγκατεστημένου/κλωνοποιημένου Tails USB stick από μια έμπιστη πηγή (το οποίο επιτρέπει να δημιουργηθεί persistent volume).
2. Χειροκίνητα μέσω του UNetbootin (το οποίο δεν επιτρέπει να δημιουργηθεί persistent volume στο USB stick – παρόλο που μπορούμε να δημιουργήσουμε persistent volumes στο Tails sticks από τα οποία κλωνοποιούμε).
3. Χειροκίνητα μέσω του Linux συστήματός (το οποίο επίσης σας επιτρέπει να δημιουργηθεί persistent volume στο USB stick).

 Όταν αποκτήσουμε το Tails USB stick, θα πρέπει να ρυθμίσουμε το μηχάνημά έτσι ώστε να πραγματοποιεί εκκίνηση από το USB όταν θα θέλουμε να χρησιμοποιήσουμε το Tails. Δείτε τον πίνακα «εκκίνηση από USB» στη σελίδα 23.

Συνιστάται να χρησιμοποιείται το Tails μέσω ενός προεγκατεστημένου/κλώνου USB stick. Η χειροκίνητη εγκατάσταση δεν είναι πολύ εύκολη, και για αυτό δεν έχει μεγάλα ποσοστά επιτυχίας.

Αναλόγως του project που έχει αναλάβει ο εκάστοτε χρήστης, ίσως χρειασθεί να εγκατασταθεί το Tails με έναν τρόπο ούτως ώστε να δημιουργηθεί persistent volume (ως εκ τούτου θα υπάρχει εύκολη πρόσβαση στο email, την επικοινωνία μέσω instant messaging, καθώς και στα έγγραφά κάθε φορά που χρησιμοποιείται η εφαρμογή).

Για την ασφάλειά του, θα πρέπει να βεβαιωθεί ότι χρησιμοποιεί την τελευταία έκδοση του Tails, γι'αυτό θα πρέπει να αναβαθμίζονται οι εκδόσεις . το συντομότερο δυνατό μέσω της επιλογής 'Updating Tails'.

Για να εγκατασταθεί η εφαρμογή Tails απο ένα σύστημα Ubuntu[15] θα χρειαστούμε:ένα άδειο USB stick (εξηγείται παρακάτω) χωρητικότητας 4GB και άνω (ιδανικά 16GB εάν σκοπεύουμε να αποθηκεύουμεκαι έγγραφα-δεδομένα μέσα σε αυτό).και την τελευταία διαθέσιμη έκδοση του Tails.

Στη συνέχεια ανοίγουμε τον Tor browser και ανακατευθυνόμαστε στον σύνδεσμο **https://tails.boum.org/download/**, κάνοντας κλικ στο **'2. Download the ISO image'**, και έπειτα κλικ στο κουμπί κάτω από το Direct Download and Latest Release ('Tails [version] ISO image'). Τέλος, αποθηκεύουμε το αρχείο.

Εκκαθάριση και προετοιμασία του USB stick

Ακόμα κι αν κάποιος έχει ξαναχρησιμοποιήσει USB στο παρελθόν, το νέο Tails USB stick, θα πρέπει να είναι εξ' ολοκλήρου καθαρό.

Θα χρειασθεί, όμως, να αλλάξουμε και μερικές ρυθμίσεις στο USB stick, έτσι ώστε να είναι προετοιμασμένο να εκκινήσει τον υπολογιστή και να φιλοξενήσει το λειτουργικό Tails.

1. Εγκατάσταση του GParted κάνοντας αναζήτηση μέσω του Ubuntu Software Centre του υπολογιστή για την εφαρμογή και στη συνέχεια εγκατάστασης της.

2. Εισαγωγή του USB stick στο laptop και άνοιγμα τουGParted(GParted > Refresh Devices).

3. Το USB θα πρέπει να εμφανίζεται ως drive στο drop down μενού που βρίσκεται στην πάνω δεξιά γωνία (π.χ. μπορεί να το συναντήσουμε ως listed as /dev/sdb ή dev/sdc) και θα μας δείξει το μέγεθος του διαθέσιμου χώρου στο USB stick). Επιλέγουμε αυτή τη συσκευή.

4. Πλέον στην κορυφή του παραθύρου εμφανίζεται ένα μακρύ ορθογώνιο με πράσινο περίβλημα και πιθανότατα ένας χώρος στα αριστέρα του ορθογωνίου. Κάνοντας δεξί κλικ, επιλέγουμε 'unmount', κάνοντας ξανά δεξί κλικ και επιλέγουμε 'διαγραφή'.

5. Τα χρώματα που υπήρχαν στο ορθογώνιο έχουν εξαφανισθεί τώρα και αντικαταστάθηκαν από το γκρι. Κάνοντας δεξί κλικ στο ορθογώνιο, επιλέγουμε 'Νέο'.

6. Μια οθόνη με τίτλο 'Create new Partition' θα εμφανισθεί. Κάτω από το 'File System' επιλέγουμε 'fat32', και κάτω από το 'Label' τον τύπο 'TAILS'. Επιλέγουμε 'Προσθήκη' fat32 = File Allocation Table 32 bits

7. Κάνουμε κλικ στο πράσινο 'tick' (ακριβώς κάτω από την επιλογή 'Partition' στη μπάρα εργαλείων στο πάνω μέρος του παραθύρου).

[15] Για περισσότερες επιλογές εγκατάστασης δείτε τα σχετικά έγγραφα για το Tails από την επίσημη διανομή στον παρακάτω σύνδεσμο: https://tails.boum.org/doc/first_steps/index.en.html

8. Στο αναδυόμενο παράθυρο, επιλέγουμε ‘Apply’ για να ενεργοποιήσουμε τις διαδικασίες στη συσκευή, και έπειτα επιλέγουμε ‘Κλείσιμο’ όταν εμφανισθεί το μήνυμα: “All operations successfully completed”.

9. Τώρα, κάνουμε δεξί κλικ, στο μακρύ πράσινο ορθογώνιο και επιλέγουμε το ‘Manage Flags’ > επιλέγουμε ‘boot’, και το κλείνουμε. Αυτή η επιλογή θα επιτρέψει στον υπολογιστή μας να κάνει εκκίνηση του συστήματος από αυτόν τον δίσκο.

Το USB stick μπορεί πλέον να αφαιρεθεί αφού έχει εγκατασταθεί επιτυχώς το Tails.

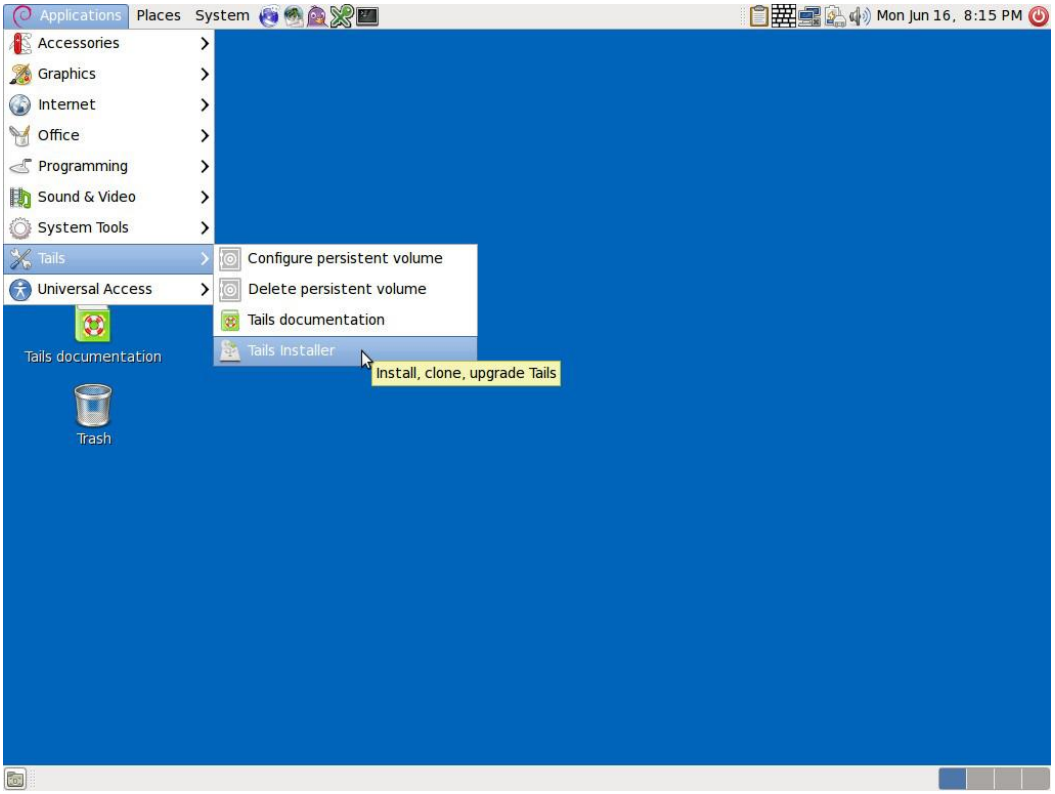
1. Κλωνοποίηση Tails USB stick

1. Μετά την δημιουργία ενός κλώνου Tails USB stick , πραγματοποιούμε επανεκκίνηση στο υπολογιστικό σύστημα εισάγοντας πρώτα το Tails stick. Με τον παρακάτω τρόπο μπορεί να δημιουργηθεί ένα νέο Tails USB stick 1. Προετοιμάζουμε ένα καθαρό, bootable USB stick με το GParted, όπως είδαμε παραπάνω , για να κλωνοποιήσουμε τα Tails σε αυτό. Αυτός ο δίσκος θα πρέπει να έχει χωρητικότητα τουλάχιστον 4 GB minimum για την εγκατάσταση των Tails, αλλά ιδανικά 8GB και άνω.

2. Ξεκινάμε το σύστημα Tails με το ήδη υπάρχον Tails stick.

3. Εισάγουμε το καθαρό, bootable USB-drive σε μία από τις ελεύθερες εισόδους USB του υπολογιστή.

4. Στην επιφάνεια εργασίας επιλέγουμε Applications > Tails > Tails Installer.



5. Ένα νέο παράθυρο θα ανοίξει. Επιλέγουμε: Clone & Install.

6. Το παράθυρο του Tails Installer θα πρέπει να εμφανίσει στην λίστα του το καθαρό USB stick. Κάνουμε κλικ στο 'Install Tails' στο κάτω μέρος του παραθύρου και επιλέγουμε το 'Yes' στο αναδυόμενο παράθυρο για να επιβεβαιώσουμε την επιλογή της συσκευής μας. Ένας κλώνος θα δημιουργηθεί τώρα στο δεύτερο USB-drive. Όταν θα ολοκληρωθεί η διαδικασία θα εμφανισθεί το μήνυμα: Installation complete.

7. Στη συνέχεια απενεργοποιούμε το σύστημα και προσπαθούμε να κάνουμε εκκίνηση του συστήματος από τον κλώνο-USB για να σιγουρευτούμε ότι λειτουργεί σωστά.

2. Χειροκίνητη εγκατάσταση των Tails μέσω UNetbootin

1. Μπορούμε να κατεβάσουμε το UNetbootin 494 για Linux (unetbootin-linux-494) από τον σχετικό σύνδεσμο[16].

   Πρέπει, όμως, να είμαστε σίγουροι οτι κατεβάσαμε την τελευταία έκδοση 494 για Linux έτσι ώστε να δουλέψει η εγκατάσταση των Tails. Όταν ολοκληρωθεί η λήψη, κάνουμε δεξί κλικ στον φάκελο UNetbootin και επιλέγουμε 'Properties' > Permissions tab > . Στη συνέχεια κάνουμε κάντε tick στο κουτάκι δίπλα από το 'Execute' ούτως ώστε να επιτραπεί η εκτέλεση του αρχείου ως πρόγραμμα 'Allow executing file as program'.

2. Για να τρέξουμε το *UNetbootin* ανοίγουμε το 'Terminal'. Το 'Terminal' είναι ένα μαύρο πλαίσιο με την εντολή: user@<name of your computer>: $. Αν δεν είναι ορατό μπορούμε να χρησιμοποιήσουμε το εργαλείο αναζήτησης του Ubuntu, το εικονίδιο που βρίσκεται στην πάνω αριστερή γωνία της οθόνης.

 Τύπος:

   cd Downloads

   (υποθέτοντας ότι Tails και UNetbootin βρίσκονται στις λήψεις 'Downloads') πατάμε Enter. Σε αυτό το σημείο καλό είναι να διευκρινιστεί οτι

   οι εντολές στο τερματικό θα πρέπει να είναι ακριβείς οπότε πρέπει να είμαστε σίγουροι οτι αφήσαμε κενό μετά το 'cd' και ότι το γράμμα D του Downloads είναι κεφαλαίο.

 Ο τύπος **sudo ./** ακολουθείται από το όνομα αρχείου του UNetbootin που έχει κατέβει. Οπότε θα μοιάζει κάπως έτσι:

   sudo ./unetbootinlinux494

[16] https://sourceforge.net/projects/unetbootin/files/UNetbootin/494/

Στη συνέχεια πατάμε enter σιγουρεύοντας οτι αφήσαμε κενό μετά το 'sudo'). Ίσως μας ζητηθεί ο κωδικός – εισάγοντας τον το UNetbootin θα πρέπει να είναι έτοιμο.

3. Για να δημιουργηθεί το αντίγραφο χρειάζεται να εισάγουμε το έτοιμο USB stick. Στο UNetbootin, επιλέγουμε το κυκλικό κουμπί στα αριστερά του 'Diskimage'. Επιλέγουμε το εικονίδιο του disk image file κάνοντας κλικ στην έλλειψη (…) στο δεξί μέρος του παραθύρου.
   Ανοίγουμε τις λήψεις 'Downloads' (υποθέτοντας πως εκεί έχει αποθηκευτεί το Tails που κατεβάσαμε πριν), και επιλέγουμε το αρχείο Tails .iso file. Κάτω από το 'Type' επιλέγουμε 'USB drive', και κάτω από το 'Drive', επιλέγουμε την τοποθεσία USB (εμφανίζεται μάλλον ως /dev/sdc, ή παρομοίως, αλλά είναι πολύ σημαντικό ότι επιλέξαμε το σωστό, στο GParted, η τοποθεσία του drive βρίσκεται κάτω από το 'partition'). Εάν δεν εμφανίζεται τίποτα κάτω από το 'Drive', περιμένουμε λίγο, ή προσπαθούμενα κάνουμε tick και untick την επιλογή 'show all drives'. Κάνουμε κλικ στο OK.

   Όταν το αντίγραφο ολοκληρωθεί, βγαίνουμε από το UNetbootin, και απενεργοποιούμε το τερματικό. Αφαιρούμε με ασφάλεια το USB και κάνουμε shutdown.
   Πλέον η διαδικασία έχει ολοκληρωθεί. Εφόσον έχει ρυθμιστεί το μηχάνημά σας να κάνει εκκίνηση από το USB (βλ. Προηγούμενο κεφάλαιο), μπορεί να εκκινηθεί με τα Tails από το USB stick.

3. Χειροκίνητη εγκατάσταση των Tails μέσω Linux[17]

1. Αρχικά πρέπει να βρεθεί το όνομα της συσκευής από το USB stick

Το όνομα της συσκευής αναφέρεται στο πως ο υπολογιστής αναγνώρισε το USB drive, και θα είναι της μορφής /dev/sdb, /dev/sdc1, κ.λπ. Εάν δεν είμαστε σίγουροι για το ακριβές όνομα της συσκευής, ακολουθούμε τα παρακάτω βήματα:

1. Σιγουρευόμαστε ότι το USB stick στο οποίο θέλουμε να εγκαταστήσουμε το Tails δεν είναι συνδεδεμένο.

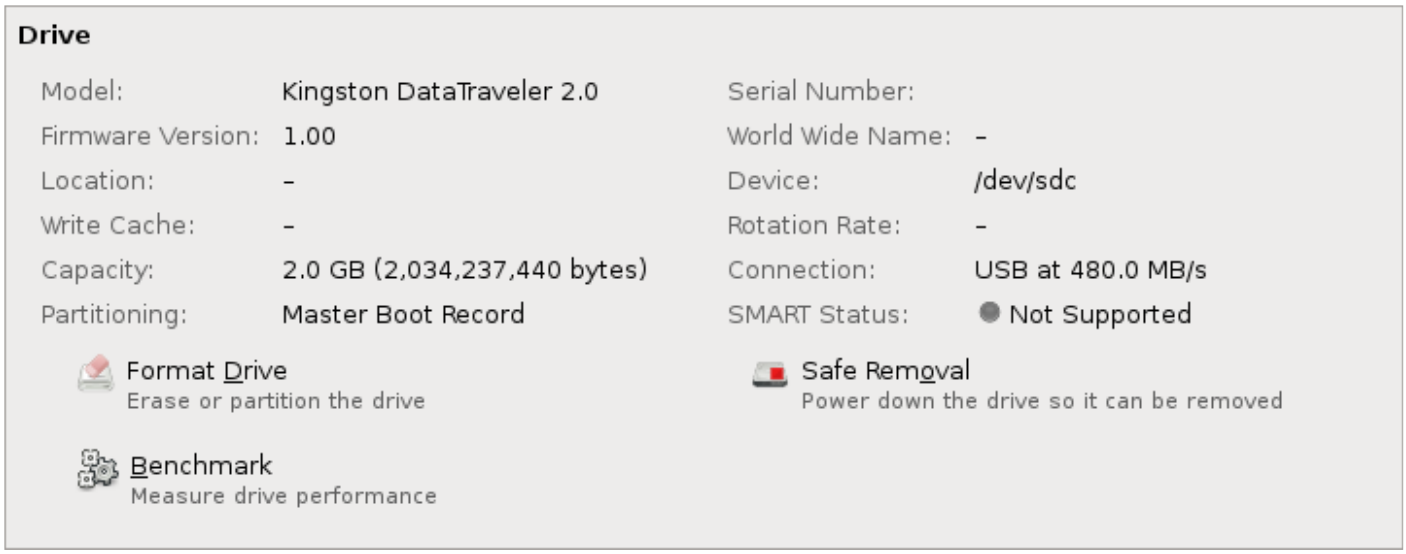
2. Ανοίγουμε το GNOME Disk Utility από το μενού Applications ▸ System Tools ▸ Disk Utility (η αναζήτηση του Ubuntu, το πάνω αριστερά εικονίδιο, εάν δεν μπορούμε να το βρούμε).

3. Το 'Disk Utility' θα εμφανίσει σε λίστα όλες τις τρέχουσες συσκευές αποθήκευσης στο αριστερό μέρος του παραθύρου.

[17] Δείτε επίσης: https://tails.boum.org/doc/first_steps/installation/manual/linux/index.en.html

4. Εισάγουμε το USB stick στο οποίο θέλουμε να εγκαταστήσουμε το Tails. Μια νέα συσκευή θα εμφανισθεί στη λίστα των διαθέσιμων για αποθήκευση συσκευών, πάνω στην οποία κάνουμε κλικ.

5. Στο δεξί μέρος του παραθύρου, μπορούμε να σιγουρευτούμε ότι τα χαρακτηριστικά ανταποκρίνονται στη συσκευή μας, μάρκα, μέγεθος, κ.λπ.



Στο ανωτέρω screenshot, το USB stick είναι το Kingston DataTraveler 2.0 GB και το όνομα συσκευής είναι /dev/sdc. Ωστόσο, σε περιπτώσεις που δεν μπορεί κάποιος να είναι σίγουρος για το όνομα της συσκευής, πρέπει να διακόψει την διαδικασία για να μη θέσει σε κίνδυνο διαγραφής τον εσωτερικό σκληρό δίσκο του μηχανήματος που χρησιμοποιεί.

2. Εισαγωγή του Tails

Αναζητάμε το αρχείο του Tails, κάνουμε δεξί κλικ, και επιλέγουμε το properties. Θα πρέπει να βλέπουμε την τοποθεσία του αρχείου (π.χ. /home/amnesia/Desktop/tails-0.6.2.iso) – κρατάμε μια σημείωση της τοποθεσίας.

3. Εισάγουμε το USB stick

4. Εγκαθιστάμε το isohybrid

Εάν χρησιμοποιούμε Ubuntu, το 'isohybrid' θα πρέπει να περιλαμβάνεται στην έκδοση. Για να ελεγχθεί ή να εγκατασταθεί, ανοίγουμε το 'Terminal' Είναι ένα μαύρο πλαίσιο εντολών:

user@<name of your computer>: $

στη συνέχεια πληκτρολογούμε το ακόλουθο πολύ προσεκτικά και με ακρίβεια στο Terminal, προτού πατήσουμε Enter:

sudo aptget install syslinux

5. Δημιουργούμε το αντίγραφο

Στο Terminal, εισάγουμε την ακόλουθη εντολή, αντικαθιστώντας [tails.iso] με την τοποθεσία του Tails που βρήκαμε στο βήμα 2, και αντικαθιστούμε το [device] με το όνομα της συσκευής του USB stick, όπως αυτό φαίνεται στο βήμα 1.

```
isohybrid [tails.iso] --entry 4 --type 0x1c dd
if=[tails.iso] of=[device] bs=16M
```

Παρακάτω βλέπουμε ένα παράδειγμα εντολής:

```
isohybrid /home/amnesia/Desktop/tails-0.6.2.iso --entry 4
--type 0x1c dd  if=/home/amnesia/Desktop/tails-0.6.2.iso
of=/dev/sdc bs=16M
```

Εάν δεν εμφανίσθηκε μήνυμα σφάλματος κατά την διαδικασία, το Tails έχει αντιγραφεί επιτυχώς στη συσκευή σας. Η όλη διαδικασία ίσως διαρκέσει κάποιο χρόνο, όχι όμως περισσότερο απο μερικά λεπτά. Πλέον μπορούμε να απενεργοποιήσουμε τον υπολογιστή σας, και να εκκινήσουμε το Tails από τη νέα συσκευή.

Επίλυση προβλημάτων - Troubleshooting

dd: /dev/sdx: No such file or directory

Ελέγχουμε διπλά το όνομα της συσκευής όπως εμφανίστηκε ακολουθώντας το βήμα 1. Εάν δεν είμαστε σίγουροι για το path που οδηγεί στην λήψη του Tails ή εάν εμφανίζεται το μήνυμα «No such file» ή κάποιο άλλο μήνυμα σφάλματος, μπορούμε να πληκτρολογήσουμε dd, μετά κενό, κι έπειτα σέρνουμε το εικονίδιο από τη λήψη του Tails από το αρχείο του browser στο Terminal. Με αυτό τον τρόπο θα εισάγουμε το σωστό path λήψης του Tails στο Terminal. Έπειτα ολοκληρώνουμε την εντολή και την εκτελούμε.

Dd: /dev/sdx: Permission denied

Σε περίπτωση που έχει γίνει λάθος στο όνομα της συσκευής, ελέγχουμε ξανά το όνομά της. Εάν είμαστε σίγουροι για το όνομα της συσκευής, τότε ίσως χρειασθεί να αποκτήσουμε πρόσβαση με δικαιώματα διαχειριστή προτού εισάγυομε τις εντολές στο terminal.

dd: tails.iso: No such file or directory

Ίσως έχει πραγματοποιηθεί σφάλμα στο path για τη λήψη του Tails στο βήμα 2.

Αναβάθμιση Tails

Το Tails θα πρέπει να αναζητά αυτόματα και να πραγματοποιεί λήψη των πρόσφατων ενημερώσεων. Παρόλο αυτά, για διάφορους λόγους, η λειτουργία της αυτόματης ανανέωσης του Tails ίσως να μην λειτουργεί πάντα.

Ένας διαφορετικός τρόπος για να ενημερώσουμε την έκδοση του Tails είναι να επιλέξυομε Applications > Tails > Tails Installer > Clone and Upgrade. Αυτή η επιλογή θα πραγματοποιήσει αναβάθμιση στη νεότερη έκδοση του Tails ενώ θα διατηρήσει και κάθε persistent volume που έχουμε αποθηκεύσει. Παρόλο αυτά, μερικοί χρήστες έχουν αναφέρει προβλήματα με αυτό – ειδικά με την διατήρηση των persistent volumes.

Έτσι λοιπόν έαν υπάρχει ενημέρωση για μια νέα έκδοση του Tails, ίσως θα μπορούσαμε να χρησιμοποιήσουμε το UNetbootin για να δημιουργήσουμε ένα νέο Tails stick με την καινούργια έκδοση. Μπορούμε χειροκίνητα να αντιγράψουμε τα αρχεία που επιθυμούμε να κρατήσουμεαπό το προηγούμενο Tails stick – ωστόσο δεν είναι η ευκολότερη μέθοδος[18].

Χρήση του Tails

Πρώτα από όλα, θα πρέπει να ρυθμιστεί το laptop έτσι ώστε να πραγματοποιεί εκκίνηση από τον USB drive.

Όταν πραγματοποιηθεί εκκίνηση του Tails, ο χρήστης θα δεί μια οθόνη να φορτώνει με τις επιλογές 'Live' και 'Live failsafe'. Εκεί μπορεί να χρησιμοποιήσει τα βελάκια για να υπογραμμίσει το 'Live' και να πατήσει enter.

Στη συνέχεια θα εμφανιστεί η επιλογή: 'More options?'. Αυτό το μενού δεν είναι απαραίτητο εκτός και αν προκύψει ανάγκη να ρυθμιστούν περαιτέρω τα Tails. Για να συνεχίσουμε χωρίς περαιτέρω ρυθμίσεις αρκεί να επιλέξουμε το 'no' και 'Login'.

Εάν επιλέξουμε 'yes' για περισσότερες επιλογές, θα δούμε:

- '*Administrative password*'. Είναι πολύ πιθανό να χρειαστεί να δημιουργηθεί ένας κωδικός εκτός κι εάν θέλουμε να έχουμε πρόσβαση στον σκληρό δίσκο του υπολογιστή (το οποίο δεν συνίσταται, και ενδεχομένως να θέσουμε σε κίνδυνο την ασφάλεια του υπολογιστή μας).

- '*Windows camouflage*'. Εάν επιλεγεί το 'Activate Microsoft Windows (version) camouflage', το Tails θα θυμίζει περισσότερο το λειτουργικό σύστημα των Windows. Αυτό μπορεί να φανεί χρήσιμο σε δημόσιους χώρους εάν υπάρχει η υποψία ότι το λειτουργικό σύστημα Tails μπορεί να αναγνωρισθεί.

[18] Δείτε το link για περαιτέρω οδηγίες: https://tails.boum.org/doc/first_steps/persistence/copy/index.en.html

- *'Spoof all MAC addresses'*. Η συγκεκριμένη επιλογή είναι προεπιλεγμένη και δίνει τη δυνατότητα να μείνουν κρυφές οι MAC διευθύνσεις, καθώς επίσης και να αποκρύψετε και η τοποθεσία του χρήστη.

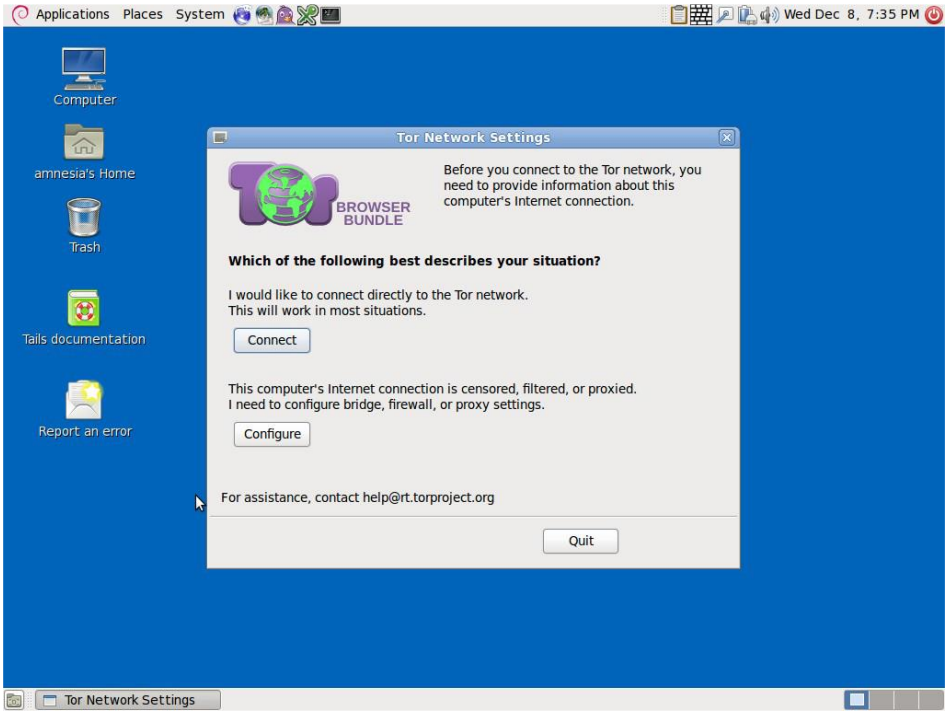
- *'Network configuration'*. Η συγκεκριμένη επιλογή έχει δύο υποεπιλογές: *'connect directly to the Tor network'*, *ή 'This computer's internet connection is censored, filtered or proxied. I need to configure bridge, firewall or proxy settings'*. Εάν το δίκτυό δεν επιτρέπει σύνδεση στο Tor, επιλέγουμε το τελευταίο.

Χρήση Tails μέσω bridges (γεφυρών)/ Παράκαμψη λογοκρισίας

Η συγκεκριμένη λειτουργία βοηθά τους χρήστες να συνδεθούν σε ένα onion-based δίκτυο[19] σε περιπτώσεις που το δίκτυό τους δεν τους επιτρέπει σύνδεση στο Tor. Οι γέφυρες (Bridges) είναι αναμεταδόσεις του Tor (κόμβοι ή σημεία του υπολογιστή που λαμβάνουν το traffic σε ένα Tor network και το μεταδίδουν σε επόμενο κόμβο) το οποίο βοηθά στην παράκαμψη της λογοκρισίας.

