# Riflessioni sulla crittografia open source[1]

di Enrico Zimuel

*“Se un sistema è veramente sicuro, lo è anche quando i dettagli divengono pubblici”*
Bruce Schneier

La crittografia è una scienza che studia le possibili tecniche di cifratura e decifrazione di un messaggio, ossia i modi per poter proteggere il contenuto di informazioni inviate su canali pubblici di comunicazione come, ad esempio, internet.

La crittografia tratta delle "scritture segrete" (significato etimologico della parola) ovvero i metodi per rendere un messaggio "offuscato" in modo da non essere comprensibile a persone non autorizzate.

L'open source è, essenzialmente, una filosofia di distribuzione del software legata alla presenza dei codici sorgenti e alla libertà di utilizzo degli stessi.

In informatica, *open source* (termine inglese che significa sorgente aperto) è un tipo di licenza per software, per la quale il codice sorgente di un'applicazione è lasciato alla disponibilità di eventuali sviluppatori, così che con la collaborazione (in genere libera e spontanea) il prodotto finale possa raggiungere una complessità maggiore di quanto potrebbe ottenere un singolo gruppo di programmazione.

## Che cos'è dunque la crittografia open source?

Si tratta per lo più di un aspetto già noto a chi si occupa di crittografia e di sicurezza informatica che ho voluto mettere in risalto tempo fa in un mio articolo [1] apparso sulla rivista italiana Linux & C. Questo neologismo consente di inquadrare meglio uno degli aspetti fondamentali legati al mondo della sicurezza informatica ed in particolare della crittografia, la “condivisione delle informazioni”.

Il mondo dell'information security si basa su un assunto fondamentale “non esiste un sistema sicuro al 100%” e soprattutto “la sicurezza è un concetto relativo”. Chi progetta sistemi di sicurezza è ben consapevole del fatto che prima o poi il suo sistema verrà violato, è solo questione di tempo.

Il fatto che non esista la sicurezza in senso assoluto di un sistema non implica che non si possano comunque progettare e organizzare sistemi realmente sicuri, è solo necessario introdurre il concetto di grado di sicurezza.

---

1 Articolo pubblicato nell’aprile 2005 nel sito dell’associazione professionale ISACA (Information Systems Audit and Control Association).

Quando si progetta un sistema di sicurezza bisogna sempre tener presente l'ambito d'applicazione e il livello o grado di sicurezza che si intende ottenere. Molto spesso il grado di sicurezza viene determinato attraverso l'analisi o la valutazione dei rischi (risk assessment) che coinvolge lo studio dei possibili scenari e delle probabilità del verificarsi di eventi dannosi (intrusioni esterne/interne, virus informatici, sicurezza fisica, etc).

In generale, non ha senso utilizzare un sistema di cifratura di livello militare, ad esempio un sistema One-time pad, per proteggere le fatture elettroniche prodotte da un'azienda.

Solo ragionando per gradi di sicurezza si riescono a progettare sistemi adeguatamente sicuri. Il problema non sembra quindi essere quello dalla sicurezza intesa in senso assoluto bensì quello di ottenere il livello di sicurezza adeguato per la realtà in cui si opera.

## Come stabilire questi livelli di sicurezza?

In questi ultimi anni ci sono state molte proposte di standardizzazione (TCSEC, ITSEC, ISO 17799, etc) si sono introdotte molte metodologie per l'organizzazione e l'auditing della sicurezza (BS 7799, ISO/IEC 15408, etc).

Uno dei principi fondamentali che dovrebbero essere presenti in tutti gli approcci al problema della sicurezza è quello della condivisione delle informazioni, perchè soltanto attraverso un sistema aperto di condivisione è possibile migliorare la sicurezza di un sistema e soprattutto è possibile stabilirne i limiti e di conseguenza il livello o grado di sicurezza.

La crittografia open source, dunque, può essere ricondatta a questo approccio di condivisione delle informazioni perchè soltanto attraverso la conoscenza dei dettagli di funzionamento di un algoritmo crittografico è possibile stabilirne la sua validità e quindi il suo livello di affidabilità (sicurezza).

A supporto di quanto detto, vorrei ricordare che l'approccio della condivisione delle informazioni e di conseguenza della possibilità, da parte di tutti, di conoscere i dettagli di funzionamento di un sistema crittografico è proprio un principio fondamentale della moderna scienza crittografica.

