TECNOLOGIA DELLA PIATTAFORMA "SISTEMA DI SEGNALAZIONE ILLECITI DEL CASINÒ DI VENEZIA"

Il sistema di Whistleblowing si basa sulla piattaforma open source **GlobaLeaks**, un'architettura progettata secondo i principi di *security by design* e *privacy by default* per garantire l'assoluto anonimato del segnalante e la protezione dei dati sensibili.

Il Modello di Crittografia

GlobaLeaks implementa un solido modello di **crittografia nativa lato server (Zero-Knowledge / End-to-End applicativo)** combinato con protocolli di rete sicuri.

- **Protezione del Canale di Trasporto:** Tutti i dati scambiati tra l'utente e la piattaforma viaggiano attraverso la rete Internet in modo già protetto grazie al protocollo sicuro **HTTPS (TLS)**. Inoltre, per garantire il massimo livello di anonimato e la non-tracciabilità dell'indirizzo IP del segnalante, la piattaforma è nativamente integrata con la rete **Tor** (Servizi Onion).

- **Crittografia a Riposo (At Rest):** Una volta che i dati raggiungono il server, le informazioni relative alla segnalazione (messaggio, metadati e file allegati) vengono immediatamente crittografate prima di essere salvate. GlobaLeaks utilizza una combinazione di crittografia asimmetrica (PGP/GPG) e crittografia simmetrica avanzata.

Gestione dei Dati e Flusso delle Chiavi

I dati anagrafici del segnalante, se inseriti, vengono rigorosamente **separati fisicamente e logicamente** dai contenuti della segnalazione. Tutti i file allegati vengono cifrati singolarmente lato server prima della persistenza sul disco.

Soltanto i riceventi, in possesso esclusivo delle credenziali di accesso e delle chiavi private (PGP), sono in grado di decifrare e visualizzare il contenuto della segnalazione e l'eventuale identità del segnalante.

Flussi di Lavoro (Data Flow)

Flusso in fase di INVIO della segnalazione: Client (Browser/Tor) -> Transito cifrato (HTTPS/Tor) -> Ricezione Server -> Cifratura lato Server (PGP/AES) -> Salvataggio su Database e File System Cifrato

Flusso in fase di LETTURA della segnalazione: Caricamento dati cifrati dal Database -> Autenticazione del Ricevitore (RPCT) -> Decifratura tramite Chiave Privata -> Visualizzazione sicura sul browser del Ricevitore

Principali Tecnologie Utilizzate

GlobaLeaks adotta tecnologie altamente ottimizzate per la sicurezza e le performance:

- **Python:** Il cuore dell'applicazione (backend) è sviluppato in Python utilizzando il framework asincrono **Twisted**, che garantisce un controllo granulare sulle connessioni e sulla sicurezza della memoria.

- **React / JavaScript (ES6):** L'interfaccia utente (frontend) è una Single Page Application moderna, reattiva e priva di tracciamenti.

- **PostgreSQL / SQLite:** Utilizzo di database relazionali robusti con estensioni di cifratura avanzate.

- **GnuPG / OpenPGP:** Lo standard di riferimento per la crittografia asimmetrica delle chiavi e dei dati a riposo.

- **Tor Integration:** Integrazione nativa con i servizi Onion per l'abbattimento dei metadati di rete e la protezione dell'anonimato dell'IP.