GlobaLeaks come esempio di protezione architetturale

Claudio Agosti
Centro Studi Hermes
E-Privacy, Novembre 2013

Cos'è GlobaLeaks

- Software Libero

- 30 utilizzatori differenti
- 2 anni di vita del progetto
- Copre esigenze giornalistiche, cittadine, aziendali, pubbliche

Essays and Op Eds

News and Interviews

Audio and Video

Speaking Schedule

Password Safe

Cryptography

About Bruce Schneier

Contact Information

Take Back the Internet

Government and industry have betrayed the Internet, and us.

[...]

This is not the Internet the world needs, or the Internet its creators envisioned. We need to take it back.

And by we, I mean the engineering community.

Yes, this is primarily a political problem, a policy matter that requires political intervention.

But this is also an engineering problem, and there are several things engineers can -- and should -- do.

One, we should expose. If you do not have a security clearance, and if you have not received a National Security Letter, you are not bound by a federal confidentially requirements or a gag order. If you have been contacted by the NSA to subvert a product or protocol, you need to come forward with your story. Your employer obligations don't cover illegal or unethical activity. If you work with classified data and are truly brave, expose what you know. We need whistleblowers.

La reazione alle pressioni, Caso LavaBit

This illustrates the difference between a business owned by a person, and a public corporation owned by shareholders. Ladar Levison can decide to shutter Lavabit -- a move that will personally cost him money -- because he believes it's the right thing to do. I applaud that decision, but it's one he's only able to make because he doesn't have to answer to public shareholders. Could you imagine what would happen if Mark Zuckerberg or Larry Page decided to shut down Facebook or Google rather than answer National Security Letters? They couldn't. They would be fired.

https://www.schneier.com/blog/archives/2013/08/lavabit_e-mail.html

Il modello di minaccia

- Supponiamo la collezione dei *big data*:
  - Sia circoscritta allo stesso necessario
  - Sia fruibile solo dai legittimi utilizzatori
  - Sia monitorata al fine di evitare anomalie

- Questo non protegge da tecnologie con *backdoor* o con pressioni al reparto tecnico!

La situazione di GlobaLeaks 1/2

- L'obiettivo è sviluppare una piattaforma sicura per l'interazione tra whistleblowers e interlocutori
  - ... e in questi anni i whistleblowers hanno avuto un ruolo dirompente
  - Con diversi scenari di rischio
  - **Noi stessi parliamo di questi temi grazie ad un whistleblower**

La situazione di GlobaLeaks 2/2

- La separazione delle responsabilità e la distribuzione di privilegi di accesso è stata definita nell'architettura.

Gli attori

- Il whistleblower
- L'amministratore del servizio (uno diverso per ogni iniziativa)
- I destinatari dei dati (persone fidate scelte dall'amministratore del servizio)
- Gli sviluppatori e la community

L'amministratore

- Espone il servizio in rete anonima Tor
- E' il responsabile del servizio, pertanto la prima persona soggetta a pressioni.
- Non ha accesso ai dati che vi transitano
- Materialmente non dispone di dati identificativi degli utenti che accedono al nodo.
  - Niente log ed indirizzi IP

Il whistleblower

- Può essere chiunque disponga di un browser
- Traccie limitate sul computer utilizzato, facilmente rimuovibili (pulizia della cache e della history)
- Iniziativa *publeaks* ha sperimentato un sistema collaborativo per "inquinare i log" di aziende che monitorano https
- Può scegliere tra segnalazione anonima e confidenziale

I destinatari

- Sono gli unici che possono decifrare i dati a loro destinati (PGP)
- Possono interloquire con il whistleblower utilizzando la piattaforma
- Non hanno modo di entrare in contatto diretto con il whistleblower
- Utilizza un ambiente sicuro per proteggersi dal malware/trojan

Gli sviluppatori e la community

- Producono software libero
  - Verificabile da tutti per scongiurare l'inserimento di backdoor
  - Viene ciclicamente sottoposto ad attacchi informatici da parte di professionisti (*penetration test*)
- Non sono a conoscenza delle iniziative esistenti, ad eccezione di quelle che ci chiedono supporto.

Thanks!

http://logioshermes.org

https://globaleaks.org