INTL JOURNAL OF ELECTRONICS AND TELECOMMUNICATIONS, 2016, VOL. 62, NO. 3, PP. 315-318
Manuscript received September 7, 2016; revised September, 2016. DOI: 10.1515/eletel-2016-0043

Steganography Training: a Case Study from University of Shumen in Bulgaria

Stanimir Stanev and Krzysztof Szczypiorski

***Abstract*—This paper summarizes the experience and the learning outcomes of students of the "Informatics" specialty at the Episkop Konstantin Preslavsky University of Shumen (Bulgaria) on the problems of computer and network security as a component of their professional training. It is a continuous process starting from the "Computer steganography" course and turning into diploma papers, masters programs, specializations and PhDs in computer and network steganography. The outcome of this training would be bachelors and masters theses, practical activities of experimentation of stego software and steganology in a parallel computing environment, joint scientific publications of lecturers and students.**

***Keywords*—training steganography, computer and network steganography, steganology, cluster systems, parallel staganography**

I. Introduction

ONE of the effective approaches to protect important information is hiding its existence (data hiding). This field includes many techniques and methods including steganography [1]. It has a thousand-year-old history and propose a lot of means for hiding messages (invisible inks, microdots, secret channels, etc.). Historical sources reveal facts about the use of Steganography techniques in the Bulgarian lands. During the national struggle against the Turkish yoke the Bulgarian national hero Vasil Levski, called the Apostle of Freedom, and the revolutionary committees created by him, had used invisible inks and Cardano grilles type stencils (called “grids”, “lozinki”, “books”) [2]. Nowadays the successors of the classical steganography methods are computer and network steganography - independent scientific aspects of information security, studying the problems of creating components with hidden information in the visible information environment generated by computer systems and networks. Unfortunately these methods are now used by malicious organizations and criminals too. The topicality of the problem is related to the responsibilities of security services for effective countering against the steganography methods and requires familiarization with the basics of modern steganology of a wider range of specialists whose task is not only developing, analyzing or countering the steganography techniques but also a qualified selection of the existing steganography technologies and their skillful use to solve specific practical problems in the field of information protection. This is particularly important for the future specialists in the field of computer science.

II. Purpose for Steganography Training

Undoubtedly one of the main measures for steganography protection is the creation of well-trained specialists in this field. For this purpose, vendors of hardware and software for data protection conduct training courses. This is also made by a number of academies, foundations and organizations. Many universities around the world are actively working on the training of specialists in information protection and are conducting serious research work on the creation of software and technical means for protection. Steganology issues are taught in a number of information security training courses, and even as separate courses. In the USA, Jessica Fridrich of SUNY Binghamton University, NY, has taught the course “Fundamentals of steganography” since 2006 and develops research works in the field of steganography and Steganalysis, mainly with students. In Poland, the team of Krzysztof Szczypiorski at Warsaw University of Technology works on cutting edge projects on network steganography with students too. In Russia steganography issues are taught in over 110 universities [3]. There is partial data for the training of specialists in universities of the USA, the UK, Russia, Germany, Poland, the Czech Republic, China, India, Finland, Romania, Turkey, Belgium, Spain, Portugal, New Zealand, and others [4].

In Bulgaria, scientific research in the field of steganography, is carried out at Konstantin Preslavsky University of Shumen, the Technical University of Varna, the Technical University of Sofia, the Institute of Information Technologies of the Bulgarian Academy of Sciences, and others [5]. In University of Shumen the problems of steganography are considered as a component of the professional training in information security of the students majoring in computer science. The pre-history of this training started at the beginning of the second millennium. A teaching course in Computer and Network Security started for the students majoring in “National Security”. There were included the themes on steganography and its perspectives. There was formed a research student group including teachers, working on projects. The creation of a “Computer Security” computer lab was a natural outcome of this preliminary work.

This work was supported in part by Project RD-08-119/2016 “Steganography in mobile devices and 3-dimensional modeling”. The Project is realized by the financial support of the Konstantin Preslavski University of Shumen, Bulgaria.

Stanimir Stanev is with the University of Shumen, Shumen, Bulgaria (e-mail: stan_stanev@yahoo.com).

Krzysztof Szczypiorski is with the Warsaw University of Technolog, Warsaw, Poland (e-mail: ksz@tele.pw.edu.pl).

III. A Case Study: University of Shumen

Since 2010, for the first time in Bulgarian Universities, at the University of Shumen, a course on “Computer steganography” with predominantly educational – research character has been held for students majoring in “Computer Science” and “Computer Information Technologies” [6]. A comprehensive training system for this subject has been built, including instructors training through specialized courses and self-study of the collected information sources, developing new lectures and training materials, continuous improvement of the curriculum, development of course works, creating student problem groups, development of theses, teaching in Master programs, participation of students and instructors in joint research projects, improvement of the research facilities, links to research and educational institutions and organizations, and others.

