https://doi.org/10.31891/csit-2022-2-11
UDC 004.3

Yelyzaveta HNATCHUK, Vitalii BASHUK, Denys KVASNITSKYI
Khmelnytskyi National University

RESEARCH OF METHODS AND MEANS OF ENSURING THE RELIABILITY OF A SPECIALIZED COMPUTER VOICE VEHICLE CONTROL SYSTEM

The methods and means of protection of reliability in modern specialized computer systems of voice control of the car are investigated in the work. The evaluation of the characteristics and properties of the system is carried out. The basic principles of work and various possibilities of constructions of voice control of the car are considered. The methods and means of detecting dangers are shown, and the shortcomings and vulnerabilities of the car systems "Android Auto" and "Apple CarPlay" regarding the impact of malicious software based on modern methods of cyberattacks are identified. Preparation for cyber attack by ultrasonic and light commands on car voice control systems is shown. Methods and means for increasing the degree of protection of the voice authentication system of specialized computer systems "Android Auto" and "Apple CarPlay" are proposed.

To solve this problem, a hardware and software product of an additional biometric automotive user authentication system was created and developed. The system was created to ensure the reliability of cyber attacks on the voice control system.

Experimental studies confirm the effectiveness of the biometric authentication system as a proposed solution to provide an additional method of protection.

Keywords: voice control systems, method, protection, ultrasonic attacks

Єлизавета ГНАТЧУК, Віталій БАШУК, Денис КВАСНІЦЬКИЙ
Хмельницький національний університет

ДОСЛІДЖЕННЯ МЕТОДІВ ТА ЗАСОБІВ ЗАБЕЗПЕЧЕННЯ НАДІЙНОСТІ СПЕЦІАЛІЗОВАНОЇ КОМПЮТЕРНОЇ СИСТЕМИ ГОЛОСОВОГО КЕРУВАННЯ АВТОМОБІЛЕМ

В роботі досліджено методи та засоби захисту забезпечення надійності в сучасних спеціалізованих комп'ютерних системах голосового керування автомобілем. Проведена оцінка характеристик та властивостей системи. Розглянуто основні принципи роботи та різні можливості конструкцій голосового керування автомобілем. Показано методи і засоби виявлення небезпек, і визначено недоліки та вразливості автомобільних систем «Android Auto» та «Apple CarPlay» щодо впливу зловмисного програмного забезпечення на основі сучасних способів кібератак. Показано підготовку для здійснення кібератаки ультразвуковими та світловими командами на системи голосового керування автомобілем. Запропоновано методи та засоби для підвищення ступеня захисту системи голосової аутинтефікації спеціалізованих комп'ютерних систем «Android Auto» та «Apple CarPlay».

Для вирішення даної проблеми було створено та розроблено апаратно-програмний продукт додаткової біометричної автомобільної системи аутентифікації користувача. Система була створена для забезпечення надійності від кібератак на систему голосового керування.

Проведені експериментальні дослідження підтверджують ефективність системи біометричної аутентифікації як запропонованого рішення щодо забезпечення додаткового методу захисту.

Ключові слова: системи голосового керування, метод, захист, ультразвукові атаки

Introduction

Today, voice-controlled systems are widely used in various industries, including automotive engineering. They are increasingly used by people of all ages, because they are quite easy to operate, and most importantly effective. This is due to the fact that such systems help the user to solve various types of problems due to the wide range of functionality. Despite such widespread popularity among users, there are a number of problems when using such systems. Modern algorithms for recognizing voice commands are not yet perfect and do not always clearly understand a given user command, so there is a problem that such systems can be subjected to different types of cyberattacks. But, thanks to the development of neural network and cloud computing technologies, and the use of modern hardware and software and methods to ensure reliability, this problem can be minimized.

Therefore, the study of methods and means to ensure the reliability of a specialized computer system for voice control of the car is an urgent task.

Subject area analysis and relevant decisions

Problems solved in computer information systems have a number of characteristic features that affect the technology of automated data processing.

The computer system has the ability to integrate with other engineering technologies, expand capabilities and create a unified management environment, using the diversity and unification of computer equipment [1].

Dedicated computer voice control system helps you with voice commands to control functions such as navigating the route in the navigator, using climate control and its functionality, controlling the multimedia system, it also has the ability to interact with the user. With the help of voice assistants, the system can respond to voice commands and display various information on the screen of the driver's multimedia device.

In modern cars, voice control is performed by uttering the appropriate commands, which by undergoing certain transformations are converted into control signals for the respective systems. Today, you can use voice control to control the following systems in the car (Table 1).

Table 1

Voice control systems

System type	Execution of functions
Climate control	With the help of the climate control system, the user can change the temperature, turn on the seat heating, change the fan speed and more.
Multimedia	Provides the ability to receive, transmit, video and audio information.
Navigation	Perform voice control of the car navigation system
On-board computer	Determining the parameters of the car

In the voice control system, one of the main functions is voice recognition, which allows you to control the mobile phone connected to it, use the various features of the multimedia system, use the radio, navigation system and much more.

