PRACE NAUKOWE AKADEMII EKONOMICZNEJ WE WROCŁAWIU
Nr 1089 — 2005
Wpływ aktywności informacyjnej podmiotów na funkcjonowanie rynków

Anna Duda, Tomasz Galewski

STEGANOGRAFICZNE METODY OCHRONY INFORMACJI W INTERNECIE

1. Wstęp

Współczesna gospodarka zdecydowanie różni się od tej sprzed paru dekad. Szczególnie widoczne to jest w sposobach osiągania przewagi konkurencyjnej przedsiębiorstw. Literatura z tamtego okresu przyzwyczaiła nas do tego, że firmy, uczestnicząc w wyścigu o jak największe zyski, zwracały baczną uwagę na takie czynniki produkcji, jak: praca, kapitał i ziemia. W dzisiejszych czasach mamy do czynienia ze wzrostem znaczenia informacji. To ona właśnie stanowi o sile przetargowej przedsiębiorstwa. W zmaganiach z rywalami rynkowymi najważniejsze staje się zapewnienie odpowiedniego dostępu do potrzebnych informacji, posiadanie dostatecznie wykwalifikowanych ludzi, by móc z tych informacji skorzystać oraz ustanowienie dostatecznych zabezpieczeń chroniących posiadany zasób informacji. Na nic zda się wysiłek poniesiony na uzyskanie ważnych danych, jeżeli nie będą one silnie chronione przed próbami kradzieży, modyfikacji, zniszczenia itp.

2. Istota steganografii

Jedną z metod ochrony swoich zasobów informacyjnych jest steganografia. W dosłownym tłumaczeniu z greckiego oznacza ona „przykryte pismo". Koncepcja steganografii polega na takiej zmianie cyfrowego zapisu tekstu, grafiki czy pliku dźwiękowego, by zmiana ta pozostała niezauważalna przez osoby nieuprawnione do odbioru tejże informacji. Początki tej techniki sięgają bardzo daleko, bo aż do starożytności. W starożytnym Egipcie i Chinach powszechne było używanie atramentu „sympatycznego", czyli cieczy, których ślad pojawia się dopiero po wykonaniu określonych czynności, np. po podgrzaniu czy posypaniu odpowiednim

środkiem chemicznym. Jako materiał do takich metod przenoszenia informacji służyły niektóre pospolite substancje, takie jak: soki owocowe (np. cytryna) albo mleko[1].

Pierwszym udokumentowanym sposobem ukrycia informacji jest przypadek opisany przez Herodota – greckiego historyka. Opisał on sytuację uwięzienia Histiausa przez króla perskiego Dariusza. W związku z niemożliwością przesłania wiadomości tradycyjnymi metodami, postanowił on ominąć wszelkie kontrole listów wychodzących spod jego pióra i jako nośnik informacji posłużyła mu skóra na głowie jego niewolnika. Dokładnie ją wygolił, a następnie polecił na niej wytatuować prośby o pomoc do swojego zięcia. Pozostało tylko poczekać, aż włosy odrosną i pod pretekstem wysłania mało istotnej wiadomości na papierze, rozkazał niewolnikowi udać się do adresata nakreślonej na głowie wiadomości. Po przybyciu wystarczyło na nowo przystrzyc włosy i odczytać ukrytą informację.

Bardziej zaawansowane techniki steganograficzne stosowali podczas II wojny światowej niemieccy szpiedzy Abwehry. Posługiwali się oni techniką fotograficzną, która umożliwiała zmniejszanie zdjęć do bardzo małych rozmiarów – tzw. mikrokropek. Ukrywano je potem w tekście nad literami „i" bądź „j" i przesyłano w ten sposób czasami bardzo istotne informacje, np. raporty dotyczące przeorganizowania swoich wojsk. Panika związana z upowszechnianiem się tej metody doprowadziła nawet do tego, że cenzura wojskowa zażądała podczas wojny zakazu publikowania krzyżówek, a w ZSRR i USA tracono mnóstwo czasu na przeglądanie listów, a nawet przyklejonych na kopertach znaczków[2].

