Come faccio a proteggere i miei messaggi? – #loptis Reply

#loptis • Tags: cifratura, crittografia, email, GPG, paranoia, password, pdf, PGP, sicurezza

Stavo scrivendo due post contemporaneamente, ambedue al di fuori del filone HTML. Contemporaneamente, perché non riuscivo a decidermi a quale dare la precedenza, quando è arrivata questa domanda di Roberta:

> A proposito di sicurezza di dati…mandare documenti (ad esempio PDF di alunni) in modalità e mail con allegato oppure condividerli con Dropbox o Drive…come funziona… quali sono le modalità più sicure? E' possibile determinarle?

Come dicevo nella risposta al commento, son mesi che studio, sperimento e annoto per aggiungere un capitolo "sicurezza" nel laboratorio. Ma è un tema vasto e complesso. E poi è necessario calibrare l'intervento sulle necessità più frequenti e cogenti, colmando una distanza fra *utenti normali* e *smanettoni paranoici* che da vent'anni è rimasta tale e quale. Colgo quindi la palla al balzo per fare un inciso, poi continueremo con il resto.

Chi ha fretta può andare direttamente alla ricetta semplice.

Un po' di contesto

Qui *paranoico* è parola gergale, che sta a significare una marcata sensibilità ai temi della privacy, della sicurezza dei dati, della libertà di espressione. Paranoici di questo tipo tendono ad essere *smanettoni*, persone con competenze informatiche medio-alte, e non di rado sensibili ai temi dell'etica hacker.

Dovendo attenermi per un paio di mesi a temi più attinenti all'editing multimediale, avevo rimandato l'argomento della sicurezza, ma la risposta che voglio dare a Roberta mi consente di anticipare la questione, perlomeno da un punto di vista molto pratico. Certo, molti amici paranoici non gradirebbero questa risposta, me ne enuncerebbero le debolezze e mi suggerirebbero modi migliori. Dal punto di vista tecnico avrebbero perfettamente ragione, ma a che vale se poi i sistemi corretti sono usati solo da un ristretto manipolo di esperti? Vediamo allora di far passare un paio di concetti sani, insieme a una soluzione parziale ma accessibile – gli approfondimenti li riprenderemo dopo avere affrontato un po' di questioni inerenti all'editing multimediale.

Intanto chiariamo che il tema è molto vasto. Anche qui, onde evitare di perdersi inutilmente, focalizziamoci sulla questione suggerita da Roberta: inviare documenti in modo "sicuro". Ma che vuol dire sicuro? Consideriamo un attimo il caso delle email, alle quali potrei pensare di allegare i documenti. Traggo e riadatto dal tutorial su privacy e posta di Autistici/Inventati (gente che ne sa molto e fa cose ottime):

> La tua posta elettronica è a rischio in vari modi: quando spedisci un messaggio, per prima cosa il client di posta [1] che usi contatta un server attraverso un protocollo detto SMTP [Simple Mail Transfer Protocol] e trasferisce a quest'ultimo il messaggio. Questo trasferimento – di solito – avviene in chiaro (nessun tipo di cifratura viene applicato al messaggio [2]). Il server SMTP a sua volta contatta il server di destinazione, e il passaggio attraverso la rete è di nuovo in chiaro.

…

Le e-mail si spostano in rete attraverso una sequenza di copie effettuate da un server di posta – ad esempio quello del tuo Internet Service Provider (ISP), il fornitore d'accesso a Internet – su un altro server di posta.

Se per esempio abiti a Roma Nord e invii una mail a una persona che abita a Roma Sud, le copie che si creeranno della tua mail saranno perlomeno:

1. Il tuo computer (**copia originale**) invia la mail a un primo computer situato presso il tuo ISP (**copia 1**);
2. il computer dell'ISP manda la copia nel migliore dei casi direttamente ad un computer dell'ISP del tuo destinatario (**copia 2**). Ma i passaggi potrebbero essere di più;
3. il computer dell'ISP del tuo destinatario mantiene una copia della mail(**copia 3**), in attesa che quest'ultimo scarichi la posta (**copia finale**);).

