ACCEPTED FROM OPEN CALL

Principles and Overview of Network Steganography

Józef Lubacz, Wojciech Mazurczyk, and Krzysztof Szczypiorski

ABSTRACT

The article discusses basic principles of network steganography, which is a comparatively new research subject in the area of information hiding, followed by a concise overview and classification of network steganographic methods and techniques.

INTRODUCTION

As the production, storage and exchange of information becomes more extensive and important in the functioning of societies, the problem of protecting the information from unintended and undesired use becomes more complex. In modern societies, protection of information involves many interdependent policy and technological issues related to information confidentiality, integrity, anonymity, authenticity, utility, etc. Classification of these issues is a problem in itself. Several such classifications have been proposed; among the most popular are the CIA Triad (Confidentiality, Integrity and Availability) and the Parkerian Hexad [9]. In this article, we do not discuss this type of conceptualisations; we focus on methods for providing confidentiality in the communication of digitised information. Our goal is to characterise a subset of such methods named network steganography which are information hiding techniques that utilise network protocols as enablers of hidden communication (the term network steganography was first coined in [12]). To authors' best knowledge this article is the first systematic discussion of network steganography principles and techniques.

Steganography is an ancient idea of hiding information; the specific methods used have evolved during its long history [2]. In the context of contemporary information and communication technology, most research work was devoted to methods of hiding secret information in numerical data, text and images [1] transmitted between communicating parties. Such methods are generally independent of the communication logic and mechanisms — the communication protocols — that are used in particular communication networks. In these methods the transmitted user-data is a protocol-independent carrier of hidden information. Network steganography differs from such methods in that it based on using — "manipulating" — specific communication protocols' features to transmit secret information. Consider, for example, a query-response type of exchange of messages for which the communication protocol assumes that the response should come within a specific time limit; otherwise, it is treated as excessively delayed and discarded. Communicating parties that want to use this protocol for steganographic purposes may make an agreement, which becomes their shared secret, that the responses carrying hidden information will be purposefully excessively delayed and that such responses will be read by the recipient (i.e., not discarded). This "trick" (manipulation of the communication protocol) may be effective only if the communication channel introduces some delay in the message transmission. Potential observers of the communication — potential attackers — who know the communication protocol and follow it during observation, do not become suspicious of the existence of hidden communication if the frequency of occurrence of excessively delayed responses is not considered to be abnormal, i.e., does not exceed some expected frequency that the observers assume, based on their knowledge of delay properties of the communication network.

Before going into detailed description of the state of the art in network steganography, we present the following remarks concerning some terminological confusion with respect to the terms: information hiding, steganography and cryptography.

As it is well known, the terms steganography and cryptography originate from the ancient Greek words *steganos*, meaning protected (covered), and *kryptos*, meaning hidden (secret), respectively. Although the Greek terms are semantically quite close, it is plausible to consider steganography and cryptography as different methods of hiding information: steganographic methods hide information, thereby making it "difficult to notice" (by means of embedding it in an information carrier), while cryptographic methods hide information by making it "difficult to recognize" (by means of transforming it). Both cryptography and steganography techniques are practically applied in imperfect communication environments imposed by physical features of information carriers. While this imperfectness is generally an obstacle for cryptography, it is an essential enabling condition for many network steganography techniques that utilise redundant communication mechanisms

Józef Lubacz, Wojciech Mazurczyk, and Krzysztof Szczypiorski are with the Warsaw University of Technology.