Όταν γίνεται εκκίνηση χρησιμοποιώντας ένα Tails USB stick και προσφέρονται 'More options?', επιλέγουμε 'Yes' και συνέχεια. Κάτω από το 'Network configuration', επιλέγουμε το 'This computer's internet connection is censored, filtered of proxied. I need to configure bridge, firewall or proxy settings'.

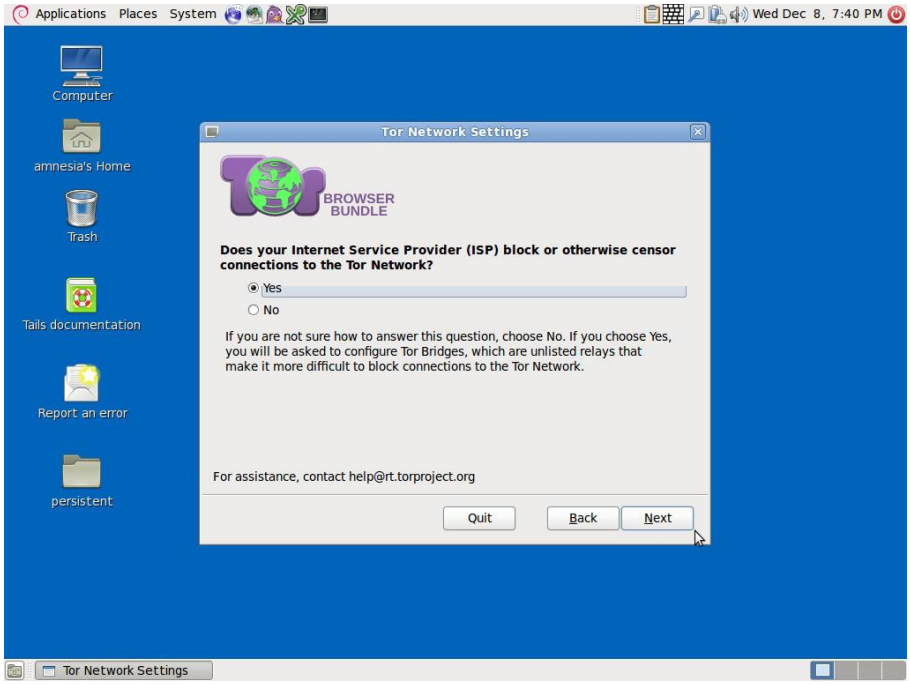
Έπειτα, όταν πραγματοποιηθεί σύνδεση στο διαδίκτυο με τον Tor browser ένα παράθυρο θα εμφανισθεί θέτωντας την ίδια ερώτηση.



Εάν εμφανισθεί η παραπάνω επιλογή, επιλέγουμε 'Configure'. Εαν ζητηθεί εάν χρειάζόμαστε να χρησιμοποιήσουμε proxy για την πρόσβασή στο διαδίκτυο –

[19] https://en.wikipedia.org/wiki/Onion_routing

επιλέγουμε 'No'. Έπειτα εάν η σύνδεση του υπολογιστή γίνει μέσω firewall που επιτρέπει συνδέσεις μόνο σε ορισμένες πύλες (ports) – επιλέγουμε και πάλι 'No'. Εάν χρειασθεί να επιβεβαιώσουμε τις γέφυρες-κόμβους (bridges), επιλέγουμε 'yes' και πατάμε next.



Θα εμφανισθεί ένα παράθυρο διαλόγου για να εισαχθούν μία ή περισσότερες γέφυρες - strings αριθμών που ορίζουν το Tor relay. Για να λάβουμε γέφυρες, μπορούμε να επισκεφτούμε την σχετική ιστοσελίδα[20] ή αν δεν έχουμε πρόσβαση σε αυτό το site, στείλνουμε ένα email στην διεύθυνση bridges@torproject.org από έναν λογαριασμό gmail.com ή yahoo.com, με θέμα 'get bridges' και κενό σώμα κειμένου, και θα μας σταλούν μερικές γέφυρες-κόμβοι. Χρησιμοποιώντας μια γέφυρα μπορεί να καθυστερήσει κατά πολύ την διαδικασία σύνδεσής με το διαδίκτυο – αλλά εάν θέλουμε να αποφύγουμε την λογοκρισία, τότε αυτός είναι ο μοναδικός τρόπος να το καταφέρουμε.

Δημιουργία μόνιμου αποθηκευτικού χώρου στο Tails

Για να δημιουγηθεί ένας μόνιμος χώρος στα Tails, επιλέγουμε Applications > Tails > Configure persistent volume. Εφόσον εισαχθεί ένας πολύ ισχυρός κωδικός, θα μπορεί να γίνει επιλογή του είδους των αρχείων που θα αποθηκεύτούν στον μόνιμο χώρο. Μπορούν να επιλεχθούν όλοι οι τύποι, για να μείνει το εύρος των επιλογών ανοιχτό.

Τώρα, κάθε φορά που γίνεται εκκίνηση από το Tails USB stick, θα ερωτάται ο χρήστης δύο ερωτήσεις: 'Use persistence?' και 'More options?' (όπως προηγουμένως). Εάν επιλέξει 'Yes' για να χρησιμοποιήσει το μόνιμο χώρο και εισάγει τον κωδικό του, θα μπορεί να έχει πρόσβαση σε όλα τα δεδομένα (π.χ. στα configured

[20] https://bridges.torproject.org

email, στα IM, στον password manager, ή και σε αρχεία) τα οποία έχει αποθηκεύσει στο μόνιμο χώρο κατά την διάρκεια των προηγούμενων ενεργειών του.

KeePassX

Το KeePassX είναι μια εφαρμογή διαχείρισης κωδικών πρόσβασης (password manager) που αποθηκεύει ονόματα χρηστών (usernames) και κωδικούς (passwords) σε μία τοπική κρυπτογραφημένη βάση δεδομένων, η οποία προστατεύεται από ένα master password. Επίσης περιέχει και το PWGen, έναν πανίσχυρο γεννήτορα τυχαίων κωδικών (random password generator). Το KeePassX βρίσκεται στις εφαρμογές.

Για να δημιουργηθεί μια νέα βάση κωδικών:

Επιλέγουμε File > New database. Δημιουργούμε ένα ισχυρό master password που θα προστατεύει τη βάση με τους κωδικούς μας. Μπορούμε να μετονομάσουμε το αρχείο της βάσης δεδομένων και να επιλέξουμε την τοποθεσία που θα αποθηκευτεί.

Groups > New groups (π.χ. 'Jabber' group, για τα usernames και passwords στο Jabber – περισσότερα για το Jabber στο κεφάλαιο 6).

Για να εισάγουμε έναν νέο κωδικό:

Επιλέγουμε group > Entries > Add new entry. Έχουμε την επιλογή να εισάγουμε έναν κωδικό, ή να δημιουγήσουμε τυχαία έναν (κάντε κλικ στο 'Gen'). Εάν επιλέξουμε εικονίδιο με το μάτι μπορούμε να δούμε τους χαρακτήρες του κωδικού – ειδάλλως, θα παραμείνει καλυμμένος.

Για να επαναφέρουμε έναν κωδικό:

Όταν έχει εισαχθεί ένας κωδικό σε μια ομάδα, μπορούμε να κάνουμε δεξί κλικ στον επιθυμητό κωδικό και να εεπιλέξου 'copy password to clipboard'. Έπειτα μπορούμε να τον επικολλήσουμε σε μια φόρμα login.

Email στο Tails

Εισαγωγή κλειδιού από άλλο laptop/λειτουργικό σύστημα

Αρκετοί χρήστες χρησιμοποιούν ξεχωριστά Tails stick, διευθύνσεις email, κ.λπ., για διαφορετικές εργασίες τους, ένας τρόπος που είναι άκρως αποτελεσματικός για να διατηρηθεί η ασφάλεια των δραστηριοτήτων τους. Παρόλα αυτά, ίσως χρειαστεί να προστεθεί ένα κλειδί που έχει δημιουργηθεί σε άλλο laptop με τον Tails key manager (αλλά πρέπει να λάβουμε υπόψιν μας ότι κάτι τέτοιο θα μπορούσε να θέσει σε κίνδυνο την ανωνυμία μας στο Tails).

Γι' αυτό τον λόγο, θα χρειαστούμε ένα επιπλέον USB stick.

Εισάγουμε, λοιπόν, το USB stick στο laptop που περιέχει το κλειδί που θέλουμε να μετακινήσουμε. Ανοίγουμε το Thunderbird, και επιλέγουμε στο Enigmail > Key management. Η διεύθυνση email/κλειδί βρίσκεται στην λίστα επαφών. Κάνονταςκάντε δεξί κλικ πάνω της για να επιλέξετε > Export keys to file > Export secret keys, βρίσκουμε τη συσκευή USB σας κι επιλέγουμε την ως την τοποθεσία στην οποία επιθυμούμε να αποθηκεύσουμε το κλειδί. Αφαιρούμε με ασφάλεια την συσκευή USB.

Κάνουμε επανεκκίνηση στο Tails. Όταν ολοκληρωθεί η εκκίνηση του Tails κι έχουμε πλέον συνδεθεί στο διαδίκτυο, εισάγουμε την συσκευή USB στην οποία έχουμε αποθηκεύσει το κλειδί. Κάνουμε κλικ στο OpenPGP, την εφαρμογή κρυπτογράφησης του Tails (είναι το εικονίδιο στο μενού στην πάνω δεξιά γωνία) κι επιλέξτε > Manage keys > File > Import.

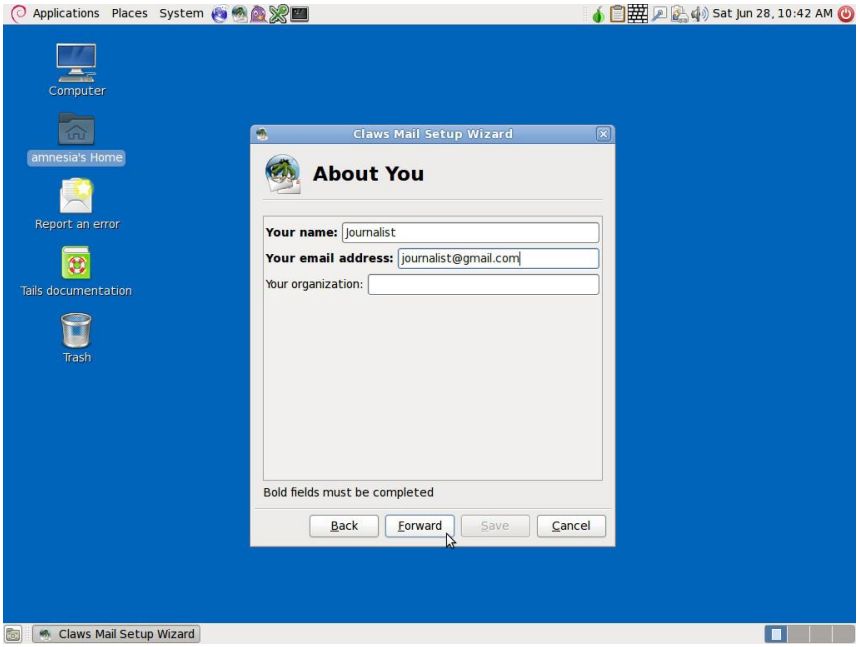
Ανοίγουμε τα αρχεία της συσκευής USB για να βρουμε το κλειδί που θέλουμε να εισάγουμε και επιλέγουμε Import.

Εφόσον ολοκληρωθεί η εισαγωγή του κλειδιού στο Tails, καλό είναι για λόγους ασφαλείας να διαγράψουμε το κλειδί από την συσκευή USB που χρησιμοποιήσαμε για να το μεταφέρουμε, από τη στιγμή που είναι άκρως επικίνδυνο να είναι αποθηκευμένο το μυστικό μας κλειδί σε μια απροστάτευτη USB συσκευή. Χρησιμοποιούμε την επιλογή 'Wipe' του Tails (κάνοντας δεξί κλικ στο αρχείο του κλειδιού στην συσκευή USB) για να διαγραφεί με ασφάλεια το αρχείο.

 Claws

Το Tails περιλαμβάνει μια προεγκατεστημένη εφαρμογή στην επιφάνεια εργασίας για τη διαχείριση των email, το Claws. Η συγκεκριμένη εφαρμογή βοηθάει στο να διαμορφωθούν λογαριασμοί email με GPG plug-in ούτως ώστε να μπορεί κάποιος να αποστέλλει κρυπτογραφημένα mail. Παρακάτω παραθέτουμε τα βήματα για διαμόρφωση του email στο Claws:

1. Χρησιμοποιούμε τον οδηγό εγκατάστασης του Claws, εισάγουμε το όνομά μας (εάν επιθυμούμε) και την διεύθυνση email.
   Πρέπει να ληφθεί υπόψη ότι ορισμένοι mail servers δεν λειτουργούν επαρκώς στο δίκτυο Tor, σε περίπτωση που η διαμόρφωση του Claws δεν λειτουργήσει. Σε αυτή την περίπτωση, μπορούμε είτε να δοκιμάσουμε διαφορετικούς παρόχους email, ή να δούμε το κομμάτι 'Άλλοι τρόποι κρυπτογράφησης στο Tails' που βρίσκεται παρακάτω.



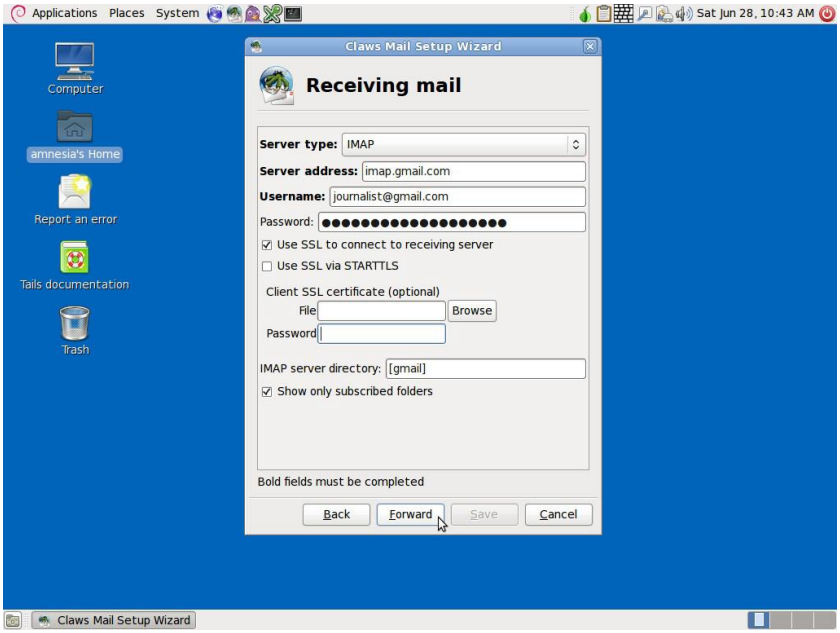
2. Λήψη mail

Ο τύπος του server, ώστε να γίνει η λήψη mail, πρέπει να είναι IMAP, αφού έχει γίνει η απαραίτητη αναζήτηση στο διαδίκτυο για την σωστή διεύθυνση IMAP server που συνάδει με τον πάροχο του εκάστοτε email.

Κάτω από το 'username' πληκτρολογούμε ολόκληρη τη διεύθυνση email.

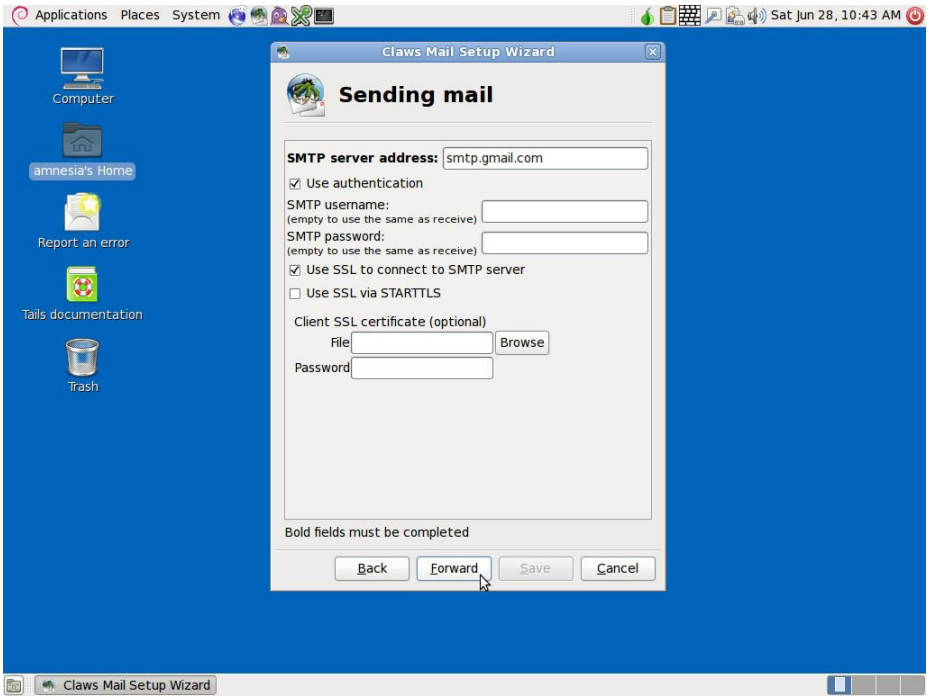
Εισάγουμε τον κωδικό του λογαριασμού μας.

Το πεδίο 'IMAP server directory' είναι προεραιτικό και μπορείτε να μείνει κενό.



3. Αποστολή mail

Θα πρέπει επίσης να γίνει αναζήτηση στο διαδίκτυο για τη σωστή διεύθυνση SMTP server που είναι συγκεκριμένη για τον πάροχο email που χρησιμοποιείται κάθε φορά.



4. Η διαμόρφωση ολοκληρώθηκε με επιτυχία.

Τώρα μπορεί να ανοίξει το Claws, να διαμορφωθεί η κρυπτογράφηση, να δημιουργηθεί ένα ζεύγος κλειδιών και να αλλάξουν οι ρυθμίσεις.

Διαμόρφωση του Claws για κρυπτογράφηση
Το Claws θα πρέπει ήδη να έχει εγκατεστημένα plugins για κρυπτογράφηση, αλλά θα πρέπει να ελεγχθεί και απο τον χρήστη:
Στο Claws, επιλέγουμε Configuration > Plugins > PGPcore > Load
Ένα νέο παράθυρο θα εμφανισθεί, 'Select the plugins to load': επιλέγουμε PGPcore και PGPinline, και στη συνέχεια επιλέγουμε Open.

Δημιουργία ζεύγους κλειδιών
Στο Claws, επιλέγουμε Configuration > Preferences for current account > GPG (κάτω από το Plugins).
- Επιλέγουμε 'Select key by your email address'.
- Εάν δεν έχει δημιουργηθεί ένα ζεύγος κλειδιών για την διεύθυνση email, επιλέγουμε 'Generate a new key pair'.

- Θα ζητηθεί να γίνει εισαγωγή ενός passphrase για τον λογαριασμό email (δύο φορές) κι έπειτα θα ξεκινήσει η διαδικασία δημιουργίας κλειδιού.

- Ο κέρσορας του ποντικιού πρέπει να βρίσκεται στην οθόνη καθώς το νέο ζεύγος κλειδιών δημιουργείται για να ενισχυθεί ο τυχαίος συνδυασμός.
- Εφόσον ολοκληρωθεί η διαδικασία, θα αναδυθεί ένα παράθυρο διαλόγου που θα ενημερώνει ότι το κλειδί δημιουργήθηκε 'Key generated' και θα ρωτάει 'Do you want to export it to a key server?'. Εάν όντως επιθυμούμε το κλειδί να είναι δημοσίως προσπελάσιμο (όταν για παράδειγμα δημιουργείται μια λίστα αριθμών στον κατάλογο τηλεφώνων), έτσι ώστε άλλοι χρήστες να μπορούν να βρουν το κλειδί και να μας στείλουν κρυπτογραφημένα emails, επιλέγουμε Ναι.

Έλεγχος κρυπτογράφησης και ρυθμίσεων σύνδεσης

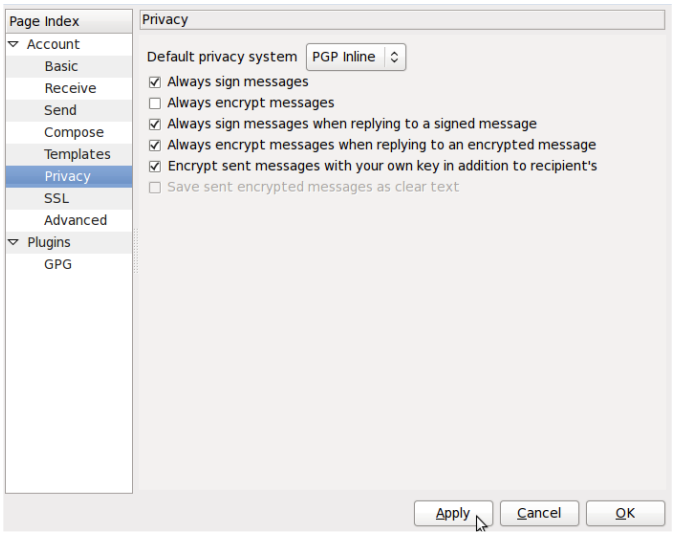
Στο Claws, επιλέγουμε Configuration > Preferences for current account > Privacy (στο μενού κάτω αριστερά).

- Ρυθμίζουμε το 'Default privacy system' σε 'PGP Inline'

- Ίσως θελήσουμε να επιλέξουμε 'Always sign messages'.

- Επίσης θα πρέπει να επιλέξουμε την επιλογή 'Encrypt sent messages with your own key in addition to recipient's' έτσι ώστε να μπορούμε να αποκρυπτογραφούμε και να διαβάζουμε τα απεσταλμένα μηνύματά μας.

- Όταν ολοκληρώσουμε τις επιλογές μας, επιλέγουμε 'Apply'.



Όλες οι προεπιλεγμένες ρυθμίσεις του Claws θα πρέπει πλέον να είναι εντάξει. Σε περίπτωση που θέλουμε να αλλάξουμε την συχνότητα που το Claws αναζητά για νέα εισερχόμενα μηνύματα, μπορούμε να το ρυθμίσουμε από εδώ:

Configuration > Preferences > Mail handling > Receiving.

Άλλοι τρόποι κρυπτογράφησης emails μέσω Tails – Εφαρμογή κρυπτογράφησης OpenPGP

Επειδή όλες οι συνδέσεις στο διαδίκτυο στο Tails γίνονται μέσω του δικτύου Tor, οι συνδέσεις στον πάροχο email του κάθε χρήστη μέσω του email client θα πραγματοποιηθεί και αυτή μέσω Tor. Οι χρήστες μερικών παρόχων email ορισμένες φορές αντιμετωπίζουν προβλήματα διαμόρφωσης των λογαριασμών email τους στο Claws μέσω Tails, επειδή η σύνδεση ανακατευθύνεται μέσω του δικτύου Tor για να είναι μη-ανιχνεύσιμη η τοποθεσία του χρήστη.

Το Tails προσφέρει μια εναλλακτική μέθοδο για την κρυπτογράφηση των email και των συννημένων που εμπεριέχονται σε αυτά. Από το να χρησιμοποιήσει κάποιος έναν email client για να κρυπτογραφήσει ολόκληρο το email, μπορεί να υπογραμμίσει το κείμενο και να το κρυπτογραφήσει με το επιθυμητό κλειδί του παραλήπτη, προτού το κάνει επικόλληση στο κρυπτογραφημένο μήνυμα του email (π.χ. όταν συντάσσεται ένα email στον web browser).

Εισαγωγή του κλειδιού επαφών

Επιλέγουμε στην εφαρμογή κρυπτογράφησης OpenPGP (στο εικονίδιο στην πάνω δεξιά γωνία) > Manage keys > Remote > Find remote keys (εάν δεν έχουμε ήδη εισάγει το κλειδί της επαφής μας). Εισάγουμε το όνομα της επαφής μας, και πατάμε αναζήτηση.

Εναλλακτικά:

Επιλέγουμε File > Import (εάν έχουμε ήδη αποθηκευμένο το κλειδί σε κάποιο αρχείο).

Κρυπτογράφηση μηνύματος

Επιλέγουμε στο Applications (αριστερά στο top menu toolbar) > Accessories > gedit Text Editor. Πληκτρολογουμε το μήνυμά μας. Μετά επιλέγουμε το όλο (Ctrl + A) και κάνουμε αντιγραφή (Ctrl + C, ή δεξί κλικ > copy) του μηνύματος στο clipboard. Στη συνέχεια επιλέγουμε στην εφαρμογή κρυπτογράφησης OpenPGP > Sign/encrypt Clipboard with Public Keys > επιλέγουμε τον παραλήπτη του email μας (θα πρέπει να έχουμε ήδη εισάγει το κλειδί του), συμπληρώνουμε την διεύθυνση email από την οποία θα αποστείλουμε το μήνυμά μας και πατάμε OK. Έπειτα κάνουμε επικόλληση το μήνυμα (Ctrl + V) στο πλαίσιο της δημιουργίας μηνύματος που φαίνεται στο παράθυρο του λογαριασμού email μας και τέλος πατάμε αποστολή (send).

Πρέπει να ληφθεί υπόψη ότι το μήνυμα είναι κρυπτογραφημένο και μόνο ο παραλήπτης που έχει επιλεγεί μπορεί να το αποκρυπτογραφήσει. Αυτό σημαίνει πως άπαξ και κρυπτογραφηθεί το μήνυμα, δεν θα είναι σε θέση ο αποστολέας να το αποκρυπτογραφήσει για να το διαβάσει. Εντούτοις, εάν χρησιμοποιηθεί αυτή η μέθοδος,

μια καλή ιδέα θα ήταν να χρησιμοποιήσουμε το δικό μας δημόσιο κλειδί, όπως και ο παραλήπτης του email, όταν κρυπτογραφούμε το μήνυμά μας. Έτσι θα μπορούμε να αποκρυπτογραφούμε τα απεσταλμένα μας μηνύματα, εάν θέλουμε να τα ξαναδιαβάσουμε.

Αποκρυπτογράφηση μηνύματος

Επιλέγουμε το κρυπτογραφημένο μήνυμα που θέλουμε να αποκρυπτογραφήσουμε. Συμπεριλαμβάνουμε τις γραμμές "-----BEGIN PGP MESSAGE-----" και "-----END PGP MESSAGE-----". Αντιγράφουμε το κείμενο στο clipboard (Ctrl + C, ή δεξί κλικ > copy). Η εφαρμογή κρυπτογράφησης OpenPGP Applet (εικονίδιο clipboard) θα εμφανίσει ένα λουκέτο, που σημαίνει ότι περιλαμβάνεται κρυπτογραφημένο κείμενο. Εάν το κείμενο που έχει επιλεγεί περιέχει μόνο υπογραφή αλλά δεν είναι κρυπτογραφημένο, το OpenPGP Applet θα εμφανίσει μια σφραγίδα, που σημαίνει ότι το clipboard περιλαμβάνει υπογεγραμμένο κείμενο.

Κάνουμε κλικ στο OpenPGP Applet (εικονίδιο clipboard) και επιλέγουμε 'Decrypt/Verify Clipboard' από το μενού. Το αποκρυπτογραφημένο κείμενο θα εμφανισθεί στο πλαίσιο κειμένου του Output του GnuPG.

Κρυπτογράφηση συνημμένων αρχείων του email

Είναι εύκολο να κρυπτογραφηθούν αρχεία χρησιμοποιώντας δημόσια κλειδιά και αποστέλλονται αυτά τα συνημμένα μέσω Tails. Κάνουμε δεξί κλικ στο επιθυμητό αρχείο > Encrypt > και επιλέγουμε την διεύθυνση του επιθυμητού παραλήπτη του μηνύματός μας. (υπογράφουμε το μήνυμα όπως η διεύθυνση από την οποία θα στείλουμε το email μας) > OK. Τώρα θα φανεί ένα διπλότυπο του επιλεγμένου αρχείου, με την κατάληξη '.pgp' – αυτό σημαίνει ότι το αρχείο είναι κρυπτογραφημένο. Επισυνάπτουμε το αρχείο .pgp στο email μας, το οποίο θα μπορεί να αποκρυπτογραφηθεί και να ανοιχθεί μόνο από τον παραλήπτη που έχουμε επιλέξει.

Κεφάλαιο 3: Ασφαλής πλοήγηση (Browsing)

Οι κύριοι κίνδυνοι της πλοήγησης στο διαδίκτυο (Web browsing) μπορούν να συνοψιστούν στα παρακάτω:

 Συλλογή προσωπικών στοιχείων – στοιχείων ταυτότητας.

 Συλλογή δεδομένων τάσης χρηστών το οποίο προκύπτει από τη διαδικτυακή συμπεριφορά σας κατά την διάρκεια της πλοήγησης, συμπεριλαμβανομένων των σελίδων που επισκέφθηκε ο χρήστης, καθώς και το πότε.

 Συλλογή δεδομένων από τους κωδικούς και τις φόρμες αυτόματης συμπλήρωσης.

 Συλλογή δεδομένων από την τοποθεσία των χρηστών (και τις προηγούμενες τοποθεσίες τους).

 Λογισμικά παρακολούθησης - Malware

 Απαγόρευση πρόσβασης σε ιστοσελίδες.

 Απαγόρευση χρήσης ανώνυμων περιηγητών.

Οι βασικές ενέργειες ενίσχυσης ασφάλειας πληροφοριακών συστημάτων είναι οι ακόλουθες:

 Χρήση ενός περιηγητή γενικής χρήσης με επεκτάσεις προστασίας ιδιωτικότητας, για τις καθημερινές ενέργειες.