Per attraversare solo qualche quartiere, insomma, la tua mail è stata salvata almeno 2 volte su 2 dischi fissi diversi (2 server server di posta degli ISP), e tutte e 2 le volte in copie perfette. E dietro ciascuno di questi dischi rigidi si nascondono imprese commerciali, informatici curiosi, amministratori pubblici dei generi più diversi, vari ed eventuali… Inoltre 2 copie è il caso migliore, se provi a visualizzare gli header delle mail che ricevi (ogni programma di posta ha un'opzione per farlo), vedrai che i passaggi sono molti più di 2, e di conseguenza anche le copie.

In teoria, per il momento queste copie multiple della tua mail dovrebbero essere cancellate nell'arco di qualche ora da ogni fornitore d'accesso. Tuttavia, le nuove leggi europee contro il "cybercrimine" e il disegno di legge Pisanu prevedono la conservazione di tutte le copie per diversi mesi, almeno per quanto riguarda le parti che indicano il mittente ed il destinatario.

Dunque:

spedire un'email è come spedire un cartolina postale, la differenza sta, come per tutte le cose del cyberspazio, in un potenziale di diffusione enormemente superiore e nell'impossibilità di andare a reperire e cancellare le tracce.

Naturalmente a maggior ragione, se uso servizi pubblici, come Dropbox o Drive, il mio documento è in mano a terzi…

Con questo, non si tratta di divenire (eccessivamente) paranoici ma di essere consapevoli di quello che si fa e, all'occorrenza, di sapere come "imbustare una lettera".

Ora, per imbustare una lettera veramente bene ci sarebbe un magnifico sistema noto come Pretty Good Privacy (PGP), qualcosa che suona come "decisamente buona privacy". Il sistema, inventato nel 1991 da Phil Zimmermann, detto in due parole, funziona nel modo seguente. Se **io** devo inviare in modo sicuro un messaggio a **te**, lo metto in un bauletto chiuso con un lucchetto particolare, dotato di due fori per due chiavi diverse. A **me**, per chiuderlo basta una chiave: è una chiave che **tu** mi avevi dato a suo tempo e che serve a chiudere il bauletto solo per **te**, è la **tua chiave pubblica**, che **tu** dai a tutte le persone con le quali vuoi comunicare. Quindi, chiudo il bauletto inserendo la **tua chiave pubblica** nell'apposito foro e **ti** spedisco il bauletto. **Tu**, quando l'avrai ricevuto lo dovrai aprire: ebbene, lo

potrai fare solo se userai un'altra chiave, **la tua chiave privata**, che conservi gelosamente e che non darai mai a nessuno. La inserirai nell'altro foro e solo allora potrai leggere il messaggio chiuso nel bauletto.

Affinché questo sistema possa essere usato bisogna che ognuno si procuri una coppia di chiavi, **quella privata** che conserverà accuratamente e **quella pubblica** che distribuirà a coloro con i quali desidera comunicare in maniera sicura.

Prima o poi torneremo su questo argomento, in particolare sull'uso di una particolare implementazione di PGP, che si chiama GPG (GNU Privacy Guard) [3], per ora ci accontentiamo di qualcosa di più semplice. Prima però occorrono un paio di precisazioni.

Fin qui abbiamo parlato di bauletti, lucchetti e chiavi, ma quali sono gli elementi reali di questo gioco? L'operazione di chiudere un documento in un bauletto allucchettato viene realizzata applicando un algoritmo di *crittazione* alla sequenza di bit che costituisce il documento. Mentre per leggere il documento dobbiamo applicare l'algoritmo inverso di decrittazione. All'atto pratico, la chiave per decrittare il documento è costituita da una password, anzi, nel caso di PGP, da una *passphrase*, che è più lunga – sulla questione delle password torniamo dopo. La crittazione che abbiamo descritto, cioè quella basata sulla coppia di chiavi pubblica e privata, si chiama *asimmetrica*, perché si usano due chiavi dalle funzioni diverse: quella pubblica chiude il messaggio e quella privata lo apre.

Esistono tuttavia anche chiavi *simmetriche*, sono quelle normali, che possono sia chiudere che aprire il messaggio: critto un messaggio con una password e poi per decrittarlo uso la stessa password. Ma perché non usare questo meccanismo che sembra così semplice e ovvio, invece di tutta quella complicazione delle doppie chiavi? La differenza è la seguente.