0163-6804/14/$25.00

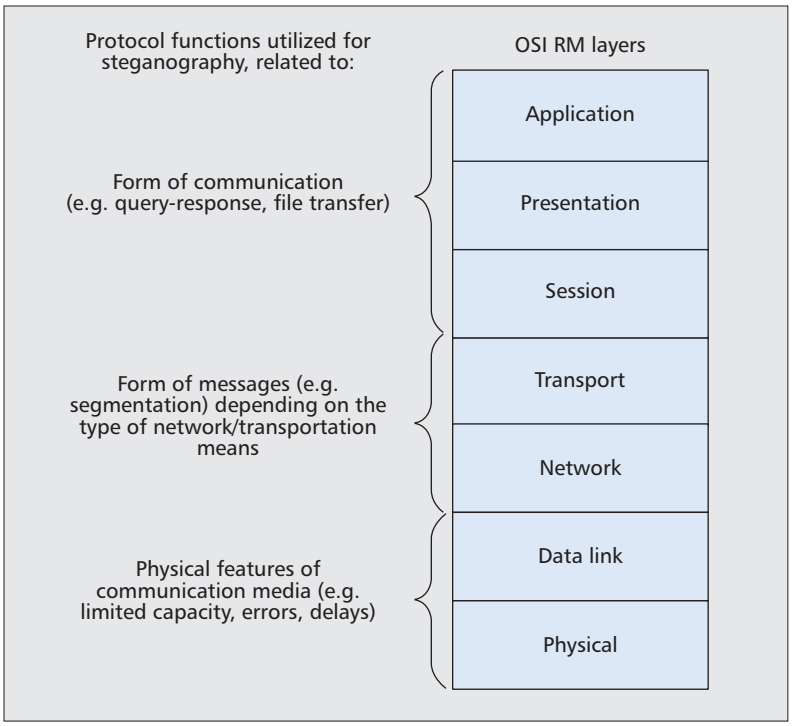

Figure 1. Protocol functions used for network steganography, associated with OSI RM layers.

(protocols) implemented to cope with such imperfect environments (to provide reliable communication). In principle, a message to be hidden with the use of a steganographic technique may be first encrypted with some cryptographic technique. Note, however, that if applied, this will potentially increase the probability that the message is noticed and thus reduces the chance of achieving the principal goal of the steganographic method in use. As will be explained in the following, there is a trade-off between the effectiveness of any network steganographic technique (in terms of potential steganographic capacity) and its susceptibility to steganalysis (i.e., to being uncovered). Essentially, evaluating the effectiveness of a particular technique requires analysis of its robustness to steganalysis. This, in principle, requires considering potential methods of uncovering the hidden communication, i.e. steganalysis methods, which constitutes another distinctive feature of steganography with respect to cryptography. Considering the above said, the main objectives, features and potential applications of information hiding with the use of steganographic and cryptographic methods should not be regarded as competitive and/or complementary.

In general, possible use of steganographic methods may be both legal and illegal. Examples of illegal use are well known: criminals' communication, exfiltration of confidential data from guarded systems, hacker tools exchange, industrial espionage. Legitimate use include circumvention of web censorship and surveillance by oppressive regimes, enabling computer/network forensic methods and copyright protection. It is less known that steganographic methods can be also used to improve quality of service (e.g. resistance to packet losses in IP telephony), to extend communication bandwidth and to provide means for secure cryptographic key distribution [16].

Basic principles of network steganography are introduced and discussed; a concise overview and classification of network steganographic methods are presented; we conclude our work with a general remark.

Network Steganography Basics and Principles

Generally speaking, when considering any communication network, three basic functionalities may be distinguished: services/applications, transport of information and information flow control. In the traditional PSTN/ISDN, i.e., circuit-switched networks, the services/applications are basically provided by the network, transport takes place through transparent channels, and the control and transport functions are virtually separated. Once the end-to-end connection and transport channel are established, information (voice or data) is transported through the network without interference. The network user has little influence on the service delivered by the network and no influence on the flow of information. The Internet, i.e., a packet switched network, has substantially changed the traditional circuit-switched network paradigm: services/applications are created by the network users rather than by the network itself, and the transport and control functions are not separated and can be influenced by the user. This change of paradigm was one of the main sources of the tremendous success of the Internet. However, these advances also introduced well-known problems with quality of service and with protecting the network and its users from harmful/undesired interference. It is thus not surprising that the Internet opened many new options for covert communication. This observation may be generalised to practically all types of contemporary fixed and mobile networks, and particularly to communication protocols, which are becoming increasingly diverse and complex, and thus susceptible to manipulation. Network steganography techniques take advantage of this susceptibility.

As indicated by the simple example described in the introduction to this article, even elementary functions of communication protocols can be utilised to construct a steganographic method. In general, the following features of network steganography techniques may be formulated:

C1: Some functions of communication protocols are modified;

C2: The modification pertains to:

C2a: Functions of the protocols that are introduced to cope with the intrinsic imperfectness of communication channels (errors, delays, etc.)

and/or to

C2b: Functions of the protocols that are introduced to define the type of information exchange (e.g. query-response, file transfer, etc.) and/or to adapt the form of messages (e.g. fragmentation, segmentation, etc.) to the information transmission carrier;

C3: The modifications are utilised by the communicating parties to make the observable effects of modifications difficult to discover (e.g., to seem to result from the imperfectness of the communication network and/or protocols).

