Algorithm for emergency deletion of files by voice command

Roman Komotsky [1], *Nikolay* Boldyrikhin[1*], and *Mikhail* Karpenko[1]

[1]Don State Technical University, 1, Gagarin Sq., 344002, Rostov-on-Don, Russia

Abstract. The Currently, there is a growing interest in various methods and means of protecting information, which is due to the growing number of crimes related to the violation of confidentiality of information, including through physical access to a computer. There are many ways to protect information from unauthorized access, such as physical security measures, password protection, and so on. However, a situation may arise when all defense lines have already been overcome and there is no other way to quickly block or destroy confidential information in any other way than with the help of a voice command. Thus, the topic of the article is relevant. The object of research is an information system containing confidential information. The subject of the research is the methods of emergency deletion of confidential information. The purpose of this article is to develop an algorithm for urgent deletion of files by voice command. In the course of the work, the algorithm for the emergency deletion of files by voice command was developed, which allows blocking the means of inputting information (keyboard and mouse) and deleting files located in a predetermined folder. The algorithm provides protection against accidental pronunciation of a voice command: before deleting files, a timer is first started, the time of which is pre-set by the user. During the duration of the timer, it is possible to cancel the deletion of files by entering a password, however, there is no way to access the information until the appropriate password is entered.
Keywords: emergency file deletion, blocking access to information input tools, deleting files by voice command

1 Introduction

Currently, in the modern world, the volume of processed and stored information is increasing every day, and therefore there is an urgent need to ensure the protection of information [1,2,3]. The list of threats to information security is constantly expanding [4,5,6]: these are threats related to the spread and impact of malicious software; threats related to the use of network protocols; threats related to leaks through technical channels. The damage from the implementation of these threats is constantly growing [7]. Methods and means of protecting information systems from cyber threats are also being developed [8,9,10,11].

An important place in the overall security system of the organization is occupied by physical protection against penetration [12,13]. To ensure the physical protection of information, each state or commercial organization has special security services that prevent

[*] Corresponding author: boldyrikhin@mail.ru

intruders from entering the protected object. However, these measures, as practice shows, do not always provide 100% protection of informatization objects [12,13]. Direct penetration of intruders beyond the perimeter of the organization using social engineering tools occurs quite often [13]. Access of intruders to the territory of the organization can also be carried out using raider technologies. In many countries, raider seizures are considered common practice [14]. Under these conditions, standard measures taken to physically protect the organization's facilities may simply be useless, since raiders often quite legitimately enter the organization's territory. Therefore, it is necessary to take additional measures to protect critical infrastructure facilities, and first it concerns informatization facilities.

Thus, the development of software tools for emergency removal of confidential information is relevant. These specialized data protection programs protect data from unauthorized access by locking the system, blocking input or output devices, and deleting files [15,16,17].

2 Materials and methods

The creation of algorithmic support for software is the initial stage of program design, which is based on the analysis of the properties of objects in the subject area and information needs.

Below are flowcharts of algorithms that provide the logic for the software implementation of the following functions: blocking the operating system, blocking information input tools, deleting files by voice command located in each folder (Fig. 1-3).

First, the software starts up, then this software constantly functions while the computer is running and starts every time you reboot.

Otherwise, before the timer expires, the keyboard and computer mouse lock is launched, which can be excited by entering the primary secret key. The corresponding key entry keys remain active.

If there is a danger of unauthorized access to information, the operator gives a voice command to delete the folder with confidential information. By voice command, a timer is started, which makes it possible to cancel the deletion. This possibility is provided in case the command was uttered by accident. If the timer has expired, the specified partitions and files are urgently deleted, then the keyboard and computer mouse are permanently blocked.

Since the voice command emergency deletion program requires the use of speech recognition algorithms, it is possible to use a ready-made tool or develop your own application. As ready-made tools, you can use the Vosk model or Google API. Vosk is an open-source standalone speech recognition tool. It allows you to use models for a variety of languages and dialects [18].

