La grande illusione di WhatsApp: Perché crittografia non significa privacy

La grande illusione di WhatsApp: Perché crittografia non significa privacy

Se c'è una cosa che mi fa sanguinare le orecchie è sentire qualche responsabile IT – di quelli cresciuti a pane e policy aziendali inutili – o qualche collega fava, ripetere come un mantra rassicurante: "Tranquillo, WhatsApp usa la crittografia end-to-end, Zuckerberg non legge i miei messaggi".

Tecnicamente è vero. Il protocollo crittografico (Signal Protocol) è lo stesso identico. Ma questa è solo mezza verità. E la metà che manca è proprio quella che vi frega.

Della metropoli di vetro e dei metadati in generale abbiamo già parlato qui (se vi siete persi l'articolo, andate a rileggervelo così non sto a ripetermi). Oggi entriamo nel merito pratico. Perché a palle ferme, bisogna capire come convincere le persone – da vostra zia al dirigente ministeriale – a mollare la baracca di Meta per passare a qualcosa di serio.

Andiamo con ordine, dal meno tecnico al più nerd.

Livello 1: Per vostra zia (quella dei "buongiornissimi")

Se provate a spiegare a vostra zia la crittografia a chiave pubblica, vi guarderà come se parlaste in aramaico antico. Con lei dovete parlare di **vaìni** e di spionaggio spicciolo.

WhatsApp è gratis. Non ci sono pubblicità (per ora). E sapete bene che a questo mondo nessuno vi regala niente per niente. Come si mantiene un'infrastruttura da miliardi di messaggi al giorno? Semplice: vendendo voi stessi. O meglio, la vostra impronta digitale.

Provate a farle vedere questa schermata. È la lista ufficiale dei dati che l'applicazione raccoglie e associa direttamente all'utente (dalla scheda di privacy ufficiale sull'App Store):

La razzia dei dati

Confronto impietoso: WhatsApp saccheggia la vostra rubrica, traccia la vostra posizione e raccoglie ID del dispositivo. Signal conosce solo una cosa: il vostro numero di telefono.

La zia capirà subito: su WhatsApp è come stare in un negozio dove il commesso vi segue ovunque, vi fruga nelle tasche, prende nota di quello che comprate, di dove andate e di chi salutate. Su Signal, entrate in una stanza chiusa, parlate e andate via senza lasciare impronte.

Livello 2: Per il collega di marketing (o l'esperto di SEO improvvisato)

Qui entriamo nel magico mondo dei **metadati** e del **grafo sociale**.

"Sì, vabbè, ma tanto i messaggi sono cifrati, cosa ci fanno con la lista dei contatti?" – dice l'esperto medio mentre sorseggia il caffè della macchinetta.

Ecco cosa ci fanno. A Meta non serve leggere che avete scritto "*Ho la febbre, oggi non vengo in ufficio*". Le basta sapere che:

1. Vi siete connessi dall'IP di un ospedale alle 08:30.
2. Avete scambiato 3 messaggi con il vostro medico.
3. Avete contattato il vostro capo subito dopo.

Incrociando questi metadati puliti, strutturati e pronti per il database con i vostri profili Instagram e Facebook e la posizione GPS (che WhatsApp vi chiede con insistenza "per farvi condividere la posizione con gli amici"), Meta ricostruisce la vostra intera esistenza. Sanno chi frequentate, le vostre idee politiche, i vostri orientamenti sessuali, i vostri problemi di salute.

Non leggono le vostre parole, ma vi leggono dentro.

Grafico di correlazione dei metadati

Un tipico grafico di correlazione dei metadati. Non serve leggere il testo per sapere chi comanda, chi si ama e chi si incontra in segreto.

I metadati valgono molto di più del testo dei messaggi, perché sono facili da elaborare per gli algoritmi di profilazione pubblicitaria. E su WhatsApp, questi dati sono il carburante per vendervi roba. Signal non raccoglie nulla di tutto questo. Zero.

Livello 3: Per i duri del terminale (sistemisti e smanettoni)

Se volete fare i raffinati e parlare a chi ha il terminale aperto sul secondo monitor, ecco le quattro differenze strutturali che fanno crollare il castello di carte di WhatsApp.

1. Il client closed-source (La scatola nera)

Il codice di Signal è interamente open-source (sia client che server). Potete andare su GitHub, compilarlo e verificare che non ci siano telemetrie o backdoor. Il client di WhatsApp è closed-source. Ti devi fidare di Meta. E nel nostro mestiere, fidarsi del codice chiuso di un'azienda che vive di sorveglianza di massa è un bug bloccante a livello logico.

2. Il protocollo Sealed Sender (Il mittente sigillato)

Nel routing normale, il server deve sapere chi invia il messaggio per consegnarlo al destinatario. Signal ha introdotto il protocollo **Sealed Sender**. In pratica, il mittente inserisce le proprie informazioni cifrate *dentro* la busta crittografica. Il server Signal legge solo l'indirizzo del destinatario all'esterno, consegna la busta e non ha idea di chi l'abbia spedita. Non viene registrata nessuna relazione di traffico.

Sealed Sender vs Routing Standard

Differenza tra routing classico (dove il server vede mittente e destinatario) e Sealed Sender di Signal (dove il mittente è nascosto dentro la cifratura).