Conditions C1, C2 and C3 constitute a proposed definition of network steganography techniques.

Note that if condition C1 is not fulfilled, i.e., if there is no interference in the communication protocol, then some form of hidden communication still may be performed, namely if the secret shared by the sender and receiver is of the form: messages a, b, c, …, are interpreted as x, y, z …. Such hidden communication cannot be discovered by observing the exchange of messages, as these are interpreted on the semantic/pragmatic level by the sender and receiver. In effect, such hidden communication can be discovered only if the shared secret is disclosed. Obviously, this is not a very interesting case for research.

Condition C2 refers to the fact that real world communication protocols must realise functions (C2a) that provide required quality-related performance of communication and functions (C2b) that govern the "logic" of communication and adapt the messages to the format of transmission carriers. If the communication functions are decomposed into functional layers, as for example in the OSI RM (Open Systems Interconnection Reference Model), then C2a functions are associated with lower layers and C2b functions with upper layers. In Fig. 1, these functions, in association with OSI RM protocol layers, are characterised in a general manner.

The effectiveness of a particular technique depends on how successfully the C3 condition is fulfilled. Three essential measures of the effectiveness can be considered: the potential throughput of hidden messages — referred to as steganographic bandwidth — and the resistance to discovering the hidden communication, i.e., resistance to steganalysis, and robustness. Robustness is defined as the amount of alteration a steganogram can withstand without secret data being destroyed. A good steganographic method should be as robust and hard to detect as possible, while offering the highest bandwidth. The three measures are interdependent: usually, the higher the steganographic bandwidth, the lower the robustness and resistance to steganalysis. The latter is usually difficult to estimate quantitatively, as it depends not only on the sophistication of a steganographic technique but also on the knowledge and efficacy of potential observers of the communication.

A Classification and Overview of Network Steganography Techniques

As this is a short article, the following overview does not cover all of the techniques proposed in the literature. The selection of techniques discussed herein is somewhat arbitrary; nevertheless, the authors tried to select techniques that seem to be most representative in their class.

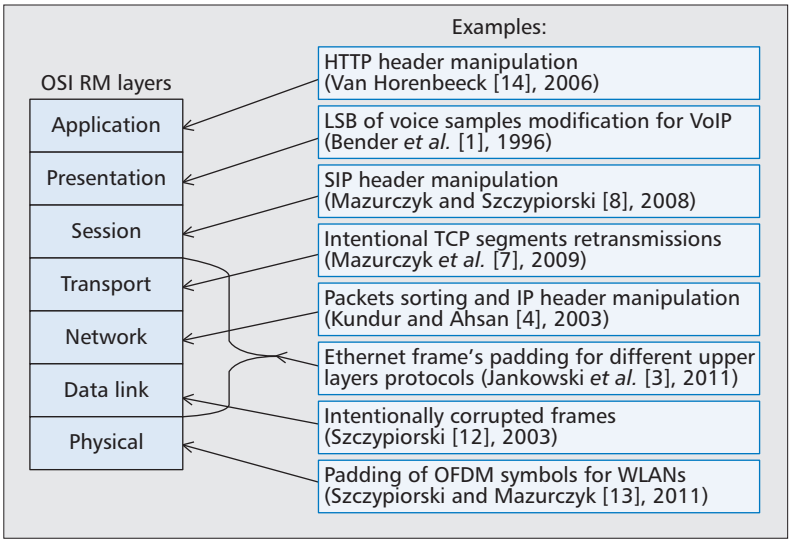

Figure 2. Network steganography methods classification based on protocol functions associated with OSI RM layers.

Classification of network steganography methods may be based on protocol functions associated with the OSI RM layers (Fig. 2).

Another possible classification of network steganography techniques may be based on the type of modification of Protocol Data Units (PDUs). Three types of modification may be considered:

1. Modification of SDUs (Service Data Units)
2. Modification of PCI (Protocol Control Information)
3. Modification of time-relations between PDUs

Case (1) includes modification of user data. Case (3) is realised, e.g., by reordering of packets and introducing purposeful delay of selected packets. Hybrid solutions involve a combination of the three cases. The classification is illustrated in Fig. 3. Hybrid solutions were introduced last; the first solutions were based on case (1), followed by solutions based on case (2).

