



With financial support from the AGIS Programme
European Commission - Directorate General Justice, Freedom and Security
Contract nr. JAI/2004/AGIS/113 - December 2004

Raggruppamento Carabinieri Investigazioni Scientifiche Reparto Investigazioni Scientifiche di Roma – Sezione Telematica

Seminario Internazionale – Roma, 23 e 24 maggio 2005

Steganografia e Steganalisi

*Cesare Maioli e Antonio Gammarota
Facoltà di Legge
Università di Bologna*

Introduzione

La steganografia è l'arte di nascondere informazioni nelle informazioni così da non destare sospetti nonché il processo di introdurre informazioni in un canale nascosto così da celare le informazioni stesse. È uno strumento utile per la protezione delle informazioni personali, e le organizzazioni stanno investendo ingenti risorse nell'analisi delle tecniche steganografiche al fine di proteggere l'integrità dei propri dati.

D'altra parte la steganografia può anche essere dannosa. Ostacola le autorità che fanno rispettare la legge nel raccogliere le prove per fermare le attività illegali, poiché le tecniche per celare le informazioni stanno diventando più sofisticate.

Sebbene la steganografia sia utilizzata in varie forme da migliaia di anni, essa è diventata più nota recentemente in forza del suo utilizzo per mascherare le comunicazioni dei terroristi così come la pornografia minorile. La steganografia cela l'esistenza di un messaggio trasmettendo le informazioni attraverso vari "portatori". Il suo scopo è di premunirsi dall'individuazione di messaggi segreti. L'uso più comune della steganografia è quello di nascondere le informazioni di un file tra le informazioni di un altro file. Per esempio portatori di copertura come immagini, audio, video, testo o codice in forma digitale, mascherano l'informazione nascosta. Questa può essere testo non elaborato, testo cifrato, immagini o informazioni inserite in un flusso di bit.

Dato che i criminali sono ben consapevoli delle capacità degli investigatori forensi di recuperare fonti di prova dai computer, fanno sempre più ricorso a tecniche di crittografia per nascondere dati incriminanti. I pornografi minorili online usano la tecnologia della steganografia per realizzare comunicazioni private e per nascondere i files che si scambiano all'interno di normali files del computer. Ci sono più di 4.000 siti web dedicati alla steganografia e molti di questi forniscono informazioni su come scoprire e nascondere materiale illecito.

Steganografia

Le due principali branche dell'occultamento di informazioni sono la steganografia e del watermarking; la differenza fondamentale tra le due è che nel watermarking l'oggetto della comunicazione è il segnale principale, con annidati i dati che forniscono la protezione copyright; il messaggio contiene informazioni come l'identificativo del proprietario e un timestamp digitale che viene normalmente utilizzato per la protezione copyright. Nella steganografia l'oggetto da

trasmettere è il messaggio annidato, e il segnale di copertura serve come una innocua maschera scelta arbitrariamente dall'utilizzatore. Nel watermarking l'esistenza del mark può essere dichiarata apertamente e ogni tentativo di rimuovere o rendere nullo il contenuto annidato rende il segnale principale inutilizzabile. La steganografia cerca di evitare la capacità di scoprire della percezione umana e degli algoritmi informatici.

La steganografia differisce dalla crittografia la quale non cela i dati da comunicare ma li codifica per evitare che venga compreso il loro contenuto; le due tecniche sono considerate ortogonali e complementari: chiunque voglia comunicare in modo nascosto può applicare un algoritmo crittografico ai dati segreti e poi ricorrere al loro annidamento.

Le immagini sono la copertura più utilizzata nella steganografia e possono essere archiviati in vari formati (BMP, GIF, JPEG); il processo di mascheramento delle informazioni può essere riassunto in due passi: identificazione dei bits ridondanti che possono essere modificati senza degradare la qualità della copertura seguita dalla selezione di un sottoinsieme dei bits ridondanti da sostituire con i dati del messaggio segreto.