Dzisiejsze techniki przesyłania informacji ze względu na rozwój technik teleinformatycznych wyglądają zupełnie inaczej. Nietrudno jest jednak domyślić się, że wraz z rozwojem sposobów komunikowania, takich jak poczta elektroniczna, sieć www czy grupy dyskusyjne, nastąpił wzrost liczebności technik ukrywania wiadomości. Zdaniem niektórych specjalistów Internet stanowi wręcz wymarzone narzędzie do zastosowania steganografii. Informacja zapisana w sposób cyfrowy daje się łatwo manipulować, niezależnie czy mamy do czynienia z wiadomością tekstową, graficzną czy też plikiem dźwiękowym. Zmysły człowieka nie są aż tak czułe, by wychwycić niektóre zmiany w zapisie cyfrowym, co pozwala na takie umiejscowienie tajnego komunikatu w pliku, by nie naruszyć w sposób widoczny jego struktury. Możliwość praktycznie niczym nie ograniczonej swobody zamieszczania plików graficznych, tekstowych i muzycznych powoduje na przykład to, że według szacunków ekspertów aż 0,6% obrazów zamieszczanych na najpopularniejszej stronie licytacyjnej eBay zawiera steganografię[3]. Często ten sam obraz jest wykorzystywany kilkakrotnie do ukrywania w nim informacji.

---

[1] www.steganografia.wsi.edu.pl/!index.php?serwis=rozdzial&ids=28.

[2] Tamże.

[3] Tamże.

3. Ukrywanie wiadomości w plikach tekstowych

Steganografia w tekście ma najdłuższą historię spośród różnych form przekazu informacji ze względu na powszechność stosowania pisma w poprzednich okresach. Niektóre metody proponują zmiany w gramatyce i pisowni danego języka, lecz szczególnie ze względu na ogólny dostęp do edytorów tekstu część z tych propozycji może okazać się nieskuteczna.

Spośród technik stosowanych w plikach tekstowych można wyróżnić metodę międzyzdaniową, metodę końca linijki i międzywyrazową. Pierwsza z nich polega na ukrywaniu bitów informacji pomiędzy zdaniami. Na przykład można zaszyfrować „0" poprzez zostawienie jednego miejsca po kropce kończącej zdanie. Zostawienie dwóch wolnych miejsc będzie oznaczać wtedy „1". Jak widać, po pierwsze, sposób ten jest bardzo narażony na wykrycie czy zniekształcenie, ponieważ niektóre programy typu MS Word same poprawiają błędy podwójnego odstępu między zdaniami i ukryta wiadomość zostaje utracona w sposób bezpowrotny. Po drugie, technika ta wymaga bardzo dużej ilości tekstu, by zmieścić w nim chociażby średniej wielkości komunikat.

Metoda końca linijki jest ulepszoną odmianą poprzedniej techniki, gdyż za jej pomocą można przesłać wiadomość, wykorzystując mniejszy tekst. Zamiast przerw między zdaniami posługuje się ona wolnymi miejscami na końcu linijki. Stąd np. pozostawione dwa wolne miejsca mogą ukryć jeden bit cztery puste miejsca odpowiednio dwa bity, itd. Technika ta nie wzbudza dużych podejrzeń, ale jest także narażona na działanie edytorów tekstu, gdyż np. po wyjustowaniu tekstu wiadomość może zostać zdeformowana.

Metoda międzywyrazowa jest bardzo podobna do międzyzdaniowej techniki ukrywania wiadomości. Zamiast przerw między kropką a początkiem nowego zdania, stosuje się przerwy pomiędzy wyrazami. Jedno miejsce pomiędzy słowami to „0", a dwa wolne miejsca to „1". W tym wypadku utrudnione jest jednak odczytanie wiadomości, gdyż problemy sprawia rozróżnienie zwykłego wolnego miejsca od zakodowanego. W tym celu wymyślono szyfr „Manchester", który interpretuje „01" jako „1", „10" jako „0", a „00" i „11" uznawane są za puste łańcuchy bitowe[4].

4. Steganografia w plikach dźwiękowych

Sposób ukrywania wiadomości w plikach dźwiękowych nie różni się zbytnio od podobnych działań na tekstach czy obrazach. Każdy zapis na dysku ma postać ciągu bajtów, zajmującego pewną ilość miejsca. Każdy taki ciąg jest odczytywany jako kolejne znaki znormalizowanego alfabetu, tzw. kodu ASCII. Składa się on z 256 symboli i zawiera m.in. duże i małe litery, cyfry, symbole działań arytmetycz-

[4] www.steganografia.wsi.edu.pl/!index.php?serwis=rozdzial&ids=28.

nych itp., tak więc nie ma większego znaczenia, czy mamy do czynienia z tekstem, grafiką czy muzyką, ponieważ zawsze można spojrzeć na to jak na szereg znaków kodu ASCII. Sposób ukrywania informacji w pliku dźwiękowym obrazuje następujący przykład.

