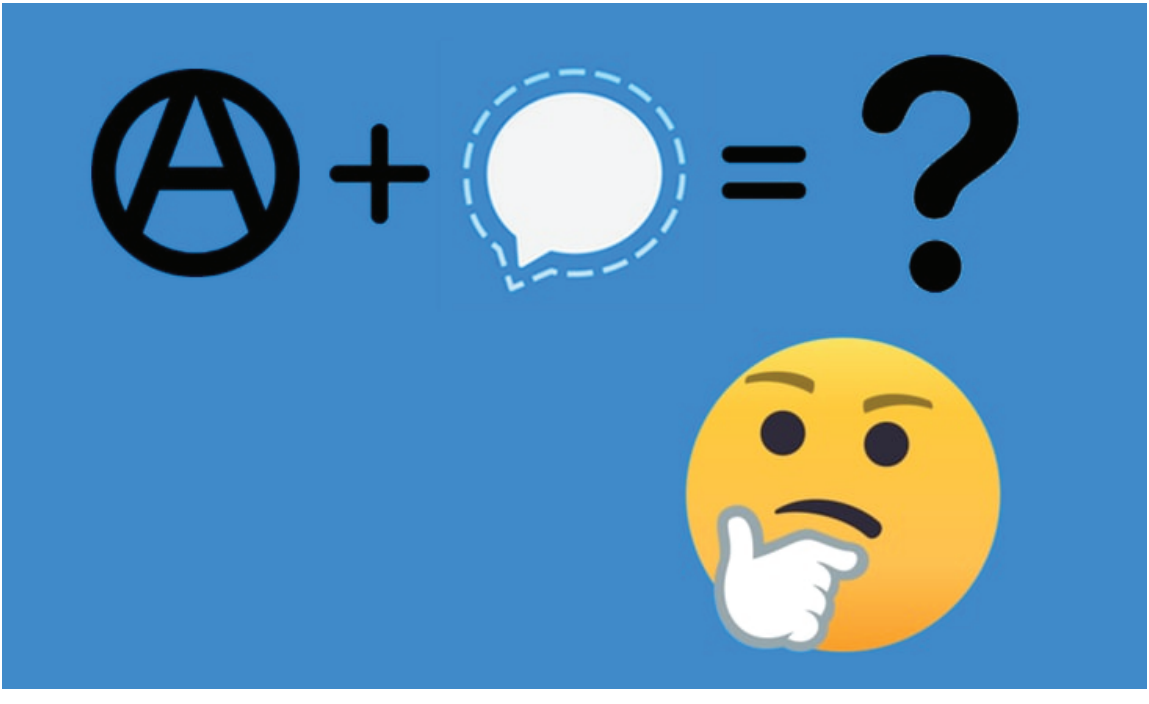
Signal Fails

Contributo anonimo sulla sicurezza informatica



"It feel so 80s
It feel so 90s
To be political
Where are my friends?
Get off the internet! - (I'll meet you in the street)
Get off the internet! - (Destroy the right wing)
This is repetitive
But nothing has changed
Am I crazy?
Where are my friends?"
Le Tigre

Introduzione

Signal è un servizio di messaggistica criptata che esiste in diverse forme da circa 10 anni. Da allora, ho visto il software ampiamente adottato dalle reti anarchiche in Canada e negli Stati Uniti. Sempre di più, nel bene e nel male, le nostre conversazioni interpersonali e di gruppo si sono spostate sulla piattaforma Signal, al punto che è diventato il modo dominante in cui gli anarchici comunicano tra loro in questo continente, con pochissimo dibattito pubblico sulle implicazioni.

Signal è solo un'applicazione per smartphone. Il vero cambiamento di paradigma che sta avvenendo è quello di una vita sempre più mediata dagli schermi degli smartphone e dai social media. Ci sono voluti solo pochi anni perché gli smartphone diventassero obbligatori per chiunque volesse avere amici o avesse bisogno di un lavoro, al di fuori di pochi soldi sporadici. Fino a poco tempo fa, la sottocultura anarchica era una di quelle sacche, dove ci si poteva rifiutare di usare uno smartphone ed esistere ancora socialmente. Ora sono meno sicuro, e questo è fottutamente deprimente. Quindi insisterò ostinatamente in tutto questo testo che non c'è sostituto alle relazioni faccia a faccia nel mondo reale, con tutta la ricchezza e la complessità del linguaggio del corpo, delle emozioni e del contesto fisico, e che continuano ad essere il modo più sicuro per avere una conversazione privata. Quindi, per favore, lasciamo i nostri telefoni a casa, incontriamoci in una strada o in un bosco, cospiriamo insieme, facciamo un po' di musica, costruiamo qualcosa, rompiamo qualcosa e nutriamoci della convivenza offline. Penso che questo sia molto più importante che usare correttamente Signal.