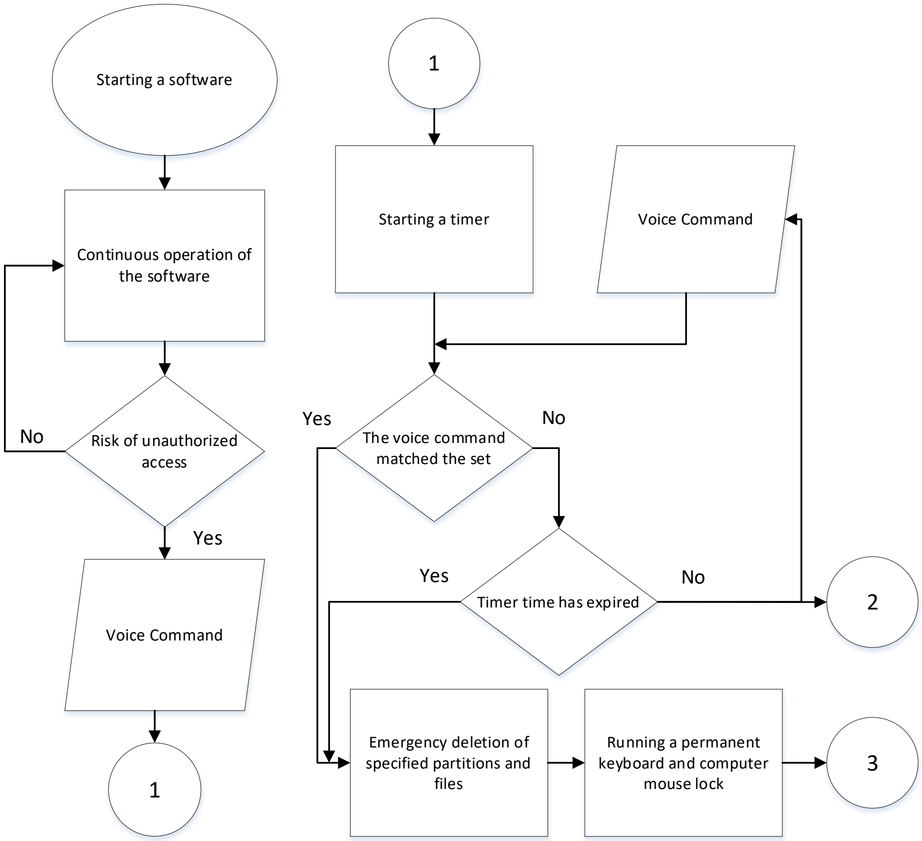
Starting a software
Continuous operation of the software
Risk of unauthorized access
No
Yes
Voice Command
1
1
Starting a timer
Voice Command
The voice command matched the set
Yes
No
Timer time has expired
Yes
No
2
Emergency deletion of specified partitions and files
Running a permanent keyboard and computer mouse lock
3

Fig. 1. Scheme of the algorithm for emergency file deletion.

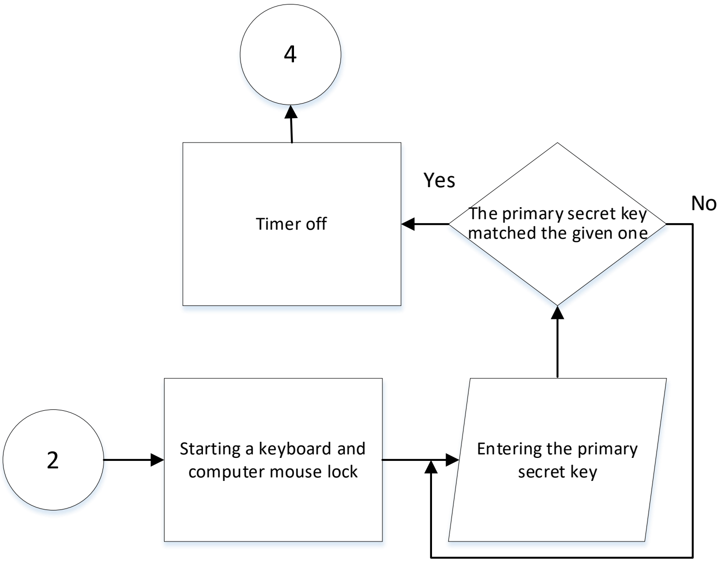
4
Timer off
Yes
The primary secret key matched the given one
No
2
Starting a keyboard and computer mouse lock
Entering the primary secret key

Fig. 2. Scheme of the algorithm for emergency file deletion (continued).

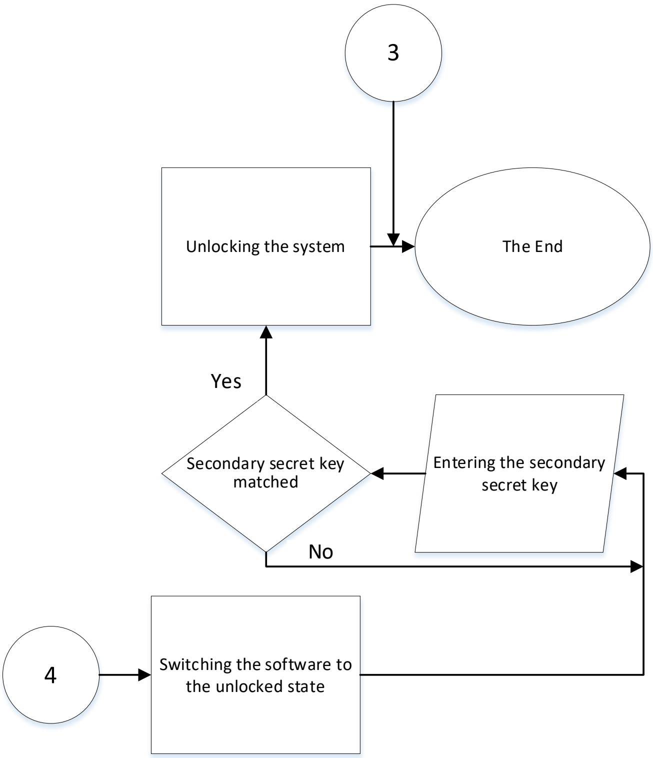
3
Unlocking the system
The End
Yes
Secondary secret key matched
Entering the secondary secret key
No
4
Switching the software to the unlocked state

Fig. 3. Scheme of the algorithm for emergency file deletion (continued).