Próbka dźwiękowa zawiera 8 bajtów informacji:

132 134 137 141 121 101 74 38.

W postaci binarnej zapis ten wygląda tak:

10000100 10000110 10001001 10001101 01111001 01100101 01001010 00100110.

Gdybyśmy chcieli ukryć binarną formę bajtu 11010101 (213) wewnątrz tej sekwencji, to zmieniłaby się ona następująco:

133 135 136 141 120 101 74 39,

czyli:

10000101 10000111 10001000 10001101 01111000 01100101 01001010 00100111 11010101.

Można łatwo zauważyć, że próbki zmieniły się co najwyżej o 1 w stosunku do poprzednich wartości. Nasz zmysł słuchowy nie jest w stanie wychwycić takiej zmiany, a udało się wewnątrz tego pliku zawrzeć 8 bitów ukrytej informacji[5].

Technika zastępowania najmniej znaczącego bitu jest chyba najbardziej znaną spośród metod wykorzystywanych w steganografii. W bardzo prosty sposób można umieścić w nośniku dużą ilość informacji, wykorzystując jedynie to, że nasze narządy zmysłu, takie jak oko czy ucho, nie są w stanie dostrzec minimalnych zmian w jakości obrazu, czy dźwięku (oczywiście, niektórzy z nas mają bardziej wyostrzone zmysły i stosunkowo duże zmiany zostaną przez nich wychwycone).

5. Ukrywanie informacji nagłówku TCP/IP

Również i w tym elemencie komunikacji między komputerami możemy odnaleźć próby przenoszenia zamaskowanych informacji. Często w nagłówkach TCP/IP pozostają nie wypełnione miejsca, daje to szansę na wprowadzenie w te miejsca odpowiednich danych. Każdy pakiet TCP zawiera standardowy 20-bajtowy nagłówek, w którym znajdują się pola obowiązkowe do wypełnienia i pola opcjonalne. Opcjonalne pola oczywiście pozostają często nie wypełnione i dają 6 bitów do ukrycia komunikatu. Podobnie jak przy metodach ukrywania treści w tekstach, używając nagłówków TCP/IP, narażeni jesteśmy na zagubienie informacji albo zniekształcenie jej z powodu mechanizmów filtrujących. Dlatego też istnieje możliwość skorzystania z pól standardowych. Są one o wiele trudniejsze do wykrycia i

[5] www.steganografia.wsi.edu.pl/!index.php?serwis=rozdzial&ids=28.

pozwalają na wymianę informacji między użytkownikami dzięki wykorzystaniu nie wzbudzających podejrzeń komunikatów nawiązujących połączenie albo je utrzymujące. Pola standardowe są konieczne do nawiązania połączenia i utrzymywania go, zatem jakiekolwiek dane wpisane w tych polach nie będą tak przyciągać uwagi „zainteresowanych", jak pola nieobowiązkowe.

6. Steganografia w plikach graficznych

Ukrywanie informacji w plikach graficznych pozostaje najczęściej używanym sposobem „kamuflowania" danych spośród dostępnych metod. Założenia są podobne do steganografii w plikach dźwiękowych. Kolor każdego punktu na obrazie jest określany za pomocą trzech barw: czerwonej, zielonej i niebieskiej. W trybie *true colour* do opisania każdego koloru używa się ośmiu bitów. Zmiana wspomnianego już najmniej znaczącego bitu spowoduje oczywiście zmiany w zapisie, ale pozostaną one niewidoczne dla ludzkiego oka. Zmieniając każdą barwę, możemy ukryć 3 bity informacji. Biorąc pod uwagę obraz o rozdzielczości 800×600 pikseli, można w nim ukryć aż do 1,5 Mb (384KB) danych[6]. Przykład ten dotyczy obrazu nie poddanego wcześniej żadnej kompresji. Istotnym ograniczeniem w ukryciu tak dużej ilości informacji jest możliwość przesyłania sporej wielkości plików. Przeszkadza w tym chociażby pojemność niektórych internetowych skrzynek pocztowych. Zresztą wysłanie takiej wiadomości wzbudziłoby natychmiast podejrzenia osób kontrolujących kanały informacyjne. Należy więc ograniczyć treść komunikatu, jednakże w typowym bannerze występującym na stronach www (480×100) można ukryć do 600 słów[7].