In the physical and data link layers, steganographic techniques can exploit physical features of communication channels and/or imitate their imperfectness. For example, Szczypiorski and Mazurczyk [13] proposed a physical layer method called WiPad (Wireless Padding) intended for IEEE 802.11 OFDM networks. It is based on the insertion of secret data into the padding of transmitted OFDM symbols. The experimental results prove that maximum steganographic bandwidth for this method can reach 1.5 Mb/s (one of the highest values for steganographic methods proposed so far).

Szczypiorski introduced a data link layer method called HICCUPS (Hidden Communication System for Corrupted Networks) [12]. The main idea of the method is to use transmission frames with intentionally wrong checksums for covert communication. In a WLAN all user terminals can "hear" data contained in frames transmitted in the medium. Normally, frames with wrong checksums are discarded by terminals, whereas terminals aware of the use of the steganographic method may read such frames

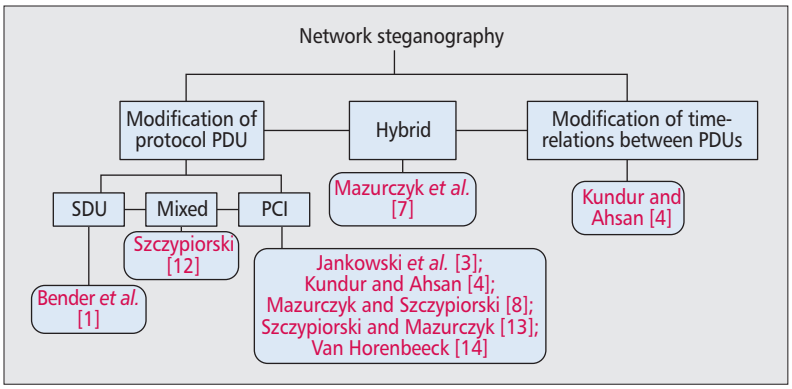

Figure 3. Network steganography classification based on the type of PDUs modification.

and extract secret data from the frame payload field. HICCUPS potentially obtains quite a high steganographic bandwidth, for example, for a IEEE 802.11g (ERP-OFDM) 54 Mb/s network with 10 terminals and 5 percent of corrupted frames, about 1 Mb/s is achievable.

Network steganography methods can also use the adjustment of the form of the messages to the type of network or means of transport. Kundur and Ahsan [4] proposed two such approaches for the OSI RM network layer. In one solution, the bits of hidden data are carried in unused or reserved parts of packet headers. This method is feasible because many protocol standards do not mandate specific/standard values for the unused and reserved parts (these are not verified at the receiver). In particular, Kundur and Ahsan proposed utilization of the IP header's DF (Don't Fragment) flag. This approach is successful if the sender generates packet sizes smaller than the path's MTU (Maximum Transfer Unit). Many similar methods, based on the reuse of other fields of various protocols, were introduced: e.g. Handel and Sandford [2] proposed using the unused bits of the IP header's ToS (Type of Service) field and of the TCP header's Flags field. The other solution that Kundur and Ahsan proposed in [4] utilises per packet sequence numbers of IP packets and their intentional re-sorting. The steganographic bandwidth achievable with these methods depends mainly on the overt communication and the frequency of embedding steganographic data.

For the OSI RM transport layer, Mazurczyk *et al.* [7] introduced the RSTEG (Retransmission Steganography) technique intended for the TCP protocol. The main idea of RSTEG is to drop acknowledgement of successfully received segments in order to invoke retransmission intentionally. The retransmitted user's segment carries secret data hidden in the payload field. Even if the rate of intentional retransmission required to mask RSTEG is low (0.1 percent) and TCP segments are generated at a rate of 200 segments/s, the resulting steganographic bandwidth is about 1.4 kbit/s.

In [8] Mazurczyk and Szczypiorski suggested the utilisation of unused fields of the session layer protocol SIP (Session Initiation Protocol). The authors introduced a new steganographic methods for SIP and the closely related SDP protocols (used in the signalling phase of IP telephony calls), based on using free or unused fields of the protocols; the achievable steganographic capacity exceeds 2000 bits in one direction of an average VoIP call.

