UDC 004.056.5

SOFTWARE FOR PROTECTING CORPORATE NETWORK FILES USING STEGANOGRAPHIC PRINTS

PAVEL LIAKH, KANSTANTSIN RAKHANAU
Polotsk State University, Belarus

Digital prints in confidential files of the company allow determining the membership to the company and the owner of the signed files without having to check the contents. A software tool that enables the introduction of digital prints when employees access confidential campaign files allows to increase the degree of protection of intellectual property contained in digital files, and the development of this software is topical.

Introduction. One of the threats to information security of an enterprise comes from insiders [1, 2]. Insiders are employees who are within the corporate network, and have some access to corporate servers and workstations [1]. Insiders include the members who misuse their privileges and perform the role of a privileged user [1]. The definition of an insider also includes incompetent employees who unintentionally violate established information security rules.

The leakage of confidential information in the form of documents for internal use, training materials, other intellectual property objects to open access or to competitors through insiders causes significant material and non-material damage to the company. The leakage of digital files is carried out through various channels and to ensure a channel protection is not always possible due to the complexity and high cost of building a security system.

One of the effective means of protecting vulnerable company files is digital marking of the files that can be accessed by insiders. Digital prints in files provide the possibility to identify them without checking the contents that can be used to detect the leak of confidential information as well as the leak channel and to protect files from unlicensed use [2].

The main disadvantages of the existing implementations [3–9] of steganographic signing tools are a limited set of supported container formats and confidential information about the algorithms used to create a digital print, which does not allow to conclude that it is protected and stable. The advantages include the unique service for searching for the signed files in the open access and the comprehensibility of the programming interface. The need to develop a software tool for protecting corporate network files using steganographic prints is caused by the closure for changes in the existing commercial implementations and the need to integrate the software with the hardware and software environment of the corporate network and the security management system.

Corporate network. In general, a corporate network built on hardware and software consists of the following functional elements [1]:

- workplaces (subscribers);
- information servers intended for storage and processing of information arrays (databases) of various functional purposes;
- means of telecommunication that provide interaction between workstations and their interaction with information servers;
- security management system of a corporate network.

One of the methods for automating the processes of analyzing and controlling the security of the distributed computer systems is the use of the intelligent software agent technology, which is built on the console-manager-agent architecture [1]. A software agent is installed on every of the monitored subsystems, which performs tasks to control the security of the automated system. Agent management is performed through the network by the program manager. The console is used by security personnel to monitor and configure the system.

One of the elements of an integrated information security system is the data leak prevention or data loss protection (DLP) systems. The system performs control over the movement of the information at the level of communication with the external network and at the level of the end devices of users. When using DLP systems the basic approaches are grounded in the search for keywords and on the implementation of fingerprints in files [2].

DLP systems are introduced at the request of the units that manage the business of companies and are responsible for its security [2]. DLP systems are used to manage risks, reduce damage from leaks and reduce leaks of confidential information.

A software tool for protecting corporate network files using steganographic prints is built on the basis of the intelligent software agent technology for the ability to be deployed in corporate information security systems. The software belongs to the class of DLP systems and it is used in risk management.

Steganographic printing. Technologies of digital watermarks (DW) and identification numbers (IN) are used to protect copyright for intellectual property from copying and to carry out authentication. DW are built into the protected object and can be either visible or invisible. The DW and IN contain the authenticated code, the owner information and the control information. The introduction of IN is called fingerprint technology. The DW and IN technologies are used to protect electronic media against copying and prevent unauthorized use of information in electronic commerce, voice mailing, video surveillance systems and office work.

Hidden annotation of documents and optimization of data banks (information) is carried out using the technology of DW and IN. For example, the information in electronic medical records is available only to the treating physician. Hidden annotation of documents is used in medicine, cartography, multimedia data banks, as well as for searching for the necessary information in them.

Depending on the stability, the following types of prints are distinguished [10]: robust – have high resistance to external influences; fragile – destroyed with a minor modification of the filled container; semi-fragile – resistant to one impact and not resistant to others.