Można również zastosować kompresję danych. W grafice mamy do czynienia z dwoma rodzajami kompresji: bezstratną i stratną. Kompresja bezstratna jest procesem dającym się w całości odwrócić. Jakość obrazu nie zmienia się, jeśli przeprowadzimy dekompresję danych. Przykładem takich kompresji jest format GIF i 8-bitowy format BMP. Kompresja stratna wywołuje utratę jakości pierwotnego obrazu. Po przeprowadzonej dekompresji pogarsza się kolorystyka i jaskrawość. Reprezentantem tej formy kompresji jest format JPEG (Joint Photographic Experts Group).

7. Steganografia a cyfrowe znaki wodne

Idea cyfrowych znaków wodnych jest taka sama, jaka służy np. produkcji banknotów. Znak wodny jest po prostu przypisany do odpowiedniej treści i niemożliwe jest jego usunięcie. Niemożliwe jest uzyskanie oryginalnej jakości poprzez pozbycie się znaku wodnego (widać to szczególnie dobrze na podrabianych

---

[6] magazyn.reporter.pl/2001/10/html/0404.php.

[7] Tamże.

banknotach, nie mających znaku wodnego charakterystycznego dla emitenta). Znak widoczny może być zauważalny dla ludzkich zmysłów albo nie, a jego zastosowanie to głównie ochrona własności intelektualnej. Rozwój technologii znaków wodnych idzie w kierunku, by usunięcie ich było niemożliwe; steganografia zaś do tego, by komunikaty pozostawały niezauważalne. Ich wspólną cechą jest fakt, że w obu technikach dołącza się informację do odpowiednich danych.

Cyfrowe znaki wodne mają swe zastosowanie w Internecie. Posługują się nimi głównie agencje fotograficzne i archiwa fotografii artystycznej. Sieć stanowi bardzo dobry kanał do promocji, jednak należy zabezpieczyć obrazy przed nielegalnym kopiowaniem. Cyfrowe znaki wodne nie chronią przed kradzieżą, ale niewidoczny podpis albo inny komunikat może sprawić, że dla fałszerza niemożliwe będzie przeprowadzenie transakcji sprzedaży. Warte odnotowania jest to, że cyfrowe znaki wodne nie ulegają uszkodzeniu czy zniszczeniu nawet po wydrukowaniu i powtórnym skanowaniu. Cyfrowe znaki wodne psują jakość danego obrazu, co nie uchroni również przed tymi, którzy gotowi są na to, by oglądać „uszkodzone" zdjęcia w zamian za darmowy do nich dostęp. Gorsza jakość fotografii (zależna od tego, jaki znak wodny został zastosowany) może zadowolić tych, którzy niekoniecznie poszukują perfekcyjnych zdjęć, lecz pragną poznać pewne dzieła sztuki, a nie mogą pozwolić sobie na podróż do muzeum czy zakup oryginalnych dzieł.

Technika cyfrowych znaków wodnych ma zastosowanie tylko do odpowiednio dużych plików o zróżnicowanej fakturze i kolorystyce. Minimalny rozmiar obrazu to 200×200 pikseli przy 256 kolorach. Przy mniejszych zdjęciach rozmiar pliku ze znakiem wodnym może stanowić zbyt duży procent fotografii i całkowicie zmienić końcowy efekt obrazu. Ostatnio taka ochrona własności intelektualnej stała się popularna i na rynku pojawiło się wiele programów do takiego „zatapiania" znaków. Komponenty do takich działań zawierają nawet takie programy graficzne, jak Photoshop czy Corel Photo Paint.

8. Porównanie steganografii i kryptografii

Te dwie formy przekazywania informacji w sposób, by osoby postronne nie mogły ich odczytać, są często mylnie utożsamiane ze sobą. Ale istnieją pomiędzy nimi istotne różnice. Steganografia ma na celu ukrycie przekazu danych, kryptografia natomiast zajmuje się zaszyfrowaniem wiadomości w sposób, który uniemożliwi odczytanie komunikatu osobom nie znającym klucza odszyfrowującego.