For the presentation layer, Bender *et al.* [1] introduced various methods that embed hidden data into user data, e.g., by modifying the least significant bits of voice samples (audio) or pixels (images). The resulting steganographic bandwidth is even up to 4 kbit/s.

Van Horenbeeck [14] proposed steganographic methods for the HTTP (Hypertext Transfer Protocol) protocol using in particular: modification of header field values, reordering of header fields, modification of lower or upper cases, influencing the presence or non-presence of optional header fields.

Network steganography can also use more than one protocol, in particular protocols from more than one OSI RM layers. Jankowski *et al.* [3] developed such a technique, called PadSteg (Padding Steganography). The term *inter-protocol steganography* has been proposed for this class of methods. PadSteg utilises protocols like ARP, TCP, UDP or ICMP, referred to as carrier-protocols, together with the Etherleak vulnerability (improper frame padding caused by ambiguities of the standardisation). To exchange steganograms, secret data is inserted into Ethernet frame padding of one of the carrier-protocols. While the secret communication occurs, hidden nodes can switch between carrier-protocols to minimise the risk of disclosure. The experimental steganographic bandwidth was roughly estimated to be 32 bit/s.

The pros and cons of the described groups of steganographic methods are highlighted in Table 1.

As can be seen from the above overview, network steganographic methods that are predecessors of the newer, more sophisticated ones, mainly utilize various unused or reserved fields of the TCP/IP stack protocols [4]. The current trend in network steganography targets mainly popular services: multimedia, real-time services like Skype [11], popular P2P (Peer-to-Peer) services like BitTorrent [10] and social media sites like Facebook [5]. Also new, popular environments are targeted, e.g. wireless network environments such as Wireless Local Area Networks (WLAN) [13] and cloud computing [15].

Conclusions

Due to the constantly increasing complexity of communication protocols, there is little doubt that new, more sophisticated steganographic techniques will be created and, in effect, the risk that they will be used for malicious purposes will rise. This concern adds new challenges to the difficult issue of providing network and information security. A deep understanding of the susceptibility of communication protocols to all types of manipulation (not only for steganographic purposes!) becomes an extremely important issue. Research in the area of network steganography may be helpful in this respect — may result in useful guidelines for a methodology of designing a new generation of robust communication protocols and communication networks in general. We strongly believe that the

Group of methods	Pros	Cons
Methods that modify protocol PDU/PCI	–High steganographic bandwidth –Easy implementation –No sender-receiver synchronization required	–Potential loss of some of the protocols' functionality –Easy to detect
Methods that modify protocol PDU/SDI	–Harder to detect than PCI-based methods –No sender-receiver synchronization required	–Lower steganographic bandwidth than PCI-based methods –Harder to implement than PCI-based methods –Potential deterioration of quality of user data
Methods that modify protocol PDU/Mixed	–High steganographic bandwidth –Hard detection –No sender-receiver synchronization required	–Harder to implement than PCI-based and SDI–based methods –Potential increased transmission error rate
Methods that modify time-relations between PDUs	–Easy implementation –Hard detection	–Very low steganographic bandwidth –Sender-receiver synchronization required –Increased transmissions' delays
Hybrid methods	–Hard to detect –No sender-receiver synchronization required –High steganographic bandwidth –Easy implementation	–Potential deterioration of quality of user data

Table 1. Comparison of steganographic methods groups (comp. Fig. 3).

results of research on network steganography should not be regarded as restricted to information hiding techniques per se.

Acknowledgments

This research was partially supported by the Polish Ministry of Science and Higher Education and Polish National Science Centre under grants: 0349/IP2/2011/71 and 2011/01/D/ST7/05054.