 χρήση ενός Tor browser για ανώνυμη πλοήγηση, για προστασία από την λογοκρισία, και για να μείνει κρυφή η πραγματική μας τοποθεσία.

Ο web browser (πλοηγητής) είναι το λογισμικό που χρησιμοποιεί κάθε χρήστης για να αποκτήσει πρόσβαση στον World Wide Web (παγκόσμιο Ιστό). Για πολλούς από εμάς, η πλοήγηση είναι συνώνυμο με το Internet, και κατά μία έννοια είναι το παράθυρο για τον έξω κόσμο.

Λόγω των τεράστιων δυνατοτήτων της πλοήγησης στο διαδίκτυο, μερικά κράτη επιβάλλουν περιορισμούς στην πρόσβαση ορισμένων websites, γεγονός το οποίο παρεμποδίζει την ανθρώπινη ελευθερία και φυσικά θέτει σοβαρά προβλήματα σε ερευνητές, δημοσιογράφους και άλλους επαγγελματίες. Ενώ η πρόσβαση στο διαδίκτυο είναι σε μεγάλο βαθμό απεριόριστη στις χώρες της δύσης, ωστόσο αντιμετωπίζουμε σαν χρήστες σοβαρά θέματα ιδιωτικότητας σχετικά με την πλοήγησή μας στο διαδίκτυο. Οι περισσότεροι πάροχοι υπηρεσιών διαδικτύου και ιστοσελίδων συλλέγουν τεράστιους όγκους δεδομένων σχετικά με τους χρήστες τους.

Σε αυτό το κεφάλαιο θα εξηγήσουμε μερικές επιλογές για να ελαχιστοποιηθεί η παρεμπόδιση της ελευθερίας και της ιδιωτικότητας κατά την πλοήγηση, υπό ορισμένες συνθήκες.

Ποιόν browser να επιλέξω;

Μερικοί χρήστες δεν είναι ενημερωμένοι όσον αφορά την ιδιωτικότητά τους όταν χρησιμοποιούν browsers. Παρόλο που όλοι έχουμε ήδη εγκατεστημένο έναν «οποιοδήποτε» περιηγητή για να σερφάρουμε στο διαδίκτυο, υπάρχουν εναλλακτικές προτάσεις οι οποίες είναι περισσότερο ασφαλείς, και μπορούν να βελτιωθούν ακόμη περισσότερο ενισχύοντάς τες με προσθήκη προεκτάσεων 'extensions' – επιπλέον λογισμικό που βελτιώνει την λειτουργικότητα του browser μας.

Ενώ κυκλοφορούν αρκετοί browsers με ειδικές λειτουργίες, σε αυτό το σημείο θα δούμε τρεις browsers ανοιχτού κώδικα:

- Firefox, γενικής χρήσης web browser για Linux και Windows.
- Chromium, γενικής χρήσης web browser για Mac.
- Tor, ασφαλής browser που κρατάει ανώνυμη την τοποθεσία και την ταυτότητά του χρήστη και γενικότερα ενεργεί ως αντισταθμιστικός παράγοντας στην λογοκρισία στο διαδίκτυο (είναι κατάλληλο για Linux, Windows και Mac).

Πληροφορίες από τους ειδικούς: Ο λόγος που προτείνουμε τον Firefox για Linux και Windows αλλά όχι για Mac, είναι επειδή ο Firefox μερικές φορές «συγκρούεται» με το Tor στα Mac (επειδή Firefox και Tor βασίζονται στον ίδιο κώδικα).

Browser γενικής χρήσης

Το καθημερινό σερφάρισμα στο διαδίκτυο περιφέρεται κυρίως γύρω από sites χωρίς περιορισμούς στα οποία συνδεόμαστε, όπως πλατφόρμες σελίδων κοινωνικής δικτύωσης, σελίδες εφημερίδων, YouTube, ηλεκτρονικά καταστήματα, κ.ο.κ.. Δεν θα ήταν λογική η χρήση Tor για sites στα οποία συνδεόμαστε με την πραγματική μας ταυτότητα, εκτός και αν το κυρίαρχο μέλημά μας είναι να προστετεύσουμε την πραγματική μας τοποθεσία (σε αυτή την περίπτωση θα πρέπει να χρησιμοποιείται το λειτουργικό σύστημα Tails).

Firefox

Ο δημοφιλής web-browser ανοιχτού κώδικα

Σε Windows, μπορεί να κατέβει ο Firefox στην γλώσσα που επιθυμούμε[21].

Σε Linux/Ubuntu, ο Firefox είναι προεγκατεστημένος.

[21] www.getfirefox.com

Chromium

Ένας κλώνος του Google Chrome ανοιχτού κώδικα

Μπορεί να κατέβει για Mac από τον σχετικό σύνδεσμο[22].

(Εναλλακτικά, μπορούμε να επισκεφτούμε το www.macupdate.com και να αναζητήσουμε τον Chromium).

Extensions (Επεκτάσεις)

Ένας browser γενικής χρήσης είναι σίγουρο πως θα εμφανίζει δημοσίως την ταυτότητα και την τοποθεσία του εκάστοτε χρήστη. Εντούτοις, για να προστατευτεί η ιδιωτικότητα μας απο ενέργειες όπως, η παρακολούθηση της συμπεριφοράς μας κατά την διάρκεια της πλοήγησης στο διαδίκτυο,η αποθήκευση και η διαρροή των κωδικών και των φόρμων αυτόματης συμπλήρωσης, καθώς και οι man-in-the-middle επιθέσεις και τα malware injections, υπάρχει διαθέσιμη μια μεγάλη ποικιλία extensions[23], τα οποία είναι κατάλληλα για Firefox και Chromium.

Μπορείτε να βρείτε διαθέσιμη μια μεγάλη ποικιλία για να προστατεύσετε την ιδιωτικότητά σας. Εδώ θα προτείνουμε τα ακόλουθα extensions ανοικτού κώδικα:

HTTPS everywhere: κρυπτογράφηση σε όλες τις συνδέσεις μεταξύ του web browser και του webserver[24].

NoScript[25]: μπλοκάρει τα JavaScript. Το JavaScript είναι ένα απαραίτητο στοιχείο για πολλά websites, αλλά μπορεί να θέσει σε κίνδυνο τους χρήστες παρακολουθώντας την συμπεριφόρα τους κατά την διάρκεια της πλοήγησης, να διαρρεύσει κωδικούς, και να επιτρέψει malware injections. Το NoScript είναι πολύ αποτελεσματικό αλλά θα πρέπει να δεχόμαστε ή να απορρίπτουμε τις δικαιοδοσίες σε κάθε website που επισκεπτόμαστε αναλόγως του κατά πόσο το εμπιστευόμαστε.

Ghostery[26]: μπλοκάρει ένα μεγάλο εύρος ανιχνευτών (agents) στην βάση δεδομένων του, οι οποίοι μπορεί να παρακολουθούν την συμπεριφορά κατά την διάρκεια της πλοήγησης. Θα πρέπει να σιγουρευτούμε ότι απενεργοποιήσαμε το 'GhostRank' επιλέγοντας Settings > Options, καθώς αυτό το στοιχείο στέλνει αναφορές των κινήσεών μας για σκοπούς μάρκετινγκ.

[22] http://www.macupdate.com/app/mac/36244/chromium
[23] https://addons.mozilla.org/en-US/firefox/extensions/privacy-security/
[24] https://www.eff.org/https-everywhere
[25] https://noscript.net/
[26] https://ghostery.com

Web Of Trust[27]: είναι μια βάση δεδομένων με βαθμολόγησεις διάφορων website, η οποία ενημερώνει τους χρήστες εάν το συγκεκριμένο website που επισκέπτονται θεωρείται (αν)ασφαλές βάσει των απόψεων άλλων χρηστών.

LastPass[28]: πρόκειται για έναν αποτελεσματικό γεννήτορα αλλά και διαχειριστή κωδικών πρόσβασης για τον Firefox.

Tor

Σχετικά με τον Tor[29]

Ο Tor browser σχεδιάσθηκε ειδικά με σκοπό την ανωνυμία στο διαδίκτυο μεταφέροντας όλη την κυκλοφορία μέσω του δικτύου Tor ('The Onion Router').

Είναι ένα παγκόσμιο δίκτυο υπολογιστών επονομαζόμενοι Tor nodes, οι οποίοι έχουν κρυπτογραφημένες συνδέσεις μεταξύ τους. Όταν γίνεται η εκκίνηση του Tor browser, συνδέεται σε ένα από αυτά τα nodes. Αυτός ο υπολογιστής θα συνδεθεί με έναν δεύτερο υπολογιστή ο οποίος με τη σειρά του θα συνδεθεί με έναν τρίτο. Αυτοί οι υπολογιστές μπορεί να βρίσκονται οπουδήποτε στον κόσμο, και ο πρώτος με τον τρίτο υπολογιστή δεν θα γνωρίζουν ότι επικοινωνούν. Ο τρίτος υπολογιστής θα συνδεθεί στο ευρύτερο διαδίκτυο και θα φέρει τις σελίδες από τα sites που επισκεπτόμαστε. Αυτά τα sites δεν θα έχουν την δυνατότητα να εντοπίσουν την τοποθεσία μας ή την ταυτότητά μας (απαραίτητη προϋπόθεση να μην συνδεόμαστε σε σελίδες με την πραγματική μας ταυτότητα).

Δεδομένου ότι ο Tor browser χρησιμοποιεί nodes (κόμβους) από κάθε διαθέσιμο σημείο στον πλανήτη, είναι επόμενο η πλοήγηση να είναι πιο αργή από ότι συνήθως. Αυτό όμως είναι το τίμημα που θα πρέπει να πληρώσει ο κάθε χρήστης για να διατηρήσει την ανωνυμία του στον διαδικτυακό κόσμο.

Για να διασφαλίσει την ασφάλειά του, ο Tor browser αυτόματα ενεργοποιεί το HTTPS-Everywhere, και αυτομάτως αποφεύγει επεκτάσεις όπως Flash, RealPlayer και QuickTime. Λόγω αυτού αλλά και του περιορισμού της ταχύτητας, υπηρεσίες όπως το YouTube δεν θα δουλέψουν στον Tor browser αποτελεσματικά. Προτείνουμε έναν browser γενικής χρήσης για τέτοιου είδους ανάγκες.

Εάν ο δικτυακός πάροχος που χρησιμοποιούμε μπλοκάρει την πρόσβαση μας στο δίκτυο Tor, μπορούμε να χρησιμοποιήσουμε τις γέφυρες για να αποκτήσουμε πρόσβαση.Οι γέφυρες (Bridges) είναι ιδιωτικοί Tor relays (υπολογιστές ή σημεία υπολογιστών που λαμβάνουν την κυκλοφορία στο Tor network και την διοχετεύουν αλλού) οι οποίοι είναι λιγότερο πιθανό να μπλοκαριστούν, κι επιπλέον σας βοηθούν να αποφευχθεί η λογοκρισία. Πως όμως μπορούν να εγκατασταθούν;

[27] https://www.mywot.com/
[28] https://lastpass.com/
[29] https://www.torproject.org/

Ξεκινάμε τον Tor Browser Bundle. Από το Vidalia Control Panel, επιλέγουμε Settings > Network > και κατόπιν επιλέγουμε 'My ISP blocks connections to the Tor network'.Τώρα θα εμφανιστεί ένα πλαίσιο στο οποίο μπορούμε να εισάγουμε μια ή περισσότερες γέφυρες – ακολουθίες αριθμών που υποδηλώνουν έναν Tor relay. Για να λάβουμε γέφυρες, μπορούμε να επισκεφτούμε τη σχετική ιστοσελίδα[30] ή εάν δεν έχουμε πρόσβαση στο site, στέλνουμε ένα email στο bridges@torproject.org, από έναν λογαριασμό gmail.com ή yahoo.com, με θέμα 'get bridges' και το ίδιο στο σώμα κειμένου και οι γέφυρες θα αποσταλλούν ως απάντηση. Χρησιμοποιώντας γέφυρες η σύνδεσή στο διαδίκτυο θα είναι πολύ αργή – αλλά εάν η αποφυγή λογοκρισίας είναι ο στόχος, τότε είναι η βέλτιστη λύση.

Ωστόσο, προτού χρησιμοποιηθούν θα πρέπει να ληφθούν υπόψη τα παρακάτω:

- Κανένα αρχείο κανένα αρχείο (όπως .doc και .pdf) που έχει κατεβάσει μέσω του Tor ενώ βρισκόμαστε ακόμη online δεν πρέπει να ανοίξει. Αυτοί οι τύποι αρχείων μπορεί να περιλαμβάνουν στοιχεία τα οποία ανεξάρτητα συνδέονται στο διαδίκτυο, κι έτσι θα αποκαλυφθεί η πραγματική διεύθυνση IP. Οπότε πρέπει πρώτα να σιγουρευτούμε ότι έχουμε αποσυνδεθεί ή να χρησιμοποιήσουμε έναν ξεχωριστό υπολογιστή για να δουλέψουμε αυτά τα αρχεία.
- Κανένα bittorrent μέσω Tor δεν θα πρέπει να τρέξει γιατί αυτό ίσως προδώσει την αληθινή διεύθυνση IP.

Εγκατάσταση Tor

Κάθε φορά που πραγματοποιείται εκκίνηση του Tor, ελέγχεται τυχόν διαθεσιμότητα νέων ενημερώσεων, οπότε θα πρέπει να γίνονται άμεσα οι –αντίστοιχες ενημερώσεις όταν εκείνες είναι διαθέσιμες.

Για *Mac και Windows* κατεβάζουμε κι εγκαθιστούμε τον Tor browser για το λειτουργικό μας σύστημα από τη σχετική ιστοσελίδα (βλ. 29) ακολουθώντας τις οδηγίες εγκατάστασης που υπάρχουν στο site.

Για Linux και Ubuntu κατεβάζουμε τον Tor browser για Linux από τη σχετική ιστοσελίδα (βλ. 29). Στην συνέχεια αποθηκεύουμε την λήψη (προσοχή: η έκδοση 32-bit ταιριάζει σε παλαιότερα μηχανήματα, ενώ η 64-bit ταιριάζει σε νεότερα) και ανοίγουμε το 'Terminal' χρησιμοποιώντας το εργαλείο αναζήτησης του Ubuntu, το πάνω αριστερά εικονίδιο στην οθόνη, εάν δεν μπορούμε να το βρούμε. Είναι ένα μαύρο πλαίσιο με μια γραμμή εντολών που αναγράφει: user@<name of your computer>: $

[30] https://bridges.torproject.org

Στο Terminal, πληκτρολογούμε μια από τις παρακάτω εντολές για να αποσυμπιεστεί το αρχείο και στη συνέχεια πατάμε Enter:

tar –xvJf tor-browser-linux32-3.6.2_LANG.tar.xz

(το υποκατάστατο LANG από τη λέξη language αναφέρεται στο όνομα αρχείου).

Ή

tar –xvJf tor-browser-linux64-3.6.2_LANG.tar.xz

(για την έκδοση 64-bit,):

Όταν ολοκληρωθεί η διαδικασία, μεταβαίνουμε στον φάκελο Tor browser. Πληκτρολογούμε την ακόλουθη εντολή στο Terminal, και πατάμε Enter.

cd tor-browser_LANG

Για να ξεκινήσει ο Tor browser σε λειτουργικό Linux, οποιαδήποτε στιγμή, πρέπει να χρησιμοποιηθεί η ακόλουθη εντολή στο Terminal:

./start-tor-browser

Αυτό θα εκκινήσει τον Tor Launcher και μόλις συνδεθεί στο δίκτυο Tor, θα εκκινήσει ο Firefox.

Μια εφαρμογή εκκίνησης του Tor browser περιλαμβάνεται ήδη στο Ubuntu 14.10, το οποίο είναι διαθέσιμα από τον Οκτώβριο του 2014. Για περισσότερες πληροφορίες, μπορούμε να επισκεφτούμε τη σχετική σελίδα[31].

[31] https://github.com/micahflee/torbrowser-launcher#tor-browserlauncher

Κεφάλαιο 4: Δεδομένα

Όταν αποθηκεύουμε ή μεταφέρουμε δεδομένα, καραδοκούν ορισμένοι κίνδυνοι που χρήζουν προσοχής: υποκλοπή/κλοπή, απώλεια, φθορά, έκθεση σε μη εξουσιοδοτημένους χρήστες κλπ. Η διαφορά μεταξύ της υποκλοπής και της κλοπής έγκειται στην ανίχνευση του αρχικού ιδιοκτήτη. Υποκλοπή συνήθως σημαίνει πως ένα αντίγραφο των δεδομένων έχει δημιουργηθεί κρυφά ενώ η κλοπή υποδηλώνει πως έχει αφαιρεθεί είτε η συσκευή αποθήκευσης που περιλάμβανε τα δεδομένα (laptop, δίσκος USB ή ο σκληρός δίσκος) είτε τα ίδια τα γνήσια δεδομένα. Η τελευταία περίπτωση ίσως είναι ανιχνεύσιμη, ενώ για την πρώτη είναι σχεδόν αδύνατο.

Εάν τα ευαίσθητα δεδομένα πέσουν σε χέρια ανταγωνιστών, μπορεί να υπάρξουν πολύ σοβαρές επιπτώσεις στον εκάστοτε χρήστη ανάλογες με τη σημαντικότητα τους.

Για την προστασία των ηλεκτρονικών αρχείων υπάρχουν αρκετές επιλογές. Η απλή αποθήκευση τους σε μια μικρή συσκευή (δίσκος USB, κάρτα μνήμης ή εξωτερικός σκληρός δίσκος) και η φύλαξή τους σε ένα ασφαλές μέρος ίσως είναι μια καλή επιλογή σε ορισμένες περιπτώσεις. Σε αυτό το σενάριο, το όλο ζήτημα ασφαλείας εξαρτάται αποκλειστικά από το εάν θα βρεθεί η συσκευή αποθήκευσης όπου αυτή είναι κρυμμένη.

Για να προστατευτούν τα δεδομένα από μη εξουσιοδοτημένη πρόσβαση, είναι επίσης σημαντικό να κρυπτογραφηθούν. Το TrueCrypt είναι ένα εύχρηστο εργαλείο για την κρυπτογράφηση αρχείων και ολόκληρων δίσκων.

TrueCrypt

Το TrueCrypt[32] είναι ένα λογισμικό κρυπτογράφησης ανοίχτου κώδικα.

Τον Ιούνιο του 2014, το website του TrueCrypt άλλαξε ξαφνικά – υπήρχε η δήλωση πως το προϊόν δεν είναι πλέον ασφαλές και οι χρήστες συμβουλεύονταν να μεταβούν στο BitLocker της Microsoft (το οποίο τρέχει μόνο σε Windows, μια ευρέως γνωστή πλατφόρμα για τα ποικίλα προβλήματα ασφάλειας όπως ήδη έχουμε αναφέρει ανωτέρω). Όλες οι προηγούμενες εκδόσεις του λογισμικού αφαιρέθηκαν και αντικαταστάθηκαν με μια νέα έκδοση, 7.2, η οποία μπορεί μόνο να αποκρυπτογραφεί τα ήδη υπάρχοντα αρχεία TrueCrypt.

Οι συζητήσεις για το τι πραγματικά έγινε, ποιός έκανε τις αλλαγές στο website και γιατί, συνεχίζονται – αλλά, μεταξύ της πλειονότητας των ειδικών, επικρατεί η άποψη πως η προηγούμενη έκδοση του TrueCrypt (η οποία είναι διαθέσιμη online από το νέο site https://truecrypt.ch/) ήταν αρκετά αποτελεσματική.

Με το TrueCrypt, είναι δυνατό να δημιουργηθεί ένα κρυπτογραφημένο 'κιβώτιο' που συμπεριφέρεται σαν ψηφιακό κουτί για αρχεία, κλειδωμένο με έναν κωδικό. Αφού

[32] https://truecrypt.ch/

δημιουργηθεί αυτό το κουτί και γεμίσει με αρχεία μπορεί να μεταφερθεί σε έναν εξωτερικό σκληρό δίσκο, όπως π.χ. ένας δίσκος USB, ή να σταλεί μέσω internet σε άλλους. Ακόμα κι αν το ίδιο το αρχείο υποκλαπεί, το κιβώτιο αυτό δεν θα αποκαλύψει το περιεχόμενό του σε κανέναν που δεν διαθέτει τον κωδικό. Κατά συνέπεια είναι ιδιαίτερα σημνατικό να μη ξεχνάμε τον κωδικό μας διότι δεν υπάρχει άλλος τρόπος να ανακτήσουμε τα δεδομένα μας εφόσον έχουν κρυπτογραφηθεί. Η απώλεια του κωδικού είναι συνώνυμη με την απώλεια των ίδιων των δεδομένων!

Προβλήματα στην εγκατάσταση του TrueCrypt

Το TrueCrypt δεν ενημερωνέται πλέον. Για αυτό το λόγο, η τελευταία διαθέσιμη έκδοση του λογισμικού δεν θα είναι εύκολο να εγκατασταθεί σε λειτουργικά συστήματα που βγήκαν από τον Ιούνιο του 2014 και μετά. Για παράδειγμα, μερικοί χρήστες έχουν αναφέρει ένα μήνυμα σφάλματος όταν προσπάθησαν να εγκαταστήσουν το TrueCrypt στα Mac OS X Yosemite, στο οποίο αναφερόταν ότι το λειτουργικό σύστημα είναι πολύ παλιό (παρόλο που είναι το νεότερο). Εάν αντιμετωπιστεί αυτό το πρόβλημα, μπορούν να πραγματοποιηθούν οι παρακάτω ενέργειες:

1. Ανοίγουμε το .dmg - το TrueCrypt αρχείο που έχουμε κατεβάσει.

2. Αντιγράφουμε το 'TrueCrypt 7.1a.mpkg' και το επικολλάμε σε ένα διαφορετικό φάκελο. Θα είμαστε πλέον σε θέση να επεξεργαστούμε την νέα έκδοση που έχουμε αντιγράψει.

3. Κάνουμε δεξί κλικ στο .mpkg που έχουμε αντιγράψει και επιλέγουμε 'Show Package Contents'.

4. Επεξεργαζόμαστε το αρχείο Contents/distribution.dist σε έναν επεξεργαστή κειμένου, όπως φαίνεται παρακάτω:

Προηγουμένως, έμοιαζε έτσι:

```
1   function pm_install_check() {
2    if(!(system.version.ProductVersion >= '10.4.0')) {
3      my.result.title = 'Error';
4      my.result.message = 'TrueCrypt requires Mac OS X 10.4 or later.';
5      my.result.type = 'Fatal';
6      return false;
7    }
8    return true;
9   }
```

Διαγράφουμε όλα τα 'if', για να μοιάζει σαν αυτό:

```
1. function pm_install_check() {
2. return true;
3. }
```

Αποθηκεύουμε το νέο αντίγραφο του .mpkg, και τρέχουμε το αντίγραφο για να εγκαταστήσουμε το TrueCrypt.

Κρυπτογράφηση αρχείων με το TrueCrypt

Παρακάτω θα δούμε πως γίνεται η κρυπτογράφηση αρχείων με το TrueCrypt

1. Download

Κατεβάζουμε το TrueCrypt από τη σχετική ιστοσελίδα και το εγκαταθιστούμε στο σύστημά μας με τον ίδιο τρόπο όπως όλες τις άλλες εφαρμογές.

Το TrueCrypt δουλεύει το ίδιο αποτελεσματικά σε Windows, Mac και Linux και τα κρυπτογραφημένα αρχεία είναι συμβατά μεταξύ αυτών των συστημάτων. Αυτό επιτρέπει στους χρήστες να συνεργάζονται ασφαλώς με άλλους χωρίς να τους απασχολεί ποιό σύστημα χρησιμοποιούν εκείνοι.

2. Δημιουργία ενός κρυπτογραφημένου συνόλου δεδομένων

Για να δημιουργηθεί ένα κρυπτογραφημένο σύνολο δεδομένων (όπως π.χ. ένας φάκελος) ξεκινάμε το πρόγραμμα και επιλέγουμε:

 'Create Volume' > ‘Create an encrypted container’ > επιλέγουμε ‘Standard TrueCrypt volume’ > επιλέγουμε την τοποθεσία που θέλουμε να αποθηκευτεί (μπορεί να μετακινηθεί αργότερα) και του δίνουμε ένα όνομα.

Για να κρυπτογραφηθεί ένας εξωτερικός σκληρός δίσκος, όπως π.χ. ένα USB stick, επιλέγουμε 'Create Volume' > Create a volume within a partition/drive'

 Θα εμφανιστεί στην οθόνη ένα παράθυρο με τίτλο ‘Encryption Options’. Οι προεπιλεγμένες επιλογές καλύπτουν συνήθως τις ανάγκες των περισσότερων χρηστών. Για ισχυρότερη κρυπτογράφηση (πολλαπλή κρυπτογράφηση), κάτω από το ‘Encryption Algorithm, επιλέγουμε ‘AES twoFish-Serpent’, και κάτω από το ‘Hash Algorithm’, επιλέγουμε SHA-512.

 Στο επόμενο παράθυρο με τίτλο ‘Volume size’ επιλέγουμε το μέγεθος του αρχείου (θα καθορίσει το μέγιστο όγκο δεδομένων που θα μπορούμε να αποθηκεύσουμε σε αυτό).

 Ορίζουμε έναν κωδικό για το αρχείο μας στο επόμενο παράθυρο. Επιλέγουμε έναν ισχυρό κωδικό τον οποίο σε κάθε περίπτωση δεν πρέπει να ξεχάσουμε.

 Το επόμενο παράθυρο έχει τίτλο Format Options. Επιλέγουμε FAT.

Το FAT είναι συμβατό με όλα τα συστήματα αλλά περιορίζει το μέγεθος των δεδομένων που μπορεί να διαχειριστεί. (τα μεμονωμένα αρχεία δεν μπορούν να έχουν μέγεθος παραπάνω από 4 GB). Συνήθως αυτό δεν αποτελεί πρόβλημα. Εάν είναι απαραίτητο να αποθηκευτούν μεγαλύτερα αρχεία και είμαστε σίγουροι ότι η επιλογή άλλης μορφής εκτός του FAT δεν θα δημιουργήσει προβλήματα, τότε επιλέγουμε κάποιον άλλο τύπο από τις επιλογές.

 Το πρόγραμμα θα δημιουργήσει ένα τυχαίο σετ δεδομένων για να κρυπτογραφήσει το σύνολο τους. εαν κινήσουμε τυχαία τον κέρσορα του ποντικιού για ένα λεπτό, προτού κάνουμε κλικ στο 'Format', το πρόγραμμα θα δημιουργήσει το πεδίο όπου θα καταχωρηθεί το σύνολο των δεδομένων. Βάσει του μεγέθους, του αλγορίθμου κρυπτογράφησης που επιλέξαμε και της ταχύτητας του υπολογιστή μας θα χρειαστούν μερικά λεπτά εώς ώρες (ισχύει για μεγάλα σύνολα δεδομένων) μέχρις ότου ολοκληρωθεί η διαδικασία.

 Όταν ολοκληρωθεί η διαδικασία κρυπτογράφησης πατάμε 'Exit' για να επιστρέψουμε στην αρχική οθόνη του προγράμματος.

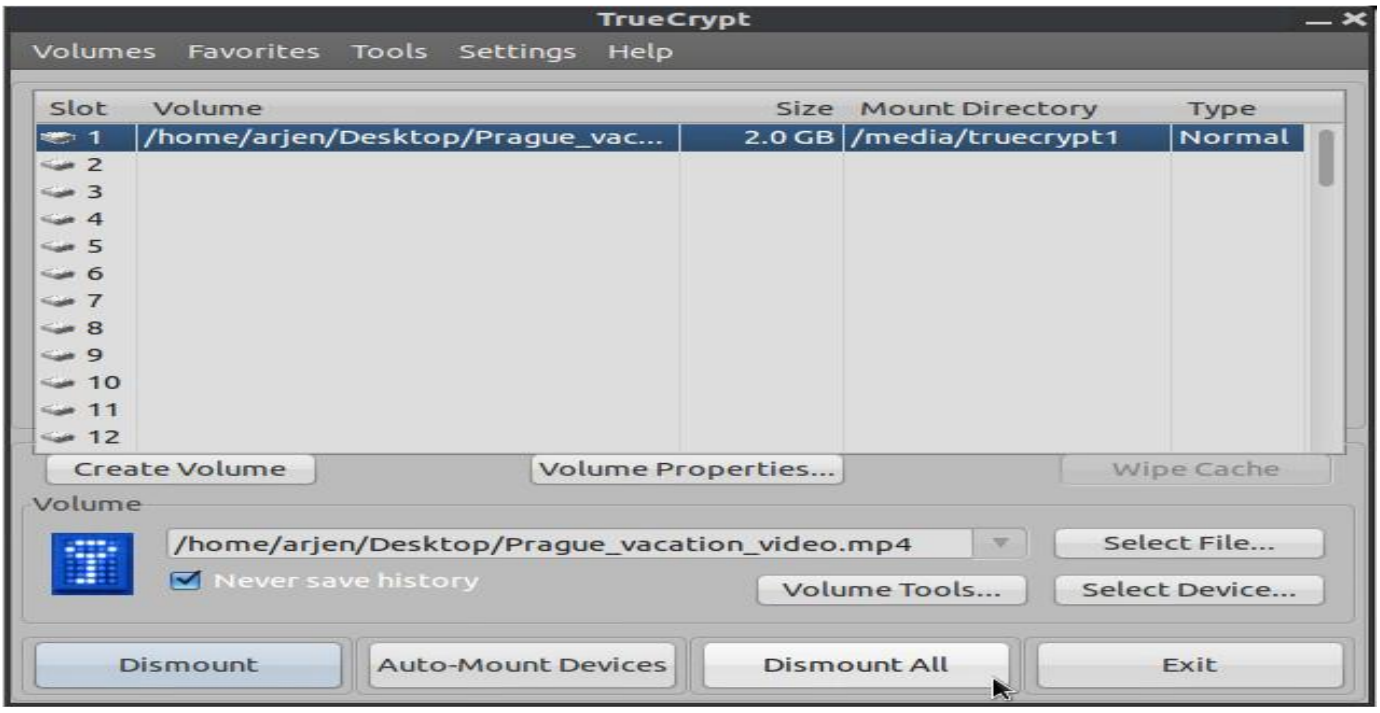
3. Τοποθετούμε τα αρχεία που θέλουμε να κρυπτογραφήσουμε στο νέο κρυπτογραφημένο πεδίο.