Entering voice commands greatly reduces your time and control, which in turn helps you focus on the road and driving. It is also possible to use voice commands to interact with navigation systems, ie paving or changing routes, etc. Voice control systems support a variety of languages, including the unpopular ones.

The process of voice recognition in specialized computer voice control systems (Figure 1) takes place in several stages. At each stage, a number of different methods are used to process the material signal. The process of voice recognition can be divided into three stages:

- receiving a voice signal and processing commands;
- recognition of phonemes and words;
- understanding of the voice command.

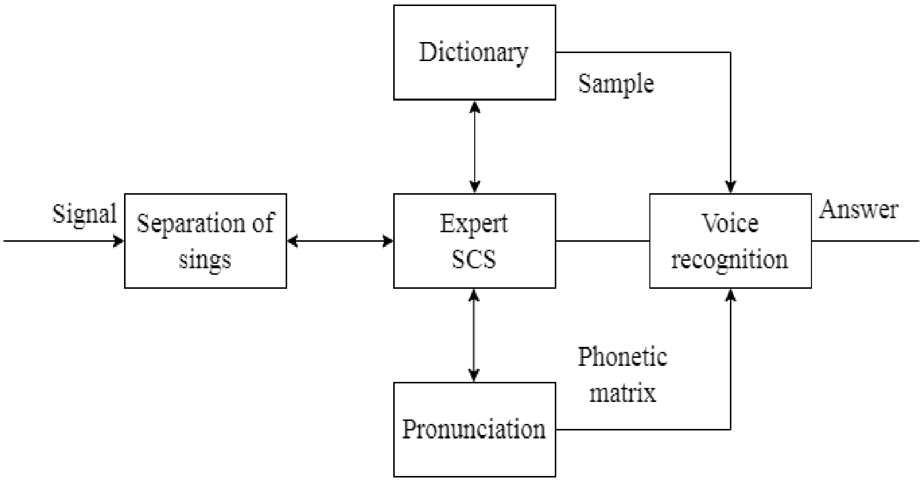

Fig 1. Scheme of the voice recognition process

The process of automatic determination of "who speaks" is performed on the basis of individual information input to the voice signal [2]. When driving a vehicle, human voice and gesture commands are entered as input data of the vehicle [3].

Today, the most popular car voice control systems are Android Auto [4] and Apple CarPlay [5]. To use the car's voice control functions, these systems use voice assistants.

After analyzing the operation of the car system "Android Auto", we can conclude that one of the problems is the voice control system - it's voice authentication. Due to this problem, criminals can perform cyber attacks, so-called inaudible or ultrasonic commands (DolphinAttak), on voice control systems.

To ensure the reliability of this system, you can use the method of "Hidden Markov model" [6]. There are two ways to send a voice signal to your device. They use the phonetic and whole word approach. The method is to identify the speaker and authorize it next to the voice database. First, the system learns with the help of certain voices, then it is tested with an unknown voice and then the system recognizes the user who owns the unknown voice. The recognition system is divided into two subsystems, such as text-dependent and text-independent.

Also, the car system "Android Auto" with voice control is vulnerable to other types of cyberattacks, such as attack by light commands performed by, giving a light command to the microphone of the voice control system with a special device for example, tinting car windows and more.

Analyzing the work of the car system "Apple CarPlay", we can conclude that the problem of voice assistant is often cloud data processing and dependence on the quality of Internet connection. So you need a quality and fast internet connection to ensure the reliability of your voice control system. To do this, you can buy a 3G / 4G WI-FI raster in the car, which will ensure the speed of your system with cloud data processing. The router can be connected to the car's cigarette lighter, to the USB port of your car, depending on your choice and characteristics of the car. But we should not forget that it is impossible to connect and configure devices from other manufacturers often enough, or they will work with limited functionality [7].

High-quality and stable Internet connection will also help to solve another shortcoming of the use of voice control, namely the malfunction, various system failures due to untimely software updates. To resolve this issue, you need to update your device to the latest available software version.

Another very serious problem that is often encountered with the voice assistant in the system "Apple CarPlay" is that it can read voice commands that were not assigned to it, ie respond to different types of noise, also due to noise voice control system may misunderstand and perform your voice team. To solve this problem, you can use the development of a system from Bose.

The company has developed a "QuietComfort Road Noise Control" system that can be installed in your car to reduce noise levels, which will ensure reliable voice control. The system consists of microphones and a set of accelerators, using acoustics installed in the car, filtering background noise, the system increases the clarity of voice commands and expands the possibilities of voice control.

