Steganografie

Ing.Marek SMETANA, Ph.D., Petr PENKALA, Vysoká škola báňská v Ostravě, Fakulta bezpečnostního managementu

---

Pokud se někdo pohybuje v blízkosti počítačů, dříve či později narazí na problém bezpečnosti svých dat. Málokterý počítač dnes pracuje odděleně od ostatních a málokterá firma není napojena na další síť, kterou je nejčastěji síť internetu. Díky tomuto vzájemnému propojení je dnes potenciálním zdrojem dat jakékoli médium, na kterém jsou ukládána data. Tato oblast je tak zajímavá a zároveň tak komplikovaná, že často přitahuje nejen „dobrodruhy“ snažící se proniknout do cizího počítače. V tomto příspěvku bychom se však nechtěli věnovat ochraně dat před jejich zneužitím, ale oblasti méně efektní a pro film tudíž méně přitažlivé. Touto oblastí je přenášení dat mezi jednotlivými počítači tak, aby to okolní pozorovatel nebo náhodný svědek nepoznal. Základní myšlenkou v tomto případě není jak uzamknout, zakódovat nebo jinak zabezpečit předávaný soubor. Základem je myšlenka jak přenést utajovanou informaci tak, aby ten, kdo danou informaci obdrží, ani netušil, že ji má. Samozřejmě v případě, že není jejím příjemcem.

Představme si situaci, kdy vy jakožto odesilatel chcete předávat některým svým podřízeným informace o tom, na kterém místě bude probíhat zásah a v kolik hodin. Nemáte však s nimi možnost jednat jednotlivě a musíte tudíž použít nástěnku na chodbě, ke které má ovšem přístup každý kolemjdoucí. Jak to uděláte? Tato zdánlivě nerešitelná situace má poměrně jednoduché řešení. Možná si vzpomenete, že během druhé světové války některá rádia vysílala „vzkazy rodinám“. Byly to zdánlivě jednoduché vzkazy, které obsahovaly určitá klíčová slova. Pokud je příjemce zaslechl, věděl, co má udělat. Problém však zůstával v tom, že takovýchto „povelů“ nemohlo

být velké množství. Řádově se toto číslo pohybovalo v jednotkách: začátek akce, konec akce, prozrazení, odvolání akce.

Vraťme se však k našemu příkladu. Jedno z jednoduchých řešení by vypadalo jako lístek na nástěnce: „Změna: Do zřízení okresní pobočky ověřuje oznámení místní stanice. Vrchní Rada“. Pokud vám připadá toto sdělení nezajímavé, právě jste přečetli informaci o tom, že příští akce bude v Mořkově a bude zítra. Chcete-li si to ověřit, přečtěte pouze druhá písmena v každém slově věty. Metoda, kterou jsme teď právě použili, spadá do kategorie kryptografie a přesněji steganografie.

Steganografie je metoda (někdy nazývaná i umění) zabývající se předáváním skrytých vzkazů. Tento výraz pochází z řečtiny. Je složen z výrazu *stenos* – kryt nebo střecha a *graphos* – psaní. Tedy metoda, jak ukrýt zprávu v jiné zprávě nebo obecně souboru. Tato metoda může být velmi účinná a efektivní při předávání informací.

Možná v tomto okamžiku uvažujete o tom, zda není jednodušší zprávu prostě zašifrovat. Jednodušší to jistě je, ale v okamžiku, kdy použijete kryptografii – tedy šifrování, vědí všichni, že se pokoušíte nějakou informaci ukrýt. Z hlediska lidské psychologie toto vědomí pak vede ke snaze zjistit, co je obsahem utajované zprávy. A to i v případě, že dotyčný ví, že zjištěné informace mu nebudou k užitku. Hnací silou pro něj bude pouze zvědavost.

Jestliže však použijete steganografii, která se nesnaží informaci nijak zašifrovat, ale pouze ji ukryje, takže mimo příjemce nikdo netuší, že má v rukou utajovanou informaci, psychologie zvědavosti nefunguje.