L'idea di questa zine è nata circa un anno fa, quando andavo a

trovare degli amici in un'altra città e scherzavo su come le conversazioni di Signal riportate si trasformano in un disastro. Gli schemi sono stati immediatamente riconosciuti, e ho cominciato a capire che questa conversazione stava accadendo in molti posti. Quando ho iniziato a chiedere in giro, tutti avevano lamentele e opinioni, ma erano emerse pochissime pratiche condivise. Così mi è venuta in mente una lista di domande e le ho fatte circolare. Sono rimasto piacevolmente sorpreso di ricevere più di una dozzina di risposte dettagliate, che unite a diverse conversazioni informali, costituiscono la maggior parte di questo testo[1].

Non sono un esperto - non ho studiato crittografia e non so codificare. Sono un anarchico con un interesse per la sicurezza olistica e un rapporto scettico con la tecnologia. Il mio obiettivo con questo contributo è riflettere su come Signal sia diventato così centrale per la comunicazione anarchica nel nostro contesto, valutare le implicazioni sia per la nostra sicurezza collettiva che per l'organizzazione sociale, e avanzare alcune proposte preliminari per lo sviluppo di pratiche condivise.

Una breve storia su Signal

25 anni fa, gli ottimisti tecnologici tra noi vedevano nell'internet emergente un enorme potenziale come strumento di liberazione. Ricordate quel vecchio segmento della CBC che elogiava "una rete di computer chiamata Internet" come "anarchia modulata"? E mentre ci sono ancora potenti modi per comunicare, coordinare e diffondere idee online in modo sicuro, è chiaro che le entità statali e aziendali stanno gradualmente catturando sempre più spazio online e lo usano per sottoporci a forme sempre più intense di sorveglianza e controllo sociale.[2]

Internet è sempre stata una corsa agli armamenti. Nel 1991, il crittografo, libertario civile e attivista per la pace Phil Zimmerman[3] ha creato Pretty Good Privacy (PGP), un'applicazione open-source per la crittografia dei file e la crittografia end-to-end per la posta elettronica. Sto evitando i dettagli tecnici, ma fondamentalmente l'importanza dell'end-to-end è che si può comunicare in modo sicuro direttamente con un'altra persona, e il servizio di posta elettronica non può vedere il messaggio, sia che si tratti di Google o di Riseup. A tutt'oggi, per quanto ne sappiamo, la crittografia PGP non è mai stata violata.[4]

Per anni, i tecnici e i nerd della sicurezza di certi ambienti - anarchici, giornalisti, criminali, ecc. - hanno cercato di diffondere PGP nelle loro reti come una sorta di infrastruttura di comunicazione sicura, con un certo successo. Come per tutto, c'erano dei limiti. La mia più grande preoccupazione per la sicurezza[5] con PGP è la mancanza di Forward Secrecy[6], il che significa che se una chiave di cifratura privata viene compromessa, tutte le email inviate con quella chiave possono essere decifrate da un aggressore. Questa è una preoccupazione reale, dato che la NSA

sta quasi certamente memorizzando tutte le vostre email criptate da qualche parte, e un giorno i computer quantistici potrebbero essere in grado di violare PGP. Non chiedetemi come funzionano i computer quantistici - per quanto mi riguarda, una maledetta magia del cazzo.

Il grande problema sociale di PGP, che ha fortemente influenzato il progetto Signal, è il fatto che non è mai stato ampiamente adottato al di fuori degli ambienti di nicchia. Nella mia esperienza, è stato persino difficile ottenere anarchici sul PGP e utilizzarlo correttamente. Ci sono stati dei workshop, molte persone sono state messe in condizione di farlo, ma non appena un computer si è bloccato o si è persa una password, si è tornati al punto di partenza. Semplicemente non ha funzionato.

Intorno al 2010, gli smartphone sono diventati popolari e tutto è cambiato. L'ubiquità dei social media, la costante messaggistica istantanea e la capacità delle aziende di telecomunicazioni (e quindi del governo) di tracciare ogni mossa degli utenti[7] ha completamente trasformato il modello di minaccia. Tutto il lavoro che le persone hanno svolto nel campo della sicurezza informatica è stato rimandato indietro di decenni: gli smartphone si basano su un'architettura completamente diversa da quella dei PC, con il risultato di un controllo dell'utente molto inferiore, e l'avvento di autorizzazioni per le applicazioni completamente libere ha reso l'idea della privacy degli smartphone quasi ridicola.
Questo è il contesto da cui è emerso Signal. L'anarchico 'cypherpunk' Moxie Marlinspike ha iniziato a lavorare su un software per portare la crittografia end-to-end negli smartphone, con Forward Secrecy, lavorando sull'idea che la sorveglianza di massa dovrebbe essere contrastata con la crittografia di massa.

Signal è stato progettato per essere utilizzabile, carino e sicuro. Moxie Marlinspike ha accettato di collaborare con i giganti della tecnologia WhatsApp, Facebook, Google e Skype per implementare il protocollo di crittografia di Signal anche sulle loro piattaforme.

