



Come creare una cassaforte virtuale - (Fabio D'Apollo)

Ho scelto di trattare questo argomento nell'articolo perché ne sono appassionato e ultimamente ho avuto modo di dedicarmi di più a ciò e perciò credevo giusto di poter condividere con altri queste conoscenze per far sì che tutti possano usare la rete in modo più consapevole e difendere i propri dati.

A volte le informazioni che immagazziniamo possono essere veri e propri gioielli da dover custodire con attenzione. Per questo diventa utile avere a disposizione di esse un proprio luogo virtuale dove poterle riporre e sapere che nessun altro al di fuori di voi possa accedervi.

La crittografia si è occupata di questo nel corso della storia partendo dagli antichi cifrari ebrei di atbash, passando per il codice polialfabetico di Tritemio, la scrittura inversa di Leonardo da Vinci, fino al sistema del francese Vigenère, poi perfezionato nel 1918 con il celebre cifrario di Gilbert Vernam. Questo definito nel 1949 da Claude Shannon, padre della teoria dell'informazione, come l'unico metodo crittografico totalmente sicuro possibile.

Per farci un'idea era il "metodo" usato per il telefono rosso tra Washington e Mosca durante la Guerra fredda e quello per il cifrario ritrovato sul corpo del Che Guevara nel 1967.

La ricerca crittografica attualmente segue due filoni:

1. Quello della "crittografia simmetrica"
2. ...e quello della "crittografia asimmetrica"

Quest'ultima è basata sull'uso di chiavi diverse per cifrare e decifrare un messaggio (in pratica c'è una chiave per crittografare, che chiunque può conoscere, e una per decifrare che ha solo il destinatario).

Esiste anche una terza strada della ricerca crittografica e riguarda l'utilizzo della "meccanica quantistica" nella fase dello scambio della chiave. Siamo ancora agli albori di una realizzazione pratica, che risulta in realtà strettamente legata all'evoluzione della fisica teorica.

La soluzione più affidabile attualmente è il "metodo simmetrico" che risulta essere molto più semplice, veloce e sicuro, grazie all'utilizzo di "algoritmi specifici" che hanno il compito di codificare con livelli di sicurezza diversi in base all'esigenza dei vostri dati preziosi.

Ma quali sono gli algoritmi in circolazione a chiave simmetrica???

I più famosi sono "Blowfish" e le sue implementazioni come "AES", "Twofish" e "Serpent".

Blowfish ha una dimensione a blocchi di 64 bit e una lunghezza di chiave che può variare ben fra i 32 e i 448 bit e pochi sanno che Scheneier, l'autore che ideò Blowfish nel 1993, progettò l'algoritmo dichiarando che "doveva essere libero da brevetti e rimanere tale in tutte le nazioni", mettendo così a disposizione il codice sorgente.

Infatti è di pubblico dominio e può essere usato liberamente e in modo gratuito da chiunque, proprio come Linux.

L'AES, ovvero l'acronimo di Advanced Encryption Standard, conosciuto anche come "Rijndael", è invece un sistema di cifratura a blocchi di 128 bit con chiavi di lunghezza fino a 256 bit e ha uno sviluppo interessante che si basa su una rete a sostituzione e permutazione che lo ha reso celebre e per questo adottato come standard di sicurezza dalla "National Institute of Standards and Technology".

Il suo appellativo è derivato dai nomi degli inventori belgi Daemen e Rijmen, che lo presentarono per il processo di selezione come "Rijndael". (in fiammingo si pronuncia "rèin-daal") (Curiosità: persino l'AES può subire un attacco teorico chiamato XSL, il quale anche se matematicamente corretto, è impraticabile per l'enorme necessità di tempo che occorre.)

"Creare una cassaforte virtuale, o meglio un non-luogo criptato, non è una magia né un trucco, ma solo un gioco della matematica che attraverso numeri e lettere prende in giro se stessa." (Possibilmente mi farebbe piacere se faceste apparire questa frase nel video in sovrapposizione, nel vostro stile.)

Ma ora vediamo come si realizza in pratica tutto ciò di cui abbiamo parlato:

Se proprio non vi accontentate di un semplice lucchetto e siete stanchi di scrivere da destra verso sinistra come Leonardo, c'è la soluzione per custodire le preziose informazioni riservate nel vostro computer.

Si tratta di alcuni software che possono cifrare uno o più documenti e altri che invece sono in grado di creare unità virtuali cifrate, criptare partizioni del sistema o addirittura cifrare l'intero contenuto del disco fisso.

Sono a disposizione vari software, di cui una parte di loro sono a pagamento, altri invece totalmente gratuiti, ma tutti sfruttano le stesse tipologie di algoritmo per criptare e decifrare. L'unica vera differenza riguarda la maggior facilità o difficoltà nell'utilizzo di alcuni di essi in base alle proprie esigenze e necessità.