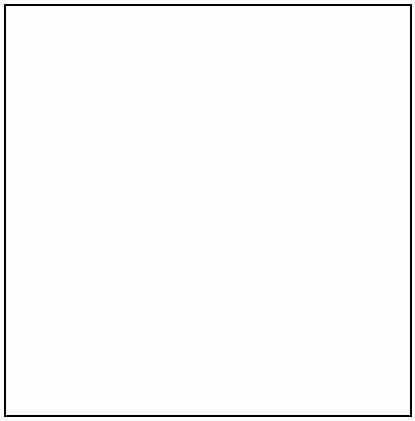
Steganografie byla široce používána už v historii, obzvláště před vytvořením kryptografie (šifrování). Jsou známy případy použití kusů dřeva, na které byla zpráva napsána a poté překryta vrstvou vosku. Mezi nejznámější patří Herodovo „využití“ otroka, kterému byl vzkaz napsán na oholenou hlavu.

Zpráva tehdy obsahovala varování Řecka před Peršany. Poté, co otrokovi dorostly vlasy, byl poslán do Řecka. Podobně zajímavou metodu přenosu zpráv vymysleli i staří Číňané, kteří čas od času psali tajné zprávy na jemné hedvábí, které pak zmačkali do malé kuličky a zalili voskem. Posel pak voskovou kuličku polkl. Hodně známá metoda skrytí textu je také použití „neviditelného“ inkoustu. Ten se objevil nejčastěji po zahřátí či jako následek působení některých chemikálií.
Pro současnou praxi si představme, že osoba chce rozeslat návod na sestrojení nástražného výbušného systému. Nejjednodušší cesta, jak tuto informaci předat, je ukrýt ji v nějakém souboru, který si budou lidé předávat mezi sebou. Pokud to bude například vtipný obrázek nebo videoklip, lidé, ke kterým se tento soubor dostane, ho rádi předají svým známým a ti zase dál. Díky tomu bude velmi obtížné vystopovat zdroj takovéto zprávy a zpráva se velmi rychle rozšíří po celé síti internetu. Pak stačí pouze informovat příjemce, aby dekódovali zprávu z toho a toho souboru. Je to velmi jednoduché a účinné. Nedávno se nám dostal do ruky článek s podtitulem: „Jak to dělá Bin Ládin“. Toto je asi ta nejhorší možná varianta využití (zneužití) steganografie.

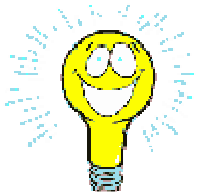
Podívejme se nyní, na jakém principu steganografie pracuje a jaké soubory pro ni lze využívat. Princip této techniky je jednoduchý. Existují určité typy počítačových dat, například bitmapové obrázky (*.bmp) nebo zvukové soubory, které mohou projít mnoha změnami, aniž by to člověk poznal. Steganografické programy vezmou zprávu určenou k utajení a vloží ji dovnitř nějakých vhodných dat. V případě zvukových souborů je možné upravovat zvuky, které jsou pro lidské ucho neslyšitelné, avšak v záznamu se objevují. Výsledný zvuk se v tomto případě pro posluchače nezmění. Jiná možnost je přidat další informace, které se projeví zvýšeným šumem. Záznam bude „nekvalitnější“, ale pokud přidaných dat nebude velké množství, nebude tato vada podezřelá. V případě obrázkových

souborů je jedna z metod užívaných ve steganografii zkreslování barev v obrázku, například posunem barevného spektra některých bodů. Výsledek bude pro lidské oko téměř stejný - obrázek jen bude obsahovat téměř nepostřehnutelný šum a kdo neví nebo neček á žádnou tajnou zprávu, nemůže nic zjistit.

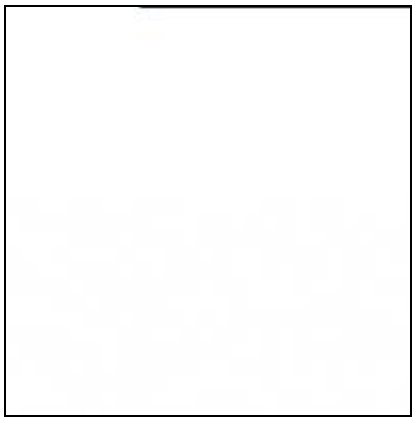
Ukázka je na obrázku 1. a 2. V prvním případě se jedná o bílou plochu. Tento případ jsme zvolili pro názornost. Pokud pomocí steganografie vložíme do obrázku č. 1. (bílé plochy) obrázek č. 2, bude výsledek vypadat například tak, jako na obrázku 3. nebo 4.