"La grande vittoria per noi sarà quando un miliardo di persone utilizzerà WhatsApp e non sapranno nemmeno che è criptato" - Moxie Marlinspike

Comprensibilmente, è più probabile che gli anarchici si affidino per le loro comunicazioni a Signal - una fondazione senza scopo di lucro gestita da un anarchico - piuttosto che a una big tech, il cui modello di business principale è la raccolta e la rivendita dei dati degli utenti. E Signal ha alcuni vantaggi rispetto a queste altre piattaforme: è open-source (e quindi soggetta a peer review), cripta la maggior parte dei metadati, memorizza il minor numero possibile di dati utente, e offre alcune caratteristiche molto utili come la scomparsa dei messaggi e la verifica del numero di sicurezza per proteggersi dalle intercettazioni.

Signal si è guadagnato un elogio quasi universale da parte degli esperti di sicurezza informatica, tra cui le approvazioni dell'informatore della NSA Edward Snowden e i punteggi più alti della prestigiosa Electronic Frontier Foundation. Nel 2014, documenti trapelati dalla NSA hanno descritto Signal come una "grande minaccia" alla sua missione (di sapere tutto di tutti). Personalmente, mi fido della crittografia.
Ma Signal protegge davvero solo una cosa, ed è la vostra comunicazione mentre viaggia tra il vostro dispositivo e un altro dispositivo. È fantastico, ma è solo un pezzo di una strategia di

sicurezza. Ecco perché è importante, quando si parla di sicurezza, iniziare con il Threat Modeling[8](modello di minaccia). Le prime domande per qualsiasi strategia di sicurezza sono chi è il vostro probabile avversario, cosa stanno cercando di catturare e come è probabile che lo ottengano. L'idea di base è che le cose e le pratiche sono sicure o insicure solo in relazione al tipo di attacco da cui ci si aspetta di difendersi. Per esempio, potreste avere i vostri dati bloccati con una solida crittografia e la migliore password, ma se il vostro aggressore è disposto a torturarvi fino a quando non consegnerete i dati, non ha importanza.

Ai fini di questo testo, proporrei un modello di minaccia funzionante che riguarda principalmente due tipi di avversari. Il primo è costituito da agenzie di intelligence globali o da potenti hacker che si occupano di sorveglianza di massa e intercettano le comunicazioni. Il secondo è costituito da agenzie di polizia, che operano su un territorio controllato dal governo canadese o americano, impegnate in una sorveglianza mirata sugli anarchici. Per la polizia, le tecniche investigative di base includono il monitoraggio delle liste di posta elettronica e dei social media, l'invio in incognito ad eventi e informatori occasionali. Nei momenti in cui dispongono di maggiori risorse, o in cui le nostre reti diventano una priorità maggiore, passano a tecniche più avanzate, tra cui infiltrazioni a lungo termine, sorveglianza fisica frequente o continua (compresi i tentativi di catturare le password), intercettazioni di dispositivi di intercettazione, intercettazioni di comunicazioni e retate domiciliari in cui i dispositivi vengono sequestrati e sottoposti ad analisi forensi.
Devo sottolineare che molte giurisdizioni europee stanno attuando leggi fondamentali sulla divulgazione che obbligano legalmente le persone a dare la loro password alle autorità a determinate

condizioni o a finire in prigione.[9] Forse è solo questione di tempo, ma per ora in Canada e negli Stati Uniti non siamo legalmente obbligati a divulgare le password alle autorità, con la notevole eccezione di quando attraversiamo il confine.[10]

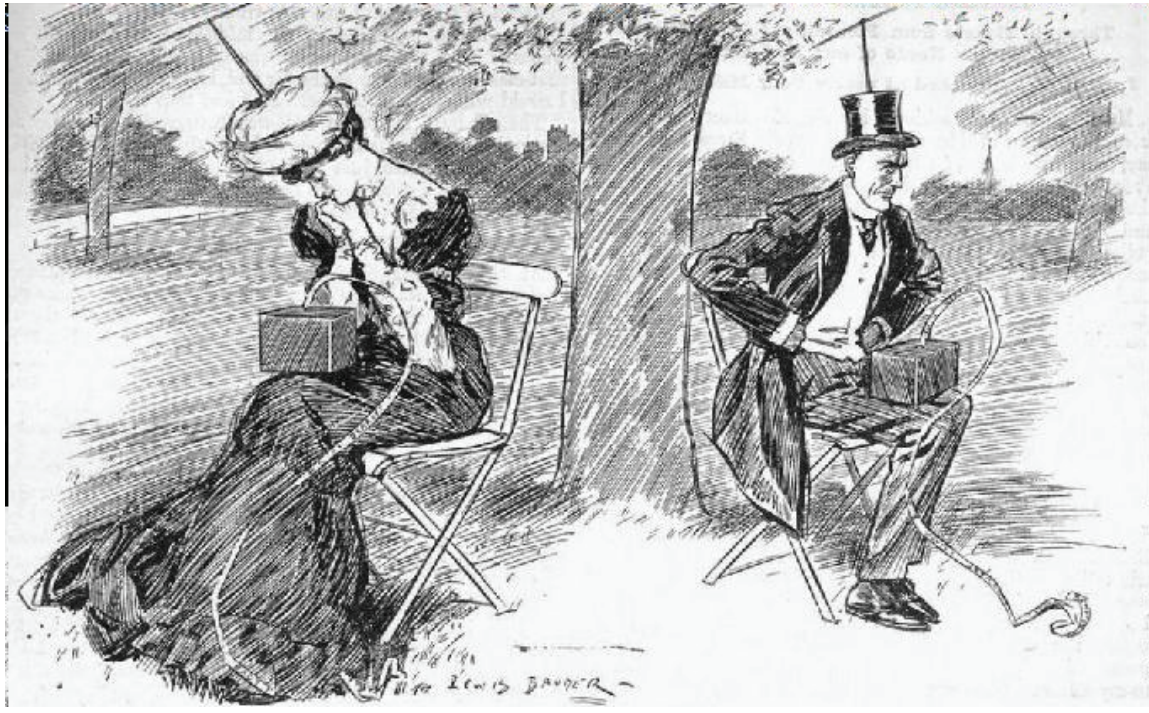
Se il vostro dispositivo è compromesso con un keylogger o altro software dannoso, non importa quanto siano sicure le vostre comunicazioni. Se siete in giro con un informatore o un poliziotto non importa se togliete la batteria del vostro telefono e parlate in un parco. La sicurezza dei dispositivi e la cultura della sicurezza sono due concetti non contemplati da questo testo che devono essere tenuti in considerazione per proteggersi da queste minacce molto reali. Ho incluso alcuni suggerimenti nella sezione Ulteriore lettura.

