De rerum chatura

Preambolo

Quando si trattano dei dati, e nello specifico nelle messaggistiche, da un punto di vista di sicurezza e tracciabilità, si deve prendere in considerazione il paradgima FBI. No aspetta, era CIA:

- **C**onfidenzalità (*confidentiality*): quello che viene detto viene letto solo dagli interlocutori
- **I**integrità (*integrity*): quello che viene detto non è alterato o alterabile
- **D**isponibilità (*availability*) (esatto, come avete capito *availability* significa disponibilità. Quindi *High Availability* significa *alta disponibilità* e non *alta avviabilità* come volevano farmi credere quelle di una nota azienda di Telco italiana): quello che viene detto è leggibile quando necessario

poi visto che ci siamo ci aggiungiamo:

- **A**utenticità: quello che viene detto è sicuramente stato detto da chi dice di essere
- **T**racciabilità (accountability): quello che viene detto, si sa chi l'ha detto, quando l'ha detto, a chi l'ha detto.

La base

Non so se avete presente qualcosa di questo (https://cdn-img-a.facciabuco.com/248/no2ns2ztab-camion-trasporto-cazzi-miei-venerdi-17-vaccata_b.jpg) tipo. La rete è un po' così, quando è cifrata. In pratica si vede il camion, vediamo il guidatore, vediamo dove va, ma non sappiamo che cosa c'è dentro.

Ok come esempio fa un po' schifo, quindi torniamo a parlare nella maniera più piatta con Alice e Bob, ovvero i Mario Rossi e Bianchi della crittografia. Questi due simpatici personaggi vogliono parlarsi tra di loro. Ci sono vari modi:

- parlano pubblicamente tra di loro, cosicché tutti possono sapere che cosa dicono

- parlano tra di loro al telefono, cosicché possono essere intercettati solo dalla compagnia telefonica (o da chi ne ha l'autorizzazione a metterci le mani)
- parlano tra di loro al telefono con alfabeto farfallino (quefellefe cafazzafatefe chefe sifi fafacefevafanofo dafa pificcofolifi)
- comunicano mediante posta: prendono una foglio, ci scrivono il alfabeto farfallino, la mettono in una busta con scritto il destinatario, poi la infilano in un'altra busta con scritto l'ufficio postale di Londra come destinatario, poi la infilano dentro un'altra busta con scritto l'ufficio postale di New York come destinatario, poi la infilano dentro un'altra busta...)

Per analogia:

- Il primo modo equivale alla chat pubblica, dove potenzialmente tutti leggono tutto: forum, siti, chat di telegram standard, etc.
- il secondo modo equivale alle chat private su server centralizzati senza crittografia end to end (ma solo di trasporto, come ssl): rocket chat, mattermost, cisco webex, e migliaia di altri software per lo più enterprise
- il terzo modo equivale alle chat cifrate end to end: whatsapp, chat segrete di telegram (non quelle standard!), matrix (nelle room cifrate, altriementi nisba), deltachat
- il quarto modo equivale alle chat cifrate end to end con onion routing

Ora, partendo dal presupposto che ci sia integrità in ogni tipo di comunicazione (ovvero si dà per scontato che almeno ci sia la crittografia sul trasporto e siamo quindi in ssl), dobbiamo capire quale tipo di comunicazione fa al caso nostro.

Confidenzialità

Se vogliamo cofidenzialità, il primo dei metodi è escluso, e sarebbe bene escludere anche il secondo: è vero che la comunicazione è cifrata tra Alice e il server e tra Bob e il server, ma chi mette le mani sul server vede tutto in chiaro (amministratori di sistema in primis).

La confidenzialità richiede almeno la cifratura E2EE (end to end encryption): solo mittente e destinatario devono poter sapere che cosa c'è scritto all'interno del messaggio. Questa cosa è possibile grazie

all'utilizzo di chiavi simmetriche incapsulate in chiavi asimmetriche. Per il profano si faccia questo esempio.

Alice ha una valigetta del peso di 50 kg a vuoto e un cofanetto di 50 grammi con una chiave a combinazione.

Alice ha anche una chiave che apre dei lucchetti che deposita presso le migliori edicole.

Anche Bob ha una chiave, che apre altri lucchetti e anche lui li deposita presso le migliori edicole.

Per far recapitare un messaggio a Bob, Alice farà questi passaggi:

- si reca in un'edicola e prende un lucchetto di Bob
- Prende il cofanetto, lo infila vuoto nella valigia, chiude la valigia con il lucchetto di Bob
- spedisce la valigia a Bob a mezzo corriere.