Πλέον το κρυπτογραφημένο πεδίο μπορεί να ενεργοποιηθεί. Επιλέγουμε 'Select File' > εντοπίζουμε κι επιλέγουμε το πεδίο που μόλις δημιουργήσαμε > κάνουμε κλικ στο 'Mount'.

Εισάγουμε τον κωδικό και πατάμε 'OK'.

Το αρχείο TrueCrypt θα εμφανιστεί στο σύστημά μας ως ένας ξεχωριστός δίσκος (όπως ένας δίσκος USB ή ένας εξωτερικός σκληρός δίσκος), και μπορούμε να εισάγουμε αρχεία σε αυτόν κατά τον ίδιο τρόπο που θα το κάναμε σε έναν δίσκο USB.

Όταν ολοκληρωθεί η διαδικασία εισαγωγής των αρχείων, κλείνουμε το κρυπτογραφημένο πεδίο κάνοντας κλικ στο 'Dismount' του TrueCrypt. Το κρυπτογραφημένο πεδίο θα εμφανίζεται πλέον όπως ένα απλό αρχείο στον υπολογιστή μας.



Μυστικά Κρυπτογραφημένα Σύνολα Δεδομένων

Τα μυστικά κρυπτογραφημένα σύνολα δεδομένων είναι κρυπτογραφημένα μη ανιχνεύσιμα πεδία μέσα σε ένα αρχείο TrueCrypt. Ο σκοπός αυτών είναι να παρέχουν ένα επιπλέον επίπεδο ασφαλείας. Αρχικά θα πρέπει να δημιουργηθεί ένας κωδικός για το εξωτερικό πεδίο του αρχείου TrueCrypt – το αρχείο που είναι ορατό στον φάκελό μας.

Μέσα στο πεδίο αυτό θα τοποθετηθούν ευαίσθητα αρχεία τα οποία πολύ πιθανόν να χρειάζονται κρυπτογράφηση για να διατηρηθούν ασφαλή. Μέσα στο συγκεκριμένο σύνολο δεδομένων υπάρχει ένα κρυμμένο πεδίο. Κανείς δεν μπορεί να τον δει, και απ' όσο γνωρίζουμε μέχρις στιγμής, ακόμα και ο πιο εξονυχιστικός έλεγχος δεν θα είναι σε θέση να αποκαλύψει την ύπαρξη του κρυμμένου πεδίου του TrueCrypt. Μόνο ο δημιουργός του γνωρίζει την ύπαρξή τους και μπορεί να έχει πρόσβαση στο συγκεκριμένο πεδίο με διαφορετικό κωδικό τον οποίο θα δημιουργήσει κατ' αποκλειστικότητα. Αυτός ο κωδικός θα πρέπει να διαφυλαχθεί με ιδιαίτερη προσοχή.

1. Δημιουργία του εξωτερικού πεδίου (όπως ανωτέρω)

Ξεκινάμε το TrueCrypt και επιλέγουμε:

 'Create Volume' > 'Create an encrypted container' > επιλέγουμε 'Hidden TrueCrypt volume' > επιλέγουμε την τοποθεσία που θέλουμε να αποθηκευτεί (μπορείτε να το μετακινήσετε αργότερα) και του δίνουμε ένα όνομα.

Για να κρυπτογραφήσετε έναν εξωτερικό σκληρό δίσκο, όπως π.χ. ένα USB stick, επιλέξτε 'Create Volume' > Create a volume within a partition/drive'

 Θα εμφανισθεί στην οθόνη ένα παράθυρο με τίτλο 'Encryption Options'. Οι προεπιλεγμένες επιλογές μας καλύπτουν σε αυτή τη φάση. Για ισχυρότερη κρυπτογράφηση (πολλαπλή κρυπτογράφηση), κάτω από το 'Encryption Algorithm, επιλέξτε 'AES twoFish-Serpent', και κάτω από το 'Hash Algorithm', επιλέξτε SHA-512.

 Στο επόμενο παράθυρο με τίτλο 'Volume size' επιλέξτε το μέγεθος του αρχείου (θα καθορίσει το μέγιστο όγκο δεδομένων που θα μπορείτε να αποθηκεύσετε σε αυτό).

 Ορίστε έναν κωδικό για το αρχείο σας στο επόμενο παράθυρο. Επιλέξτε έναν ισχυρό κωδικό (δείτε το κεφάλαιο 8).

 Το επόμενο παράθυρο έχει τίτλο Format Options. Επιλέξτε FAT.

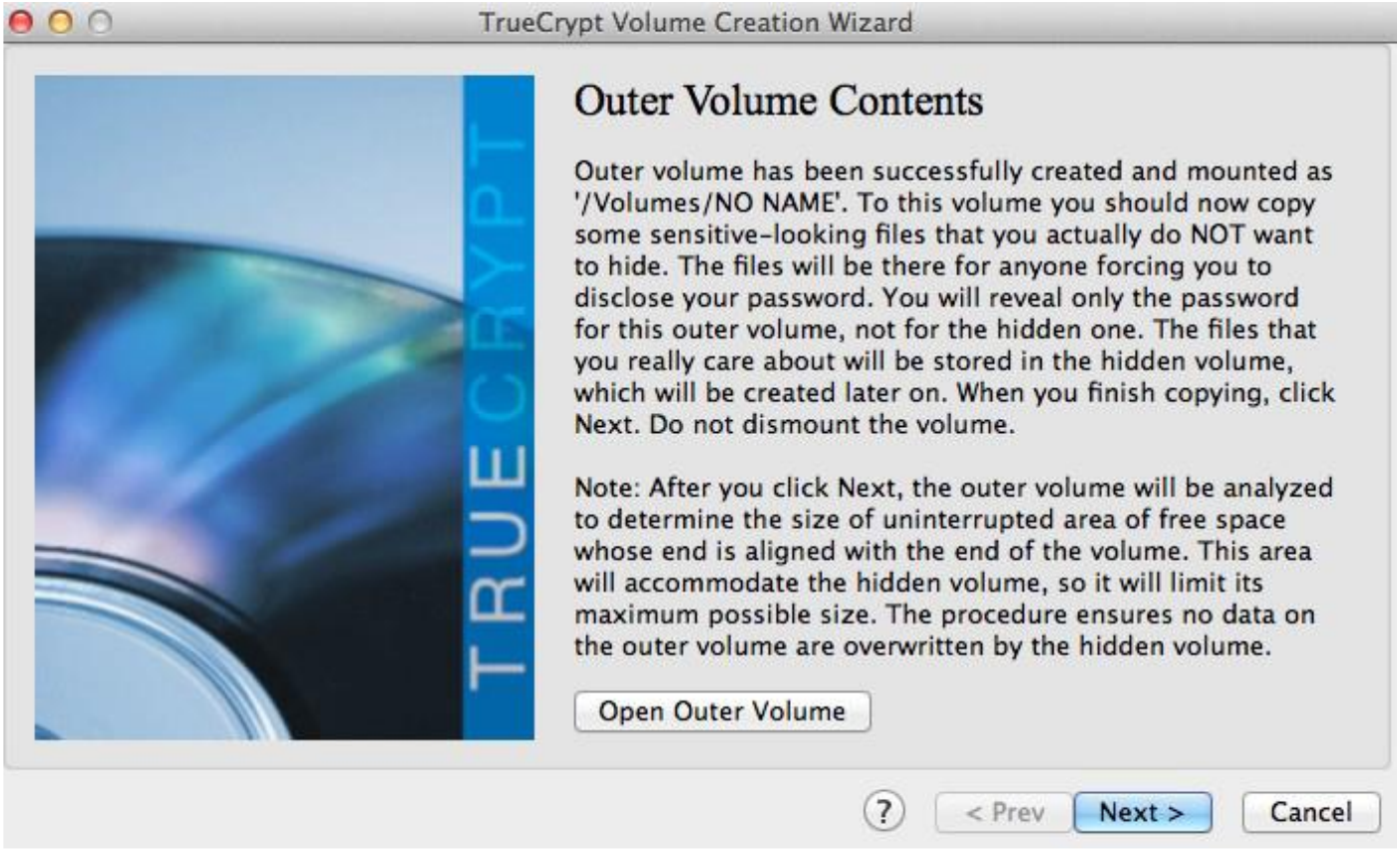
Επιπλέον πληροφορίες: Το FAT είναι συμβατό με όλα τα συστήματα αλλά περιορίζει το μέγεθος των δεδομένων που μπορεί να περιλάβει. (τα μεμονωμένα αρχεία δεν μπορούν να έχουν μέγεθος παραπάνω από 4 GB). Συνήθως αυτό δεν αποτελεί πρόβλημα. Εάν για εσάς είναι απαραίτητο να αποθηκεύσετε μεγαλύτερα αρχεία και είσθε σίγουροι ότι η επιλογή άλλης μορφής εκτός του FAT δεν θα σας δημιουργήσει προβλήματα, τότε επιλέξτε κάποιον άλλο τύπο από τις επιλογές.

 Το πρόγραμμα θα δημιουργήσει ένα τυχαίο σετ δεδομένων για να κρυπτογραφήσει το σύνολο. Κινείστε τυχαία τον κέρσορα του ποντικιού για ένα λεπτό, προτού επιλέξετε

‘Format’. Το πρόγραμμα θα δημιουργήσει το νέο πεδίο-φάκελο. Βάσει του μεγέθους, του αλγορίθμου κρυπτογράφησης που επιλέξατε και της ταχύτητας του υπολογιστή σας θα χρειασθούν μερικά λεπτά εώς ώρες (ισχύει για μεγάλους όγκους δεδομένων) μέχρις ότου ολοκληρωθεί η διαδικασία.

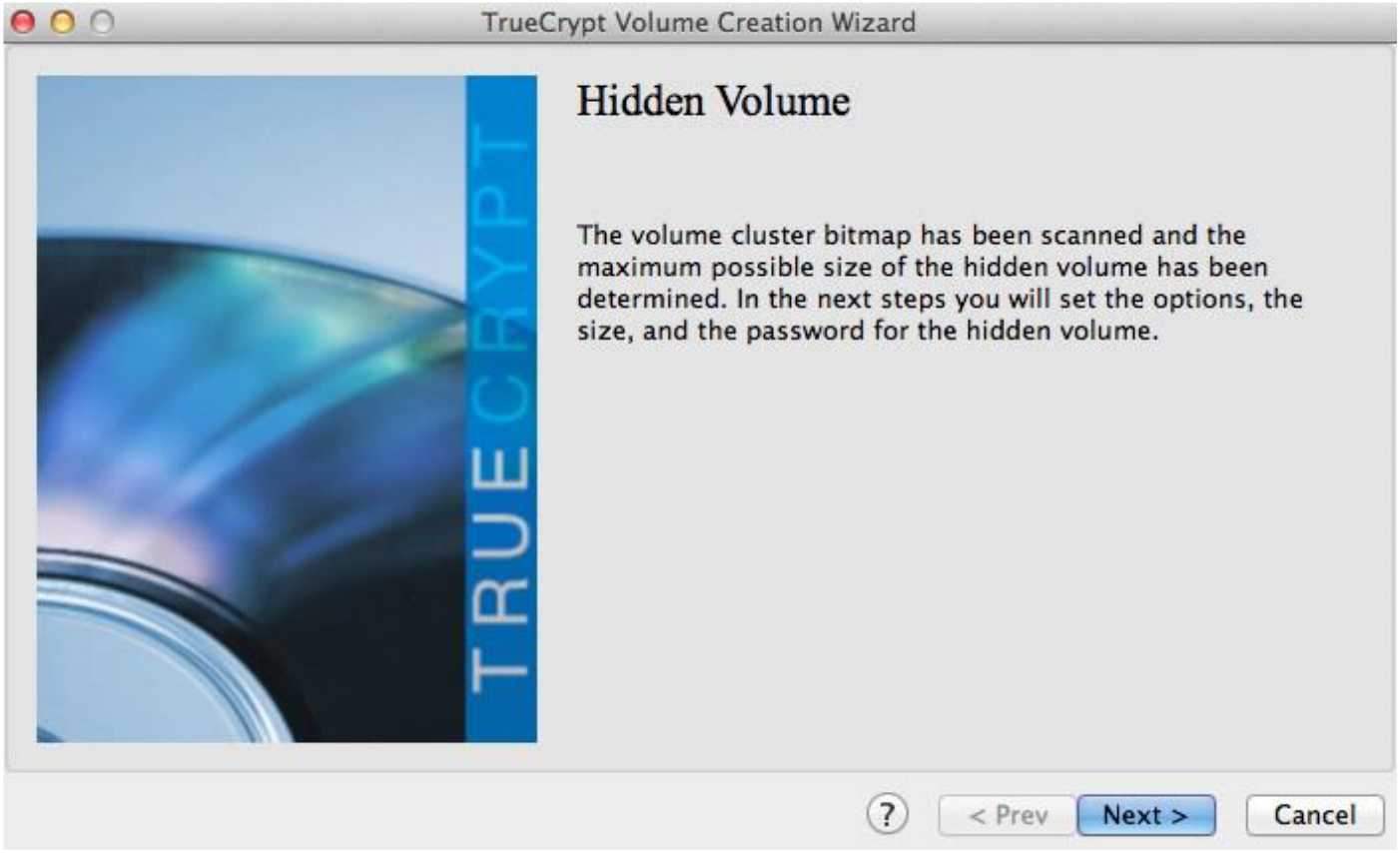
 Το επόμενο παράθυρο έχει τίτλο ‘Outer volume’ – πρέπει να διαβαστεί προσεκτικά. Πρέπει να αντιγραφούν μερικά αρχεία που μοιάζουν ευαίσθητα σε αυτό το σύνολο δεδομένων, π.χ. κάνοντας copy-paste μερικά αρχεία στο πεδίο TrueCrypt που εμφανίζεται στο My Computer/Finder). Έπειτα επιλέγουμε ‘Next’.

 Το επόμενο παράθυρο έχει τίτλο ‘Hidden Volume’. Το διαβάζουμε, και μετά πατάμε Next.



2. Δημιουργία του μυστικού συνόλου δεδομένων

Τώρα που έχει δημιουργηθεί το εξωτερικό πεδίο, θα λάβουμε οδηγίες για την δημιουργία του νέου κρυφού πεδίου. Θα ακολουθήσουμε την ίδια διαδικασία του προηγούμενου μέρους, αλλά αυτή τη φορά για το νέο πεδίο. Ακολουθούμε τα ίδια βήματα μέσω των παραθύρων ‘Encryption Options’, ‘Hidden Volume Size’ (η διαθεσιμότητα του χώρου εξαρτάται από το μέγεθος των αρχείων που έχουμε χρησιμοποιήσει ως δόλωμα στο εξωτερικό σύνολο δεδομένων), ‘Hidden Volume Password’ και ‘Format Options’.



Είναι σημαντικό να επιλεγεί διαφορετικός κωδικός για το μυστικό σύνολο από αυτόν που είχε επιλεγεί για το εξωτερικό. Ειδάλλως, εάν αυτοί οι δυο κωδικοί είναι ίδιοι, τότε θα υπάρξει πρόσβαση και στο μυστικό πεδίο.

3. Εισάγουμε τα αρχεία που θέλουμε να κρυπτογραφήσουμεστο μυστικό πεδίο

Πλέον το νέο πεδίο μπορεί να ενεργοποιηθεί. Επιλέγουμε 'Select File' > εντοπίζουμε κι επιλέγουμε το πεδίο που μόλις δημιουργήσαμε > κάνουμε κλικ στο 'Mount'.

Τώρα πληκτρολογούμε είτε τον κωδικό για το εξωτερικό πεδίο είτε για το μυστικό, αναλόγως σε ποιο επιθυμούμε να αποκτήσουμε πρόσβαση και πατάμε 'OK'.

Θα πρέπει να έχουμε υπόψη μας πως εάν προσθέσουμε περισσότερα αρχεία στο εξωτερικό πεδίο, μπορεί να υπερκαλύψουμε χώρο, ή δεδομένα του μυστικού πεδίου. Ιδανικά, δεν θα πρέπει να αλλαχθούν ή να προστεθούν επιπλέον δεδομένα στο εξωτερικό πεδίο μετά την δημιουργία του μυστικού πεδίου.

Το αρχείο TrueCrypt θα εμφανιστεί στο σύστημά ως ένας ξεχωριστός δίσκος (όπως ένας δίσκος USB ή ένας εξωτερικός σκληρός δίσκος), και μπορούν να εισαχθούν αρχεία σε αυτόν κατά τον ίδιο τρόπο που θα γινόταν σε έναν δίσκο USB.

Όταν ολοκληρωθεί η διαδικασία εισαγωγής των αρχείων, κλείνουμε το πεδίο επιλέγοντας 'Dismount' στο TrueCrypt. Το πεδίο θα εμφανίζεται πλέον όπως ένα απλό αρχείο στον υπολογιστή μας.

Κρυπτογράφηση σκληρών δίσκων

Τα συστήματα Mac και Linux έχουν προεγκατεστημένες επιλογές για την κρυπτογράφηση ενός ολόκληρου σκληρού δίσκου.

Linux/Ubuntu:

Ήδη απο το κεφάλαιο (2) το οποίο αναφέρεται στην εγκατάσταση των Ubuntu, δόθηκε η συμβουλή να κρυπτογραφείται η εγκατάσταση των Ubuntu 'encrypt the Ubuntu installation' καθώς και ο φάκελος Home 'encrypt the home folder'. Αυτές οι επιλογές κρυπτογραφούν ολόκληρο τον σκληρό δίσκο και τον φάκελο Home με ξεχωριστούς κωδικούς.

Mac:

Επιλέγουμε System Preferences > Security and Privacy > FireVault > Ενεργοποιούμε το FireVault

Windows:

Ο πιο ασφαλής τρόπος να κρυπτογραφηθεί ένας σκληρός δίσκος σε ένα σύστημα Windows είναι η χρήση του TrueCrypt.

Αυτή η μέθοδος είναι η ίδια με αυτή που περιγράφηκε παραπάνω, μόνο που για να ξεκινήσει η διαδικασία θα πρέπει να επιλέξουμε 'Create Volume' > 'Encrypt a nonsystem partition/drive' > 'Standard TrueCrypt volume' > Επιλέγουμε τον σκληρό δίσκο.

Αναλυτικές οδηγίες υπάρχουν στον σχετικό σύνδεσμο[33].

Ασφαλής διαμοιρασμός δεδομένων

Οι κίνδυνοι που ελοχεύουν κατα τον διαμοιρασμό δεδομένων είναι η παρακολούθηση, παρέμβαση, ενδεχόμενη καταστροφή των δεδομένων του αποστολέα/συνεργάτη, ενδεχόμενος προσδιορισμός του αποστολέα/συνεργάτη, καθώς και ενδεχόμενος προσδιορισμός της ταυτότητάς. Οι ενέργειες για την ενίσχυση της ασφάλειας κατα των διαμοιρασμό δεδομένων είναι α. η ανταλλαγή κρυπτογραφημένων δίσκων USB ή σκληρών δίσκων (εάν είναι δυνατή η συνάντηση πρόσωπο με πρόσωπο με τον παραλήπτη), β. η ανταλλαγή μικρού όγκου δεδομένων μέσω κρυπτογραφημένων συνημμένων με κρυπτογραφημένα emails, γ. Η ανταλλαγή μεγάλου όγκου κρυπτογραφημένων δεδομένων μέσω υπηρεσιών διαμοιρασμού αρχείων (file-sharing service).

[33] https://download.truecrypt.ch/documentation/TrueCrypt%20User%20Guide.pdf

Φυσική ανταλλαγή – Ανταλλαγή πρόσωπο με πρόσωπο

Η ασφαλέστερη μέθοδος διαμοιρασμού μεγάλου όγκου δεδομένων είναι η φυσική ανταλλαγή μιας συσκευής αποθήκευσης (ιδανικά ένας δίσκος USB ή ένας σκληρός δίσκος) που περιλαμβάνει τα δεδομένα σε κρυπτογραφημένη μορφή.

Μπορεί να κρυπτογραφηθεί ολόκληρη η συσκευή, ή ξεχωριστά οι φάκελοι που είναι αποθηκευμένοι μέσα σε αυτήν με ξεχωριστούς κωδικούς, έτσι ώστε η πρόσβαση σε αυτούς να πραγματοποιείται με ελεγχόμενο τρόπο από τον αποστολέα (ο οποίος μπορεί να παρέχει τους κωδικούς μέσω ασφαλών καναλιών, όπως τα κρυπτογραφημένα email ή το OTR-chat – δείτε τα κεφάλαια 5 και 6).

Έτσι, το μόνο που χρειαζόμαστε για να ανταλλάξουμε δεδομένα με κάποιο πρόσωπο είναι ένα λογισμικό κρυπτογράφησης (όπως το TrueCrypt) κι έναν δίσκο USB, οι οποίοι είναι πλέον πολύ φτηνοί, ακόμα κι αυτοί με μεγάλη χωρητικότητα.

Ηλεκτρονική ανταλλαγή

Εάν ένας χρήστης δεν μπορείτε να συναντηθείτε πρόσωπο με πρόσωπο με κάποιον για να ανταλλάξουν δεδομένα, θα χρειασθεί να το κάνει διαδικτυακά.

Μικροί όγκοι δεδομένων μπορούν να διαμοιρασθούν ως κρυπτογραφημένα συνημμένα κρυπτογραφημένων email, εάν και τα δυο πρόσωπα χρησιμοποιούν κρυπτογραφημένα email (δείτε το κεφάλαιο 5).

Μεγάλοι όγκοι δεδομένων μπορούν να κρυπτογραφηθούν, με τη χρήση του TrueCrypt για παράδειγμα, και στη συνέχεια να μετονομαστούν με ένα όνομα το οποίο δεν θα σχετίζεται με τη φύση των δεδομένων που εμπεριέχονται σε αυτό. Στη συνέχεια το αρχείο μεταφορτώνεται σε μια υπηρεσία διαμοιρασμού αρχείων, και αποστέλλεται στον παραλήπτη ένας σύνδεσμος για το online αρχείο και τον κωδικό (ή τους κωδικούς) για την αποκρυπτογράφηση του αρχείου μέσω ενός διαφορετικού ασφαλούς καναλιού.

Εάν το hardware ή το λειτουργικό σύστημα που χρησιμοποιούνται σε αυτή την περίπτωση δεν είναι ασφαλή, τα αρχεία που θα ανταλλάσσονται και οι κωδικοί που θα διαμοιράζονται ενδεχομένως να είναι και αυτά επισφαλή – ένας κακόβουλος χρήστης θα μπορούσε να αποκτήσει απομακρυσμένη πρόσβαση ή έλεγχο του υπολογιστή.

Ιδανικά, θα πρέπει να ανταλλάσσονται έγγραφα μεταξύ ασφαλών συστημάτων, όπως το Tails. Για μέγιστη ασφάλεια, θα πρέπει να υπάρχει πρόσβαση σε έγγραφα μόνο από ένα air-gapped μηχάνημα.

Mega

Το 'Mega'[34] προτείνεται ως μια εναλλακτική πλατφόρμα διαμοιρασμού αρχείων, ακριβώς όπως είναι το Dropbox και το Google Drive.

Το Mega χρησιμοποιεί κρυπτογράφηση μεταξύ του browser προτού το αρχείο μεταφορτωθεί για να προστατεύσει τον χρήστη από υποκλοπές αλλά και για την νόμιμη προστασία του ίδιου του Mega ενάντια σε κατηγορίες για την παράβαση των πνευματικών δικαιωμάτων (εφόσον δεν μπορούν να έχουν πρόσβαση και να γνωρίζουν το περιεχόμενο των αρχείων που διαμοιράζονται). Η κρυπτογράφησή προσθέτει ένα λεπτό προστατευτικό στρώμα ενάντια στην υποκλοπή δεδομένων, όπως γίνεται μέσω μιας ανοιχτής σύνδεσης μέσω Wi-Fi στο καφέ ή στην βιβλιοθήκη της επιλογής σας. Όπως οι περισσότεροι πάροχοι υπηρεσιών διαμοιρασμού αρχείων, το Mega παρέχει χωρητικότητα 50 GB για κάθε μοναδική διεύθυνση email. Όπως και με κάθε άλλη πτυχή της ασφάλειας πληροφοριακών συστημάτων, ο κατακερματισμός των δεδομένων σε διαφορετικούς, μη συσχετιζόμενους λογαριασμούς συνιστάται.

SecureDrop

Υπάρχουν ορισμένοι οργανισμοί, κατά κύριο λόγο ειδησεογραφικοί, με αρκετούς πόρους και επενδύσεις σε τεχνολογίες πληροφορικής οι οποίοι έχουν υιοθετήσει τα δικά τους συστήματα για να διαμοιράζονται με ασφάλεια τα αρχεία τους – ένα απο αυτά τα συστήματα είναι το SecureDrop, το οποίο είναι ένα σύστημα υποβολής καταγγελιών ανοιχτού πηγαίου κώδικα. Παρόλο αυτά, η δημιουργία τέτοιων συστημάτων, καθώς και η τήρηση της ασφάλειάς τους, είναι ένα ζήτημα μείζονος σημασίας και θα πρέπει να πραγματοποιείται από ειδικούς με μεγάλη εμπειρία.

OnionShare

Το OnionShare είναι ένα ανοιχτού πηγαίου κώδικα εργαλείο που επιτρέπει ανώνυμα και με ασφάλεια (μέσω του δικτύου Tor) να διαμοιράζονται αρχεία οποιουδήποτε μεγέθους. Πρόκειται για μια αρκετά ρεαλιστική λύση για τους ανεξάρτητους χρήστες.

Ασφαλής διαγραφή αρχείων

Στα περισσότερα συστήματα, η διαγραφή ενός αρχείου δεν αφαιρεί επί της ουσίας τα δεδομένα από τον σκληρό δίσκο του υπολογιστή (ή τον δίσκο USB, εάν έχουν αποθηκευθεί εκεί). Το αρχείο εξακολουθεί να υπάρχει αλλά ο χώρος που καταλαμβάνει έχει σηματοδοθεί ως 'no longer in use', και τελικώς θα ξαναχρησιμοποιηθεί και θα αντικατασταθεί από άλλα αρχεία. Παρόλο αυτά, μέχρι τότε, τα διεγραμμένα αρχεία μπορούν να ανακτηθούν με τα σωστά εργαλεία και την κατάλληλη τεχνογνωσία.

[34] https://mega.co.nz/

Για να διαγραφούν αυτά τα αρχεία, είναι δυνατό να χρησιμοποιηθούν ειδικά εργαλεία που θα αντικαταστήσουν τα αρχεία αυτά με τυχαία δεδομένα. Αυτή η μέθοδος είναι αρκετά ασφαλής, αλλά μπορεί να καταναλώσει πολύ χρόνο για μεγάλους όγκους δεδομένων.

Mac

Ασφαλής διαγραφή αρχείων:

Αφού τοποθετηθεί το αρχείο στον κάδο ανακύκλωσης (Trash), ανοίγουμε τον φάκελο (κάντε κλικ στο εικονίδιο του κάδου), πηγαίνουμε στην αναζήτηση (Finder) (στο μενού στην πάνω αριστερή γωνία) κι επιλέγουμε 'Secure Empty Trash'. Όλα τα αρχεία του κάδου θα διαγραφούν από το ευρετήριο του Mac (directory), και ο χώρος του σκληρού δίσκου θα υπερκαλυφθεί με τυχαία δεδομένα.

Ασφαλής εκκαθάριση USB δίσκου (ή οποιουδήποτε εξωτερικού σκληρού δίσκου):

Εισάγυομε τον δίσκο USB. Ξεκινάμε το 'Disk Utility' > επιλέγουμε τον δίσκο που θέλουμε να διαγράψουμε (απο το μενού στα αριστερά) > επιλέγουμε 'Erase'. Επιλέγουμε στη συνέχεια 'Security Options' και 'Most Secure'* > 'OK' > "Erase'.

Ασφαλής εκκαθάριση όλου του ελεύθερου χώρου του σκληρού δίσκου ενός Mac:

Με αυτή τη διαδικασία αναζητούνται οι περιοχές του δίσκου που είναι καθορισμένες ως διαθέσιμες για νέα δεδομένα και υπερκαλύπτονται από τυχαία δεδομένα.

Ξεκινάμε το 'Disk Utility' > Επιλέγουμε τον δίσκο που θέλουμε να διαγράψουμε (απο το μενού στα αριστερά) > επιλέγουμε 'Erase' > κάνουμε κλικ στο 'Erase Free Space'.

Θα εμφανισθεί ένα παράθυρο με τίτλο 'Erase Free Space Options' – επιλέγουμε 'Most Secure'* και κάνουμε κλικ το 'Erase Free Space'.

*(Σε μερικές εκδόσεις των Mac OS, θα εμφανιστεί η επιλογή '35-Pass Erase of Deleted Files').

Windows, Linux/Ubuntu

Για τα συστήματα Linux και Windows, υπάρχει το BleachBit[35] , ένα εργαλείο εκκαθάρισης ανοιχτού πηγαίου κώδικα, θεωρείται εξαιρετικά αξιόπιστο.

