Γρήγορη έναρξη

1. Τοποθετήστε το φλασάκι σε ένα λαπτοπ όσο αυτό είναι κλειστό.
2. Ενεργοποιήστε το.
3. Πατήστε γρήγορα το πλήκτρο που ελέγχει από ποιά συσκευή κάνει boot (εκκίνηση) ο υπολογιστής (εξαρτάται από το μοντέλο, πχ συχνά είναι τα Esc, Del, F12, και άλλα)
4. Θα πρέπει να δείτε μια οθόνη με επιλογές έναρξης Tails. Αν όχι κλειστε τον υπολογιστή από το κουμπί του και επιστρέψτε στο βήμα 2.
5. Επιλέξτε την πρώτη επιλογή
6. Θα δείτε τον διάλογο υποδοχής του Tails

Αποθηκευτικός χώρος και εξωτερικός δίσκος

Για να χρησιμοποιήσω εξωτερικό δίσκο θα πρέπει πρώτα να διαμορφώσω τον αποθηκευτικό χώρο. Αν ο αποθηκευτικός χώρος είναι ήδη διαμορφωμένος τότε στην αρχική οθόνη θα πρέπει να επιλέξω την τρίτη επιλογή αντί της πρώτης. Τότε θα μπορώ να βλέπω άλλα φλασάκια και δίσκους μέσα από το Tails.

Προσοχή όμως. Αν έχω ευαίσθητο υλικό στον αποθηκευτικό χώρο του Tails τότε θα πρέπει να το κρυπτογραφήσω πριν το αντιγράψω στο εξωτερικό δίσκο ή στο φλασάκι μου. Αν έχω ευαίσθητα αρχεία και τα αντιγράψω εκτός Tails χωρίς κρυπτογράφηση, τότε θα μπορούν να διαβαστούν από τον καθένα.

Σε αντίθεση, ο αποθηκευτικός χώρος του Tails είναι κρυπτογραφημένος. Διαμορφώστε ένα ασφαλές passphrase ακολουθώντας τις οδηγίες του EFF και μην το χρησιμοποιήσετε πουθενά αλλού.

Επίσης μπορεί να καταστραφεί ολοσχερώς μέσα από τις επιλογές του σχετικού διαλόγου εντός του Tails.

Ενημέρωση του λογισμικού

Ενημερώνουμε το λογισμικό αμέσως, οποτεδήποτε έχουμε ειδοποίηση για διαθέσιμη ενημέρωση.

Επίσης, πάντα ενημερώνουμε το λογισμικό αν έχουμε δημιουργήσει το φλασάκι Tails σε υπολογιστή που δεν εμπιστευόμαστε απόλυτα.

Σύνδεση σε δημόσια WIFI με τον “ανασφαλή περιηγητή”

Το Tails δεν είναι ένα λειτουργικό για να σερφάρουμε στο διαδίκτυο, ούτε για να συνδεόμαστε στους λογαριασμούς μας κοινωνικής δικτύωσης. Μεταβαίνουμε σε μία περιοχή που δεν πηγαίνουμε ποτέ, μετακινούμαστε με μέσα δημόσιας μεταφοράς, χρησιμοποιούμε μόνο μετρητά, και καθόμαστε σε μία καφετέρια με την πλάτη στον τοίχο και έξω από το οπτικό

πεδίο ανθρώπων ή καμερών.

Όταν χρησιμοποιούμε το Tails δεν μπαίνουμε σε κανένα απολύτως σάιτ του κανονικού διαδικτύου. Γενικά δεν συνδεόμαστε σε καμία σελίδα που μπορεί να μας ταυτοποιήσει προσωπικά. Δεν ανοίγουμε περισσότερα του ενός παράθυρα του Tor.

Χρησιμοποιούμε τον "μη ασφαλή περιηγητή" του Tails μόνο για ένα σκοπό, να υποβάλλουμε όνομα και κωδικό σε ένα δημόσιο δίκτυο (πχ βιβλιοθήκη, καφετέρια, ή hot-spot) για να συνδεθούμε.