Główną zaletą steganografii pozostaje mała popularność tej technologii. Osoby nie posiadające wiedzy o istnieniu takiego sposobu ochrony danych będą bezskutecznie poszukiwać zaszyfrowanych wiadomości, podczas gdy najważniejsze dane będą po prostu ukryte wśród zwykłych dokumentów. Steganografię można stosować w wielu rodzajach nośników, co zwiększa obszar jej zastosowań. Wadą tego rodzaju kamuflażu jest to, że wiadomość raz odkryta może wskazać drogę prze-

pływu i sposób ukrywania następnych, z czego nadawca komunikatu nie zawsze musi zdawać sobie sprawę. Po wykryciu stosowanych technik steganograficznych nie istnieją już żadne przeszkody na drodze do odczytania komunikatu. Pewnym mankamentem tego systemu jest fakt, że pomimo szerokiego zastosowania w różnych formatach, techniki te są rozwijane praktycznie wyłącznie dla znanych już rodzajów plików i nie szukane są zastosowania dla kolejnych dziedzin.

Kryptografia z kolei to duże bezpieczeństwo przesyłu, jeżeli użyliśmy w tym celu odpowiednich algorytmów. Niestety duża powszechność stosowania tej technologii powoduje, że algorytmy szyfrujące są znane, a i moc komputerów zwiększa się z dnia na dzień, co daje większe szanse na złamanie trudnych kodów i wymusza dalsze badania nad rozwojem metod szyfrowania. Wadą metod kryptograficznych pozostaje także fakt, że osoby kontrolujące wyjściowe komunikaty przedsiębiorstwa albo instytucji rządowej doskonale wiedzą, że jakiś komunikat został nadany i pozostaje go „tylko" odczytać.

W takim wypadku logiczne wydaje się połączenie obu technik: steganografii i kryptografii. W wyniku takiej syntezy otrzymujemy silnie wzmocnione bezpieczeństwo przesyłu danych, gdyż komunikat zaszyfrowany i ukryty w celu odbioru przez osoby nieupoważnione musi zostać poddany kilku procesom. Po pierwsze, utrudnione jest jego wykrycie dzięki zakamuflowaniu pomiędzy nie wzbudzającymi niczyich podejrzeń danymi, a po drugie, komunikat odnaleziony wymaga odszyfrowania, co wymaga czasami sporej mocy obliczeniowej komputerów. Jeżeli utajnione informacje są użyteczne jedynie przez jakiś czas, to tym bardziej połączenie zalet obu metod będzie korzystne. Czas poświęcony na rozkodowanie wiadomości ukrytej przy zastosowaniu steganografii i kryptografii będzie dłuższy niż przy wykorzystaniu jednej z nich.

9. Przeciwdziałanie steganografii, czyli stegoanaliza

Stegoanaliza polega na zapobieganiu albo odnajdowaniu zastosowań steganografii. Dzięki jej użyciu można odkryć utajniony komunikat i doprowadzić go do bezużyteczności lub po prostu usunąć. Jak już wspomnieliśmy, metody takie, jak dodawanie wolnych miejsc między zdaniami czy pozostawianie wolnych miejsc na końcu linijki, mogą być łatwo wykrywalne i dodatkowo narażone są na zniszczenie przez działanie edytorów tekstu.

Ważne również jest to, ile informacji ukryto w dokumencie. Jeżeli ilość danych utajnionych w porównaniu z wielkością całego pliku jest duża, to większe są szanse na wykrycie takiego komunikatu.

W plikach graficznych do zakłócania odbioru ukrytych informacji wykorzystuje się wspomnianą kompresję stratną. Kompresja danych, np. do formatu JPEG, wywołuje utratę ukrytych w obrazie danych, mimo iż dla oka ludzkiego grafika pozostaje bez większych strat jakościowych.

Pliki graficzne oraz pliki audio i wideo narażone są na proces tzw. zagłuszania, czyli dodawania do wiadomości „podejrzewanych" o posiadanie ukrytych danych pewnych informacji, które w efekcie zagłuszają oryginalną treść. Zagłuszanie wykorzystuje się wtedy, gdy wiadomości ukryte są w taki sposób, że nie da się ich wyodrębnić. Pozostaje nam jedynie przedsięwziąć takie działania, by nikt ich nie mógł odczytać.

