ΟΔΗΓΟΣ ΓΙΑ PEER-TO-PEER, ΚΡΥΠΤΟΓΡΑΦΗΣΗ ΚΑΙ TOR

διανέμεται με ελεύθερη συνεισφορά

faura books

για τη φαούρα των
ανατρεπτικών ιδεών

Οδηγός για Peer-to-Peer, Κρυπτογράφηση, και TOR: νέες υποδομές επικοινωνίας για αναρχικά

[The Guide to Peer-to-Peer, Encryption, and Tor: New Communication Infrastructure for Anarchists] by anonymous contributor

πρώτη δημοσίευση: itsgoingdown.org οκτώβρης 2022

πρώτη έκδοση: χειμώνας 2023, 250 αντίτυπα
δεύτερη έκδοση: άνοιξη 2024, 250 αντίτυπα

ευχαριστούμε την αναρχική δομή εκτυπώσεων pyco nero (αθήνα) για την εκτύπωση της 2ης έκδοσης

μετάφραση: faura books

Σημείωμα μετάφρασης

Έχει περάσει πάνω από ένας χρόνος από την πρώτη δημοσίευση αυτού του οδηγού και ενώ τα τεχνολογικά δεδομένα αλλάζουν, το περιεχόμενο του ελάχιστα έχει επηρεαστεί. Αυτός είναι και ο λόγος που θεωρήθηκε σημαντικό να μεταφραστεί, καθώς δεν πρόκειται για εγχειρίδιο εγκατάστασης ασφαλών εφαρμογών, αλλά για μια προσέγγιση στο πως πρέπει να βλέπουμε και να κριτικάρουμε τις υπάρχουσες αλλά και τις νέες τεχνολογίες.
Από τη στιγμή που βασιζόμαστε σε διάφορες υποδομές για να επικοινωνούμε θα πρέπει να προσπαθούμε να κατανοούμε πως λειτουργούν, πώς μας προστατεύουν ή μας καθιστούν ευάλωτα και να ψάχνουμε συνεχώς τρόπους ενίσχυσης τους. Στο κείμενο γίνεται μια βαθιά κριτική ανάλυση του Signal και προτείνονται δυο νέα εργαλεία, το Briar & το Cwtch. Η κριτική στο Signal δεν έχει σαν στόχο να σπείρει τον πανικό αλλά να δείξει πως δεν υπάρχουν κάλες ή κακές εφαρμογές παρά μόνο εργαλεία που κάνουν κάτι αλλά δεν κάνουν κάτι άλλο. Το ίδιο ισχύει και με τα Briar & Cwtch που ενώ ενισχύουν κατά πολύ την ασφάλεια των επικοινωνιών μας, έρχονται με ένα «κόστος» στην χρηστικότητα τους. Φυσικά δεν πρέπει να ξεχνάμε ότι ο πιο ασφαλής τρόπος για να επικοινωνούμε είναι οι συναντήσεις πρόσωπο με πρόσωπο, μακριά από κάμερες και κινητά.

Οι επικοινωνίες μας όμως εξαρτώνται σε μεγάλο βαθμό από τις διάφορες εφαρμογές σήμερα. Από τις ομαδικές στο Signal που κάποιες φορές αντικαθιστούν τις συνελεύσεις, το #antireport και τα events στο Facebook. Αυτή η συνθήκη δημιουργεί κάποια ερωτήματα που είναι σημαντικό να τίθενται. Πέραν του κατά ποσό μπορούμε να εμπιστευόμαστε καπιταλιστικούς κολοσσούς που συνεργάζονται ανοιχτά με τα κράτη, πως θα αντιμετωπίσουμε ένα πιθανό κλείσιμο του Twitter, του Signal και γενικά μια διακοπή του ίντερνετ εν μέσω μιας μαζικής εξέγερσης;

Αυτά τα ερωτήματα πρέπει να συζητηθούν και όσο το δυνατόν να δοθούν απαντήσεις και λύσεις το συντομότερο πριν από κάποιο blackout. Αυτός είναι και ο σκοπός αυτής της μετάφρασης.

faura books
νοέμβρης ‘23

Μια εκτενής επισκόπηση από αναρχική σκοπιά, και ένας οδηγός για διάφορες εφαρμογές και τεχνολογίες που χρησιμοποιούν peer-to-peer και κρυπτογράφηση

Οι εφαρμογές συνομιλίας με ασφαλή κρυπτογράφηση αποτελούν ένα σημαντικό εργαλείο για τους αναρχικούς και πρέπει να ελέγχονται εξονυχιστικά. Το Signal είναι το κύριο εργαλείο ασφαλούς κρυπτογράφησης που χρησιμοποιούν οι αναρχικές σήμερα. Προσπερνώντας τις θεωρίες συνωμοσίας, η βάση και οι στόχοι ανάπτυξης του Signal έχουν ενδεχομένως επιπτώσεις στην ασφάλεια των αναρχικών που το χρησιμοποιούν. Το Signal είναι μια κεντρικοποιημένη υπηρεσία επικοινωνίας, και η κεντρικοποίηση έχει ως αποτέλεσμα πιθανές επιπτώσεις στην ασφάλεια, ειδικά όταν εντάσσεται στο πλαίσιο σημερινών απειλών. Εναλλακτικές ασφαλείς εφαρμογές συνομιλίας όπως το Briar και το Cwtch είναι εργαλεία **P**eer-to-peer επικοινωνίας που, εκτός από κρυπτογραφημένα (**E**ncrypted) όπως το Signal, δρομολογούν όλη την κυκλοφορία μέσω του **T**or (**PET**). Αυτή η προσέγγιση ασφαλούς επικοινωνίας προσφέρει μεγάλα πλεονεκτήματα για την ασφάλεια, την ανωνυμία και την ιδιωτικότητα σε σχέση με πιο κοινές υπηρεσίες όπως το Signal, αλλά με κάποια μειονεκτήματα. Ωστόσο, οι αναρχικοί θα πρέπει να εξετάσουμε σοβαρά το ενδεχόμενο να δοκιμάσουμε και να χρησιμοποιήσουμε το Briar ή/και το Cwtch, για την ανάπτυξη πιο ανθεκτικών και ασφαλέστερων υποδομών επικοινωνίας.

Παρ' όλα αυτά, ο καλύτερος τρόπος για να επικοινωνήσετε οτιδήποτε με ασφάλεια εξακολουθεί να είναι πρόσωπο με πρόσωπο.

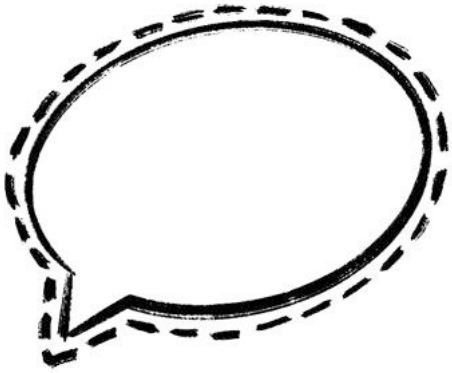
Σσσσ...

Έχετε στα χέρια σας μια ανάλυση σχετικά με ψηφιακά εργαλεία για ασφαλή και ιδιωτική επικοινωνία. Αρχικά, πρέπει να τονιστεί ότι μια συνάντηση πρόσωπο με πρόσωπο, μακριά από κάμερες και από τα αυτιά άλλων ανθρώπων και συσκευών, είναι ο πιο ασφαλής τρόπος επικοινωνίας. Οι αναρχικοί κάναμε βόλτες για να συνομιλήσουμε πολύ πριν την ύπαρξη κρυπτογραφημένων γραπτών μηνυμάτων και θα πρέπει να το κάνουμε και τώρα, όποτε είναι δυνατόν.

Με βάση αυτό, είναι αδιαμφισβήτητο ότι τα ασφαλή ψηφιακά εργαλεία επικοινωνίας αποτελούν πλέον μέρος των αναρχικών μας υποδομών. Ίσως πολλές από εμάς βασίζονται σε αυτά περισσότερο από όσο θα έπρεπε, αλλά έχουν γίνει σε ένα βαθμό αναπόφευκτα για τον συντονισμό, τη συνεργασία και την επικοινωνία. Δεδομένου ότι αυτά τα εργαλεία αποτελούν σημαντική υποδομή για εμάς, είναι ζωτικής σημασίας να εξετάζουμε και να επαναξιολογούμε συνεχώς την ασφάλεια και την αποτελεσματικότητά τους στην προστασία των επικοινωνιών μας από τους αντιπάλους μας.

Τις τελευταίες δύο δεκαετίες, οι αναρχικοί έχουμε υιοθετήσει από νωρίς ασφαλή εργαλεία και τεχνικές επικοινωνίας, και έχουν παίξει ρόλο στην κανονικοποίηση και διάδοση της χρήσης τους στις δικές μας κοινότητες, καθώς και σε άλλες κοινότητες που αντιστέκονται και αγωνίζονται. Το κείμενο που ακολουθεί έχει σκοπό να παρουσιάσει σε κόσμο της αναρχίας νεότερα εργαλεία ασφαλούς κρυπτογραφημένης επικοινωνίας και να υποστηρίξει ότι πρέπει να τα υιοθετήσουμε προκειμένου να ενισχύσουμε την ανθεκτικότητα και την αυτονομία της υποδομής μας. Μπορούμε να μάθουμε τα πλεονεκτήματα αυτών των νέων εφαρμογών - πώς μπορούν να μας βοηθήσουν να αποφύγουμε την παρακολούθηση και την

καταστολή - και στη συνέχεια να τα χρησιμοποιήσουμε αποτελεσματικά στα κινήματά μας και να βοηθήσουμε στην ευρύτερη διάδοση της χρήσης τους.



Είναι πιο εύκολο να πλαισιωθεί μια συζήτηση σχετικά με τις νέες ασφαλείς εφαρμογές συνομιλίας παρουσιάζοντάς τες σε αντιδιαστολή με την ασφαλή εφαρμογή συνομιλίας που όλοι γνωρίζουν: το Signal. Το Signal είναι η de facto επιλογή ασφαλούς επικοινωνίας για πολλούς, τουλάχιστον στη Βόρεια Αμερική, και γίνεται ταχύτατα πανταχού παρόν και εκτός των αναρχικών κύκλων. Αν διαβάζετε αυτό το κείμενο, πιθανότατα χρησιμοποιείτε το Signal, και υπάρχει μεγάλη πιθανότητα η μαμά σας ή ο συνάδελφός σας να χρησιμοποιεί επίσης το Signal. Η χρήση του Signal αυξήθηκε μαζικά τον Ιανουάριο του 2021 (τόσο πολύ που η υπηρεσία τέθηκε εκτός λειτουργίας για 24 ώρες), φτάνοντας τα 40 εκατομμύρια καθημερινούς χρήστες. Το Signal επιτρέπει στους χρήστες να ανταλλάσσουν πολύ εύκολα κρυπτογραφημένα μηνύματα. Προέκυψε από ένα προηγούμενο έργο που ονομαζόταν TextSecure, το οποίο προσέθετε κρυπτογράφηση στα μηνύματα SMS (παλιομοδίτικα μηνύματα κειμένου για τους ζούμερς που μας διαβάζουν). Το TextSecure, και αργότερα το Signal, τα εμπιστεύτηκαν και τα δύο δικαίως αναρχικές από νωρίς, σε μεγάλο βαθμό λόγω του δικτύου εμπιστοσύνης στην πραγματική ζωή μεταξύ του βασικού προγραμματιστή, Moxie Marlinspike, και άλλων αναρχικών.

Στις αρχές του 2022 ο Moxie έφυγε από το Signal, και αυτό πυροδότησε ένα νέο κύμα συνωμοσιολογικής κινδυνολογίας. Ο αναρχικός διευθύνων σύμβουλος του Signal παραιτήθηκε. Το Signal ξόφλησε. Ένα άρθρο με τίτλο “Signal Warning” που δημοσιεύτηκε στο It’s Going Down[1] προσπάθησε να διαλύσει αυτές τις ανησυχίες και τις θεωρίες συνωμοσίας, και ανέλυσε το αν οι αναρχικοί μπορούν ακόμα να «εμπιστεύονται» το Signal (μπορούν, με επιφυλάξεις όπως πάντα), και επανέλαβε γιατί το Signal είναι, στην πραγματικότητα, αρκετά ασφαλές και αξιόπιστο (ελέγχεται και εξετάζεται σε μεγάλο βαθμό από ειδικούς ασφαλείας).

Ωστόσο, το “Signal Warning” υπέδειξε ότι η αποχώρηση του Moxie σηματοδότησε, τουλάχιστον, μια υπενθύμιση της αναγκαιότητας συνεχούς ελέγχου και σκεπτικισμού απέναντι στο Signal και οποιουδήποτε εργαλείου ή λογισμικού τρίτων που χρησιμοποιούμε εμείς οι αναρχικοί.

«Τώρα, που έπεσαν οι μάσκες, η ανάλυση του Signal και η αξιολόγηση της χρήσης του στα

δικά μας πλαίσια, μπορεί να αρχίσει να λαμβάνει χώρα έξω από τις όποιες στρεβλώσεις δημιουργεί κάποτε η εμπιστοσύνη. Τώρα πρέπει να εξετάσουμε την εφαρμογή και το πρωτόκολλο της ως έχουν, ως κώδικα που εκτελείται μέσα σε έναν υπολογιστή, με όλα τα οφέλη και τους περιορισμούς που αυτό συνεπάγεται. Αυτό απέχει πολύ από το τέλος [στμ: του Signal], και δεν κινείται καν, για την ώρα, προς αυτή την κατεύθυνση. Αλλά, όπως όλα τα τεχνικά συστήματα, πρέπει να τα προσεγγίζουμε με πληροφορίες και καχυποψία».

Το Signal εξακολουθεί να τυγχάνει ευρείας εμπιστοσύνης και δεν υπάρχει ακόμη τίποτα που να πλησιάζει σε αποδεικτικά στοιχεία που υποδεικνύουν ελλείψεις ασφάλειας. Αυτό που ακολουθεί δεν αποτελεί έκκληση για εγκατάλειψη του Signal - το Signal παραμένει ένα εξαιρετικό εργαλείο. Όμως, δεδομένου του υπέρμετρου ρόλου του στις αναρχικές υποδομές επικοινωνίας και του ανανεωμένου ενδιαφέροντος για το αν μπορούμε ή πρέπει να εμπιστευτούμε το Signal, μπορούμε να εκμεταλλευτούμε αυτή την ευκαιρία για να εξετάσουμε προσεκτικά την εφαρμογή, τον τρόπο λειτουργίας της, τον τρόπο που τη χρησιμοποιούμε και να διερευνήσουμε εναλλακτικές λύσεις.

Ένας εξονυχιστικός έλεγχος του Signal δεν αποκαλύπτει μυστικές κερκόπορτες ή κενά τρωτά σημεία. Αποκαλύπτει όμως την προτεραιότητα που δίνεται στην εμπειρία και ευκολία του χρήστη και την βελτιωμένη ανάπτυξη ενός προϊόντος σε βάρος των στόχων ασφαλείας. Οι ευρύτεροι στόχοι του έργου και τα χαρακτηριστικά του Signal τώρα μπορεί να μην ταιριάζουν ακριβώς με το μοντέλο απειλών που αντιμετωπίζουμε. Και εξαιτίας του τρόπου λειτουργίας του Signal σε δομικό επίπεδο, οι αναρχικοί εξαρτόμαστε από μια κεντρικοποιημενη υπηρεσία για το μεγαλύτερο μέρος των ασφαλών διαδικτυακών επικοινωνιών μας. Αυτό έχει συνέπειες για την ασφάλεια, την ιδιωτικότητα και την αξιοπιστία.

Υπάρχουν όμως εναλλακτικές λύσεις που έχουν αναπτυχθεί σε μεγάλο βαθμό για να αντιμετωπίσουν συγκεκριμένα αυτά τα ζητήματα. Το Briar και το Cwtch είναι δύο νεότερες εφαρμογές ασφαλούς συνομιλίας που, όπως και το Signal, επιτρέπουν επίσης την ανταλλαγή κρυπτογραφημένων μηνυμάτων. Επιφανειακά, φαίνεται να λειτουργούν όπως το Signal, αλλά ο τρόπος με τον οποίο λειτουργούν στην πραγματικότητα είναι αρκετά διαφορετικός. Ενώ το Signal είναι μια υπηρεσία κρυπτογραφημένων μηνυμάτων, αντίθετα το Briar και το Cwtch είναι εφαρμογές PET - είναι αυτοτελείς εφαρμογές που επιτρέπουν την ανταλλαγή μηνυμάτων Peer-to-peer και κρυπτογραφημένων μηνυμάτων μέσω Tor.

Αυτές οι εφαρμογές PET και ο τρόπος λειτουργίας τους θα παρουσιαστούν λεπτομερώς. Αλλά ο καλύτερος τρόπος για να εξηγήσουμε πραγματικά τα πλεονεκτήματά τους (και γιατί οι αναρχικοί θα πρέπει να ενδιαφέρονται για άλλες ασφαλείς εφαρμογές συνομιλίας όταν έχουμε ήδη το Signal) είναι να κάνουμε μια βαθιά κριτική ανάλυση του Signal.

Μοντέλο απειλών και Προειδοποιήσεις

Πριν ξεκινήσουμε, είναι σημαντικό να διαμορφώσουμε το πλαίσιο αυτής της συζήτησης, ορίζοντας το σχετικό μοντέλο απειλών και παρέχοντας κάποιες προειδοποιήσεις.

