Esteganografia

Autor:
Data de publicació: 03-09-2014

L'esteganografia és l'art i la ciència d'escriure missatges ocults de tal manera que només en conegui l'existència el destinatari previst; a diferència de la criptografia, en què l'existència del missatge per ell mateix no s'oculta, però el contingut és amagat. La paraula "steganografia" té origen grec i vol dir "escrit ocult o tapat". Els seus orígens es remunten a l'any 440 aC. L'historiador Heròdot va mencionar dos exemples d'esteganografia a les seves Històries. Demeratus va escriure un missatge per alertar d'un possible atac a Grècia, escrivint-lo en una tauleta de fusta i la va cobrir de cera. Les tauletes de cera s'utilitzaven com a superfície d'escriptura re-usable. Un altre exemple de l'ús de l'esteganografia fou practicat per Histiaeus, que rapava el cap dels seus esclaus més fidels i els tatuava un missatge. Quan el cabell els creixia, el missatge quedava ocult. El propòsit d'aquests missatges fou instigar una revolta contra els perses. Més tard, Johannes Trithemius va escriure Steganographia, un tractat de criptografia i esteganografia disfressat de llibre de màgia negra.

Normalment, un missatge esteganogràfic aparentarà ser una altra cosa: una fotografia, un article, una llista d'anar a comprar, o algun altre missatge. Aquest missatge aparent és el text tapadora. Per exemple, un missatge es podria ocultar fent servir tinta invisible entre les línies visibles d'un document inofensiu.

L'avantatge de l'esteganografia sobre la criptografia sola és que els missatges no atreuen l'atenció a si mateixos, als missatgers, o als destinataris. Un missatge codificat no ocult generarà sospites per molt robust que sigui el mètode criptogràfic i pot resultar incriminador per si mateix, ja que en alguns països l'encriptació és il·legal.

L'esteganografia utilitzada en les comunicacions electròniques inclou codificacions esteganogràfiques en la capa de transport, com per exemple en un fitxer MP3, o en un protocol com UDP.

Un missatge esteganogràfic (el text clar) sovint s'encripta primer per mètodes tradicionals, i després el text tapadora es modifica en certa manera per contenir el missatge encriptat (text xifrat), resultant en un text esteganogràfic. Per exemple, la mida de lletra, l'espaiat, l'estil o altres característiques del text tapadora es poden manipular per dur el missatge ocult. Només el destinatari (que ha de conéixer la tècnica usada) pot recuperar el missatge i desxifrar-lo. Se sap que Francis Bacon va suggerir aquesta tècnica per ocultar missatges (Xifratge de Bacon).

En la segona guerra mundial, s'usaven molt els "microfilms". Consistia a microfilmar un missatge i reduir-lo fins a l'extrem d'un punt, de forma que podia passar com un signe de puntuació d'un caràcter dins d'un altre text. Per exemple, el punt d'una "i" podia ser en realitat un microfilm amb un missatge. Un cop rebut el missatge amb el microfilm, s'ampliava el microfilm projectant amb una llum a una superfície blanca per a poder fer llegible el missatge vertader.

A continuació s'il·lustra i s'esquematitza la síntesi d'un procés esteganogràfic i la seva necessitat, tenint en compte el conegut cas de "El problema del presoner" (GJ Simmons, 1983).[1]

La idea és enviar el missatge ocult (E) "embegut" en un missatge d'aparença innòcua (C) que servirà de coberta. A això se li aplica una funció de esteganografia {displaystyle f(E)}, que amb una clau associada (K) permet extreure el missatge (necessària encara si es coneix l'algorisme esteganográfico). Després, missatge ocult i la coberta formen

l'objecte de l'esteganografia (O), que pot enviar per un canal insegur i ser vist sense problemes pel guardià. Finalment, l'altre presoner rep l'objecte compost i, aplicant la funció inversa {displaystyle f(O)} = {displaystyle f(E)} -1 , pot recuperar el missatge ocult.[2]

Com poden comunicar dos presoners, per exemple, per acordar un pla de fuga, si estan en cel separades i tots els missatges que intercanvien passen a través d'un guardià?