Co do informacji ukrytych w nagłówkach plików albo wiązki pakietów TCP/IP, to istnieje groźba, że system operacyjny lub specjalny filtr uzna pola, w których są ukryte wiadomości za puste i samoczynnie je wykasuje. Jeżeli próbujemy wysłać pliki ze zmienionym, fałszywym adresem IP, to musimy się również liczyć z tym, że odpowiednie programy mogą porównywać adres IP w DNS (Domain Name System) i potwierdzić autentyczność nadawcy. Jeżeli adresy nie będą się zgadzać, to nastąpi zniszczenie przesyłanego komunikatu.

10. Programy steganograficzne oraz narzędzia wykrywające ich użycie

Programy steganograficzne rozwijają się z dnia na dzień i obecnie na rynku można odnaleźć kilkadziesiąt różnych rozwiązań dotyczących ukrywania wiadomości.

Bardzo powszechnym i jednym z najprostszych programów jest JPHS (JP Hide and Seek)[8]. Podczas jego używania wystarczy tylko podać hasło, a program samoczynnie zaproponuje, jaka ma być wielkość pliku, by szanse na wykrycie dokumentu były jak najmniejsze.

Przyjaźniejszym programem dla użytkownika przyzwyczajonego do „windowsowego" interfejsu jest BMP Secrets. Jak sama nazwa wskazuje, jest to program do utajniania danych w formacie BMP. Podczas jego użytkowania widzimy na ekranie obraz przed schowaniem komunikatu i po jego kamuflażu. Daje nam to szanse na własne porównanie i ocenę, czy ktokolwiek może rozpoznać różnicę jakości i domyślić się charakteru wiadomości.

Obecnie za jeden z najlepszych programów do ukrywania informacji w plikach graficznych uchodzi „Steganos". Podobnie jak w innych wypadkach, należy podać nazwę pliku, który chcemy ukryć, oraz nazwę jego „nośnika". Do wyboru pozostaje jeszcze opcja zaszyfrowania, jeżeli chcemy zwiększyć prawdopodobieństwo bezpiecznego transferu danych. W tym celu polecany jest PGP (Pretty Good Privacy).

Przykładem programu ukrywającego informacje w plikach dźwiękowych jest MP3Stego. Po schowaniu danych w muzyce kompresuje on plik do formatu mp3, wykorzystując przy tym technikę MPEG Audio Layer III.

---

[8] Programy do steganografii można odnaleźć pod następującymi adresami: www.steganography.tripod.com; www.steganos.com; www.outguess.org; www.demcom.com.

Oczywiście równocześnie z rozwojem technik ukrywania równolegle następuje proces tworzenia programów do nich przeciwstawnych, czyli wychwytujących utajnione treści. Zamówienie opracowania takich programów złożyło chociażby Dowództwo Sił Powietrznych USA. Od momentu rozpowszechnienia informacji o stosowaniu steganografii, uczeni Uniwersytetu Michigan opracowują programy do poszukiwania dokumentów, w których zastosowano niektóre metody ukrywania informacji. Cały proces rozłożyli oni na dwa etapy. W pierwszym chcą się zająć steganografią na stronach www, a w dalszej kolejności grupami dyskusyjnymi. To właśnie dzięki nim ustalono, że na najwięcej przypadków ukrywania komunikatów natrafimy na stronach eBay. Aby dać wiarę w możliwości ich programu, przeprowadzono test w ramach akcji jednej z amerykańskich stacji telewizyjnych. Na jej stronach internetowych zamieszczono obraz z ukrytym w nim zdjęciem samolotów B-52. Okazało się, że program naukowców potrzebował jedynie 1 s, by odnaleźć i odczytać tajny przekaz[9].

Drugi etap obejmujący prace nad „oczyszczaniem" grup dyskusyjnych koncentruje się na grupach najbardziej obleganych, czyli tych, które dotyczą pornografii i sportu. Terroryści, wykorzystując popularność takich czatów, starają się stopić z tłumem i, nie wzbudzając podejrzeń, wysyłać stosowne komunikaty.

Darmowym programem służącym do wykrywania użycia metod steganografii jest Stegdetect. Przeszukuje on pliki JPG, posługując się kilkoma najczęściej wykorzystywanymi algorytmami ukrywania informacji. Program ten jest również zaopatrzony w możliwość łamania haseł. Posługuje się w tym celu *brute force*, która polega na przeszukiwaniu w słownikach stosownych terminów, które mogłyby posłużyć jako hasło[10].