Vosk models are divided into two groups: small and large.

The small model is a high–speed model, high-speed import of the necessary libraries and modules, has less weight and less efficiency of correct speech recognition than the large model.

The large model is a slow–acting model, low speed of importing the necessary libraries and modules, has more weight and greater efficiency of correct speech recognition than the small model.

When speech recognition using the Google API requires a permanent Internet connection [19]. In this case, using a microphone, speech is recorded on a local device, after that the recorded audio signal is transmitted over the Internet to the Google API, then the sent audio signal is processed by a specialized system and a speech recognition model, as a result of which the finished text. However, if there is no Internet connection or it is unstable, speech recognition will not occur, respectively, the command to delete the file urgently will not be recognized.

3 Results and Discussion

Thus, within the framework of this work, algorithmic support was developed for a software tool for emergency deletion of files by voice command. This algorithm provides speech recognition to determine the voice command, emergency deletion of sections and files by voice command, locking the keyboard and computer mouse with the ability to unlock, unlocking the system by entering secret keys.

4 Conclusion

The algorithm developed in the framework of this work can be implemented as a separate program that provides emergency deletion of confidential information by voice command. Also, these algorithms can be used as part of an integrated hardware and software system to protect information from unauthorized access.

This algorithmic support has prospects in the future, and in the future its functionality can be expanded with additional features.

References

1. A. Andersson, K. Hedström, F. Karlsson, Information & Management **59(3)**, 103623 (2022) DOI: https://doi.org/10.1016/j.im.2022.103623
2. A. Vedadi, M. Warkentin, A. Dennis, Information & Management **58(8)**, 103526 (2021) DOI: https://doi.org/10.1016/j.im.2021.103526
3. J. Kim, H. Kwon, Computers & Security **120**, 102789 (2022) DOI: https://doi.org/10.1016/j.cose.2022.102789
4. M. Hemmatfar, M. Salehi, M. Bayat, International Journal of Business and Management **5(7)**, 158-169 (2010) DOI: https://doi.org/10.5539/ijbm.v5n7p158
5. H. Elkhannoubi, M. Belaissaoui, Fundamental pillars for an effective cybersecurity strategy in Computer Systems and Applications (AICCSA) (2015) DOI: https://doi.org/10.1109/AICCSA.2015.7507241
6. S. Kramer, J.C. Bradfield, J Comput Virol **6**, 105– 114 (2018) DOI: https://doi.org/10.1007/s11416-009-0137-1
7. *McAfee. Net losses: Estimating the Global Cost of Cybercrime* (2014) URL: https://www.csis.org/analysis/net-losses-estimating-global-cost-cybercrime
8. H. Hu, W. Han, S. Kyung, J. Wang, et all., Computers & Security **87**, 101597 (2019) DOI: https://doi.org/10.1016/j.cose.2019.101597
9. I. Smirnov, O. Safaryan, P. Razumov, V. Porksheyan et al, 3rd International Conference on Computer Applications and Information **9096741** (2020) https://doi.org/10.1109/ICCAIS48893.2020.9096741
10. A. Khraisat, I. Gondal, P. Vamplew, J. Kamruzzaman, Cybersecurity **2(1)**, 1-21 (2019) DOI: https://doi.org/10.1186/s42400-019-0038-7
11. L. Cherckesova, P. Chub, 3rd International Conference on Computer Applications and Information Security **9096729** (2020) https://doi.org/10.1109/ICCAIS48893.2020.9096729
12. *Physical Penetration Testing Methods (That Actually Work), available at: https://purplesec.us/physical-penetration-testing/, Date Views 29.12.2022*
13. T. Dimkov, W. Pieters, Physical Penetration Testing: A Whole New Story in Penetration Testing (2011) https://www.researchgate.net/publication/254860594_Physical_Penetration_Testing_A_Whole_New_Story_in_Penetration_Testing
14. *Corporate Raider: Definition, Tactics, Example,* URL: https://www.investopedia.com/terms/c/corporate-raider.asp
15. *CCleaner Professional,* URL: www.ccleaner.com/ru-ru/ccleaner
16. Free File Shredder, URL: www.fileshredder.org
17. *High-level file operations, available at: https://www.docs.python.org/3/library/shutil.html*

18. *Vosk real-time voice recognition, available at: https://www.programmer-sought.com/article/696510547189/*
19. *Speech-to-Text request construction, available at: https://cloud.google.com/speech-to-text/docs/speech-to-text-requests*