SOCIETY FOR SCIENCE AND EDUCATION
UNITED KINGDOM

TNC TRANSACTIONS ON NETWORKS AND COMMUNICATIONS

VOLUME 8, NO. 1
ISSN: 2054 -7420

Exploring the Personal Data Protection Methods through Programs

Shafagat Mahmudova
Institute of Information Technology of ANAS, Baku, Azerbaijan
shafagat_57@mail.ru

ABSTRACT

The paper highlights the personal data and the stages of its protection. Some provisions of the Law of the Republic of Azerbaijan on the personal data are reviewed. The protection of personal data through programs is explored. The studies in this area are reviewed. Data protection methods through programs are studied and analyzed. Some recommendations for the further developments in this field are provided.

Keywords: personal data; protection; software; technical task; SDN.

1 Introduction

Personal data protection is one of the most pressing issues of our time. The development of information technology requires more attention in this area and necessitates the development of specific tools.

Personal data protection is a set of organizational and technical measures aimed at protecting the personal data of a physical person (subject of personal data) based on the specified information [1]. Personal data protection is included in the labor protection section of an institution. A state guarantees the protection of the workers' labor rights taking into account the use of their personal data (ID cards). The steps to protect the personal data is illustrated in Figure 1.

Figure 1. The steps to protect the personal data

Personal data processing is a set of automated tools or operations related to personal data processing; writing, systematizing, collecting, storing, specifying, using, transmitting, protecting, deleting and destroying the personal data, etc. [1].

DOI: 10.14738/tnc.81.7682
Publication Date: 04th March 2020
URL: http://dx.doi.org/10.14738/tnc.81.7682

The Law of the Republic of Azerbaijan on Personal Data (No. 998-IIIQ) was issued by the President of the Republic of Azerbaijan, May 11, 2010 [2].

This law regulates the issues related to the collection, processing and protection of personal data, the formation of a personal data unit of the national information space, as well as the transboundary transfer of personal data. It also specifies the rights and obligations of the state and local self-governing authorities, and the legal entities and individuals operating in this area.

The main goal of this law is the development of the legislative basis and general principles for the collection, processing and protection of personal data, as well as the formation of the rules and requirements of the state regulation in this area, and the determination of the rules for the formation of personal data in information resources. It also aims to specifying the rules for the provision and transfer of data, defining the basis for their responsibility and protecting the rights and freedoms of individuals and citizens, including the right to protect the privacy of personal and family life.

In this law, several notions as data, information technologies, information systems and resources, and corporate information systems are used in the context specified by the laws of the Republic of Azerbaijan regulating the relationships in the field of data collection, processing and protection.

As specified in the law, the protection of personal data at the state level is of great importance. Moreover, the protection of personal data through programs is also of great significance and relevance. Data protection through programs is a system of special programs that provide data protection and are included in the software. This article mainly focuses on this issue.

2 Personal Data Protection through Programs

Personal data protection through programs is a system of special programs that provide information protection and are included in the software. Protective software code can be supplemented separately or included in the software. This is because the protective functions of multifunctional programs do not have significant self-protective tools and are less protective than specialized software for their appointment. Any important computer system requires a valuable integration of personal data protection software [3].

Program tools used for data protection is illustrated in Figure 2.

Keylogger is a special type of malware that allows attackers to spy on users (sensitive information, bank details, credentials, etc.).

Although software and functions are identical in many aspects, they should not be confused with computer protection or unauthorized use of computers. Although the data is digital in the operating system, it is still protected. Full protection of data on a computer running a server requires the use of various types of security programs that combine several types of protection at the same time.

Information systems (IS) play a key role in personal data protection.

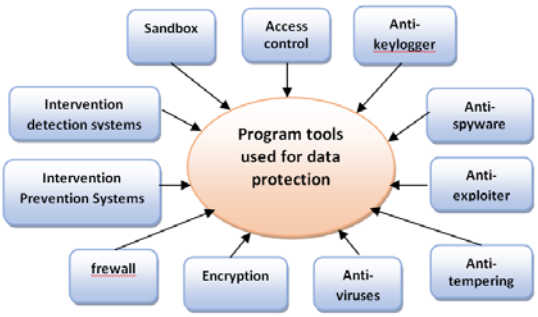

Figure 2. Program tools used for data protection

IS refers to data storage, retrieval and processing and the provision and dissemination of relevant organizational resources (people, techniques, etc., ISO / IEC 2382: 2015) [4].