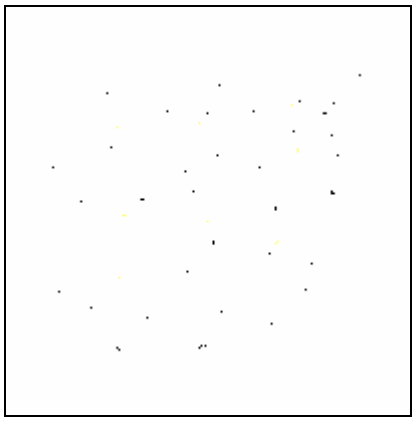
Obr.1



Obr.2



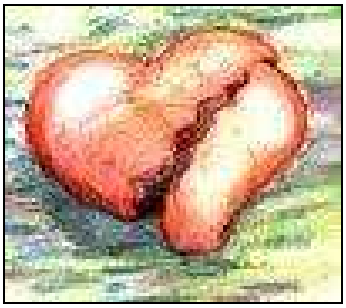
Obr.3



Obr.4

Pokud přemýšlíte o tom, že změny jsou jasně patrné, a tudíž rychle odhalitelné, zkuste si přestavit tyto změny například u

obrázku 5. Navíc, je potřeba počítat s tím, že většina programů nevyužívá „jednoduchou“ steganografii. Jednoduchou je teď myšlená ta, která využívá algoritmů ukládajících data vždy do stejných míst v dokumentu (například do každého 10. bodu obrázku). Modernější a hlavně účinnější algoritmy vycházejí z teorie náhodných čísel. Jsou tedy měněny náhodné buňky. Dále je potřeba si uvědomit, že klíč k dekódování není nikdy umístěn v „nosném“ souboru. To přidává do problému další dimenzi. Jestliže budete mít k dispozici nějaký steganografický program a jestliže bychom připustili, že přesně víte, ve kterém souboru jsou data uložena, ještě to neznamená, že je přečtete. Díky velkému množství variant nejsou jednotlivé programy vzájemně kompatibilní. Jakožto příjemce tedy musíte použít identický program, ve kterém byla informace do souboru přidána.



Obr.5

Do jednoho obrázku můžeme ukrýt více zpráv. Použijeme-li například modrou k ukrytí jedné zprávy, k ukrytí zprávy druhé můžeme použít kupříkladu červenou, a to bez nebezpečí, že poškodíme první ukrytou zprávu.

Tato metoda má však také svá omezení. Jedno z těch nejvýraznějších je množství přenášených dat. Pouze pokud není poměr mezi "nevinnými" a zabezpečovanými daty vyloženě nevhodně zvolen, je velmi obtížné cokoliv postřehnout. Z toho nám vyplývá jedno z omezení, jímž je přenosová kapacita.

Velikost ukryté zprávy nemůže být větší než velikost nosného média, ale musí být naopak podstatně menší. Zpravidla se volí poměr kolem 1:10. V případě ukrytí většího množství dat se zvyšuje pravděpodobnost odhalení. Jednodušší je tedy ukrývat texty, které jsou objemově malé, než obrázky či hudbu. Zdánlivě toto omezení neznamená výraznější problém. Pokud ale uvážíme, že pro přenesení 100 kb textu je potřeba 1Mb obrázek, a uvědomíme si rychlost připojení běžného uživatele a tedy množství času potřebného pro přijetí takto ukryté zprávy, jedná se jistě o problém významný.

Pokud se podíváme na nabídku programů, které využití steganografie nabízejí, zjistíme, že v kategorii volně šiřitelných programů se budeme pohybovat v řádu několika desítek programů. Přitom některé z těchto programů jsou i přes možnost volného použití považovány odborníky za velmi kvalitní. Samozřejmě zde existuje i celá řada licencovaných programů. Některé programy umožňují i detekci dodatečně připsaných dat, avšak vždy jen pro několik nejčastějších metod zápisu. Díky tomuto množství variant se opravdu jeví použití steganografie jako ideální pro přenos utajovaných informací.