Vale anche la pena ricordare che Signal non è progettato per l'anonimato. Il tuo account Signal è registrato con un numero di telefono, quindi a meno che non ti registri con un telefono usa e getta acquistato in contanti o con un numero online usa e getta, non sei anonimo. Se perdi il controllo del numero di telefono usato per registrare il tuo account, qualcun altro potrebbe appropriarsi del tuo account. Ecco perché è molto importante, se si utilizza un numero anonimo per registrare il proprio account, attivare la funzione di "blocco della registrazione".

Soprattutto per motivi di sicurezza, negli ultimi 4 anni Signal è diventato il mezzo di comunicazione standard negli ambienti anarchici, eclissando tutto il resto. Ma così come "il mezzo è il messaggio", Signal sta avendo effetti profondi sul modo in cui gli anarchici si relazionano e si organizzano insieme che vengono troppo spesso trascurati.

La socialità di Signal

"Signal è utile nella misura in cui sostituisce forme meno sicure di comunicazione elettronica, ma diventa dannoso ... quando sostituisce la comunicazione faccia a faccia". - Unx collaboratrice/tore



La maggior parte delle implicazioni sociali di Signal non riguardano specificamente l'app. Sono le implicazioni di spostare sempre più le nostre comunicazioni, l'espressione personale, l'organizzazione degli sforzi e tutto il resto su piattaforme virtuali e la mediazione con gli schermi. Ma una cosa che mi è venuta in mente quando ho iniziato a vagliare le risposte al questionario è che prima di Signal, conoscevo diverse persone che rifiutavano gli smartphone sia per motivi di sicurezza che per ragioni sociali. Quando Signal è emerso con le risposte alla maggior parte dei problemi di sicurezza, la posizione di resistenza è stata

significativamente erosa. Oggi, la maggior parte di chi si è opposto ha uno smartphone, sia perché era convinto di usare Signal, sia perché è diventato effettivamente obbligatorio se voleva rimanere coinvolto. Signal ha funto da punto d'ingresso per alcuni anarchici agli smartphone.

D'altra parte, nella misura in cui Signal è una riduzione del danno per quelli di noi già intrappolati dagli smartphone, questa è una buona cosa. Sono contento che le persone che stavano principalmente socializzando e facendo organizzazione politica su canali non criptati come Facebook siano passate a Signal. Nella mia vita, la chat di gruppo ha sostituito la "piccola lista di email" ed è abbastanza utile per fare piani con gli amici o condividere link. Nelle risposte che ho raccolto, i gruppi Signal che erano i più preziosi per la gente, o forse solo i meno fastidiosi, erano quelli piccoli, concentrati e pragmatici. Signal può anche essere un potente strumento per spargere la voce in modo rapido e sicuro su una questione urgente che richiede una risposta rapida. Se l'organizzazione basata su Facebook ha portato troppi anarchici a credere che organizzare con qualsiasi elemento di sorpresa sia impossibile, Signal ha parzialmente salvato quell'idea, e di questo sono grato.

Signal Fails

Inizialmente ho immaginato questo progetto come una breve serie di vignette a fumetti che ho pensato di chiamare "Signal Fails", modellato liberamente sul libro "Come Hell or High Water: A Handbook on Collective Process Gone Awry". A quanto pare è difficile disegnare immagini interessanti che rappresentino i fili di Signal e io faccio schifo a disegnare. Scusate se ho promesso a qualcuno che, forse nella seconda edizione... In ogni caso, voglio

ancora includere alcuni Signal Fails, come un modo per prenderci in giro (mi ci includo anch'io!) e forse per spronare gentilmente tutti a smettere di essere così fottutamente fastidiosi.