The following options should be used to protect data in the information system through programs (Figure 3).

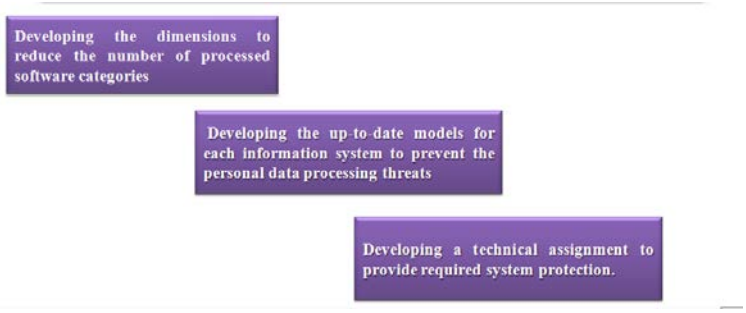

Figure 3. Options should be used to protect data in the information system through programs

- developing the dimensions to reduce the number of processed software categories;
- developing the up-to-date models for each information system to prevent the personal data processing threats;
- developing a technical assignment to provide required system protection.

Software protection is a series of measures aimed at preventing unauthorized arrangement, use, sharing, modification and study of analogues.

Protection against unauthorized use of software is a measure aimed at preventing unauthorized use of software. It can be used for the organizational, legal software and hardware protection.

Software copying protection is rarely applied which is related to the users' need for deploying and installing it on their computers. For software copying protection, its separate algorithms can be protected through a license.

The common law for the protection of personal data by the Ministers of Justice of the European countries shall be applied throughout the EU. Currently, in fact, 28 member states adopt a law that protects 28 different types of personal data. The law is aimed at developing a model for working with the citizens' personal data by the state. The initiator of this project is Viviane Reding, the Luxembourg Commissioner of the European Commission. According to the rules, personal data is processed by the companies in several EU countries, but monitoring should be implemented by only one regulatory body. This authority

is referred to the control body of the country where the general representative of the data processing company is located. Previously, the French government called for control at the national level, but other EU countries opposed this model. Thus, the Mini One-Stop Shop (MOSS) has a significant impact on the US companies such as Facebook or Google. Today, these companies process and store data in one country, while their offices operate in other countries and accumulate funds. In Europe, it is Ireland where the major company representatives are located. "Our goal is to create common rules for the EU, as well as to reduce administrative barriers for national regulators," Lithuanian Justice Minister Juozas Bernatonis says [5].

Concerns about the confidentiality and protection of personal data have led to reforms in the European Union (EU) legislation. The General Data Protection Regulation is aimed at strengthening the existing directive on the protection of EU citizens' personal data in regard to the establishment of personal data processing rules [6].

3 Analysis of Data Protection through Programs

The problems of Internet security, such as malware, computer viruses, phishing and theft of personal data, have become more acute in recent years and aggravated by inappropriate behavior of the Internet users. The experts in this field educate the people about the Internet. Moreover, the experts play an important role in shaping teenagers' security behaviors on the Internet and are able to assist them to comprehend the concept of the Internet security through interactive relationships in their daily life. As a result, the experts need to further explore the motives of adolescents' risky behavior on the Internet. Through the group analysis, the role of moderators and social norms are explored. Qualitative interviews are also conducted to verify the results of the statistical analysis. The results show that in order to prevent the adolescents' risky behavior on the Internet, it is necessary to improve the educators' skills to solve the Internet security problems or create an environment that encourages them to take protective measures. [7] discusses the theoretical concepts and practical implications for online security training.

Unauthorized access or theft of confidential personal data occurs very often. Illegal distribution of confidential data in media results in millions of recovery and losses. Target Inc. survey system report in 2013 estimated the damage of more than one billion dollars to 70 million customers. Stolen information is used to harm policymakers and negatively affects both foreign and domestic policies. [8] presents some methods for better protection of the state and security of networks. These techniques will help the professionals to identify network behavior, anomalies and hidden and systemic problems.

Unauthorized access to certain parts of personal data may give the impression of an intimidating task. To improve the network state, it is necessary to identify the network abnormalities that indicate malicious activity and other hidden system problems. [9] offers a network path analysis service that can be used to identify the hidden systems problems, create more secure network, and prevent data theft by cyber criminals.