Για τους σκοπούς της παρούσας συζήτησης, οι αντίπαλοι μας είναι οι εθνο-κρατικές ή τοπικές αρχές επιβολής του νόμου με κάποια πρόσβαση σε πόρους των εθνο-κρατικών αρχών. Παρά την κρυπτογράφηση από άκρο σε άκρο (end-to-end) που αποκρύπτει το περιεχόμενο των μηνυμάτων κατά τη μεταφορά, αυτοί οι αντίπαλοι έχουν πολλές δυνατότητες που θα

μπορούσαν να χρησιμοποιηθούν για να αποκαλύψουν ή να διαταράξουν τις δραστηριότητες, τις επικοινωνίες ή τα δίκτυά μας, ώστε να μπορούν να μας καταστείλουν. Ειδικότερα, θα εξεταστούν οι ακόλουθες δυνατότητες των αντιπάλων μας:

• Έχουν γενική πρόσβαση σε ιστότοπους κοινωνικής δικτύωσης και άλλες δημόσιες πληροφορίες.
• Σε ορισμένες περιπτώσεις, μπορούν να παρακολουθούν όλη την κίνηση του διαδικτύου ενός σπιτιού ή κινητού τηλέφωνου, για κάποιο συγκεκριμένο άτομο.
• Μπορούν να έχουν πρόσβαση σε «ανώνυμα» δεδομένα χρήστη ή μεταδεδομένα από εφαρμογές, παρόχους κινητής τηλεφωνίας, παρόχους υπηρεσιών διαδικτίου (ISP) κλπ
• Μπορούν να έχουν πρόσβαση σε καταγεγραμμένη κίνηση δικτύου που συλλέγεται μαζικά από πολλά σημεία συμφόρησης στην υποδομή του διαδικτύου.
• Με διαφορετικό βαθμό επιτυχίας κάθε φορά, μπορούν να συνδυάσουν, να αναλύσουν και να συσχετίσουν αυτά τα δεδομένα και την κίνηση δικτύου, προκειμένου να αποανωνυμοποιήσουν τους χρήστες, να χαρτογραφήσουν τα κοινωνικά τους δίκτυα ή να αποκαλύψουν άλλες δυνητικά ευαίσθητες πληροφορίες σχετικά με άτομα ή ομάδες και τις επικοινωνίες τους.
• Μπορούν να θέσουν σε κίνδυνο υποδομές του διαδικτύου (διαδικτυακοί και άλλοι πάροχοι υπηρεσιών, εταιρείες, προγραμματιστές εφαρμογών) είτε μέσω εξαναγκασμού είτε μέσω hacking.[2]
• Μπορούν να διαταράξουν την κυκλοφορία του διαδικτύου γενικά ή στοχευμένα, είτε επειδή ελέγχουν την υποδομή του διαδικτύου, είτε με κυβερνοεπιθέσεις κατά της υποδομής του διαδικτύου.

Ο παρών οδηγός ασχολείται με τον μετριασμό των παραπάνω δυνατοτήτων αυτών των αντιπάλων, αλλά υπάρχουν και πολλές άλλες που δεν μπορούν να εξεταστούν εδώ:
• Σε ακραίες περιπτώσεις, μπορούν να μολύνουν εξ αποστάσεως συσκευές στοχευμένων ατόμων με keylogger και κακόβουλο λογισμικό παρακολούθησης.
• Μπορούν να αποκτήσουν πρόσβαση σε κρυπτογραφημένη επικοινωνία μέσω εμπιστευτικών πληροφοριοδοτών ή μυστικών πρακτόρων.
• Μπορούν να ασκήσουν μεγάλη πίεση ή βασανιστήρια για να εξαναγκάσουν άτομα να ξεκλειδώσουν το τηλέφωνο ή τον υπολογιστή τους ή να δώσουν κωδικούς πρόσβασης.
• Αν και δεν μπορούν να σπάσουν την καλή κρυπτογράφηση εντός οποιουδήποτε πρακτικού χρονικού πλαισίου, σε περίπτωση κατάσχεσης μπορεί να είναι σε θέση να λάβουν δεδομένα από φαινομενικά κρυπτογραφημένες συσκευές λόγω άλλων τρωτών σημείων (π.χ. στο λειτουργικό σύστημα της συσκευής) ή λειτουργικών αστοχιών ασφαλείας.

Οποιαδήποτε ασφαλής μέθοδος επικοινωνίας εξαρτάται σε μεγάλο βαθμό από τις πρακτικές ασφαλείας του χρήστη. Δεν έχει σημασία αν χρησιμοποιείτε την προτιμώμενη εφαρμογή ασφαλής επικοινωνίας του Edward Snowden (στμ: εννοεί μια φανταστική, ιδανική εφαρμογή), αν ο εχθρός σας έχει εγκαταστήσει keylogger στο τηλέφωνό σας, ή αν κάποιος μοιράζεται screenshots των κρυπτογραφημένων κειμένων σας στο Twitter, ή αν το τηλέφωνό σας κατασχεθεί και δεν είναι σωστά ασφαλισμένο.[3]

Η πλήρης εξήγηση της επιχειρησιακής ασφάλειας, της κουλτούρας ασφάλειας, των συναφών εννοιών και βέλτιστων πρακτικών δεν περιλαμβάνονται στο παρόν κείμενο - η συζήτηση αυτή αποτελεί μόνο *ένα μέρος* της επιχειρησιακής ασφάλειας που σχετίζεται με το μοντέλο απειλών με το οποίο ασχολούμαστε. Πρέπει να εξετάσετε γενικότερα την κουλτούρα ασφαλείας για την προστασία από την απειλή των εισβολέων και των πληροφοριοδοτών,

τον τρόπο ασφαλούς χρήσης συσκευών όπως τα τηλέφωνα και οι φορητοί υπολογιστές ώστε να μην μπορούν να βοηθήσουν στη δημιουργία μιας υπόθεσης εναντίον σας εάν κατασχεθούν, και τον τρόπο δημιουργίας συνηθειών για την πλήρη ελαχιστοποίηση των δεδομένων που αφήνονται σε ηλεκτρονικές συσκευές (συναντηθείτε πρόσωπο με πρόσωπο και αφήστε το τηλέφωνό σας στο σπίτι!).

Η λεγόμενη «κυβερνοασφάλεια» κινείται ταχύτατα: υπάρχει ένας πόλεμος φθοράς μεταξύ των απειλών και των προγραμματιστών εφαρμογών. Οι πληροφορίες που παρέχονται εδώ μπορεί να είναι ξεπερασμένες τη στιγμή που διαβάζετε αυτό το κείμενο. Χαρακτηριστικά ή υλοποιήσεις εφαρμογών ενδέχεται να αλλάξουν, ακυρώνοντας εν μέρει ορισμένα από τα επιχειρήματα που διατυπώνονται εδώ (ή ενισχύοντάς τα). Εάν η ασφάλεια των ηλεκτρονικών σας επικοινωνιών είναι ζωτικής σημασίας για την ασφάλειά σας, δεν πρέπει να εμπιστεύεστε οποιαδήποτε σύσταση που δίνεται εδώ ή αλλού χωρίς να την αμφισβητήσετε.

Signal Loss

πώς ξεκίνησε vs πώς πάει

Πιθανώς χρησιμοποιήσατε το Signal σήμερα. Και τίποτα δεν είναι πραγματικά τόσο κακό με το Signal. Είναι σημαντικό να δηλώσουμε ότι παρά τις παρακάτω κριτικές, ο στόχος εδώ δεν είναι να προκαλέσουμε πανικό σχετικά με τη χρήση του Signal. Το συμπέρασμά σας δεν πρέπει να είναι να διαγράψετε αμέσως το Signal, να κάψετε το τηλέφωνό σας και να τρέξετε στο δάσος. Ίσως θα πρέπει να το κάνετε αυτό ούτως ή άλλως για τη δική σας ψυχική υγεία, αλλά, όχι μόνο εξαιτίας αυτού του οδηγού. Σκεφτείτε τουλάχιστον να πάτε πρώτα μια πεζοπορία.

Μια προσπάθεια για την αντιμετώπιση ορισμένων θεωριών συνωμοσίας

Ένα γρήγορο duckduckgoing [στμ: εναλλακτική του googling] (ή μήπως αναζήτηση στο Twitter;) για το “Signal CIA” θα σας φέρει άφθονη παραπληροφόρηση και θεωρίες συνωμοσίας σχετικά με το Signal. Δεδομένης της ήδη κριτικής φύσης αυτού του οδηγού και της σημασίας του να προσεγγίζουμε τέτοια ευαίσθητα ζητήματα, παρακαλώ επιτρέψτε ένα μικρό παραλήρημα σχετικά με αυτές τις θεωρίες συνωμοσίας.

Η πιο συνηθισμένη θεωρία συνωμοσίας σχετικά με το Signal είναι ότι αναπτύχθηκε κρυφά από τη CIA και επομένως είναι "backdoored". Κατά συνέπεια, η CIA (ή μερικές φορές η NSA) έχει τη δυνατότητα να έχει εύκολη πρόσβαση σε ό,τι λέτε στο Signal, εισχωρώντας από τη μυστική τους πίσω πόρτα.[4]

Η αλήθεια που πυροδότησε αυτή τη θεωρία έχει ως εξής:

> *Μεταξύ 2013 και 2016, οι προγραμματιστές του Signal έλαβαν χρηματοδότηση από το Open Technology Fund κοντά στα 3 εκατομμύρια αμερικανικά δολάρια. Το OTF ήταν αρχικά ένα πρόγραμμα του Radio Free Asia, το οποίο εποπτεύεται από την Αμερικανική Υπηρεσία για τα Παγκόσμια Μέσα Μαζικής Ενημέρωσης (από το 2019, το OTF χρηματοδοτείται απευθείας από την USAGM). Η USAGM είναι μια "ανεξάρτητη υπηρεσία της αμερικανικής κυβέρνησης", η οποία προωθεί τα εθνικά συμφέροντα των ΗΠΑ διεθνώς και χρηματοδοτείται και διοικείται απευθείας από την αμερικανική κυβέρνηση. Η κυβέρνηση των ΗΠΑ διαχειρίζεται και χρηματοδοτεί το usagm/Radio Free Asia, το οποίο χρηματοδοτεί το OTF, το οποίο χρηματοδότησε την ανάπτυξη του Signal (και η Hilary Clinton ήταν τότε υπουργός Εξωτερικών!!!) - επομένως, η CIA δημιούργησε το Signal.*

Η USAGM (και όλα τα έργα της, όπως το Radio Free Asia και το OTF) προωθεί τα εθνικά συμφέροντα των ΗΠΑ υπονομεύοντας ή διαταράσσοντας κυβερνήσεις με τις οποίες οι ΗΠΑ βρίσκονται σε ανταγωνισμό ή σύγκρουση. Εκτός από την προώθηση αντίθετων αφηγήσεων των μέσων ενημέρωσης (μέσω της υποστήριξης ενός «ελεύθερου και ανεξάρτητου Τύπου» σε αυτές τις χώρες) αυτό περιλαμβάνει επίσης την παραγωγή εργαλείων που μπορούν να χρησιμοποιηθούν για την παράκαμψη της λογοκρισίας και την αντίσταση σε «καταπιεστικά καθεστώτα».

Οι δικαιούχοι του OTF αποκαλύπτονται με διαφάνεια[5] και δεν είναι μυστικό ότι ο στόχος του OTF είναι να δημιουργήσει εργαλεία για την υπονόμευση της εξουσίας καθεστώτων που βασίζονται σε μεγάλο βαθμό σε ανοιχτή διαδικτυακή καταστολή, μαζική παρακολούθηση και ισχυρή λογοκρισία στο διαδίκτυο για να διατηρήσουν την εξουσία τους (και ότι αυτά τα καθεστώτα είναι εκείνα που η κυβέρνηση των ΗΠΑ τυχαίνει να μην συμπαθεί). Το πώς και το γιατί συμβαίνει αυτό σε σχέση με έργα όπως το Signal αναφέρεται ξεκάθαρα από κυρίαρχα μέσα όπως η Wall Street Journal.[6] Μέσα όπως το RT αναφέρουν τις ίδιες πληροφορίες με εντυπωσιακή σάλτσα από πάνω[7] που οδηγεί στην ανάπτυξη θεωριών συνωμοσίας.

Το Signal είναι ανοικτού κώδικα (open-source), πράγμα που σημαίνει ότι όλος ο κώδικάς του ελέγχεται και εξετάζεται από ειδικούς. Είναι το μοναδικό μέρος που όλοι ψάχνουν για μια κερκόπορτα (back-door) της CIA. Όσον αφορά τη μαζική παρακολούθηση, είναι ευκολότερο και αποτελεσματικότερο για τους εχθρούς μας να εισάγουν κρυφά κάποιο κώδικα επιτήρησης σε ευρέως χρησιμοποιούμενες διαδικτυακές εφαρμογές και υποδομές κλειστού κώδικα (closed-source) με τη συνεργασία συνυπεύθυνων εταιρειών.[8] Όσον αφορά τη στοχευμένη παρακολούθηση, είναι ευκολότερο να εγκαταστήσουν κακόβουλο λογισμικό στο τηλέφωνό σας.[9]

Πολλά έργα λογισμικού ανοικτού κώδικα, όπως το Signal, έχουν λάβει χρηματοδότηση από παρόμοιες πηγές. Το OTF χρηματοδοτεί επίσης ή έχει χρηματοδοτήσει πολλά άλλα πρότζεκτ που ίσως έχετε ακούσει: Το Tor (για το οποίο υπάρχουν παρόμοιες θεωρίες συνωμοσίας), το K-9 Mail, το NoScript, το F-Droid, το Certbot και το Tails (στους προγραμματιστές του οποίου περιλαμβάνονται αναρχικές).

Η χρηματοδότηση αυτή γνωστοποιείται πάντοτε με διαφάνεια. Απλά ελέγξτε τη σελίδα των χορηγών του Tails[10], όπου μπορείτε να δείτε την OTF να αναφέρεται ως ο παλαιότερος χορηγός (και ότι ο σημερινός κορυφαίος χορηγός τους είναι... το Υπουργείο Εξωτερικών των ΗΠΑ!). Και οι δύο εφαρμογές PET που εξετάζονται σε αυτόν τον οδηγό χρηματοδοτούνται εν μέρει από παρόμοιες πηγές.

Υπάρχει μια ατελείωτη συζήτηση σχετικά με τις πηγές χρηματοδότησης των έργων ανοικτού κώδικα που διευκολύνουν την προστασία της ιδιωτικής ζωής ή την αντίσταση στην επιτήρηση: σύγκρουση συμφερόντων, ηθική, αξιοπιστία, τέτοια εργαλεία να αναπτύσσονται στο πλαίσιο της νεοφιλελεύθερης γεωπολιτικής... Είναι καλό να υπάρχει ένας υγιής σκεπτικισμός και κριτική σχετικά με τον τρόπο χρηματοδότησης αυτών των πρότζεκτ, αλλά δεν πρέπει να μας οδηγεί σε θεωρίες συνωμοσίας που θολώνουν τις συζητήσεις σχετικά με την πραγματική τους ασφάλεια στην πράξη. Το Signal έχει λάβει χρηματοδότηση από πολλές τέτοιες «περίεργες» πηγές: Η αρχική ανάπτυξη του Signal χρηματοδοτήθηκε από την πώληση του έργου που υπήρξε πρόδρομός του, του TextSecure, στο Twitter έναντι άγνωστου ποσού. Πιο πρόσφατα, το Signal έλαβε δάνειο ύψους 50 εκατομμυρίων αμερικανικών δολαρίων, με επιτόκιο 0%, από τον ιδρυτή του WhatsApp, ο οποίος είναι τώρα ο διευθύνων σύμβουλος του Signal Foundation. Υπάρχουν πολλά έγκυρα στοιχεία που εξηγούν γιατί και πώς το Signal χρηματοδοτήθηκε από κάποια πρωτοβουλία της προσπάθειας των ΗΠΑ για παγκόσμια κυριαρχία, τα οποία σε καμία περίπτωση δεν υποδηλώνουν ή υπονοούν την ύπαρξη κάποιας αδύνατης προς απόκρυψη κερκόπορτας της CIA που προορίζεται να στοχεύσει τους χρήστες του Signal.

Είναι εντάξει το Signal τελικά;

Οπότε, αν το Signal δεν είναι επιχείρηση της CIA, τότε όλα καλά, σωστά; Τα πρωτόκολλα κρυπτογράφησης του Signal θεωρούνται ευρέως ασφαλή και το Signal έχει μεγάλο ιστορικό βελτίωσης των χαρακτηριστικών του και έγκαιρης και διαφανούς αντιμετώπισης των τρωτών σημείων. Το Signal κατάφερε να κάνει με επιτυχία την κρυπτογραφημένη συνομιλία από άκρο σε άκρο (end-to-end) αρκετά εύκολη ώστε να γίνει πραγματικά δημοφιλής. Η ευρεία υιοθέτηση του Signal είναι σχεδόν σίγουρα κάτι καλό.

Αλλά πέρα από τις θεωρίες συνωμοσίας, υπάρχουν καλοί λόγοι για τα αναρχικά να έχουν επιφυλάξεις απέναντι στο Signal. Ο Moxie είχε μια κάπως δογματική προσέγγιση σε πολλές τεχνικές και επιλογές σχετικά με τη δομή του λογισμικού που έγιναν κατά την ανάπτυξη του Signal. Αυτές οι αποφάσεις ελήφθησαν σκόπιμα (όπως εξηγήθηκε σε αναρτήσεις, σε ομιλίες και σε διάφορα απόκρυφα θέματα στο GitHub) για να διευκολυνθεί η ευρεία υιοθέτηση του Signal Messenger από χρήστες με λιγότερες τεχνολογικές γνώσεις, να διευκολυνθεί η μακροπρόθεσμη ανάπτυξη του πρότζεκτ και να επιτραπεί η ομαλή εξέλιξη και η προσθήκη νέων χαρακτηριστικών.