References

[1] W. Bender *et al.*, " Techniques for Data Hiding," *IBM System J.*, vol. 35, no. 3,4, 1996, pp. 313–36.
[2] T. Handel and M. Sandford, "Hiding Data in the OSI Network Model," *Proc. 1st Int'l. Wksp. Information Hiding*, 1996, pp. 23–38.
[3] B. Jankowski, W. Mazurczyk, and K. Szczypiorski, "PadSteg: Introducing Inter-Protocol Steganography," *Telecommunication Systems J.*, vol. 52, issue 2, 2013, pp. 1101–11.
[4] D. Kundur and K. Ahsan, "Practical Internet Steganography: Data Hiding in IP," *Proc. Texas Wksp. Security of Information Systems*, Apr. 2003.
[5] S. Nagaraja *et al.*, "Stegobot: A Covert Social Network Botnet," *Information Hiding*, Springer, 2011, pp. 299–313.
[6] J. Lubacz, W. Mazurczyk, and K. Szczypiorski, "Vice Over IP," I*EEE Spectrum*, ISSN: 0018-9235, Feb. 2010, pp. 40–45.
[7] W. Mazurczyk, M. Smolarczyk, and K. Szczypiorski, "Retransmission Steganography and Its Detection," *Soft Computing*, vol. 15, issue 3, 2011, p. 505.
[8] W. Mazurczyk and K. Szczypiorski, "Covert Channels in SIP for VoIP Signaling," *Proc. 4th Int'l. Conf. Global E-security 2008*, London, United Kingdom, 23–25 June 2008, pp. 65–72.
[9] D. B. Parker, "Toward A New Framework for Information Security," S. Bosworth and M. E. Kabay, *The Computer Security Handbook (4th Ed.)*, New York, John Wiley & Sons. ISBN 0-471-41258-9, 2002.
[10] P. Kopiczko, W. Mazurczyk, and K. Szczypiorski, "StegTorrent: A Steganographic Method for P2P Files Sharing Service," *Proc. Int'l. Wksp. Cyber Crime (IWCC 2013)*, San Francisco, USA, May 2013, pp. 151–57.
[11] W. Mazurczyk, M. Karaś, and K. Szczypiorski, "SkyDe: a Skype-based Steganographic Method," *Int'l. J. Computers, Communications & Control (IJCCC)*, ISSN: 1841-9836, vol. 8, no. 3, June 2013, pp. 389–400.
[12] K. Szczypiorski, "Steganography in TCP/IP Networks. State of the Art and A Proposal of A New System — HICCUPS," Institute of Telecommunications' Seminar, Warsaw University of Technology, Poland, Nov. 2003, URL:http://krzysiek.tele.pw.edu.pl/pdf/steg-seminar-2003.pdf.
[13] K. Szczypiorski and W. Mazurczyk, "Steganography in IEEE 802.11 OFDM Symbols," *Int'l. J. Security and Communication Networks*, John Wiley & Sons, vol. 3:1–12, 2011.
[14] M. Van Horenbeeck, "Deception on the Network: Thinking Differently About Covert Channels," *Proc. 7th Australian Info, Warfare and Security Conf.*, Dec. 2006.
[15] T. Ristenpart *et al.*, "Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds," *Proc. 16th ACM Conf. Comp. and Commun. Security*, ACM, 2009, pp. 199–212.
[16] Y. Huang *et al.*, "Key Distribution over the Covert Communication Based on VoIP," *Chinese J. Electronics*, vol. 20, no. 2, 357–60.

Biographies

Józef Lubacz (jl@tele.pw.edu.pl) Ph.D. (1976), D.Sc. (1986), Prof. (title, 1995); prof. at Warsaw University of Technology (WUT, Poland); head of the Dep. of Teleinformatics (WUT, 1987–2002), Dean of the Faculty of Electronics and Information Technology (WUT, 2002–2005); Director of Institute of Telecommunications (WUT, since 2009), Chairman of the General Council for Science and Higher Education of Poland (2010–2013); main scientific interests: teleinformatics, philosophy of science and technology.

Wojciech Mazurczyk [SM] (wm@tele.pw.edu.pl) holds an M.Sc. (2004) and a Ph.D. (2009, with honours) in telecommunication both from Faculty of Electronics and Information Technology, WUT; assistant professor at WUT; author of over 80 scientific papers, 1 patent application and 30 invited talks on information security and telecommunications; main research interests: information hiding techniques, network anomalies detection, digital forensics, network security and multimedia services. Research co-leader of Network Security Group (secgroup.pl).

Krzysztof Szczypiorski [SM] (ksz@tele.pw.edu.pl) holds M.Sc. (1997, with honours), Ph.D. (2007, with honours) and D.Sc. (habilitation, 2012) in telecommunications from Faculty of Electronics and Information Technology, Warsaw University of Technology (WUT). Professor of Telecommunications at WUT. Research leader of Network Security Group at WUT (secgroup.pl). His research interests include: network security and wireless networks. He is the author or the co-author of 170+ publications.