Μαθαίνουμε κρυπτογραφία σαν βασική προϋπόθεση ασφάλειας (βλ επόμενο τμήμα για Kleopatra και Veracrypt.)

Το μοντέλο απειλής

Από ποιόν προφυλασσόμαστε; Τί μπορεί να κάνει για να αποκαλύψει τη δράση μας ή την τοποθεσία μας;

Οι απαντήσεις μας σε αυτά τα ερωτήματα αποτελούν ένα βασικό "μοντέλο απειλής". Ας σκεφτούμε μερικές τυπικές περιπτώσεις χρήσης του Tails.

- Ο μάρτυρας δημοσίου συμφέροντος, ή whistleblower, που έχει πληροφορίες για έναν οργανισμό ή μία εταιρεία για έκνομες, αντιδεοντολογικές ενέργειες. Μπορεί να χρησιμοποιήσει το Tails σαν επιπλέον επίπεδο ασφάλειας για να συνδεθεί με ένα ιστότοπο που επεξεργάζεται τέτοιες καταγγελίες, και να αρχίσει μια ανώνυμη υποβολή την οποία μπορεί να συνεχίσει, και πάλι ανώνυμα. Δεν μιλάει σε κανένα άτομο για τις σκέψεις του να προβεί σε ανώνυμη καταγγελία, και χρησιμοποιεί το Tails για να μελετήσει τον ιστότοπο επεξεργασίας της καταγγελίας, να κάνει περαιτέρω έρευνα, να μεταφέρει κρυπτογραφημένα έγγραφα που θέλει να κοινοποιήσει.
- Ο ερευνητής-δημοσιογράφος που μελετά ευαίσθητα θέματα όπως είναι το τράφικινγκ ή η διαφθορά, και θέλει να διεξάγει έρευνα χωρίς να ταυτοποιηθεί, ή χωρίς να γίνει καν αντιληπτό από εκείνους που παρατηρεί ότι βρίσκονται υπό έρευνα (παθητική αναγνώριση στο πλαίσιο της απόκτησης πληροφοριών ανοικτής πρόσβασης, passive reconnaisance, open source intelligence). Σε μερικές χώρες αυτές οι ενασχολήσεις μπορεί να θέτουν όντως τη ζωή ή την οικογένεια του ερευνητή σε άμεσο κίνδυνο, και η ανωνυμία είναι θέμα που απαιτεί προσεκτική σκέψη.
- Ακτιβιστές και δημοσιογράφοι που εκφράζουν αντιδημοφιλείς απόψεις και αυτό μπορεί να τους φέρει αντιμέτωπους με "οργισμένους όχλους", που μπορεί να είναι πάρα πολύ αποτελεσματικοί και επικίνδυνοι, τόσο για τη σωματική ακεραιότητα όσο και για την ψυχική υγεία και την ελευθερία έκφρασης. Η ανωνυμία μπορεί να επιτρέψει σε αυτά τα άτομα που μπορεί να ανήκουν σε ευάλωτες και στοχοποιημένες ομάδες να διατηρούν μπλογκ και ιστότοπους με ακτιβιστικό, θεωρητικό, και ερευνητικό περιεχόμενο, μειώνοντας τον κίνδυνο να ταυτοποιηθούν και να στοχοποιηθούν από οργισμένα πλήθη και ομάδες μίσους.
- Δημοσιογράφοι που μελετούν ευαίσθητα θέματα σε τοπική ή διεθνή κλίμακα, που μπορούν να τους καταστήσουν στόχους παρακολούθησης.