Οι πορωμένοι με την κυβερνοασφάλεια χρήστες διαδικτύου έχουν από καιρό επικρίνει αυτές τις αποφάσεις ως συμβιβασμούς που θυσιάζουν την ασφάλεια των χρηστών, την ιδιωτικότητα ή την ανωνυμία προς όφελος των στόχων του Moxie για το Signal. Το να εμβαθύνουμε πολύ σε αυτό το θέμα ενέχει τον κίνδυνο να εισέλθουμε στην περιοχή της συζήτησης που κυριαρχείται από σχολαστικούς ποζεράδες φαν του ελεύθερου λογισμικου (αν δεν έχουμε φτάσει ήδη σε αυτό το σημείο). Για να είμαστε εξαιρετικά σύντομοι, οι δικαιολογίες του Moxie μπορούν να συνοψιστούν στο να διατηρήσει το Signal ανταγωνιστικό

στο καπιταλιστικό, κερδοσκοπικό οικοσύστημα της Silicon Valley. Πέρα από τις συζητήσεις σχετικά με τις στρατηγικές ανάπτυξης λογισμικού στον ύστερο καπιταλισμό, οι πτυχές του Signal που επικρίνονται συχνότερα είναι οι εξής:

- Το Signal βασίζεται σε μια κεντρικοποιημένη υποδομή server
- Το Signal απαιτεί κάθε λογαριασμός να συνδέεται με έναν αριθμό τηλεφώνου
- Το Signal διαθέτει ενσωματωμένο σύστημα πληρωμών με κρυπτονόμισμα

Ίσως ο Moxie να είχε δίκιο και οι συμβιβασμοί του να άξιζαν τον κόπο: σήμερα, το Signal είναι εξαιρετικά δημοφιλές, η εφαρμογή έχει επεκταθεί σημαντικά με ελάχιστες δυσκολίες, πολλά νέα χαρακτηριστικά (τόσο για τη χρηστικότητα όσο και για την ασφάλεια) έχουν εισαχθεί εύκολα και φαίνεται να είναι βιώσιμο για το άμεσο μέλλον.[11]

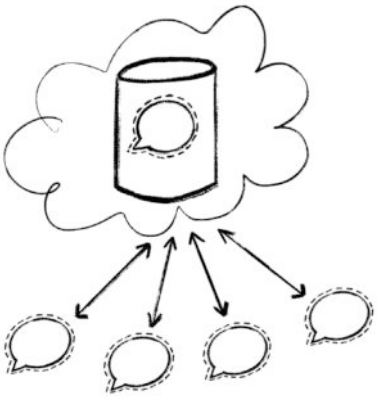
Όμως η διευρυμένη παρουσία του Signal ως αναρχική υποδομή απαιτεί προσεκτική εξέταση αυτών των κριτικών, ειδικά όσον αφορά τις περιπτώσεις χρήσης και το μοντέλο απειλών εναντίον μας σε έναν μεταβαλλόμενο κόσμο. Η εξέταση αυτών των κριτικών για το Signal θα βοηθήσει να εξηγήσουμε πώς οι εφαρμογές PET όπως το Briar και το Cwtch, οι οποίες χρησιμοποιούν μια εντελώς διαφορετική προσέγγιση για την ασφαλή επικοινωνία, μπορούν ενδεχομένως να μας προσφέρουν μεγαλύτερη ασφάλεια.

Το Signal ως κεντρικοποιημένη υπηρεσία

Το Signal είναι στην πραγματικότητα λιγότερο εφαρμογή και περισσότερο υπηρεσία. Το Signal (Open Whisper Systems/The Signal Foundation) παρέχει την εφαρμογή Signal (την οποία μπορείτε να κατεβάσετε και να ανοίξετε στο τηλέφωνο ή τον υπολογιστή σας) και λειτουργεί τον Server του Signal.[12] Η εφαρμογή Signal από μόνη της δεν μπορεί να κάνει τίποτα. Ο Server του Signal παρέχει την υπηρεσία με το να χειρίζεται και να αναμεταδίδει όλα τα μηνύματα που αποστέλλονται και λαμβάνονται μέσω Signal.

Έτσι λειτουργούν οι περισσότερες εφαρμογές συνομιλίας. Το Discord, το WhatsApp, το iMessage, το Instagram/Facebook Messenger και τα απευθείας μηνύματα στο Twitter είναι όλες κεντρικοποιήμενες υπηρεσίες επικοινωνίας, όπου τρέχετε μια εφαρμογή στη συσκευή σας και ένας κεντρικός server που λειτουργεί από κάποιο τρίτο μέρος αναμεταδίδει τα μηνύματα μεταξύ των ατόμων. Ένας τέτοιος συγκεντρωτισμός παρέχει πολλά οφέλη στα άτομα που χρησιμοποιούν την εφαρμοή. Μπορείτε να συγχρονίσετε τα μηνύματα και το προφίλ σας μέσω του server για να έχετε πρόσβαση σε αυτά σε διαφορετικές συσκευές. Μπορείτε να στείλετε ένα μήνυμα στον φίλο σας ακόμη και όταν αυτός είναι εκτός σύνδεσης και ο server θα αποθηκεύσει το μήνυμα μέχρι ο φίλος σας να συνδεθεί και να το ανακτήσει. Οι ομαδικές συνομιλίες μεταξύ πολλών χρηστών λειτουργούν άψογα, ακόμη και αν οι χρήστες μπορεί να είναι εντός ή εκτός σύνδεσης σε διαφορετικές χρονικές στιγμές.

Το Signal χρησιμοποιεί end-to-end κρυπτογράφηση, πράγμα που σημαίνει ότι ο Server του Signal δεν μπορεί να διαβάσει κανένα από τα μηνύματά σας. Όμως το γεγονός ότι είναι μια κεντρικοποιημένη υπηρεσία επικοινωνίας έχει πολλές σημαντικές επιπτώσεις στην ασφάλεια και την αξιοπιστία του.



Το Ταχυδρομείο του Signal

Σκεφτείτε ότι το Signal είναι σαν μια ταχυδρομική υπηρεσία. Είναι μια πολύ καλή ταχυδρομική υπηρεσία, όπως ίσως να έχουν κάπου στην Ευρώπη. Σε αυτό το παράδειγμα, ο Server του Signal είναι σαν ένα ταχυδρομείο. Γράφετε ένα γράμμα στον φίλο σας και το σφραγίζετε σε έναν φάκελο με διεύθυνση (ας πούμε ότι κανείς άλλος εκτός από τον φίλο σας δεν μπορεί να ανοίξει τον φάκελο - αυτή είναι η κρυπτογράφηση). Όταν σας βολεύει, αφήνετε όλα τα γράμματα που στέλνετε στο ταχυδρομείο Signal, όπου ταξινομούνται και αποστέλλονται στους διάφορους φίλους στους οποίους απευθύνονται. Αν κάποιος φίλος δεν είναι στο σπίτι, κανένα πρόβλημα! Το ταχυδρομείο Signal θα κρατήσει το γράμμα μέχρι να βρει τον φίλο σας στο σπίτι, ή ο φίλος σας μπορεί απλώς να το παραλάβει από το τοπικό ταχυδρομείο Signal. Το ταχυδρομείο Signal είναι πολύ καλό (Ευρώπη, σωστά;) και σας επιτρέπει ακόμη και να προωθήσετε την αλληλογραφία σας οπουδήποτε θέλετε να την παραλάβετε.

Ίσως μπορείτε να εντοπίσετε το δυνητικό ζήτημα ασφάλειας που προκύπτει από τη στήριξη στο ταχυδρομείο Signal για τη διαχείριση του συνόλου της αλληλογραφίας σας. Οι σφραγισμένοι φάκελοι σημαίνουν ότι κανένας από τους ταχυδρόμους ή τους υπαλλήλους του ταχυδρομικού γραφείου Signal δεν μπορεί να διαβάσει τα γράμματά σας (κρυπτογράφηση = δεν μπορούν να ανοίξουν τους φακέλους). Όποιος όμως έχει έναν κανονικό ταχυδρόμο, γνωρίζει ότι μπορεί να μάθει πολλά για εσάς μόνο και μόνο με το χειρισμό του συνόλου της αλληλογραφίας σας. Γνωρίζουν από ποιον λαμβάνετε επιστολές, όλες τις συνδρομές σας σε περιοδικά, πότε είστε στο σπίτι ή όχι, όλα τα διαφορετικά μέρη στα οποία προωθείτε την αλληλογραφία σας και όλες τις ντροπιαστικές μαλακίες που παραγγέλνετε στο διαδίκτυο. Αυτό είναι το πιθανό πρόβλημα με μια κεντρικοποιημένη υπηρεσία που χειρίζεται όλη την αλληλογραφία σας - εννοώ τα μηνύματα!

Τα μεταδεδομένα διαρκούν για πάντα

Οι πληροφορίες που γνωρίζουν όλοι στο ταχυδρομείο Signal για εσάς και την αλληλογραφία σας είναι τα μεταδεδομένα. Τα μεταδεδομένα είναι δεδομένα για τα δεδομένα. Αυτά μπορεί να περιλαμβάνουν πράγματα όπως ο αποστολέας και ο παραλήπτης ενός μηνύματος, η ώρα που στάλθηκε και ο τόπος όπου παραδόθηκε. Όλη η κίνηση στο διαδίκτυο παράγει εγγενώς αυτού του είδους τα μεταδεδομένα. Οι κεντρικοποιημένοι servers παρέχουν ένα εύκολο

σημείο όπου όλα αυτά τα μεταδεδομένα θα μπορούσαν να παρατηρηθούν ή να συλλεχθούν, δεδομένου ότι όλα τα μηνύματα περνούν από ένα μόνο σημείο.

Πρέπει να τονιστεί ότι το παραπάνω παράδειγμα σχετικά με το ταχυδρομείο Signal είναι απλώς μεταφορικό για να καταδείξει τι είναι τα μεταδεδομένα και γιατί είναι ένα σημαντικό ζήτημα για τις κεντρικοποιημένες υπηρεσίες επικοινωνίας. Το Signal είναι στην πραγματικότητα *εξαιρετικά καλό* στο να ελαχιστοποιεί ή να αποκρύπτει τα μεταδεδομένα. Χάρη στην κρυπτογραφική μαύρη μαγεία και τον έξυπνο σχεδιασμό του λογισμικού, υπάρχουν πολύ λίγα μεταδεδομένα στα οποία ο Server του Signal μπορεί εύκολα να έχει πρόσβαση. Με τα ίδια τα λόγια του Signal:

> *«Δεν αποθηκεύουμε πράγματα που περιλαμβάνουν οτιδήποτε σχετικά με τις επαφές ενός χρήστη (όπως οι ίδιες οι επαφές, ένα hash των επαφών, οποιεσδήποτε άλλες παράγωγες πληροφορίες επικοινωνίας), οτιδήποτε σχετικά με τις ομάδες ενός χρήστη (όπως σε πόσες ομάδες είναι ένας χρήστης, σε ποιες ομάδες είναι ένας χρήστης, τις λίστες μελών των ομάδων ενός χρήστη), ή οποιαδήποτε αρχεία σχετικά με το με ποιους έχει επικοινωνήσει ένας χρήστης».[13]*

Υπάρχουν μόνο δύο είδη μεταδεδομένων που είναι γνωστό ότι αποθηκεύονται πάντα:
• εάν ένας συγκεκριμένος αριθμός τηλεφώνου είναι καταχωρημένος σε λογαριασμό Signal
• η τελευταία φορά που ένας συγκεκριμένος λογαριασμός Signal συνδέθηκε με τον server

Αυτό είναι καλό! Θεωρητικά, αυτό είναι το μόνο που μπορεί να μάθει για εσάς οποιοσδήποτε περίεργος υπάλληλος στο ταχυδρομείο Signal. Αλλά αυτό οφείλεται, εν μέρει, στην προσέγγιση «δεν το βλέπω» του ίδιου του Signal Server. Σε κάποιο βαθμό, πρέπει να εμπιστευτούμε τον Server του Signal ότι κάνει αυτό που ισχυρίζεται...

Η εμπιστοσύνη είναι μονόδρομος

Όπως και η εφαρμογή Signal στο τηλέφωνο ή τον υπολογιστή σας, ο Server του Signal βασίζεται επίσης σε (ως επί το πλείστον)[14] ανοιχτό κώδικα και, ως εκ τούτου, υπόκειται στον ίδιο έλεγχο και τις ίδιες επιθεωρήσεις από ειδικούς ασφαλείας.

Ωστόσο, υπάρχει μια σημαντική και αναπόφευκτη πραγματικότητα που πρέπει να λάβουμε υπόψη σχετικά με τον Server του Signal: είμαστε αναγκασμένοι να εμπιστευτούμε το γεγονός ότι ο Server του Signal εκτελεί πράγματι τον ίδιο open-source κώδικα που μοιράζεται μαζί μας. Αυτό είναι ένα θεμελιώδες πρόβλημα με την εμπιστοσύνη σε οποιονδήποτε κεντρικό server που εκτελείται από τρίτους.

> *«Δεν συλλέγουμε ούτε αποθηκεύουμε ευαίσθητες πληροφορίες για τους χρήστες μας και αυτό δεν πρόκειται να αλλάξει ποτέ».[15]*

Ως τεράστιος δημόσιος μη κερδοσκοπικός οργανισμός, το Signal δεν είναι σε θέση να αρνηθεί να συμμορφωθεί με εντάλματα ή κλήσεις για δεδομένα χρηστών. Το Signal διαθέτει μάλιστα μια σελίδα στον ιστότοπό του[16] στην οποία απαριθμούνται διάφορες κλητεύσεις που έχουν λάβει και οι απαντήσεις τους. Θυμηθείτε τα δύο κομμάτια μεταδεδομένων που αποθηκεύει ο Server του Signal και τα οποία μπορούν να αποκαλυφθούν:

Account	Responsive Information in Signal's Possession
[redacted]	Last connection date: 1634169600000 (unix millis) Account created: 1606866784432 (unix millis)

Οι απαντήσεις του Signal δείχνουν την τελευταία ημερομηνία σύνδεσης, την ημερομηνία δημιουργίας λογαριασμού και τον αριθμό τηλεφώνου (τροποποιημένο).

Τη στιγμή που γράφονται αυτές οι γραμμές δεν υπάρχει λόγος να αμφισβητηθούν τα παραπάνω, αλλά θα πρέπει να σημειωθεί ότι το Signal συμμορφώνεται επίσης με εντολές φίμωσης που το εμποδίζουν να αποκαλύψει ότι έχει λάβει ακόμη και κλήτευση ή ένταλμα.[17] Ιστορικά, το Signal καταπολεμά αυτές τις εντολές αποσιώπησης, αλλά δεν ξέρουμε τι δεν ξέρουμε και το Signal δεν χρησιμοποιεί κάποιο τρόπο (ένα "warrant canary") για να ειδοποιεί τους χρήστες για τυχόν κλητεύσεις ή εντάλματα που δεν έχουν ακόμη αποκαλυφθεί. Δεν υπάρχει κανένας σοβαρός λόγος να πιστεύουμε ότι το Signal συνεργάστηκε με τις διωκτικές αρχές είτε συχνότερα είτε σε μεγαλύτερο βαθμό από ό,τι ισχυρίζεται, αλλά υπάρχουν τρία σενάρια που πρέπει να εξετάσουμε:

• Οι αλλαγές στη νομοθεσία θα μπορούσαν να οδηγήσουν στο να υποχρεωθεί το Signal να συλλέγει και να αποκαλύπτει περισσότερες πληροφορίες για τους χρήστες του κατόπιν αιτήματος, και αυτό θα μπορούσε να συμβεί χωρίς να το γνωρίζει το κοινό.
• Το Signal θα μπορούσε να πεισθεί με ηθικά, πολιτικά ή πατριωτικά επιχειρήματα να συνεργαστεί κρυφά με αντιπάλους μας.
• Οι εχθροί μας θα μπορούσαν να διεισδύσουν στο Signal ή να το παραβιάσουν για να συλλέξουν περισσότερα δεδομένα χρηστών κρυφά ή να έχουν πρόσβαση με άλλο τρόπο στα ελάχιστα μεταδεδομένα που υπάρχουν πιο εύκολα.

Όλα αυτά τα σενάρια είναι πιθανά και έχουν ιστορικά προηγούμενα αλλού, αλλά δεν είναι απαραίτητα δυνατά. Λόγω της προαναφερθείσας «κρυπτογραφικής μαύρης μαγείας» και της πολυπλοκότητας των πρωτοκόλλων δικτύου, ακόμη και αν ο Server του Signal είχε τροποποιηθεί ώστε να είναι κακόβουλος, εξακολουθεί να υπάρχει ένα όριο στο πόσα μεταδεδομένα θα μπορούσαν να συλλεχθούν χωρίς να γίνουν αντιληπτά από τους χρήστες ή τους παρατηρητές. Δεν θα ήταν ισοδύναμο, ας πούμε, με το ταχυδρομείο Signal να αφήνει έναν κατάσκοπο (μέσω μιας κυριολεκτικής «κερκόπορτας της CIA!») ο οποίος διαβάζει και καταγράφει όλα τα μεταδεδομένα για κάθε επιστολή που περνάει από εκεί. Αλλαγές στις πολιτικές και τον κώδικα του Signal θα μπορούσαν να έχουν ως αποτέλεσμα μικρές αλλά αυξανόμενες ποσότητες μεταδεδομένων ή άλλων πληροφοριών να είναι εύκολα διαθέσιμες στους αντιπάλους μας, και αυτό θα μπορούσε να συμβεί με ή χωρίς τη γνώση μας. Δεν υπάρχει κανένας ιδιαίτερος λόγος να μην εμπιστευόμαστε τον Server του Signal σε αυτό το σημείο, αλλά ο κόσμος της αναρχίας πρέπει να ζυγίσει πόσο εμπιστεύεται κάποιον τρίτο, ακόμη κι αν είναι ιστορικά αξιόπιστος όπως είναι το Signal.

Μεγάλα δεδομένα (Big Data)

Πολλοί ισχυροί αντίπαλοι μας είναι σε θέση να καταγράφουν και να αποθηκεύουν τεράστιες ποσότητες κίνησης στο διαδίκτυο.[18] Αυτό μπορεί να περιλαμβάνει τα πραγματικά περιεχόμενα μηνυμάτων για μη κρυπτογραφημένη κίνηση, αλλά με την ευρεία χρήση της κρυπτογράφησης, πλέον καταγράφονται και αποθηκεύονται κυρίως μεταδεδομένα σχετικά με την κίνηση και τη δραστηριότητα της καθεμιάς στο διαδίκτυο.