Se io ti invio un messaggio crittato con una chiave semplice ti devo inviare anche la chiave, e lo devo fare in un modo che ne preservi la segretezza, quindi non certo insieme al messaggio stesso! Magari te la dico a voce per telefono, oppure te la invio per SMS o qualche altro canale indipendente da quello del messaggio. Meglio di tutti se te la dico a voce quando ci si vede una volta, magari accordandosi sul fatto di usare sempre quella. Ma se poi scrivo ad un'altra persona allora va ripetuto tutto. E in ogni caso mi trovo nella condizione di avere le mie chiavi segrete a giro per il mondo.

Con il metodo delle chiavi doppie (crittazione asimmetrica), la chiave segreta non va mai da nessuna parte, la sua sicurezza sta tutta nella mia accortezza di conservarla adeguatamente. Perché il meccanismo funzioni basta che diffonda la mia chiave pubblica, che può andare a giro quanto si vuole. Anzi, per facilitare il meccanismo la posso appoggiare in un apposito server (*keyserver*) dal quale chiunque la possa ritirare. Ecco che cosa rappresenta il codice nella firma che metto ai miei messaggi di email, e che vedete riportata pari pari in fondo alla pagina di questo blog, a destra:

```
Key-ID: ECE6C950 - http://keyserver.linux.it
```

Il Key-ID è il codice identificativo della mia coppia di chiavi e http://keyserver.linux.it è l'URL del server delle chiavi pubbliche. Queste informazioni sono quelle minime necessarie per scrivermi un messaggio crittato.

E con la chiave doppia (crittazione simmetrica) la finiamo qui per davvero, per ora.

Ricetta semplice

Ciò che propongo, per dare una risposta di prima istanza a domande come quella di Roberta è di usare la crittazione simmetrica. E qui ci vuole la seconda precisazione:

in qualsiasi sistema di crittazione il fattore di sicurezza determinante è la qualità della password

E tanto vale enunciare il seguente principio:

la qualità di una password è proporzionale alla sua scomodità

Fatevene una ragione. Ecco i fattori che rendono **più sicura** una password

- lunghezza: meglio se almeno **15 caratteri**
- contiene sia **minuscole** che **maiuscole**
- contiene anche **numeri**
- contiene **simboli**, tipo: |!"£$%&/()=?^*;:_
- **non** è uguale ad una vostra **precedente password**
- **non** contiene il vostro **nome**
- **non** contiene il vostro **cognome**
- **non** contiene il vostro nome di **login**
- **non** è una parola che si trova nel **dizionario**
- **non** è un **nome proprio** di uso comune
- **non** è una **sequenza di caratteri sulla tastiera**, tipo: asdfg… o qwerty… o 12345…
- **non** è stato generata da un **servizio web di generazione di password**

Consapevole che se non vi sono rimasto antipatico fino qui forse ora ci son riuscito, provo a spiegare.

> In un tempo remoto e insicuro, un contadino voleva mettere in salvo il gruzzolo. Non del tutto convinto ma desideroso di trovare una soluzione ne prese una parte e andò a sotterrarlo in corrispondenza di una delle dieci viti nel filare che aveva davanti a casa. Era una cosa comoda e facile da fare. Inoltre per avere certezza di ricordarsi del luogo, scelse la settima vite, sette come i peccati capitali – roba che non si scorda.
>
> Passò del tempo finché un giorno uscendo di casa trovò sette buche, e il gruzzolo non c'era più. Si rammaricò assai, eccetto che del fatto di non essersi fidato troppo della propria furbizia, investendo solo una parte dei propri risparmi in quell'esperimento. Riflettendoci, capì i seguenti fatti:
>
> 1. non si ricordava come e quando, ma in qualche occasione doveva aver lasciato intendere qualcosa che aveva indotto qualcuno a scavare sistematicamente una buca per ogni vite del filare
> 2. 7 viti su 10 eran troppo poche, una notte bastava a scavare 10 buche
>
> Accidenti alla pigrizia! – concluse. Prese quindi il resto del gruzzolo, che ormai troppe erano le storie di furti nei casolari vicini, e si recò nella vigna grande, che aveva 100 filari di 100 viti. Andò da qualche parte nel mezzo, scegliendo per il filare e la vite in esso due numeri che non gli ricordavano nulla, e ci sotterrò il gruzzolo.

