Tajomstvá steganografie

História nás naučila chrániť si svoje tajomstvá, či už ide o vojenské tajomstvá, konkurentov v priemysle, alebo o snahu ochrániť sa pred intrigami a úkladmi. Na druhej strane sa môžeme usilovať o získanie výhod tým, že sa dostaneme k tajomstvám iných.

Už od počiatku civilizácie existovali spôsoby, ako ochrániť informácie. Najznámejším z nich je kryptografia, ktorá je dnes diskutovanejšou témou ako kedykoľvek predtým. Existujú však aj iné, dokonca ešte staršie metódy, o ktorých sa hovorí veľmi málo. Príkladom môže byť steganografia, ktorá je témou tohto článku. Na prvý pohľad sa zdá, že je iba chudobnou príbuznou kryptografie, ale nie je to celkom tak.

V minulosti bola steganografia pred kryptografiou uprednostňovaná a s príchodom výpočtovej techniky a internetu znova naberá na sile. Akoby prežívala renesanciu, jej využitie je stále reálnejšie a účinnejšie.

Steganografiu spolu s watermarkingom možno zaradiť pod termín ukrývanie informácií. Technológie ukrývania dát sa do popredia dostali najmä po roku 1996, keď sa konala prvá konferencia venovaná tejto téme. Zaujala tak odbornú verejnosť, ako aj priemyselné kruhy. Odvtedy steganografia zažíva búrlivý rozvoj. Ten je podporený aj reštrikciami, ktoré sú uvalené na používanie kryptografie. Štáty si totiž chcú ponechať možnosť nahliadnuť ponad plece komukoľvek, aby mohli zhodnotiť, či nevyvíja činnosť, ktorá sa prieči zákonom alebo záujmom štátu. Kryptografia by im v tom mohla brániť, a preto jej používanie obmedzujú zákonmi. Reakciou je zvýšené používanie steganografie, ktorá zatiaľ nie je obmedzovaná. Ďalším podnetom pre záujem o steganografiu sú správy, že ju používajú teroristi, čo zvyšuje atraktivitu tejto témy u laickej verejnosti.

Steganografia disponuje širokou paletou rôznych techník. O časti z nich si môžete prečítať vo vloženom článku o histórii steganografie. V tomto článku sa budeme zaoberať najmä tými, ktoré súvisia s výpočtovou technikou a internetom. Najčastejším médiom na ukrývanie dát sú obrázky, a preto aj väčšina príkladov uvedených v tomto článku bude založená práve na nich.

TERMINOLÓGIA

Slovo steganografia má základ v gréčtine a znamená tajné písanie. Je to veda zaoberajúca sa ukrývaním správ do iných správ. V steganografii sa používa niekoľko základných výrazov. Cover medium znamená obálku, teda médium, do ktorého sa ukrýva správa. Tá sa nazýva embedded message. Ak používame heslo, nazýva sa to stegokey. Výsledkom je potom stego-medium.

KRYPTOGRAFIA

Veľmi dôležité je vysvetliť rozdiel medzi kryptografiou a steganografiou a pochopiť ich vzájomný vzťah.

Kryptografia sa snaží správu pozmeniť použitím matematických operácií tak, aby nebola čitateľná pre nikoho, kto neovláda postup jej dešifrovania. Správa sa teda posiela verejnými informačnými kanálmi a každý ju môže bez problémov počuť alebo vidieť. Predpokladá sa pri tom, že nikto okrem adresáta ju nebude schopný rozlúštiť. Preto sa vyvíjajú čoraz zložitejšie kryptografické techniky, ktoré majú správu zašifrovať stále zložitejším spôsobom.

Existujú totiž metódy, ako sa k pôvodnej správe dostanú aj tí, ktorým nebola určená. Tieto metódy využívajú najmä tajné služby, vojsko, ale aj priemyselná špionáž a podobne.

V dešifrovaní výdatne pomáhajú počítače, ktoré sú schopné svojou hrubou výpočtovou silou rozlúštiť aj dokonale šifrované správy. V kryptografii sa preto niekedy hodnotí kvalita šifry aj tým, ako dlho bude počítaču s určitým výkonom trvať rozšifrovanie danej správy. Za dobrú šifru sa považuje taká, ktorej doba rozšifrovania je dlhšia ako doba, po ktorú musí byť zašifrovaná správa utajená.