Steganografie však může být velmi užitečná. Existuje zde tzv. vodoznak. Jedná se o ukrytou značku, pomocí které lze dokázat původ daného dokumentu. Anebo je možné takovýto dokument sledovat bez toho, že by mohlo dojít k jeho záměně. Americká tajná služba zveřejnila dohodu s vybranými výrobci barevných laserových tiskáren. Na základě této dohody jsou rozmístěny na vytištěných stránkách malé body, které informují o tom, kde a kdy byl proveden tisk. Každá regionální část světa má jedinečnou kombinaci těchto bodů. [1]

Protože si vyspělé státy světa uvědomují sílu, kterou tato metoda v sobě skrývá, zuří v této oblasti nelítostný boj mezi zastánci svobody osobnosti a zastánci „bezpečnostních“

aspektů. Některé země (například USA nebo Francie) použití kryptografických technologií v počítačovém průmyslu omezuj, nebo přímo zakazují. Steganografii také zakazují některé firmy v obavě před průmyslovou špionáží. Ve Spojených státech existuje norma DMCA (Digital Millennium Copyright Act) z roku 1998. Ta staví mimo zákon všechny nástroje, jež by mohly být použity k porušování autorských práv. Tato norma byla široce rozebírána v tisku v roce 2002 hlavně v souvislosti s případem profesora Faltena. Ten se svým vědeckým týmem vypracoval metodu na odstraňování digitálních vodoznaků v nahrávkách, což je druh „podpisu“ výrobce daného uměleckého díla. [2] [3]

O steganografii v souvislosti s terorismem se začalo hodně mluvit v roce 2001. Tehdy byly zachyceny instrukce, které si předávali členové al-Kaidá mezi sebou uschované do pornografických fotek. Ve stejném roce proběhla tiskem také informace o tom, že podobným způsobem byly využity fotografie internetové aukční síně Ezay.com. Předpokládá se, že plány pro provedení útoku na Světové obchodní centrum byly rozeslány stejným způsobem. Je však známo, že Usáma bin Ládin a jiní teroristé používali steganografický software k ukrývání zpráv již dlouho před útokem na Světové obchodní centrum 11. září. Problémy v dohledání užití této metody v praxi jsou dány především snahou některých „reportérů“ vytvořit senzaci i za cenu podání nepodložené informace. Vzpomeňme v této souvislosti například na případ Johna Kellyho, který byl válečným dopisovatelem New York Times. Jiný případ pak jsou cílené kampaně některých výrobců software pro odhalování ukrytých zpráv v dokumentech. Tito výrobci se snaží uměle vyvolat dojem, že jejich software je nezbytný, a tudíž šíří poplašné zprávy. [4]

Stejně tak jako v jiných oblastech s bezpečnostními riziky i zde probíhá intenzivní výzkum v oblasti možností detekce ukrytých informací. Metoda vedoucí k odhalení informace ukryté

pomocí steganografie se nazývá stegoanalýza. Nejjednodušší typ metod z této skupiny jsou metody založené na porovnávání. Pracují tak, že sledují různé soubory a kontrolují jejich charakteristické znaky. Jako příklad můžeme uvést kontrolu velikosti souboru. Program tedy sleduje soubory, které procházejí určitým uzlem – řekněme serverem elektronické pošty ve formě příloh. Pokud zjistí, že soubor z názvem „XX.bmp“ prošel tímto bodem různě veliký, ohlásí tento fakt obsluze. Tím upozorní na soubor, v němž mohou být ukryta dodatečná data.

Poměrně spolehlivým indikátorem přidaných dat může být nepřiměřená velikost souboru. Jestliže máme obrázek o velikosti 500 Mb, jistě to vyvolá podezření, jelikož velikosti obrázku se běžně pohybují v řádech 1 Mb a méně. Je samozřejmé, že tento obrázek může být velmi kvalitní fotografie, kdy velikost je dána potřebou kvalitního zápisu. Je však jednodušší zjistit, zda nadměrná velikost několika obrázků je opodstatněná, a tím odfiltrovat pouze „podezřelé“ obrázky z relativně malého souboru, než postupně kontrolovat všechny obrázky.