Non se ne seppe più nulla, speriamo per lui che lo strattagemma abbia funzionato per tutto il tempo che gli occorreva. A noi però la sua storia è servita per riflettere. La prima volta aveva usato una password troppo limitata: un solo carattere con sole dieci possibilità. Meglio sarebbe stato usare un filare più lungo, magari di 100 viti. Noi possiamo aggiungere tutte le lettere dell'alfabeto, quelle minuscole e quelle maiuscole e anche qualche simbolo strano. Ma meglio ancora sarebbe stato aggiungere un secondo carattere, cioè fare una password di due caratteri, anziché uno. Che è come dire aggiungere una dimensione: 100 viti per 100 viti fanno 10000 viti. Giustamente, il contadino aveva pensato che nessuno avrebbe potuto cimentarsi nell'impresa di scavare migliaia di buche in una notte – almeno con

quelle tecnologie, se fossero esistite le macchine scavatrici allora i calcoli sarebbero cambiati!

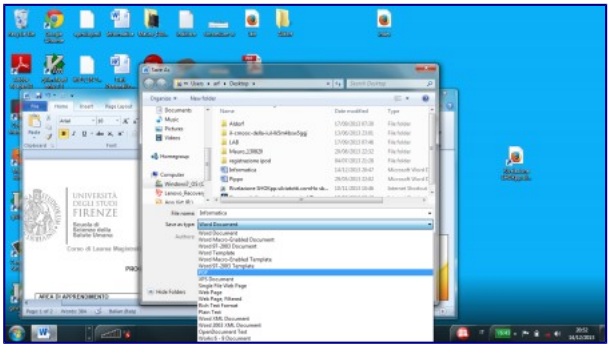
I sistemi per scardinare le password in buona parte sono del tipo “forza bruta” (*brute forse attack*): disponendo di computer sufficientemente veloci e di sufficiente tempo, si possono scoprire anche password apparentemente buone. Ecco perché conviene aumentare le dimensioni dello spazio nel quale scegliamo la nostra password, e questo lo possiamo fare con il numero di caratteri e con il numero di valori che può assumere ciascun carattere. Ma perché tutte quell’altre regole antipatiche che abbiamo snocciolato prima? Chi *cracca* password non si affida solo alla potenza del sistema di calcolo ma fa dei ragionamenti per restringere lo spazio probabile dove si trova la password o per iniziare ad esplorarne le zone che la gente tende ad usare. Quindi ogni craccatore che si rispetti, inizia da nomi e riferimenti privati se li trova, poi usa una serie di dizionari digitalizzati delle lingue appropriate, mostruose raccolte di vocaboli e simboli. E se scopre una password che funziona in qualche cosa, potrebbe poi andare a provarla anche in altri servizi protetti da password, e ne proverà anche delle varianti plausibili.

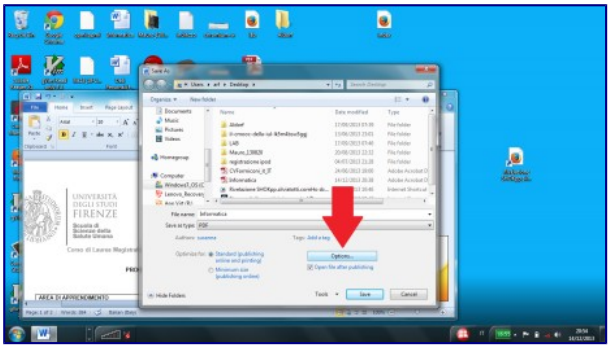
Antipatico eh? Spiace, non ho mezzo per indorare la pillola. Eccetto il fatto seguente: dipende, spedire un messaggio privato come se fosse un carico di plutonio è forse esagerato. Ma mettere il messaggio in una busta è decisamente sensato. Insomma, son sempre tutti pronti a rimpiangere com’era bello quando si scrivevano lettere ma ora ci fa fatica tutto… Scegliamo quindi una busta da poco, che è meglio di niente – e si turino però il naso eventuali amici paranoici che passassero da queste parti: prometto che con il tempo farò di tutto per accompagnare le persone verso lidi più sicuri.