Steganografia používa inú technológiu. Stegospráva nie je nijako upravená, a ak ju nájde niekto nepovolaný, bez problémov si ju prečíta. Podstatou steganografie je však snaha ukryť správu tam, kde by ju nikto nehľadal. Správa je teda ukrytá v inej, neškodnej správe a môže sa dostať ku komukoľvek, pretože nikto okrem adresáta si ju nevšimne.

Steganografia a kryptografia sa teda navzájom dopĺňajú. Kryptografia urobí správu nečitateľnou a steganografia neviditeľnou. Každú z technológií možno použiť osobitne, ale ich vzájomnou kombináciou, ktorá sa takmer nikdy nevylučuje, možno dosiahnuť oveľa vyšší stupeň utajenia. V praxi takmer všetky steganografické programy disponujú aj možnosťou použiť slabšie alebo silnejšie šifrovanie.

TERORIZMUS

Steganografia sa dostala do popredia záujmu aj v súvislosti s terorizmom. Teroristi totiž s obľubou využívajú internet v kombinácii so steganografiou. Scenár môže byť napríklad takýto:

Teroristi získali fotografiu objektu, ktorý je ich cieľom. Steganograficky ju ukryjú do fotografie obrazu známeho maliara a uložia na internetovú stránku zaoberajúcu sa umením. Odtiaľ si fotografiu tohto obrazu stiahne príjemca, ktorý môže byť na opačnej strane zemegule. Pomocou steganografického softvéru extrahuje fotografiu cieľového objektu.

Daná fotografia je prístupná aj širokej verejnosti a môžu si ju stiahnuť mnohí iní. Krása steganografie je v tom, že nevedia, že práve v tejto fotografii je ukrytá stegospráva.

Obr. 1 Na obrázku vpravo je originál, fotografia vľavo obsahuje steganograficky ukrytú fotografiu základne v Menwith Hill, ktorú vidíte vpravo dole. Obidva obrázky sú na pohľad takmer identické a majú obidva rovnakú veľkosť v KB. Použitý bol program S-tools.

WATERMARKING

Veľkým problémom počítačovej éry je ochrana digitálneho obsahu pred nelegálnym kopírovaním. Spôsobov, ako ho ochrániť, je mnoho, ich účinnosť je však diskutabilná. Jednou z možností je tzv. watermarking, technológia príbuzná steganografii.

V procese watermarkingu sa do digitálneho diela vkladá ďalšia informácia, buď v podobe obrázka, alebo čísla, prípadne textu. Táto informácia sa pri bežnom prezeraní diela nezobrazuje, dá sa však zobraziť pomocou špeciálnych nástrojov. Vďaka tomu je možné identifikovať majiteľa autorských práv k danému dielu. Typickým príkladom je digitálna fotografia. Jej autor do nej vloží svoje meno, priezvisko alebo ľubovoľné iné údaje a potom ju môže pokojne ponúknuť na publikovanie. Keby ju niekto digitálne publikoval bez jeho súhlasu a tvrdil by, že autorom je on, vložená informácia by to vyvrátila. Podobne je to možné v prípade akéhokoľvek digitálneho obsahu, ako je video alebo zvuk.

Watermarking je veľmi podobný steganografii, ale má určité špecifiká. Je predovšetkým robustnejší, pretože predpokladá, že dôjde k snahe vyextrahovať watermark z digitálneho obsahu. Ten môže byť úplne zjavný a dobre viditeľný, na rozdiel od stegosprávy, ktorá je ukrytá.

Niektoré spoločnosti ponúkajú watermarking spolu s technológiou prehľadávania internetu. Neustále sťahujú z internetu obrázky a kontrolujú, či majú watermark a či v ich databáze je záznam o tom, že tento obrázok je v danej webovej lokalite legálne. Ak nie je, upozornia na to majiteľa autorských práv.

Opísaný scenár údajne nepoužil nik iný ako Bin Ládin pri plánovaní útoku na dve ambasády USA vo východnej Afrike v roku 2001.

V tejto súvislosti je steganografia veľmi nebezpečná pre vyspelé krajiny, ktoré si zakladajú na tom, že vďaka výkonným počítačom dokážu rozlúštiť kryptosprávy. Steganografia však ich technologickú výhodu eliminuje a dáva tak teroristom šancu.