3. La gestione della rubrica

WhatsApp carica in chiaro la vostra rubrica sui server di Meta. Signal usa un sistema basato su hashing crittografico locale e interrogazione

delle enclavi sicure sul server (Intel SGX). I numeri di telefono vengono verificati senza che il server di Signal possa mai conoscerli o salvarli in chiaro.

4. I backup sul cloud (Il capolavoro del "botch")

Questo è il capolavoro assoluto del pasticcio all'italiana targato Meta. WhatsApp vi spinge a fare il backup delle chat su Google Drive o iCloud. Di default, questi backup vengono caricati sul cloud in chiaro (o con chiavi gestite da Google/Apple). In pratica cifrate i dati per poi regalarli a chi gestisce lo spazio cloud. Signal non prevede backup su server terzi: i backup sono solo locali, cifrati con una passphrase forte a 30 cifre. Se volete spostarli, ve li gestite voi. Sicuro, ma senza pippe mentali per delegare la sicurezza a terzi.

Livello 4: Il suicidio organizzativo e di Stato (Per aziende e Governi)

Se a livello personale usare WhatsApp è solo pigrizia, a livello organizzativo — e ancora di più in un ente pubblico o governativo — è puro suicidio.

Eppure, quanti gruppi di coordinamento ministeriale, quanti canali di comunicazione tra sindaci e dirigenti girano su WhatsApp? Infiniti. Tonnellate di documenti riservati scambiati sulla piattaforma di Meta.

1. Il codice chiuso e lo spyware di Stato

Il fatto che il client sia closed-source lo rende una scatola nera impenetrabile. Nessuno può farne l'audit. E mentre vi fidate della parola di Meta, le agenzie di intelligence e i produttori di software di sorveglianza (avete presente *Pegasus*?) trovano zero-day nel codice per installare trojan governativi e rubarvi l'intera esistenza digitale.

WhatsApp è storicamente uno dei vettori preferiti per lo spyware di Stato. Grazie a vulnerabilità "zero-click" (dove basta ricevere una chiamata, anche senza rispondere, per essere infettati), diplomatici, funzionari e politici si sono ritrovati con i telefoni completamente violati. Con l'open source le falle verrebbero scovate molto prima. Con il codice chiuso, siete seduti su una mina con un timer casuale.

2. La perdita di sovranità digitale

Tutti i flussi di comunicazione dello Stato o della vostra azienda transitano sui server di Meta, azienda privata statunitense soggetta a leggi come il **FISA 702** e il **CLOUD Act**. Se l'intelligence americana decidesse di mappare le relazioni interne di un ministero italiano, le basterebbe imporre a Meta di consegnare i metadati. Avete appena regalato il vostro grafo sociale a una potenza straniera.

E per finire il pasticcio, i dipendenti pubblici fanno il backup di queste chat di lavoro sui loro account Google Drive o iCloud personali, esponendo dati sensibili dello Stato a ulteriori server terzi senza alcun controllo centralizzato.

Le uniche vie di fuga reali

Per un privato cittadino, un'azienda seria o un ente governativo, le soluzioni sono solo due. Non ci sono terze vie.

1. Matrix: La via sovrana per l'on-premise (Aziende e PA)

Per le organizzazioni complesse e la Pubblica Amministrazione, la scelta obbligata si chiama **Matrix**.

Matrix è un protocollo aperto e federato per la comunicazione cifrata in tempo reale.

- **On-Premise totale**: Lo Stato o l'azienda installano il proprio server Matrix all'interno dei propri datacenter. Tutti i messaggi, gli utenti e i log restano su macchine proprie. Nessun dato esce all'esterno.
- **Federazione sicura**: I server dei vari reparti comunicano tra loro in modo federato (es. il server del Ministero dell'Interno parla con quello della Difesa), ma mantengono il controllo assoluto sui propri server locali.
- **Open Source**: Il codice è interamente verificabile, escludendo rischi di backdoor silenti.

Non è fantascienza: la Francia ha creato **Tchap** (un client Matrix governativo per tutti i dipendenti pubblici) e la Germania usa **BundesMessenger** per le sue forze armate e amministrazioni. Loro hanno capito. Noi quando ci svegliamo?

2. Signal: Per il transito rapido e sicuro

Se non avete le risorse o la necessità di ospitare un server on-premise, ma avete bisogno di far comunicare al sicuro un team di persone o i vostri contatti personali, l'unica alternativa commerciale accettabile è **Signal**.

- **Cifratura impeccabile**: Il protocollo è lo stesso, ma qui il client è interamente open-source.
- **Minimizzazione dei dati**: Signal non memorizza metadati. Se qualcuno chiede i log di un utente, ottiene solo la data di creazione dell'account e l'ultima connessione.
- **Centralizzato ma pulito**: Certo, i server sono gestiti dalla Signal Foundation negli USA (quindi c'è comunque un elemento di centralizzazione), ma l'architettura è progettata per non sapere nulla di voi.

In conclusione

Continuare a usare WhatsApp per le comunicazioni personali, aziendali o istituzionali è da irresponsabili. Significa spalancare le porte a malware di Stato e regalare la sovranità dei propri dati a piattaforme proprietarie.

Se gestite un'organizzazione, spingete per l'adozione di Matrix on-premise. Se siete un privato o un piccolo team che deve coordinarsi in sicurezza senza pippe mentali di configurazione server, installate Signal. Ma fatevi un favore: disinstallate WhatsApp dai telefoni.

[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).