Μπορεί τα μέτρα αυτά να φαντάζουν υπερβολικά για το μέσο άνθρωπο. Αλλά το μοντέλο

απειλής είναι ένα σοβαρό θέμα που για τις παραπάνω κατηγορίες ανθρώπων, και άλλες ακόμα, μπορεί να γίνει ακόμα και θέμα ζωής και θανάτου. Ας μην ξεχνάμε ότι σε μερικές περιπτώσεις ο αντίπαλος μπορεί να έχει μέσα, πόρους, και αποφασιστικότητα στο να εντοπίσει τον ερευνητή ή τον ακτιβιστή. Ως εκ τούτου σε αυτές και σε άλλες περιπτώσεις, τα πιο προηγμένα μέτρα απαιτούνται, αφού μπορεί ο αντίπαλος να έχει τεχνικές γνώσεις και δεξιότητες γεωεντοπισμού και απο-ανωνυμοποίησης του ακτιβιστή, του ερευνητή, ή του μάρτυρα δημοσίου συμφέροντος.

Κοντά σε αυτά, το άτομο που εμπλέκεται με τέτοιες δραστηριότητες θα πρέπει να προσέξει και τέτοια μέσα απο-ανωνυμοποίησης, όπως είναι η αναγνώριση της φωνής, του ύφους γραφής, του προσώπου, ή η ανάλυση των χρονικών στιγμών δραστηριότητας (πχ ύπνου-εργασίας-μετακίνησης) που μπορεί να αξιοποιηθούν από έναν αντίπαλο με αξιόλογους πόρους και θέληση για την αναγνώριση και τον εντοπισμό του ατόμου.

Μέτρα ασφαλείας στη χρήση του δικτύου Tor

Για την ασφαλή χρήση του Tor είναι σημαντικό να καταλάβουμε ότι το Tor λειτουργεί με ένα συγκεκριμένο τρόπο. Αν καταλάβουμε αυτόν τον τρόπο και αντιληφθούμε τους περιορισμούς του, τότε μόνο θα το χρησιμοποιοήσουμε σωστά, γιατί δεν υπάρχουν μαγικές λύσεις.

Συγκεκριμένα, πρέπει να καταλάβουμε ότι ορισμένοι κόμβοι ελέγχονται από κακόβουλους δράστες και μυστικές υπηρεσίες κρατών. Αν ένας ελεγχόμενος κόμβος είναι πρώτος στην ομάδα κόμβων που δρομολογεί τα αιτήματά μας, τότε προφανώς η κυκλοφορία δικτύου μας είναι έκθετη στις μυστικές υπηρεσίες.

Γενικά ο περιηγητής Tor αλλάζει το “κύκλωμα” κόμβων σε αραιά διαστήματα. Αν κάνουμε τις πράξεις, με βάση τον πολλαπλασιαστικό κανόνα των πιθανοτήτων, προκύπτει οτι η πιθανότητα να πέσουμε στον “κακό” κόμβο είναι μεγαλύτερη όταν αλλάζουμε συνέχεια κύκλωμα. Σε κάθε περίπτωση η σύνδεσή μας μπορεί να είναι ανώνυμη, μπορεί και να μην είναι.

Για αυτό και απαιτούνται και άλλα μέτρα προφύλαξης, που εκτείνονται πέρα από το τεχνικό κομμάτι των δικτύων και περιλαμβάνουν τις τακτικές ασφάλειας γενικότερα, ειδικά αν η εργασία μας το απαιτεί.

Κρυπτογράφηση τόμων και μέσων αποθήκευσης με το Veracrypt

Το Veracrypt είναι λογισμικό κρυπτογράφησης δίσκων το οποίο έρχεται μαζί με το Tails.

https://www.veracrypt.fr/code/VeraCrypt/

Το μοντέλο απειλής εδώ είναι ότι το αποθηκευτικό μέσο μας πέφτει στα χέρια ενός αντιπάλου μας. Σε αυτήν την περίπτωση θα μπορεί να διαβάσει όλο του το περιεχόμενο και αυτό να μας αφήσει έκθετα σε οτιδήποτε επιτρέπει το περιεχόμενό του.