Le tecniche sono valutate in relazione alla loro sicurezza contro la rilevazione, la consistenza del carico (la quantità di dati da nascondere) e la robustezza contro attacchi non intenzionali e dolosi. Le tecniche sono classificate nei seguenti gruppi; per ciascuno di essi sono disponibili dei tools software:

- modificazione del Least Significant Bit (LSB); è applicata ai LSB dei pixels; la stegoimmagine è visivamente identica alla copertura;
- masking; i valori dei pixels nelle aree mascherate vengono alterati in una certa percentuale; viene realizzato una specie di patchwork in cui coppie di patches sono scelte a caso e i loro pixels cancellati e sostituiti da una pari quantità di dati;
- domain transform; i dati sono annidati secondo i metodi delle trasformate matematiche, per esempio modulazione dei coefficienti in una trasformata di dominio come il Coseno Discreto, Onda Discreta, Fourier Discreto; i dati mascherati sono sparpagliati all'interno dell'intera immagine e poi mescolati e sottoposti ad una trasformazione di secondo livello;
- compression; l'annidamento dei dati è integrata nell'algoritmo di compressione dell'immagine, come il JPEG; data la popolarità delle immagini JPEG su Internet queste tecniche hanno un grande potere attrattivo;
- spread spectrum; i dati nascosti sono sparsi all'interno dell'immagine copertura. Si utilizza una chiave per selezionare casualmente i canali di frequenza dei colori e poi si applica un processo di crittografia

Steganalisi

Anche se gli strumenti steganografici alterano soltanto i componenti meno significativi dell'immagine, essi lasciano tracce rilevabili nell'immagine stego; la steganalisi si riferisce all'evidenziazione della presenza di informazioni nascoste in un'immagine; si aggiunge che l'immagine copertura non è disponibile a chi la analizza.

L'idea più semplice per individuare file modificati è di confrontarli con l'originale: la soluzione normale per evidenziare informazioni nascoste è di costruire una libreria degli hash sets e di confrontarli con gli hash values del file sotto indagine; l'hash set identificherà le corrispondenze steganografiche del file. Gli investigatori devono utilizzare hash sets sicuri per escludere file affidabili dall'indagine. I file di sistema non modificati dopo la loro installazione sono da includere in un hash set sicuro. NIST ha iniziato il progetto di ricerca *Libreria Software di Riferimento Nazionale* che calcola un identificatore unico per ciascun file nel sistema operativo sulla base del

contenuto del file: gli identificatori sono creati utilizzando l'algoritmo SHA-1; se un criminale cerca di nascondere un'immagine pornografica rinominandola come un file ordinario del sistema operativo o rinominando un file .JPG come .EXE, l'hash value derivato dall'immagine non corrisponderà con quello dei file del sistema operativo e sarà così individuato.

La steganalisi include due principali tipi di tecniche:

- visual analysis; cerca di rilevare la presenza di comunicazioni segrete attraverso l'ispezione, sia attraverso la vista sia con l'aiuto di un sistema di computer, tipicamente decomponendo l'immagine nei suoi livelli di bit;
- statistical analysis; è in grado di rilevare se un'immagine è stata modificata testando se le sue proprietà statistiche deviano dalla norma. Può identificare minuscole alterazioni nel comportamento statistico causate dall'annidamento steganografico; sono disponibili molteplici metodi differenti, mirati per ciascuno dei differenti tipi di tecniche di annidamento sopra menzionate.

Anche se nei manuali delle forze dell'ordine degli USA (per esempio l'Istituto di Ricerca Americano dei Pubblici Ministeri) non sono disponibili delle linee guida sulla steganografia, ci sono regole empiriche che gli investigatori utilizzano quando cercano indicazioni che possano rivelare l'uso della steganografia; sono:

- capacità tecniche o sofisticazione del proprietario del computer;
- indizi software nel computer; per esempio nomi di file, riferimenti a siti web, cookies, file della cronologia, crittografia;
- file programma; per esempio editor hex, software per la pulizia dei dischi, software per specializzati per chat;
- file multimediali; per esempio file abbastanza grandi per l'utilizzo di steganografia con duplicazione;
- tipi di crimine; per esempio pornografia minorile, frodi contabili, furto d'identità, terrorismo.

Questioni legali

La steganografia e la steganalisi possono essere utilizzate dalle forze dell'ordine come strumenti ordinari per contrastare il crimine e, in particolare, la pornografia minorile.

Il Codice Italiano fornisce la legge n. 269 del 3 agosto 1998 come strumento principale per la lotta alla pornografia minorile; l'articolo 14 fornisce lo strumento di legge per accertare comportamenti illeciti ed autorizza gli investigatori della polizia ad agire sotto copertura per scoprire le responsabilità civili per atti illeciti e il traffico di materiale pornografico. Poche tecniche hanno superato l'esame di legittimità dei giudici e quindi sono considerati legittimati ed utilizzabili.