INTERNET

Steganografia má jednu nevýhodu. Na ukrytie správy určitého typu potrebuje oveľa viac správ podobného typu ako „krovie“. Ak chcete na ukrytie použiť ako obálku obrázok, potrebujete stovky iných obrázkov, aby sa medzi nimi ten váš nenápadne stratil. Túto nevýhodu účinne eliminuje internet, ktorý je súčasne novým motorom pre rozvoj steganografie.

Internet je skutočným kyberpriestorom, ktorého veľkosť je úchvatná. V súčasnosti sa vymkol spod kontroly a nikto nie je schopný efektívne ho riadiť. Vyhľadávače, ktoré skenujú internet nepretržite, dokážu nájsť iba zlomok jeho obsahu. Predpokladá sa, že to môže byť dokonca menej ako jedno percento. Odhadovaný objem informácií publikovaných na internete totiž môže presiahnuť až 500 miliárd dokumentov, pričom najväčšie vyhľadávače sa teraz blížia k hodnote 4 mld. indexovaných dokumentov. Počet obrázkov, ktoré sú na skrývanie dát najatraktívnejšie, je odhadovaný na 28 miliárd. V takomto obrovskom priestore, ktorý nepodlieha žiadnej kontrole, nie je problém ukryť nijaký dokument. Dokonca je tu možné ukryť obrovské množstvo informácií.

Kuriozitou je, že do jedného obrázka môže ukryť svoju správu pomocou rôznych softvérových nástrojov aj niekoľko ľudí bez toho, aby o sebe navzájom vedeli, a dokonca bez toho, aby dokázali rozlúštiť správu toho druhého.

Informácie vďaka internetu ľahko prenikajú aj cez hranice, a tak nie je možné zabrániť prenosu správ počas vojen za frontovú líniu alebo do krajín, na ktoré je uvalené embargo.

VÍRUSY

Čo možno uložiť ako stegosprávu? Odpoveď znie: všetko, čo sa dá zapísať v binárnom kóde. Môžu to byť textové správy, zvuk, obrázky. Teoreticky aj video, kde, samozrejme, narážame na problém kapacity stegomédia.

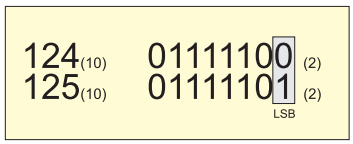
Ak sa do médií dajú vložiť akékoľvek dáta a ich objem môže byť až niekoľko kilobajtov, nie je žiadny problém ukryť do nich aj vírusy a červy. O tejto možnosti sa v tichosti diskutuje.

OBRÁZKY

Obrázky sú ideálnym médiom na ukrývanie stegospráv. Majú obrovskú kapacitu, obrázok vo formáte BMP s rozlíšením 1024 × 768 bodov v 24-bitových farbách má veľkosť 2,25 MB.

Existujú dva typy kompresie obrázkov, a to bezstratová a stratová. Bezstratová má rovnaké množstvo údajov o obrázku pred kompresiou aj po nej. Je vhodnejšia na steganografiu a používajú ju obrázky typu BMP a GIF. Stratová kompresia dokáže ušetriť veľa miesta potrebného na uloženie obrázka, ale za cenu vypustenia časti informácií. Po kompresii teda obrázok neobsahuje toľko informácií ako pred kompresiou. Túto kompresiu používa formát JPG. Práve pre stratovú kompresiu sa tento formát menej odporúča na steganografické účely.

Obrázok si možno predstaviť ako maticu čísel, pričom každé z nich predstavuje číslo príslušnej farby. Čiernobiele obrázky majú iba jednu maticu, ktorej čísla predstavujú odtiene sivej. Farebné obrázky sú zložené akoby z troch matíc, každá pre jednu farebnú zložku, ktorými sú červená (R) zelená (G) modrá (B). Každý bod je zložený z týchto troch zložiek. Hodnota odtieňa sivej farby je v rozmedzí od 0 do 255 a takisto každá zložka R, G, B má hodnotu od 0 do 255. Dajú sa teda zakódovať do 8 bitov. Dve farby, ktoré sú v palete v tesnej blízkosti, to znamená, že ich číselná hodnota sa líši o 1, napríklad farba číslo 124 a 125, sú také príbuzné odtiene, že človek si nemusí uvedomiť ich vzájomnú zámenu v obrázku. Súčasne sa tieto farby líšia v bitovom zápise iba posledným, najmenej dôležitým bitom, ktorý sa nazýva Least Significant Bit (LSB). V praxi vyzerá binárny zápis týchto dvoch čísel takto:



Obr. 2

V dobre vybraných prípadoch je teda možné zameniť farbu bodu za veľmi podobnú farbu tak, aby sa to vo výslednom obrázku neprejavilo výraznými zmenami. Znamená to, že pre výsledný obraz je prakticky jedno, ako vyzerá LSB. Vytvára sa tak priestor na uloženie dodatočnej informácie ľubovoľného charakteru. Informácia je zapísaná v binárnom tvare, a to tak, že do každého LSB bitu každého bajtu obrázka sa zapíše 1 bit stegosprávy. Teoreticky je teda možné zapísať do obrázka BMP stegosprávu s kapacitou 1/8 pôvodného BMP. V prí-

Obr. 3

pade spomínaného obrázka je to až 288 KB. To je slušná kapacita pre celú knihu alebo pre viacero obrázkov vo formáte JPG.

Ako vidieť z obrázka č. 3, na ktorom je vľavo médium bez stegosprávy a vpravo médium so stegosprávou, iba bity v sivých poliach boli skutočne zmenené, pretože ostatné LSB bity sa náhodou zhodovali s tými, ktoré bolo potrebné zapísať. Podľa teórie pravdepodobnosti potom možno povedať, že iba jednu polovicu z LSB bitov bude potrebné pozmeniť. To je dôležité preto, aby sa pôvodná snímka menila čo najmenej. Vcelku bolo zo všetkých bitov nesúcich informáciu o bodoch obrázka zmenených iba 6,25 %.

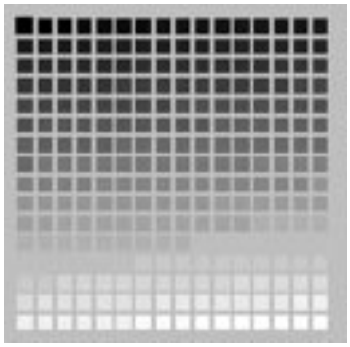
Ak sa obrázok skladá z menšieho počtu farieb, napríklad z tridsiatich dvoch, potom ich možno zakódovať do piatich bitov. Tri najmenej dôležité bity v každom bajte možno použiť na zakódovanie troch bitov utajovanej správy. V praxi sa to často využíva a obrázok, ktorý mal pôvodne paletu 256 odtieňov sivej, sa degraduje na 32 odtieňov. Na pohľad sú tieto obrázky vo väčšine prípadov od seba nerozoznateľné, pričom kapacita degradovaného obrázka pre stegosprávy sa strojnásobila.

Táto metóda je jednou z najjednoduchších metód steganografie. Vyžaduje si bezstratovú kompresiu. Obrázok BMP s kapacitou 2,25 MB však nenájdete na internete tak často, a preto nie je dosť nenápadný. Navyše správa je citlivá na akékoľvek zmeny v obrázku. Keby niekto chcel zmeniť jas obrázka alebo ho orezal na menší, zmenil jeho veľkosť a pod., správa je nenávratne stratená.

Pre obrázky, do ktorých je možné zakódovať informácie touto metódou, navyše platia reštrikcie. Nesmú to byť obrázky s paletou farieb, ktorá je optimalizovaná pre daný obrázok, pretože tam neplatí, že farba č. 2 je len o malý odtieň iná ako farba č. 3. Môže ísť o farby, ktoré sú v spektre ďaleko od seba, napríklad o červenú a modrú farbu. Zakódovanie informácie do takéhoto obrázka by spôsobilo nielen to, že by odhalilo steganografický obsah, ale priamo by zničilo aj obrázok určený na jej prenos.

Vyberať by sa mal aj motív obrázka, nemali by sa v ňom vyskytovať homogénne jednofarebné plochy a už vôbec nie čierne plochy. Steganografický obsah by na nich spôsobil síce sotva badateľný, ale predsa odhaliteľný šum a mohol by tak skrytý obsah prezradiť. Úplne nevhodné sú napr. zábery nočnej bezmesačnej oblohy (☺).