Μπορούμε να επιλέξουμε να εμπιστευτούμε ότι το Signal δεν βοηθά ενεργά τους αντιπάλους μας στη συλλογή μεταδεδομένων σχετικά με τις επικοινωνίες των χρηστών του, αλλά οι αντίπαλοί μας έχουν πολλούς άλλους τρόπους για να συλλέξουν αυτά τα δεδομένα: είτε με τη συνεργασία εταιρειών φιλοξενίας όπως η Amazon ή η Google (το Signal φιλοξενείται επί του παρόντος από την Amazon Web Services), είτε στοχεύοντας τέτοιες εταιρείες φιλοξενίας[19] χωρίς τη συνεργασία τους, είτε απλά παρακολουθώντας την κίνηση στο διαδίκτυο σε μαζική κλίμακα.[20]

Τα μεταδεδομένα σχετικά με τις δραστηριότητες του καθενός στο διαδίκτυο είναι επίσης όλο και περισσότερο διαθέσιμα σε λιγότερο ισχυρούς αντιπάλους, οι οποίοι είναι σε θέση να τα αγοράσουν σε ακατέργαστη ή αναλυμένη μορφή από μεσίτες δεδομένων, οι οποίοι με τη σειρά τους τα αγοράζουν ή τα αποκτούν από οντότητες όπως οι προγραμματιστές εφαρμογών ή οι πάροχοι κινητής τηλεφωνίας.[21]

Τα μεταδεδομένα που συλλέγονται με αυτόν τον τρόπο οδηγούν σε μεγάλα, δύσχρηστα σύνολα δεδομένων, τα οποία ήταν προηγουμένως δύσκολο να αναλυθούν. Όμως, όλο και περισσότερο οι αντίπαλοί μας (ακόμη και οι εταιρείες ή οι δημοσιογράφοι) μπορούν να πάρουν αυτά τα τεράστια σύνολα δεδομένων, να τα συνδυάσουν και να εφαρμόσουν ισχυρά εργαλεία αλγοριθμικής ανάλυσης για να αποδώσουν χρήσιμες συσχετίσεις σχετικά με άτομα ή ομάδες ανθρώπων (αυτό συχνά αναφέρεται ως “Big Data”). Ακόμα και η πρόσβαση σε μικρές ποσότητες αυτών των δεδομένων και οι ακατέργαστες τεχνικές ανάλυσης μπορούν να αποανωνυμοποιήσουν άτομα και να αποδώσουν χρήσιμα αποτελέσματα.[22]

Ο Tommy ο μηνυματάκιας

Αυτό είναι ένα υποθετικό παράδειγμα για να καταδειχθεί πώς η ανάλυση της κίνησης και η συσχέτιση των μεταδεδομένων μπορούν να αποανωνυμοποιήσουν έναν χρήστη του Signal.

Φανταστείτε έναν θαμώνα του κινηματογράφου με κακούς τρόπους, τον Tommy, ο οποίος στέλνει συνέχεια μηνύματα στο Signal κατά τη διάρκεια της ταινίας. Η αντανάκλαση της οθόνης του τηλεφώνου του (ο Tommy δεν χρησιμοποιεί τη σκοτεινή λειτουργία) ενοχλεί τους πάντες στην αίθουσα. Αλλά κατά τα άλλα είναι πολύ σκοτεινά στο σινεμά για να καταλάβει ο Tanner, ο πολυάσχολος διευθυντής, ποιος ακριβώς στέλνει συνέχεια μηνύματα. Ο Tanner αρχίζει να συλλέγει όλα τα δεδομένα που περνούν από το Wi-Fi του θεάτρου αναζητώντας συνδέσεις με τον Signal Server. Οι συχνές συνδέσεις του Tommy με τον Signal Server ξεχωρίζουν αμέσως. Ο Tanner είναι σε θέση να καταγράψει τη διεύθυνση MAC (ένα μοναδικό αναγνωριστικό που σχετίζεται με κάθε τηλέφωνο) και να επιβεβαιώσει ότι η ίδια συσκευή χρησιμοποιεί συχνά το Signal στο Wi-Fi του θεάτρου κατά τη διάρκεια της παράστασης. Στη συνέχεια, ο Tanner είναι σε θέση να το συσχετίσει με τα αρχεία συναλλαγών πιστωτικών καρτών από το ταμείο τους και να ανακαλύψει μια πιστωτική

κάρτα που αγοράζει πάντα εισιτήρια για ταινίες περίπου την ίδια ώρα που είναι ενεργή η συσκευή που χρησιμοποιεί συχνά το Signal (αποκαλύπτεται επίσης το όνομα του κατόχου της κάρτας: Tommy). Έχοντας προσδιορίσει τη διεύθυνση MAC του τηλεφώνου του Tommy, το όνομα και την πιστωτική κάρτα, ο Tanner μπορεί να παράσχει αυτές τις πληροφορίες σε έναν ύπουλο ιδιωτικό ντετέκτιβ, ο οποίος θα αγοράσει πρόσβαση σε μεγάλα σύνολα δεδομένων που συλλέγονται από μεσίτες δεδομένων (από παρόχους κινητής τηλεφωνίας και εφαρμογές κινητής τηλεφωνίας) και θα προσδιορίσει μια τοποθεσία όπου το ίδιο κινητό τηλέφωνο χρησιμοποιείται συχνότερα. Εκτός από τον κινηματογράφο, αυτό είναι το σπίτι του Tommy. Ο Tanner πηγαίνει στο σπίτι του Tommy τη νύχτα και ανατινάζει το αυτοκίνητό του (ο κινηματογράφος είναι βιτρίνα των Hell's Angels).

Οπλισμένα μεταδεδομένα

> *«Σκοτώνουμε ανθρώπους με βάση τα μεταδεδομένα... ...αλλά δεν το κάνουμε αυτό με τα συγκεκριμένα μεταδεδομένα!» (χαμογελά ύπουλα, το ακροατήριο ξεσπά σε γέλια)[23]* - Στρατηγός Michael Hayden, πρώην διευθυντής της NSA 1999-2005 και διευθυντής της CIA 2006-2009

Σε ένα διαδίκτυο όπου οι αντίπαλοι μας έχουν τις δυνατότητες να συλλέγουν και να αναλύουν τεράστιες ποσότητες μεταδεδομένων και κίνησης, η χρήση κεντρικών server μπορεί να αποτελέσει τον αδύναμο κρίκο. Οι αντίπαλοι μας μπορούν ευκολότερα να στοχεύσουν συσκευές που επικοινωνούν με τον server του Signal είτε παρακολουθώντας την κυκλοφορία στο διαδίκτυο γενικά, είτε σε επίπεδο παρόχου υπηρεσιών διαδικτύου, είτε ενδεχομένως σε σημεία σύνδεσης με τον ίδιο τον serer του signal. Στη συνέχεια, μπορούν να προσπαθήσουν να χρησιμοποιήσουν τεχνικές ανάλυσης για να αποκαλύψουν συγκεκριμένα πράγματα για μεμονωμένους χρήστες ή τις επικοινωνίες τους μέσω του Signal.

Στην πράξη αυτό μπορεί να είναι δύσκολο. Μπορεί να αναρωτηθείτε αν κάποιος που παρατηρεί όλη την κίνηση που εισέρχεται και εξέρχεται από τον Server του Signal θα μπορούσε να προσδιορίσει ότι εσείς και ο φίλος σας ανταλλάσσετε μηνύματα, παρατηρώντας ότι ένα μήνυμα στάλθηκε από τη δική σας διεύθυνση IP στον Signal Server στις 14:01 και στη συνέχεια ο Signal Server έστειλε ένα μήνυμα ίδιου μεγέθους στη διεύθυνση IP του φίλου σας στις 14:02. Ευτυχώς, μια πολύ απλή ανάλυση συσχέτισης όπως αυτή δεν είναι εφικτή τόσο λόγω του όγκου της κίνησης που εισέρχεται και εξέρχεται συνεχώς από τον Signal Server όσο και λόγω του τρόπου με τον οποίο ακριβώς αυτή η κίνηση αντιμετωπίζεται σε αυτό το επίπεδο. Αυτό ισχύει λιγότερο για τις κλήσεις βίντεο/φωνής, όπου τα χρησιμοποιούμενα πρωτόκολλα διαδικτύου καθιστούν πιο εύλογη τη συσχετιστική ανάλυση της κίνησης για να καταλάβουμε ποιος κάλεσε ποιον.[24] Έτσι, κάποιος που παρατηρεί όλη την κίνηση που εισέρχεται και εξέρχεται από τον Signal Server και προσπαθεί να προσδιορίσει ποιος μιλάει σε ποιον έχει πολύ δύσκολο έργο. Ίσως αδύνατο, μέχρι στιγμής.

Και όμως, οι τεχνικές συλλογής δεδομένων και τα εργαλεία αλγοριθμικής ανάλυσης που συνήθως αναφέρονται ως "Big Data" γίνονται κάθε μέρα όλο και πιο ισχυρά. Οι αντίπαλοί μας βρίσκονται στην πρώτη γραμμή. Η ευρεία χρήση της κρυπτογράφησης όλων των τηλεπικοινωνιών έχει καταστήσει την παραδοσιακή υποκλοπή πολύ λιγότερο αποτελεσματική και, κατά συνέπεια, οι αντίπαλοί μας έχουν ισχυρό κίνητρο να αυξήσουν την ικανότητά τους να συγκεντρώνουν και να αναλύουν με χρήσιμο τρόπο τα μεταδεδομένα. Το λένε ξεκάθαρα: «αν έχεις αρκετά μεταδεδομένα, δεν χρειάζεσαι πραγματικά περιεχόμενο».[25] Σκοτώνουν ανθρώπους με βάση τα μεταδεδομένα.

Έτσι, παρόλο που μπορεί να μην είναι δυνατόν να προσδιοριστεί με βεβαιότητα κάτι τόσο ακριβές όσο το ποιος μίλησε με ποιον σε μια συγκεκριμένη χρονική στιγμή, οι αντίπαλοί μας εξακολουθούν να βελτιώνουν ταχύτατα την ικανότητά τους να προσδιορίζουν όποια ευαίσθητη πληροφορία μπορούν από τα μεταδεδομένα. Αποκαλύπτεται τακτικά μέσω διαρροών ότι έχουν στην κατοχή τους πιο ισχυρές ή επεμβατικές δυνατότητες παρακολούθησης από ό,τι πιστεύαμε προηγουμένως - δεν είναι παράλογο να υπολογίσουμε ότι οι δυνατότητές τους είναι πιο προηγμένες από ό,τι γνωρίζουμε.

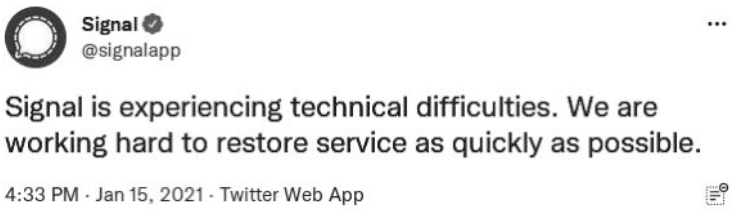
Το Signal είναι πιο ευάλωτο σε αυτό το είδος παρακολούθησης και ανάλυσης, επειδή είναι μια κεντρικοποιημένη υπηρεσία. Η κυκλοφορία του Signal στο διαδίκτυο δεν είναι δύσκολο

να εντοπιστεί και ο Signal Server παρέχει ένα εύκολο κεντρικό σημείο για την παρατήρηση ή τη συλλογή μεταδεδομένων σχετικά με τους χρήστες του Signal και τις δραστηριότητές τους. Πιθανές παραβιάσεις του Signal ή αλλαγές στις πολιτικές του ή στο νόμο θα μπορούσαν να αποφέρουν ακόμη ευκολότερη συλλογή της κίνησης και των μεταδεδομένων του Signal για να τα αναλύσουν οι αντίπαλοί μας.

Οι μεμονωμένοι χρήστες μπορούν να χρησιμοποιήσουν κάποια μέτρα αντιμετώπισης αυτού του φαινομένου, όπως η εκτέλεση του Signal μέσω Tor ή VPN, αλλά αυτό μπορεί να είναι τεχνικά δύσκολο να εφαρμοστεί και επιρρεπές σε σφάλματα των χρηστών. Οποιαδήποτε προσπάθεια να γίνει πιο δύσκολη η σύνδεση ενός χρήστη του Signal με ένα συγκεκριμένο άτομο περιπλέκεται επίσης από το γεγονός ότι το Signal απαιτεί κάθε λογαριασμός να συνδέεται με έναν αριθμό τηλεφώνου (περισσότερα σχετικά με αυτό αργότερα).

Εξαρτήσεις και τρωτά σημεία

Μια κεντρικοποιημένη υπηρεσία σημαίνει ότι δεν υπάρχει μόνο ένα κεντρικό σημείο παρατήρησης, αλλά και ένα μοναδικό ευάλωτο σημείο - το Signal δεν λειτουργεί αν ο Signal Server δεν λειτουργεί. Είναι εύκολο να ξεχάσουμε ότι ισχύει αυτό μέχρι την ημέρα που θα συμβεί. Το Signal μπορεί να κάνει μια λάθος ρύθμιση παραμέτρων ή να χτυπηθεί από μια πλημμύρα νέων χρηστών λόγω ενός viral Tweet και ξαφνικά το Signal απλά δεν λειτουργεί.



[Το Signal αντιμετωπίζει τεχνικές δυσκολίες.
Εργαζόμαστε σκληρά για να αποκαταστήσουμε την υπηρεσία το συντομότερο δυνατό.]

Το Signal θα μπορούσε επίσης να πέσει λόγω σκόπιμων ενεργειών ενός αντιπάλου. Φανταστείτε μια κατανεμημένη επίθεση άρνησης παροχής υπηρεσιών (DDoS) (ή άλλη κυβερνοεπίθεση) με σκοπό τη διακοπή της λειτουργίας του Signal κατά τη διάρκεια μιας μαζικής εξέγερσης. Οι πάροχοι υπηρεσιών που φιλοξενούν στην πραγματικότητα τον Server του Signal θα μπορούσαν επίσης να επιλέξουν να θέσουν εκτός λειτουργίας τον Server του Signal χωρίς προειδοποίηση για διάφορους λόγους: αναγκασμένοι από πολιτική πίεση, από την κοινή γνώμη ή για οικονομικούς λόγους.

Μια κεντρικοποιημένη υπηρεσία είναι επίσης ευκολότερο να διαταραχθεί από κάποιους που ελέγχουν άμεσα την τοπική υποδομή του διαδικτύου τους.[26] Όταν αυτό συμβαίνει σε ορισμένα μέρη, το Signal συνήθως ανταποκρίνεται γρήγορα, εφαρμόζοντας ενεργά δημιουργικές αλλαγές ή παρακάμψεις, με αποτέλεσμα ένα παιχνίδι γάτας και ποντικιού μεταξύ του Signal και οποιουδήποτε έθνους-κράτους προσπαθεί να μπλοκάρει το Signal στην επικράτειά του. Και πάλι, είναι θέμα εμπιστοσύνης ότι τα συμφέροντα του Signal θα ευθυγραμμίζονται πάντα με τα δικά μας, όταν ένας αντίπαλος μας προσπαθεί να διαταράξει το Signal με αυτόν τον τρόπο σε μια συγκεκριμένη περιοχή.

Κρυπτοδιαμάχη

Το 2021, το Signal άρχισε να ενσωματώνει ένα σύστημα πληρωμών στην εφαρμογή χρησιμοποιώντας το κρυπτονόμισμα MobileCoin. Αν δεν είχατε ιδέα, μάλλον δεν είστε οι μόνοι, αλλά μπορείτε να το βρείτε στις ρυθμίσεις.

Το MobileCoin είναι ένα ελάχιστα γνωστό κρυπτονόμισμα που εστιάζει στην προστασία της ιδιωτικότητας και το οποίο ο Moxie βοήθησε επίσης να αναπτυχθεί. Πέρα από τις συζητήσεις σχετικά με τα κρυπτονομίσματα και τις απάτες τύπου pyramid scheme, η ανησυχία εδώ είναι ότι, συμπεριλαμβάνοντας πληρωμές με κρυπτονομίσματα μέσα στην εφαρμογή, το Signal ανοίγεται σε πολύ μεγαλύτερο νομικό έλεγχο από τις αρχές. Τα κρυπτονομίσματα είναι καλά για το έγκλημα και τις απάτες και η κυβέρνηση των ΗΠΑ ασχολείται όλο και περισσότερο με τη ρύθμιση της χρήσης τους. Το Signal δεν είναι μια ομάδα πειρατών - είναι μια υψηλού προφίλ μη κερδοσκοπική εταιρεία, και δεν μπορεί να αντισταθεί βιώσιμα στους όποιους νέους νόμους μπορεί να περάσει η κυβέρνηση των ΗΠΑ για τη ρύθμιση των κρυπτονομισμάτων.

Εάν τα εκατομμύρια των χρηστών του Signal χρησιμοποιούσαν πράγματι το MobileCoin για καθημερινές συναλλαγές, δεν είναι δύσκολο να φανταστούμε ότι το Signal θα αντιμετώπιζε μεγαλύτερο έλεγχο από την Επιτροπή Κεφαλαιαγοράς των ΗΠΑ ή άλλους ρυθμιστικούς φορείς. Στην κυβέρνηση δεν αρέσει η κρυπτογράφηση, αλλά αυτό που πραγματικά δεν αρέσει είναι να πληρώνουν οι κανονικοί άνθρωποι για ναρκωτικά ή να αποφεύγουν τους φόρους. Φανταστείτε ένα σενάριο όπου οι εγκληματίες του κυβερνοχώρου βασίζονται στο Signal και το MobileCoin για να δέχονται πληρωμές από θύματα ransomware. Αυτό θα μπορούσε πραγματικά να φέρει τα πάνω κάτω, και αυτό θα μπορούσε να είναι πολύ αποδιοργανωτικό για το Signal ως αξιόπιστο και ασφαλές εργαλείο επικοινωνίας.

357-99-ρουφιανε

Αυτό το παράπονο θα πρέπει να είναι ήδη γνωστό στα αναρχικά που χρησιμοποιούν το Signal: Οι λογαριασμοί Signal απαιτούν έναν αριθμό τηλεφώνου. Οποιοσδήποτε αριθμός τηλεφώνου συνδέεται με έναν λογαριασμό αποκαλύπτεται επίσης στον οποιονδήποτε συνδέεστε στο Signal. Επιπλέον, είναι εύκολος ο προσδιορισμός του αν ένας συγκεκριμένος αριθμός τηλεφώνου συνδέεται με έναν ενεργό λογαριασμό Signal.

