



EVROPSKÁ UNIE
Evropské strukturální a investiční fondy
Operační program Výzkum, vývoj a vzdělávání



Kryptologie

Steganografie

Strategický projekt UTB ve Zlíně, reg. č. CZ.02.2.69/0.0/0.0/16_015/0002204

Obsah prezentace

- Steganografie – úvod a rozdělení
- Fyzická steganografie
- Lingvistická steganografie
- Digitální steganografie
- Stegoanalyza

1. Úvod do Steganografie

Steganografie: Úvod

- “Doplněk” Kryptografie.
- Umění a zároveň věda o psaní a ukrývání zpráv.
- Výhoda - skrytá zpráva “nepřitahuje” pozornost.
- Kryptografie - snaží se ochránit obsah zprávy, zatímco Steganografie chrání obojí
 - jednak zprávu a jednak zejména účastníky utajené komunikace.

Rozdělení Steganografie

- Fyzická Steganografie (Technická)
 - Různé technické postupy pro skrytí informace
- Digitální Steganografie
 - Využití veškerých nástrojů a možností digitální komunikace
 - Především ukrývání zpráv do multimedialních souborů
- Tištěná Steganografie (Lingvistická)
 - Modifikace nosného textu, tak aby ukryl tajný text

2. Fyzická (technická) steganografie

Fyzická (Technická) Steganografie

- “Historické přístupy:
 - Např. skryté zprávy uvnitř voskových tabulek (Řecko),
 - skryté zprávy vytetované na tělech “messengerů” (Čína).
- Technologie Mikroteček – spolu s vynálezem mikrofilmu - fotografie velikosti tečky za větou v tištěném textu, které skrývaly zcela čitelný text standardní stránky psané na stroji se “tvářily” jako tečka napsaná strojem na obálce. Přestože byly tak malé, mikrotečky dokázaly skrýt velké objemy dat včetně kreseb a fotografií. Zpráva nebyla šifrovaná, jen tak malá, že na sebe (zprvu) neupoutala pozornost. Jiným přístupem bylo, že mikroskopické obrázky byly přepravovány v uchu, nosní dírce nebo za nehtem agenta [1].

Fyzická (Technická) Steganografie

- Neviditelné Inkousty - Mezi řádky na první pohled zcela nevinného dopisu se mohla ukrývat velmi odlišná zpráva. Běžnými zdroji jsou mléko, ocet, ovocné šťávy a moč, které po zaschnutí nejsou na papíře vidět, ale po zahřátí ztmavnou a zpráva se tak objeví. ALE - příliš jednoduché odhalení takto skryté zprávy → vývoj složitějších technologií založených na "inkoustech" reagující na určité chemikálie. Některé zprávy bylo možné zviditelnit pouze v laboratoři za pomocí několika "vývojek" (podobně jako fotografie). Později po vynalezení "univerzálních vývojek" založených na rozpoznání míst, která byla navlhčena, podle změn na povrchu vláken papíru, bylo od těchto metod Steganografie opuštěno.
- Dnes se obdoba této metody používá např. při výrobě bankovek (v papíru jsou vlákna viditelná pouze v určitém druhu světla) [1].

3. Lingvistická steganografie (STEGOTEXT)

Lingvistická Steganografie (STEGOTEXT)

- Jednoduchá modifikace/konstrukce nosného textu (často veřejně dostupného – novinový sloupek, tisková zpráva) pro ukrytí tajné zprávy.
- Tzv. **nulové šifry** (nezašifrované zprávy) - skutečná zpráva je obsažena v textu jiné, neškodně vypadající.
- Nejčastěji šlo o písmena nebo celá slova na určité (pravidelné) pozici v textu.
- Např: text „Pershing sails from NY June 1.“

„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.“

Lingvistická Steganografie (STEGOTEXT)

- Teoreticky velké množství přístupů, vzhazem může být každé první/poslední slovo ve větě, každé velké písmeno (na začátku vět + jmen/názvů), nebo například každé první písmeno nového řádku (tedy první „sloupec“ textu od shora dolů, atd...).
- Alternativní postup: tzv. **čínská mřížka** - pomocí ní lze zprávu rozmístit do krycího textu v podstatě náhodně. Zpráva je vepsána do otvorů v čtvercové mřížce (šabloně) nebo napsána na čtverečkovaný papír na předem domluvená místa a poté je doplněna nezávadným textem - vytvoření uceleného dopisu.

