Józef LUBACZ*, Wojciech MAZURCZYK*, Krzysztof SZCZYPIORSKI*

Steganografia sieciowa

Istota steganografii

Istotą steganografii jest przekazywanie tajnych informacji w taki sposób, by nie ujawniać osobom postronnym ich istnienia ani samego faktu ukrytej komunikacji. Steganografia jest odmienna od kryptografii, której celem jest ochrona treści przesyłanej wiadomości przed jej odczytaniem przez osoby nieuprawnione, przy czym sam fakt komunikacji może być znany.

Do przeprowadzenia steganograficznej wymiany danych jest niezbędne wykorzystanie nośnika, w którym ukrywa się tajne informacje. W historii nośnikami tajnych informacji były: skóra głowy, tabliczki woskowe i zapisane kartki papieru. Aby nośnik nadawał się do prowadzenia ukrytej komunikacji, muszą zostać spełnione dwa warunki. Po pierwsze, wprowadzenie ukrytej wiadomości nie może powodować łatwo wykrywalnych zmian samego nośnika, a po drugie, nośnik powinien być powszechnie wykorzystywany.

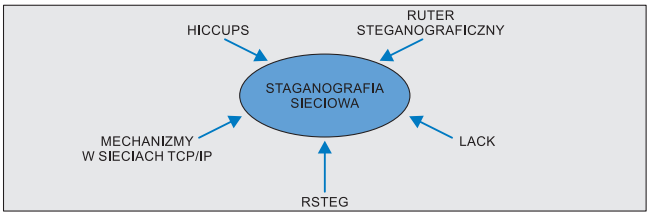
Steganografia sieciowa

Metody steganograficzne ewoluują wraz z rozwojem nowych form komunikacji międzyludzkiej, zatem ewoluuje też rodzaj nośnika tajnych danych. Współczesne rozwiązania i prace badawcze w dziedzinie steganografii koncentrują się głównie na ukrywaniu informacji w treściach multimedialnych (cyfrowych obrazach, plikach dźwiękowych, filmach wideo, przesyłanym tekście) oraz w sieciowych protokołach komunikacyjnych. W pierwszym przypadku, podobnie jak w metodach historycznych, istotą rozwiązań steganograficznych jest wpisanie ukrytych danych w nośnik w taki sposób, aby były one niewykrywalne przez zmysły człowieka (wzrok, słuch). W przypadku steganografii, wykorzystującej jako nośnik protokoły sieciowe, modyfikacji podlegają określone właściwości protokołów, takie jak zawartość pól opcjonalnych, sekwencje wysyłanych wiadomości itp. Stąd metody steganograficzne, wykorzystujące jako nośnik ukrytych informacji jednostki danych lub sposób ich wymiany w sieciach telekomunikacyjnych, określa się mianem steganografii sieciowej (termin ten został wprowadzony w [1] w 2003 roku).

Przedstawiony w pracy [1] system **HICCUPS** (*Hidden Communication System for Corrupted Networks*) otworzył zainteresowanie świata naukowego na steganografię w sieciach bezprzewodowych, a także był przykładem pierwszego systemu, w którym zastosowano filozofię zepsutych sieci, tj. sieci o pozornie wadliwej funkcjonalności. Wadliwe, niezgodne ze specyfikacją zachowanie się sieci umożliwia tworzenie ukrytego systemu wymiany informacji. Kolejne propozycje grupy, w tym [3] i [10], są nowymi zastosowaniami filozofii zepsutych sieci.

Badania nad steganografią sieciową w ITPW

W Instytucie Telekomunikacji Politechniki Warszawskiej w 2002 roku powstała Grupa Bezpieczeństwa Sieciowego **GBS** (*Network Security Group*). Jednym z kierunków jej działania są badania nad nowoczesnymi metodami ukrywania informacji, w szczególności steganografią sieciową, oraz nad sposobami ich detekcji (rys. 1). Do osiągnięć Grupy w tej dziedzinie można zaliczyć: około 25 publikacji, 2 doktoraty, 2 patenty, zespołową nagrodę Rektora Politechniki Warszawskiej I stopnia za osiągnięcia naukowe za 2008 rok, uczestnictwo w projektach zarówno zagranicznych (m.in. dla Sił Zbrojnych Stanów Zjednoczonych, a także w ramach FP7), jak i krajowych (PBZ, granty MNiSW). Ponadto w listopadzie 2009 roku w Wuhan w Chinach została zorganizowana przez członków GBS pierwsza konferencja poświęcona steganografii sieciowej – **IWNS 2009** (*International Workshop on Network Steganography*). Druga edycja jest planowana na jesieni 2010 r. również w Chinach w mieście Nankin. Od 2006 roku GBS współorganizuje międzynarodową konferencję *Secure Information Systems* w ramach *International Multiconference on Computer Science and Information Technology.*



Rys. 1. Nowoczesne metody steganografii sieciowej opracowane przez GBS w ITPW

W 2003 roku zespół zaproponował pierwszy system steganograficzny dla bezprzewodowych sieci lokalnych (**WLAN**) o akronimie HICCUPS [1] wykorzystujący do ukrytej transmisji ramki z celowo niepoprawnymi sumami kontrolnymi. Idea działania tego systemu została zgłoszona do Urzędu Patentowego RP jako wynalazek (przyznanie prawa wyłącznego nastąpiło w 2009 roku), a wyniki badań jego własności zawarto w rozprawie doktorskiej [2].