Υπάρχουν λύσεις για αυτό το πρόβλημα, αλλά όλες περιλαμβάνουν την απόκτηση ενός αριθμού τηλεφώνου που δεν μπορεί να ταυτοποιηθεί, ώστε να μπορείτε να τον χρησιμοποιήσετε για να εγγραφείτε σε έναν λογαριασμό Signal. Ανάλογα με το πού βρίσκεστε, τους πόρους που έχετε στη διάθεσή σας και το επίπεδο των τεχνικών σας δεξιοτήτων, αυτό μπορεί να είναι δύσκολο ή και αδύνατο.

Το Signal δεν επιτρέπει επίσης εύκολα τη χρήση πολλαπλών λογαριασμών από το ίδιο τηλέφωνο ή φορητό υπολογιστή. Η δημιουργία πολλαπλών λογαριασμών Signal για διαφορετικές ταυτότητες/ιδιότητες, ή για σύνδεση με διαφορετικά πρότζεκτ, γίνεται μια τεράστια αποστολή, ειδικά από τη στιγμή που χρειάζεστε έναν ξεχωριστό αριθμό τηλεφώνου για το καθένα.

Είναι συνήθως αρκετά εύκολο για τους αντιπάλους μας ακόμα και με περιορισμένους πόρους να αναγνωρίσουν ένα άτομο με βάση τον αριθμό τηλεφώνου του. Επιπλέον, εάν πέσει στα χέρια τους ένα τηλέφωνο που δεν είναι σωστά κλειδωμένο ή κρυπτογραφημένο, αποκτά πρόσβαση στους αριθμούς τηλεφώνου των επαφών και των μελών της ομάδας. Προφανώς πρόκειται για ένα ζήτημα επιχειρησιακής ασφάλειας που υπερβαίνει το Signal, αλλά το γεγονός ότι το Signal απαιτεί κάθε λογαριασμός να συνδέεται με έναν αριθμό τηλεφώνου, επιτείνει σημαντικά τις δυνατότητες χαρτογράφησης δικτύου και τις διάφορες επιζήμιες επιπτώσεις.

Δεν είναι γνωστό αν το Signal θα επιτρέψει ποτέ την ύπαρξη λογαριασμών χωρίς να συνδέονται με αριθμό τηλεφώνου ή κάποιο άλλο παρόμοιο αναγνωριστικό στοιχείο. Έχει αναφερθεί ως κάτι που δεν θα κάνουν ποτέ, ή ως κάτι το οποίο επεξεργάζονται αλλά παραμένει στον αέρα.[27] Όπως και να έχει, είναι ένα σημαντικό πρόβλημα για πολλές περιπτώσεις χρήσης από κόσμο της αναρχίας.

Σκληρό PETting

(στμ: στα αγγλικά petting σημαίνει χάιδεμα)

Έχοντας συζητήσει εκτενώς το Signal, είναι ώρα να παρουσιάσουμε κάποιες εναλλακτικές λύσεις που λύνουν ορισμένα από τα θέματα που έχει το Signal: Το Briar και το Cwtch.

Το Briar και το Cwtch έχουν σχεδιαστεί να είναι εξαιρετικά ανθεκτικά σε μεταδεδομένα και παρέχουν καλύτερες δυνατότητες ανωνυμίας. Είναι επίσης πιο ασφαλή, καθώς δεν διαθέτουν κεντρικό server ή ενιαίο σημείο αποτυχίας. Αλλά αυτά τα πλεονεκτήματα έχουν κόστος - η μεγαλύτερη ασφάλεια συνοδεύεται από κάποιες ιδιορρυθμίες στη χρηστικότητα, τις οποίες θα πρέπει να συνηθίσετε.

Υπενθύμιση, τόσο το Cwtch όσο και το Briar είναι εφαρμογές **PET** επειδή είναι:
• **P**eer-to-peer
• όπως το Signal, τα μηνύματα είναι end-to-end κρυπτογραφημένα (**E**ncrypted)
• οι ταυτότητες και οι δραστηριότητες των χρηστών είναι ανώνυμες με την αποστολή όλων των μηνυμάτων μέσω **T**or

Επειδή μοιράζονται μια βασική αρχιτεκτονική, έχουν κοινά χαρακτηριστικά και λογική.

Peer-to-Peer

Το Signal είναι μια κεντρικοποιημένη υπηρεσία επικοινωνίας, η οποία χρησιμοποιεί έναν server για να αναμεταδίδει και να μεταδίδει κάθε μήνυμα που στέλνετε. Τα προβλήματα με αυτό το μοντέλο έχουν συζητηθεί εκτενώς! Πιθανότατα έχετε βαρεθεί να ακούτε γι' αυτό μέχρι τώρα. Το P στο PET σημαίνει peer-to-peer. Σε ένα peer-to-peer μοντέλο ανταλλάσσετε μηνύματα απευθείας με τα φιλαράκια σας. Δεν υπάρχει κάποιος ενδιάμεσος κεντρικός server που να διοικείται από κάποιον τρίτο. Κάθε άμεση σύνδεση βασίζεται μόνο στην ευρύτερη υποδομή του διαδικτύου.

Θυμάστε το ταχυδρομείο Signal; Με ένα μοντέλο peer-to-peer, δεν χρησιμοποιείτε μια ταχυδρομική υπηρεσία για τη διαχείριση της αλληλογραφίας σας. Παραδίδετε εσείς οι ίδιοι

κάθε επιστολή απευθείας στο φιλαράκι σας. Το γράφετε, το σφραγίζετε σε ένα φάκελο (end-to-end κρυπτογράφηση), το βάζετε στην τσάντα σας και διασχίζετε με το ποδήλατο την πόλη, όπου και το παραδίδετε.

Η επικοινωνία peer-to-peer παρέχει μεγάλη αντίσταση στα μεταδεδομένα. Δεν υπάρχει κεντρικός server που να χειρίζεται κάθε μήνυμα στο οποίο μπορούν να εκτεθούν μεταδεδομένα. Είναι πιο δύσκολο για τους αντιπάλους μας να προσπαθήσουν να συλλέξουν μαζικά μεταδεδομένα σχετικά με τις επικοινωνίες παρά να παρακολουθήσουν την κίνηση που εισέρχεται και εξέρχεται από γνωστούς κεντρικούς server. Και δεν υπάρχει κάποιο ενιαίο σημείο αποτυχίας. Εφόσον υπάρχει μια διαδρομή μέσω του διαδικτύου για να συνδεθείτε εσείς και οι γνωστοί σας, τότε μπορείτε να συνομιλήσετε.

Συγχρονικότητα

Υπάρχει ένα σημαντικό πράγμα που πρέπει να σημειώσετε σχετικά με την επικοινωνία peer-to-peer: επειδή δεν υπάρχει κεντρικός server για την αποθήκευση και αναμετάδοση των μηνυμάτων, τόσο εσείς όσο και η συνομιλήτρια σας πρέπει να έχετε την εφαρμογή σε λειτουργία και σε απευθείας σύνδεση για να ανταλλάξετε μηνύματα. Εξαιτίας αυτού, αυτές οι εφαρμογές P2P τείνουν προς τη συγχρονισμένη επικοινωνία.

Τι γίνεται αν διασχίσετε με το ποδήλατο την πόλη για να παραδώσετε ένα γράμμα σε κάποιον και... δεν είναι σπίτι!; Αν θέλετε πραγματικά να είστε peer-to-peer θα πρέπει να παραδώσετε το γράμμα απευθείας στο φίλο σας. Δεν μπορείτε απλά να το αφήσετε γι' αυτόν (δεν υπάρχει πουθενά κάτι αρκετά ασφαλές!). Πρέπει να μπορείτε να φτάσετε απευθείας στο φίλο σας για να του παραδώσετε το μήνυμα - αυτή είναι η συγχρονισμένη πτυχή της επικοινωνίας peer-to-peer.

Οι τηλεφωνικές κλήσεις αποτελούν επίσης ένα καλό παράδειγμα συγχρονισμένης επικοινωνίας. Δεν μπορείτε να έχετε μια τηλεφωνική συνομιλία αν δεν είστε και οι δύο μαζί στο τηλέφωνο την ίδια στιγμή. Αλλά ποιος κάνει πραγματικά τηλεφωνήματα πια; Αυτές τις μέρες, είμαστε πολύ περισσότερο συνηθισμένοι σε ένα μείγμα συγχρονισμένων και ασύγχρονων μηνυμάτων, και οι κεντρικές υπηρεσίες επικοινωνίας όπως το Signal είναι εξαιρετικές για αυτό. Μερικές φορές εσείς και η φίλη σας είστε και οι δύο online και ανταλλάσσετε μηνύματα σε πραγματικό χρόνο, αλλά πιο συχνά υπάρχει μεγάλη καθυστέρηση μεταξύ των μηνυμάτων που πηγαινοέρχονται. Τουλάχιστον για κάποιους ανθρώπους... Κάποιοι αναγνώστες έχουν πιθανώς το τηλέφωνό τους ανοιχτό και σε απόσταση αναπνοής ανά πάσα στιγμή και απαντούν σε κάθε μήνυμα που λαμβάνουν αμέσως, όλες τις ώρες της ημέρας. Γι' αυτούς, όλη η επικοινωνία είναι και πρέπει να είναι συγχρονισμένη... ξέρετε ποιες είστε.

Η μετάβαση σε αποκλειστικά συγχρονισμένη γραπτή επικοινωνία μπορεί να είναι ένα πραγματικό σοκ στην αρχή. Ορισμένοι αναγνώστες μπορεί να θυμούνται πώς ήταν αυτό από τη χρήση του AIM, του ICQ ή του MSN Messenger (αν τα θυμάστε αυτά, πονάει η πλάτη σας). Πρέπει να έχετε επίγνωση του αν κάποιος είναι πραγματικά συνδεδεμένος ή όχι. Δεν μπορείτε να εκτοξεύσετε ένα σωρό μηνύματα αν είναι εκτός σύνδεσης, για να παραδοθούν αργότερα. Αν κάποιος από τους δύο σας δεν κρατάει απλώς την εφαρμογή σε λειτουργία και σε σύνδεση ανά πάσα στιγμή, μπορεί εσείς και ο φίλος σας να συνηθίσετε να ορίζετε ημερομηνίες και ώρες για να συνομιλήσετε. Αυτό μπορεί να είναι κάτι πολύ ωραίο. Παραδόξως, η κανονικοποίηση της ασύγχρονης επικοινωνίας έχει οδηγήσει σε μια προσδοκία να είστε online και να ανταποκρίνεστε ανά πάσα στιγμή. Η συγχρονισμένη επικοινωνία ενθαρρύνει μια προμελέτη στην επικοινωνία μας, περιορίζοντάς την σε στιγμές που είμαστε πραγματικά συνδεδεμένοι, αντί της προσδοκίας να είμαστε αυθόρμητα διαθέσιμοι λίγο πολύ όλη την ώρα.

Ένα άλλο σημαντικό επακόλουθο του συγχρονισμού των συνδέσεων peer-to-peer: μπορεί να κάνει τις ομαδικές συζητήσεις λίγο περίεργες. Τι γίνεται αν δεν είναι όλοι στην ομάδα συνδεδεμένοι την ίδια στιγμή; Το Briar και το Cwtch χειρίζονται αυτό το πρόβλημα με διαφορετικό τρόπο, γι' αυτό θα αναλυθεί στην αντίστοιχη ενότητα της κάθε εφαρμογής.

Tor

Παρόλο που η επικοινωνία peer-to-peer είναι πολύ ανθεκτική στα μεταδεδομένα και αποφεύγει άλλες παγίδες της χρήσης ενός κεντρικού server, από μόνη της δεν προστατεύει από τη συλλογή μεταδεδομένων και την ανάλυση της κίνησης "Big Data". Το Tor είναι μια πολύ καλή λύση για αυτό, και οι εφαρμογές P2P δρομολογούν όλη την κυκλοφορία μέσω του Tor.

Αν είστε στην αναρχία και διαβάζετε αυτό το κείμενο, θα πρέπει να είστε ήδη εξοικειωμένη με το Tor και το πώς μπορεί να αξιοποιηθεί για να παρέχει ανωνυμία (ή τη μη σύνδεση σας με κάτι).[28] Οι εφαρμογές P2P σχηματίζουν απευθείας συνδέσεις peer-to-peer για την ανταλλαγή μηνυμάτων μέσω του Tor. Αυτό καθιστά πολύ, πολύ πιο δύσκολο για οποιονδήποτε αντίπαλο, είτε αυτός που σας παρακολουθεί στοχευμένα είτε αυτός που προσπαθεί να παρατηρήσει και να συσχετίσει τη δραστηριότητα σε όλο το διαδίκτυο, να εντοπίσει ποιος μιλάει με ποιον ή να κάνει οποιουσδήποτε άλλους χρήσιμους προσδιορισμούς. Είναι πολύ πιο δύσκολο να συνδεθεί ένας συγκεκριμένος χρήστης μιας εφαρμογής P2P με μια πραγματική ταυτότητα. Το μόνο που μπορεί να δει οποιοσδήποτε παρατηρητής είναι ότι χρησιμοποιείτε το Tor.

Το Tor δεν είναι αλεξίσφαιρο, και είναι πιθανόν να προκύψουν προβλήματα με το Tor ή επιθέσεις στο δίκτυο Tor. Το να μιλήσουμε για τις λεπτομέρειες του τρόπου λειτουργίας του Tor θα καταλάμβανε πολύ χώρο εδώ, και υπάρχουν πολλές πηγές στο διαδίκτυο για να διαβάσετε κάτι παραπάνω.[29] Η κατανόηση των γενικών επιφυλάξεων για τη χρήση του Tor είναι επίσης σημαντική.[30] Όπως και το Signal, η κυκλοφορία του Tor μπορεί επίσης να διακοπεί από παρεμβολές στο επίπεδο της υποδομής του διαδικτύου ή από επιθέσεις άρνησης υπηρεσίας (DoS Attack) που στοχεύουν ολόκληρο το δίκτυο Tor.[31] Εξακολουθεί να είναι πολύ πιο δύσκολο για έναν αντίπαλο να μπλοκάρει ή να διαταράξει το Tor απ' ό,τι είναι να ρίξει ή να μπλοκάρει τον κεντρικό server του Signal.

Πρέπει να σημειωθεί ότι σε ορισμένες περιπτώσεις, η χρήση του Tor μπορεί να σας κάνει να ξεχωρίζετε. Αν είστε η μόνη που χρησιμοποιεί το Tor σε μια συγκεκριμένη περιοχή ή σε συγκεκριμένες ώρες, ξεχωρίζετε. Αλλά αυτό μπορεί να ισχύει για κάθε ασυνήθιστη εφαρμογή που χρησιμοποιείται. Το να έχετε το Signal στο τηλέφωνό σας επίσης σας κάνει να ξεχωρίζετε. Όσο περισσότεροι άνθρωποι χρησιμοποιούν το Tor τόσο το καλύτερο, και αν χρησιμοποιείται σωστά το Tor παρέχει καλύτερη προστασία από τις προσπάθειες αναγνώρισης των χρηστών παρά απο το να μην χρησιμοποιείται. Οι εφαρμογές PET χρησιμοποιούν το Tor για τα πάντα, από προεπιλογή, με τρόπο που παρέχει αρκετή ασφάλεια.

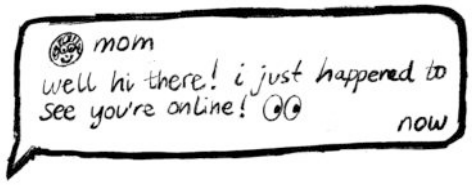
Ούτε τηλέφωνο, ούτε ζημιά

Μια εύκολη νίκη. Και οι δύο εφαρμογές PET που παρουσιάζονται εδώ δεν απαιτούν αριθμό τηλεφώνου για την εγγραφή λογαριασμού. Ο λογαριασμός σας δημιουργείται τοπικά στη συσκευή σας και το αναγνωριστικό στοιχείο του λογαριασμού είναι μια πολύ μεγάλη τυχαία σειρά χαρακτήρων που μοιράζεστε με τους φίλους σας για να γίνουν επαφές. Μπορείτε εύκολα να χρησιμοποιήσετε αυτές τις εφαρμογές απλά σε έναν υπολογιστή, σε ένα τηλέφωνο χωρίς κάρτα sim ή σε ένα τηλέφωνο, αλλά χωρίς απευθείας σύνδεση με τον αριθμό τηλεφώνου σας.

Γενικές επιφυλάξεις για τις εφαρμογές PET
Η κατάσταση διαρροών

Η επικοινωνία Peer-to-peer διαρρέει αναπόφευκτα κάποια μεταδεδομένα: την κατάσταση online/offline ενός συγκεκριμένου χρήστη. Οποιοδήποτε έχετε προσθέσει ως επαφή ή στον οποίο έχετε εμπιστευτεί το user id (αναγνωριστικό χρήστη) σας (ή οποιοσδήποτε αντίπαλος που έχει καταφέρει να το αποκτήσει) μπορεί να καταλάβει αν είστε συνδεδεμένος ή μη συνδεδεμένος ανά πάσα στιγμή. Αυτό δεν είναι κάποιου είδους σοβαρή απειλή, εκτός αν είστε ιδιαίτερα απρόσεκτοι με το ποιον προσθέτετε ως επαφή, ή για δημόσια πρότζεκτ

που δημοσιεύουν το user id τους. Αξίζει όμως να σημειωθεί επειδή μερικές φορές δεν θέλετε να ξέρει κάποιο άτομο που αποφεύγετε ότι είστε συνδεδεμένοι!



Ένας λογαριασμός μία συσκευή

Όταν ανοίγετε αυτές τις εφαρμογές για πρώτη φορά, δημιουργείτε έναν κωδικό πρόσβασης που χρησιμοποιείται για την κρυπτογράφηση του προφίλ χρήστη, των επαφών και του ιστορικού μηνυμάτων σας (αν επιλέξετε να το αποθηκεύσετε). Τα δεδομένα αυτά παραμένουν κρυπτογραφημένα στη συσκευή σας όταν δεν χρησιμοποιείτε την εφαρμογή.