Altre tecniche come i *vasi di miele* sono stati dichiarati illegittimi dalla Corte di Cassazione (rif. 37074/2004) in relazione a pochi casi di mancanza di gravi illeciti. In accordo con questa decisione il ricorso ad un agente provocatore è permesso solo quando il suo comportamento non è in conflitto con le norme costituzionali e deve essere limitato a circostanze eccezionali nel rispetto degli obblighi legali e di rigide procedure. Al di fuori di queste clausole restrittive le attività non sono permesse, sono considerate illegittime e, in alcuni casi, illegali; pertanto gli indizi raccolti non sarebbero ammessi dalla Corte.

Vi è pertanto la necessità di definire nuove tecniche e nuovi strumenti che permettano l'individuazione, il contrasto e la punizione dei comportamenti illeciti, all'interno di una struttura di operazioni legali strettamente connesse con soluzioni tecniche di informazione e comunicazione di elevato livello.

Il succitato articolo 14 autorizza sia attività di acquisto sia di intermediazione. Se l'attività di intermediazione include l'azione dinamica di commercio (acquisto e vendita) di materiale pornografico minorile, allora le possibilità di successo nel contrasto del crimine potrebbero basarsi sulle nuove stego-tecniche e non più sui *vasi di miele*.

Le tecniche di steganografia possono essere utilizzate dalle forze dell'ordine per:

- contrassegnare con segni predefiniti, con tecnica steganografica, i materiali d'intermediazione, dopo l'autorizzazione e sotto il controllo del pubblico ministero;
- permettere il tracciamento del materiale scambiato;
- definire e fornire nodi nel network in cui monitorare lo scambio di materiale;
- progettare e realizzare una banca dati internazionale (seguendo il modello dell'Europol) per raccogliere dati sugli scambi, sotto il controllo degli enti investigativi;
- riunire ed analizzare le fonti di prova per verificare l'univocità di acquisto e scambio da parte della persona sotto indagine.

Conclusioni

La lotta tra steganografia e steganalisi rappresenta una parte importante del cyber-guerra con profonde implicazioni sulla sicurezza dei computer. Il tentativo di trasmettere messaggi segreti, sotto la copertura di innocui segnali multimediali, è in disaccordo con gli sforzi per rilevare e prevenire tali comunicazioni nascoste.

Dal punto di vista della legge, sono stati sviluppati diversi strumenti steganografici e solo alcuni sono disponibili online. Alcuni semplici metodi sono sconfitti dalla steganalisi ma contromisure contro la steganalisi stanno emergendo. Cominciano ad essere utilizzati strumenti steganografici che resistono agli attacchi statistici. Per esempio, nell'annidamento dei dati, si sta dedicando molta attenzione a preservare le caratteristiche statistiche del mezzo di copertura; per resistere agli strumenti di steganalisi basati sull'analisi dell'aumento dei colori unici in un'immagine, nuovi metodi di annidamento possono essere progettati per evitare la creazione di nuovi colori; in alternativa modificazioni che portino a parti rilevabili possono essere compensate, in maniere diverse, mentre si garantisce che il destinatario designato resti in grado di estrarre il messaggio segreto.

Dal punto di vista della legge si deve sottolineare che l'uso di tecniche stego da parte delle forze dell'ordine potrebbe incrementare le possibilità di presentare alla Corte, durante le fasi del processo, fonti di prova ben definite e verificate, riducendo così le possibilità di ricorso ed aumentando riscontri credibili nei confronti della persona sotto indagine. Il successo delle indagini della polizia aumenterebbe così come crescerebbe la cooperazione internazionale; in questo ambito la steganografia, utilizzata dagli organi di polizia trans-nazionali per marcare il materiale scambiato per via della condivisione delle banche dati internazionali, diventerebbe un importante strumento per il tracciamento, per esempio, dello scambio di pornografia minorile e per rendere le indagini più efficaci.

Riferimenti essenziali

- Amin M. M. et alii, *Information hiding using steganography*, IEEE, 4th National Conference on Telecomm Technologies, Malaysia, 2003
- Curran H., et alii, *An evaluation of image based steganography methods*, International Journal of Digital Evidence, v. 2, n. 2., Fall 2003
- Johnson N. and S. Lajodia, *Exploring steganography: seeing the unseen*, IEEE Computer, v. 31, n. 2, Feb. 1998
- Kessler G., *Steganography: implications for the prosecutor and computer forensics examiner*, Child Sexual Exploitation Update, APRI, v.1, n. 1, Summer 2004
- Li X. and Seberry J., *Forensics computing*, LNCS 2904, Springer, 2003
- Provos N. and P. Honeyman, *Detecting steganographic content on the Internet*, ISOC NDSS, San Diego, 2002
- Wang H. and S. Wang, *Cyber warfare: steganography vs. steganalysis*, CACM v. 47, n. 10, October 2004