Bond, James Bond: Avere Signal non ti rende a prova di proiettile. Date ad alcune persone un po' di crittografia, e immediatamente sottoporranno la loro intera lista di contatti alla merda più schifosa in assoluto. Il tuo telefono è ancora un dispositivo di tracciamento, e la fiducia è ancora costruita. Parlate con le persone di quali cose vi sentite a vostro agio a parlare al telefono e di cosa non vi sentite a vostro agio.

Il silenzio non è consenso: Siete mai andati ad un incontro, avete mai fatto un piano con altri, avete mai creato un gruppo Signal per coordinare la logistica, e poi avete subito una o due persone che cambiano rapidamente i vostri piani collettivi con una rapida serie di testi a cui nessuno ha il tempo di rispondere? Non è bello.

L'inferno è un incontro senza fine: Un gruppo Signal non è un incontro continuo. Sono già troppo incollato al mio telefono, quindi non mi piace quando il mio telefono viene fatto esplodere da un gruppo e si tratta solo di una lunga conversazione laterale tra due persone o del flusso di coscienza di qualcuno che non ha alcun rapporto con lo scopo del gruppo. Apprezzo quando le conversazioni hanno un inizio e una fine.

Vuole nutrirsi: Odio soprattutto questo. Probabilmente a causa dei social media, alcuni di noi sono abituati ad avere informazioni curate per noi da una piattaforma. Ma Signal non è un social media, grazie al cazzo. Quindi attenzione, perché quando un grande gruppo di Signal inizia a diventare il feed[II], sei nei guai. Questo

significa che se non ci sei e fai attenzione, ti perderai ogni tipo di informazione importante, sia che si tratti di eventi imminenti, di persone che cambiano i loro pronomi, o di flamewar che portano a conflitti sociali. La gente inizia a dimenticare la tua esistenza e, alla fine, sparisci letteralmente. Kill THE FEED.

Fuoco in un teatro affollato: il problema del pulsante anti panico. Ti stai rilassando in un grande gruppo di Signal con tutti i tuoi amici schizzati e tutti i loro numeri di telefono, qualcuno viene pizzicato per taccheggio o qualcosa del genere, e *sorpresa* il suo telefono non è criptato! Tutti vanno fuori di testa e saltano la nave, ma è troppo poco e troppo tardi, perché se i poliziotti stanno controllando quel telefono in questo momento, possono vedere tutti quelli che se ne sono andati e la mappatura sociale è fatta. Womp womp.

Missione subdola: Qualcuno ha creato un gruppo di Signal per coordinare un evento specifico e limitato nel tempo. È finita, ma nessuno vuole abbandonare il gruppo. In qualche modo, questa formazione ad hoc molto specifica è ora L'ORGANIZZAZIONE PERMANENTE che ha il compito di decidere tutto ciò che deve fare su tutte le cose - a tempo indeterminato.

Verso pratiche condivise

Se pensavi che questa fosse una guida alle migliori pratiche sul galateo di Signal o chat, mi dispiace che tu sia arrivato a questo punto senza renderti conto che non lo è. Questo è molto più di un "dobbiamo parlare di Signal". Credo nello sviluppo di pratiche condivise all'interno di specifici contesti sociali, e consiglio di iniziare ad avere questa conversazione esplicitamente nelle nostre reti. A tal fine, ho alcune proposte.

Ci sono alcuni ostacoli alla condivisione delle pratiche. Alcune persone non hanno Signal. Se è perché stanno costruendo relazioni senza smartphone, ho solo rispetto per questo. Se è perché passano tutto il giorno su Facebook ma Signal è "troppo difficile", non me la bevo. Se non altro, Signal è facile da installare e da usare per chiunque abbia uno smartphone e una connessione a internet.

Sono anche in disaccordo con la prospettiva orwelliana-fatalista che vede la crittografia come inutile: "I poliziotti sanno già tutto!" E' super-disincentivante interpretare il governo in questo modo, e per fortuna non è vero - la resistenza non è ancora futile. Il CSEC o la NSA hanno capacità da incubo, comprese molte che ancora non conosciamo. Ma ci sono anche ampie prove che la crittografia sta frustrando le indagini della polizia, ed è per questo che i governi stanno approvando leggi per contrastare questi strumenti.

Forse il più grande ostacolo alla condivisione delle pratiche è la generale mancanza di un "noi" - fino a che punto dobbiamo rendere conto a qualcuno, e se sì a chi? Come possiamo costruire eticamente norme sociali condivise? La maggior parte degli anarchici concorda sul fatto che è sbagliato fare la spia, per esempio, ma come ci siamo arrivati? Penso che una sorta di volgare

individualismo liberale stia influenzando l'anarchismo e rendendo quasi tabù discutere la questione stessa delle "aspettative". Ma questo è un testo diverso per un altro giorno.

Poche proposte per migliori pratiche

1. Keep it IRL - Come ha detto un collaboratore, "La comunicazione non è solo una questione di condivisione di informazioni". La comunicazione faccia a faccia costruisce intere relazioni, compresa la fiducia, e continua ad essere il modo più sicuro per comunicare.