Další metody jsou založeny na kontrole známých užívaných postupů ve steganografii. Program bere postupně soubor za souborem a zkoumá, zda při použití některého z postupů vyjde nějaká smysluplná informace. Tento postup je však značně zdlouhavý. Obecně jej však lze velmi urychlit, pokud v daném počítači nebo jeho okolí najdeme některý ze steganografických programů. Lze předpokládat, že jak odesilatel, tak příjemce nebude danou metodu posílání dat používat pouze jednou, ale opakovaně. V takovém případě bude potřebovat kódovací program několikrát a nebude jej tudíž uchovávat daleko. Pokud se podaří takovýto program nalézt, je pak již jen otázka času, který je potřeba k prohlédnutí všech souborů daného typu, které se v počítači nacházejí. Na trhu dnes existuje řada

programů, které některou z metod detekce ukrytých zpráv ovládají. [5]

Do budoucna se dá říci, že užití steganografie je s přibývajícím užíváním zápisu dat pomocí komprimace (zhušťování – vznikají soubory typu jpg, mpg, zip, apod.) stále těžší. Vysokohustotní zápis neumožňuje přidat tak velká množství dat. [6]

Steganografie je metoda, která umožňuje skrývat informace ve veřejně dostupných dokumentech. Je to metoda, která je z hlediska své filozofie velmi stará, i když její užívání není příliš časté. V případě potřeby ukrývat pouze krátké informace se jeví jako výhodnější používání kódových slov, v případě dlouhých zpráv je to kryptografie (šifrování). Hlavní výhodou steganografie je možnost šíření ukryté zprávy spolu s jejím nosičem veřejnými cestami, a to naprosto nepozorovaně. V současnosti se užití této metody ubírá dvěma hlavními směry. Legálním – tedy užitím této metody k autorizaci uměleckých děl, a nelegálním – hlavně v oblasti předávání dat mezi technicky vyspělými zločineckými organizacemi po celém světě. Hlavním důvodem pro užívání steganografie je její složitá a doposud velmi obtížná detekce, daná hlavně množstvím přenášených souborů.

Literatura:

[1.] Electronic Frontier Foundation „DocuColor Tracking Dot Decoding Guide“, http://www.eff.org/Privacy/printers/docucolor, cit. 14. 7. 2006.

[2.] Komarek, J.: MP3 týden: Boj proti DMCA končí. Internetové noviny idnes.cz, 12. 2. 2006, http://technet.idnes.cz, cit. 14. 7. 2006.

[3.] Zouzalík, M.: Internet: Přichází skutečně cenzura? Internetové noviny idnes.cz, 15. 04. 2002. http://technet.idnes.cz, cit. 14.7.2006

[4.] Stříž, M.: Tajemství steganografie. PC svět, 13. 7. 2003, http://www.pcsvet.cz.

[5.] Praktické základy kraptologie a steganografie. http://www.security-portal.cz/clanky, cit. 14. 7. 2006.

[6.] Universal Steganography. http://www.outguess.org, cit. 14. 7. 2006.

Smetana, M. – Penkala, P.

Steganografie

SOUHRN

Steganografie je metodou, která umožňuje skrývat informace ve veřejně dostupných dokumentech. Je to metoda, která je z hlediska své filozofie velmi stará, i když její užívání není příliš časté. Hlavní výhodou této metody je možnost šíření ukryté zprávy spolu s jejím nosičem veřejnými cestami, a to naprosto nepozorovaně. Hlavním důvodem pro užívání steganografie je její složitá a doposud velmi obtížná detekce, dána hlavně množstvím přenášených souborů.

Smetana, M. – Penkala, P.

Steganografy

SUMMARY

Steganografy is a method which make it possible to hide information in public documents. This is very old method in consonance with philosophy. The main advantage of this method is stealthy sending information over the world with difficulty detection of using it among the huge number of similar documents and dates which are transferring.

Smetana, M. - Penkala P.

Steganographie

ZUSAMMENFASSUNG

Die Methode der Steganographie ermröglicht Informationen in den öffetlich erreichbaren Dokumenten zu verstecken. Diese Methode ist aus der Sicht der Philosophie sehr alt, obwohl ihre Anwendung nicht häufig ist. Hauptvorteil dieser Methode ist die Möglichkeit der Verbreitung der verstecten Nachricht durch öffentliche Wege zusammen mit dem Träger, und zwar absolut unaufmerksam. Der Hauptgrund für die Anwendung der Steganographie ist ihre komplizierte und bisher sehr schwierige Detektion, besondesrs für die Anzahl der übertragenen Daten.