[35] http://bleachbit.sourceforge.net/

Tails

Το λειτουργικό Tails διαθέτει ένα ασφαλές εργαλείο εκκαθάρισης το οποίο είναι εύκολα προσβάσιμο κάνοντας δεξί κλικ πάνω στο αρχείο και επιλέγοντας 'Wipe'. Μπορεί να διαγραφεί όλος ο ελεύθερος χώρος ενός φακέλου με ασφάλεια κάνοντας δεξί κλικ μέσα στον φάκελο και επιλέγοντας 'Wipe available diskspace'.

Φυσική διαγραφή

Εάν υπάρχει η επιθυμία να διαγραφεί ένας ολόκληρος δίσκος, υπάρχει και η επιλογή της φυσικής καταστροφής της συσκευής αποθήκευσης. Για να είμαστε σίγουροι ότι κανένα δεδομένο δεν θα μπορέσει να ανακτηθεί θα πρέπει να διαλυθεί η συσκευή αποθήκευσης σε κομμάτια μικρότερα του 1 mm. Μην θεωρείτε ότι μπορείτε Απλά σπάζοντας τον δίσκο με ένα σφυρί ή βρέχοντάς τον, μπορεί τουνα καταστρέψουμε την λειτουργικότητα του δίκσου αλλά δεν μπορούμε να υπερνικήσουμε ορισμένες προηγμένες μεθόδους ανάκτησης δεδομένων.

Επιλογή δίσκων USB

Εφόσον η αποθήκευση δεδομένων στον εσωτερικό δίσκο ενός λάπτοπ εκθέτει τα δεδομένα σε επιπλέον κινδύνους και καθιστά την ασφαλή διαγραφή τους δύσκολη, το να αποθήκευουμε τα ευαίσθητα αρχεία μας σε έναν εξωτερικό δίσκο μεσαίου μεγέθους, όπως είναι ένας δίσκος USB ή ένας εξωτερικός σκληρός δίσκος (για μεγάλους όγκους δεδομένων) συνιστάται ως ασφαλής μέθοδος. Η κρυπτογράφηση αυτών των συσκευών είναι πολύ σημαντική για την προστασία τους.

Μεταδεδομένα (Metadata)

Τα μεταδεδομένα είναι τα δεδομένα των δεδομένων. Τα μεταδεδομένα μπορεί να περιλαμβάνουν τον συγγραφέα ενός Microsoft Word εγγράφου, ή τα στοιχεία GPS της τοποθεσίας στην οποία λήφθηκε μια φωτογραφία. Τα αρχεία ήχου, βίντεο, και τα PDF επίσης περιλαμβάνουν μεταδεδομένα και κρυμμένα δεδομένα (όπως σχόλια, ή ιστορικό αναζήτησης, ονόματα αρχείων κ.λπ.).

Οι περισσότεροι έγχρωμοι εκτυπωτές laser εκτυπώνουν το μοντέλο τους και τον σειριακό αριθμό τους με μικροσκοπικές τελείες σε κάθε τετραγωνικό εκατοστό του χαρτιού – ούτως ώστε τα έγγραφα αυτά να είναι ανιχνεύσιμα εάν ο σειριακός αριθμός του εκτυπωτή είναι συνδεδεμένος με τον χρήστη με οποιονδήποτε τρόπο (π.χ. εάν παραγγείλατε τον εκτυπωτή online).

Κάθε πρόγραμμα που χρησιμοποιείται μπορεί να έχει ορισμένες ρυθμίσεις μεταδεδομένων, έτσι κάθε φορά που κάνουμε μια έρευνα online (ή απευθυνόμαστε σε κάποιον ειδικό) οποιοδήποτε πρόγραμμα και αν χρησιμοποιήσουμε και οποιοδήποτε

αρχείο σκοπεύουμε να αποθηκεύσουμε, πρέπει να έχουμε κατά νου πάντοτε τι είδους πληροφορίες αποθηκεύουμε, πώς μπορούμε να τις διαγράψουμε και τον τρόπο με τον οποίο μπορουμε να σιγουρευτούμε ότι το υλικό αυτό είναι αβλαβές.

LibreOffice

Το LibreOffice[36] είναι ένα δωρεάν πρόγραμμα ανοιχτού κώδικα.

Στο LibreOffice, τα δεδομένα του χρήστη είναι εμφανή και μπορούν να διαγραφούν επιλέγοντας: File > Properties > General tab

 Κάνουμε κλικ στο 'Reset' για να τροποποιήσουμε τα γενικά δεδομένα χρήστη (π.χ. συνολικός χρόνος επεξεργασίας, αριθμός επαναλήψεων)

 Αποεπιλέγουμε το 'Apply user data'καικατόπιν επιλέγουμε 'Description' και 'Custom Properties' και διαγράφουμε τα δεδομένα που δεν θέλουμε να μοιράζονταιε. Κάτω από το 'Security', αποεπιλέγουμε το 'Record changes' εάν δεν είναι ήδη αποεπιλεγμένο. Κάτω από το Edit > Changes > Accept or Reject: μπορούμε να τα διαγράψουμε εάν ο παραλήπτης δεν τα χρειάζεται.

Εάν χρησιμοποιείται το χαρακτηριστικό Versions, επιλέγουμε File > Versions και διαγράφουμε όλες τις παλαιότερες εκδόσεις του αρχείου που ενδέχεται να είναι αποθηκευμένες εκεί.

(Μόνο για τον Writer) View > Hidden Paragraphs, ελέγχουμε όλες τις κρυμμένες παραγράφους που είναι εμφανείς.

(Μόνο για το Calc) Format > Sheet, ελέγχουμε εάν υπάρχουν κρυμμένα φύλλα.

[36] https://www.libreoffice.org/

Κεφάλαιο 5: Email

Το Email είναι ο πιο πιθανός τρόπος που επιλέγουν οι χρήστες για να επικοινωνούν με τους συναδέλφους και τους συνεργάτες τους. Είναι άκρως απαραίτητο να υπάρχει ένα ασφαλές email, όχι μόνο για την καθημερινή χρήση αλλά και ως ένα ασφαλές κανάλι για τις αρχικές επαφές με πιθανούς συνεργάτες.

Οι κίνδυνοι για τις επικοινωνίες μέσω email περιλαμβάνουν τις εξής ενέργειες στις οποίες μπορεί να προβεί ο εκάστοτε κακόβουλος χρήστης:

 Ανάγνωση του περιεχομένου του email

 Ανάγνωση του θέματος και των κεφαλίδων

 Παρακολούθηση των επαφών καθώς και της συχνότητας με την οποία επικοινωνούν οι χρήστες

 Υποκλοπή των συνημμένων αρχείων από τα email Επιθέσεις "Man in the middle" (ένας μιμητής υποκλέπτει τις συνομιλίες)

 Παρακολούθηση της τοποθεσίας από την οποία στέλνονται τα email

Ενέργειες Ασφάλειας Πληροφοριακών Συστημάτων:

 Χρήση ισχυρών κωδικών

 Χρήση αξιόπιστου παρόχου email

 Κρυπτογράφηση email

 Επιβεβαίωση κλειδιών

 Αναφορά ελάχιστων πληροφοριών στα θέματα των emails

 Αποστολή Email μέσω Tails (εάν και εφόσον κριθεί απαραίτητο)

 Χρήση ανώνυμων διευθύνσεων email για συγκεκριμένους σκοπούς

Κίνδυνοι

Για την προστασία ενάντια στις πιο κοινότοπες επιθέσεις, η χρήση ενός ισχυρού κωδικού πρόσβασης αποτελεί μια καλή άμυνα ενάντια στην μη εξουσιοδοτημένη πρόσβαση τρίτων σε έναν λογαριασμό email. Παρόλα αυτά, σε ορισμένες περιπτώσεις, αυτό από μόνο του δεν αποτελεί καμία απολύτως άμυνα.

Ένας πάροχος email θεωρείται αξιόπιστος όταν έχει καλές υποδομές ασφαλείας, και φυσικά δεν θα παραδώσει ποτέ τα δεδομένα που διαχειρίζεται σε καμία υπηρεσία πληροφοριών. Εάν οι χρήστες δεν εμπιστεύονται την χώρα στην οποία βρίσκεται ο πάροχος που έχουν επιλέξει, τότε δεν θα πρέπει να χρησιμοποιείται καμία διεύθυνση email

του συγκεκριμένου παρόχου. Για παράδειγμα, γνωρίζουμε πως η τακτική των υπηρεσιών πληροφοριών της Μεγάλης Βρετανίας και των Η.Π.Α. είναι να καταγράφουν και να αποθηκεύουν όσο το δυνατόν περισσότερες επικοινωνίες μέσω email μπορούν. Ακόμα και αν αισθανόμαστε πως οι επικοινωνίες μας δεν ενδιαφέρουν αυτές τις υπηρεσίες στο παρόν, θα πρέπει να έχουμε κατά νου πως οι επικοινωνίες μπορούν να γίνουν προσβάσιμες από τις συγκεκριμένες υπηρεσίες ακόμα και αν το έργο μας αποκτήσει σημασία για αυτούς κάποια στιγμή στο μέλλον. Έτσι, εάν δεν εμπιστευόμαστε την τακτική που ακολουθεί η αμερικάνικη υπηρεσία πληροφοριών όσον αφορά την ιδιωτικότητα των email, δίνουμε ιδιαίτερη προσοχή στους πάροχους που εδρεύουν εκεί (Outlook, Gmail, Riseup, κ.λπ.). Μερικοί πάροχοι email είναι περισσότερο συνεργάσιμοι από ότι άλλοι, αλλά - εκτός και αν έχουμε τον δικό μας server (ή η εταιρεία / οργανισμός στον οποίο εργαζόμαστε έχει τον δικό του server σε χώρες με καλή πολιτική όσον αφορά την ιδιωτικότητα, όπως είναι η Σουηδία ή η Ισλανδία), θεωρούμε πως τα emails και τα μεταδεδομένα των email δεν είναι ασφαλή οποιονδήποτε πάροχο κι εάν επιλέξουμε. Ακόμα θα πρέπει να προσέχουμε τα στοιχεία που ζητούνται από τον πάροχο για να ανοιχθεί ένας λογαριασμός, όπως ο αριθμός του κινητού τηλεφώνου, ο ταχυδρομικός κώδικας ή η διεύθυνση, ή κάποιο άλλο email, και το κατά πόσο είμαστε διατεθείμενοι να παρέχουμε αυτού του είδους τις πληροφορίες (και ειδικά έαν κι εφόσον χρησιμοποιείται μια ανώνυμη διεύθυνση email).

Μεταδεδομένα Email

Όπως αναφέρθηκε και σε προηγούμενο κεφάλαιο, τα μεταδεδομένα είναι τα δεδομένα των δεδομένων. Τα μεταδεδομένα του Email περιλαμβάνουν τα ονόματα τόσο του αποστολέα όσο και του παραλήπτη, τις διευθύνσεις Emails και τις IP διευθύνσεις τους, πληροφορίες των server, ημερομηνία, ώρα και ζώνη ώρας, το μοναδικό αναγνωριστικό του email καθώς και των σχετιζόμενων με αυτό emails, τον τύπο του περιεχομένου, την κωδικοποίηση, την προτεραιότητα και τις κατηγορίες, το θέμα του email, την κατάσταση του email, και κάθε αίτημα ανάγνωσης παραλαβής του μηνύματος.

Αυτές οι πληροφορίες είναι εκτενείς και αποκαλυπτικές από μόνες τους, αλλά πολλές υπηρεσίες πληροφοριών και νομικές υπηρεσίες (και σε μερικές περιπτώσεις ακόμη και hackers) είναι σε θέση να ανακτήσουν το πλήρες περιεχόμενου ενός email.

Συνεπώς,δεν είναι εύκολο να προστεύσουμε τα μεταδεδομένα των emails μας, άρα θα πρέπει να παρέχουμε όσο το δυνατόν λιγότερες ή ασαφείς πληροφορίες στο θέμα του μηνύματός μας, και ίσως να αποκρύψουμε την πραγματική τοποθεσία μας ή την IP διεύθυνση χρησιμοποιώντας τον Tor browser, παρόλο που πλέον οι περισσότεροι πάροχοι υπηρεσιών ηλεκτρονικού ταχυδρομίου δεν αποκαλύπτουν την ακριβή τοποθεσία (IP) του εκάστοτε χρήστη στο view source.

Για παράδειγμα,οι κρατικές υπηρεσίες των ΗΠΑ αιτήθηκαν πρόσβασης στα μεταδεδομένα ενός ανώνυμου χρήστη του Lavabit[37], ενός ασφαλούς πάροχου email, καθώς και τα ιδιωτικά κλειδιά κρυπτογράφησης της εταιρείας (που επιτρέπει την πρόσβαση στους κωδικούς των χρηστών) το καλοκαίρι του 2013. Πιθανότατα, ζήτησαν άδεια επειδή δεν κατάφεραν να την αποκτήσουν μόνοι τους. Η επιχείρηση παραβίασης θεωρείται πως έγινε επειδή ο πληροφοριοδότης της NSA Edward Snowden διατηρούσε έναν λογαριασμό email στο Lavabit. Στον ιδρυτή του Lavabit απαγορεύθηκε νομίμως να ανακοινώσει τα ακριβή αιτήματα της αμερικάνικης κυβέρνησης. Αντί να επιτρέψει την παραβίαση των δικαιωμάτων ιδιωτικότητας των χρηστών, ο ιδρυτής[38] προτίμησε να ανασταλεί ολόκληρη η λειτουργία του Lavabit, τον Αύγουστο του 2013.

Κρυπτογράφηση Email

Η ιδιωτικότητα του περιεχομένου ενός email μπορεί να προστατευτεί χρησιμοποιώντας 'δημόσια κλειδιά κρυπτογράφησης'. Τα δημόσια κλειδιά κρυπτογράφησης κατακερματίζουν το περιεχόμενο ενός email] σε έναν άθραυστο κώδικα χρησιμοποιώντας το δημόσιο κλειδί του παραλήπτη. Το κρυπτογραφημένο email μπορεί με αυτό τον τρόπο να αποκρυπτογραφηθεί μόνο χρησιμοποιώντας το ιδιωτικό κλειδί του παραλήπτη.

Οι παρακάτω ενέργειες αναφέρονται στο GNU Privacy Guard[39], το 'GPG' (μια εφαρμογή ανοιχτού κώδικα του Pretty Good Privacy, ή PGP[40]).

Η χρήση του GPG, ενώ διαφέρει πολύ από την τυπική αποστολή email, δεν είναι δύσκολο να εφαρμοστεί και η κατανόηση της λειτουργίας του μοιάζει με πρόκληση.

Ζεύγη κλειδιών

Τα κλειδιά είναι ουσιαστικά ένας μοναδικός και μεγάλος συνδυασμός αριθμών, και κάθε χρήστης κρυπτογράφησης email έχει ένα ζεύγος κλειδιών – ένα δημόσιο κλειδί και ένα ιδιωτικό.

Δημόσιο κλειδί: Το δημόσιο κλειδί είναι αυτό που θα χρησιμοποιήσουν οι άλλοι χρήστες για να κρυπτογραφήσουν τα emails που θα στείλουν. Όπως ακριβώς αποθηκεύεται ένας αριθμός τηλεφώνου στο ευρετήριό, έτσι κι εδώ μπορεί να αποθηκευτεί το δημόσιο κλειδί στον δημόσιο keyserver ή όχι (εάν πρόκειται για έναν μυστικό ή ανώνυμο λογαριασμό email, δεν συνιστάται η αποθήκευση του δημόσιου κλειδιού στον keyserver). Εάν αποθηκευτεί το δημόσιο κλειδί στον keyserver, θα είναι διαθέσιμο έτσι ώστε να μπορεί ο καθένας να επικοινωνήσει με ασφάλεια.

[37] https://en.wikipedia.org/wiki/Lavabit
[38] http://www.theguardian.com/commentisfree/2014/may/20/why-did-lavabit-shut-down-snowden-email
[39] https://www.gnupg.org/download/
[40] http://www.pgpi.org/

Ιδιωτικό κλειδί: Το ιδιωτικό κλειδί επιτρέπει την αποκρυπτογράφηση των emails που λαμβάνουμε από άλλους, οι οποίοι έχουν χρησιμοποιήσει το δημόσιο κλειδί μας. Παρόλο που το δημόσιο κλειδί μας είναι διαθέσιμο και ελεύθερα προσβάσιμο, το ιδιωτικό μας κλειδί είναι ιδιωτικό. Το ιδιωτικό κλειδί επικοινωνεί με το δημόσιο κλειδί, διασφαλίζοντας πως κανένα τρίτο πρόσωπο δεν μπορεί να έχει μη εξουσιοδοτημένη χρήση του δημόσιου κλειδιού μας. Πολύ πιθανό να μην δούμε ποτέ το ιδιωτικό μας κλειδί – βρίσκεται και λειτουργεί κάτω από το bonnet του GPG.

Το μήκος, η τυχαιότητα, και η πολυπλοκότητα της κρυπτογράφησης του δημόσιου κλειδιού (4096 bit keys, όπως θα δούμε παρακάτω) πρέπει είναι τέτοια ούτως ώστε η κρυπτογράφηση να παραμένει άθραυστη.

Επιβεβαίωση κλειδιών

Είναι σημαντικό να επιβεβαιώνεται πάντα ότι τα κλειδιά που χρησιμοποιούνται ανήκουν στους παραλήπτες στους οποίους στέλνουμε το κρυπτογραφημένο μήνυμά μας. Παρόλο που η διεύθυνση email μπορεί όντως να ανήκει στο πρόσωπο που θέλουμε να στείλουμε το μήνυμά, υπάρχει μια μικρή πιθανότητα (σε περιπτώσεις υψηλού κινδύνου) το δημόσιο κλειδί που εμφανίζεται να μην είναι δικό του. Αυτές είναι γνωστές ως επιθέσεις 'Man-In-The-Middle' (MITM) – η συγκαλυμμένη υποκλοπή των επικοινωνιών με την πλαστογράφηση του στόχου. Επομένως, θα πρέπει να σιγουρευτούμε ότι τόσο η διεύθυνση email όσο και το δημόσιο κλειδί ανήκουν στο πρόσωπο με το οποίο θέλουμε να επικοινωνήσουμε.

Προστασία ταυτότητας και τοποθεσίας κατά την αποστολή email

Σε περιπτώσεις υψηλού κινδύνου, όσοι επιθυμούν να αποκρύψουν την πραγματική τους ταυτότητα ή/και την ταυτότητα των προσώπων με τα οποία επικοινωνούν, θα πρέπει να χρησιμοποιήσουν ανώνυμους λογαριασμούς email, οι οποίοι φυσικά δεν θα πρέπει να σχετίζονται με κανέναν τρόπο με την πραγματική τους ταυτότητα. Το Gmail και το Hotmail συνηθίζουν να ζητούν έναν αριθμό κινητού τηλεφώνου ή ένα εναλλακτικό email κατά την διαδικασία δημιουργίας νέου λογαριασμού, έτσι δεν ενδείκνυνται για τη δημιουργία ανώνυμων λογαριασμών. Σε πολλές χώρες, το GMX και το Yandex επιτρέπουν στους χρήστες να δημιουργήσουν λογαριασμό χωρίς να παρέχουν τέτοιου είδους πληροφορίες.

Ωστόσο, εάν δημιουργήσουμε έναν ανώνυμο λογαριασμό email όσο είμαστε συνδεδεμένοι στο διαδίκτυο με τρόπο που σχετίζεται με την πραγματική μας ταυτότητα, η ανωνυμία μας τίθεται σε κίνδυνο. Επιπλέον, όταν στέλνουμε ή λαμβάνουμε emails, και είμαστε συνδεδεμένοι στο διαδίκτυο – η τοποθεσία μας είναι γνωστή στον διαδικτυακό πάροχο που χρησιμοποιούμε. Εάν θέλουμε να παραμείνουν άγνωστες η ταυτότητα και η τοποθεσία μας, μπορούμε να χρησιμοποιήσουμε έναν ανώνυμο λογαριασμό για να στείλουμε κρυπτογραφημένα emails μέσω του webmail του Tor browser (κεφάλαιο 3), ή

μπορούμε να χρησιμοποιήσουμε το λειτουργικό Tails, το οποίο αποκρύπτει την πραγματική τοποθεσία όλων των επικοινωνιών που πραγματοποιούνται από ένα λάπτοπ μέσω διαδικτύου (δείτε το κεφάλαιο 2). Το Tails μέσω του email client (το οποίο υποστηρίζει την κρυπτογράφηση) στέλνει και λαμβάνει πληροφορίες/mail από και προς το διαδίκτυο μέσω του δικτύου Tor, με αποτέλεσμα να αποκρύπτει την πραγματική τοποθεσία της σύνδεσης.

Ίσως επιθυμείτε περισσότερο να αποκρύψετε την τοποθεσία σας παρά την ταυτότητά σας. Στην περίπτωση που μας ενδιαφέρει να αποκρύψουμε περισσότερο την τοποθεσία μας παρά την ταυτότητα μας, η μόνη λύση είναι το λειτουργικό σύστημα Tails.

Βασικές σημειώσεις για την κρυπτογράφηση των email

Πρέπει να ληφθεί υπόψη ότι η κρυπτογράφηση των email δεν αποκρύπτει τα μεταδεδομένα όπως τον παραλήπτη του μηνύματος, το θέμα του email, ή την τοποθεσία (εκτός και αν, όπως αναφέρεται παραπάνω, αποκρύπτεται η τοποθεσία χρησιμοποιώντας Tor/Tails). Σε περιπτώσεις υψηλού κινδύνου, μια καλή επιλογή είναι η αναφορά όσο το δυνατόν λιγότερων πληροφοριών ή ασαφών πληροφοριών στο θέμα του μηνύματος. Δεν μπορούμε να κρυπτογραφήσουμε ή να αποκρυπτογραφήσουμε ένα email από το κινητό μας τηλέφωνο. Παρόλο που σε μερικά κινητά Android υπάρχει αυτή η ρύθμιση, δεν ενδείκνυται καθώς τα κινητά τηλέφωνα είναι εξαιρετικά επίφοβα και ανασφαλή (δείτε το κεφάλαιο 7).

Επίσης δεν μπορούμε να κρυπτογραφήσουμε ή να αποκρυπτογραφήσουμε ένα mail στον web browser, παρα μόνο νααν χρησιμοποιούμε Tails.Με αυτή την εφαρμογή θα χρησιμοποιήσουμε το Thunderbird email client στον υπολογιστή μας, με το πρόσθετο λογισμικό κρυπτογράφησης, για να κρυπτογραφήσουμε ή να αποκρυπτογραφήσουμε ένα Mail.

Τέλος, μπορούμε να στείλουμε κρυπτογραφημένα μηνύματα σε τρίτους που επίσης χρησιμοποιούν κρυπτογραφημένα email. Αυτοί οι χρήστες ήταν μια μικρή κοινότητα στην προ-Snowden εποχή, αλλά τώρα ο αριθμός τους αυξάνεται ραγδαία.

Οδηγίες εγκατάστασης για την κρυπτογράφηση email

1.1. UBUNTU/LINUX: Thunderbird email client και λογισμικό κρυπτογράφησης GPG

Στα Ubuntu υπάρχει προεγκατεστημένο το Thunderbird (email client) και το λογισμικό κρυπτογράφησης GPG και μπορεί να βρεθεί χρησιμοποιώντας το εργαλείο αναζήτησης των Ubuntu στο μενού της επάνω αριστερής γωνίας στην επιφάνεια εργασίας.

1.1. MAC: Thunderbird email client και το λογισμικό κρυπτογράφησης GPG

Θα χρειαστεί να κατέβει:

 Ένας email client/mail manager για τον υπολογιστή –προτείνουμε το πρόγραμμα ανοιχτού κώδικα της Mozilla, το 'Thunderbird'[41]

 το GPG[42] – Gnu Privacy Guard, το οποίο είναι λογισμικό κρυπτογράφησης Το πρώτο ροζ κουμπί download, 'Download GPG suite' θα περιέχει την τελευταία έκδοση.Όταν ολοκληρωθούν οι λήψεις, ανοίγουμε το Thunderbird από το Downloads και σέρνουμε το εικονίδιο του Thunderbird στον φάκελο Applications.

1.1. WINDOWS: Thunderbird email client και λογισμικό κρυπτογράφησης GPG

Θα χρειαστεί να κατέβει:

 Ένας email client/mail manager για τον υπολογιστή –προτείνουμε το πρόγραμμα ανοιχτού κώδικα της Mozilla, το 'Thunderbird' (βλ. 41).

 το GPG (βλ. 42) – Gnu Privacy Guard[43], το οποίο είναι λογισμικό κρυπτογράφησης Το πρώτο πράσινο κουμπί download, 'Download GPG suite' θα περιέχει την τελευταία έκδοση.

1.2. UBUNTU/LINUX, MAC και WINDOWS:

Το επόμενο βήμα είναι να ανοίξουμε το Thunderbird. Εάν το ανοίγουμε για πρώτη φορά, πιθανόν να εμφανιστούν παράθυρα 'Integration' ή 'Set up wizard', τα οποία πρέπει να παραβλεφθούν. Το Thunderbird θα ζητήσει να επιβεβαιωθεί ο λογαριασμός email, και θα προτείνει μια νέα διεύθυνση email. Πατάμε 'Skip this and use my existing email'. Εισάγουμε την διεύθυνση email που θέλουμε να χρησιμοποιήσουμε για την κρυπτογράφηση και τον κωδικό. Στο σημείο αυτό θα πρέπει να αποφασίσουμε εάν επιθυμούμε να αποθηκευτεί ο κωδικός ή όχι. Είναι, όμως, περισσότερο ασφαλές να μην επιτρέπουμε στον υπολογιστή να θυμάται τον κωδικό, αλλά θα πρέπει να τον εισάγουμε κάθε φορά που επιθυμούμε να αποκτήσουμε πρόσβαση στο λογαριασμό μας στο Thunderbird. Πατάμε 'Continue'.

Θα πρέπει να σημειλωσουμε οτι εαν χρησιμοποιούμε μια ανώνυμη διεύθυνση email, προφανώς δεν πρέπει να εισάγουμε το πραγματικό μας όνομα.

Στη συνέχεια θα εμφανιστεί ένα παράθυρο 'Configuration found in Mozilla ISP database'.

Επίλυση προβλημάτων: Εάν εμφανιστεί ένα μήνυμα σφάλματος, 'Configuration cannot be verified', ο λόγος ίσως είναι ότι ο πάροχος email χρησιμοποιεί επιβεβαίωση δύο-βημάτων (two-factor verification) (π.χ. πολλοί λογαριασμοί Gmail χρησιμοποιούν αυτό το σύστημα). Σε αυτή την περίπτωση, δεν μπορούμε να χρησιμοποιήσουμε το

[41] http://www.mozilla.org/en-US/thunderbird/
[42] https://gpgtools.org/
[43] http://www.gpg4win.org/download.html

συνηθισμένο webmail κωδικό. Το Gmail θα μας επιτρέψει να αποκτήσουμε μια εφαρμογή κωδικών 'application- specific password', τις οποίες μπορούμε να βρούμε στη σελίδα με τίτλο 'authorizing applications and sites' των ρυθμίσεων του Google Account. Περισσότερες πληροφορίες βρίσκονται στη σχετική ιστοσελίδα[44].

Τώρα υπάρχει η επιλογή ανάμεσα σε IMAP ή POP3. Επιλέγουμε IMAP εάν χρησιμοποιούμε webmail, και πατάμε 'Done'.

Επιπλέον πληροφορίες: Το IMAP προσφέρει αμφίδρομη επικοινωνία μεταξύ του online λογαριασμού email και του email client του υπολογιστή ενός χρήστη. – Έτσι οι αλλαγές που γίνονται στον email client ενημερώνονται αυτόματα και στον online λογαριασμό (π.χ. εάν επιλεγεί ένα μήνυμα ως διαβασμένο στο Thunderbird, με IMAP, θα εμφανισθεί ως διαβασμένο και στο webmail). Αυτό δεν συμβαίνει με το POP3.

2. Enigmail, επέκταση ασφαλείας στο Thunderbird

Στο πάνω μέρος του παραθύρου του Thunderbird, επιλέγουμε Tools > Add-ons > Extensions. Εάν δούμε το 'Enigmail', τότε είναι ήδη εγκατεστημένο. Εάν όχι, πηγαίνουμε στο εργαλείο αναζήτησης στην πάνω δεξιά γωνία του παραθύρου, και κάνουμε αναζήτηση 'Enigmail'. Πατάμε 'Install', και επανεκκινούμε το Thunderbird.

3. Ζεύγος κλειδιών

Στην κορυφή του παραθύρου του Thunderbird, κάνουμε κλικ στο OpenPGP > Key Management. Στην μπάρα εργαλείων που βρίσκεται στο πάνω μέρος επιλέγουμε > Generate > New key pair.

 Η διεύθυνση email που θέλουμε να χρησιμοποιήσουμε για το κρυπτογραφημένο μήνυμα πρέπει να είναι επιλεγμένη.

 Επιλέγουμε το 'Use generated key for the selected identity' και στη συνέχεια επιλέγουμε το κλειδί να απενεργοποιηθεί σε 5 χρόνια.

 Εισάγουμε μια φράση-κλειδί (αυτή θα είναι η φράση-κλειδί για την κρυπτογράφηση του mail – όχι μόνο για τον online λογαριασμό mail – θα πρέπει να είναι πολύ ισχυρή).

 Κάτω από το 'Key expiry', το κλειδί θα πρέπει να λήγει σε 5 χρόνια.

 Επιλέγουμε 'Advanced', και στη συνέχεια επιλέγουμε το μέγιστο μέγεθος κλειδιού 4096, και τον τύπο κλειδιού 'RSA'.