The students at the University of Shumen are definitely interested in this course. The instructors from the Computer Systems and Technologies Department at the Faculty of Mathematics and Informatics have issued the monograph ”Steganologic Protection of the Information” and ”A Manual on Steganography Exercises” to facilitate the training of the students [2,7]. The students are also advised to use sources of foreign authoritative authors [8,9]. Within the scope of scientific relations with the Povolzhsky State University of Telecommunication and Informatics – Samara, Russia, there have been exchanged two textbooks and software for network steganography [10]. The course teachers are guided by the idea that it is impossible to consider the steganography methods in isolation from cryptography in which field another instructors from Shumen University work as well.

Although historically steganography has appeared earlier than cryptography, first some principles of the information crypto protection are learnt because its theory has been developed considerably deeper in comparison with that of steganography. Since cryptography algorithms are widely used to form a pseudo-random number, the University of Shumen conducts research in this field. That material is discussed at the educational seminars [11]. Due to the use of various multimedia containers for steganographic hiding of information the study of file formats of graphic, audio, text and video files is included within the curriculum, as well as in WEB-applications. Following the rapid development of the scientific field and the constant introduction of new methods and programs, together with the experience gained in teaching each year the content of the subject has been changing as well. The last change was the introduction of the topic on network steganography [24], based on materials from the web-site of the stegano.net project [12]. The current version of the program of the "Computer steganography" course includes 50 hours of training, including 25 hours of lectures and 25 hours seminars conducted in classrooms and the Computer Security Lab. The lectures include topics like "Problems of computer and network security " (it includes general issues on computer security, threats and attacks and approaches to protect computer systems and networks), "Cryptographic algorithms in steganography", "Fundamentals of computer steganography”, "Selecting Steganography containers", "Network steganography", "Hidden identification systems" (Digital watermarks, fingerprints), "Steganalysis and effectiveness of Steganography algorithms and programs", "Development of protection systems". Through the self-training tasks and the instructors guidance the students are in constant touch via the Internet with current steganologic software. Course works are assigned on studying the effectiveness of free Internet stegoprograms, finding current information about various Steganography methods and its translation from English and Russian, development of papers on specific steganology issues. The instructors offer for analysis and comparison stego programs developed by instructors and graduates. They use some of their scientific developments as well and discuss them during the seminars with the students. Seminars in practical terms discuss issues like “Standards for Information Security”, "Security Policy", “Information Encryption”, “Software for encryption of messages on the Internet”, “Algorithms and programs for Steganography protection of text files”, “Development of own programs for the implementation of the LSB method”, “Use of audio containers and video sequences to hide the information”, “Analysis of methods and tools for network steganography”, “High-tech Steganography approaches for mobile computing devices”, “Types of Steganalysis”, “Programs for Steganalysis”, “Comparative analysis of stego programs”, ”Studying the effectiveness of the Steganalysis software”. The teaching material is connected with the most popular algorithms (for example the LSB method).

Students have the opportunity to learn about and offer their ideas in clarifying the terminology, the research parameters, benchmarking of steganography and stegoanalytical programs, choice of ciphers to further provide steganography transmission, ideas for stegoanalytical programs and others. Due to the hard work of the students on their assignments one of the joint results and definition of the key steganalogy terms in Bulgarian and detailed taxonomy of the steganology methods have been reached, and namely there were compared and found the closest in meaning equivalent terms in English and Russian [13]. There is an interesting example from the seminars. Students logically reached the term steganology themselves - a collective term for steganography and steganalysis, by analogy with cryptology consisting of cryptography and cryptanalysis. Then they were surprised to find that not so long ago - in 2005, this term was adopted by the global scientific community. The term effectiveness of the stego system was introduced as a set of specialized software and hardware, not just as a steganography method [14]. There was introduced the concept of steganologic protection (stegoprotection) to the complex of organizational and hardware and software measures to prevent stego incidents and there were considered two main aspects of the stegoprotection - protection of secret information using the steganalysis methods against exfiltration, and stegoprotection of information against unauthorized access by hiding malware in seemingly harmless media files [2,15]. There was introduced the concept of steganologic subsystem for information security (SSIS) for the combination of hardware and software to protect information in computer systems and networks through the methods of steganography and steganalysis. An emphasizes was placed on the application of systematic approach when developing information protection systems (IPS) – the stegoprotection is to be realized as part of IPS. Variants of architectures of SSIS are presented in [16].

One of the main objectives of the study of steganography algorithms and programs was to prepare students for detecting hidden messages through steganalysis. The collaboration of students and teachers led to several articles on these issues [17,18].