Government agencies are required to cooperate with one another to provide high quality e-government services. This collaboration is generally based on a service-oriented approach and supported by interoperability platforms. Such platforms are the specialized secondary software-based infrastructures that provide appropriate software services. In turn, many governments have developed a law to protect personal information, given that the personal data processed by the governments are highly sensitive.

This document proposes solutions for monitoring and reinforcing the data protection laws as an element of the e-government interoperability platform [10].

The acquisition of linear programs and their interconnection is widely used in software research. [11] aims at facilitating the software analysis by creating a single data provider for the structure of the analyzed software. The proposed approach in this work is aimed at deciphering and presenting a program code in the form of interconnected linear units and their relationships. The code presented in this form can be analyzed to facilitate the process of developing secure software and to identify the patterns with specific features. The proposed method is based on the development of a plugin that combines the data from available tools. A method is developed for extracting the data from the dismantling device "MAR" and presenting it in a necessary form for further work. An example is given for method testing. The data obtained in accordance with the methodology is intended for use in target software tools.

[12] aims at discussing the security of IT systems and identifying the elements that should be protected against unauthorized access. Software is developed based on the characteristics of the cyber area. The complexity of software systems makes information security more complex and unreliable. The development of technology is inseparably linked to the development of threats, that is, improving software solutions has become extremely important for all uses. This study shows what security elements should be considered both as the software security user and when creating a security system.

Software-Defined Networking (SDN) enables collecting the network configurations from traditional networks. SDN also empowers the development of software protocols and tools that improve program visibility.

At present, SDN is evolving rapidly due to a new structure that separates the data broadcasting of control network devices. Many researchers have studied such a specific network. However, some constraints still limit the development of SDNs. On the one hand, in a normal model, a controller carries all the threats and causes damage to the network. On the other hand, there will be greater increase in SDN keys in data broadcasting where the storage of these keys is limited. [13] offers two relevant protocols to address these problems. In particular, one is an anonymous flight control protocol, and another is an external source protocol that validates the data on the aircraft. Assessment shows that the proposed protocol is accurate, safe and effective.

Acquisition, application and development of information systems are the basis for competitive advantage. Rapid advances in technology also originate the ethical problems related to the protection and confidentiality of end-user data. [14] discusses the standard quality assurance methods that guarantee high-quality software products while supporting the strategic needs of the organization. It presents a framework that links the improvement of the quality software development process to the strategic needs of an organization. The Balance Score Card methodology is used to define the standardized practices and the strategic goals of an organization, and to track the effectiveness of the development of information systems. In addition, for coordination, the "Control Objectives for Information and Related Technology" (COBIT) provided by the Audit Association comprises 5 information management systems [14].

The rapid development of IoT technology and the increased computing power of computer-based devices make it more probable to be open to security threats and attacks. Recently adopted Trusted Execution Environment (TEE) enables the random code to be executed in the environments completely isolated from certain parts of the system. TEE is a protected area of the main processor. However, the existing methods

for TEE memory protection are insufficient. Generally, the formal software methods are not practical, and the advanced approaches to the implementation are not theoretically verified. To address the isolation and memory problems at TEE, the Advanced RISC Machine (ARM) platform offers a practical way to protect the memory integrity against security threats. The ARM is used to create the isolated work environments that can protect sensitive code and data against attacks. Xilinx Zynq ZC702 evaluation board applies the ARM. The automatic inspection rate of machines is approximately 78.32%, and the proposed method is cost-effective and feasible both in terms of loading time and cost [15].

The use of the European General Data Protection Regulation (GDPR) has recently gained popularity in the management of personal data. [16, 17] present GDPR articles to attract the software vendors, and explain how they can be used through most advanced technologies, such as tracking the origin of computer scientists' requirements, usage control and dissemination of remote protocols.

4 Conclusions

The modern digital world, which is based on the network communication, globalization and information sharing, identifies new important tasks that represent the principles of reliable access to the data structures proposed in the field of privacy and protection of personal data. In this regard, reliable access to all sources of electronic environment is essential. Besides, certain technological and organizational measures should be applied to identify, authorize and protect the personal data. After successful registration, serious security procedures should be offered to protect the user profiles and all personal information collected during training [18, 19].