Ένας τρόπος που προτείνει το ίδιο το Veracrypt για τον κοινό χρήστη είναι να δημιουργεί κρυπτογραφημένους τόμους. Αυτοί κατοικούν ως απλά αρχεία στον υπολογιστή μας και

μπορούν να αποκρυπτογραφηθούν μέσα από το γραφικό περιβάλλον του Veracrypt. Τότε εμφανίζονται ως συνδεδεμένα αποθηκευτικά μέσα με τον ίδιο ακριβώς τρόπο που εμφανίζονται οι εξωτερικοί δίσκοι.

Εκεί μπορούμε να εργαστούμε κανονικά, ανοίγοντας και τροποποιώντας αρχεία, αντιγράφοντας αρχεία από και προς τον δίσκο. Όταν τελειώσουμε μπορούμε να εξαγάγουμε το μέσο, πάλι μέσα από το γραφικό περιβάλλον του Veracrypt, και τότε αυτό δεν μπορεί να διαβαστεί μέχρι να επαναλάβουμε την παραπάνω διαδικασία.

Το Veracrypt είναι ένα ολοκληρωμένο λογισμικό και παρέχει και άλλες επιλογές για προχωρημένους χρήστες. Συνιστούμε να διαβάσετε την τεκμηρίωση για να ενημερωθείτε για τις επιλογές αυτές καθώς και άλλες απειλές που ενδεχομένως υπάρχουν.

Η μονάδα μόνιμης αποθήκευσης του Tails

Όταν ανοίγουμε το Tails ο αρχικός διάλογος μας παρέχει τη δυνατότητα να “φορτώσουμε” τη μονάδα μόνιμης αποθήκευσης (permanent storage). Αυτή λειτουργεί με τον τρόπο που εκτέθηκε πιό πάνω. Ας σημειώσουμε ότι για να “κλωνοποιήσουμε” το Tails σε άλλο φλασάκι, καθώς και για να εγκαταστήσουμε επιπρόσθετες εφαρμογές, θα πρέπει να είναι ενεργή η μονάδα αποθήκευσης. Αν ξεχάσαμε να το κάνουμε, απλά επανεκκινούμε το Tails και διαλέγουμε την ενεργοποίηση της αποθηκευτικής μονάδας. Για να δημιουργήσουμε για πρώτη φορά αποθηκευτική μονάδα πρέπει να πάμε μέσα από το μενού του Tails όπου θα βρούμε τη σχετική επιλογή στις “Δημοφιλείς Εφαρμογές”.

> Για την επιλογή του passphrase συνίσταται να ακολουθήσουμε τις οδηγίες του eff για τις λίστες τυχαίων λέξεων https://www.eff.org/dice . Εδώ μπορεί ακόμα να βρείτε έναν προσομοιωτή ζαριών, αν και το καλύτερο σενάριο είναι να χρησιμοποιήσετε πραγματικά ζάρια για απαλοιφή της ψευδοτυχαιότητας. https://dice-simulator.com/ Οι λίστες λέξεων του eff μπορούν να δώσουν κάποιες λέξεις για να συνθέσουμε τη φράση κλειδί.

Δεν πρέπει να επαναπαυόμαστε σε μυστήρια χόμπι ή στίχους από άγνωστα γκρουπ για να συνθέτουμε μόνες μας τις φράσεις κλειδιά. Οι επαγγελματίες του χώρου έχουν αρκετά gigabyte με στίχους τραγουδιών και την εγκυκλοπαίδεια των Κλίγκον σε μορφή απλού κειμένου, και θα χρησιμοποιήσουν εξατομικευμένες λίστες λέξεων για να βρουν ένα συνδυασμό τριών ή τεσσάρων ή πέντε λέξεων Κλίγκον που ξεκλειδώνουν το φλασάκι σας. Μπορεί η όλη έρευνα και η ολοκλήρωση της “επίθεσης με λεξικό” να τους πάρει μία εβδομάδα.

Οι λίστες λέξεων του eff είναι καταρτισμένες για μεγιστοποίηση της εντροπίας, που είναι ο φυσικός εχθρός αυτού του τύπου επίθεσης.