11. Steganografia w praktyce

Niestety, podobnie jak z innymi wynalazkami technik kryptograficznych, nie ma możliwości ochrony dostępu do technik steganograficznych przed przestępcami. Nietrudno się domyślić, że steganografia jest dużym utrudnieniem w pracy instytucji rządowych i organów ścigania. Ukrywanie przesyłania pewnych komunikatów stanowi poważne zagrożenie dla wykrywania przestępczości oraz może zmniejszyć bezpieczeństwo kraju. Głośno się zrobiło o steganografii w związku z atakami terrorystycznymi na Stany Zjednoczone. Dla terrorystów Internet stanowi bardzo wygodne narzędzie komunikacji. Natłok informacji na stronach internetowych, w grupach dyskusyjnych, poczcie elektronicznej itp. powoduje, że łatwo „zginąć w tłumie" i przesłać informacje niepostrzeżenie. Nie ma na razie takiej możliwości, by kontrolować wszystkie wiadomości, które są przesyłane w Internecie[11].

---

[9] kwp.radom.pl/pgm/pgm02_07.htm.

[10] magazyn.reporter.pl/2001/10/html/0404.php.

[11] W tym momencie należy wspomnieć o systemie kontrolowania informacji przesyłanych przez Internet – Echelon, który jest wykorzystywany przez USA. Jego zasięg oraz skuteczność pozostają jednak w tajemnicy i można się jedynie domyślać ingerencji w sferę komunikacji między internautami.

Najbardziej nagłośnionym przypadkiem zapobiegania steganografii było nakłanianie przez rząd USA wszystkich stacji telewizyjnych, by nie pokazywały wypowiedzi największego wroga Stanów Zjednoczonych – Osamy bin Ladena. Obawiano się, że może on przekazywać ukryte wiadomości dla agentów al-Kaidy rozsianych po całym świecie. Tygodnik „Time" z kolei w jednym z artykułów przedstawił dane świadczące o wykorzystywaniu przez terrorystów z al-Kaidy steganografii w Internecie. Posługiwali się oni w tym celu stronami pornograficznymi i kanałami IRC traktującymi o sporcie[12]. Natychmiast po atakach we wrześniu 2001 r. agenci FBI wkroczyli do siedzib dostawców internetowych z urządzeniami do podsłuchu (tzw. carnivore'ami)[13], których użycie w normalnych warunkach wymaga uzyskania nakazu sądowego. Agenci siatek terrorystycznych wcale nie ukrywają faktu stosowania steganografii: „To wspaniałe, że można teraz wysłać list zawierający cytat z Koranu, a w rzeczywistości wezwanie do świętej wojny" – oświadczył przedstawiciel Hezbollahu[14].

Steganografia znajduje również zastosowanie w praktyce gospodarczej. Firmy posługują się nią w nadziei, że uda się im przesłać niezauważenie jakieś ważne dokumentacje. Oczywiście, tak jak wspomnieliśmy, lepsze efekty uzyskuje się, łącząc metody ukrywania wiadomości z technikami kryptograficznymi. Należy również wybrać odpowiedni rodzaj nośnika utajnionego komunikatu. Jeśli firma zajmuje się obróbką zdjęć, to najmniejsze podejrzenia będą wzbudzać pliki graficzne. Format np. MPEG lub MP3 mógłby zwrócić uwagę tych, którzy śledzą pocztę wysyłaną prze dane przedsiębiorstwo.

Nie bez znaczenia pozostaje także wielkość danych, które chcemy ukryć. Programy wykrywające utajnione dane dość często „wyłapują" te z zaszyfrowanych plików, które objętościowo stanowią 10% wielkości całego transmitowanego dokumentu. Te, które stanowią ok. 1% wielkości pliku, są wykrywane już o wiele rzadziej[15]. Zatem można zastosować przesyłkę częściową, składającą się z dwóch części. Pierwsza będzie zawierała duży dokument opatrzony hasłem dostępu do niego, a druga – już znacznie mniejszych rozmiarów, będzie zawierała jedynie to hasło.