A questo punto

- Bob riceve la valigia: la apre con la sua chiave, prende il cofanetto, imposta la combinazione e la lascia su aperto. In realtà Bob era andato in bagno proprio mentre passava il corriere che ha quindi lasciato un avviso di deposito in cassetta delle lettere; dopo svariati tentativi di chiamare il servizio clienti, ha deciso di prendere la propria auto 3 giorni dopo per andare presso il centro distribuzioni che è a non meno di 10 km di distanza ed è aperto al pubblico dalle 10 alle 11 i venerdì pari delle settimane dispari.
- Bob prende un lucchetto di Alice nelle migliori edicole, rimette il cofanetto nella valigia e la chiude con il lucchetto appena acquistato
- Bob, non senza sforzi, spedisce la valigetta ad Alice a mezzo posta

A quel punto Alice riceve quel catafalco di valigetta, la apre con la sua chiave, e trova il cofanetto con la combinazione impostata, ma aperta.

Da ora in poi, sia Alice che Bob sanno con che combinazione aprire il cofanetto: potranno inviarsi i messaggi cartacei spedendo semplicemente il cofanetto perché la combinazione è nota ad entrambi,

e solo a loro, e si possono risparmiare le dure tariffe intercontinentali per pesi oltre i 45 kg. E lo sconto c'è solo i giovedì dispari delle settimane pari degli anni bisesti, anni funesti.

Metadati

Adesso si entra nel campo minato dei metadati.

Che cosa sono? Sono quelle robe che stanno intorno al contenuto del messaggio e che servono a recapitarlo.

- Mittente
- Destinatario
- Paese di invio
- Paese di destinazione
- Frequenza di scambio dei messaggi
- Orario di scambio dei messaggi e pattern (la mattina, la sera, la notte)
- Appartenenza a gruppi

Questi metadati vengono spesso utilizzati dalle Big Tech (spoiler: non c'è complottismo, è triste realtà) per profilare i corrispondenti e - nel caso più lasco - propinare consigli per gli acquisti.

Supponiamo che Alice parli con Bob, ed entrambi usino *Whatsapp*. Supponiamo che Alice abbia anche un account Facebook. Ora pensiamo a un terzo, Charlie (tanto per cambiare) che non ha whatsapp, non ha Facebook, non ha fatto niente di male se non avere il proprio numero di telefono nella rubrica di Alice e Bob.

Alice e Bob chiacchierano fitto fitto su *Whatsapp*. Bob scrive ad Alice via Instagram.

L'azienda Meta capisce che sono tutti e tre amici: hanno la rubrica (sincronizzata con whatsapp da Bob e Alice), Alice e Bob si parlano, Charlie è un amico in comune. Il grafo sociale è costruito per cui, quando Charlie andrà in giro a navigare e verrà tracciato tramite pixel, quella informazione entra nel grande calderone dei dati raccolti dall'azienda. Se il sistema ha già correlato Charlie ad Alice e Bob (rubrica, contatti in comune, interazioni), è possibile che segnali simili si riflettano anche su di loro: non perché "Charlie ha cercato X", ma perché fanno parte dello stesso cluster.

In pratica, anche senza conoscere il contenuto dei messaggi che si scambiano i 3 amici, i metadati bastano spesso a ricostruire relazioni, abitudini e contesto meglio del contenuto stesso. Non serve sapere cosa si dicono Alice e Bob. Basta sapere che parlano ogni sera alle 22, per 40 minuti, da due città diverse.

L'uso dei metadati

I metadati quindi, a meno di non entrare in roba spinta (onion routing, comunicazioni senza identità persistenti o difficili da correlare), ci sono. La differenza sta in mano a chi li mettiamo: se finiscono a qualcuno che li minimizza, li usa solo per far funzionare il servizio e poi li butta via, tarabaralla. Se invece li diamo a chi costruisce modelli e business sui dati, il discorso cambia. Perché i metadati non restano fermi: vengono aggregati, correlati, incrociati con altre fonti. E a quel punto non è più solo “con chi parli”, ma cosa si può dedurre da quello. E sì, in certi casi quei dati possono anche finire — direttamente o indirettamente — nelle mani di soggetti che magari non avreste scelto voi.

Il contenuto racconta una conversazione. I metadati raccontano le persone.

E quindi?

E quindi la situazione è un po' tragica, ma una linea guida me la sono fatta.

- Servizi legati al numero di telefono e gestiti da big tech: no, grazie. Il gruppo mamme, cavolo, fatelo altrove.
- Servizi legati al numero di telefono ma con un modello più rispettoso: qui si entra nel grigio.
    - Telegram: meh. La cifratura end-to-end non è attiva di default, quindi per me è un no.
    - Signal: decisamente meglio. Usa E2EE ovunque, è open source, minimizza i metadati per quanto possibile e non basa il proprio modello di business sulla profilazione. Il numero di telefono c'è, ma viene trattato in maniera meno invasiva (hash, discovery controllata, possibilità di pseudonimi).