 Επιλέγουμε 'Generate key' και μετακινούμε τον κέρσορα του ποντικιού στην οθόνη ενώ το πρόγραμμα δημιουργεί τυχαία το κλειδί (αυτό θα βοηθήσει στην τυχαία δημιουργία του κλειδιού). Η παραπάνω διαδικασία μπορεί να διαρκέσει μερικά λεπτά.

[44] https://support.google.com/mail/answer/1173270?hl=en

 Θα εμφανιστεί στη συνέχεια ένα πλαίσιο διαλόγου που θα ενημερώνει ότι η δημιουργία του κλειδιού έχει ολοκληρωθεί. Επιλέγουμε 'Generate Certificate' σε αυτό το πλαίσιο (αυτό θα δημιουργήσει ένα πιστοποιητικό ανάκλησης σε περίπτωση που θέλουμε να ακυρώσουμε το κλειδί, για παράδειγμα, εάν το ζεύγος κλειδιών έχει χαθεί ή έχει τεθεί σε κίνδυνο). Αποθηκεύουμε το πιστοποιητικό ανάκλησης σε ένα ασφαλές μέρος. Θα μας ζητηθεί στη συνέχεια να εισάγουμε τη φράση-κλειδί προκειμένου να ολοκληρωθεί η διαδικασία.

Ρυθμίσεις Thunderbird

Επανεκκινούμε εκ νέου τον Thunderbird για να αλλάξουμε μερικές ρυθμίσεις.

Expert settings

Enigmail > Preferences > Display Expert Settings

 Basic > Passphrase settings: εδώ θα πρέπει να επιλέξουμε για πόσο καιρό επιθυμούμε να θυμάται το Thunderbird την φράση-κλειδί μας.

 Sending: Επιλέγουμε

o 'Encrypt/sign replies to encrypted/signed messages'

o 'If possible', κάτω από το 'Automatically send encrypted'

o 'All valid keys I have', κάτω από το 'To send encrypted, accept'

o 'Always', κάτω από το 'Confirm before sending'

Το enigmail μας ενημερώνει κάθε φορά που στέλνουμε ένα email εάν το μήνυμα είναι κρυπτογραφημένο ή περιέχει υπογραφή – έτσι έχουμε λιγότερες πιθανότητες να ξεχαστούμε και να αποστείλουμε ένα μη κρυπτογραφημένο email.

 Key Selection: Επιλέγουμε τα 'By Per-Recipient Rules', 'By Email Addresses according to Key Manager', και 'Manually if Keys are Missing'.

 Advanced: οι επιλογές εδώ είναι προεραιτικές, αλλά ενδείκνυται να επιλεγεί το 'Re-wrap signed HTML text before sending' καθώς τα κείμενα HTML δεν δουλεύουν καλά με τα κρυπτογραφημένα emails.

Πατάμε 'Ok'.

Τοπική αποθήκευση φακέλων

Σίγουρα δεν θέλουμε να αποθηκεύονται τα πρόχειρα, μη κρυπτογραφημένα μηνύματά μας στους online φακέλους μας. Είναι περισσότερο ασφαλές να είναι αποθηκευμένα στον σκληρό δίσκο έτσι ώστε να υπάρχει μεγαλύτερος έλεγχο όσον αφορά στην ασφάλειά τους.

Στο μενού στην αριστερή μεριά του παραθύρου του Thunderbird, θα βρίσκονται όλοι οι φακέλους email. Στο κάτω μέρος, είναι οι 'Local Folders' – κάνουμε δεξί κλικ και επιλέγουμε 'New Folder' για να δημιουργηθούν οι φάκελοι'Sent' και 'Draft', οι οποίοι θα φανούν χρήσιμοι.

Επιλέγουμε Edit (για Linux) ή Tools (για Mac) > Account Settings > Copies & Folders. Μπορούμε να επιλέξουμε σε ποιό σημείο θέλουμε να αποθηκεύονται τα μηνύματά μας. Για παράδειγμα, κάτω από το 'Drafts and Templates', επιλέγουμε 'Local Folders' ως την τοποθεσία που θα αποθηκεύονται τα πρόχειρα μηνύματά μας.

Στο ίδιο παράθυρο [Edit (Linux) ή Tools (Mac) > Account Settings] επιλέγουμε OpenPGP Security > και στη συνέχεια επιλέγουμε 'Encrypt draft messages on saving'.

Email με απλό κείμενο

Η HTML δεν κρυπτογραφείται καλά, για αυτόν τον λόγο θα πρέπει να συντάσσονται τα μηνύματά με απλό κείμενο.

Edit (Linux) ή Tools (Mac) > Account Settings > Composition & Addressing. Αποεπιλογή του 'Compose messages in HTML format'

Κοινοποίηση της PGP υπογραφή με τις επαφές

Η κοινοποίηση της PGP υπογραφής σας με τα πρόσωπα που επικοινωνούν οι χρήστες, ακόμη και αν το ίδιο το email δεν είναι κρυπτογραφημένο, ενημερώνει τον παραλήπτη ότι υπάρχει κρυπτογράφηση PGP και (τεχνικά) τους επιτρέπει να επιβεβαιώσουν την ταυτότητά του αποστολέα.

Edit (Linux) ή Tools (Mac) > Account Settings > OpenPGP Security, το 'Enable OpenPGP support (Enigmail) for this identity' θα πρέπει να είναι επιλεγμένο.

Επιλέγουμε 'Sign non-encrypted messages by default' και στη συνέχεια επιλέγουμε 'sign encrypted messages by default'. Πατάμε 'OK'.

Εμφάνιση του δημόσιου κλειδιού

Το να ανέβει το δημόσιο κλειδί στον keyserver είναι σαν να αποθηκεύεται το τηλέφωνό μας σε ένα ευρετήριο. Επιτρέπει στους άλλους να μας αναζητήσουν με την βοήθεια του ονόματος ή της διεύθυνσης email μας, και να χρησιμοποιήσουν το δημόσιο κλειδί μας ούτως ώστε να μας στείλουν ένα κρυπτογραφημένο email. Αυτή η διαδικασία είναι πολύ σημαντική για όσους επιθυμούν να λαμβάνουν κρυπτογραφημένα mail προστατεύοντας με αυτόν τον τρόπο τη μετάδοση των δεδομένων/πληροφοριών τους. Παρόλο αυτά, εάν μιλάμε για μια ανώνυμη διεύθυνση email που θα χρησιμοποιείται για να επικοινωνούμε μόνο με συγκεκριμένα άτομα, άτομα υψηλού κινδύνου, φυσικά το να ανεβάσουμε το δημόσιο κλειδί στον keyserver δεν έχει μεγάλη ουσία και δεν ενδείκνυται.

Enigmail > Key management.

Επιλέγουμε το 'Display All Keys by Default'. Κάνουμε δεξί κλικ στην διεύθυνση email, κι επιλέγουμε 'Upload Public Keys to Keyserver' εάν θέλουμε άλλοι χρήστες να μπορούν να επικοινωνήσουν μαζί μας. Ο προεπιλεγμένος keyserver είναι pool.sks-keyservers.net.

Αναζήτηση δημόσιων κλειδιών τρίτων

Μπορούμε να αναζητήσουμε ένα πρόσωπο με την βοήθεια του ονόματος ή της διεύθυνσης email του για να διαπιστώσουμε εάν το συγκεκριμένο άτομο διαθέτει δημόσιο κλειδί, ούτως ώστε να μπορούμε να του στείλουμε κρυπτογραφημένο mail (η διαδικασία είναι ίδια όπως η αναζήτηση ενός αριθμού τηλεφώνου σε ένα ευρετήριο).

Enigmail > Key management > Keyserver (στο πάνω μενού) > Search for keys. Εισάγουμε το όνομα ή την διεύθυνση email του προσώπου και αναζητάμε τα αποτελέσματα. Επιλέγουμε τη διεύθυνση email των προσώπων, των οποίων τα κλειδιά θέλουμε να εισάγουμε και πατάμε ok.

Εισαγωγή κλειδιού

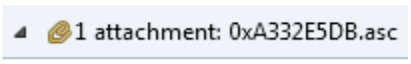
Σε περίπτωση που διαθέτουμε ήδη το κλειδί της επαφής μας σε ένα αρχείο ή online, αλλά θέλουμε να το εισάγουμε στον key manager του Thunderbird.

Εισαγωγή κλειδιού από αρχείο:

Στο Thunderbird, επιλέγουμε Enigmail > Key management. Πηγαίνουμε πάλι πίσω στη μπάρα εργαλείων που βρίσκεται στην κορυφή του παραθύρου κι επιλέγουμε File > Import keys from file.

Εισαγωγή κλειδιού από email:

Εάν η επαφή μας έχει επισυνάψει το δημόσιο κλειδί της σε ένα αρχείο στο email, ανοίγουμε το επισυναπτόμενο στο Thunderbird και κάνουμε κλικ στο 'Import'. Το επισυναπτόμενο θα είναι της μορφής:



Εισαγωγή κλειδιού από ένα δημόσιο key block:

Πολλοί χρήστες έχουν το δικό τους δημόσιο key 'block' (π.χ. το δημόσιο κλειδί τους σε κείμενο) στο website τους. Αυτό επιτρέπει στους άλλους χρήστες να εμπιστεύονται το website ως την πηγή του κλειδιού περισσότερο από τον keyserver, και συν τοις άλλοις αποτρέπει τις επιθέσεις man-in-the-middle.

Απλά αντιγράφουμε όλο το key block (όλο το block, όπως φαίνεται παρακάτω), και στη συνέχεια στο Thunderbird επιλέγουμε Enigmail > Key management > (πίσω στην

μπάρα εργαλείων) Edit > Import keys from clipboard > κάνουμε κλικ στο 'Import' στο πλαίσιο διαλόγου.

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1

mQINBFOypIgBEADEXjFLXnFDraRWa6YzzdnO8gKJKOzD8aonyQvh251QGVOIwbg2
J1AfC+Ro3xhAxxX1kYzIwqeVIxlfNXCzZqn2KE7P0udF4EVrkVsWP1VcX8B65V0K
7BURi5hFFNNsk2UdnQdwc8bP77cZDkgDJofXF5hrUN1TCoLhxZ2WvpT9FfOR+Ph2
8r/8IfcQ9K6ktsGpG5y6KafpvtI9sI+eo8OXxDd8Jyelq27mM492pcnfWjD6mlvJ
61U98CjBqLIH8rsgxVivNbRxOrler5avxZjP5+691TDRCtBIn3+2WqWrzXKfMn44
1+iIKiqllMNJhmsuP3bEWHKGDZFk2/MafAqBWuXHOfclADX4GligLnv3EXm8hlYd
uKtR8PvpcCwuKgM6cVjCBrpLB+lbbq+6ILMDrTt9n4WoV3kb5iUMV5gMrNT8dp8m
Gs7zMZQFXsavlR7CjKTIFhmnPYK+v4262m7ZWvXzCVIseAtbIRYMWptzolMR8zBZ
gqfcTeTQYWdljWrbyAziE22wmfvUtqUlRQbh/okiCEcObHsPAr4QGtHyRBzBHkub
XjHopG4E+Zh1KbHTlg/wftfKDdODDfgkrrgWkIToe6x3140ogX/Bk6Al6crn4d2R
OV36KWeVx25EfVY1mEE+62mF3GrquzxKAkx2UF7s2Jk+JIlpZUCZuMZMdwARAQAB
tB5DSUogaW5mb3N1YyA8aW5mb3N1Y0B0Y21qLm9yZz6JAj4EEwECACgFAlOypIgC