Claus:

No s'hauria d'utilitzar només criptografia. Com ja es va esmentar, xifrar els missatges només oculta el significat però no el fet que hi ha un missatge. Si el guardià veu que hi ha un missatge, encara que no pugui entendre, sospitarà immediatament dels presoners.
Els missatges han de semblar innocus. Només així el guardià passarà el missatge entre els presoners sense adonar-se que estan tramant en contra.
L'esquema ha d'estar preacord entre les parts, perquè les parts (els presoners) puguin desxifrar el missatge.

Sota les condicions de l'escenari anterior, el com l'esteganografia ajudaria, es descriu en el diagrama de la dreta.

Contingut

Història

Aquests són alguns exemples i/o històries que demostren que l'esteganografia ha estat present des de temps antics i constantment va evolucionant.

Heròdot

Probablement un dels exemples més antics de l'ús de l'esteganografia sigui el referit per Heròdot en Les històries .[3] En aquest llibre descriu com un personatge va prendre un quadernet de dos fulls o tauletes; ratllar bé la cera que les cobria i en la fusta mateixa va gravar el missatge i el va tornar a cobrir amb cera regular. Una altra història, en el mateix llibre, relata com un altre personatge havia rasurat a navalla el cap del seu esclau de més confiança, li va tatuar el missatge al cuir cabellut, va esperar després que li tornés a créixer el cabell i el va enviar al receptor del missatge, amb instruccions que li rasurés el cap.

Segle XV

El científic italià Giovanni Battista della Porta va descobrir com amagar un missatge dins d'un ou cuit. El mètode consistia en preparar una tinta barrejant una unça d'alum i una pinta de vinagre, i després s'escrivia a la closca. La solució penetra en la closca porosa i deixa un missatge en la superfície de l'albúmina de l'ou dur, que només es pot llegir si es pela l'ou.

Portada d'un exemplar de Steganographia

Primer llibre

L'origen del vocable esteganografia es remunta a principis del segle XVI. L'abat alemany Johannes Trithemius va escriure un llibre al qual va titular Steganographia en el qual es tractaven temes referents a l'ocultació de missatges, així com mètodes per conjurar els esperits. El llibre en qüestió està avui considerat com un llibre maleït i és molt apreciat pels esoteristes del món sencer. A part d'aquest llibre, també va publicar Polygraphiae Libri Sex, un compendi de sis llibres en criptografia que no participava dels elements esotèrics del seu altre gran llibre.

Altres llibres

Al Somni de Polifilo (Hypnerotomachia Poliphili, Ed Aldus Manutius) , escrit per Francesco Colonna el 1499, es pot obtenir la frase 'poliam frater Franciscus Columna peramavit '(' El germà Francesco Colonna estima apassionadament a Poli ') si es pren la primera lletra dels trenta-vuit capítols.
Gaspar Schott (1665) Schola steganographica.
Ian Caldwell, Dustin Thomason (2004) Enigma del quatre.

Segona Guerra Mundial
Durant la Segona Guerra Mundial es van usar els microfilm és, en els punts de les i's o en signes de puntuació per enviar missatges. Els presoners usen i, j, tyf per ocultar missatges en codi morse. Però un dels sistemes més enginyosos es coneix amb el nom de "Null CIPHA".[4] Aquest últim consisteix en enviar un missatge, del més comú possible, i triar certa part d'ell per amagar el missatge. Un exemple és el text següent: Apparently neutral's Protest is thoroughly descartaven and ignored. Isman hard hit. Bloqueig issue Affects pretext for però on by products, ejecting suets and Vegetable oils . (Pel que sembla la protesta neutral és completament descomptada i ignorada. Isman afectats. Qüestió de bloqueig afecta pretext d'embargament sobre els productes, aconsegueix expulsar sèu i olis vegetals)

Si prenem la segona lletra de cada paraula apareix el missatge: Pershing Sails from NYr June i (velers Pershing des de Nova York l'1 de juny).