Ale steganografia nie tylko służy przestępcom i firmom mającym tajemnice handlowe. Otóż na izraelskim uniwersytecie Ben Guriona Berszebie dopracowuje się oprogramowania służące do wyrobu dokumentów tożsamości, które będą się opierały wszelkim próbom fałszowania. Techniki steganograficzne, które zostały omówione wcześniej, wykorzystane mają być do ukrywania w dowolnym elemencie graficznym danych pozwalających na uzyskanie pewności co do autentyczności. Na przykład odcisk palca mógłby zostać schowany w zdjęciu na paszporcie i ludzkie oko nie byłoby w stanie wychwycić tego szczegółu. Podmienienie zdjęcia

[12] www.cert.pl/index2.html?action=show_news_more&nid=201.
[13] Tamże.
[14] www.delphi-kurs.piwko.pl/sprytek/.
[15] www.zpw.most.org.pl/STEGANOS.HTM.

wyszłoby na jaw po przeskanowaniu dokumentu i stwierdzeniu braku w nim utajnionych danych. Takie zastosowanie steganografii wymaga, niestety, wyposażenia wszystkich służb uprawnionych do legitymowania obywateli w specjalne skanery zdolne do wykrywania ukrytych znaków[16].

Niebezpieczeństwo takiego rozwiązania wiąże się z faktem, że przy produkcji takich dokumentów pracowałyby osoby, którym z różnych powodów mogłoby zależeć na sprzedaży algorytmów wykorzystanych do „zatapiania" identyfikatorów. Upowszechnienie sekretów takiej technologii wiązałoby się prawdopodobnie z koniecznością poniesienia ogromnych kosztów na jej modernizację.

Konieczność poufności kodów chowających dane w innych dokumentach wymaga, by prace nad ich tworzeniem przebiegały indywidualnie albo w małych zespołach. Im większa grupa ekspertów, tym większe prawdopodobieństwo, że algorytmy dostaną się w niepowołane ręce.

12. Podsumowanie

Steganografia podobnie do innych nowoczesnych technologii niesie ze sobą dwojakiego rodzaju emocje. Po pierwsze, stanowi ona podporę dla internautów wierzących, że dzięki zastosowaniu metod steganograficznych uda się zachować najważniejszą ideę Internetu, czyli wolność wypowiedzi. Coraz częściej pojawiające się wypowiedzi polityków o tym, że powinno się wprowadzić cenzurę wśród użytkowników Internetu, stanowią wyzwanie dla internautów, by dążyli do doskonalenia metod pozwalających zachować ochronę prywatności i swobodę wyrażania swoich poglądów.

Niestety wraz z rozwojem steganografii mamy do czynienia z pewnymi negatywnymi skutkami. Metody ukrywania informacji są znane również przestępcom i ułatwiają tym samym przekazywanie sobie informacji dotyczących łamania prawa. Szczególnie może to być niepokojące w epoce terroryzmu. Na nic mogą zdać się starsze metody wykrywania komunikacji między przestępcami stosowane przez policję, jeśli nie będzie mogła ona dostrzec komunikatów przesyłanych przez Internet.

W przyszłości należy się spodziewać rozwoju metod steganograficznych, przynajmniej teraz, gdy są one niezbyt popularne i stosowanie ich może umknąć konkurencji.

Literatura

Gałęzowski G., *Ukryty przekaz*, www.magazyn.reporter.pl/2001/10/html/0404.php.
Kaczmarek T., *Steganografia – szyfr w biuście*, www.kwp.radom.pl/pgm/pgm02_07.htm.

[16] www.steganografia.wsi.edu.pl/!index.php?serwis=rozdzial&ids=28.

Kościelny C., *Steganografia*, wykład wygłoszony 1 października 1999 r. w auli Politechniki Zielonogórskiej, Biuletyn nr 10/1 (grudzień 1999-styczeń 2000).
Stanuch S.M., *Steganografia w Intenecie*, www.jusky.delno.com.pl/stegan/2002/12/02/html.
Steganografia, www.zpw.most.org.pl/STEGANOS.HTM.
Steganografia na cenzurowanym, /arch.ipsec.pl/snews/302.html (Thu Feb 22 17:40:18 2001).
www.delphi-kurs.piwko.pl/sprytek/.
www.steganografia.wsi.edu.pl/!index.php?serwis=rozdzial&ids=28.

STEGANOGRAPHICAL METHODS OF PROTECTING DATA IN INTERNET

Summary

This article presents one the data protection methods used in companies – steganography. At the beginning there is a short presentation of the history of hiding information. The next part of the article shows some techniques which might be use in steganography. These are: text files, audio files, TCP/IP header, and the most popular – graphic. It turns out, that the best solution to protect company's data is combining steganography and cryptography. There is a low probability of detecting and encoding hidden information. In the end of the article there is a short description of steganography applications.