Obrázky GIF pracujú s paletou 256 farieb, vyberaných z väčšej palety. Je výhodnejšie, ak sa pracuje s čiernobielym obrázkom, tu sú prechody medzi jednotlivými odtieňmi takmer nerozoznateľné. Ak používame farebný GIF s paletou farieb, posun farby o jeden bit môže znamenať použitie úplne odlišnej farby, napríklad namiesto svetlozelenej krik-



Obr. 4

HISTÓRIA STEGANOGRAFIE

Počiatky steganografie siahajú až ku koreňom našej civilizácie. Počas jej vývoja sa používali rôzne metódy ukrývania správ v závislosti od stupňa vývoja civilizácie a jej záznamových techník.

Používali ju už v starovekom Grécku a prvú písomnú zmienku o nej prináša Herodotos. Bežný bol v tom období spôsob písania na drevené platne, ktoré boli pokryté voskom. Doň bola správa vyrytá. Ak však chceli správu ukryť, zotreli z platne vosk a text napísali na drevenú platňu. Potom ju znova prekryli voskom, a tak sa zdalo, že ešte nebola použitá. Podľa Herodota použil tento spôsob Demeratus, keď chcel varovať Sparťanov pred Xerxesovým plánom zaútočiť.


STEGANOGRAPHIAE
ARS PER OC.
CVLTAM SCRIPTV
RAM ANIMI SVI VO
LVNTATEM ABSENTIBVS

Obr. 5

Inou metódou bolo vytetovanie správy na temeno hlavy, z ktorej oholili vlasy. Keď potom vlasy vyrástli, správa bola ukrytá. Príjemca správy posla oholil, a tak si mohol posolstvo prečítať.

Písomnosti o steganografii sa zachovali už zo stredoveku. Na snímke si možno pozrieť titulnú stranu diela Steganografia, ktoré napísal Johannes Trithemius v roku 1500.

Neviditeľný atrament je známy už zo staroveku. Využíval sa však dokonca ešte v druhej svetovej vojne. Jeho použitie si môžete bez problémov vyskúšať aj doma. Stačí na to obyčajné mlieko, ktorým napíšete text na biely papier. Text by mal byť napísaný medzi riadkami normálneho textu, aby bol nenápadnejší. Nahriatím papiera nad plameňom mlieko zhnedne a objaví sa stegospráva. Ak to chcete vyskúšať, dávajte pozor, aby sa papier pri zahrievaní nezapálil. Okrem tohto jednoduchého neviditeľného atramentu existujú ešte ďalšie typy, mnohé reagujú iba na veľmi špecifické typy chemikálií, čo zabraňuje ich náhodnému zviditeľneniu.

Ďalšou metódou je použitie neformálnej a nič nehovoriacej správy vo forme čistého textu, z ktorého je možné vyextrahovať stegosprávu. Napríklad v texte

Popierať moc korenia pre nevedomosť vnucuje prestíž.

Táto nič nehovoriaca veta s „trochu“ zahmleným významom skrýva v sebe stegosprávu. Ak totiž vyextrahujete každé tretie písmeno z každého slova danej vety, získate názov časopisu, ktorý práve čítate, teda

PC REVUE

Rovnako ako písmená môžu byť použité aj celé slová. Existujú aj zložitejšie technológie výberu písmen, napr. z prvého slova prvé písmeno, z druhého druhé atď.

Veľmi významná v oblasti steganografie je tzv. mikrobodka. Vyvinuli ju Nemci počas druhej svetovej vojny. Je to mikrofotografia, ktorá sa podobá svojou veľkosťou štandardnej bodke za vetou, napísanej písacím strojom. Do tejto mikrofotografie však možno uložiť celú stránku textu, napísanú písacím strojom, alebo aj fotografiu. Mikrobodka bola uložená do štandardnej korešpondencie, ktorá bola úplne nevinná a nahradila v nej jednu z bodiek za vetou. Nie je v ľudských silách skontrolovať každú bodku pod mikroskopom, či neobsahuje mikrofotografiu, a tak tieto stegosprávy unikali pozornosti cenzorov a prechádzali cez hranice k nepriateľským špionážnym službám.