Fragile prints are destroyed with a minor modification of signals and are used for signal authentication. Semi-fragile prints are purposefully designed to be unstable for certain types of operations, for example, cutting or inserting fragments, but to be resistant to compression.

In this paper, it is assumed that the protected files can undergo numerous changes in the container, therefore, algorithms for creating fragile prints are not applicable. Protection is subject to intellectual property which is represented by the contents of the protected files therefore the algorithm for creating a print must have the properties of resistance to the container modifications possessed by robust and semi-fragile prints for use in this work.

There are many algorithms for introducing the print into the images [11, 13, 14]. Algorithms applicable to the images are used [15] for the introduction of the prints into the video stream. Subject to changes are several target sequence frames which are selected for the printing. Existing methods of introducing the print into the text are unstable to changes in the container that is reflected in works [1, 12, 14]. The introduction of prints into the images contained in the documents is used to protect text documents. Documents will not be subject for the introduction of the prints if they do not contain images suitable for modification.

Specific methods for creating robust and semi-fragile prints are selected on the basis of the format features for implementation, the computational complexity, the availability of existing implementations, the requirements of normative acts and other criteria.

Functional requirements. Software is designed to protect corporate confidential files by introducing prints using the steganographic method. Digital files subject to protection are educational materials in text and media formats and internal documents. The software is operated as a software agent on the information server. The agent is managed through the corporate network security management system.

The software can be used to detect leakage of confidential information, to determine the leakage path and to protect files from unlicensed use. The type of files for protection is determined at the stage of risk identification and analysis. There is the need to scan and search for digital prints of the campaign in files that are in open access for security implementation.

The software shall provide the following functions:

- creation and implementation of a sustainable print without violating the integrity of the contents of container;
- detection, retrieval and verification of the print from files;
- management of the software agent through the corporate network security management system.

Functioning. The structural diagram of the software is shown in the figure.

The software has three main components:

- the console on the corporate network security management server;
- the software agent on controlled information servers;
- the service for checking signed files.

The console is used to monitor and manage running software agents. Software agents are embedded in the software environment of the information servers and ensure that the confidential files that are given for reading are signed. Further distribution of files after copying from information servers is considered unknown. Signed Files Search Service performs the search and verification of the signed files in the open access and it is represented by a separate software tool in the campaign environment or by a third-party service that provides the functions of scanning Internet resources.