Questo principio fondamentale è noto in letteratura come il principio di Kerckhoffs: “la sicurezza di un sistema crittografico deve essere legata alla sola conoscenza della chiave”.

August Kerckhoffs pubblicò questo principio nel lontano 1883 in un suo celebre articolo [2] intitolato “La cryptographie militaire” nel Journal des Sciences Militaires sulle tecniche d’utilizzo della crittografia nella strategia militare.

Secondo questo principio la sicurezza di un sistema crittografico deve essere affidata esclusivamente alla conoscenza della chiave e quindi si deve dare per scontato che il “nemico” sia a conoscenza delle specifiche del cifrario o, per dirla in termini moderni, che sia a conoscenza dei codici sorgenti dell’algoritmo crittografico.

Il principio di Kerckhoffs, introdotto più di cento anni fa quando i computer erano ancora nei sogni di pochi visionari e i problemi legati alla privacy delle comunicazioni di massa non erano neanche agli albori, può essere considerato come il precursore di uno dei principi dell’open source: la libera diffusione dei codici sorgenti.

Certo, esso afferma semplicemente che si deve dare per scontato che le specifiche tecniche dei cifrari siano di dominio pubblico e non parla di libera circolazione del software ma adattandone il contesto ai giorni nostri se ne deduce che solo grazie ad una libera diffusione dei codici sorgenti, con il conseguente studio della validità tecnica da parte dell’opinione pubblica, si può ottenere sicurezza.

“Poiché la sicurezza non ha niente a che vedere con la funzionalità, il beta testing non può in alcun modo rilevare i problemi di sicurezza; l’unico modo di verificare che un sistema è sicuro è sottoporlo all’esame degli esperti per molto tempo e l’unico modo per ottenere il parere degli esperti è rendere pubblici i dettagli” così afferma Bruce Schneier, esperto di fama internazionale su temi di sicurezza e crittografia, nel suo libro *“Secret and Lies”* [3].

Da un principio puramente tecnico legato alla sicurezza dei sistemi crittografici segue dunque un principio “etico” legato alla libertà d’informazione, alla libera diffusione del software; a mio avviso, questa riflessione può essere considerata come un’ulteriore verifica della validità del fenomeno dell’open source soprattutto sui temi della sicurezza dell'informazione.

Il legame crittografia ed open source risulta quindi inevitabile, non si può ottenere sicurezza offuscando o addirittura nascondendo i dettagli tecnici, sono tanti gli esempi di sistemi di sicurezza informatici, basati su fantomatici algoritmi crittografici proprietari che si sono rivelati totalmente insicuri una volta resi noti i codici sorgenti.

La sfida della crittografia è proprio questa, rendere noti i particolari tecnici, i codici sorgenti, ma essere sicuri che nessuno riuscirà a violarli, almeno in tempi utili.

Questa apparente contraddizione può essere spiegata solo attraverso una comprensione profonda dei sistemi crittografici, nei quali la sicurezza è affidata alla matematica, il problema è che la matematica è una scienza pura e che molte volte non si adatta bene alla realtà fatta di persone che interagiscono, computer che sono programmati da persone e sui quali viene affidata la sicurezza delle nostre informazioni, “La matematica è assoluta, mentre la realtà è soggettiva. La matematica è qualcosa di ben definito, mentre i computer sono aleatori. La matematica è logica, mentre le persone sono fallibili,

capricciose e spesso incomprensibili” prosegue Schneier nel suo libro, per cui è bene tenere presente che la crittografia come scienza può essere considerata sicura ma le applicazioni crittografiche, poiché realizzate da esseri umani e non da numeri e teoremi hanno i loro difetti che possono in parte essere eliminati solo grazie all’open source e alla libera circolazione dei codici sorgenti.

## Riferimenti


1. Enrico Zimuel, *Introduzione alla crittografia open source*, Linux & Co., Piscopo Edizioni, Num. 27-28, ISSN 1129-2296, 2002
2. Auguste Kerckhoffs, *La cryptographie militaire*, Journal des Sciences Militaires, vol. IX, p. 5-38, janvier 1883
3. Bruce Schneier, *Secrets and Lies: Digital Security in a Networked World*, Wiley Editore, 448 pagine, ISBN 978-0-471-45380-2, 2004