2. Lasciate i vostri apparecchi a casa - almeno qualche volta? Soprattutto se si va oltre il confine, dove si può essere costretti a decifrare i propri dati. Se avete bisogno di un telefono quando viaggiate, acquistate un telefono da viaggio con i vostri amici che non contenga dati sensibili, compreso l'elenco dei vostri contatti.

3. Proteggere i dispositivi - La maggior parte dei dispositivi (telefoni e computer) hanno ora la possibilità di crittografia completa del disco. La crittografia è valida solo quanto la password protegge i dati "a riposo", cioè quando il dispositivo è spento o i dati non vengono utilizzati dai programmi. Il vostro lock screen fornisce una certa protezione mentre il vostro dispositivo è acceso, ma può essere bypassato da un sofisticato aggressore. Alcuni sistemi operativi vi costringono ad utilizzare la stessa password per la cifratura e il vostro lock screen, il che è un peccato in quanto non è pratico inserire una password lunga 25 volte al giorno (a volte in presenza di occhi indiscreti o telecamere di sorveglianza).

4. Spegnere i dispositivi - Se si lascia il dispositivo incustodito o si va a dormire, spegnerlo. Acquistate una sveglia a buon mercato. Se

la vostra casa viene saccheggiata durante la notte, sarete felici di averlo fatto. Se il vostro dispositivo è spento e criptato con una password forte quando viene sequestrato, è molto meno probabile che i poliziotti riescano ad introdursi in esso. Se volete davvero fare il passo più lungo della gamba, acquistate una cassaforte decente e chiudete i vostri dispositivi all'interno quando non li usate, il che ridurrà il rischio che vengano manomessi fisicamente di nascosto.

5. Stabilire dei confini - Abbiamo diversi sensi di ciò che è sicuro parlare al telefono e ciò che non lo è. Discutiamo e sviluppiamo i confini collettivi, e dove non siamo d'accordo, rispettiamo i confini delle altre persone anche se pensiamo che sia sicuro.

6. Concordare un sistema di cooperazione - Se siete in un gruppo che discute di cose delicate, sviluppate un'esplicita comprensione collettiva di ciò che costituisce una cooperazione per una nuova persona che aderisce. In un'epoca in cui gli anarchici sono accusati di cospirazione, le comunicazioni errate possono far finire la gente in prigione.

7. Chiedi prima - Se vuoi aggiungere qualcuno a un gruppo, rivelando così il suo numero di telefono a tutto il gruppo, chiedi prima il suo consenso e quello del gruppo.

8. Ridurre al minimo il processo decisionale - Considerare la possibilità di lasciare le decisioni diverse da sì/no per le riunioni di persona, se possibile. Secondo la mia esperienza, Signal impoverisce qualsiasi processo decisionale.

9. Scopo definito - Idealmente, un gruppo Signal avrà uno scopo specifico. Ogni nuova persona aggiunta a quel gruppo dovrebbe

avere questo scopo chiaramente spiegato loro. Se lo scopo è stato raggiunto, lasciare il gruppo e cancellarlo.

10. Messaggi a scomparsa - Molto utile per le pulizie. Da 5 secondi a 1 settimana, i messaggi a scomparsa possono essere impostati selezionando l'icona del cronometro nella barra superiore di una conversazione. Molte persone usano un tempo standard di 1 settimana per la scomparsa di tutti i messaggi, sia che la conversazione sia sensibile o meno. Selezionare il tempo di scadenza in base al modello di minaccia. Questo vi protegge anche in qualche modo se la persona con cui state comunicando utilizza pratiche di sicurezza telefonica non ideali.

11. Verificare i numeri di sicurezza - Questa è la vostra migliore protezione contro un "man-in-the-middle attack"[12]. È abbastanza semplice da fare e più facile di persona - aprite la vostra conversazione con la persona con cui volete verificare e navigate in Impostazioni di conversazione > Visualizza il numero di sicurezza e scansionate il codice QR o confrontate i numeri. La maggior parte degli intervistati ha detto: "Dovrei farlo, ma non lo faccio". Approfittate dei grandi incontri per verificare i contatti. Va bene essere un nerd!

12. Abilita il blocco della registrazione - Abilitalo nelle Impostazioni sulla privacy di Signal, quindi se qualcuno è in grado di violare il tuo numero di telefono usato per registrare il tuo account, deve comunque ottenere il tuo PIN per appropriarsi della tua identità. Questo è particolarmente importante per gli account Signal anonimi registrati con numeri di telefono usa e getta, dato che quasi certamente qualcun altro userà di nuovo questo numero.

13. Disattivare le anteprime dei messaggi - Impedire che i messaggi appaiano sulla schermata di blocco. Sul mio dispositivo, ho dovuto impostarlo sulle impostazioni del dispositivo (non sulle impostazioni Signal) sotto Preferenze schermata di blocco > Nascondi contenuti sensibili.

14. Cancellare i vecchi messaggi - Permettendo l'eliminazione dei gruppi o cancellando manualmente le conversazioni completate, non tenete più in giro messaggi di cui non avete bisogno.