Lingvistická Steganografie (STEGOTEXT)

- Změna řezu písma
- Změna velikosti významných znaků
- Změna barvy, sytosti
- Nepatrná změna polohy znaků, slov, řádků
- Rozložení dokumentu - mezery navíc apod.
- Whitespaces v HTML kódu

Lingvistická Steganografie (STEGOTEXT)

- Jakákoliv zpráva může být teoreticky zakódována jako sekvence 0 a 1:
 - Využití podobných symbolů (0 - 0 a 1 - 1),
 - Počty mezer mezi větami.
 - Počty mezer na konci řádků.
 - ...
- Vložení bílých symbolů na konce řádků, nebo do mezer mezi slovy/větami.

4. Digitální steganografie

Digitální Steganografie

- Využití veškerých možností „digitálního světa“
- Nejčastější aplikací je ukrytí zpráv do multimedialních souborů (obrázky, audio, video).
- Digitální vodoznak

Digitální Steganografie

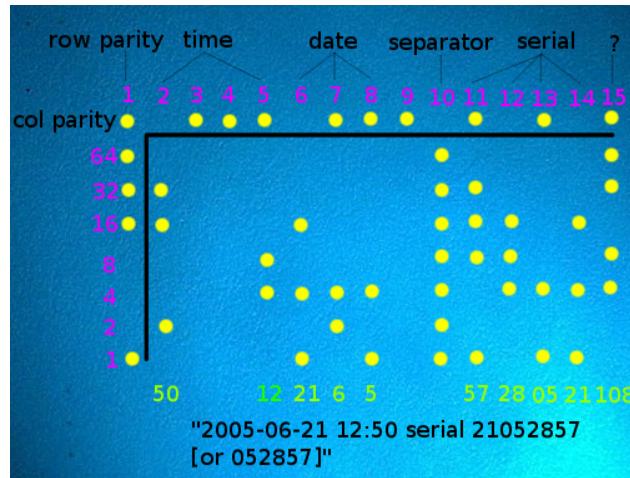
- Příklady:
 - Obrázky vložené do video materiálů
 - Ukrývání dat do audio formátů (wav, mp3, ogg atd...) - Vkládání náhodných krátkých nepostřehnutelných ozvěn (echo), nebo využití nedokonalosti lidského sluchu - Frekvenčního/Časového maskování.
 - Obecné ukrývání do obrázků (změna bitů barvy, změna jasu, kontrastu)
 - Ukrývání dat do “nejnižších” bitů zašuměných obrázků či zvuků.
 - Ukrývání dat do redundantních bitů (LSB) - bez koprese (TIFF, BMP, TGA).
 - Ukrývání dat do redundantních bitů (LSB) pro komprimované (JPEG) formáty.

Digitální Steganografie

- Příklady:
 - Ukrývání dat do náhodného či šifrového textu (data musí být již zašifrovány).
 - Skrývání dat do .exe souborů, prodlevách v paketech posílaných po síti např z klávesnice, pohyby myší (vzdálené pracovní plochy, atd).
 - ...

Digitální Steganografie

- Další metody - Žluté mikrotečky vytvářené moderními barevnými laserovými tiskárny.



Zdroj obrázku: [2]

- Předpokládá se, že téměř všechny moderní laserové tiskárny za poslední více než dekádu (veřejně se o problematice mluví od roku 2004) obsahují nástroje jak pomocí forenzní analýzy vystopovat zdrojovou tiskárnu (nemusí být nutně mikrotečky).