Tintes invisibles
No està clar des de quin època es van començar a utilitzar, però sens dubte s'han fet servir al llarg de la història i fins a l'actualitat. Les més conegudes es poden classificar en dos Categories

Bàsiques: substàncies amb alt contingut en carboni: llet, orina, suc de llimona, suc de taronja, suc de poma, suc de ceba, solució ensucrada, mel diluïda, coca cola diluïda, vi, vinagre, etc. Bàsicament, sense importar quina de les "tintes" esmentades s'utilitzin, a escalfar la superfície on es va escriure el missatge invisible, el carboni reacciona apareixent el missatge en un to cafè.

Més sofisticades: apareixen després d'una reacció química, o després de ser exposades a la llum de certa longitud d'ona (infraroig, ultraviolat, ...).

Esteganografia clàssica vs. moderna
Esteganografia "clàssica": mètodes completament foscos.[5]

Protecció basada en desconèixer el canal encobert específic que s'està usant.

Esteganografia moderna: ús de canals digitals:

fitxer de text (inc. pàgines web, codi font, etc.)
Àudio digital
Imatges i vídeo digitals
fitxers executable s
Protocols de comunicacions

Tècniques digitals
Existeixen nombrosos mètodes i algorismes utilitzats per ocultar la informació dins d'fitxers multimèdia: imatges, àudio i vídeo. A continuació s'indiquen alguns dels més usats.

Emmascarament i filtrat (Masking and Filtering)
En aquest cas la informació s'oculta dins d'una imatge digital utilitzant marques d'aigua que inclouen informació, com el dret d'autor, la propietat o llicències. L'objectiu és diferent de la esteganografia tradicional (bàsicament comunicació encoberta), ja que és afegir un atribut a la imatge que actua com a coberta. D'aquesta manera s'amplia la quantitat d'informació presentada.

Algorismes i transformacions (Algorithms and Transformations)
Aquesta tècnica oculta dades basades en funcions matemàtiques que s'utilitzen sovint en algorisme s de la compressió de dades. La idea d'aquest mètode és amagar el missatge en els bits de dades menys importants.

Inserció en el bit menys significatiu (Least Significant Bit Insertion)
Aquest és el mètode modern més comú i popular utilitzat per esteganografia, també és un dels anomenats mètodes de substitució . Consisteix en fer ús del bit menys significatiu dels píxels d'una imatge i alterar. La mateixa tècnica pot aplicar-se a vídeo i àudio, encara que no és el més comú. Fet així, la distorsió de la imatge en general es manté al mínim (la perceptibilitat és pràcticament nul), mentre que el missatge és escampat al llarg dels seus píxels. Aquesta tècnica funciona millor quan l'fitxer d'imatge és gran, té fortes variacions de color ("imatge sorollosa") i també avantatja com més gran sigui la profunditat de color. Així mateix aquesta tècnica pot utilitzar-se eficaçment en imatges a escala de gris, però no és apropiada per a aquelles en color de 8 bits paletitzades (mateixa estructura que les d'escales de gris, però amb paleta de color). En general, els millors resultats s'obtenen en imatges amb format de color RGB (tres bytes, components de color, per píxel).

Exemple:

El valor (1 1 1 1 1 1 1 1) és un nombre binari de 8 bits. Al bit situat més a la dreta se l'anomena "bit menys significatiu" (LSB) perquè és el de menys pes, alteracions canvia en la menor mesura possible el valor total del nombre representat.

Un exemple d'esteganografia: Ocultació de la lletra "A". Si es té part d'una imatge amb píxels amb format RGB (3 bytes), la seva representació original podria ser la següent (3 píxels, 9 bytes):

(1 1 0 1 1 0 1 0) (0 1 0 0 1 0 0 1) (0 1 0 0 0 0 1 1)

(0 0 0 1 1 1 1 0) (0 1 0 1 1 0 1 1) (1 1 0 1 1 1 1 1)

(0 0 0 0 1 1 1 0) (0 1 0 0 0 1 1 1) (0 0 0 0 0 1 1 1)

El missatge a xifrar és 'A' la representació ASCII és (1 0 0 1 0 1 1 1), llavors els nous píxels alterats serien:

(1 1 0 1 1 0 1 1) (0 1 0 0 1 0 0 0) (0 1 0 0 0 0 1 0)