Το μόνο που απομένει είναι να “σκαρώσετε μία ιστοριούλα” που να συνδέει τον παράδοξο συνδυασμό λέξεων, που να μπορεί να το θυμάστε. Αν δεν έχετε καλό μνημονικό μπορεί αν πρέπει να το καταγράψετε χρησιμοποιήστε χρηματοκιβώτιο, ή συρτάρι με κλειδαριά. Αν καταφύγετε στην επιλογή του χρηματοκιβωτίου, να ξέρετε πως και αυτή συνεπάγεται δικά της θέματα ασφαλείας και δικά της μοντέλα απειλής!

Ας σημειωθεί, τέλος, ότι **όταν κλωνοποιούμε ένα φλασάκι Tails με το εργαλείο Tails Cloner μας δίνεται η επιλογή να το κλωνοποιήσουμε με ή χωρίς τη μονάδα αποθήκευσης.**

Μπορούμε έτσι αν θέλουμε να δώσουμε μόνο το λειτουργικό σε ένα άλλο άτομο, χωρίς τα προσωπικά μας αρχεία, να το κάνουμε. Αν θέλουμε να μεταφέρουμε αρχεία σε άλλο αποθηκευτικό μέσο, κάνουμε την επιλογή “with external drive” στον αρχικό διάλογο. **Μπορούμε τότε να μεταφέρουμε αρχεία από τη μονάδα μόνιμης αποθήκευσης του Tails στο εξωτερικό αποθηκευτικό μέσο που συνδέουμε, συνήθως σε άλλη θύρα USB του ίδιου υπολογιστή.**

Προσοχή όμως, αν μεταφέρουμε τα αρχεία μας αποκρυπτογραφημένα, τα αρχεία αυτά θα είναι αναγνώσιμα από όποιο άτομο έχει πρόσβαση στο νέο αποθηκευτικό μέσο. Ως εκ τούτου είναι καλή πρακτική να κρυπτογραφούμε τα ευαίσθητα αρχεία όταν πρόκειται να φύγουν από το χώρο μόνιμης αποθήκευσης του Tails.

Πριν συνδεθείτε

Το εγχειρίδιο αυτοάμυνας του Electronic Frontier Foundation https://ssd.eff.org/
Ο περιηγητής Tor είναι ένα πρόγραμμα περιήγησης στο διαδίκτυο όπως είναι ο Firefox, που όμως δρομολογεί τα αιτήματά μας μέσα από το ομώνυμο δίκτυο Tor.

Ας έχουμε υπόψη ότι ο Tor δεν έρχεται με προεπιλεγμένες τις βέλτιστες ρυθμίσεις. Επιλέγουμε το εικονίδιο της ασπίδας πάνω δεξιά και στο διάλογο ρυθμίσεων όπου μας κατευθύνει επιλέγουμε το Safest. Αυτό πρέπει να γίνεται κάθε φορά γιατί το Tails ξεχνάει κάθε φορά που αποσυνδέουμε το φλασάκι!

- Μερικοί ιστότοποι μπορεί να μην λειτουργούν. Αυτό είναι απλά παρενέργεια της ασφάλειας και της ιδιωτικότητας που παρέχει ο περιηγητής. Αποφύγετέ τους.

- Ακόμα, δεν εγκαθιστούμε άλλα πρόσθετα στον Tor πέρα από αυτά που έρχονται προεγκατεστημένα.

- Οι γέφυρες Tor (Tor bridges) θεωρούνται επισφαλείς. Χρησιμεύουν σε περιπτώσεις χωρών που απαγορεύουν τη χρήση Tor.

Σε αυτό το σημείο να θυμίσουμε ότι ο πάροχος δικτύου σας μπορεί να δεί ότι χρησιμοποιείτε Tor. Σε μερικές χώρες αυτό προσελκύει την προσοχή των διωκτικών αρχών.

