L'arte di non esserci: Anonimato e negabilità plausibile

L'arte di non esserci: Anonimato e negabilità plausibile

Nel magico circo di Internet, quando si parla di "privacy", la maggior parte della gente pensa a nascondere la cronologia del browser alla moglie o al datore di lavoro. Robetta. Roba da dilettanti.

Se saliamo di livello e iniziamo a parlare di crittografia e diritti digitali seri, ci scontriamo con due concetti che fanno venire il mal di pancia a qualsiasi agenzia governativa e che rappresentano le vere colonne portanti della difesa digitale: **l'anonimato** e la **negabilità plausibile**.

Cerchiamo di smontare questi concetti senza matematica per capire perché dovrebbero interessarci.

Anonimato vs Pseudonimato (Ovvero: no, il nickname non ci salva)

Partiamo dalle basi, perché c'è un malinteso gigantesco che gira sui forum.

Se ci creiamo un account su una piattaforma chiamandoci *HackerPippo99* e scriviamo post deliranti contro il sistema, noi **non siamo anonimi**. Siamo **pseudonimi**.

Lo pseudonimato associa tutte le azioni a un'identità fittizia (il nickname). Il problema è che se *HackerPippo99* fa tre post al giorno, si connette sempre dallo stesso blocco di indirizzi IP, ha uno stile di scrittura riconoscibile e scambia messaggi con le stesse persone, l'analista di turno ci metterà pochissimo a risalire alla nostra faccia. Lo pseudonimato crea un filo conduttore che unisce tutti i nostri comportamenti.

L'**anonimato vero**, invece, significa che ogni singola azione o messaggio non può essere ricondotto né a noi, né a un nostro alter-ego

fisso, né a un'azione precedente. È la totale assenza di fili conduttori.

Nel web normale l'anonimato è quasi impossibile da ottenere, perché i browser e i sistemi operativi sputano telemetrie come fontane. Ecco perché si usa la rete Tor o sistemi di routing particolari: per spezzare il legame tra la sorgente e la destinazione di ogni singolo pacchetto dati.

La Negabilità Plausibile: L'arma segreta della crittografia

Ma passiamo al pezzo forte: la **negabilità plausibile** (*plausible deniability*).

In parole povere, è la capacità di negare matematicamente e logicamente di aver compiuto un'azione, scritto un messaggio o posseduto un dato, in modo tale che nessuno possa dimostrare il contrario.

Non si tratta di mentire dicendo "non sono stato io" sperando che vi credano. Si tratta di fare in modo che la matematica stessa renda la vostra smentita perfettamente plausibile e indimostrabile.

Vediamo come funziona nei due scenari principali.

1. Nel disco fisso (Deniable Encryption)

Immaginate lo scenario classico del film di spionaggio: un'autorità coercitiva ci cattura, ci sequestra il portatile cifrato e ci punta una luce in faccia (o una minaccia di prigione) per costringerci a inserire la password. Se ci rifiutiamo, siamo spacciati. Se inseriamo la password, vedono i nostri file segreti.

Qui entra in gioco la cifratura denegabile (resa famosa da software come VeraCrypt). Il sistema permette di creare un **volume nascosto** dentro un altro volume cifrato.

- Noi creiamo un contenitore cifrato con password `A` contenente file innocui (le foto dei gattini, le ricette della nonna).
- Dentro lo spazio apparentemente vuoto di questo contenitore, creiamo un secondo volume nascosto con password `B` contenente i file sensibili.

Se ci costringono a dare la password, noi forniamo la password `A`. Il sistema si sblocca, mostra le ricette della nonna, e i dati sensibili restano indistinguibili dal rumore di fondo casuale che riempie lo spazio vuoto del disco. Matematicamente, è impossibile per chiunque dimostrare che esista una password `B` o un secondo volume nascosto. Noi possiamo negare in modo plausibile di avere altri dati.

2. Nelle chat (MAC simmetrici vs Firme digitali)

Nel mondo reale, se firmiamo un contratto con la penna, quella firma ci lega a quel documento. Nessun altro avrebbe potuto farla. In crittografia, le firme digitali a chiave asimmetrica (come GPG) funzionano nello stesso modo: se firmiamo un file con la nostra chiave privata, chiunque abbia la nostra chiave pubblica può dimostrare a un giudice che quel file lo abbiamo scritto noi. Zero negabilità.

Ma se parliamo di chat private, noi vogliamo l'esatto contrario. Vogliamo essere sicuri che la persona con cui stiamo parlando sia chi dice di essere (autenticazione), ma vogliamo anche che questa persona **non possa andare da un giudice e dimostrare che siamo stati noi a scrivere quei messaggi**.

I protocolli moderni (come OTR, Signal o SimpleX) risolvono questo paradosso usando le chiavi simmetriche e i **MAC (Message Authentication Codes)**.

- Quando Alice scrive a Bob, il messaggio viene autenticato con una chiave segreta condivisa *solo* da Alice e Bob.
- Bob sa che il messaggio viene da Alice perché lui non lo ha scritto, e solo loro due hanno quella chiave.
- Ma se Bob va da un giudice a mostrare la chat, Alice può dire: "Quella chiave ce l'aveva anche Bob. Poteva benissimo aver generato lui quel messaggio per incastrarmi".

Bob sa la verità, ma non può dimostrarla a terzi. Plausibile deniability matematica applicata alla conversazione.

Perché tutto questo è vitale?

C'è sempre il solito scafato che dice: "Ma io non faccio nulla di male, che mi frega della negabilità plausibile?".

Ci deve fregare eccome. In molti paesi, il semplice dissenso politico o il giornalismo investigativo sono considerati reati. Senza anonimato e negabilità plausibile, i whistleblower non potrebbero esistere, le fonti dei giornalisti verrebbero arrestate dopo cinque minuti e le comunicazioni personali sarebbero costantemente usate come prove nei processi farsa.

Questi strumenti non sono fatti per i criminali, sono fatti per proteggere l'integrità dell'essere umano di fronte a poteri asimmetrici. Sono le barriere matematiche che separano una società libera da una distopia di sorveglianza totale.

[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).