gen 10 2013

La Steganografia: Comunicare Come Una Spia

OpenPuff è uno strumento professionale di **steganografia.** La steganografia è una tecnica che si prefigge di nascondere la comunicazione tra due interlocutori. Spesso confusa con la **crittografia**, anche se in realtà esiste una differenza ben precisa tra i due concetti: lo scopo della crittografia è quello di nascondere il contenuto di un file o di un messaggio, mentre la steganografia si prefigge di nasconderne l'esistenza.

OpenPuff: Nascondi Tutte le Tue Comunicazioni

Essa nasce perché in molte situazioni il solo uso della crittografia non è sufficiente.Si pensi ad esempio ad un soldato che viene sorpreso a scambiare messaggi cifrati con un governo ostile: indipendentemente dal contenuto del messaggio, il solo fatto che vengono scambiati messaggi cifrati desta ovvi sospetti.

Le origini della steganografia sono antiche, il primo episodio di cui si ha notizia riguarda la civiltà persiana. Erodoto racconta la storia di un nobile che fece tagliare a zero i capelli di uno schiavo fidato al fine di poter tatuare un messaggio sul suo cranio; una volta che i capelli furono ricresciuti, inviò lo schiavo alla sua destinazione, con la sola istruzione di tagliarseli nuovamente.

Un altra possibilità molto praticata consiste nel nascondere il messaggio in un testo apparentemente innocuo. Una spia durante al seconda guerra mondiale inviò il seguente messaggio, il cui contenuto è apparentemente privo di valore:

> *Apparently neutral's protest is thoroughly discounted and ignored. Isman hard hit. Blockade issue affects pretext for embargo on by products, ejecting suets and vegetable oils.*

Ma basta prendere la seconda lettera di ogni parola per ottenere il messaggio:

> *Pershing sails from NY (r) June 1*

C'è una erre di troppo ma il messaggio è ampiamente comprensibile. Esistono varie tecniche simili, legate ad esempio al numero di virgole all'interno di una pagina, il cui numero tra 1 e 26 identifica una lettera. Certo è un metodo molto dispendioso poichè per ogni lettera bisogna trovare una pagina di testo, ma è ovviamente piuttosto complesso da individuare. Esistono altre varianti, come l'inchiostro simpatico o la tecnica dei micropunti, inventata dall'FBI durante la seconda guerra mondiale, ma con l'avvento delle tecnologie informatiche si sono aperte nuove potenzialità.

L'idea di base consiste nell'iniettare del testo in un file apparentemente di altra natura, ad esempio un immagine o un file musicale. Alterando leggermente ad esempio il colore di alucuni bit di sfondo, l'occhio umano non noterà alcuna differenza, ma questi bit modificati potrebbero nascondere un'informazione preziosa!
OpenPuff si occupa proprio di questo tipo di steganografia (detta iniettiva per ovvi motivi), in cui un file di testo viene "iniettato" in un altro file detto carrier. OpenPuff supporta come carrier diversi formati tra cui:

- Immagini (BMP, JPG, PCX, PNG, TGA)
- File Audio(AIFF, MP3, NEXT/SUN, WAV)
- File Video (3GP, MP4, MPG, VOB)
- File Flash/Adobe (FLV, SWF, PDF)

Inoltre il testo iniettato può essere crittografato in modo che anche se qualcuno intuisse la presenza del messaggio, non potrebbe in alcun modo distinguerlo da una serie casuale di lettere (a meno di intuire la crittografia e rompere l'algoritmo utilizzato). Chi volesse cimentarsi nello scambio di messaggi offuscati può visitare il sito di OpenPuff a questo link. Ricordiamo che si tratta di un **software gratuito e open source**, per il quale è presente anche un ottimo manuale in italiano (essendo l'autore del programma l'italiano Cosimo Oliboni)