W latach 2007 – 2008 w ramach projektu badawczego dla Sił Zbrojnych Stanów Zjednoczonych GBS uczestniczyła w opracowywaniu i badaniu koncepcji rutera steganograficznego, urządzenia mającego wiele mechanizmów steganograficznych i potrafiącego komunikować się z innymi tego rodzaju urządzeniami za pomocą ukrytych kanałów komunikacyjnych [4]. Steganograficzny ruter został zrealizowany w technice agentów mobilnych, a więc może pełnić rolę programowego szpiega.

W 2008 roku zespół opublikował artykuł [3], w którym – oprócz analizy możliwości ukrywania informacji w telefonii IP – zawarto propozycję nowej metody steganograficznej o akronimie **LACK** (*Lost Audio Packets Steganography*). LACK jest przeznaczony dla szerokiej klasy usług czasu rzeczywistego, w szczególności dla telefonii IP. Został on zgłoszony do Urzędu Patentowego RP jako wynalazek. Metoda LACK celowo wykorzystuje opóźnione w nadajniku pakiety jako metodę do prowadzenia ukrytej komunikacji. Taki sposób ukrywania informacji spotkał się z dużym zainteresowaniem środowiska naukowego, jak również mediów na całym świecie. Artykuł na temat LACK zamieściło prestiżowe czasopismo *New Scientis* w numerze z dnia 31.05.2008 roku. W tym samym czasie metody ukrywania informacji w telefonii IP otrzymały miano steganofonii. Badania nad metodą steganograficzną LACK zostały zawarte w rozprawie doktorskiej [6], a także w artykule [9]. Natomiast zwieńczeniem badań nad steganografią w telefonii IP jest artykuł zaproszony w lutowym wydaniu prestiżowego czasopisma *IEEE Spectrum* w 2010 roku [8].

* **Instytut Telekomunikacji, Wydział Elektroniki i Technik Informacyjnych Politechniki Warszawskiej,**
e-mail: {jl, wmazurczyk, ksz}@tele.pw.edu.pl

Kontynuacja prac badawczych w 2009 roku zaowocowała opracowaniem nowej metody RSTEG (*Retransmission Steganography*), wykorzystującej do ukrytej wymiany danych protokoły stosujące mechanizmy retransmisji [10]. Również to rozwiązanie cieszyło się dużą popularnością medialną, m.in. opis tej metody steganograficznej w *New Scientist* z dnia 26.05.2009 roku. Zespół koncentrował się również na metodach steganografii sieciowej wykorzystujących inne mechanizmy sieci TCP/IP np. fragmentację pakietów IP [7] oraz metody możliwe do zastosowania w innych usługach czasu rzeczywistego niż telefonia IP [5].

Obecnie Grupa Bezpieczeństwa Sieciowego w Instytucie Telekomunikacji PW skupia się na opracowaniu nowoczesnych i szybkich metod detekcji zastosowania steganografii sieciowej w sieciach IP, co jest przedmiotem badań w ramach uzyskanego projektu badawczego MNiSW pt.: *Metody i środowisko badawcze steganografii sieciowej*.

* * *

W niniejszym artykule przedstawiono badania oraz osiągnięcia w dziedzinie steganografii sieciowej Grupy Bezpieczeństwa Sieciowego, działającej w Instytucie Telekomunikacji Politechniki Warszawskiej. Przedstawiono kierunki badań, zaprezentowano w sposób ogólny sposób działania zaproponowanych rozwiązań oraz wskazano obecne i przyszłe tematy badawcze podejmowane przez GBS.

LITERATURA

[1] Szczypiorski K.: *HICCUPS: Hidden Communication System for Corrupted Networks* In Proc. of: The Tenth International Multi-Conference on Advanced Computer Systems ACS'2003, October 22 – 24, 2003 – Międzyzdroje, Poland

[2] Szczypiorski K.: *Stenografia w bezprzewodowych sieciach lokalnych*, rozprawa doktorska, styczeń 2007, Instytut Telekomunikacji PW

[3] Mazurczyk W., Szczypiorski K.: *Steganography of VoIP Streams*, In: R. Meersman and Z. Tari (Eds.): OTM 2008, Part II – Lecture Notes in Computer Science (LNCS) 5332, Springer-Verlag Berlin Heidelberg, Proc. of The 3rd International Symposium on Information Security (IS'08), Monterrey, Mexico, November 10 – 11, 2008