Επειδή δεν υπάρχει κεντρικός server, δεν μπορείτε να συγχρονίσετε το λογαριασμό σας σε πολλές συσκευές. Μπορείτε να μεταφέρετε χειροκίνητα το λογαριασμό σας από τη μία συσκευή στην άλλη, όπως από ένα παλιό τηλέφωνο σε ένα νέο τηλέφωνο, αλλά δεν υπάρχει μαγικός συγχρονισμός στο cloud. Η ύπαρξη ξεχωριστού λογαριασμού σε κάθε συσκευή είναι μια εύκολη λύση που ενθαρρύνει οργανωτικούς διαχωρισμούς. Το να μην χρειάζεται να ανησυχείτε για μια συγχρονισμένη έκδοση σε έναν κεντρικό server (ακόμη και αν είναι κρυπτογραφημένη) ή σε μια άλλη συσκευή είναι επίσης ένα πλεονέκτημα. Επιβάλλει μια πιο σκόπιμη εξέταση του πού βρίσκονται τα δεδομένα σας και πώς έχετε πρόσβαση σε αυτά, αντί να διατηρείτε απλώς τα πάντα στο cloud (δηλαδή στον υπολογιστή κάποιου άλλου). Επίσης, δεν υπάρχει αντίγραφο των δεδομένων του λογαριασμού σας που να είναι αποθηκευμένα σε server τρίτου, ο οποίος θα επαναφέρει τον λογαριασμό σας εάν ξεχάσετε τον κωδικό πρόσβασης ή χάσετε τη συσκευή σας. Αν χαθούν, χάθηκαν.

Υπενθυμίζουμε ότι οι μόνοι τρόποι για να τα παρακάμψετε όλα αυτά είναι είτε να εμπιστευτείτε έναν κεντρικό server με αντίγραφο των επαφών και του κοινωνικού σας δικτύου, είτε να βασιστείτε σε ένα άλλο κοινωνικό δίκτυο, όπως το Signal χρησιμοποιεί τη λίστα επαφών σας με τους τηλεφωνικούς αριθμούς. Δεν θα έπρεπε να εμπιστευόμαστε έναν κεντρικό server για την αποθήκευση αυτών των πληροφοριών (ακόμη και σε κρυπτογραφημένη μορφή), ούτε να χρησιμοποιούμε κάτι σαν τους αριθμούς τηλεφώνου. Η πιθανότητα να πρέπει να ξαναχτίσουμε το κοινωνικό μας δίκτυο από την αρχή είναι το κόστος της αποφυγής αυτών των ζητημάτων ασφαλείας και στην πραγματικότητα ενθαρρύνει μια πρακτική διατήρησης και επαναδημιουργίας αξιόπιστων συνδέσεων με τα συντρόφια μας.

Διάρκεια ζωής της μπαταρίας

Η λειτουργία peer-to-peer Tor συνδέσεων σημαίνει ότι αυτή η εφαρμογή πρέπει να είναι συνδεδεμένη και να λαμβάνει συνεχώς, σε περίπτωση που κάποια από τις φίλες σας σας στείλει μήνυμα. Αυτές οι εφαρμογές μπορεί να καταναλώνουν πολύ μπαταρία σε παλιότερα τηλέφωνα. Αυτό όμως γίνεται όλο και λιγότερο πρόβλημα, καθώς η χρήση της μπαταρίας βελτιώνεται γενικά και οι μπαταρίες των τηλεφώνων γίνονται καλύτερες.

Δεν είναι φιλικό προς το iOS

Καμία από αυτές τις εφαρμογές δεν τρέχει στο iOS της Apple, κυρίως λόγω του ότι το iOS είναι εχθρικό προς οποιαδήποτε εφαρμογή που δημιουργεί peer-to-peer Tor συνδέσεις. Αυτό είναι δύσκολο να αλλάξει στο μέλλον (αν και όχι αδύνατο).

Ο κήπος με τα PETs

Ήρθε η ώρα να γνωρίσετε αυτές τις εφαρμογές PET. Και οι δύο διαθέτουν εξαιρετικούς οδηγούς που παρέχουν λεπτομερείς πληροφορίες σχετικά με τον τρόπο χρήσης τους, αλλά εδώ είναι μια γρήγορη επισκόπηση του τρόπου λειτουργίας της καθεμιάς, των χαρακτηριστικών τους και της χρήσης τους.

Briar

Ιστοσελίδα Briar: https://briarproject.org
Εγχειρίδιο χρήσης Briar: https://briarproject.org/manual/

Background & vibe check

Το Briar αναπτύχθηκε από το Briar Project, το οποίο είναι μια συλλογικότητα προγραμματιστών, χάκερς και φανς του Ελεύθερου Λογισμικού, που εδρεύει κυρίως στην Ευρώπη. Εκτός από την αντίσταση στην επιτήρηση και τη λογοκρισία, το ευρύτερο όραμα του έργου είναι η δημιουργία υποδομών επικοινωνίας και εργαλείων που θα χρησιμοποιηθούν κατά τη διάρκεια μιας καταστροφής ή ενός μπλακ-άουτ στο διαδίκτυο. Προφανώς αυτό το όραμα ενδιαφέρει τον κόσμο της αναρχίας που βρίσκεται σε περιοχές όπου υπάρχει μεγάλη πιθανότητα μερικής ή ολικής διακοπής του διαδικτύου κατά τη διάρκεια μιας εξέγερσης ή γενικής κατάρρευσης των υποδομών (δηλαδή παντού). Εάν το διαδίκτυο είναι εκτός λειτουργίας, το Briar μπορεί να συγχρονίσει μηνύματα μέσω Wi-Fi ή Bluetooth. Το Briar επιτρέπει επίσης τον εύκολο διαμοιρασμό της ίδιας της εφαρμογής απευθείας με κάποια φίλη. Μπορεί ακόμη και να σχηματίσει ένα υποτυπώδες δίκτυο μεταξύ χρηστών, ώστε ορισμένα είδη μηνυμάτων να μεταπηδούν από χρήστη σε χρήστη.

Το Briar είναι ανοικτού κώδικα και ανέθεσε επίσης έναν ανεξάρτητο έλεγχο ασφαλείας το 2013.[32]
• Τη στιγμή που γράφονται αυτές οι γραμμές, το Briar είναι διαθέσιμο για Android και η τρέχουσα έκδοση είναι 1.4.9.
• Υπάρχει διαθέσιμη μια beta έκδοση desktop για Linux (τρέχουσα έκδοση 0.2.1.) αν και λείπουν πολλά χαρακτηριστικά.
• Έχουν προγραμματιστεί εκδόσεις σε desktop για Windows και macOS.

Χρησιμοποιώντας το Briar - Βασικό chat

Το βασικό chat λειτουργεί εξαιρετικά. Οι φίλοι πρέπει να προσθέσουν ο ένας τον άλλον για να μπορέσουν να συνδεθούν. Το Briar έχει μια ωραία μικρή διεπαφή για να το κάνετε αυτό προσωπικά, όπου σαρώνει ο ένας τους QR κωδικούς του άλλου. Αλλά αυτό μπορεί επίσης να γίνει από απόσταση με την ανταλλαγή user id (ως σύνδεσμος "briar://"), ή οποιοσδήποτε χρήστης μπορεί να «συστήσει» χρήστες μέσα στην εφαρμογή, επιτρέποντας σε δύο χρήστες να γίνουν επαφές μεταξύ τους μέσω κάποιου κοινού τους φίλου. Οι μικρές παραξενιές στον τρόπο με τον οποίο προσθέτετε επαφές μπορεί να σας φανούν άβολες, αλλά σκεφτείτε πώς αυτό το μοντέλο ενθαρρύνει καλύτερες και πιο σκόπιμες πρακτικές εμπιστοσύνης. Το Briar διαθέτει ακόμη και μια μικρή ένδειξη δίπλα σε κάθε όνομα χρήστη για να σας υπενθυμίζει πώς τους «γνωρίζετε» (αυτοπροσώπως, μέσω ανταλλαγής συνδέσμων ή μέσω μιας σύστασης).

Προς το παρόν, στις απευθείας συνομιλίες μπορείτε να στέλνετε αρχεία, να χρησιμοποιείτε emojis, να διαγράφετε μηνύματα και να ορίζετε τα μηνύματα να εξαφανίζονται αυτόματα μετά από επτά ημέρες. Αν η φίλης σας δεν είναι συνδεδεμένη, μπορείτε να της γράψετε ένα μήνυμα και αυτό θα σταλεί αυτόματα την επόμενη φορά που θα την δείτε συνδεδεμένη.

Ιδιωτικά γκρουπ

Τα ιδιωτικά γκρουπ του Briar είναι συνηθισμένες ομαδικές συνομιλίες. Μόνο ο δημιουργός του γρκουπ μπορεί να προσκαλέσει επιπλέον μέλη, οπότε τα Ιδιωτικά γκρουπ προορίζονται για συγκεκριμένο σκοπό. Τα Ιδιωτικά γκρουπ υποστηρίζουν τη δημιουργία νήματος (thread) (μπορείτε να απαντήσετε απευθείας σε ένα συγκεκριμένο μήνυμα, ακόμη και αν αυτό δεν είναι το πιο πρόσφατο μήνυμα σε μια συνομιλία), αλλά αυτό είναι σε κάπως ακατέργαστη μορφή. Δεν μπορείτε να στείλετε εικόνες σε μια ομαδική συνομιλία, ούτε να ενεργοποιήσετε την εξαφάνιση μηνυμάτων.

Επειδή οι ομαδικές συνομιλίες του Briar είναι πραγματικά χωρίς server, τα πράγματα μπορεί να είναι λίγο περίεργα όταν δεν είναι όλοι στην ομάδα συνδεδεμένοι την ίδια στιγμή. Θυμάστε τη συγχρονικότητα; Κάθε ομαδικό μήνυμα θα αποστέλλεται σε όλα τα μέλη μιας ομάδας που είναι συνδεδεμένα εκείνη τη στιγμή. Το Briar βασίζεται σε όλα τα μέλη μιας ομάδας για να αναμεταδίδει μηνύματα σε άλλα μέλη που είναι εκτός σύνδεσης. Αν χάσατε κάποια μηνύματα σε μια ομαδική συνομιλία, οποιοδήποτε από τα άλλα μέλη που έλαβαν αυτά τα μηνύματα μπορεί να σας τα μεταβιβάσει όταν είστε και οι δύο συνδεδεμένοι.

Φόρουμ

Το Briar διαθέτει επίσης ένα χαρακτηριστικό που ονομάζεται Φόρουμ. Τα φόρουμ λειτουργούν όπως τα ιδιωτικά γκρουπ, με τη διαφορά ότι κάθε μέλος μπορεί να προσκαλέσει περισσότερα μέλη.

Blog

Η λειτουργία του blog του Briar είναι κάπως ωραία; Κάθε χρήστης έχει εξ ορισμού ένα Blog

feed. Οι αναρτήσεις στο blog που γίνονται από τις επαφές σας εμφανίζονται στο δικό σας blog feed. Μπορείτε επίσης να σχολιάσετε μια ανάρτηση Blog ή να “αναδημοσιεύσετε” μια ανάρτηση Blog από μια επαφή, ώστε να κοινοποιηθεί σε όλες τις επαφές σας (με το δικό σας σχόλιο) - πρόκειται για ένα στοιχειώδες κοινωνικό δίκτυο που λειτουργεί μόνο στο Briar.

Αναγνώστης ροής RSS

Το Briar διαθέτει επίσης ενσωματωμένο πρόγραμμα ανάγνωσης ροής RSS, το οποίο αντλεί νέες δημοσιεύσεις από ειδησεογραφικές ιστοσελίδες μέσω του Tor. Αυτός μπορεί να είναι ένας πολύ καλός τρόπος για να διαβάσετε το νεότερο ανακοινωθέν από την αγαπημένη σας σκιώδη αναρχική ιστοσελίδα αντιπληροφόρησης (η οποία πιθανότατα παρέχει ροή rss, αν δεν το γνωρίζατε ήδη!). Οι νέες δημοσιεύσεις από τις ροές rss που έχετε προσθέσει εμφανίζονται στο Blog feed και μπορείτε να τις «αναδημοσιεύσετε» για να τις μοιραστείτε με όλες τις επαφές σας.

Δικτυώσου

Το Briar κάνει πολλά ωραία πράγματα για να μεταφέρει μηνύματα μεταξύ επαφών χωρίς κεντρικούς server. Παρόμοια με τον τρόπο με τον οποίο τα Ιδιωτικά γκρουπ συγχρονίζουν τα μηνύματα μεταξύ των μελών χωρίς σέρβερ, τα φόρουμ και τα blogs αναμεταδίδονται από επαφή σε επαφή. Όλες οι επαφές σας μπορούν να λάβουν ένα αντίγραφο μιας ανάρτησης ενός blog ή φόρουμ, ακόμη και αν δεν είστε ποτέ συνδεδεμένοι την ίδια στιγμή - οι κοινές επαφές μεταδίδουν το μήνυμα για εσάς. Το Briar δεν δημιουργεί κάποιο πλέγμα δικτύωσης, όπου τα μηνύματα διαβιβάζονται μέσω οποιουδήποτε άλλου χρήστη του Briar (κάτι που θα μπορούσε να δώσει την ευκαιρία σε έναν αντίπαλο να χρησιμοποιεί πολλούς κακόβουλους λογαριασμούς Briar και να συλλέξει μεταδεδομένα). Το Briar δεν εμπιστεύεται κανένα από τα μηνύματά σας σε χρήστες για τους οποίους δεν προορίζονται. Αντιθέτως, κάθε χρήστης που υποτίθεται ότι πρέπει να λάβει ένα μήνυμα συμμετέχει επίσης στη μετάδοση του μηνύματος αυτού σε άλλους που επίσης πρέπει να το λάβουν, και μόνο με τις δικές του επαφές.

Αυτό μπορεί να είναι ιδιαίτερα χρήσιμο για τη δημιουργία ενός αξιόπιστου δικτύου επικοινωνίας που λειτουργεί ακόμη και αν το διαδίκτυο δεν λειτουργεί. Οι χρήστες του Briar μπορούν να συγχρονίσουν μηνύματα μέσω Wi-Fi ή Bluetooth. Θα μπορούσατε να περπατήσετε μέχρι την τοπική κατάληψη ή στέκι, να δείτε μερικές φίλες και να συγχρονίσετε μια σειρά από μηνύματα σε blog και φόρουμ. Στη συνέχεια, επιστρέφετε στο σπίτι και οι συγκάτοικοί σας μπορούν να συγχρονιστούν μαζί σας για να λαμβάνουν τις ίδιες ενημερώσεις από όλες τις κοινές επαφές σας.

Επιφυλάξεις για το Briar

Κάθε εφαρμογή υποστηρίζει μόνο έναν λογαριασμό. Επομένως, δεν μπορείτε να έχετε πολλούς λογαριασμούς στην ίδια συσκευή. Αυτό δεν αποτελεί πρόβλημα αν χρησιμοποιείτε το Briar μόνο για να μιλάτε με μια στενή ομάδα φίλων, αλλά δυσκολεύει τη χρήση του Briar για διαφορετικά πρότζεκτ ή δίκτυα που θα θέλατε να κατατμήσετε αλλιώς. Το Briar παρέχει διάφορες σχετικές με την ασφάλεια αιτιολογίσεις, και μια απλή είναι η εξής: αν η

ίδια συσκευή χρησιμοποιεί πολλαπλούς λογαριασμούς, θα μπορούσε θεωρητικά να είναι ευκολότερο για έναν αντίπαλο να προσδιορίσει ότι οι λογαριασμοί αυτοί συνδέονται, παρά τη χρήση του Tor. Εάν «ο επιστάτης» και «το φάντασμα» δεν εμφανίζονται ποτέ ταυτόχρονα στο διαδίκτυο, υπάρχει μεγάλη πιθανότητα να χρησιμοποιούν το ίδιο κινητό τηλέφωνο για τους επιμέρους λογαριασμούς τους στο Briar. Υπάρχουν και άλλοι λόγοι, αλλά και πιθανές λύσεις, αλλά προς το παρόν η ύπαρξη πολλαπλών προφίλ στην ίδια συσκευή δεν υποστηρίζεται.

Το πρωτόκολλο Briar απαιτεί επίσης από τους δύο χρήστες να προσθέσουν ο ένας τον άλλον ως επαφές ή να τους συστήσει ένας κοινός φίλος, προτού μπορέσουν να αλληλεπιδράσουν. Αυτό εμποδίζει τη δημοσίευση μιας διεύθυνσης Briar για να λαμβάνετε ανώνυμα εισερχόμενα μηνύματα, όπως για παράδειγμα αν θέλατε να δημοσιεύσετε το Briar user id για να λάβετε ειλικρινείς κριτικές σχετικά με ένα κείμενο που συγκρίνει διάφορες ασφαλείς εφαρμογές συνομιλίας.

Briar και ασυγχρονικότητα

Στους χρήστες αρέσει πολύ η ασύγχρονη επικοινωνία τους. Το Briar Project εργάζεται πάνω σε ένα Briar Mailbox, το οποίο είναι μια άλλη εφαρμογή που θα μπορούσε να τρέξει εύκολα σε ένα παλιό τηλέφωνο Android ή άλλο φτηνό μηχάνημα. Το Mailbox θα παραμένει ουσιαστικά online για να λαμβάνει μηνύματα για εσάς και στη συνέχεια θα συγχρονίζεται με την κύρια συσκευή σας μέσω Tor όταν είστε online. Αυτή είναι μια ενδιαφέρουσα ιδέα. Ένα ενιαίο γραμματοκιβώτιο Briar θα μπορούσε δυνητικά να χρησιμοποιηθεί από πολλούς χρήστες που εμπιστεύονται ο ένας τον άλλον, όπως συγκάτοικες σε ένα συλλογικό σπίτι, ή τακτικοί θαμώνες μιας κατάληψης/στεκίου. Αντί να βασίζεται σε έναν κεντρικό σέρβερ για τη διευκόλυνση της ασυγχρονικότητας, ένας μικρός και εύκολος στη ρύθμιση σέρβερ που ελέγχετε εσείς χρησιμοποιείται για την αποθήκευση των εισερχόμενων μηνυμάτων για εσάς και τις φίλες σας ενώ είστε εκτός σύνδεσης. Αυτό είναι ακόμη υπό ανάπτυξη, οπότε το πόσο ασφαλές θα είναι (π.χ. θα είναι επαρκώς ασφαλή τα αποθηκευμένα μηνύματα ή άλλα μεταδεδομένα εάν κάποιος αντίπαλος έχει πρόσβαση στο Mailbox;) δεν είναι γνωστό και θα πρέπει να αξιολογηθεί.