(0 0 0 1 1 1 1 1) (0 1 0 1 1 0 1 0) (1 1 0 1 1 1 1 1)

(0 0 0 0 1 1 1 1) (0 1 0 0 0 1 1 1) (0 0 0 0 0 1 1 1)

Observar que s'ha substituït el bit del missatge (lletra A, marcats en negreta) en cada un dels bits menys significatius de color dels 3 píxels. Van ser necessaris 8 bytes per al canvi, un per cada bit de la lletra A, el novè byte de color no es va utilitzar, però és part del tercer pixel (la seva tercera component de color).

El mètode del LSB funciona millor en els fitxers d'imatges que tenen una alta resolució i fan servir gran quantitat de colors. En cas d'fitxers d'àudio, afavoreixen aquells que tenen molts i diferents so és que tenen una alta taxa de bits.

A més aquest mètode no altera en absolut el mida de l'fitxer portador o coberta (per això és "una tècnica de substitució"). Té el desavantatge que la mida de l'fitxer portador ha de ser major com més gran sigui el missatge a embeure; es necessiten 8 bytes d'imatge per cada byte de missatge a amagar, és a dir, la capacitat màxima d'una imatge per emmagatzemar un missatge ocult és del seu 12,5%. Si es pretén emprar una major porció de bits de la imatge (per exemple, no només l'últim, sinó els dos últims), pot començar a ser percebut a l'ull humà l'alteració general provocada.

Tècniques més utilitzades segons el tipus de mitjà
Cetel
L'ús d'esteganografia en els documents pot funcionar amb només afegir un espai en blanc i les fitxes als extrems de les

línies d'un document. Aquest tipus de esteganografia és extremadament eficaç, ja que l'ús dels espais en blanc i tabuladors no és visible per al ull humà, almenys en la majoria dels editors de text, i es produeixen de forma natural en els documents, de manera que en general és molt difícil que aixequi sospites.

En imatges [6]

Exemple utilitzant tècnica de LSB.

El mètode més utilitzat és el LSB, ja que per a un ordinador un fitxer d'imatge és simplement un fitxer que mostra diferents colors i intensitats de llum en diferents àrea s (píxels). El format d'imatge més apropiat per ocultar informació és el BMP color de 24 bits Bitmap), ja que és el de major proporció (imatge no comprimida) i normalment és de la més alta qualitat. Eventualment es prefereix optar per formats BMP de 8 bits o bé altres com ara el GIF, per ser de menor mida. S'ha de tenir en compte que el transport d'imatges grans per Internet pot despertar sospites.

Quan una imatge és d'alta qualitat i resolució, és més fàcil i eficient ocultar i emmascarar la informació dins d'ella.

És important notar que si s'oculta informació dins d'un fitxer d'imatge i aquest és convertit a un altre format, el més probable és que la informació oculta dins quedi malmesa i, conseqüentment, resulti irrecuperable.

En àudio [6]
Quan s'amaga informació dins d'fitxers d'àudio, generalment la tècnica utilitzada és low bit encoding (baixa bit de codificació), que és similar a la LSB que sol emprar-se en les imatges. El problema amb el low bit encoding és que en general és perceptible per al sentit humà, pel que és més aviat un mètode arriscat que algú ho faci servir si estan tractant d'ocultar informació dins d'un fitxer d'àudio.

Spread Spectrum també serveix per amagar informació dins d'un fitxer d'àudio. Funciona mitjançant l'addició de sorolls a l'atzar al senyal que la informació s'oculta dins d'una companyia aèria i la propagació en tot l'espectre de freqüències.

Un altre mètode és Echo data Hiding , que usa els ecos en fitxers de so per tal de tractar d'ocultar la informació. Simplement afegint extra de so a un ressò dins d'un fitxer d'àudio, la informació pot ser amagada. El que aquest mètode aconsegueix millor que altres és que pot millorar realment el so de l'àudio dins d'un fitxer d'àudio.