Λέγεται ότι πολλές γέφυρες είναι προσβεβλημένες και ορισμένες είναι ορατές στις αρχές, που και έτσι ακόμα μπορούν να αντιληφθούν τη χρήση του Tor. Για αυτό σε περιπτώσεις κρατικών εμποδίων στην πρόσβαση στο δίκτυο Tor προτείνεται η χρήση του Snowflake ενός προσθέτου του Firefox που δίνει δίοδο σε χώρες όπως αυτές για να συνδεθούν στο δίκτυο Tor.

Οδηγούμαστε στη διεύθυνση https://whatsmybrowser.org/ και επιβεβαιώνουμε ότι το

Javascript είναι απενεργοποιημένο, και ότι δεν διαρρέουν άλλες πληροφορίες για την τοποθεσία μας ή τα χαρακτηριστικά του περιηγητή μας.

Μερικές ακόμα προφυλάξεις:

- **Μην ανοίγετε πολλαπλά παράθυρα Tor, ακόμα και με το ίδιο σάιτ.**
- **Μην μεγιστοποιείτε το παράθυρο του Tor, άλλωστε στο Tails δεν υπάρχει τέτοια επιλογή.**
- **Μην συνδέεστε σε λογαριασμούς σας των μέσων κοινωνικής δικτύωσης.**
- **Μη χρησιμοποιείτε ίδια usernames και emails για εγγραφή σε διαφορετικές υπηρεσίες, γιατί αυξάνουν την επιφάνεια επίθεσης εναντίον της ανωνυμίας σας.**
- **Χρησιμοποιείστε ψευδώνυμα και λογαριασμούς ηλεκτρονικού ταχυδρομείου που δεν μπορούν να συνδεθούν με εσάς ή την εργασία σας.**
- **Μην χρησιμοποιείτε το Tails μέσα σε εικονικές μηχανές σε υπολογιστές που δεν εμπιστεύεστε.**
- **ΔΕΝ ΧΡΗΣΙΜΟΠΟΙΟΥΜΕ ΠΟΤΕ ΤΟ ΦΛΑΣΑΚΙ TAILS ΓΙΑ ΑΠΟΘΗΚΕΥΣΗ ΑΣΧΕΤΩΝ ΑΡΧΕΙΩΝ Ή ΓΙΑ ΟΠΟΙΑΔΗΠΟΤΕ ΑΛΛΗ ΧΡΗΣΗ**
- **Δεν δουλεύουμε ποτέ χωρίς να έχουμε ένα συγκεκριμένο μοντέλο απειλής.**

Παρόλο που το Tails μέσα από το live USB δεν αφήνει ίχνη στο μηχάνημα που το φιλοξενεί, καλό είναι αν υπάρχουν σοβαροί κίνδυνοι στο μοντέλο απειλής να χρησιμοποιείτε μηχάνημα καθαρό το οποίο δεν έχει εκτεθεί ποτέ στα προσωπικά σας στοιχεία.

> Ορισμένοι οργανισμοί όπως ο Guardian, το Tech Crunch και άλλα, προτείνουν στους whistleblowers να ταξιδέψουν σε μία τυχαία περιοχή, με μέσα μαζικής μεταφοράς, να χρησιμοποιήσουν ένα ανώνυμο δίκτυο, να προσέξουν για το ενδεχόμενο φυσικής υποκλοπής των μηνυμάτων τους (βλ κοίταγμα πάνω από τον ώμο), και να προμηθευτούν έναν υπολογιστή αποκλειστικά για τον σκοπό χρήσης του whistleblowing. Όλες οι πληρωμές πρέπει να γίνονται με μετρητά.

Η χρήση του Tails καθιστά πιο εύχρηστη την πρόσβαση στο δίκτυο Tor, και πολλές από αυτές τις προφυλάξεις μπορεί να φαντάζουν υπερβολικές. Καλό είναι όμως, πάντα λαμβάνοντας υπόψη το μοντέλο απειλής, να φροντίζουμε για την πλήρη σχάση ανάμεσα στην ακτιβιστική δράση και την επαγγελματική και προσωπική ταυτότητα.