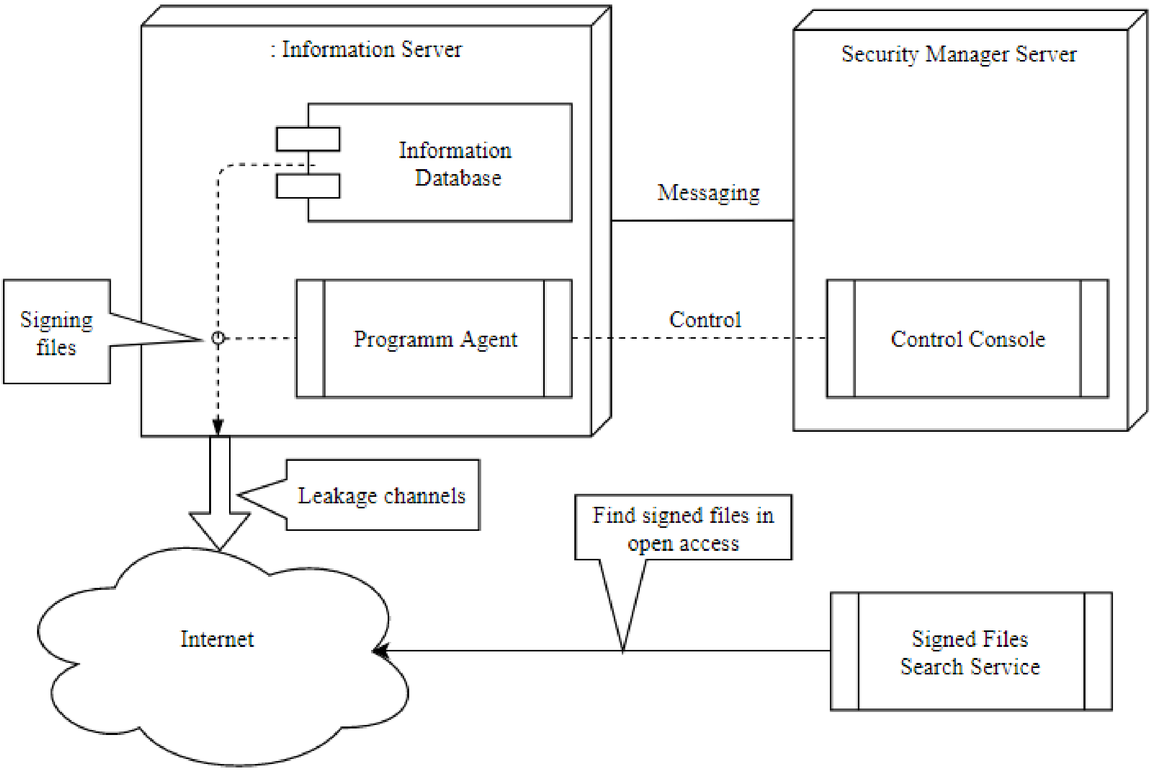

Fig. Structural diagram of the software

Conclusions. The threat of information security of confidential company files coming from insiders is considered in this paper. The description of the corporate network and the construction of information security systems are presented. DLP security systems and their use in risk management are presented. The tasks and algorithms for the introduction of steganographic prints for file protection are considered. The functional requirements for development are defined. The technology of construction of the system is grounded.

REFERENCES

1. Безопасность корпоративных сетей / Т.А. Биячуев ; под ред. Л.Г. Осовецкого. – СПб. : СПб ГУ ИТМО, 2004. – 161 с.
2. Защита от утечек конфиденциальной информации. DLP. – LETA IT-company, 2010.
3. Steganography and Digital Watermarking // Jonathan Cummins, Patrick Diskin, Samuel Lau and Robert Parlett. – 2004.
4. Embedded SW software company site [Electronic resource] // Mode of access: http://embeddedsw.net/OpenPuff_Steganography_Home.html.
5. Raymond company blog [Electronic resource] // Mode of access: https://www.raymond.cc/blog/signmyimage-protects-your-image-with-invisible-signature.
6. Phibit software company site [Electronic resource]. – Mode of access: http://www.phibit.com/icemark/.
7. OpenStego software developers site [Electronic resource]. – Mode of access: https://www.openstego.com/.
8. OutSecret software company site [Electronic resource]. – Mode of access: https://oursecret.soft112.com/.
9. SureSign software developers site [Electronic resource]. – Mode of access: http://www.suresign.com/.
10. Цифровая стеганография / В.Г. Грибунин [и др]. – СОЛОН-Пресс, 2002.
11. Шелухин, О.И. Стеганография. Алгоритмы и программная реализация / О.И. Шелухин, С.Д. Канаев. – Горячая линия-Телеком, научно-техническое издательство, 2017.

12. Абазина, Е.С. Цифровая стеганография: состояние и перспективы / Е.С. Абазина, А.А. Ерунов // Системы управления, связи и безопасности : научный рецензируемый сетевой электронный журнал. – 2016.
13. Положение по оформлению и защите диссертации на соискание степени магистра наук / Полоцкий государственный университет. – 2014.
14. Ярмолик, С.В. Стеганографические методы защиты информации / С.В. Ярмолик, Ю.Н. Листопад. – Белорусский государственный университет информатики и радиоэлектроники. – 2005.
15. Григорьян, А.К. Применение вейвлет-преобразования для внедрения ЦВЗ в видеопоток в режиме реального времени // А.К. Григорьян, М.Ю. Литвинов. – Санкт-Петербургский государственный университет аэрокосмического приборостроения, 2011.
16. Безопасность информационных технологий / под ред. В.И. Волчихина, С.Л. Зефирова // Труды научно-технической конференции, Пенза, 2003.
17. Information Hiding, Digital Watermarking and Steganography. An Introduction to Basic Concepts and Techniques. Nasir Memon. – Polytechnic University, Brooklyn, 2005.