Medzi ďalšie techniky patrí ukrývanie textu pod známku na liste.

Správy sa kódovali aj do kreslených obrázkov, kde význam mali typy čiar, ich hrúbka, použitá farba, rôzne prvky obrázka atď. Keďže táto metóda bola všeobecne známa, počas prvej a druhej svetovej vojny existoval zákaz posielania detských kresieb v listoch.

Zaujímavou metódou, ktorá už súvisí s počítačmi, je použitie neproporčného písma. Tu je každé písmeno rovnako široké, a teda sú v správe úhľadne podpísané pod sebou. Ak však chceme umiestniť do takéhoto textu stegosprávu, stačí správne slovíčka v nič nehovoriacom texte posunúť o jediný pixel doprava. Ľudský zrak nie je schopný tento posun zaregistrovať, ale počítač to zistí a vyextrahovaním takto posunutých slovíčok poskladá stegosprávu.

■

ľavú oranžovú. Takáto chyba by sa na obrázku hneď prejavila a stegospráva by bola prezradená. Stegoprogramy preto dokážu paletu farieb editovať a upraviť tak, aby k tomu nedochádzalo.

Obrázky JPG, ktoré sú v praxi najčastejšie, používajú stratovú kompresiu, a preto aj ukladanie dát do nich je trochu zložitejšie. Stegospráva sa ukladá do obrázka JPG počas operácie, ktorá sa nazýva diskrétna kosínusová transformácia (DCT). V procese integrácie tu dochádza k zaokrúhľovaniu. To však môže prebiehať buď smerom dolu, alebo smerom hore. Manipuláciou s nastavením, či zaokrúhľujeme dolu alebo hore, tak môžeme kódovať bit 1 alebo bit 0. Zmenou zaokrúhľovania teda zapisujeme do obrázka JPG stegosprávu. Mnoho stegoprogramov JPG nepodporuje alebo neodporúča.

Ešte zložitejšou metódou je napríklad zmena luminancie farieb, na ktorú ľudské oko reaguje príliš málo, a tak je vhodná na steganografiu.

Dôležité je, aby sa pri operáciách zápisu stegosprávy nemenila veľkosť obrázka v bajtoch. Niektoré primitívnejšie techniky však fungujú tak, že jednoducho správu pribalia do súboru na jeho koniec. To je menej vhodná technika. Výhodou je v tomto prípade jednoduchosť stegoprogramu, nevýhodou je ľahká detegovateľnosť takto ukrytej stegosprávy.

Zaujímavou metódou ukrývania je generovanie fraktálových obrázkov, pri ktorých tvorbe sa súčasne ukrýva stegospráva. V tomto prípade nie je potrebné hľadať obálku pre dáta.

UKRÝVANIE DO ZVUKU

Tak ako do obrázkov možno ukrývať správy aj do zvuku. Takisto sa tu využíva nedokonalosť ľudského ucha, ale je potrebné dávať si väčší pozor na výsledné stegomédium, pretože ľudské ucho je veľmi citlivé.

Možno použiť techniku, keď sa dáta ukrývajú do posledného signifikantného bitu (LSB) podobne ako v prípade obrázkov. Množstvo dát, ktoré je možné ukryť, je potom dané vzorkovacou frekvenciou a počtom kanálov zvuku. Na dva kanály zvuku vzorkovaného s frekvenciou 44 kHz je možné ukryť 11 KB dát na sekundu záznamu. Priveľká hustota stegodát spôsobuje počuteľný šum.

Stegosprávu možno ukryť aj v súboroch MP3, kam sa správa ukrýva počas konvertovania nahrávky z formátu WAV do MP3.

DISK

Na uloženie stegodát je možné použiť aj disketu alebo pevný disk. Špeciálny steganografický softvér použije na zápis dát sektory, ktoré sa operačnému systému javia ako voľné. Iba steganografický softvér z nich dokáže vyextrahovať dáta. Pre ostatné programy zostávajú tieto sektory naďalej prázdne. Takto je možné využiť relatívne menšiu kapacitu diskety alebo skutočne obrovskú kapacitu pevného disku. Nevýhodou môže byť to, že pri akomkoľvek zápise údajov na toto médium môže dôjsť k porušeniu integrity stegodát ich náhodným prepísaním.