The first theses of students majoring in |Computer Sciences at the University of Shumen on issues of steganography were successfully defended in 2004. From 2004 until now there have been defended more than 23 Bachelor and Master theses, there are more than 36 joint publications of instructors and students. Examples of the topics of the theses are “Efficiency of programs for Steganography protection”, “Exploring the possibilities of contemporary programs for steganalysis”, “Analysis of the possibilities of network protocols and devices for network steganography”, “Exploring the possibilities of Steganography parallel processing with a cluster computer system”. They were developed theses in the field of network steganography based on RDP protocol and others [19].

In the last year there have been developed and successfully defended student theses on steganography applications for mobile phones, stegoprotection by steganography sterilization of any multimedia containers and steganography in social networks [20,21].

The research on steganology is carried out in the Computer Security scientific research laboratory at Faculty of Mathematics and Informatics, where the research student group works. Work is done on steganography and steganalysis in parallel computing environment. Eight steganology projects have been implemented with the participation of instructors and students. They were financed by the Research fund of the University of Shumen. There is one interesting fact with that project. The pupil Katerina Velcheva from the Math and Science High School in Shumen took part in the research steganography student group. During the period 2009 - 2011 due to her excellent training as a programmer and her cooperation with the laboratory, she successfully developed and defended steganography projects. She successfully graduated as a Bachelor from the Massachusetts Institute of Technology (MIT) – USA, in 2016.

In 2012 a cluster computer system “Radian-M” with 32 cores with a total performance of 180 GFLOPS, developed by a team from the University of Shumen was assembled in the Computer Security Lab. Through it had been developed a number of programs for parallel steganography and staganalisis.

Besides the developed of stegoprograms and scientific publications, an important result is that a new direction was gradually formed not only for the University of Shumen - computer steganologiy in parallel computing environments [2,22].

The scientific qualifications of the instructors in this subject is increasing – two doctoral theses in this field were defended in 2014 (Zhelezov, Paraskevov) and a professor (Stanimir Stanev) was elected. Scientific and technical cooperation is carried out with the Institute of Defence, Universities in Russia (Moscow, Samara and Makhachkala), the Institute of Information Technologies at the Bulgarian Academy of Sciences, the University of Library Studies and Information Technologies, and the National Military University, University Politehnica of Bucharest, Warsaw University of Technology and others.

Two international scientific seminars on steganography - SHUSTEG14 and SHUSTEG16 were organized and held at the University of Shumen in 2014 and 2016. Specialists in the field of steganography and Steganalysis from Bulgaria and from foreign universities discussed the directions for practical research in the field of steganography and Steganalysis in the universities and discussed scientific publications on the subject of the seminar [21,23].

IV. Conclusions

1. A comprehensive system for training students in the field of information protection from steganography attacks has been developed in the University of Shumen by the Computer Steganography Course, which has been introduced for the first time and a research direction for parallel steganography and steganalysis is being developed. University of Shumen is a leading university in Bulgaria in this scientific field.

2. The best way for the students to master steganography is the implementation of research tasks with the laboratory works through courseworks, diploma projects and solving practical problems to extract hidden information from various containers. Although classical steganography algorithms are being studied, the students have to be aware that this is only a base for studying the new steganography methods which are constantly developing, for the purpose of a follow-up effective steganalysis.

3. Some educational and methodological problems in teaching computer steganography stood out as well. The experimental methodology of conducting classes lead to the division of students into two groups. The first group was formed by students, willing and able of creative learning and willing to participate in research works. The second group, consisting of a large number of students did not want to be away from the traditional methods of teaching and learning. In this group there were problems in the development of the courseworks, participation in seminars, and as a result - underachievement on the semester examination.

The progress of computer technologies and mobile communications will inevitably address the new challenges towards the training of specialists in high-tech steganography, and they have to be ready to meet them. The role of the higher education institutions must remain leading in the process of their education.

References

[1] Cox,I., Miller, M., Bloom, , J. Fridrich and T. Kalker. Digital Watermarking and Steganography, Second Edition. Elsewier, Morgan Kaufmann Publishers, 2008.

[2] Stanev,S. Steganological protection of information. Konstantin Preslavski University Press, Shumen, 2013. 320 p. ISBN 978-954-577-825-4. (Monography, In Bulgarian).

[3] Галяев, В. Современный уровень преподавания стеганографии в России. В: Сборник научни трудове на международната научна конференция MATTEX14, Том 1, Шумен, 2014. стр.115-119. ISBN 1314-3921.

[4] Станев,С. Предизвикателствата на стеганографията към информационната сигурност и обучението на специалисти в университетите. Сборник трудове на научна конференция „Новите предизвикателства пред системите за информационна сигурност”. ФАПВОКИС на НВУ, Шумен, 2015.ISBN 978-954-9681-65-9.стр. 36-55.