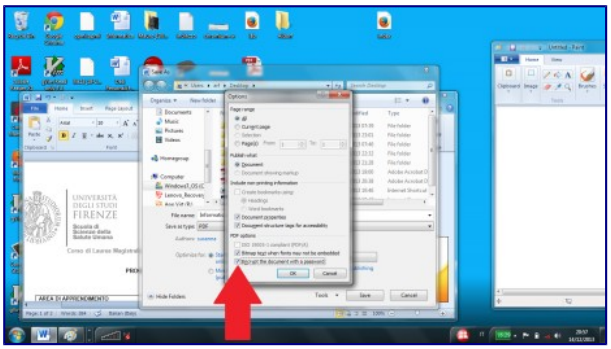
Ecco quindi la risposta a Roberta, per ora volta alla soluzione immediata del problema e limitatamente al suo caso: inviare in modo protetto un documento Word da un sistema Windows – tutta roba che non uso, ma mi sono messo nelle condizioni più simili possibile. Aggiungeremo varianti alla bisogna – Mac, Linux ecc.

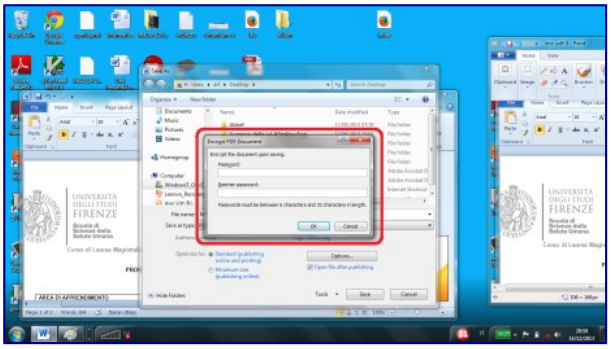
L’idea è di salvare in un documento PDF il documento Word e farlo in modo che si possa leggere solo se si conosce la password che gli abbiamo imposto. Purtroppo dispongo solo di un sistema in inglese, ma credo che sia facile dedurre i comandi in italiano – comunque, se qualcuno prova e scrive in un commento qui i comandi italiani gli do un più!

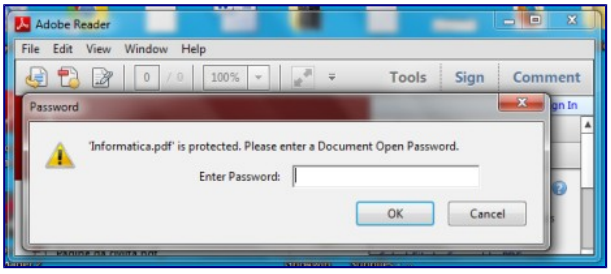
Salviamo il documento con **File->Save As** e chiediamo di farlo scegliendo il formato PDF. Cliccate il pulsante **Options**. Si apre una finestra in fondo alla quale si trova la casella **Encrypt the document with a password**: spuntate questa casella. Si apre un’altra finestra dove dovete scrivere la password due volte: il sistema vuole essere ragionevolmente sicuro che non abbiate commesso errori di battitura. Fatto. Ora chiunque voglia aprire quel documento con un lettore di PDF, tipo Acrobat Reader, deve inserire quella password.











A questo punto inviate il documento crittato come volete, via allegato email o servizio web, ma…

Due regole fondamentali:

1. cercare di attenersi almeno in parte alle succitate regole per la scelta della password
2. comunicate ai destinatari la password attraverso un canale indipendente e riservato

---

Note

- [1] Il client di posta è il programma che si usa per leggere e gestire le email, roba tipo Eudora, Oulook, Mail, Thunderbird, Mutt ecc. Molti usano direttamente un web server, ma il discorso non cambia.

- [2] Cifrare: rendere indecifrabile un’informazione in maniera che solo chi possiede la chiave corretta la possa recuperare.
- [3] GPG è software libero. Questo è un fatto fondamentale in fatto di crittografia e sicurezza, perché significa che gli algoritmi non si trovano sotto l’esclusivo controllo di nessuna terza parte. Può essere scaricato per tutti i sistemi operativi e può essere integrato in vari popolari client di posta, ma non tutti.