Digitální Steganografie - Příklad

BEZtajné zprávy



Stajnou zprávou



Dialog v otevřeném textu:

Ivánku, kamaráde, můžeš mluvit?

Jo můžu, jasně.

Hele, kontrolní otázka, došly ti ty ryby?

Jo kapříci připluli, v pohodě.

Ty vole dyť víš, že s mnicí není problém, ty vole,

vždyť se znám ne, co?

Dialog zašifrovaný : AES-256

```
ke0FJ87TSZoav7I5UfJpp8E0i75Gb6xVa3LFXGehXlr
45YnVV03pwqnBsD3kFmEvvGVhZ9zY5X62NVS
xHJ4/4mEBdhwWQV5FCFHxV+/niu+P7r0v0NZM
b+C/K3IFE3OKKvqFa6SevII2wsXwKNdkQR5kv9
oOiFks4+0leEJjlyA4bSybuq5mhx9mqrziljLC229w
0CWb6YCnjSyBPXrgdD2Prr1Xb9ZUflRN0fUSpD
8NFhEdrESWpj08e/+/RAdygCsM0blapTkIVw==
```

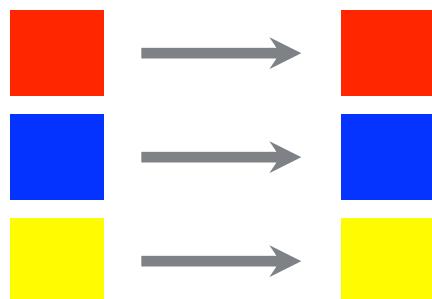
LSB (LST) Metoda

- Princip použití LSB (Least Significant Bit - nejméně významný bit) spočívá v neschopnosti lidského oka poznat rozdíl mezi dvěma barvami, které se liší právě v LSB.
- ALE! Nesmí být proveden zásah do původních dat. Tato primitivní technika vyžaduje použití neztrátové komprese (TIFF, TGA, BMP,...), protože jakákoliv ztráta přesných dat znamená i ztrátu těch tajných. Převedením do JPEG, nebo změnou velikosti, použitím jakékoliv transformace nebo filtru, dojde k nenávratné ztrátě skryté informace.
- Do TIFF obrázku 1024 x 768 bodů (24 bit) lze vměstnat až 288 kB dat

LSB (LST) Metoda

255 000 000 – 11111111 00000000 00000000 – červená
000 000 255 – 00000000 00000000 11111111 – modrá
255 255 000 – 11111111 11111111 00000000 – žlutá

Původní 3 pixely



255 000 001 – 11111111 00000000 00000001 – červená
001 000 255 – 00000001 00000000 11111111 – modrá
255 254 001 – 11111111 11111110 00000001 – žlutá

Skrytá zpráva 101101101

Digitální vodoznak

- Jedná se o techniku, která do digitálního dokumentu (obrázek, zvuk, text) vkládá informaci tak, že je ji obtížné najít nebo odstranit.
- Vodoznak odstranit zkopírováním nebo běžnou úpravou nelze.
- Odhalit vodoznak je obtížné, neboť většinou není znám použitý algoritmus.
- Dokument může obsahovat více vodoznaků najednou.
- Digitální vodoznak lze využít:
 - k ochranně autorských práv (lze dokázat, kdo je autorem dokumentu),
 - ke sledování zdrojů (lze zjistit z jaké stránky byl dokument zkopirován),
 - ke skryté komunikaci [3].

Steganografický SW - přehled

- S-tools 4 - Steganografický freeware pro Windows, ukrývá do BMP, GIF, WAV.
- mp3stego - Ukryje data do mp3 v průběhu komprimace. Data nejdřív zkomprimuje, zašifruje a schová do mp3 streamu. Windows/Linux/Unix - GUI i Command Line.
- westfeld - Experimentální software pro pokročilou steganografii, který je odolnější proti statistickým útokům, vyvinutý na Drážďanské univerzitě. Naprogramován v Javě.
- Outguess - Jeden z nejlepších programů pro Linux/UNIX. Umí schovat data do PNG a JPG souborů, používá šifrování a dodatečné antidetekční techniky.
- JSteg Shell - pro Windows/DOS s podporou šifrování a GUI rozhraním.
- Steghide - pro windows i linux.