- Servizi che non richiedono numero di telefono (user/password o equivalenti): qui le cose si fanno interessanti.
    - Delta Chat: modello molto pulito. Usa l'email come trasporto, i relay (chatmail) tendono a non trattenere dati e, volendo, il server può essere completamente sotto il vostro controllo.
    - Matrix: potente ma più complesso. Può essere self-hostato (Synapse, Conduit, ecc.), ma i metadati esistono e, in un ambiente federato, possono essere distribuiti tra più server. Il vantaggio è che, se il server è vostro, avete controllo su retention, log e politiche.

Esistono alternative senza metadati e cifrate?

Sì, esistono: Session e SimpleX Chat. Per me però sono ancora progetti piuttosto immaturi.

- Session: punta molto sull'anonimato (niente numero di telefono, routing tipo onion), ma ha diversi compromessi. L'architettura è più complessa e questo si riflette sull'affidabilità: il multidevice è instabile, i messaggi possono arrivare in ritardo o in ordine strano. Dal punto di vista crittografico è solido, ma il problema qui è più pratico che teorico.
- SimpleX Chat: è forse il modello più interessante lato privacy e anonimato. Non ha identità globali persistenti, quindi non esiste un grafo sociale da costruire. Il rovescio della medaglia è l'usabilità: niente vero multidevice, sincronizzazione limitata e consumo di batteria non banale.

Riepilogo veloce (CIA + AT + Anonimato)

Servizio	Confidenzialità	Integrità	Disponibilità	Autenticità	Tracciabilità	Anonim
WhatsApp	✔✔✔	✔✔✔	✔✔✔	✔✔	❌	❌
Telegram	⚠	✔✔	✔✔✔	✔✔	❌	❌
Signal	✔✔✔	✔✔✔	✔✔	✔✔✔	✔	⚠
Delta Chat	✔✔✔	✔✔✔	✔✔	✔✔	✔✔	❌
Delta Chat (Arcane)	✔✔✔	✔✔✔	✔✔	✔✔✔	✔✔	✔
Matrix	✔✔✔	✔✔✔	✔✔✔	✔✔✔	⚠	✔
Session	✔✔✔	✔✔✔	⚠	✔✔	✔✔✔	✔✔✔
SimpleX	✔✔✔	✔✔✔	⚠	✔✔	✔✔✔	✔✔✔

Legenda:
✔✔✔ = molto buono
✔✔ = buono
✔ = accettabile
⚠ = dipende / limitazioni
❌ = scarso

Nota:

- "Autenticità" = autenticità crittografica del peer (protezione da MITM), non identità reale.
- "Anonimato" = possibilità di non essere direttamente riconducibili alla propria identità reale.

Sì ma alla fine della fiera, che cosa usiamo?

Utenti standard, comunicazioni standard:

- Se non ve ne frega niente di essere tracciati come tutti, andate pure con Whatsapp. Il protocollo di crittografia che usa è quello

di Signal, quindi è gold standard. È solo che avrete sempre un grande fratello dietro e fornite i vostri dati a Meta. Quello che mi manda fuori di cervello, però, è che così facendo date a Meta pure le vostre rubriche dove magari c'è qualcuno che sui suoi server non ci vorrebbe finire.
- L'alternativa plug and play è Signal. Personalmente, alla fine, credo che sia il miglior compromesso: bisognerebbe che almeno i vostri maggiori interlocutori avessero un account (o perché ce l'hanno o perché glielo fate creare voi).

Utenti enterprise:

- tiratevi su un server matrix e isolatelo; è vero che ci sono metadata, ma tanto siete voi a gestirlo. Non usate server pubblici (matrix.org per intenderci)

Utenti shadow:

- session / simplexchat: per shadow non intendo che vogliono nascondersi dai curiosi, ma proprio dai governi per il tipo di attività che intendono svolgere con gli altri (attivisti).

Non credo che in condizioni standard l'anonimato spinto sia necessario: dipendenti pubblici, di aziende, famiglie, amici non hanno bisogno di anonimato: hanno bisogno di integrità, confidenzialità ed è bene che sia noto chi ha mandato il messaggio (il mio capo, la mamma, l'amico). Basta essere sicuri di non essere profilati da chi non ne ha diritto.

Se poi volete iscrivervi al partito terroristi italiani, allora la cosa cambia e vorrete l'anonimato: ma sappiate che anche in quel vedrete che qualcuno vi scova, principalmente per chiedervi *quali sono i compiti di matematica per domani e a che ora parte il bus per la gita*

[Che il talpone sia con voi]

[EOF]

Fluxer Icon

Canale di discussione e supporto

Canale di discussione e supporto. Per confrontarti su configurazioni o altro entra su fluxer.dreadful.work (https://fluxer.dreadful.work/invite/dreadful).