Σημεία εισόδου στον κρυμμένο ιστό

Όλοι γνωρίζουμε τα γνωστά μας link ως ένα σήμα κατατεθέν της εποχής του διαδικτύου.

Το ισοδύναμό του στον κόσμο του Tor είναι οι διευθύνσεις onion.

Ως επί το πλείστον είναι δυσανάγνωστες αλφαριθμητικές ακολουθίες, αν και ορισμένες μεγάλες εταιρείες έχουν εξασφαλίσει διευθύνσεις onion που τουλάχιστον θυμίζουν αμυδρά την εμπορική τους ονομασία.

Οι ιστότοποι στον κρυμμένο ιστό λέγονται “κρυμμένες υπηρεσίες” (hidden services).
Ποτέ δεν ακολουθούμε μία διεύθυνση onion κάνοντας κλικ σε σύνδεσμο.

Πάντα επαληθεύουμε την προέλευση μίας διεύθυνση onion, και την επικολλούμε στην γραμμή διευθύνσεων του Tor.

> Μερικές ευυπόληπτες διευθύνσεις onion https://github.com/alecmuffett/real-world-onion-sites

Αξίζει να αναφερθεί η κοινότητα RiseUp η οποία παρέχει μία σειρά από ψηφιακά εργαλεία ακτιβισμού.

Για παράδειγμα, το Etherpad που φιλοξενεί η οργάνωση αποτελεί ενδιαφέρουσα επιλογή για συνεργατική επεξεργασία εγγράφων σε πλαίσιο ακτιβισμού.

Εισαγωγή στη κρυπτογράφηση

Ας σταθούμε στην υπηρεσία της RiseUp για λίγο, αφού μας παρέχει ένα εξαιρετικό παράδειγμα για το ρόλο που έχει η υπογραφή ενός μηνύματος στο σύστημα κρυπτογραφίας δημοσίου κλειδιού.

Υπάρχει μία βασική παραδοχή που κάνουμε στην κρυπτογραφία δημόσιου κλειδιού, ότι υπάρχει ένα ιδιωτικό κλειδί στο οποίο εμείς και μόνο έχουμε πρόσβαση και το οποίο προστατεύουμε ως κόρην οφθαλμού.

Αν το ιδιωτικό κλειδί διαρρεύσει τότε όλη η συζήτηση που ακολουθεί είναι απλά κενή νοήματος.

Η κρυπτογραφία δημόσιου κλειδιού είναι μία μορφή ασύμμετρης κρυπτογράφησης. Αυτό ίσως γίνει περισσότερο κατανοητό σε αντιπαραβολή με την συμμετρική κρυπτογράφηση. Στην τελευταία, τόσο ο αποστολέας του μηνύματος όσο και ο αποδέκτης έχουν το ίδιο κλειδί αποκρυπτογράφησης με το οποίο διαβάζουν τα μηνύματα η μία της άλλης. Αυτό θέτει το πρόβλημα του πως ενημερώνονται και τα δύο μέρη όταν το κλειδί αλλάζει.

Αυτό το πρόβλημα λύνει η κρυπτογραφία δημόσιου κλειδιού. Όταν έχω δημοσιοποιήσει το δημόσιο κλειδί μου, μπορεί κατ᾽ αρχάς όποιο άτομο θέλει να μου στείλει ένα κρυπτογραφημένο μήνυμα, το οποίο ωστόσο μόνο εγώ μπορώ να διαβάσω, ξεκλειδώνοντάς το με το δικό μου ιδιωτικό κλειδί.

Δεύτερον, μπορώ να υπογράψω ένα μήνυμα έτσι ώστε (με την παραδοχή ότι κανένας άλλος δεν έχει πρόσβαση στο ιδιωτικό κλειδί μου), ο αποδέκτης να μπορεί να χρησιμοποιήσει το δημόσιο κλειδί μου ώστε να επαληθεύσει ότι εγώ συνέταξα το μήνυμα.