Conclusione

Ho intrapreso questo progetto per riflettere e raccogliere feedback sull'impatto che Signal ha avuto sulle reti anarchiche negli Stati Uniti e in Canada, sia dal punto di vista della sicurezza che da quello dell'organizzazione sociale. Così facendo, credo di aver colto alcune frustrazioni comuni che la gente ha avuto, specialmente con i grandi gruppi di Signal, e ho raccolto alcune proposte da far circolare. Continuo a insistere sul fatto che gli smartphone stanno facendo più danni che bene alle nostre vite e alle nostre lotte, perché per me è importante. Dobbiamo preservare e costruire altri modi di organizzarci, specialmente offline, sia per la qualità della vita che per la sicurezza dei movimenti. Anche se continuiamo a usare gli smartphone, è pericoloso quando le nostre comunicazioni sono centralizzate. Se i server di Signal andassero fuori uso stasera, o Riseup.net, o Protonmail, immaginate quanto sarebbe devastante per le nostre reti. Se gli anarchici dovessero mai rappresentare una grave minaccia per l'ordine costituito, verranno per noi e per la nostra infrastruttura senza pietà, compresa la sospensione delle "protezioni legali" da cui potremmo dipendere. Nel bene e nel male, credo che questo scenario sia possibile nella nostra vita, e quindi dovremmo pianificare la resilienza.

Chi ha capacità tecniche tra noi dovrebbe continuare a sperimentare altri protocolli, software e sistemi operativi,[13] condividendoli se si rivelano utili. Le opposizioni all'uso di smartphone dovrebbero continuare a resistere, e trovare il modo di prosperare offline. Per il resto di noi, cerchiamo di ridurre al minimo il grado di cattura degli smartphone. Insieme alla capacità di lottare, dovremmo costruire una vita degna di essere vissuta, con una qualità di relazioni che i potenziali amici e co-cospiratori troveranno irresistibilmente coinvolgenti. Potrebbe essere l'unica speranza che abbiamo.

Note

1. Un grande grazie a tutti coloro che si sono presentati! Ho rubato molte delle vostre idee.

2. Le modalità di governance dell'era di Internet variano da un luogo all'altro - gli Stati più autoritari potrebbero preferire il filtraggio e la censura, mentre gli Stati democratici producono una sorta di "cittadinanza digitale" - ma la sorveglianza di massa e la guerra informatica stanno diventando la norma.

3. Ironia della sorte, il governo degli Stati Uniti avrebbe poi cercato di accusare Zimmerman di aver pubblicato liberamente il codice sorgente di PGP, sostenendo che stava "esportando armi". Così pubblicò il codice sorgente in un libro cartonato e lo inviò per posta in tutto il mondo, con la motivazione che l'esportazione dei libri è protetta dalla Costituzione degli Stati Uniti.

4. I processi contro le Brigate Rosse in Italia (2003) e contro i pedopornografi negli Stati Uniti (2006) hanno dimostrato che le agenzie di polizia federale non sono riuscite a penetrare nei

dispositivi e nelle comunicazioni protette da PGP. Invece, gli agenti hanno fatto ricorso a dispositivi di intercettazione, approvando una legislazione che richiede la consegna delle password e, naturalmente, informatori e infiltrazioni sotto copertura.

5. Fino a poco tempo fa, PGP non criptava i metadati (chi inviava le email a chi, su quali server, in quale momento), il che era un problema enorme. Un avvocato dell'NSA una volta disse: "se hai abbastanza metadati, non hai bisogno di contenuti".

6. In crittografia, il forward secrecy (in italiano: "segretezza in avanti"), conosciuto anche come perfect forward secrecy o PFS[1], è una proprietà dei protocolli di negoziazione delle chiavi che assicura che se una chiave di cifratura a lungo termine viene compromessa, le chiavi di sessione generate a partire da essa rimangono riservate.
Se la chiave usata per cifrare i dati non viene usata per generare altre chiavi, e a loro volta le chiavi a lungo termine da cui è stata generata non sono usate per derivare altre chiavi di sessione, la compromissione di una sola chiave di sessione permetterà l'accesso solo ai dati protetti da tale chiave.

7. Vuoi leggere qualcosa di spaventoso? Cercate su internet "Google's Sensorvault".

8. Il Threat modeling è un processo attraverso il quale possono essere individuate, enumerate e prioritarie potenziali minacce, come le vulnerabilità strutturali o l'assenza di adeguate salvaguardie. Lo scopo della modellazione delle minacce è quello di fornire ai difensori un'analisi sistematica di quali controlli o

difese devono essere inclusi, data la natura del sistema, il profilo dell'aggressore probabile, i vettori di attacco più probabile e le risorse più utilizzate da un aggressore. Il Threat modeling risponde a domande come "Dove sono più vulnerabili agli attacchi?" "Quali sono le minacce più rilevanti?" e "Cosa devo fare per proteggermi da queste minacce?".

9. La negabilità plausibile, il "forward secrecy" e la distruzione sicura dei dati sono stati progettati in alcuni strumenti di privacy per cercare di contrastare questa minaccia o almeno di minimizzarne i danni.

10. Le impronte digitali (e altri dati biometrici) non sono considerate password in molte giurisdizioni, il che significa che i blocchi delle impronte digitali non sono soggetti alle stesse protezioni legali.