[4] Szczypiorski K., Margasiński I., Mazurczyk W., Cabaj K., Radziszewski P.: *TrustMAS – Trusted Communication Platform for Multi-Agent Systems*, In: R. Meersman and Z. Tari (Eds.): OTM 2008, Part II – Lecture Notes in Computer Science (LNCS) 5332, Springer-Verlag Berlin Heidelberg, Proc. of The 3rd International Symposium on Information Security (IS'08), Monterrey, Mexico, November 10-11, 2008

[5] Mazurczyk W., Lubacz J., Szczypiorski K.: *Hiding Data in VoIP*, In Proc of: The 26th Army Science Conference (ASC 2008), Orlando, Florida, USA, December 1 – 4, 2008

[6] Mazurczyk W.: *Steganografia w telefonii IP*, rozprawa doktorska, listopad 2009, Instytut Telekomunikacji PW

[7] Mazurczyk W., Szczypiorski K.: *Steganography in Handling Oversized IP Packets,* In Proc. of: First International Workshop on Network Steganography (IWNS'09), Wuhan, Hubei, China, 18-20 November, 2009 – co-located with 2009 International Conference on Multimedia Information Networking and Security (MINES 2009), Vol. I

[8] Lubacz J., Mazurczyk W., Szczypiorski K.: Vice over IP – In: IEEE Spectrum, ISSN: 0018-9235, February 2010

[9] Mazurczyk W., Lubacz J.: *LACK – a VoIP Steganographic Method* – In: Telecommunication Systems: Modelling, Analysis, Design and Management, Vol. 45, Numbers 2-3, 2010, ISSN: 1018-4864 (print version), ISSN: 1572-9451 (electronic version), Springer US, Journal no. 11235

[10] Mazurczyk W., Smolarczyk M., Szczypiorski K.: *RSTEG: Retransmission Steganography and its Detection,* to be published in: Soft Computing in 2010, ISSN: 1432-7643 (print version) ISSN: 1433-7479 (electronic version), Journal no. 500, Springer

Józef LUBACZ, Wojciech STAŃCZUK**

Modelowanie aukcji i giełd zasobów transportowych sieci telekomunikacyjnych

PRZEDMIOT I ZAKRES BADAŃ

Badania nad giełdami przepustowości prowadzone w Instytucie Telekomunikacji Politechniki Warszawskiej wpisują się w poszukiwania nowych modeli biznesowych zarządzania zasobami sieci telekomunikacyjnych. Ich stały rozwój jest motywowany z jednej strony zwiększaniem stopnia komplikacji relacji rynkowych między uczestnikami rynku i pojawianiem się nowych ról biznesowych, z drugiej ewolucją architektury sieci telekomunikacyjnych w kierunku **NGN** (*Next Generation Network*), w której warstwa przesyłu danych (transportowa) jest oddzielona od realizacji usług. Stwarza to potrzebę stałej wymiany handlowej różnych towarów i usług między uczestnikami rynku telekomunikacyjnego, w szczególności również w odniesieniu do zasobów transportowych sieci, tworzących techniczną infrastrukturę przesyłu informacji.

*** Instytut Telekomunikacji, Wydział Elektroniki i Technik Informacyjnych Politechniki Warszawskiej, e-mail: jl@tele.pw.edu.pl, w.stanczuk@tele.pw.edu.pl**

Badania nad mechanizmami handlowymi w kontekście zasobów sieci telekomunikacyjnej wywodzą się z prac związanych z taryfikacją usług i rozliczeniami międzyoperatorskimi. Dotyczą one kwestii racjonalnego i sprawiedliwego dostępu do współdzielonych zasobów sieci przez wielu klientów/użytkowników oraz przedsiębiorstw telekomunikacyjnych. Istotnym wnioskiem z analizy dotychczas stosowanych mechanizmów handlowych jest zauważalna trudność, zarówno techniczna, jak i koncepcyjna, realizacji rynku zasobów sieci na poziomie dostępu do usług i aplikacji w obu stykach: usługodawca-klient, usługodawca-usługodawca. Duża dynamika zmian na rynku i pojawianie się nowych usług powoduje komplikację ewentualnego systemu informacyjnego wspierającego handel zasobami w warstwie usługowej. Obecnie bardziej realna (technicznie i ekonomicznie) jest możliwość organizacji rynku zasobów transportowych sieci (np. połączeń cyfrowych w sieci SDH czy połączeń optycznych w sieci WDM), gdzie dynamika zmian jest mniejsza oraz określenie przedmiotów handlu może być łatwiejsze.

Prowadzone prace badawcze mają charakter interdyscyplinarny i dotyczą technicznych oraz ekonomicznych aspektów wymiany handlowej na rynku zasobów sieci. Ich zakres został zilustrowany na rys. 1.