

# Reti e Sicurezza



Le reti stanno oramai espandendosi all'interno della nostra società, Internet oramai sta' entrando in tutti gli ambienti in cui viviamo: di per se questo non ha alcunché di pericoloso, semplicemente accresce le nostre potenzialità comunicative. Spesso pero' l'aspetto della sicurezza viene messo in secondo piano, o viene considerato una cosa per paranoici e aziende miliardarie; ebbene, questo e' assolutamente falso ed estremamente pericoloso, in quanto ci porta a considerare come sicuro un mezzo che sicuro non e' come Internet. Pensate, per esempio, che oggi esistono delle apparecchiature che a 200 metri di distanza sono in grado di percepire le radiazioni elettromagnetiche emesse dai monitor e quindi riprodurre quello che viene visto sul monitor stesso; oppure analoghi meccanismi con le tastiere, che permettono di individuare tutti i tasti che si premono (i.e. passwords, codici, etc..).

In realtà questo non è il vero pericolo, perché magari nessuno potrà mai mettere queste apparecchiature a controllare ogni singolo computer collegato sulla rete; il vero pericolo arriva dall'utilizzo della posta elettronica. E' bene sapere che tutto quello che noi spediamo come messaggi di posta elettronica transita sulla rete "in chiaro" e chiunque, con un minimo di "know-how", può leggere quello che e' scritto nella mail. Questo porta ad una semplice considerazione: se prima per controllare posta e telefono occorre autorizzazioni della magistratura nonché diverso personale per effettuarlo (e questo, di fatto, impediva un controllo generalizzato) ora per controllare un gran numero di e-mail che passano sulla rete e' sufficiente fare un programmino in C od in Pearl e farlo girare. Provate a pensare alla Digos che legge tutte le mail che contengono la parola "droga", o "comunismo", o "sistema"...

La domanda e' quindi: come difendersi da questo incubo orwelliano? Un metodo abbastanza semplice e' utilizzare un programma di crittografia per la posta elettronica che si invia sulla rete. Il sistema piu' semplice e potente che ora e' in circolazione e' il PGP (Pretty Good Privacy). Il PGP e' stato ideato da un tale Zimmermann, uno statunitense; il fatto di essere statunitense e' stato abbastanza problematico, in quanto gli Stati

Uniti classificano la crittografia come arma strategica e come tale ne vietano l'esportazione in forma elettronica (le versioni di Internet Explorer o Netscape che usiamo noi europei, anche in modalità sicura, sono di fatto insicuri, in quanto i codici utilizzati sono a pochi bits e non a molti bits come le versioni americane) . Siccome PGP era uscito dagli Stati Uniti, Zimmermann e' finito sotto processo. La versione attuale (6.02) e' finalmente perfettamente legale anche in versione internazionale, questo perché Zimmermann ha stampato tutti i sorgenti e la documentazione relativa al PGP, lo ha esportato sotto forma cartacea (e quindi non punibile) e lo ha riconvertito, al di fuori degli Stati Uniti, in forma elettronica, lavoro che e' costato molta fatica ma ha fatto si' che il PGP ora e' disponibile nella versione completa in tutto il mondo, senza che gli USA possano dire nulla. Potete scaricare PGP a [www.pgpi.com](http://www.pgpi.com), e' completamente freeware (gratis!) per uso non commerciale.

PGP si basa su due chiavi, una pubblica e l'altra privata. Un documento "chiuso" con la chiave pubblica puo' essere "aperto" solo con quella privata e viceversa; non e' possibile ricavare la chiave privata da quella pubblica o viceversa. Questo significa che se io voglio mandare una mail al Sig. X devo procurarmi la sua chiave pubblica (e questa e' a disposizione pubblicamente), usarla per "chiudere" la mail e spedirla. A questo punto solo il Sig.X con la sua chiave privata puo' aprirla e leggerla. Viceversa, se voglio essere sicuro che una mail mi arriva proprio dal Sig. X, lui chiuderà la mail con la sua chiave privata e se io posso aprirla con la sua chiave pubblica vuol dire che la mail mi arriva proprio dal Sig. X. Ovviamente alla base di questo c'è l'assunzione che la chiave privata sia effettivamente tale, e non lasciata accessibile a tutti!!

Per chi si diletta di matematica, il principio cardine su cui si basa PGP e' dato dall'impossibilità di dire se un numero  $n$  e' primo se non con algoritmi di complessità  $n$ . Questo fa' si che io possa prendere due numeri primi molto grandi (sono tabulati fino ad un certo numero) e li moltiplichino tra loro; il numero risultante e' divisibile solo per 1, per se' stesso, e per i 2 numeri primi, che diventano le due chiavi. Ovviamente poi l'algoritmo e' piu' complesso, ma se una mattina vi svegliate e trovate un algoritmo che e' in grado di decidere se il numero  $n$  e' primo con un algoritmo di complessità, diciamo,  $\log n$ , allora tutta la crittografia se ne va' a catafascio!! Insomma, e' opportuno imparare ad usare PGP per evitare di far leggere alla Digos (o alla CIA, peggio!!) tutto quello che scriviamo via e-mail... non lasciamo che il lavoro dell'Equipe di Zimmermann vada perduto!!!