En vídeo [6]
En vídeo, sol utilitzar el mètode DCT (Discrete Cosín Transform). DCT funciona canviant lleugerament cadascuna de les imatges al vídeo, només de manera que no sigui perceptible per l'ull humà. Per ser més precisos sobre com funciona DCT, DCT altera els valors de certes parts de les imatges, en general les arrodoneix. Per exemple, si part d'una imatge té un valor de 6,667, l'aproxima fins a 7.

Esteganografia en vídeo és similar a l'aplicada a les imatges, a més de la informació està oculta en cada fotograma de vídeo. Quan només una petita quantitat d'informació que està oculta dins del codi font en general no és perceptible a tots. No obstant això, com més informació es oculti, més perceptible serà.

Altres
Una nova tècnica esteganográfica implica el injectar retards (coneguts per la seva traducció a l'anglès com "delays") imperceptibles als paquets enviats sobre la xarxa del teclat. Els retards en el clic dels comandaments en alguns usos (telnet o programari de escriptori remot) poden significar un retard en paquets, i els retards en els paquets es poden utilitzar per a codificar dades.

Esteganálisis
El que la esteganografia essencialment fa és explotar les limitacions de la percepció humana, ja que els sentits humans no estan capacitats per buscar fitxers que tenen informació amagada dins d'ells, encara que hi ha algorismes disponibles que poden fer el que s'anomena esteganálisis (Steganalysis).

Com que la esteganografia és invasiva, és a dir, deixa empremtes en el mitjà de transport utilitzat, les tècniques de esteganálisis es basen en com detectar aquests canvis.

Eines
Aquesta és una selecció de eina s tant per amagar missatges com per descobrir-los.

Eines per esteganografia
MP3Stego
MP3Stego oculta informació en fitxers MP3 durant el procés de compressió. Les dades són primer comprimits, xifrats i després amagats en el flux de bits.

http://www.petitcolas.net/fabien/steganography/mp3stego/

JPHide i JPSeek
JPHIDE i JPSEEK són programes que permeten amagar un fitxer en una imatge jpeg.

http://linux01.gwdg.de/# alatham/stego.html

BlindSide Cryptographic Tool
El Blindside pot amagar un fitxer (o fitxers) de qualsevol varietat, dins d'una imatge de mapa de bits de Windows (fitxer BMP).

http://www.mirrors.wiretapped.net/security/steganography/blindside/

GIFShuffle
El programa GIFShuffle s'utilitza per ocultar els missatges d'imatges GIF de remenar el mapa de colors, el que deixa la imatge visible sense canvis. GIFShuffle treballa amb totes les imatges GIF, incloent aquelles amb transparència i animació, ia més proporciona compressió i xifrat dels missatges ocults.

http://www.darkside.com.au/gifshuffle/

WbStego
wbStego és una eina que oculta qualsevol tipus de fitxer de mapa de bits en imatges, fitxers de text, fitxers HTML o fitxers PDF d'Adobe. L'fitxer on s'oculten les dades no és òpticament canviat.

http://wbstego.wbailer.com/

StegoVideo
MSU StegoVideo permet amagar qualsevol fitxer en una seqüència de vídeo. Quan el programa va ser creat, diferents còdec populars es van analitzar i es va elegir un algorisme que preveu la pèrdua de dades petits després de la compressió de vídeo. Podeu utilitzar MSU StegoVideo VirtualDub com a filtre o com a programa. Exe autònom, independent de VirtualDub.

http://compression.ru/video/stego_video/index_en.html

StreamSteganography
StreamSteganography és una Classe PHP que permet escriure i llegir cadenes que es troben ocultes en els bits menys significatius d'una imatge.

http://deerme.org/articles/view/12-esteganografa-en-php-oculta-informacin-en-imgenes

Eines per estegoanálisis
Stegdetect
http://www.outguess.org/download.php

Steganography Analyzer Signature Scanner (StegAlyzerSS)
StegAlyzerSS té la capacitat per escanejar tots els fitxers en els mitjans de comunicació en què se sospita la presència de patrons de byte hexadecimal o signatura s, en particular aplicacions de esteganografia en els fitxers. Si una signatura coneguda es detecta, pot ser possible extreure la informació amagada.