Apro una parentesi per mettere in evidenza l'importanza di proteggere le proprie informazioni soprattutto se si adoperano sistemi di "file sharing"(client server o peer to peer), con cui si mette fisicamente a disposizione di tutti, all'interno di una rete comune, una



parte del proprio hard disk diffondendo così involontariamente dati sensibili o aziendali. Ma anche la semplice navigazione sul web può essere vittima di spyware, per cui è sempre importante tutelarsi con sistemi di sicurezza per la vostra privacy, chiudo la parentesi.

Sembrerà inverosimile ma uno dei software più avanzati, in grado di assicurare la migliore prestazione per la sicurezza, è totalmente gratuito (open source) e si chiama True Crypt 5.1.

(per trovare il software su internet basta cercarlo in un motore di ricerca o altrimenti più comodamente sul sito www.ilsoftware.it)

Questo programma non è proprio facilissimo da usare, ma con un po' di pratica si può facilmente imparare a creare dischi virtuali cifrati da utilizzare come casseforti invisibili.

Abbiamo già detto che è un programma "open source" e inoltre è disponibile nelle versioni per Windows, Linux o MacOs a seconda del tipo di sistema operativo che avete scelto. Il software offre una vasta gamma di algoritmi per criptare i vostri dati, come AES, Blowfish, Twofish, Serpent, Cast5 o Triple DES oppure è possibile finanche utilizzare questi algoritmi a cascata per un livello di sicurezza estremamente elevato.

Dopo l'installazione basta cliccare su "create volume" visualizzato nella finestra principale... successivamente possiamo selezionare le opzioni di segretezza:

- "Create a file container" ci permetterà di realizzare un file crittografato... in pratica la nostra cassaforte virtuale. Basterà indicare nella sezione "Volume Location" il tipo di file (ad es. una pagina di word o blocco note) e poi scegliere l'algoritmo che preferiamo.
 - Il file segreto potrà essere standard o nascosto e una volta creato potrà essere montato cliccando "Select File" e poi il tasto "Mount", associando il file ad una lettera e digitando la password scelta; in tal modo il file sarà accessibile direttamente da "Risorse del computer"... comodo no???
 - E se il computer si spegne o viene riavviato cosa succede?
 - La cassaforte virtuale verrà automaticamente smontata e tutti i dati in essa contenuti saranno resi inaccessibili per chi non sarà in possesso della password.
- La seconda opzione "Create a volume within a non-system partition/device" permette invece di cifrare l'intero contenuto di qualsiasi partizione, come quello di drive secondari o unità removibili tipo chiavette USB.
- Non siete ancora soddisfatti??? La terza opzione riguarda la possibilità di crittografare l'intero "disco fisso" o una parte di esso, cliccando "Encrypt the system partition or entire system drive".
 - In tal caso il programma vi chiederà di effettuare automaticamente una copia di backup di tutti i contenuti del disco fisso per sicurezza.

Se questa soluzione appare complessa e difficile da realizzare... ci sono scorciatoie per rendere segreti i vostri dati.

Come ad esempio "EncryptOnClick" o "AxCrypt", software open source con algoritmo AES, con cui è possibile criptare e decodificare singoli documenti o folder. Basterà solo scegliere una password e selezionare il file da rendere segreto, così i vostri dati saranno custoditi in maniera facile e veloce.

Ora dovete avere solo qualcosa da nascondere!!!

Ma come si fa a ricordare poi tutte le diverse password delle varie casseforti virtuali???

Ci sono programmi open source come "Password Corral" che vi permettono di custodire a sua volta la "lista" segreta delle password, dando una linea guida alle sezioni crittografate e orientando tutte le vostre informazioni. In tal modo potrete legare tutte le password ad una sola e avere la lista sempre a portata di mano.

Ps: La lista dovrà a sua volta essere tenuta ben segreta per non consentire gli accessi a tutti gli altri dati ben custoditi.

Sarà però fondamentale per la sicurezza dei vostri dati la "scelta" della password. Una chiave molto lunga e composta da lettere, numeri e altri "segni particolari" potrà rendere le informazioni inviolabili da chiunque. Molti di questi programmi contengono anche un "Keyfile Generator" che potrà rendervi conto di quanto debba essere complessa una password per elevare la vostra sicurezza.

Concludiamo dicendo che in realtà la "crittografia" è ogni giorno insidiata dalla "crittoanalisi" che si occupa appunto di violare la prima. Perciò qualsiasi dato può considerarsi sicuro solo per un certo arco temporale, che può coincidere o meno con il proprio contesto storico senza doverne garantire la durata.

Fabio D'Apollò