Με αυτόν τον τρόπο οργανώσεις όπως η RiseUp δημοσιεύουν σε τακτά χρονικά διαστήματα μηνύματα υπογεγραμμένα από τους ίδιους, με την προειδοποίηση ότι αν σε ένα διάστημα χρόνου δεν δημοσιευτεί επαληθεύσιμο μήνυμα με το πιο πρόσφατο έγκυρο κλειδί τους, αυτό θα σημαίνει πως οι εξυπηρετητές τους θα έχουν καταληφθεί από τις αρχές.

Έτσι, χρησιμοποιούν την κρυπτογραφία δημόσιου κλειδιού και τη δυνατότητα που αυτή παρέχει για επαληθεύσιμη υπογραφή των μηνυμάτων ως ένα άλλο “καναρίνι των ανθρακωρυχείων”, τα οποία λιποθυμώντας έδιναν το σήμα στους εργάτες και εργάτριες ότι τα

επίπεδια διοξειδίου του άνθρακα ήταν επικίνδυνα για να εκκενώσουν το χώρο.

Πρακτικές οδηγίες κρυπτογράφησης

Το εγχειρίδιο χρήσης του ίδιού του GnuPG (GNU Privacy Guard) δίνει μία απλή και εφαρμόσιμη λίστα οδηγιών για τις βασικές λειτουργίες του προγράμματος καθώς και κάποιες σκέψεις σχετικά με τις κατάλληλες επιλογές για μία σειρά περιπτώσεων.

https://www.gnupg.org/gph/en/manual.html

Ας επισκοπήσουμε τις βασικές λειτουργίες του GnuPG

- **Δημιουργία ενός ζεύγους κλειδιών (δημόσιο - ιδιωτικό)**
- **Δημιουργία ενός πιστοποιητικού αποκήρυξης κλειδιού (για τις περιπτώσεις που χάσουμε τον έλεγχο του ιδιωτικού μας κλειδιού)**
- **Εξάγωγή ενός δημοσίου κλειδιού για διαμοιρασμό**
- **Εισαγωγή ενός ιδιωτικού κλειδιού στην κλειδοθήκη μας**
- **Κρυπτογράφηση και αποκρυπτογράφηση εγγράφων**
- **Δημιουργία και επαλήθευση υπογραφών**
- **Καθαρή υπογραφή εγγράφων**
- **Αποσπασμένες υπογραφές**

Ας σημειωθεί πως υπάρχει και το γραφικό περιβάλλον Kleopatra που διευκολύνει πολύ το χρήστη σε όλες τις παραπάνω λειτουργίες, αρκεί φυσικά να έχουν γίνει καλά κατανοητές οι έννοιες και η παραπάνω περιπτωσιολογία.

Και αυτές ακόμα οι πηγές μπορούν να εξηγήσουν καλύτερα τον τρόπο λειτουργίας του GnuPG

https://privacy.ellak.gr/wp-content/uploads/sites/9/2017/06/gnupg-leaflet.el2_.pdf

https://privacy.ellak.gr/2019/08/26/mia-mikri-isagogi-sto-gnupg-2/

Το λογισμικό Kleopatra παρέχει τις λειτουργίες αυτές σε γραφικό περιβάλλον χρήσης, χρησιμοποιώντας το πολύ συγγενικό λογισμικό PGP (Pretty Good Privacy).

https://www.openpgp.org/software/kleopatra/

Μπορείτε να ασκηθείτε στα λογισμικά Veracrypt και Kleopatra σε οποιοδήποτε λειτουργικό σύστημα και μάλιστα στα Ελληνικά. Όταν έχετε κατακτήσει τις απαραίτητες δεξιότητες μπορείτε με μεγαλύτερη αυτοπεποίθηση να χρησιμοποιήσετε την κρυπτογραφία δημοσίου κλειδιού σε πραγματικές συνθήκες.