GyMFCQlmAYAGCwkIBwMCBhUIAgkKCwQWAgMBAh4BAheAAAoJEE3Wpo5++N4yJgUP
/Atbshkafwk+GfNcsauNfqSg6u4V3p8DpBTAE4oUUk753gPSJVBiGsigztmCSpxJ
6N7iqIDZ0f72Ahq3lbwZ34NDPBVKrL7jRc8IwsFvTIAylMYz9eR2cWC81ff6XMY+
OaclRD+J3ksY6DfLzJfZWORAHcITuBzIgZZ47DwCGNzey0zIHS/u8w7o71C+h0WV
oNFPdzlCidxCtretZke3qvBcUNJWvx3r90Foh3lotqhneCwrXgp1JNEZx/xKypex
cReY+N6UyKQMeDOn7gj0O+fuxEq8s8x8IgtALrevm37JLz732wEZIBHiB6fh+s8i
M0TpcMC//9sbL86GXGwUdosbrGnPoCCMsgE3jDJqIVz4jEoN5XPffYCmSWNb2w9s
LfQBny8s0JcRgxClytdOCDHOboBJ83ytUnUcHo/NvkpAeCEGCTvaoOtlRywdF55p
G8izK3brjKEY/ldGAx5g6aWiliraSBOMlAHeZ/J8KOMRcEwU8sozuNeomGr3WNdR
bDTaD37F0TBOzxx+QNjeSiVzleLJeHBHyZCpizXOe2wWEtRLq9WRHM4VUI/UGHOL
xChZhwLailgkmhl3eHl+47mTArbrl+P7R6Y79bmw+wld3EaE9XbnKoislon8uciW
cr2qHr/PvPN8o+4hJ7rsmsZBvX9JI+74ouyIsp0qW3rXiQIcBBMBAgAGBQJTsqfx
AAoJECN9TFARig7CU2YP/igQSe8pXbJAhrQPtTk7HByHITE81rE51uFRwCVbvTav
sRN3978ob4B7QZanVlUH2YarDoLn/a90kmpECZdxlh0ZTlKKfj32jLNTWy8biQUc
i/rOgli8N87jeszquo+sB7ofPP/o3DKU4QvnR8SqyIxhgae80F+mnkAOyTTWDi7H
NHGq2sdLBOQALHVIVUJ5SOOEANYKZYklrR7v4iK0pc0TZDLdJ3Vm5T05N8vjCzLa
TRMgNh397ElnR9n6AGw+QRKlA21i7dAxTMecaC0nYmZx/ZVkxMRXtiSjbr2OZ163
gVxUl3o0eOjcHUX3LsX90Tew2Z+1jjaXrPJmJkxghxL/BkZx5V+knn9wTaJdP0r6
mO32n/lPEtG0mYeQQ84ZYbath3VqsY/QODG+7grce6mJUU3jszo6AzfHMBRdipRb
bFrnOoVsDMuu4kRvPzDXiu4kJZxZiwinDuen5uu8//QUyuVXkls3ATUiwUGgK8F2
CuYlutl/5E5x+MFS21IRCf2O3tFh8WIheO4BwQXErZ7FY9L7aaZa93WAcl6ueHUM
IBEs06+CaPUQCcWnxO2qwZm76aYNKwsVqptKEXcZ/mofol2/pgOjVtddLw9+4zpK
Gmk2erPtMPp4eMwBkZVcRz9kGfzFn3fNanmCQ22NW5x/HFrsi/+ZSURcO/Pcp8yk
uQINBFOypIgBEADIThi9K7ioKz8vqSR3yrQlVp9NjPit2urzgJhW3HjLenVfvwQl
zAoks1jDoOwuFizV9vpWpHN/ovRZqJQiKws0haOU8FboLrwmQMvzFaf+8rIQjVM9
YOZimEEL8a2va8M9bn8pfPO9L3beq4bWgNnxZEhEOg4ovscXUfp+ktDG/L5f5z+R
77Co07XUM8KrNcYlDL76lKNrNumUTGJu/F+LR7LnNyRmpMi91LcyX4UkRar9xdTB
/OmpwBqbH4hG3hl4xB329NL5jsCAL6gqDKIe/bD6oecWhY2GodrX9bqtwCyMGb6/
rS+2Rv4ggwnRroRTGIlB2I+LlqRfMI2XZVZp9gt0Vj25D7LBmxyffGOFIszjrXfG
yVavBQo/cHB8u3CW1Pi9bQ5ZF82f9e42IazeWwrpUkyFQpiy4m8JTL2kMKt7tWEN
MI2jYPIjHnhjwBGXjyAGWchM4F0TO6q+714S8xtvDQKPemWqopnKbL1Q8Y9OzPxRv
jKliFOYLDCBu/uYyKsll4pqr5OokRs8Q9fO9MU+jye8O48mu91vP070bHYAKvw9N
4B28acET9JlpQOHmhLWRENz4ZNap8fe1BAhHg2AE7M4ZQUS6GkPGeUclhZhC7vs5
/ty9IHA2bk2+fMwDr+Oye21Dife0JtbL3+krD9RLqEpSZ8SDq/BNvYJcUQARAQAB
iQI1BBgBAgAPBQJTsq8IAhsMBQkJZgGAAAoJEE3Wpo5++N4yCp8P+wW7y5fbdt/O
F+4IUuVIun8yH62iQbfUBL21rWKXaTBywyWpLvlOjfAlqylVFZnDGoGrkc6LEhFE
Wb7a53GzFyVNSM1K/U+SF0UtdT2h0WFDqwphjtD71+L6uOve0ahRyTq0PTXnk/uT
JfQ76yt71d/6cHvvtcpYMk2n9IbeVuTWdjXLEG5Gmr4rDThUppq26oVYG5KGCuuW
s5J+k6gLPh9oNL5KKO8t8vHYbGEx3rMcd3YXXZDvYZZUDcjTE3hVXXFN3xwyHObE
L20UGFJ6y3GTL2jH0i8RtquAJlMMwttey5DOUPULu5z9prHSo961SkkZqXDhbgBp
ZO6Av0Q9FyTYoxfhhf3KH5v4CivmrPZYRD/gu/doO2JGqRyWYGDYOy0E8rgNY8wJ
JD9rMneDB9qE4vsv3AmYIF5ov5dkuQe6x8TpS11h20aokru9fJvTpNNNan8A/cPu
Y1Qvc06qzz0eHG4VnyAGBZ3j4cbT9B8KBt8136aLCNa60Kzl4qLx8FO/+wDb6dgf
ToHfdTNDZT48VjhfzoBVslNIbXzF1rgDGgBax2aR856hHfx4GERRO8ZZVBvPtjqy
5TrFSI9NsdNwmetMh8rxb+dz+fJYEE5yrNs9MJPHVgeVgj0UJLawhlCGME+/1PFJ
Cr8XhDwzI2n6gFvwtWQ1NNMqdn1UiF+Y
=3DCe
-----END PGP PUBLIC KEY BLOCK-----
```

Επιβεβαίωση κλειδιών

*Για να σιγουρευτούμε ότι το πρόσωπο με το οποίο νομίζουμε πως επικοινωνούμε είναι όντως το πρόσωπο που ισχυριζόμαστε ότι είναι*στο Thunderbird, επιλέγουμε Enigmail > Key management > και κάνουμε δεξί κλικ στην επιλεγμένη διεύθυνση email > View Properties. Εδώ είναι εμφανή το κλειδί του προσώπου και το ψηφιακό του αποτύπωμα. Μπορεί να επιβεβαιωθεί ότι το κλειδί όντως ανήκει στο πρόσωπο αυτό ανταλλάζοντας ψηφιακά αποτυπώματα από άλλο μέσο επικοινωνίας (με προσωπική επαφή, μέσω τηλεφώνου, είτε μέσω της προσωπικής κάρτας του ή του website), και ελέγχοντας αν αιριάζουν απόλυτα. Στο ίδιο παράθυρο μπορούμε στην συνέχεια να επιλέξουμε Select Action > Set Owner Trust > και στη συνέχεια επιλέγουμε αν και κατά πόσο εμπιστευόμαστε ότι το κλειδί ταιριάζει όντως με αυτό του προσώπου που θέλουμε να επικοινωνήσουμε.

Εισαγωγή υπογραφής στο email

Γράψτε το όνομα, το επάγγελμά σας, το website, την διεύθυνση email σας, το PGP δακτυλικό απότυπωμα και οποιαδήποτε πληροφορία επιθυμείτε να προσθέσετε.

Edit (Linux) ή Tools (Mac) > Account Settings.

Εδώ μπορείτε να εισάγετε το κείμενο της υπογραφής που θα φαίνεται στα emails σας.

Edit (Linux) ή Tools (Mac) > Account Settings > Composition & Addressing

Επιλέξτε 'Include signature for replies'.

Λήψη νέου mail

Μπορεί να ρυθμιστεί πόσο συχνά θα αναζητά ο mail client για νέα μηνύματα.

Edit (Linux) ή Tools (Mac) > Account Settings > Server settings

Αποστολή email

Όταν έχουν ολοκληρωθεί οι ρυθμίσεις, στέλνουμε ένα δοκιμαστικό μήνυμα σε κάποιον που έχει κρυπτογραφημένο mail. Εισάγουμε το κλειδί του ή το βρίσκουμε από τον keyserver, και σιγουρευόμαστε ότι επιβεβαιώσαμε το κλειδί του και συμπληρώσαμε την φόρμα εμπιστοσύνης που αναφέραμε παραπάνω, προτού προχωρήσουμε στην αποστολή του email (ειδάλλως ο email client μπορεί να μην μας επιτρέψει να στείλουμε το κρυπτογραφημένο μήνυμα – το Thunderbird ενθαρρύνει τις ενέργειες ασφάλειας με αυτό τον τρόπο).

Διαλέγουμε έναν παραλήπτη του οποίου το κλειδί έχουμε ήδη εισάγει και επιβεβαιώσει. Προχωράμε με την σύνταξη του email, και προτού πατήσουμε 'Send', πηγαίνουμε στο 'Enigmail' μέσα στο παράθυρο σύνταξης νέου μηνύματος κι επιλέγουμε 'Force

Encryption'. Πατάμε 'Send', και κατόπιν θα ενημερωθούμε από ένα πλαίσιο διαλόγου ότι το email μας περιέχει υπογραφή και είναι κρυπτογραφημένο (εάν όχι, πηγαίνουμε πίσω και ελέγχουμε ότι έχουμε επιλέξει την κρυπτογράφηση). Κάνουμε κλικ στο 'Send Message', και το κρυπτογραφημένο μήνυμά μας θα αποσταλεί με επιτυχία.

Τώρα που στείλαμε στον παραλήπτη το κρυπτογραφημένο email, έχει δημιουργηθεί μια προεπιλεγμένη ρύθμιση με την οποία όλα τα επόμενα emails που θα στείλουμε σε αυτήν την επαφή στο μέλλον θα κρυπτογραφόνται αυτόματα. Εκτός και αν έχουμε αποφασίσει διαφορετικά, τότε δεν θα πρέπει να έχουμε επιλεγμένο το 'force encryption'.

Αποστολή/Λήψη συνημμένων

Μπορούμε επίσης να κρυπτογραφήσουμε και να αποκρυπτογραφήσουμε επισυναπτόμενα αρχεία με το GPG.

Κατά την αποστολή ενός αρχείου ως επισυναπτόμενου σε ένα κρυπτογραφημένο email, μπορούμε να επιλέξουμε εάν επιθυμούμε να κρυπτογραφήσουμε και το επισυναπτόμενο. Αφού συντάξουμε το μήνυμά μας, επισυνάπτουμε το αρχείο, και πατάμε 'Send'. Προτού σταλεί το email, θα μας δοθούν οι εξής επιλογές. Η πρώτη επιλογή είναι να κρυπτογραφήσουμε το μήνυμα αλλά όχι το επισυναπτόμενο αρχείο. Η δεύτερη επιλογή είναι να κρυπτογραφήσουμε το μήνυμα, και ξεχωριστά να κρυπτογραφήσουμε το επισυναπτόμενο αρχείο.

Επιλέγουμε τη δεύτερη επιλογή ('Encrypt/sign each attachment separately and send the message using inline PGP'), και πατάμε OK.

Στη συνέχεια θα εμφανιστεί το συνηθισμένο πλαίσιο που θα ενημερώνει πως το μήνυμα και το επισυναπτόμενο αρχείο περιέχουν υπογραφή και είναι κρυπτογραφημένα – επιλέγουμε 'Send Message' για επιβεβαίωση, και το επισυναπτόμενο αρχείο θα αποσταλεί.

Όταν κάποιος μας στέλνει ένα κρυπτογραφημένο επισυναπτόμενο αρχείο μέσω email, κάνουμε δεξί κλικ στο αρχείο και επιλέγουμε 'Decrypt and Save As'. Το αποθηκεύουμε στην τοποθεσία της επιλογής μας, και στην συνέχεια πηγαίνουμε εκεί που το αποθηκεύσαμε και ανοίγουμε το αρχείο.

Φυσικά, εάν το επισυναπτόμενο που μας έχει σταλεί έχει κρυπτογραφηθεί ήδη από άλλα μέσα (π.χ. TrueCrypt), δεν χρειάζεται να το αποκρυπτογραφήσουμε εκ νέου με το GPG.

Εισαγωγή νέου λογαριασμού

Για να προσθέσουμε νέο λογαριασμό email στο Thunderbird, ανεξαρτήτως του αν σκοπεύουμε να χρησιμοποιήσουμε σε αυτόν τον λογαριασμό κρυπτογράφηση ή όχι, πηγαίνουμε στο Thunderbird επιλέγουμε Tools > Account Settings > Account Actions > Add mail account.

Κεφάλαιο 6: Αποστολή άμεσων μηνυμάτων (Instant Messaging)

Η αποστολή άμεσων μηνυμάτων είναι ένας καλός τρόπος να ξεκινήσουμε και να διατηρήσουμε την επικοινωνία μας με μια επαφή μας. Είναι γρήγορο και εύκολο να ρυθμιστεί η κρυπτογράφηση για τους 'off-the-record' (OTR) instant messengers (IM) – ειδικά σε σύγκριση με τις ρυθμίσεις για την κρυπτογράφηση των mail. Χρησιμοποιώντας έναν OTR IM, μπορούμε να συζητήσουμε για τα απαραίτητα πρωτόκολλα ασφαλείας προτού συνεχίσουμε την επικοινωνία μας, τις συναντήσεις, την αποστολή email, την αποστολή/λήψη εγγράφων ή πληροφοριών με τη συγκεκριμένη επαφή, κ.ο.κ.. Είναι επίσης ένα χρήσιμο εργαλείο για την επικοινωνία μας με τους συναδέλφους εάν συνεργαζόμαστε σε ένα project απο μακριά.

Η off-the-record αποστολή άμεσων μηνυμάτων επιτρέπει τις ιδιωτικές συζητήσεις, που όχι μόνο είναι κρυπτογραφημένες αλλά δεν αποθηκεύονται. Δηλαδή, είναι ένα chat που περιλαμβάνει έναν λογαριασμό chat που συνδέεται με τον χρήστη, αλλά επί της ουσίας δεν είναι αυτός.

Όπως συμβαίνει και με την κρυπτογράφηση των email, ο OTR IM χρησιμοποιεί δημόσια κλειδιά με τα οποία επιβεβαιώνεται η ταύτοτητα του παραλήπτη. Παρόλο αυτά, κάθε φορά που ξεκινάει μια νέα συζήτηση στο chat με μια επαφή (η οποία έχει επιβεβαιωθεί από το δημόσιο κλειδί της), το chat κρυπτογραφείται χρησιμοποιώντας νέα κλειδιά. Ωστόσο δεν θα χρειαστεί να κάνουμε κάτι εμείς, ούτε θα τα δούμε – υπάρχουν και λειτουργούν ως under-the-bonnet κρυπτογράφηση την οποία ο ίδιος ο messenger client κάνει για εμάς.

Εάν χρησιμοποιούμε Linux ή Windows, προτείνουμε να χρησιμοποιηθεί ο IM client Pidgin, με ένα OTR plug-in.

Εάν χρησιμοποιούμε Mac, προτείνουμε τον IM client Adium.

Οι χρήστες των Pidgin και Adium μπορούν να επικοινωνούν εύκολα μεταξύ τους. Παρόλο αυτά, στις υπάρχουσες εκδόσεις, οι μέθοδοι επιβεβαιώσης για αυτούς τους δύο messenger clients είναι διαφορετικές.

Οδηγίες για το Adium των Mac:

1. Μεταφορτώνουμε κι εγκαθιστούμε το 'Adium[45]' για Mac

2. Δημιουργούμε και ρυθμίζουμε τον IM λογαριασμό

Μετά την λήψη, ανοίγουμε το Adium και επιλέγουμε 'File' > 'Add account' > 'Jabber'. Κάτω από το 'Jabber ID', επιλέγουμε ένα (ανώνυμο) όνομα και εισάγουμε ένα domain

[45] http://adium.im/

στο τέλος[46]. Ένα πλήρες Jabber ID θα πρέπει να είναι της μορφής kissinger@jabber.ccc.de .

Κάτω από το 'password', επιλέγουμε έναν ισχυρό κωδικό.

Πρώτα επιλέγουμε το 'Options' του ίδιου παραθύρου και όχι 'register account' ακόμη.

- Στο 'options' επιλέγουνε 'Require SSL/TLS' και στη συνέχεια 'Do strict certificate checks'.

- Έπειτα πηγαίνουμε στο 'Privacy' και στο μενού κάτω από το 'encryption' επιλέγουμε 'Force encryption and refuse plain text' (το τελευταίο της λίστας).

Πηγαίνουμε πίσω στο Accounts κι επιλέγουμε 'register account'.

Θα εμφανιστεί ένα νέο παράθυρο: στο 'server', πληκτρολογούμε το domain που επιλέξαμε προηγουμένως (π.χ. 'jabber.ccc.de' εάν επιλέξαμε αυτό) και στη συνέχεια επιλέγουμε 'Request new account'. Στη συνέχεια, θα ενημερωθούμε ότι ο λογαριασμός μας έχει δημιουργηθεί επιτυχώς.

3. Ρυθμίσεις Adium

Επιλέγουμε Adium > Preferences > General > αποεπιλέγουμε το 'Log messages'.

Οδηγίες για το Pidgin των Linux (Ubuntu)/Windows

1. Μεταφόρτωση του Pidgin και του OTR plug-in

Το Pidgin και το OTR συχνά συμπεριλαμβάνονται στις εκδόσεις Linux, έτσι απλά κάνουμε μια αναζήτηση στο Ubuntu (ή σε όποια έκδοση έχουμε εγκατεστημένη) Software Centre.

Μεταφορτώνουμε και εγκαταθιστούμε το Pidgin[47] (Windows), εάν χρησιμοποιούμε Ubuntu, θα μεταφερθούμε από αυτή την σελίδα στο Pidgin PPA package, το οποίο και θα πρέπει να μεταφορτώσουμε.

Για τα Windows, μεταφορτώνουμε το OTR plug in[48]. Για τα Ubuntu, πηγαίνουμε στο Ubuntu Software Centre, αναζητάμε το Pidgin OTR, κι εγκαθιστούμε το 'Pidgin Internet Messenger Off-the-record Plug-in'.

2. Ρυθμίσεις Pidgin

Ανοίγουμε το Pidgin. Εάν είναι η πρώτη φορά που ανοίγουμε το Pidgin, δεν θα έχουμε κάποιο λογαριασμό ρυθμισμένο και θα μας ζητηθεί να προσθέσουμε έναν λογαριασμό. Επιλέγουμε 'Add' (εάν δεν μας ζητηθεί, μπορούμε να το βρούμε στο Accounts > Manage Accounts > Add).

α. Κάτω από το 'Protocol' επιλέγουμε XMPP/Jabber (ΟΧΙ Facebook XMPP).

[46] https://list.jabber.at
[47] www.pidgin.im
[48] https://otr.cypherpunks.ca

b. Επιλέγουμε ένα (σχεδόν ανώνυμο) username.

c. Κάτω από το domain, πληκτρολογούμε το domain που επιλέξαμε (για παράδειγμα, jabber.ccc.de) – για περισσότερες επιλογές στον παρακάτω σύνδεσμο: https://list.jabber.at

d. Δημιουργούμε έναν ισχυρό κωδικό.

e. Επιλέγουμε 'Advanced' και στο πεδίο 'Connection security', σιγουρεύουμε ότι το 'Require encryption' είναι επιλεγμένο.

f. Κατευθυνόμαστε στο βασικό μενού και σιγουρευούμε ότι επιλέξαμε 'Create this new account on the server' στο κάτω μέρος του παραθύρου προτού επιλέξουμε 'Add'.

3. Δημιουργία ενός λογαριασμού IM

Η διεύθυνση Jabber θα πρέπει να εμφανίζεται στο παράθυρο 'Accounts'.

Επιλέγουμε το πλαίσιο 'Enabled' και στη συνέχεια 'register' στο παράθυρο 'Register New XMPP Account' που θα εμφανιστεί.

4. Ρυθμίσεις OTR

Στο Pidgin, επιλέγουμε Tools > Plug-ins > 'Off-the-record messaging'. Στη συνέχεια επιλέγουμε 'Configure plug-in'. Επιλέγουμε όλες τις προεπιλεγμένες ρυθμίσεις του OTR: Enable private messaging, Automatically initiate private messaging, Require private messaging, και Don't log OTR conversations. Στη συνέχεια επιλέγουμε 'generate' για να δημιουργήσουμε ένα κλειδί για τον λογαριασμό μας.

Επιλέγουμε Tools > Preferences > Logging, και αποεπιλέγουμε όλες τις επιλογές καθώςδεν θέλουμε να συνδεόμαστε στα chats.

Πλέον έχουμε ρυθμίσει τον OTR IM και μπορούμε να απολαύσουμε off-the-record, κρυπτογραφημένο chat.

Ξεκινήστε το OTR chat

Προσθήκη επαφών

Pidgin

Στο Pidgin, επιλέγουμε Buddies > Add a buddy και πληκτρολογούμε την πλήρη διεύθυνση του προτού επιλέξουμε 'Add'. Όταν η επαφή συνδεθεί στο διαδίκτυο, θα λάβει ένα αίτημα από εμάς.

Για να αρχίσουμε μια συνομιλία με μια επαφή που βρίσκεται συνδεδεμένη στο διαδίκτυο, κάνουμε διπλό κλικ στην επαφή buddy της λίστας μας, και επιλέγουμε OTR > 'start private conversation' στο παράθυρο του chat.

Adium

Στο Adium, επιλέγουμε Contact στην μπάρα εργαλείων στο πάνω μέρος > Add contact. Κάτω από το 'Contact type', υποθέτοντας ότι η επαφή αυτή επίσης χρησιμοποιεί Jabber, επιλέγουμε XMPP/Jabber, ή εισάγουμε την πλήρη διεύθυνσή της στο 'Jabber ID', και στη συνέχεια επιλέγουμε 'Add'.

Επιβεβαίωση επαφής

Ιδανικά, θα πρέπει να χρησιμοποιούμε επιβεβαίωση μέσω δακτυλικού αποτυπώματος και εάν γνωρίζουμε το πρόσωπο αρκετά καλά, θα πρέπει να του θέσουμε μια ερώτηση της οποίας την απάντηση γνωρίζει μόνο εκείνο το πρόσωπο.

Pidgin

Εάν δεν έχουμε ταυτοποιήσει την επαφή, κάνουμε διπλό κλικ στη διεύθυνσή της για να ανοίξουμε ένα παράθυρο chat μαζί της, πηγαίνουμε στο OTR στο παράθυρο και επιλέγουμε 'Authenticate buddy'. Μπορούμε να ταυτοποιήσουμε μια επαφή μέσω:

 Ερώτησης – απάντησης, είναι ένας καλός προσωποποιημένος τρόπος.

 Κοινού μυστικού, πρέπει να το έχουμε συνεννοηθεί εξαρχής μέσω διαφορετικού τρόπου επικοινωνίας.

 Χειροκίνητης ταυτοποίησης μέσω ψηφιακού αποτυπώματος, μια χρήσιμη και αρκετά αποδοτική μέθοδος. Είναι η μόνη μέθοδος με την οποία οι χρήστες των Adium και Pidgin μπορούν να ταυτοποιήσουν ο ένας τον άλλο.

Σε αυτό το παράθυρο, επιλέγουμε 'Manual fingerprint verification' και στη συνέχεια θα μπορούμε να δούμε το αποτύπωμα της επαφής. Ελέγχουμε το αποτύπωμα – εάν ταιριάζει, επιλέγουμε 'I have verified that this is in fact the correct fingerprint', και επιλέγουμε 'Authenticate'.

Adium

Εάν δεν έχουμε ταυτοποιήσει την επαφή, κάνουμε διπλό κλικ στην διεύθυνσή της για να ανοίξουμε ένα παράθυρο chat (ακόμα κι αν φαίνεται offline – θα φαίνεται offline και μη επιβεβαιωμένη μέχρις ότου την ταυτοποιήσουμε). Κάνουμε κλικ στο εικονίδιο κι επιλέγουμε 'Initiate Encrypted OTR chat'.

Το εικονίδιο με την κλειδαριά θα εμφανιστεί πλέον κλειστό. Ενώ έχουμε το παράθυρο chat ακόμη ανοιχτό, πηγαίνουμε στη μπάρα εργαλειών στο πάνω μέρος του Adium και επιλέγουμε Contact > Encryption > Verify. Στη συνέχεια θα μπορούμε να δούμε το αποτύπωμα της επαφής.

Έλεγχος ψηφιακών αποτυπωμάτων

Θα πρέπει να ελέγξει ο ένας τα αποτυπώματα του άλλου μέσω κάποιας διαφορετικής μορφής επικοινωνίας εκτός του IM (email, τηλέφωνο). Εάν δεν υπάρχει κάποιος ασφαλής τρόπος να γίνει αυτό, ένας κοινός φίλος ή κάποιος τρίτος στο IM μπορεί να στείλει στην επαφή μια μερική έκδοση του αποτυπώματος μας (π.χ. 0---A7-0 D—706-D 2—65--1 --3D-9C2 0-57B—1), και αντίστοιχα το αποτύπωμα της επαφής σε εμάς, έτσι ώστε να ελέγξουν και οι δυο κατά πόσο ταιριάζει με το αποτύπωμα που φαίνεται. Θα πρέπει να σημειωθεί οτι μερικά σημεία του δακτυλικού αποτυπώματός θα πρέπει να είναι επιμελώς επεξεργασμένα ώστε να αποτραπούν οι 'man-in-the-middle' επιθέσεις πλαστογραφίας.

Εύρεση του δακτυλικού αποτυπώματος

Οι χρήστες του Adium μπορούν να βρουν το δακτυλικό τους αποτύπωμα στο Adium > Preferences > Advanced > Encryption.

Οι χρήστες του Pidgin μπορούν να βρουν το δακτυλικό τους αποτύπωμα ανοίγοντας ένα παράθυρο chat με μια επαφή, κάνοντας κλικ στο μικρό εικονίδιο buddy (δεξιά από το 'OTR') Re/Authenticate buddy > Manual fingerprint verification. Και οι δύο χρήστες θα πρέπει να λάβουν υπόψη τους να μην επιτρέπουν στο Adium ή στο Pidgin να θυμάται αυτόματα τον κωδικό Jabber password, επειδή ίσως να μην είναι ασφαλώς αποθηκευμένο. Θα πρέπει να εισάγουν τον Jabber κωδικό τους χειροκίνητα κάθε φορά που συνδέονται.

Κεφάλαιο 7: Κλήσεις/ Βιντεοκλήσεις μέσω διαδικτύου

Ασφάλεια κινητών τηλεφώνων

Πολλοί από εμάς θεωρούν τα κινητά τους τηλέφωνα άκρως σημαντικά τόσο για την εργασία τους όσο και για την καθημερινότητά τους. Τα πλεονεκτήματα της διαρκούς σύνδεσης με τους λογαριασμούς email, τους web browsers, τα μέσα κοινωνικής δικτύωσης, τα ημερολόγια, καθώς επίσης και η εύκολη πρόσβαση σε κάμερες υψηλής ανάλυσης, τα καθιστούν χρήσιμα και πολύτιμα εργαλεία. Παρόλο αυτά, δεν θεωρούνται ιδιαίτερα ασφαλή.

Η μόνη επαρκής λύση για την ασφάλεια των δεδομένων σας είναι τα κινητά τηλέφωνα μιας χρήσης (ίσως είναι γνωστά ως burner phones).

Οι βασικότεροι κίνδυνοι που μπορεί ένας χρήστης να αντιμετωπίσει είναι:

 Αυτόματη σύνδεση από την παρούσα/ πρόσφατη τοποθεσία.

 Αυτόματη συλλογή μεταδεδομένων, π.χ. ο αριθμός και η τοποθεσία κάθε καλούντα, οι μοναδικοί σειριακοί αριθμοί των τηλεφώνων που συμπεριλαμβάνονται, ο χρόνος και η διάρκεια της κλήσης.

 Κλοπή και απώλεια δεδομένων.

 Απομακρυσμένη πρόσβαση στα δεδομένα όταν το τηλέφωνο είναι συνδεδεμένο σε δημόσιο δίκτυο Wi-Fi.

 Απομακρυσμένη πρόσβαση σε όλα τα δεδομένα σε οποιοδήποτε σημείο το τηλέφωνο είναι ενεργοποιημένο.

 Παρακολούθηση, υποκλοπή ή καταγραφή κλήσεων/βιντεοκλήσεων.

 Μη εξουσιοδοτημένη ενεργοποίηση του μικροφώνου για την καταγραφή ήχου.

 Μη εξουσιοδοτημένη ενεργοποίηση της κάμερας για την καταγραφή εικόνας.

Dragnet παρακολούθηση τηλεφώνου

Οι τηλεφωνικές συσκευές διαρρέουν μεγάλο όγκο πληροφοριών για τον κάτοχό τους στις υπηρεσίες πληροφοριών, και γνωρίζουμε από τις αποκαλύψεις του Snowden ότι υπάρχουν προγράμματα που συλλέγουν όλα τα αρχεία ήχου των κλήσεων που πραγματοποιούνται σε αρκετές χώρες ανά τον κόσμο. Αυτή η μορφή παρακολούθησης είναι εξαιρετικά επικίνδυνη για την δημοκρατία, πόσο μάλλον για τη δημοσιογραφία, και είναι σε θέση να επιτρέψει μια πιο επεμβατική «αναδρομική» διερεύνηση των ατόμων που θα μπουν στο στόχαστρο των υπηρεσιών πληροφοριών τόσο τώρα όσο και στο μέλλον.

Ως εκ τούτου, αξίζει να χρησιμοποιούμε το τηλέφωνό μας έχοντας πάντα κατά νου το ενδεχόμενο ότι εμείς ή κάποιος από τους συνεργάτες ή τα πρόσωπα με τα οποία επικοινωνούμε μπορεί να βρεθούν στο στόχαστρο των υπηρεσιών πληροφοριών κάποια στιγμή στο μέλλον. Τα κινητά τηλέφωνα δεν είναι ασφαλείς συσκευές επικοινωνίας, έτσι κάθε χρήστης τους πρέπει να αναλογιστεί καλά πώς και πόσο θέλει να τα χρησιμοποιεί για τη μετάδοση εμπιστευτικών και απόρρητων πληροφοριών και δεδομένων.

Στοχευμένη παρακολούθηση τηλεφώνου

Χαμηλό επίπεδο κινδύνου

Σε περιπτώσεις χαμηλού επιπέδου κινδύνου, ο κίνδυνος που πιθανόν θα αντιμετώπισουμε είναι η απόκτηση φυσικής πρόσβασης στο τηλέφωνό μας από μη εξουσιοδοτημένο χρήστη. Εάν συμβεί αυτό, ένας κακόβουλος χρήστης ακόμα και με ελάχιστες γνώσεις πληροφορικής μπορεί να σπάσει τον κωδικό μας (εάν χρησιμοποιούμε κωδικό για το κλείδωμα της συσκευής μας), ο οποίος μας παρέχει την ελάχιστη ασφάλεια. Εάν βρισκόμαστεσε μια κατάσταση χαμηλού επιπέδου κινδύνου, σιγουρευόμαστε ότι έχουμε δημιουργήσει αντίγραφα ασφαλείας (back up) των δεδομένων σας και έχουμε στείλει όλα τα βίντεο ή τα αρχεία ήχου που έχουμε καταγράψει με την συσκευή μας σε μια ασφαλή αποθηκευτική τοποθεσία cloud το συντομότερο δυνατό.

Μπορούν επίσης να χρησιμοποιηθούν εφαρμογές που βοηθούν να εντοπιστεί η συσκευή σε περίπτωση που κλαπεί. Για τα iPhone, η Apple προσφέρει μια δωρεάν εφαρμογή που ονομάζεται ‘Find my iPhone’ και η οποία ενημερώνει για την παρούσα τοποθεσία μιας συσκευής. Μια ακόμη δωρεάν αντικλεπτική εφαρμογή είναι το ‘Prey’ το οποίο, από την στιγμή που θα δηλωθεί ότι ένα κινητό έχει κλαπεί, θα καταγράψει όχι μόνο την παρούσα τοποθεσία της συσκευής, αλλά και όλες τις υπόλοιπες τοποθεσίες στις οποίες θα εμφανιστεί από την στιγμή της κλοπής.

Μεσαίο επίπεδο κινδύνου

Σε περιπτώσεις μεσαίου επιπέδου κινδύνου, ίσως αντιμετωπίσουμε κάποιον κακόβουλο χρήστη ο οποίος προσπαθεί να αποκτήσει πρόσβαση στα δεδομένα μας, όχι μόνο με φυσικό τρόπο, αλλά και απομακρυσμένα. Όταν συνδεόμαστε με το κινητό μας τηλέφωνο σε ένα δημόσιο δίκτυο Wi-Fi, για παράδειγμα, ένας κακόβουλος χρήστης με ελάχιστες γνώσεις πληροφορικής, μπορεί να υποκλέψει πολλές πληροφορίες σχετικές με εμάς από τους συνδεδεμένους email λογαριασμούς μας, καθώς και από τους λογαριασμούς μας στα κοινωνικά δίκτυα.

Επομένως, σε περιπτώσεις μεσαίου επιπέδου κινδύνου, οφείλουμε να επιτηρούμε την φορητή μας συσκευή όσο το δυνατόν πιο στενά, να κλείνουμε τις εφαρμογές μετά την χρήση τους, να απενεργοποιούμε το Wi-Fi σε δημόσιους χώρους, και να χρησιμοποιούμε την επιλογή πτήσης (flight mode) όταν δεν χρειάζεται να είμαστε συνδεδεμένοι.

 Σημείωση για τα smartphones: οι ευπάθειες των smartphones είναι αμέτρητες, από τις οποίες μερικές υπάρχουν στο hardware, και ως εκ τούτου δεν μπορούν να επιδιορθωθούν. Μπορεί να χρησιμοποιηθεί ένα λογισμικού ανοιχτού κώδικα στο smartphone, ακόμη και εφαρμογές για κρυπτογραφημένο chat. Παρόλο αυτά, όπως ανακαλύψαμε στο κομμάτι 'Προστασία συστήματος', όταν το hardware είναι ευπαθές, το λογισμικό δεν μπορεί να παρέχει 100% ασφάλεια.

Όπως είδαμε στο πρόσφατο σκάνδαλο hacking τηλεφώνων που έλαβε χώρα στην Μ. Βρετανία[49], απλοί hackers που ενεργούσαν για λογαριασμό ανήθικων δημοσιογράφων ήταν σε θέση να ακούσουν και να παρακολουθήσουν προσωπικούς τηλεφωνητές. Αρκετοί ιδιωτικοί ερευνητές έχουν επίσης την δυνατότητα να ακούν και να καταγράφουν όχι μόνο τον τηλεφωνητή, αλλά και κάθε κλήση που πραγματοποιείται ή λαμβάνεται από έναν αριθμό. Επομένως, όλοι οι χρήστες θα πρέπει να σκεφτούν καλά προτού συζητήσουν μέσω κινητού ή σταθερού τηλεφώνου για οποιοδήποτε ευαίσθητο θέμα.

Υψηλό επίπεδο κινδύνου

Σε περιπτώσεις υψηλού κινδύνου, το τηλέφωνό μας είναι στην ουσία ο εχθρός μας. Το λιγότερο που μπορεί να αποκαλυφθεί είναι η τοποθεσία μας και όλα τα σχετιζόμενα μεταδεδομένα να βρεθούν κατευθείαν στα χέρια της εκάστοτε υπηρεσίας πληροφοριών. Το χειρότερο σενάριο είναι ότι, μπορεί να χρησιμοποιηθεί για να συλλέξει μυστικά το περιεχόμενο όλων των κλήσεών μας, όλα τα δεδομένα που υπάρχουν αποθηκευμένα στο τηλέφωνό μας, ακόμη και να ενεργοποιηθεί απομακρυσμένα το μικρόφωνο και η κάμερα για την καταγραφή εικόνας και ήχου (εάν υπάρχει κάμερα στο κινητό). Αυτού του είδους η παρακολούθηση τηλεφώνου δεν είναι τόσο σπάνιο φαινόμενο και επί της ουσίας με μηδενικό κόστος για μια υπηρεσία πληροφοριών.Έτσι δεν είναι απαραίτητο να είμαστε ένας σημαντικός στόχος για να πραγματοποιηθεί μια τέτοιου είδους εισβολή στα προσωπικά μας δεδομένα.

Ο μόνος αποτελεσματικά ασφαλής τρόπος για να πραγματοποιήσουμε τηλεφωνικές επικοινωνίες είναι η χρήση των κινητών τηλεφώνων μιας χρήσης. Ιδανικά, το τηλέφωνο μιας χρήσης και το κανονικό μας τηλέφωνο δεν θα πρέπει ποτέ να εκπέμπουν σήμα ταυτόχρονα, αφού (εάν αποτελούμε στόχο), το πραγματικό μας τηλέφωνο θα πιάσει το σήμα του τηλεφώνου μιας χρήσης, κι έτσι θα μετατραπεί σε στόχο και αυτό.

Προτού χρησιμοποιήσουμε ένα τηλέφωνο μιας χρήσης, σιγουρευόμαστε ότι το τηλέφωνο που είναι συσχετισμένο με εμάς (π.χ. το smartphone μας) δεν εκπέμπει σήμα. Αλλάζοντας το κινητό μας σε κατάσταση πτήσης, αφαιρώντας την μπαταρία (μπορεί να γίνει ακόμη και σ' ένα iPhone), και απενεργοποιώντας το εξ' ολοκλήρου είναι λύσεις, αλλά όχι αρκετές. Καλό είναι να πραγματοποιήσουμε τις προαναφερθείσες ενέργειες και στη συνέχεια να το τοποθετήσουμε σε κουτί Faraday (αποτροπή οποιασδήποτε επικοινωνίας).

[49] http://www.bbc.com/news/uk-28086528

Τα τηλέφωνα μιας χρήσης είναι αρκετά οικονομικές συσκευές, αγορασμένες με μετρητά, οι οποίες μπορούν να πεταχτούν μετά την χρήση τους. Οι συσκευές μιας χρήσης είναι παλιάς τεχνολογίας – καθόλου προηγμένες – και περιέχουν μια προπληρωμένη κάρτα SIM που δεν συνδέεται με τον χρήστη εξασφαλίζοντας ανωνυμία. Σε ορισμένες χώρες είναι δύσκολο να αγοραστεί μια κάρτα SIM χωρίς να ενεργοποιηθεί παρέχοντας προσωπικά στοιχεία. Επομένως, η αγορά μιας κάρτας από δεύτερο χέρι, ή το να έχουμε ένα πρόσωπο που θα μπορέσει να μας προμηθεύσει με τέτοιες κάρτες, είναι δυο καλές επιλογές.

Αφού χρησιμοποιήσουμε μερικές φορές αυτό το τηλέφωνο, υπάρχει η πιθανότητα να συνδεθεί μαζί μας και να αποτελέσει στόχο παρακολούθησης. Στο σημείο αυτό μπορούμε να καταστρέψουμε τη συσκευή και να προμηθευτούμε μια νέα. Το να αλλάξουμε απλά την κάρτα SIM δεν είναι αρκετό – κάθε συσκευή τηλεφώνου έχει έναν κωδικό IMEI (International Mobile Equipment Identity) ο οποίος προσδιορίζει την φορητή συσκευή. Εάν η κάρτα SIM έχει συνδεθεί με εμάς, το ίδιο θα έχει συμβεί και με το αντίστοιχο IMEI – έτσι το μόνο που απομένει είναι η πλήρης καταστροφή του τηλεφώνου.

Λόγω του ότι οι υπηρεσίες πληροφοριών είναι σε θέση να καταγράψουν πλήρως τις τηλεφωνικές κλήσεις των στόχων, θα πρέπει να αποφεύγουν οι χρήστες να μοιράζονται στις τηλεφωνικές τους κλήσεις ευαίσθητες πληροφορίες – ακόμη κι εάν χρησιμοποιούν τηλέφωνο μιας χρήσης.

Κλήσεις και βιντεοκλήσεις μέσω Διαδικτύου

Τα λογισμικά που μας παρέχουν την δυνατότητα να πραγματοποιήσουμε κλήσεις και βιντεοκλήσεις μέσω διαδικτύου (Voice over Internet Protocol, VoIP), όπως είναι το Skype, είναι εξαιρετικά δημοφιλή και χρήσιμα. Το Skype από μόνο του απαριθμεί περισσότερους από 700 εκατομμύρια χρήστες.

Ωστόσο, το Skype δεν παρέχει μεγάλη ασφάλεια και για τον λόγο αυτό προτείνουμε εναλλακτικά τη χρήση της εφαρμογής Viber. Παρόλα αυτά, δυστυχώς δεν υπάρχει ακόμη κάποια ασφαλής εναλλακτική επιλογή που να είναι φιλική προς το χρήστη.

Μέσα στις αποκαλύψεις του Snowden υπάρχουν πληροφορίες για την ικανότητα της Εθνικής Υπηρεσίας Πληροφοριών των Η.Π.Α. (NSA) να υποκλέπτει και να αποθηκεύει τις επικοινωνίες που πραγματοποιούνται μέσω Skype (μην ξεχνάμε ότι πλέον ανήκει στη Microsoft). Θα πρέπει να λάβουμε υπόψη μας πως όλες οι επικοινωνίες που πραγματοποιούμε μέσω Skype δεν μένουν μεταξύ ημών και των επαφών μας, αλλά τις μοιραζόμαστε και με τις υπηρεσίες πληροφοριών ή τον εκάστοτε ωτακουστή.