Steganografický SW - přehled

- Steganos 3 - Komerční software, pro windows, který schová vaše data v nejrůznějších formátech, umí šifrování a několik antidetekčních technik. Obsahuje možnosti vytvořit virtuální disk chráněný heslem, tento disk pak rozložit do obrázků nebo audio souborů. Mimo to umožňuje odesílat šifrované e-maily, destruktivní vymazávání souborů, cookies manager a další bezpečnostní software.
- Scramdisk/DriveCrypt - podobný jako Steganos3. Steganografie - uložení do zvukových souborů WAV.
- Securengine - schovává data do BMP, JPG a txt souborů. Zahrnuje silné šifrování a zametání po souborech.
- Cameleon - steganografický freeware, GIF, silné šifrování (256bit AES).
- Stego-Lame - Schovává data v různých audio streamech (MP3, Ogg Vorbis, MPEG 2/4 AAC, G.72x).
- Další SW - přehled na: [4]

5. Stegoanalýza

Stegoanalýza

- **Stegoanalýza je opakem steganografie.** Zabývá se detekcí nebo odhadem skryté informace.
- Třetí strana může skrytu informaci extrahovat, zneplatnit (aby ji příjemce nemohl přečíst) nebo pozměnit (aby byl příjemce naopak oklamán).
- Techniky stegoanalýzy jsou klasifikovány podle typu útoku nebo podle dostupnosti informací o možném provedení steganografie (ukrytí informace).
- Vliv na přesnost odhadu skryté zprávy mají následující tři faktory: charakter nosiče, úroveň šumu a umístění zprávy [5].

Stegoanalýza

- Útoky na digitální vodotisk se provádí tak, že útočník se snaží odstranit digitální vodotisk, aniž by zničil označené médium – nosič.
- Vizuálním útokem se rozumí odstranění všech částí obrázku, které „kryjí“ utajené informace [6].
 - Dochází k extrakci bitů potenciální utajené informace,
 - dále k vizuální ilustraci těchto bitů na pozici jejich zdrojových pixelů.
- Nejčastější je statistický útok - speciálními testy (RQP, RS), couple detektory a klasifikátory (i s využitím A.I. Nebo strojového učení).

Seznam odkazů

- [1] VONDRAŠKA, Pavel. Kryptologie, šifrování a tajná písma. Ilustroval Bára BUCHALOVÁ. Praha: Albatros, 2006. Oko (Albatros). ISBN 80-00-01888-8.
- [2] Machine identification code. [online]. Dostupné z:
https://en.wikipedia.org/wiki/Machine_Identification_Code#/media/File:Machine_Identification_Code_von_Druckern.png
- [3] KOCIÁNOVÁ, Helena. Digitální steganografie. České Budějovice, 2009. Diplomová práce. Jihočeská univerzita v Českých Budějovicích.
- [4] Steganography Software. [online]. Dostupné z: <http://www.jjtc.com/Steganography/tools.html>
- [5] PRUDIL, Jan. Moderní metody stegoanalýzy. Brno, 2009. Diplomová práce. Mendelova univerzita v Brně.
- [6] ŽILKA, Roman. Steganografie a stegoanalýza. Brno, 2008. Diplomová práce. Masarykova univerzita v Brně.



EVROPSKÁ UNIE
Evropské strukturální a investiční fondy
Operační program Výzkum, vývoj a vzdělávání



Děkuji za pozornost

Strategický projekt UTB ve Zlíně, reg. č. CZ.02.2.69/0.0/0.0/16_015/0002204