[5] Ilchev,S.,Z.Ilcheva. A new approach to Data Hiding for Web-based Applications. Prof. Marin Drinov Academic Publishing House, Sofia,2014.ISBN 978-954-322-780-8.151 p.

[6] Станев,С., С. Железов и Х. Параскевов. Обучението по компютърна стеганография в Шуменския университет „Епископ Константин Преславски". Наука, образование, сигурност. София: Издателство на НБУ, 2013. стр.445-451. ISBN:978-954-535-796-1.

[7] Stanev,S.,S.Zhelezov, H.Paraskevov and H.Hristov.Manual for steganography exercises. Konstantin Preslavski University Press, Shumen, 2015. 140 p. ISBN 978-619-201-011-9. (In Bulgarian).

[8] Fridrich, J. Steganography in Digital Media: Principles, Algorithms, and Applications. Cambridge University Press, 2010.437 p. ISBN 978-0521190190.

[9] Аграновский, А., А. Балакин , В. Грибунин и С. Сапожников. Стеганография, цифровые водяные знаки и стеганоанализ. Москва, Вузовская книга, 2009. ISBN 978-5-9502-0401-2.

[10] Алексеев, А. и В. Орлов. Стеганографические и криптографические методы защиты информации (Учебное пособие). Самара, ИУНЛ ПГУТИ, 2010. 330 с. ISBN 978-5-904029-12-8.

[11] Stoyanov, B., K. Kordov. Pseudorandom Bit Generator with Parallel Implementation (2014), Large Scale Scientific Computing 2013, Lecture Notes in Computer Science 8353, 557-564.

[12] Network Steganography Principles. [on-line]. [February,2013] http://www.stegano.net/tutorial/net-steg.html.

[13] Galyaev,V, S.Stanev. Semantic maching of scientific terms in English and Russian languages in computer steganography. Collection of the international scientific-practical conference. GAOU VPO "Dagestan State Institute of National Economy." - Makhachkala.: DGINH, 2013. p.51-56. (In Russian).

[14] Nachev, A., & Zhelezov, S. Assessing the efficiency of information protection systems in the computer systems and networks. Information Technology and Security,2013 (1), 79-85.

[15] Stanev,S., H. Hristov and D. Dimanova. Aproaches for stego defense of sensitive information. 10th International Conference on Bionics and Prosthetics, Biomechanics and Mechanics, Mechatronics and Robotics, June 2-7,2014, Liepaya, 2014.

[16] Zhelezov,S., H. Paraskevov, H. Hristov, P. Boyanov and B. Uzunova-Dimitrova. An architecture of staganological subsystem for information protection. Proceedings of ICBBM 2014, Volume 10, RTU Press, Riga, 2014. ISBN 978-9934-10-573-9. pp.123-128.

[17] Stanev,S., I. Yakimov and S. Zhelezhov. A realization of parallel stegoanalysis with a cluster system. In: Proceedings of International Scientific Conference "Modern methods and technologies in the scientific researches", University of Economics,Varna, 2012 (In Bulgarian). pp. 224-228.

[18] Zhelezov, S. Modified Algorithm for Steganalysis. Mathematical and Software Engineering, 2016, 1(2), pp. 31-36.

[19] Stanev,S., H. Paraskevov and E. Stefanova. An approach for network steganography based on RDP protocol. In: Proceedings of scientific session with international participation on the European Maritime Day, May 20 , Naval Academy, Varna, 2013.

[20] Aliev,S. Steganography applications for sterilization of multi-media objects and their application in mobile communication (Стеганографско приложение за стерилизация на мулти-медийни обекти и приложението им в мобилната комуникация). Diploma bachelor project, University of Shumen,2016.

[21] Галяев, В. О некоторых экспериментах по передаче стегосообщений через социальные сети. В: Сборник научни трудове на международната научна конференция MATTEX14, Том 1, ISBN 1314-3921. Шумен, 2014. стр.119-122.

[22] Stanev, S.,S. Zhelezov and I. Yakimov. An aproach for parallel steganalisys based on data compression. In: Proceedings of Jubilee International Congress "40 years Bulgaria – Space State ", Varna,2012, pp. 360-367.

[23] Szczypiorski, K. Art of Information Hiding in Data Networks. SHUSTEG'16, Shumen, Bulgaria, 19 May 2016.

[24] Mazurczyk, W., S. Wendzel, S. Zander, A. Houmansadr, K. Szczypiorski, "Information Hiding in Communication Networks: Fundamentals, Mechanisms, Applications, and Countermeasures", Wiley-IEEE Press; 1 edition, April 2016