11. il termine feed, detto in italiano flusso, è un'unità di informazioni, formattata secondo specifiche precedentemente stabilite, al fine di rendere interpretabile e interscambiabile il contenuto fra diverse applicazioni o piattaforme. Viene utilizzato per fornire agli utenti una serie di contenuti frequentemente aggiornati. I distributori del contenuto rendono disponibile il feed e consentono agli utenti di iscriversi. L'aggregazione consiste in un insieme di feed accessibili simultaneamente, eseguita da un software aggregatore.

12. Attacco man-in-the-middle (spesso abbreviato in MITM, MIM, MIM attack o MITMA, in italiano "uomo nel mezzo") è una terminologia impiegata nella crittografia e nella sicurezza informatica per indicare un attacco informatico in cui qualcuno

segretamente ritrasmette o altera la comunicazione tra due parti che credono di comunicare direttamente tra di loro.

13. Sul mio telefono ho recentemente sostituito Android con LineageOS, che è un sistema operativo orientato alla privacy, de-Googled, basato su codice Android. È fantastico, ma è costruito solo per alcuni dispositivi, si annulla la garanzia del telefono, e c'è sicuramente bisogno di imparare a impostarlo, tenerlo aggiornato e passare a un software open-source.

Ulteriori letture

Questa zine è stata pubblicata nel maggio 2019(Versione originale in Inglese). Signal aggiorna periodicamente le sue caratteristiche. Per le informazioni tecniche più aggiornate, vai su signal.org, community.signalusers.org, e /r/signal su reddit.

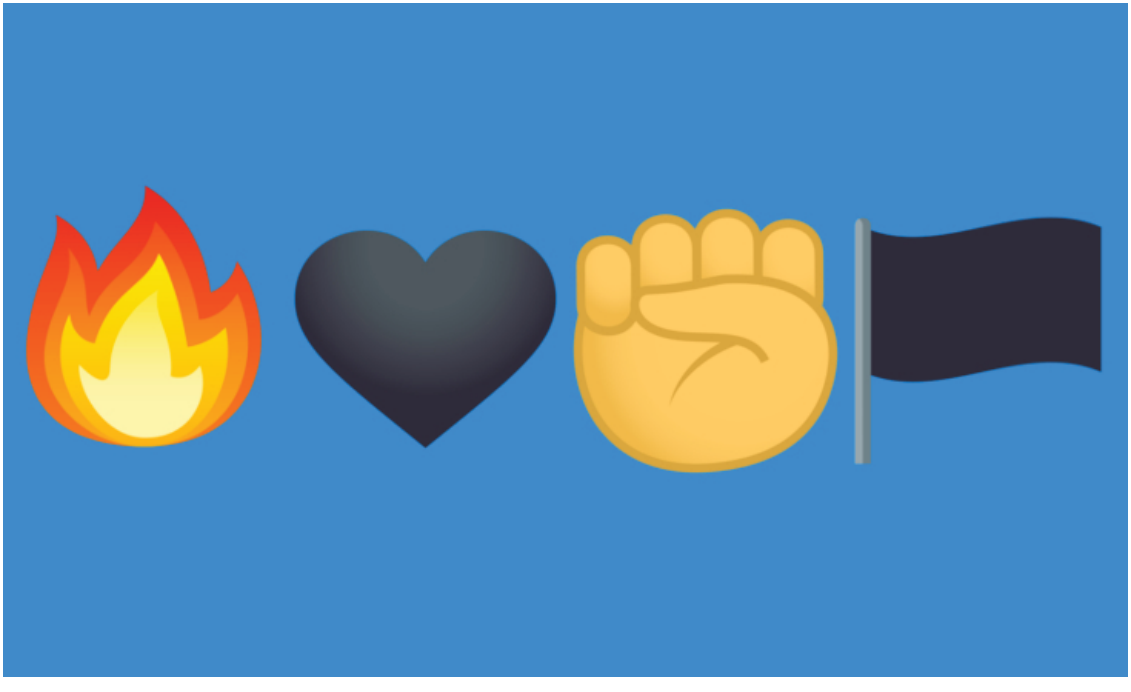
Your Phone is a Cop
https://itsgoingdown.org/phone-cop-opsecinfosec-primer-dystopian-present/

Choosing the Proper Tool for the Task
https://crimethinc.com/2017/03/21/choosing-the-proper-tool-for-the-task-assessing-your-encryption-options

EFF Tool Guides for Surveillance Self-Defense (including Signal)
https://ssd.eff.org/en/module-categories/tool-guides

Towards a Collective Security Culture
https://crimethinc.com/2009/06/25/towards-a-collective-security-culture
Riseup Security Guide
https://riseup.net/security

Toronto G20 Main Conspiracy Group: The Charges And How They Came To Be
https://north-shore.info/archive/



La versione originale, in Inglese, è stata pubblicata a Maggio 2019. *La versione in italiano è di Marzo* 2020.

Per contattare l'autore dell'opuscolo originale:

Signalfails[at]riseup[dot]net