Cwtch

Ιστοσελίδα Cwtch: https://cwtch.im/
Εγχειρίδιο χρήσης Cwtch: https://docs.cwtch.im/

Background and vibe check

Το όνομα... κάνει ομοιοκαταληξία με το 'butch'. Είναι μια ουαλική λέξη που σημαίνει αγκαλιά που δημιουργεί ένα ασφαλές μέρος.

Το Cwtch αναπτύχθηκε από την Open Privacy Research Society, μια μη κερδοσκοπική εταιρεία που εδρεύει στο Βανκούβερ. Το vibe του Cwtch θα μπορούσε να περιγραφεί ως "queer Signal". Η Open Privacy επενδύει πολύ στη δημιουργία εργαλείων που «εξυπηρετούν περιθωριοποιημένες κοινότητες» να αντιστέκονται στην καταπίεση. Έχουν επίσης εργαστεί σε άλλα ωραία πρότζεκτ, όπως στην έρευνα για κάτι που ονομάζεται "Shatter Secrets" και έχει σχεδιαστεί για την προστασία μυστικών από σενάρια όπου τα άτομα μπορεί να εξαναγκαστούν να αποκαλύψουν έναν κωδικό πρόσβασης (όπως σε μια διέλευση συνόρων).

Το Cwtch είναι επίσης ανοικτού κώδικα και το πρωτόκολλό του βασίζεται εν μέρει στο προηγούμενο έργο PET Ricochet. Το Cwtch είναι νεότερο έργο από το Briar, αλλά η ανάπτυξή του έχει προχωρήσει γρήγορα και νέες εκδόσεις κυκλοφορούν συχνά.

* Τη στιγμή που γράφονται αυτές οι γραμμές, η τρέχουσα έκδοση είναι η 1.8.0.
* Το Cwtch είναι διαθέσιμο για Android, Windows, Linux και macOS.

Χρησιμοποιώντας το Cwtch

Όταν ανοίγετε για πρώτη φορά το Cwtch, δημιουργείτε το πρώτο σας προφίλ, το οποίο προστατεύεται με έναν κωδικό πρόσβασης. Το νέο σας προφίλ αποκτά ένα χαριτωμένο μικρό avatar και μια διεύθυνση Cwtch. Σε αντίθεση με το Briar, το Cwtch υποστηρίζει πολλαπλά προφίλ στην ίδια συσκευή και μπορείτε να έχετε πολλαπλά προφίλ ξεκλειδωμένα ταυτόχρονα. Αυτό είναι ιδανικό αν θέλετε να έχετε κατανεμημένες ταυτότητες για διαφορετικά πρότζεκτ ή δίκτυα χωρίς να χρησιμοποιείτε πολλαπλές συσκευές (αλλά προσέξτε τα πιθανά θέματα ασφάλειας που μπορεί να έχει αυτό!).

Για να προσθέσετε μια φίλη, απλώς δώστε της τη διεύθυνση Cwtch σας. Εσείς και ο φίλος σας δεν χρειάζεται να ανταλλάξετε πρώτα διευθύνσεις για να συνομιλήσετε. Αυτό σημαίνει ότι με το Cwtch μπορείτε να δημοσιεύσετε δημόσια μια διεύθυνση Cwtch και οι φίλες και οι κριτικοί να επικοινωνούν μαζί σας ανώνυμα. Μπορείτε επίσης να ρυθμίσετε το Cwtch να μπλοκάρει αυτόματα τα εισερχόμενα μηνύματα από αγνώστους.

Εδώ είναι μια διεύθυνση Cwtch για να επικοινωνήσετε με τον συγγραφέα αυτού του κειμένου με σχόλια ή μηνύματα μίσους [στμ: Η διεύθυνση είναι του συγγραφέα του κειμένου και όχι του μεταφραστή]: g6px2uyn5tdg2gxpqqktnv7qi2i5frr5kf2dgnyielvq4o4emry4qzid

Στην άμεση συνομιλία, το Cwtch διαθέτει κάποιες ωραίες επιλογές διαμόρφωσης κειμένου, emojis και απαντήσεων. Κάθε συνομιλία μπορεί να ρυθμιστεί για «αποθήκευση ιστορικού» ή «διαγραφή ιστορικού» όταν κλείνει το Cwtch.

Αυτά είναι τα βασικά χαρακτηριστικά και λειτουργούν εξαιρετικά. Προς το παρόν, όλα τα άλλα χαρακτηριστικά του Cwtch είναι «πειραματικά» και μπορείτε να τα επιλέξετε στις ρυθμίσεις. Αυτό περιλαμβάνει ομαδικές συνομιλίες, κοινή χρήση αρχείων, αποστολή φωτογραφιών, εικόνες προφίλ, προεπισκόπηση εικόνων και συνδέσμους με δυνατότητα κλικ με προεπισκόπηση συνδέσμων. Η ανάπτυξη του Cwtch προχωράει αρκετά γρήγορα, οπότε μέχρι τη στιγμή που θα διαβάζετε αυτό το κείμενο, όλα αυτά τα χαρακτηριστικά μπορεί να έχουν αναπτυχθεί πλήρως και να είναι διαθέσιμα.

Ομαδικές συνομιλίες

Το Cwtch προσφέρει επίσης ομαδικές συνομιλίες ως «πειραματικό χαρακτηριστικό». Το Cwtch χρησιμοποιεί επί του παρόντος servers που διαχειρίζονται οι χρήστες για να διευκολύνει τις ομαδικές συνομιλίες, κάτι που διαφέρει πολύ από την προσέγγιση της Briar. Το Open Privacy θεωρεί ότι οι ομαδικές συνομιλίες που είναι ανθεκτικές στα μεταδεδομένα είναι ένα υπάρχον πρόβλημα και ανοιχτό ερώτημα, και ελπίζω ότι διαβάζοντας μέχρι εδώ μπορείτε να καταλάβετε γιατί. Παρόμοια με τον τρόπο λειτουργίας του Signal Server, οι servers του Cwtch είναι σχεδιασμένοι έτσι ώστε οι servers να θεωρούνται πάντα «αναξιόπιστοι» και να μαθαίνουν όσο το δυνατόν λιγότερα για τα περιεχόμενα των μηνυμάτων ή τα μεταδεδομένα. Αλλά φυσικά αυτοί οι servers λειτουργούν από μεμονωμένους χρήστες και όχι από ένα κεντρικό τρίτο σώμα.

Οποιοσδήποτε μεμονωμένος χρήστης του Cwtch μπορεί να γίνει “server” για μια ομαδική συνομιλία. Αυτό είναι εξαιρετικό για ομαδικές συνομιλίες μιας χρήσης, όπου ένας χρήστης μπορεί να γίνει ο «οικοδεσπότης» για μια συνάντηση ή μια γρήγορη συζήτηση. Οι servers ομαδικής συνομιλίας του Cwtch επιτρέπουν επίσης την ασύγχρονη παράδοση μηνυμάτων, έτσι ώστε μια ομάδα ή κοινότητα να μπορεί να λειτουργεί συνεχώς τον δικό της server ως υπηρεσία προς τα μέλη της.

Ο τρόπος με τον οποίο το Cwtch προσεγγίζει τις ομαδικές συνομιλίες είναι ακόμα υπό ανάπτυξη και μπορεί να αλλάξει στο μέλλον, αλλά αυτή τη στιγμή είναι μια πολύ ελπιδοφόρα και ωραία λύση.

Cwtch και ασυγχρονικότητα

Οι ομαδικές συνομιλίες στο Cwtch επιτρέπουν την ασύγχρονη ανταλλαγή μηνυμάτων (εφόσον ο server/host είναι συνδεδεμένος), αλλά όπως και στο Briar, το Cwtch απαιτεί και οι δύο επαφές να είναι συνδεδεμένες για την αποστολή άμεσων μηνυμάτων. Σε αντίθεση με το Briar, το Cwtch δεν σας επιτρέπει να βάλετε μηνύματα σε αναομονή για να τα στείλετε σε μια επαφή όταν αυτή συνδεθεί.

Προειδοποίηση για κρυπτονόμισμα στο Cwtch

Στα τέλη του 2019, η Open Privacy, η οποία αναπτύσσει το Cwtch, έλαβε μια δωρεά 40.000 δολαρίων από το ίδρυμα Zcash. Το Zcash είναι ένα άλλο κρυπτονόμισμα με επίκεντρο την ιδιωτικότητα, παρόμοιο αλλά σαφώς κατώτερο από το Monero.[33] Το 2019, το Cwtch βρισκόταν σε πολύ πρώιμο στάδιο ανάπτυξης και το Open Privacy έκανε κάποια διερευνητικά πειράματα γύρω από τη χρήση του Zcash ή παρόμοιων κρυπτονομισμάτων blockchain ως δημιουργικές λύσεις σε διάφορες κρυπτογραφικές προκλήσεις, με την ιδέα ότι θα μπορούσε να ενσωματωθεί στο Cwtch κάποια στιγμή.[34] Έκτοτε, καμία περαιτέρω εργασία με το Zcash ή άλλα κρυπτονομίσματα δεν έχει συσχετιστεί με το Cwtch και φαίνεται ότι δεν αποτελεί προτεραιότητα ή τομέα έρευνας για το Open Privacy. Πρέπει όμως να αναφερθεί ως ένα πιθανό πρόβλημα για τους ανθρώπους που είναι ιδιαίτερα επιφυλακτικοί με τα συστήματα κρυπτονομισμάτων. Υπενθυμίζουμε ότι το Signal διαθέτει ήδη ένα πλήρως λειτουργικό κρυπτονόμισμα ενσωματωμένο μέσα στην εφαρμογή που επιτρέπει στους χρήστες να στέλνουν και να λαμβάνουν MobileCoin.

Συμπεράσματα «...αποχώρησε από την ομαδική»

Πολλές αναγνώστριες μπορεί να λένε στον εαυτό τους «Οι εφαρμογές PET δεν φαίνεται να υποστηρίζουν πολύ καλά τις ομαδικές συνομιλίες... και λατρεύω τις ομαδικές συνομιλίες!» Πρώτον, ποιος αγαπά πραγματικά τις ομαδικές συνομιλίες; Δεύτερον, αξίζει να αναφερθούμε στις κριτικές για το πώς τα αναρχικά καταλήγουν να χρησιμοποιούν τις ομαδικές συνομιλίες στο Signal έτσι ώστε να γίνει κατανοητό ότι ο τρόπος με τον οποίο υλοποιούνται στο Briar και το Cwtch δεν αποτελεί εμπόδιο.

Το Signal, το Cwtch και το Briar σας επιτρέπουν να έχετε εύκολα μια ομαδική συνομιλία σε πραγματικό χρόνο (συγχρονισμένη!) για μια συνάντηση ή μια γρήγορη συλλογική συζήτηση, η οποία δεν θα μπορούσε να γίνει αυτοπροσώπως. Αλλά όταν οι άνθρωποι αναφέρονται σε μια «ομαδική συνομιλία» (ειδικά στο πλαίσιο του Signal) δεν εννοούν συνήθως αυτό. Οι ομαδικές συνομιλίες του Signal συχνά μετατρέπονται σε τεράστιες, μακροσκελής ροές ημι-δημόσιων ενημερώσεων, shit-posts, συνδέσμων κ.λπ., που στην πράξη μοιάζουν περισσότερο με τα μέσα κοινωνικής δικτύωσης. Υπάρχουν περισσότερα μέλη από όσα θα μπορούσαν ρεαλιστικά να έχουν μια λειτουργική συζήτηση, πόσο μάλλον να λαμβάνουν αποφάσεις. Η μείωση της χρησιμότητας και της ασφάλειας με την αύξηση του μεγέθους, της εμβέλειας και της επιμονής των ομάδων του Signal συζητήθηκε καλά στο εξαιρετικό άρθρο “Signal Fails”.[35] Όσο περισσότερο απομακρύνεται μια ομαδική συνομιλία από το μικρό, βραχυπρόθεσμο, μονοσήμαντο σκοπό, τόσο πιο δύσκολο είναι να υλοποιηθεί με το Briar και το Cwtch - και αυτό δεν είναι κακό. Αν μη τι άλλο, το Briar και το Cwtch προάγουν πιο υγιείς και ασφαλείς συνήθειες, στερούμενα τα «χαρακτηριστικά» του Signal που διευκολύνουν τη δυναμική της ομαδικής συνομιλίας που επικρίνεται σε κείμενα όπως το “Signal Fails”.

Πρόταση

Το Briar και το Cwtch είναι και τα δύο νέα έργα. Ορισμένες αναρχικές έχουν ήδη ακούσει γι’ αυτά και προσπαθούν να χρησιμοποιήσουν το ένα ή το άλλο για συγκεκριμένα πρότζεκτ ή περιπτώσεις χρήσης. Οι τρέχουσες εκδόσεις μπορεί να φαίνονται πιο δύσχρηστες από το Signal και να υποφέρουν από το φαινόμενο του δικτύου[στμ: ονομάζεται εκείνο το χαρακτηριστικό γνώρισμα κατά το οποίο η αξία ενός αγαθού ή υπηρεσίας εξαρτάτε από τον αριθμό των ατόμων που κατέχουν το συγκεκριμένο αγαθό ή χρησιμοποιούν τη συγκεκριμένη υπηρεσία] - όλες είναι στο Signal, οπότε κανείς δεν θέλει να χρησιμοποιεί κάτι άλλο.[36] Αξίζει να επισημανθεί ότι τα προφανή εμπόδια για τη χρήση του Cwtch και του Briar αυτή τη στιγμή (ακόμα σε beta έκδοση, φαινόμενο του δικτύου, διαφορετικά από αυτά που έχετε συνηθίσει, δεν υπάρχει έκδοση iOS) είναι όλα ακριβώς τα ίδια εμπόδια που αποθάρρυναν τους ανθρώπους νωρίτερα για τη χρήση του Signal (ή αλλιώς TextSecure!).

Είναι δύσκολο το να κάνεις ανθρώπους να μάθουν και να αρχίσουν να χρησιμοποιούν οποιοδήποτε νέο εργαλείο. Ειδικά όταν το τρέχον εργαλείο που έχουν συνηθίσει φαίνεται να λειτουργεί μια χαρά! Δεν υπάρχει αμφιβολία για την πρόκληση. Αυτός ο οδηγός κατέληξε να είναι τόσες πολλές σελίδες σε μια προσπάθεια να προβάλει ένα πειστικό επιχείρημα ότι ο κόσμος της αναρχίας, ο οποίος ενδεχομένως ενδιαφέρεται περισσότερο για αυτά τα ζητήματα, θα πρέπει να δοκιμάσει να χρησιμοποιήσει αυτές τις εφαρμογές PET.

Οι αναρχικοί έχουν στο παρελθόν επιτύχει να υιοθετήσουν νέα ηλεκτρονικά εργαλεία που ήταν πρόκληση, να τα διαδώσουν και να τα χρησιμοποιήσουν αποτελεσματικά κατά τη διάρκεια πράξεων αγώνα και αντίστασης. Η κανονικοποίηση της χρήσης των εφαρμογών PET επιπλέον ή αντί του Signal για την ηλεκτρονική επικοινωνία θα ενισχύσει την ανθεκτικότητα των κοινοτήτων μας και εκείνων που

μπορούμε να πείσουμε να χρησιμοποιήσουν αυτά τα εργαλεία. Θα μας βοηθήσουν να προστατευτούμε από την ολοένα και πιο ισχυρή συλλογή και ανάλυση μεταδεδομένων, θα μας προστατεύσουν από την εξάρτηση σε κεντρικοποιημένες υπηρεσίες και θα παρέχουν ευκολότερη πρόσβαση στην ανωνυμία.

Οπότε αυτή είναι η πρόταση. Αφού διαβάσετε αυτόν τον οδηγό, εφαρμόστε τον και μοιραστείτε τον. Δεν μπορείτε να δοκιμάσετε το Cwtch ή το Briar μόνες σας, χρειάζεστε τουλάχιστον έναν φίλο για να τα δοκιμάσετε μαζί του. Εγκαταστήστε τα μαζί με την ομάδα σας και δοκιμάστε να χρησιμοποιήσετε το ένα ή το άλλο για ένα συγκεκριμένο πρότζεκτ που σας ταιριάζει. Κάντε μια εβδομαδιαία συνάντηση με ανθρώπους που δεν μπορούν να συναντηθούν από κοντά για να συζητήσουν τα νέα που διαφορετικά μοιράζονταν σε μια εκτεταμένη συνομιλία ομάδας Signal. Κρατήστε επαφή με μερικές φίλες που βρίσκονται μακριά ή με μια ομάδα που έχει χωριστεί λόγω απόστασης. Δεν χρειάζεται (και μάλλον δεν θα έπρεπε) να διαγράψετε το Signal, αλλά τουλάχιστον θα βοηθήσετε στην οικοδόμηση ανθεκτικότητας δημιουργώντας εναλλακτικές συνδέσεις με τα δίκτυά σας. Καθώς τα πράγματα κλιμακώνονται, η πιθανότητα της έντονης καταστολής ή των κοινωνικών ρηγμάτων που διακόπτουν το Signal σε άλλες χώρες γίνεται όλο και πιο πιθανή παντού, και θα μας εξυπηρετήσει να έχουμε τις εναλλακτικές μας επικοινωνίες σε λειτουργία μάλλον νωρίτερα παρά αργότερα!

Το Briar και το Cwtch είναι και τα δύο υπό ενεργή ανάπτυξη, από αναρχικές και ανθρώπους που συμφωνούν με τους στόχους μας. Χρησιμοποιώντας τα, είτε σοβαρά είτε για διασκέδαση, μπορούμε να συμβάλουμε στην ανάπτυξή τους, αναφέροντας σφάλματα και θέματα, και να εμπνεύσουμε τους προγραμματιστές τους να συνεχίσουν, γνωρίζοντας ότι το έργο τους χρησιμοποιείται. Ίσως ακόμη και κάποιοι από εμάς που είμαστε πιο εξοικειωμένοι με τους υπολογιστές να μπορούμε να συνεισφέρουμε άμεσα, ελέγχοντας τον κώδικα και τα πρωτόκολλά τους ή ακόμη και συμμετέχοντας στην ανάπτυξή τους.