KOMPRESNÉ ALGORITMY

Stegosprávy je možné ukladať aj do archívov, ktoré vytvárajú kompresné programy. Počas komprimovania sa do archívu pribalí stegospráva. Tú však obyčajný dekompresný program nedokáže vyextrahovať, môže to urobiť iba dekompresor so špeciálnou úpravou.

STEGANALÝZA

Aj keď steganografia je veľmi silný nástroj, v niektorých prípadoch sa dá stegomédium rozoznať a dokonca sa vyhľadávanie týchto médií dá automatizovať. Proces vyhľadávania ukrytých správ sa nazýva steganalýza.

Steganalýzu možno rozdeliť na niekoľko prístupov, a to podľa toho, čo všetko sa v čase analýzy o stegomédiu vie. Najhoršia možnosť je, ak sa nevie nič a k dispozícii je iba stegomédium. Lepšie je, ak je k dispozícii stegomédium aj originál, ktorý tvorí obálku média. Podobne je to aj v prípade, ak je k dispozícii stegomédium a dokonca aj správa, ktorá v ňom bola ukrytá. Stáva sa to vtedy, ak bola správa získaná iným spôsobom. Vtedy sa pristupuje k analýze stegomédia s cieľom odhaliť algoritmus zápisu stegosprávy, aby bolo možné v budúcnosti vyextrahovať pomocou tohto algoritmu ďalšie správy zo stegomédií z daného zdroja.

Niektoré steganografické algoritmy a najmä ich implementácie obsahujú chyby, ktoré ich prezrádzajú. Niekedy je ako obálka stegomédia použitý nevhodný obrázok, čo spôsobí nekvalitný výsledok ukrývania dát, ktoré sú ľahko odhaliteľné. Najjednoduchšia metóda je teda sledovanie ľudským okom, to je však málo automatizovateľné.

Inou metódou je štatistická analýza digitálneho obsahu. Odchýlky od štatisticky overených hodnôt totiž môžu indikovať prítomnosť stegosprávy. Aby bolo možné túto techniku použiť, muselo sa pristúpiť k analýze obrovského množstva obrázkov. Na základe toho bolo určené, čo je pre obrázky „normálne“. Ak sa obrázok vymyká z tejto charakteristiky, považuje sa za stegomédium.

Typickým príkladom sú 24-bitové farebné obrázky. Dva susediace body sa zvyčajne líšia v jednej z farebných zložiek o určitú minimálnu hodnotu, ale iba málokedy sa líšia vo všetkých troch zložkách. Ak sa vyskytuje takáto odlišnosť pri drvivej väčšine bodov alebo dokonca pri všetkých, je viac ako pravdepodobné, že ide o stegomédium.

Na internete možno nájsť softvér na steganalýzu, napríklad Stegbreak alebo Stegdetect /1/. Tento nástroj umožňuje automatizovane vyhľadávať steganografické záznamy v obrázkoch.

Z uvedeného vyplýva, že nemožno automaticky považovať každý nástroj steganografie za stopercentne účinný. Platí to, čo pre kryptografiu. Ak neviete, akým spôsobom program pracuje, radšej ho nepoužívajte. Mohlo by sa stať, že je založený na nekvalitnom algoritme alebo obsahuje chybu a vďaka tomu je extrémne ľahko odhaliteľný.

ZÁVER

Tak ako bolo spomenuté v úvode, steganografia je celá veda a tvrdí sa, že aj umenie. Nebolo preto možné vtesnať do tohto článku všetko a nebolo to ani cieľom.

Steganografia nie je iba nástroj špiónov a živlov, ktoré si nezaslúžia úctu. Možno ju použiť aj na ochranu citlivých dát vo firmách pred konkurenciou a priemyselnou špionážou, teda na úplne legálne ciele. V každom prípade má steganografia svoje miesto v bezpečnostných technológiách.

Branislav Madoš

Zdroje:

/ 1 / *www.outgress.com*
/ 2 / *www.jjtc.com/steganography*
/ 3 / *www.petitcolas.net/fabien/steganography*
/ 4 / *www.watermarkingworld.com*
/ 5 / *http://www.lnt.de/~hartung/watermarkinglinks.html*