Consequently, the article explored the ways to protect the personal data through programs. Personal data protection programs provide more efficient and high-performance rates. The adoption of new laws in this field at the global and national levels proves the relevance of these issues once again. The Council of Europe should pay great attention to this area. The further creation and development of new programs in this area will allow for the protection of personal data more thoroughly. The studies in this area were recommended to be strengthened and new quality programs to be developed to protect personal data.

REFERENCES

[1] (1). Protection of personal information, 25 мая 2018, retrieved from https://ru.wikipedia.org/wiki/ Protection of personal information

[2] Law of the Republic of Azerbaijan on personal data, 11.05.2010, retrieved from http://www.e-qanun.az/framework/19675

[3] Software Information Protection, 2000-2019, retrieved from http://rus.safensoft.com/security.phtml?c=882

[4] Maglinets, YU.A. (2008) Analysis of requirements for automated information systems, Moscow: Бином.

[5] A new law on the protection of personal information, 08.10.2013, retrieved from http://www.lawreform.az/index.php?module=news&name=view&id=1098&lang=az

[6] Ferreira, G., Sousa, M., Silva, B.S., Antunes, L., Frade, S., Beale, T. and Correia, C. (2019) Open EHR and General Data Protection Regulation: Evaluation of Principles and Requirements, JMIR medical informatics, vol. 7, no. 1, retrieved from https://www.ncbi.nlm.nih.gov/pubmed/30907730

[7] Hui-Lien, C. and Jerry, S. (2017) The moderating roles of gender and social norms on the relationship between protection motivation and risky online behavior among in-service teachers, Computers & education, , vol. 112, pp. 83-96.

[8] Joshua, A., Scott, M., Edward, C. (2017) SDN Data Path Confidence Analysis, IEEE Conference on dependable and secure computing, pp. 209-216.

[9] Joshua, A., Scott, M. and Edward, C. (2017) A Framework for SDN Network Evaluation, 47th annual ieee/ifip international conference on dependable systems and networks workshops (DSN-W 2017), pp. 111-112.

[10] Andres, E., Dahiana, M. and Laura, G. (2015) Monitoring and Enforcing Data Protection Laws within an E-government Interoperability Platform, XLI Latin American computing conference (CLEI), pp. 548-559, 2015.

[11] Bazhenov, I.O. (2018) Lubkin Methodology of software code decomposition analysis, 2018 12th international IEEE Scientific and technical conference on dynamics of systems, mechanisms and machines (dynamics).

[12] Anna, K. and Lidia, O. (2018) Data Security in Cognitive Information Systems, Proceedings 2018 IEEE 32nd international conference on advanced information networking and applications (AINA), pp. 631-635.

[13] Pawel, K. (2017) Digital image integrity a survey of protection and verification techniques, Digital signal processing, vol. 71, pp. 1-26.

[14] Syeda Umema, H. and Abu Turab, A. (2017) Software Development for Information System Achieving Optimum Quality with Security, International journal of information system modeling and design, vol: 8, no. 4, pp. 1-20.

[15] Rui, C., Liehui, J., Wenzhi, C., Yang, X., Yuxia C. and Alelaiwi, A. (2017) MIPE: a practical memory integrity protection method in a trusted execution environment, Cluster computing-the journal of networks software tools and applications, , vol. 20, no. 2, pp. 1075-1087.

[16] Pascal, B., Erik, K., Paul Georg, W. and Juergen, B. (2017) Identity Management and Protection Motivated by the General Data Protection Regulation of the European Union-A Conceptual Framework Based on State-of-the-Art Software Technologies, Technologies, vol. 6, no. 4, pp. 1-14.

[17] Hui-Lien, C. and Jerry Chih-Yuan, S. (2017) The moderating roles of gender and social norms on the relationship between protection motivation and risky online behavior among in-service teachers, Computers & Education, vol. 112, pp. 83-96.

[18] Radi, R., and Irina, N. (2017) Architecture of Combined e-Learning Environment and Investigation of Secure Access and Privacy Protection, International journal of human capital and information technology professionals, vol. 7, no. 3, pp. 89-106.

[19] Peter, K. and Glenn, D. (2007) Practical uses of virtual machines for protection of sensitive user data, Information security practice and experience, proceedings, vol. 4464, 145 p.

