La steganografia in pratica

Crittografia, Open Source, Privacy, Segretezza, Steganografia

ottobre 19, 2011

Sicurezza, Software

Se vi siete interessati alle problematiche connesse alla segretezza dei dati avrete sicuramente acquisito informazioni relative alle due principali tecniche utilizzate allo scopo, vale a dire la crittografia e la steganografia. Esse raggiungono lo stesso obiettivo partendo da due diversi approcci, mirando rispettivamente a proteggere ed a nascondere il messaggio scambiato tra due parti e per questo si prestano nella pratica a diversi casi d'uso.

Ma che cosa significa esattamente "nascondere il messaggio"? Se avete visto "A Beautiful Mind", il film dedicato alla vita del matematico e premio Nobel John Forbes Nash Jr., ricorderete che ad un certo punto il protagonista passa la quasi totalità del proprio tempo ad ispezionare giornali e riviste alla ricerca di messaggi segreti inviati dai traditori comunisti ai propri agenti negli Stati Uniti. Ovviamente non sarebbe stato possibile pubblicare messaggi palesemente crittografati su un quotidiano, perché i lettori e le autorità si sarebbero ben presto insospettiti e ne avrebbero bloccata la diffusione. L'intuizione del personaggio impersonato dall'attore Russell Crowe era invece che i destinatari a conoscenza della chiave di interpretazione (la prima lettera della seconda parola di ogni frase, per fare un esempio banale) potessero leggere, da quello che a tutti appariva essere un normalissimo articolo giornalistico, il messaggio a loro indirizzato. Intuizione fondamentalmente corretta, ma difficile da provare con i mezzi dell'epoca.

Ora torniamo al periodo attuale e pensiamo ad una fotografia memorizzata in formato digitale, nella quale ciascun singolo pixel é codificato nelle proprie componenti RGB. Se per alcuni pixels si modifica il bit meno significativo di una componente (facendo passare il valore R da 00001111 a 00001110 ad esempio), si ottiene una foto indistinguibile dall'originale ma che può recare (utilizzando più bits in più pixels) un messaggio se mittente e destinatario si sono preventivamente accordati su posizione ed ordine dei bits modificati. E' l'algoritmo noto come steganografia LSB (acronimo di Least Significant Bit) ed é applicabile ad ogni contenuto rappresentato in maniera digitale (audio e video).

Per fare qualche prova con questa tecnica possiamo utilizzare Steganography Studio, un tool open source esplicitamente sviluppato (in Java, quindi portabile su più ambienti) allo scopo di fornire uno strumento per lo studio degli algoritmi steganografici. All'interno dell'immagine che accompagna questo articolo ho inserito, mediante la funzione "Encode" di tale software, il logo del sito (il messaggio scambiato non è quindi necessariamente in forma testuale) utilizzando l'algoritmo SLSB (una variante di LSB che secondo l'autore possiede un maggior grado di immunità rispetto alle tecniche di steganalisi, con le quali un attaccante potrebbe essere in grado di dimostrare l'esistenza di dati nascosti all'interno di un contenuto multimediale). Il logo potrebbe essere ora estratto dall'immagine contenitore selezionando lo stesso algoritmo e la funzione "Decode" del software citato.

Steganography Studio é solo un tool didattico ma se abbiamo necessità concreta di utilizzare le tecniche di steganografia esiste un altro prodotto, ancora open source, veramente affidabile e completo. Mi riferisco ad OpenPuff, che é oltretutto in grado di utilizzare come contenitori multimediali non solo le immagini ma anche i files audio e video.