Εκτός από την ανάγνωση αυτού του οδηγού, η πραγματική προσπάθεια χρήσης αυτών των εφαρμογών ως μια ομάδα χρηστών με περιέργεια είναι ο καλύτερος τρόπος για να εκτιμήσετε πώς διαφέρουν δομικά από το Signal. Ακόμη και αν δεν μπορείτε να πείσετε τον εαυτό σας να χρησιμοποιεί αυτές τις εφαρμογές τακτικά, το να δοκιμάζετε διαφορετικά ασφαλή εργαλεία επικοινωνίας και να *κατανοείτε* πώς και γιατί διαφέρουν από αυτά που γνωρίζετε, θα βελτιώσει την ψηφιακή σας παιδεία σε θέματα ασφάλειας. Δεν χρειάζεται να κατακτήσετε τα απαιτητικά μαθηματικά που διέπουν το πρωτόκολλο κρυπτογράφησης του Signal, αλλά η καλύτερη γνώση και κατανόηση του τρόπου με τον οποίο λειτουργούν αυτά τα εργαλεία στη θεωρία και στην πράξη οδηγεί σε καλύτερη λειτουργική ασφάλεια συνολικά. Όσο βασιζόμαστε σε υποδομές για να επικοινωνούμε, θα πρέπει να προσπαθούμε να κατανοούμε πώς λειτουργεί αυτή η υποδομή, πώς μας προστατεύει ή μας καθιστά ευάλωτους και να ψάχνουμε ενεργά τρόπους για την ενίσχυσή της.

Επίλογος

Όλη αυτή η συζήτηση αφορούσε τις εφαρμογές συνομιλίας ασφαλούς επικοινωνίας που τρέχουν στα τηλέφωνα και τους υπολογιστές μας. Κλείνουμε με μια υπενθύμιση ότι όσο κι αν η χρήση εργαλείων που κρυπτογραφούν και ανωνυμοποιούν τις διαδικτυακές επικοινωνίες μπορεί να σας προστατεύσει από τους αντιπάλους μας, δεν πρέπει ποτέ να πληκτρολογείτε ή να λέτε οτιδήποτε σε οποιαδήποτε εφαρμογή ή συσκευή χωρίς να υπολογίζεται ότι μπορεί να διαβαστεί πίσω σε εσάς στο δικαστήριο. Η συνάντηση με τους φίλους σας, πρόσωπο με πρόσωπο, σε εξωτερικούς χώρους και μακριά από κάμερες και άλλα ηλεκτρονικά μέσα είναι μακράν ο ασφαλέστερος τρόπος για να κάνετε οποιαδήποτε συζήτηση που πρέπει να είναι ασφαλής και ιδιωτική. Κλείστε το τηλέφωνό σας, αφήστε το κάτω και βγείτε έξω!

Παράρτημα: μερικές άλλες εφαρμογές που μπορεί να έχετε ακούσει

Ricochet Refresh
https://www.ricochetrefresh.net/

Το Ricochet ήταν μια πολύ πρώιμη εφαρμογή PET για σταθερούς υπολογιστές που χρηματοδοτήθηκε από το Blueprint for Free Speech με έδρα την Ευρώπη. Το Ricochet Refresh είναι η τρέχουσα έκδοση. Βασικά μοιάζει πολύ με το Cwtch και το Briar, αλλά είναι αρκετά υποτυπώδες - διαθέτει βασική άμεση συνομιλία και μεταφορά αρχείων και τρέχει μόνο σε MacOS, Linux και Windows. Είναι λειτουργικό, αλλά γυμνό, και δεν διαθέτει εφαρμογές για κινητά.

OnionShare
https://onionshare.org

Το OnionShare είναι ένα φανταστικό έργο που τρέχει σε οποιονδήποτε desktop υπολογιστή και υπάρχει σε πακέτο στο Tails και άλλα λειτουργικά συστήματα. Σας διευκολύνει να στέλνετε και να λαμβάνετε αρχεία ή να έχετε ένα υποτυπώδες εφήμερο δωμάτιο συνομιλίας μέσω του Tor. Είναι επίσης PET!

Telegram
Το Telegram είναι ουσιαστικά Twitter. Το να έχετε παρουσία εκεί μπορεί να είναι χρήσιμο σε ορισμένα σενάρια, αλλά δεν πρέπει να χρησιμοποιείται για ασφαλείς επικοινωνίες και διαρρέει μεταδεδομένα παντού. Το να αφιερώσουμε περισσότερο χρόνο στην κριτική του Telegram μάλλον δεν είναι χρήσιμο εδώ, αλλά δεν θα πρέπει να χρησιμοποιείται όπου είναι επιθυμητή η ιδιωτικότητα ή η ασφάλεια.[38]

Tox
https://tox.chat

Το Tox είναι παρόμοιο πρόγραμμα με το Briar και το Cwtch, αλλά δεν χρησιμοποιεί το Tor - είναι απλά το PE. Το Tox θα μπορούσε να δρομολογηθεί μέσω του Tor χειροκίνητα. Καμία από τις εφαρμογές που αναπτύχθηκαν για το Tox δεν είναι ιδιαίτερα φιλική προς το χρήστη.

Session
https://getsession.org

Το Session αξίζει να εξεταστεί εκτενώς. Το vibe είναι πολύ ελευθεριακό και ακτιβιστικό. Το Session χρησιμοποιεί το ισχυρό πρωτόκολλο κρυπτογράφησης του Signal, είναι peer-to-peer για απευθείας μηνύματα και χρησιμοποιεί επίσης δρομολόγηση Onion για ανωνυμία (η ίδια ιδέα πίσω από το Tor). Ωστόσο, αντί για το Tor, το Session χρησιμοποιεί το δικό του δίκτυο δρομολόγησης Onion, όπου απαιτείται ένα «οικονομικό μερίδιο» για τη λειτουργία ενός κόμβου υπηρεσίας για τη δημιουργία του δικτύου Onion. Το σημαντικότερο είναι ότι αυτό το οικονομικό μερίδιο έχει τη μορφή κρυπτονομίσματος που διαχειρίζεται το ίδρυμα που αναπτύσσει το Session. Το έργο είναι ενδιαφέρον από τεχνολογικής άποψης, έξυπνο μάλιστα, αλλά είναι μια πολύ "web3" λύση βυθισμένη στην κρυπτοκουλτούρα. Παρ' όλη τη στάση τους, οι ομαδικές συνομιλίες τους δεν είναι κατασκευασμένες ώστε να είναι τρομερά ανθεκτικές στα μεταδεδομένα, και οι μεγάλες ημι-δημόσιες ομαδικές συνομιλίες απλά φιλοξενούνται σε κεντρικούς servers (και προφανώς κατακλύζονται από δεξιούς οπαδούς των crypto). Ίσως αν το blockchain επικρατήσει στο τέλος, αυτό να είναι μια καλή επιλογή, αλλά αυτή τη στιγμή δεν μπορούμε να το συστήσουμε.

Molly
https://molly.im

Το Molly είναι μια παραλλαγμένη έκδοση client του Signal για Android. Εξακολουθεί να χρησιμοποιεί τον server Signal, αλλά παρέχει λίγη επιπλέον ασφάλεια και δυνατότητες στη συσκευή.

Σημειώσεις και πηγές

[1] https://itsgoingdown.org/signal-warning-why-moxies-departure-is-not-the-end-of-signal/
[2] Με τον ένα ή τον άλλο τρόπο
[3] https://pugetsoundanarchists.org/snitches-sleuths-an-update-from-puget-sound-prisoner-support/
[4] Δείτε την honeypot κρυπτογραφημένη εφαρμογή συνομιλίας Anom του FBI για ένα πραγματικό παράδειγμα αυτού www.vice.com/en/article/akgkwj/operation-trojan-shield-anom-fbi-secret-phone-network
[5] https://www.opentech.fund/results/supported-projects/open-whisper-systems/
[6] http://www.wsj.com/articles/moxie-marlinspike-the-coder-who-encrypted-your-texts-1436486274
[7] https://www.rt.com/op-ed/513732-signal-messenger-us-national-security/
[8] https://www.theverge.com/2013/7/17/4517480/nsa-spying-prism-surveillance-cheat-sheet
[9] https://www.politico.com/news/2022/06/29/canada-national-police-spyware-phones-00043092
[10] https://tails.boum.org/sponsors/index.en.html
[11] Παρόλο που το Signal φαίνεται να θέλει περισσότερες δωρεές από τους χρήστες, παρά το γεγονός ότι απολαμβανει ένα δάνειο ύψους 50 εκατομμυρίων δολαρίων. (στμ: στο πρωτότυπο παρατίθεται παλιό emoji με ανθρωπάκι που σπκώνει τα χέρια ψηλά)
[12] Αντί για έναν μεμονωμένο ενιαίο server, πρόκειται στην πραγματικότητα για ένα τεράστιο δίκτυο από cloud servers που νοικιάζονται σε κέντρα δεδομένων της Amazon σε όλες τις ΗΠΑ - αυτό μπορεί να εκφραστεί αφηρημένα σε έναν μοναδικό Signal Server για τους σκοπούς της συζήτησής μας.
[13] https://signal.org/bigbrother/eastern-virginia-grand-jury/
[14] Πρόσφατα, το Signal επέλεξε να καταστήσει μέρος του κώδικα του server του σε κλειστό κώδικα, δήθεν για να μπορέσει να καταπολεμήσει το spam στην πλατφόρμα (βλ. https://signal.org/blog/keeping-spam-off-signal/). Αυτό σημαίνει ότι υπάρχει πλέον ένα μικρό κομμάτι του κώδικα του Signal Server που δεν μοιράζεται δημόσια. Η αλλαγή αυτή υποδηλώνει επίσης μια αύξηση, αν και εξαιρετικά ελάχιστη, στη συλλογή μεταδεδομένων από την πλευρά του διακομιστή, δεδομένου ότι είναι απαραίτητη για να διευκολυνθεί η αποτελεσματική καταπολέμηση του spam, έστω και σε στοιχειώδη βαθμό. Δεν υπάρχει κανένας λόγος να υποπτευόμαστε κάτι εδώ, αλλά είναι σημαντικό να σημειωθεί ότι πρόκειται για άλλη μια απόφαση πολιτικής που θυσιάζει τις ανησυχίες για την ασφάλεια προς όφελος της εμπειρίας του χρήστη.
[15] https://signal.org/blog/sealed-sender/
[16] https://signal.org/bigbrother/
[17] https://signal.org/blog/looking-back-as-the-world-moves-forward/
[18] https://www.nationalgeographic.com/pages/article/130612-nsa-utah-data-center-storage-zettabyte-snowden
[19] https://www.wired.com/2013/10/nsa-hacked-yahoo-google-cables/
[20] https://theintercept.com/2018/06/25/att-internet-nsa-spy-hubs/
[21] https://www.aclu.org/news/privacy-technology/new-records-detail-dhs-purchase-and-use-of-vast-quantities-of-cell-phone-location-data
[22] Για παράδειγμα, δείτε αυτή την ιστορία σχετικά με τους καθολικούς δημοσιογράφους που έπιασαν έναν ιερέα που χρησιμοποιούσε το Grindr αγοράζοντας δεδομένα της εφαρμογής και αποανωνυμοποιώντας τα για να τον ταυτοποιήσουν: https://www.pillarcatholic.com/p/pillar-investigates-usccb-gen-sec
[23] https://www.youtube.com/watch?v=kV2HDM86XgI (το απόσπασμα είναι στο 18 λεπτό)
[24] Δείτε ένα παράδειγμα, το οποίο έκτοτε έχει επιδιορθωθεί, εδώ: https://medium.com/tenable-techblog/turning-signal-app-into-a-coarse-tracking-device-643eb4298447
[25] Ο γενικός σύμβουλος της NSA Stewart Baker.
[26] Αναφορά της OONI σχετικά με τα τρέχουσα προφανή μπλοκαρίσματα του Signal: https://explorer.ooni.org/search?until=2021-07-13&since=2021-06-12&test_name=signal&failure=false&only=anomalies
[27] Συγχωρήστε αυτό το εκτενές σημείωμα σχετικά με τους αριθμούς τηλεφώνου. Παρόλο που το Signal έχει αναφέρει ότι είναι ανοιχτό στο να απομακρυνθεί από την απαίτηση ενός αριθμού τηλεφώνου στα θέματα του GitHub, δεν έχει υπάρξει κάποια επίσημη ανακοίνωση ότι πρόκειται για ένα επερχόμενο χαρακτηριστικό που

βρίσκεται σε φάση εντατικής ανάπτυξης. Υποτίθεται ότι ένα από τα ζητήματα με την κατάργηση των αριθμών τηλεφώνου για την εγγραφή είναι ότι θα χαλάσει η συμβατότητα με παλαιότερους λογαριασμούς Signal λόγω του τρόπου με τον οποίο τα πράγματα υλοποιούνταν τις ημέρες του TextSecure. Αυτό είναι ειρωνικό, δεδομένου ότι το κύριο επιχείρημα του Moxie κατά των αποκεντρωμένων μοντέλων είναι ότι καθιστά πολύ δύσκολο το «να κινείσαι γρήγορα» - υπάρχει πολύ μεγάλη επιβάρυνση για την υλοποίηση νέων χαρακτηριστικών.
Και όμως, το Signal έχει κολλήσει με ένα δύσκολο ζήτημα εξαιτίας του παλιού κώδικα γύρω από την εγγραφή λογαριασμών σε έναν κεντρικό διακομιστή. Ο Moxie εξήγησε επίσης ότι οι αριθμοί τηλεφώνου χρησιμοποιούνται ως βάση της ταυτότητάς σας στο Signal για να διευκολυνθεί η διατήρηση του «κοινωνικού γραφήματος» σας. Αντί το Signal να πρέπει να διατηρεί κάποιο είδος κοινωνικού δικτύου για λογαριασμό σας, όλες οι επαφές σας ταυτοποιούνται από τον αριθμό τηλεφώνου τους στο βιβλίο διευθύνσεων του τηλεφώνου σας, καθιστώντας εύκολη τη συντήρηση και τη διατήρηση της λίστας επαφών σας καθώς μετακινείστε από άλλες εφαρμογές στο Signal, ή αν αποκτήσετε νέο τηλέφωνο, ή οτιδήποτε άλλο. Για το Moxie, ακούγεται ότι το να πρέπει να «ξανά ανακαλύπτετε» τις επαφές σας ανά τακτά χρονικά διαστήματα σε οποιοδήποτε σημείο είναι μια τρομερή ταλαιπωρία. Για τα αναρχικά, θα πρέπει να θεωρείται πλεονέκτημα το να πρέπει να διατηρούμε σκόπιμα το «κοινωνικό γράφημά» μας με βάση τη συγγένεια, τις επιθυμίες και την εμπιστοσύνη μας. Το ποιος είναι στο «κοινωνικό γράφημά» μας θα πρέπει να είναι κάτι που συνεχώς επανεκτιμούμε και επανεξετάζουμε για λόγους ασφαλείας (εξακολουθώ να εμπιστεύομαι όλους όσους έχουν τον αριθμό τηλεφώνου μου από πριν 10 χρόνια;) και για να ενθαρρύνουμε τις σκόπιμες κοινωνικές σχέσεις (είμαι ακόμα φίλος με όλους όσους έχουν τον αριθμό τηλεφώνου μου από πριν 10 χρόνια;). Τελευταία ασήμαντα στοιχεία σχετικά με τη χρήση τηλεφωνικών αριθμών από το Signal: Το Signal ξοδεύει περισσότερα χρήματα για την επαλήθευση τηλεφωνικών αριθμών από ό,τι για το κόστος φιλοξενίας της υπόλοιπης υπηρεσίας: 1.017.990 δολάρια για την υπηρεσία επαλήθευσης τηλεφώνου της Twillio έναντι 887.069 δολαρίων για την υπηρεσία webhosting της Amazon. (https://projects.propublica.org/nonprofits/display_990/824506840/02_2021_prefixes_81-83%2F824506840_201912_990_2021022217742945).
[28] Ή ίσως ακριβέστερα μη συνδεσιμότητα: https://code.briarproject.org/briar/briar/-/wikis/FAQ#does-briar-provide-anonymity
[29] Αν δεν είστε εξοικειωμένοι με τον τρόπο λειτουργίας του Tor, εδώ είναι ένα καλό βίντεο: https://www.youtube.com/watch?v=QRYzre4bf7I
[30] Δύο καλές πηγές για αυτό είναι τα εξής https://tails.boum.org/doc/about/warnings/tor/index.en.html και https://www.whonix.org/wiki/Why_does_Whonix_use_Tor
[31] Αναφορά για την τρέχουσα κατάστασή του Tor σε όλο τον κόσμο, υποδεικνύοντας πού μπορεί να υπάρχουν διαταραχές στο Tor δίκτυο: https://status.torproject.org/
[32] https://briarproject.org/raw/BRP-01-report.pdf
[33]Ο δημιουργός του Zcash, ένας άγριος τύπος με το όνομα Zooko Wilcox-O'Hearn, φαίνεται αποφασισμένος να διασφαλίσει ότι το Zcash είναι ιδιωτικό, αλλά δεν μπορεί να χρησιμοποιηθεί για εγκλήματα!
[34] https://openprivacy.ca/blog/2019/12/03/Incentivizing-Trustlessness-ZcashFoundation-Donation/
[35.] https://north-shore.info/2019/06/02/signal-fails/
[36] Έχετε ένα λεπτό για να μιλήσουμε για τη διαλειτουργικότητα και την ομοσπονδία; Ίσως αργότερα;
[37] Μια σπουδαία πηγή για την κατανόηση του πρωτοκόλλου του Signal: https://www.redshiftzero.com/signal-protocol/
[38] https://nitter.net/m_hoppenstedt/status/1532706414635978760#m

faurabooks@riseup.net
faurabooks.noblogs.org

003

THE RIOT IS ONE NIGHT...

...BUT METADATA LASTS FOREVER.