http://www.sarc-wv.com/stegalyzerss.aspx

Digital Invisible Ink Toolkit
Aquest projecte proporciona una eina simple que pot amagar un missatge dins d'una imatge de color de 24 bits. Tot i sabent com s'incrusten, o realitzant anàlisi estadística, no per això és més fàcil trobar la informació oculta.

http://sourceforge.net/project/showfiles.php?group_id=139031

VSL: Virtual Steganographic Laboratory
http://vsl.sourceforge.net/

Vegeu també

Estenotípia.
Francesc de Paula Martí Mora.
Trampa per a canaris

Referències

? G. J. Simmons, "The Prisoner's problem and the subliminal channel", publicat a "Advances in Cryptology - crypto '83", D. Chaume, ed., Plenum Press, 1984, 51-67
? Arturo Ribagorna G., Juan Estévez-Tapiador i juliol Hernández, "esteganografia, Esteganálisis i Internet. Descobrint el revers d'Internet: web mining, missatges ocults i secrets aparents".
? Tábara, Luís. Breu Història de la Criptografia Clàssica.
? Roberto Gómez Cárdenas, "l'esteganografia". Article publicat a la revista Bsecure de març del 2004
? esteganografia Clásiva Vs Moderna, i Conceptes bàsics burmeste/CIS5371-Crypto/Steganography.ppt
? Anar a :6,0 6,1 6,2 http://www.infosecwriters.com/text_resources/pdf/Steganography_AMangarae.pdf

Bibliografia

Peter Wayne, Disappearing Cryptography
Information Hiding-Techniques for Steganography and Digital watermarking editat per Stefan Katzenbeisser i Fabien, AP Petitcolas
Neil F. Johnson, Zoran Duric i Sushil Jajodia, Information Hiding: Steganography and watermarking-Attacks and Countermeasures

Articles

QuickStudy: Steganography: Hidden Data En computerworld.com (anglès)
Steganography Articles, Links, and Whitepapers En Forensics.nl (anglès)
Exemples que demostren les imatges ocultades en altres imatges
FBI Article: An Overview of Steganography for the Computer Forensics Examiner (anglès)
Cryptography and Steganography (versió web de diapositives de PowerPoint), 2002. Elonka Dunin 'presentació d'una descripció de esteganografia, així com una discussió de si Al - Qaida va poder haver utilitzat esteganografia per planejar els atacs de l'11 setembre 2001 (anglès)
Steganography & Digital watermarking - Papers i informació relacionada amb la esteganografia i el esteganálisis per Neil F. Johnson des de 1995 fins al present (anglès)
Detecting Steganographic Content on the Internet, 2001. Paper by Niels Proves and Peter Honeyman, Center for Information Technology Integration, University of Michigan (anglès)
mercantil/Rights Protection for Natural Language Text, inclou diversos articles sobre aquest tema
Steganography Project, includes articles on network steganography (Wireless LAN and VoIP) - provided by Krzysztof Szczypiorski and Wojciech Mazurczyk. (anglès)
Principle and applications of BPCS-Steganography, Paper original de BPCS-Steganography (anglès)
Channels in the TCP/IP Suite - Paper de 1996, de Craig Rowland detallant l'ocultació d'informació en paquets

TCP/IP (anglès)

Articles de esteganàlisi

Steganography Analysis and Research Center (SARC) Un centre de la seguretat que proporcionen les eines per a la detecció i l'extracció de esteganografia, així com l'entrenament de l'examinador de l'esteganálisis (anglès)
Cyber Warfare: steganography vs. steganalysis Per a molts mètodes i eines llestos que són desenvolupats per ocultar la informació en dades de multimèdia, un nombre igual de mètodes llestos i eines que s'estan desenvolupant per detectar i revelar els seus secrets (anglès)
"Detecting Steganographic Content on the Internet", PDF 813 KB (anglès)
Alguna pàgines d'exemples Schott's Schola steganographica (anglès)
Group Un exemple de la investigació en curs sobre esteganografia (anglès)
steganography applications Exemples pràctics en com un cert nombre de programaris de esteganografia treballa (anglès)