Για παράδειγμα,ο Glenn Greenwald διηγείται μια εμπειρία του[50], όταν χρησιμοποίησε το Skype στο Hong Kong για να καλέσει τον συνεργάτη του που βρισκόταν στο Rio, τον David Miranda, για να τον ενημερώσει ότι θα λάβει μερικά κρυπτογραφημένα έγγραφα

[50] http://www.buzzfeed.com/natashavc/david-miranda-is-nobodys-errand-boy#.qvbm8Q4NzK

μέσω email, και να τα αποθηκεύσει σε ένα ασφαλές μέρος. Ο Greenwald ποτέ δεν έστειλε τα αρχεία – αλλά 48 ώρες αργότερα, το λάπτοπ του Miranda κλάπηκε από το σπίτι του στο Rio.

Θα πρέπει επίσης να υποθέσουμε ότι δεν είναι μόνο οι προηγμένες υπηρεσίες που έχουν συγκεκαλυμμένη πρόσβαση, ή που εκμεταλλεύονται τα ελαττώματα ασφαλείας. Για παράδειγμα, η μυστική αστυνομία της Αιγύπτου είναι γνωστό πως έχει αγοράσει εργαλεία διείσδυσης για το Skype.Επίσης, πολλές επιθέσεις man-in-the-middle μέσω Skype έχουν αναφερθεί από ακτιβιστές στην Ασία[51].

Οι ασφαλείς κλήσεις και βιντεοκλήσεις εξελίσσονται με τον καιρό (π.χ. αναζητήστε το Jitsi) αλλά προς το παρόν δεν είναι προσβάσιμες στους μη-ειδικούς.

[51] http://www.dailynewsegypt.com/2015/07/06/egypts-purchase-of-hacking-software-documented-in-new-leaks/

Κεφάλαιο 8: Κωδικοί Πρόσβασης

Όλα τα συστήματα και τα εργαλεία στο παρόν έγγραφο χρησιμοποιούν κωδικούς ως μέθοδο αναγνώρισης των εξουσιοδοτημένων χρηστών και προστασίας ενάντια στην μη εξουσιοδοτημένη πρόσβαση. Οι ισχυροί κωδικοί αποτελούν το πρωταρχικό – και τις περισσότερες φορές το μοναδικό – πλέγμα άμυνας σε όλα τα επίπεδα της ασφάλειας δεδομένων.

Παρόλο αυτά, ας έχουμε κατά νου ότι οι κωδικοί στους διαδικτυακούς λογαριασμούς προστατεύουν κυρίως από κακόβουλους χρήστες με χαμηλούς πόρους.

Ίσως υπάρχουν κερκόπορτες πρόσβασης στους online λογαριασμούς σε κρατικό επίπεδο, καθιστώντας έτσι τον κωδικό μας άχρηστο. Αυτός είναι ένας καλός λόγος για να κρυπτογραφούμε τα emails μας – μπορεί να έχουμε έναν πολύ ισχυρό κωδικό πρόσβασης στο Hotmail, αλλά αυτό από μόνο του δεν θα σταματήσει τις υπηρεσίες πληροφοριών να πιέσουν τον εκάστοτε πάροχο για να τους παρέχει όλα τα emails μας (ή πολύ πιθανόν, να συλλέξουν μυστικά και να υποκλέψουν τα μηνύματά μας χωρίς να ζητήσουν καν άδεια).

Εάν τα emails μας είναι κρυπτογραφημένα, το μόνο που θα μπορέσουν να συλλέξουν από το Hotmail είναι ένας σωρός από κωδικούς που δεν σπάνε.

Έτσι, ενώ οι ισχυροί κωδικοί παραμένουν πάντα μια καλή ιδέα, οι κωδικοί που προστατεύουν το σύστημά μας (π.χ. κρυπτογράφηση σκληρού δίσκου) και τα προγράμματα κρυπτογράφησης είναι κατά πολύ περισσότερο σημαντικοί από τους κωδικούς που χρησιμοποιούνται στους διαδικτυακούς λογαριασμούς.

Ο κίνδυνος έγκειται στο να:

- Ξεχαστούν / χαθούν οι κωδικοί.
- Υπερπηδήσουν (bypass)τους κωδικούς (για τους διαδικτυακούς λογαριασμούς).
- Χακάρουν τον κωδικό (σχετικά μη προηγμένο hacking κωδικών).
- Σπάσουν τον κωδικό (εξελιγμένη τακτική).
- Παρακολουθήσουν το πληκτρολόγιο (Key logger).
- εκβιάσουν για να αποκαλυφθεί ένας κωδικός.

Ενέργειες Ασφάλειας Πληροφοριακών Συστημάτων:

- Εκμάθηση δημιουργίας ισχυρών κωδικών.
- Χρήση του KeePassX password manager (εάν υπάρχει εμπιστοσύνη στο σύστημα).
- Απομνημόνευση των πιο σημαντικών κωδικών.
- Χρήση κρυφών χώρων αποθήκευσης για τα πιο σημαντικά κρυπτογραφημένα αρχεία.

Παραβίαση κωδικών (Password cracking): κατανοώντας τον κίνδυνο

Εάν το σύστημά κάποιου χρήστη είναι επισφαλές, η παραβίαση του κωδικού σε μια στοχευμένη επίθεση είναι μια απλή υπόθεση. Ο εκάστοτε κακόβουλος χρήστης θα μπορούσε με φυσικό τρόπο ή απομακρυσμένα να εισάγει ένα key logger (σύστημα παρακολούθησης πληκτρολόγησης) στο σύστημά του, για να καταγράψει κάθε χαρακτήρα που πληκτρολογεί. Αυτό πρακτικά σημαίνει ότι ο εκάστοτε κακόβουλος χρήστης καταγράφει κάθε πάτημα που κάνει ο χρήστης στο πληκτρολόγιό του, συμπεριλαμβανομένων των κωδικών του. Για να το καταφέρει αυτό δεν χρειάζεται κάποιο εξαιρετικά προηγμένο εργαλείο και επιπλέον ακυρώνει άλλα μέτρα ασφαλείας που πιθανόν να έχει λάβει. Επιπλέον, είναι εξαιρετικά σημαντικό να ασφαλιστεί το σύστημά από την πρώτη κιόλας στιγμή, όπως περιγράψαμε νωρίτερα στα κεφάλαια 1 και 2.

Παρόλο αυτά, εάν το σύστημά είναι ασφαλές και ο εκάστοτε κακόβουλος χρήστης δεν (μπορεί να) χρησιμοποιεί εργαλεία key logging, ένας επιτιθέμενος ίσως προσπαθήσει να σπάσει τους κωδικούς που προστατεύουν το σύστημά, το λογισμικό και τους λογαριασμούς (και αυτό μπορεί να συμβεί είτε μέσω μιας μαζικής επίθεσης σε χιλιάδες χρήστες, είτε μια στοχευμένη επίθεση εναντίον ενός χρήστη).

Τα προγράμματα που εξειδικεύονται στην παραβίαση κωδικών πρόσβασης χρησιμοποιούνται από τις νομικές αρχές ανά τον κόσμο, αλλά οι προηγμένες εκδόσεις τους είναι επίσης διαθέσιμες ως εμπορικά προϊόντα. Ένα πρόγραμμα password cracker μπορεί αυτόματα να ελέγξει το λιγότερο οκτώ εκατομμύρια κωδικούς ανά δευτερόλεπτο και μπορεί να τρέχει για μέρες, σε πολλές μηχανές ταυτόχρονα. Για έναν στόχο υψηλού προφίλ, ένας password cracker μπορεί να τρέχει σε πολλαπλές μηχανές, για μήνες.

Τα προγράμματα σπασίματος κωδικών -Password crackers- δοκιμάζουν πρώτα τους πιο συνηθισμένους κωδικούς. Ένα πρόγραμμα password cracking θα ξεκινήσει με την βοήθεια λεξικού, με τους πιο κοινούς κωδικούς, όπως είναι τα "letmein," "temp," "123456," κ.ο.κ., και στη συνέχεια τους εξετάζει σε συνδυασμό με τις 100 πιο κοινές καταλήξεις: "1," "4u," "69," "abc," "!," κ.ο.κ.. Θεωρείται ότι περίπου το ένα τέταρτο όλων των κωδικών μπορούν να σπάσουν μόνο με αυτούς τους 100.000 συνδυασμούς.

Οι crackers χρησιμοποιούν διαφορετικά λεξικά: Αγγλικές λέξεις, ονόματα, ξένα ονόματα, φωνητικούς συνδυασμούς, και το ίδιο κάνουν και για τις ρίζες, δύο ψηφία, ημερομηνίες κλπ.. Τρέχουν και λεξιλόγια με διάφορους τρόπους γραφής και τα συνηθισμένα υποκατάστατα: το "$" αντί του "s", το "@" αντί του "a," "1" αντί του "l" κ.ο.κ.. Μέσω της συγκεκριμένης στρατηγικής παραβιάζονται περίπου τα δυο τρίτα όλων των κωδικών πρόσβασης σε ελάχιστο χρονικό διάστημα.

Ο εκάστοτε κακόβουλος χρήστης μπορεί να προσφέρει όλες τις προσωπικές πληροφορίες που βρίσκει για τον δημιουργό του κωδικού στα προγράμματα σπασίματος κωδικών. Ένας καλός password cracker θα εξετάσει τα ονόματα και τις διευθύνσεις από το ευρετήριο (οι ταχυδρομικοί κωδικοί είναι συνηθισμένο εξάρτημα κωδικού), σημαντικές ημερομηνίες, και οποιαδήποτε άλλη πληροφορία έχει στη διάθεσή του.

Μια τέτοιου είδους εξελιγμένη επίθεση μπορεί να ξεκινήσει εάν το hardware είναι επισφαλές. Ο εκάστοτε επιτιθέμενος μπορεί να δει τον σκληρό δίσκο του στόχου και να δημιουργήσει ένα λεξικό που περιλαμβάνει κάθε εκτυπώσιμο string, συμπεριλαμβανομένων των διεγραμμένων αρχείων. Εάν ποτέ αποθηκεύσαμε κάποιον κωδικό μας σε ένα ανεξαρτήτου τύπου αρχείο κάπου στον υπολογιστή μας, ή εάν κάποιο πρόγραμμα το έχει αποθηκεύσει στην μνήμη του, τότε μέσω αυτής της διαδικασίας θα πάρει τον κωδικό και θα τον χρησιμοποιήσει με σκοπό να παραβιάσει τον εκάστοτε λογαριασμό μας.

Πως δημιουργείται ένας ισχυρός κωδικός πρόσβασης

Ο ισχυρός κωδικός είναι αυτός που δεν θα μπορέσει να παραβιαστεί από την διαδικασία που περιγράψαμε παραπάνω.

Password manager

Μια επιλογή είναι να χρησιμοποιήθεί ένα λογισμικό διαχείρισης κωδικών ανοιχτού πηγαίου κώδικα όπως είναι το KeePassX[52] για να δημιουργηθούν τυχαίοι, μεγάλοι αλφαρηθμικοί κωδικοί (με σύμβολα επίσης, εάν κι εφόσον επιτρέπονται), και στην συνέχεια να αποθηκευτούν στην κρυπτογραφημένη βάση δεδομένων.

Επιπλέον, είναι ένας καλός τρόπος να αποθηκεύονται πολλαπλοί πολύπλοκοι κωδικοί για πολλαπλούς λογαριασμούς, με το KeePassX να διαθέτει επίσης πεδία εισαγωγής URLs, ονομάτων λογαριασμών και σχολίων για κάθε κωδικό που αποθηκεύεται, έτσι ώστε να μπορούν να φυλάσσονται με ασφάλεια όλες οι πληροφορίες που χρειάζεται ο εκάστοτε χρήστης για τον εκάστοτε λογαριασμό. Οι τυχαίοι κωδικοί που δημιουργούνται δεν μπορούν να απομνημονευθούν, γεγονός που ενισχύει την ισχυρότητά τους. Παρόλο αυτά, το KeePassX επιτρέπει εύκολα και απλά να γίνει αντιγραφή και επικόλληση των κωδικών από την βάση δεδομένων, έτσι ώστε να μην είναι απαραίτητη η πληκτρολόγησή τους. Υπάρχει μια αμφισβήτηση ως προς την ικανότητα αυτών των προγραμμάτων να δημιουργούν αποδοτικούς τυχαίους συνδυασμούς, αλλά το ανθρώπινο μυαλό πραγματικά υστερεί σε αυτό το σημείο. Έτσι τα προγράμματα αυτά παραμένουν οι καλύτερες επιλογές που διαθέτουμε μέχρι στιγμής.

Θα χρειαστεί να δημιουργηθεί ένας master κωδικός για το KeePassX, ο οποίος θα πρέπει να είναι πολύ ισχυρός. Θα πρέπει να προσπαθήσουμε να τον αποθηκεύσουμε στο μυαλό μας και μόνο και φυσικά να μην τον ξεχάσουμε.

[52] https://www.keepassx.org/

Σχήμα Schneier (Schneier Scheme)[53]

Θα πρέπει να δημιουργούνται χειροκίνητα οι κωδικοί για την κρυπτογράφηση ενός συστήματός, οποιουδήποτε κρυπτογραφημένου USB stick ή άκρως σημαντικού αρχείου (π.χ. έγγραφα της πηγής των χρηστών), και του password manager. Αυτοί οι σημαντικοί κωδικοί θα πρέπει να αποθηκεύονται αποκλειστικά και μόνο στην μνήμη των χρηστών, και για αυτόν ακριβώς το λόγο θα πρέπει να είναι εύκολοι στην απομνημόνευση.

Φυσικά, για να ελαχιστοποιηθεί ο κίνδυνος της έκθεσης ενός κωδικού, θα πρέπει να αποφευχθεί να επαναχρησιμοποιείται.

Για να δημιουργηθεί χειροκίνητα ένας κωδικός, προτείνουμε το 'σχήμα Schneier', μια μέθοδος που ανακαλύφθηκε από τον Bruce Schneier, έναν διεθνούς φήμης κρυπτογράφο και ειδικό σε θέματα ασφαλείας.

Ο Schneier συμβουλεύει να πάρουμε μια φράση που μπορούμε να την απομνημονεύσουμε εύκολα, και να την παραφράσουμε με τη χρήση συμβόλων, αριθμών και χαρακτήρων κι έτσι να την μετατρέψουμε σε έναν ισχυρό κωδικό πρόσβασης.

Για παράδειγμα, η φράση "This little piggy went to market" μπορεί να μετατραπεί σε "tlpWENT2m". Αυτός ο κωδικός των εννέα χαρακτήρων δεν μπορεί να συμπεριλαμβάνεται στα κοινά λεξικά. Διαλέγουμε την δική μας πρόταση η οποία όμως να μην συνδέεται με τα προσωπικά μας δεδομένα που είναι διαθέσιμα δημόσια.

Παρακάτω μπορούμε να δούμε μερικά παραδείγματα:

- Wlw7,mstmsritt... = When I was seven, my sister threw my stuffed rabbit in the toilet.
- Wow...doestcst = Wow, does that couch smell terrible.
- Ltime@go-inag~faaa! = Long time ago in a galaxy not far away at all.
- uTVM,TPw55:utvm,tpwstillsecure = Until this very moment, these passwords were still secure.

(Φυσικά, δεν θα πρέπει να χρησιμοποιηθούν τα παραπάνω παραδείγματα – από την στιγμή που χρησιμοποιήθηκαν είναι μη ασφαλείς επιλογές κωδικών).

Εξαναγκασμός για αποκάλυψη ενός κωδικού

Ας ελπίσουμε πως ποτέ δεν θα βρεθεί κάποιος σε αυτή την κατάσταση. Παρόλο αυτά, ας υποθέσουμε πως μια κακόβουλη ομάδα ή υπηρεσία μας έχει απαγάγει, και έχουμε πάνω μας ένα κρυπτογραφημένο USB stick (που περιέχει τα πιο σημαντικά μας έγγραφα ή τα έγγραφα που πήραμε απο κάποιον συνεργάτη μας), και είναι έτοιμοι να κάνουν τα αδύνατα δυνατά για να αποκτήσουν τον κωδικό αποκρυπτογράφησής του. Πως θα αντιδρούσαμε;

[53] https://www.schneier.com/blog/archives/2014/03/choosing_secure_1.html

Για τέτοιες περιπτώσεις, θα ήταν πολύ χρήσιμο, να διατηρούμε έναν κρυμμένο χώρο στον USB δίσκο μας. Ένας κρυμμένος χώρος δεν μπορεί να είναι ορατός από κανέναν και δεν φαίνεται πως καταλαμβάνει χώρο στον δίσκο. Για αυτόν τον λόγο, μπορεί να υπερκαλυφθεί από άλλα δεδομένα σχετικά εύκολα. Αυτό σημαίνει ότι ένα ορατό κρυπτογραφημένο σύνολο δεδομένων μπορεί να λειτουργήσει ως δόλωμα. Σε αυτό το ορατό κρυπτογραφημένο σύνολο δεδομένων, μπορούμε να αποθηκεύσουμε αρχεία τα οποία εύλογα θα πρέπει να έχουν αποθηκευτεί με ασφάλεια και να έχουν κρυπτογραφηθεί, και αυτό το σύνολο δεδομένων θα πρέπει να έχει τον δικό του κωδικό πρόσβασης. Παρόλο αυτά, το κρυμμένο κρυπτογραφημένο σύνολο δεδομένων θα υπάρχει μη ανιχνεύσιμο κάτω από το ορατό, και θα έχει έναν διαφορετικό κωδικό.

Μπορούμε να δημιουργήσουμε ένα κρυφό κρυπτογραφημένο σύνολο δεδομένων μέσω του TrueCrypt (κεφάλαιο 4). Αυτή η μέθοδος θα μας βοηθήσει να προστατεύσουμε τα δεδομένα μας από τυχόν υποκλοπές, αλλά όχι από την απώλεια – μπορεί εύκολα να καταστραφεί ή να υπερκαλυφθεί με άλλα δεδομένα, και έτσι θα πρέπει να διατηρούνται πάντοτε αντίγραφα ασφαλείας για τα σημαντικά έγγραφα.

Κεφάλαιο 9: Επίλογος

Στην εποχή της παγκοσμιοποίησης, οι απειλές μεταβάλλονται συνεχώς και μαζί με αυτές αλλάζουν και οι τεχνολογίες που είναι διαθέσιμες για την προστασία των πολιτών, αλλά και στην περίπτωση αυτού του εγχειριδίου των δημοσιογράφων. Τα στοιχεία που αναφέρθηκαν παραπάνω και η ανάλυση που ακολούθησε αποδεικνύουν την σημασία της κατανόησης της ασφάλειας των πληροφοριακών συστημάτων και κατ' επέκταση των πληροφοριών και των δεδομένων που αυτά διαχειρίζονται εις βάθος, τόσο σε θεωρητικό όσο και σε πρακτικό επίπεδο.

Είναι αρκετά σημαντικό να αναφερθεί ότι το σύνολο του παρόντος οδηγού αναφέρεται σε δωρεάν διαθέσιμα εργαλεία που αποσκοπούν στην ενίσχυση της ασφάλειας των χρηστών. Με την ανωτέρω αναφορά παρατηρούμε ότι τελικά η ασφάλεια των υπολογιστικών συστημάτων, τουλάχιστον σε επίπεδο μεμονομένων χρηστών, δεν είναι «ακριβό σπόρ» όπως αρκετοί θεωρούν εσφαλμένα. Στην περίπτωση που ο εκάστοτε χρήστης αφιερώνει τον ελάχιστο χρόνο για να ενημερώνεται για εργαλεία ασφάλειας και πρακτικές λύσεις στην κατεύθυνση αυτή, το αποτέλεσμα θα είναι αρκετά ικανοποιητικό. Είναι καλό ο κάθε ένας να εφαρμόσει τα περισσότερα από τα βήματα που αναφέρουμε εάν είναι δυνατόν μόνος του, ώστε να κατανοήσει καλύτερα τι είναι αυτό που υλοποιείται ανά περίπτωση αλλά και να διδαχθεί από το εκάστοτε λάθος. Μέχρι στιγμής είδαμε ένα σύνολο από σχετικά εύκολα βήματα – ενέργειες τα οποία μπορούν συνδυαστικά να οδηγήσουν στο επιθυμητό επίπεδο ασφάλειας ανά περίπτωση.

Τέλος, η ασφάλεια των υπολογιστικών συστημάτων που διαχειριζόμαστε ξεκινάει απο εμάς πρωτίστως και σε δεύτερο χρόνο από τις εφαρμογές και τα πρόσθετα που χρησιμοποιούμε, είτε υλικά είτε λογισμικά. Επομένως η ενημέρωση μας για τις πιο πρόσφατες τεχνικές και μεθόδους ασφάλειας αποτελεί προτεραιτότητα για την επίτευξη του βέλτιστου επιπέδου ασφάλειας.

Γλωσσάριο

Air-gapped =σε κενό αέρος. Μέτρο ασφαλείας σύμφωνα με το οποίο ένας φορητός υπολογιστή είναι τελείως offline, διαχωρισμένος από άλλα τοπικά δίκτυα και το διαδίκτυο.

Backdoors Μυστικές ευπάθειες ασφαλείας που επιτρέπουν την παράκαμψη γνωστών μηχανισμών ασφαλείας ενός συστήματος, επιτρέποντας μη ανιχνεύσιμη πρόσβαση στον υπολογιστή ή τα δεδομένα του.

BIOS Basic Input/Output System – ένα σύνολο οδηγιών υπολογιστή στο firmware που ελέγχουν λειτουργίες εισόδου και εξόδου.

Bridges (Tor) Οι γέφυρες είναι κόμβοι του δικτύου Tor που βοηθούν στην αποφυγή λογοκρισίας.

Dragnet Ένα σύστημα επιτήρησης που λειτουργεί μέσω προγραμμάτων που συλλέγουν online και τηλεπικοινωνιακά δεδομένα ανά τον κόσμο.

Faraday cage Ένα μεταλλικό (συνήθως) περίβλημα που αποτρέπει την είσοδο ή τη διαφυγή του ηλεκτρομαγνητικού πεδίου.

Firmware Λογισμικό προγραμματισμένο πάνω στο hardware για να παρέχει οδηγίες για το πώς η συσκευή επικοινωνεί με τα άλλα υλικά του υπολογιστή (συμπεριλαμβανομένου του BIOS).

Hardware Τα φυσικά στοιχεία που περιλαμβάνουν ένα σύστημα υπολογιστή.

Malware Κακόβουλο λογισμικό, συνήθως spyware, που έχει σχεδιαστεί για να διαταράξει ή να καταστρέψει ένα υπολογιστικό σύστημα.

Man-in-the-middle attack Η συγκεκαλυμμένη παρακολούθηση των επικοινωνιών μέσω της πλαστοπροσωπίας ενός στόχου.

Metadata Δεδομένα των δεδομένων.

Middleware Πρόγραμμα το οποίο μεσολαβεί μεταξύ δύο διαφορετικών και συχνά ήδη υπάρχοντων προγραμμάτων: π.χ. επιτρέπει στα προγράμματα πρόσβαση σε βάσεις δεδομένων.

Open source Λογισμικό του οποίου ο πηγαίος κώδικας είναι διαθέσιμος στο κοινό.

Operating system το λογισμικό του υπολογιστή που είναι υπεύθυνο για τη διαχείριση και τον συντονισμό των εργασιών, καθώς και την κατανομή των διαθέσιμων πόρων. Το λειτουργικό σύστημα παρέχει ένα θεμέλιο, ένα μεσολαβητικό επίπεδο λογικής διασύνδεσης μεταξύ λογισμικού και υλικού, διαμέσου του οποίου οι εφαρμογές αντιλαμβάνονται εμμέσως τον υπολογιστή.

Βιβλιογραφία

1. MASHABLE NEWS. (2014) The 10 Biggest Revelations From Edward Snowden's Leaks. [Online] Available from: http://mashable.com/2014/06/05/edward-snowden-revelations/#SNq8ERbziiqI [Accessed: 24th August 2015].
2. CBS NEWS. (2015) Ethiopian journalists jailed for government criticisms. [Online] Available from: http://www.cbsnews.com/videos/ethiopian-journalists-jailed-for-government-criticisms/ [Accessed: 23th August 2015].
3. FUTURE-TENSE NEWS. (2012) Mexico Turns to Surveillance Technology To Help Fight Drug War. [Online] Available from: http://www.slate.com/blogs/future_tense/2012/08/03/surveillance_technology_in_mexico_s_drug_war_.html [Accessed: 25th August 2015].
4. WIKIPEDIA. (2006-2015) List of journalists and media workers killed in Mexico [Online] Available from: https://en.wikipedia.org/wiki/List_of_journalists_and_media_workers_killed_in_Mexico [Accessed: 29th August 2015].
5. THE NEW YORK TIMES. (2015) N.S.A Collection of Bulk Call Data Is Ruled Illegal [Online] Available from: http://www.nytimes.com/2015/05/08/us/nsa-phone-records-collection-ruled-illegal-by-appeals-court.html?_r=0 [Accessed: 26th August 2015].
6. THE CRYPTO LAW SURVEY. (2013) A survey of existing and proposed laws and regulations on cryptography - systems used for protecting information against unauthorized access. [Online] Available from: http://www.cryptolaw.org/ [Accessed: 30th August 2015].
7. WIKIPEDIA. (2014) Glenn Greenwald [Online] Available from: https://en.wikipedia.org/wiki/Glenn_Greenwald [Accessed: 29th August 2015].
8. COMMON DREAMS NEWS. (2015) Victory for Privacy, Vindication for Snowden as Phone Dragnet Sunsets [Online] Available from: http://www.commondreams.org/news/2015/06/01/victory-privacy-vindication-snowden-phone-dragnet-sunsets [Accessed: 28th August 2015].
9. BBC NEWS. (2014) Edward Snowden: Leaks that exposed US spy programme [Online] Available from: http://www.bbc.com/news/world-us-canada-23123964 [Accessed: 28th August 2015].
10. PREY PROJECT. (2013) A lightweight theft protection software that lets you recover your devices if ever lost or stolen. [Online] Available from: https://preyproject.com [Accessed: 1st September 2015].
11. OPEN SOURCE INITIATIVE. (1998) A non-profit corporation with global scope formed to educate about and advocate for the benefits of open source and to build bridges among different constituencies in the open source community. [Online] Available from: www.opensource.org/osd [Accessed: 1st September 2015].
12. TAILS PROJECT. (2013) A live operating system which aims at preserving a users privacy and anonymity. [Online] Available from: https://tails.boum.org/ [Accessed: 1st September 2015].
13. UBUNTU PROJECT. (2004) A Debian-based Linux operating system and distribution. [Online] Available from: http://www.ubuntu.com/download/desktop [Accessed: 2nd September 2015].
14. UBUNTU PROJECT. (2004) A Debian-based Linux operating system and distribution – guide for live usb. [Online] Available from: http://www.ubuntu.com/download/desktop [Accessed: 2nd September 2015].
15. TAILS PROJECT. (2013) First steps for Tails - the live operating system which aims at preserving a user's privacy and anonymity. [Online] Available from: https://tails.boum.org/doc/first_steps/index.en.html [Accessed: 1st September 2015].
16. UNETBOOTIN PROJECT. (2010) Bootable live USB creator for Ubuntu, Fedora, and Linux distributions. [Online] Available from: https://sourceforge.net/projects/unetbootin/files/UNetbootin/494/ [Accessed: 2nd September 2015].
17. TAILS PROJECT. (2013) Manual install Tails using Linux. [Online] Available from: https://tails.boum.org/doc/first_steps/installation/manual/linux/index.en.html [Accessed: 1st September 2015].

18. TAILS PROJECT. (2013) Manually copying persistent data to a new device. [Online] Available from: https://tails.boum.org/doc/first_steps/persistence/copy/index.en.html [Accessed: 1st September 2015].
19. WIKIPEDIA. (2014) Onion Rooting [Online] Available from: https://en.wikipedia.org/wiki/Onion_routing [Accessed: 26th August 2015].
20. BRIDGES – TOR PROJECT. (2012) Tor relays that help circumvent censorship. [Online] Available from: https://bridges.torproject.org/ [Accessed: 3rd September 2015].
21. MOZILLA FIREFOX PROJECT. (2013) Downloading Mozilla's web browser. [Online] Available from: http://www.getfirefox.com/ [Accessed: 3rd September 2015].
22. GOOGLE CHROMIUM PROJECT. (2015) Downloading Chromium web browser from MacUpdate. [Online] Available from: http://www.macupdate.com/app/mac/36244/chromium [Accessed: 4th September 2015].
23. PRIVACY & SECURITY – FIREFOX ADD-ONS. (2015) Privacy & Security related add-ons for Firefox browser. [Online] Available from: https://addons.mozilla.org/en-US/firefox/extensions/privacy-security/ [Accessed: 4th September 2015].
24. ELECTRONIC FRONTIER FOUNDATION. (2013) HTTPS Everywhere a Firefox, Chrome, and Opera extension that encrypts communications with many major websites, making browsing more secure. [Online] Available from: https://www.eff.org/https-everywhere [Accessed: 7th September 2015].
25. NOSCRIPT PROJECT. (2013) provides extra protection for web browsers. [Online] Available from: https://noscript.net/ [Accessed: 7th September 2015].
26. GHOSTERY PROJECT. (2013) provides extra protection blocking a great range of agents. [Online] It was available from: https://ghostery.com/ [Accessed: 26th January 2015].
27. WEB OF TRUST PROJECT. (2013) A free browser extension that tells you which websites you can trust. [Online] Available from: https://www.mywot.com/ [Accessed: 9th September 2015].
28. LAST PASS PROJECT. (2013) A tool that remembers passwords. [Online] Available from: https://lastpass.com/ [Accessed: 9th September 2015].
29. THE TOR PROJECT. (2002) A free software for enabling anonymous communication.. [Online] Available from: https://www.torproject.org/ [Accessed: 5th August 2015].
30. TOR PROJECT - BRIDGES. (2012) Tor relays that help circumvent censorship. [Online] Available from: https://bridges.torproject.org/ [Accessed: 3rd September 2015].
31. MICAHFLEE - TOR BROWSER LAUNCHER. (2012) A program to help download, keep updated, and run the Tor Browser Bundle. [Online] Available from: https://github.com/micahflee/torbrowser-launcher#tor-browserlauncher [Accessed: 3rd September 2015].
32. TRUE CRYPT PROJECT. (2004) A discontinued source-available freeware utility used for on-the-fly encryption. [Online] Available from: https://truecrypt.ch/ [Accessed: 8th August 2015].
33. TRUE CRYPT PROJECT. (2010) A guide to install and configure True Crypt. [Online] Available from: https://download.truecrypt.ch/documentation/TrueCrypt%20User%20Guide.pdf [Accessed: 8th August 2015].
34. MEGA PROJECT. (2013) A cloud storage and file hosting service. [Online] Available from: https://mega.co.nz/ [Accessed: 4th September 2015].
35. BLEACHBIT PROJECT. (2008) Quickly frees disk space and tirelessly guards your privacy. [Online] Available from: http://bleachbit.sourceforge.net/ [Accessed: 10th September 2015].
36. LIBRE OFFICE PROJECT. (2011) A free and open source office suite, developed by The Document Foundation. [Online] Available from: https://www.libreoffice.org/ [Accessed: 10th September 2015].
37. LAVABIT PROJECT. (2004-2013) A discontinued encrypted webmail service currently unavailable. [Online] Available from: https://en.wikipedia.org/wiki/Lavabit [Accessed: 12th September 2015].
38. THE GUARDIAN NEWS. (2014) Secrets, lies and Snowden's email: why I was forced to shut down Lavabit. [Online] Available from: http://www.theguardian.com/commentisfree/2014/may/20/why-did-lavabit-shut-down-snowden-email [Accessed: 21st August 2015].

39. GNU PRIVACY GUARD PROJECT. (1999) A free software replacement for Symantec's PGP cryptographic software suite. [Online] Available from: https://www.gnupg.org/download/ [Accessed: 12th September 2015].
40. PRETTY GOOD PRIVACY PROJECT. (1991) A data encryption and decryption computer program that provides cryptographic privacy and authentication for data communication. [Online] Available from: http://www.pgpi.org/ [Accessed: 12th September 2015].
41. MOZILLA THUNDERBIRD PROJECT. (2003) A free open source, cross-platform email, news, and chat client. [Online] Available from: http://www.mozilla.org/en-US/thunderbird/ [Accessed: 13th September 2015].
42. GPG TOOLS PROJECT. (2015) An installation package for Mac OS X (10.6 - 10.11) with software tools for email and file encryption (similar to Gpg4win for Windows). [Online] Available from: https://gpgtools.org/ [Accessed: 14th September 2015].
43. GPG 4WIN PROJECT. (2014) An email and file encryption package for most versions of Microsoft Windows, which uses GnuPG public-key cryptography for data encryption and digital signatures. [Online] Available from: http://www.gpg4win.org/download.html [Accessed: 14th September 2015].
44. GOOGLE APP PASSWORDS. (2015) A 16-digit passcode that gives an app or device permission to access your Google Account. [Online] Available from: https://support.google.com/mail/answer/185833?hl=en&rd=1 [Accessed: 16th September 2015].
45. ADIUM PROJECT. (2001) A free instant messaging application for Mac OS X that can connect to AIM, MSN, XMPP (Jabber), Yahoo, and more. [Online] Available from: https://adium.im/ [Accessed: 17th September 2015].
46. LIST JABBER PROJECT. (2011) A list of public XMPP servers, free for everyone to use. XMPP is a open, free and decentralized instant messaging network. [Online] Available from: https://list.jabber.at/ [Accessed: 19th September 2015].
47. PIDGIN PROJECT. (1998) A free and open-source multi-platform instant messaging client, based on a library named libpurple that has support for many instant messaging protocols, allowing the user to simultaneously log into various services from one application. [Online] Available from: http://www.pidgin.im/ [Accessed: 21st September 2015].
48. OFF THE RECORD MESSAGING PROJECT. (2004) A cryptographic protocol that provides encryption for instant messaging conversations. [Online] Available from: https://otr.cypherpunks.ca/ [Accessed: 22nd September 2015].
49. BBC NEWS. (2014) Andy Coulson and Clive Goodman face retrial. [Online] Available from: http://www.bbc.com/news/uk-28086528 [Accessed: 22nd August 2015].
50. BUZZFEED NEWS. (2013) David Miranda Is Nobody's Errand Boy. [Online] Available from: http://www.buzzfeed.com/natashavc/david-miranda-is-nobodys-errand-boy#.qvbm8Q4NzK [Accessed: 23rd August 2015].
51. DAILY NEWS EGYPT. (2015) David Miranda Is Nobody's Errand Boy. [Online] Available from: http://www.dailynewsegypt.com/2015/07/06/egypts-purchase-of-hacking-software-documented-in-new-leaks/ [Accessed: 26th August 2015].
52. KEEPASSX PROJECT. (2010) Started as a Linux port of KeePass, which was at that time an open source but Windows-only password manager. [Online] Available from: https://www.keepassx.org/ [Accessed: 26th September 2015].
53. SCHNEIER. (2014) Schneier on Security - Choosing Secure Passwords. [Online] Available from: https://www.schneier.com/blog/archives/2014/03/choosing_secure_1.html [Accessed: 28th September 2015].