You can also use the method of speech enhancement integrates the display of characteristics, time domain in a unified structure using the GAN network, it processes voice command waves and separates speech and noise signals coming into two one-dimensional layers of Fourier transform convolution, which reflect signal shapes in speech and noise spectrograms, which in turn are used to calculate losses. This method is superior to methods for improving voice commands, based on the DNN neural network.

One of the significant shortcomings of automotive systems is the voice authentication mechanism, for example, a criminal can bypass the security function of the voice assistant by pretending to be the owner by attacking light commands, thereby gaining unauthorized access to the vehicle. The study clearly demonstrated [8] how you can secretly and remotely enter voice commands with your own voice, in various ways without even attracting the attention of users.

To ensure reliability, you can use the method of dynamic time scale transformation (DTW) [9]. This method allows you to find the proximity, for two measurement sequences, in a certain period of time. It can be used to recognize a voice command if two speech signals represent the same output voice command, even at different speeds and lengths. One of the advantages of this method is ease of implementation.

Apple CarPlay, like Android Auto, is also vulnerable to cyberattacks, such as light commands. Next, the example of the threat model will show how such an attack occurs. The purpose of the thief is to remotely enter commands that pose a threat to the user's device, using a special device (laser). For example, an offender does not have physical access to a user's device, so he cannot change settings that are not available by voice, but he can gain remote access to the target device and its microphone by entering light commands. It should also be noted that remote access to the target device allows you to monitor the LEDs of the device, which in turn shows him how they react (light up) after recognizing the voice command and allows remote use as feedback. to determine the success of the attack attempt. To protect the reliability of the voice control device in the car as protection, you can use both hardware and software protection.

Methods of ensuring the reliability and protection against modern methods of cyber attacks on the voice control system

Today, Apple's Siri or Google Assistant voice assistants, used for voice control on Apple CarPlay [4] and Andoid Auto [5], respectively, are becoming popular. the method of human interaction with the car through voice control. With the advent of these systems, there has also been a need to provide protection for them. As previously described, these systems have a common vulnerability to the voice authentication system.

Next, we will discuss the methods of protection and reliability against cyber attacks by ultrasonic and light commands on a specialized computer system of voice control of the car. It should be understood that the voice control system, which depends directly on the speaker, is performed locally, and not the dependent voice control system is performed through the cloud service [10].

When a user uses a cloud service, signals that have been pre-processed are sent to servers where these signals will be recognized by machine algorithms. If the SCS recognizes the command, it will run the program to perform the operation. All commands and actions are system dependent and defined. Dedicated computer voice control systems have a wide range of functions and voice commands that are quite difficult to activate. Most security research for voice control systems focuses on cyberattacks, voice recognition algorithms [11], or malicious software.

In order to have access to control of the voice control system, Dolphin Attack must generate activation commands before the general introduction of voice control commands. Next, on the example of the voice assistant "Siri" who works in "Apple CarPlay" [4], how exactly is the generation of voice commands. Siri Voice Assistant works in two modes, namely activation and recognition. Before executing voice commands, you need to activate it, so you need to generate two types of voice commands, for activation and basic control commands. Activation is considered successful if the voice command meets the requirements: has wake-up words "Hello, Siri" and mimics the user's voice under which the voice assistant was trained. For a thief, creating an activation team is quite difficult, unless of course he is able to record the words of the user's activation.

Generating a certain voice in "Hello, Siri" using the current speech methods and functions extracted from the recordings [12] is extremely difficult, and sometimes not possible at all, because it is unclear what set of functions is required for voice identification. Therefore, you can use two methods to create activation commands for the voice assistant.

DolphinAttax can use different voice command activation kits, with different voice tones, using speech synthesis systems. The method is used when the offender has the ability to write words or phrases of the user, with the possibility of further breaking them into phonemes and combining them into different words, including those necessary for activation.

After undergoing activation, the offender may have access to general voice control commands. it is possible to select the text of the control command and create it using language synthesis systems. The voice recognition system does not verify the identity of the control commands.

To ensure the reliability of voice control of the car, from ultrasonic (inaudible) cyber attack, I want to offer my own method of protection, which will use hardware protection and contain a device for future use.

The specialized computer voice control systems "Android Auto" [5] and "Apple Car Play" [4] have shortcomings with voice authentication. That is, the criminal for a successful cyber attack (DolphinAttack) must first remotely send an inaudible (ultrasonic) signal to wake up the system.

Such a signal, the offender can receive by recording the voice of the user on whose device the cyberattack will be directed, to further break the signal into words that are necessary for activation. The proposed method will help increase the protection of the system in the first stage of preparation for a successful cyber attack.

The essence of the method is to reduce the possibility of the offender to obtain a recording of the user's voice. To do this, use an ultrasonic microphone recording blocker. To date, there are many different types, with different characteristics and capabilities. Next (Figure 2), will show the use of an ultrasonic blocker using the algorithm of this device.

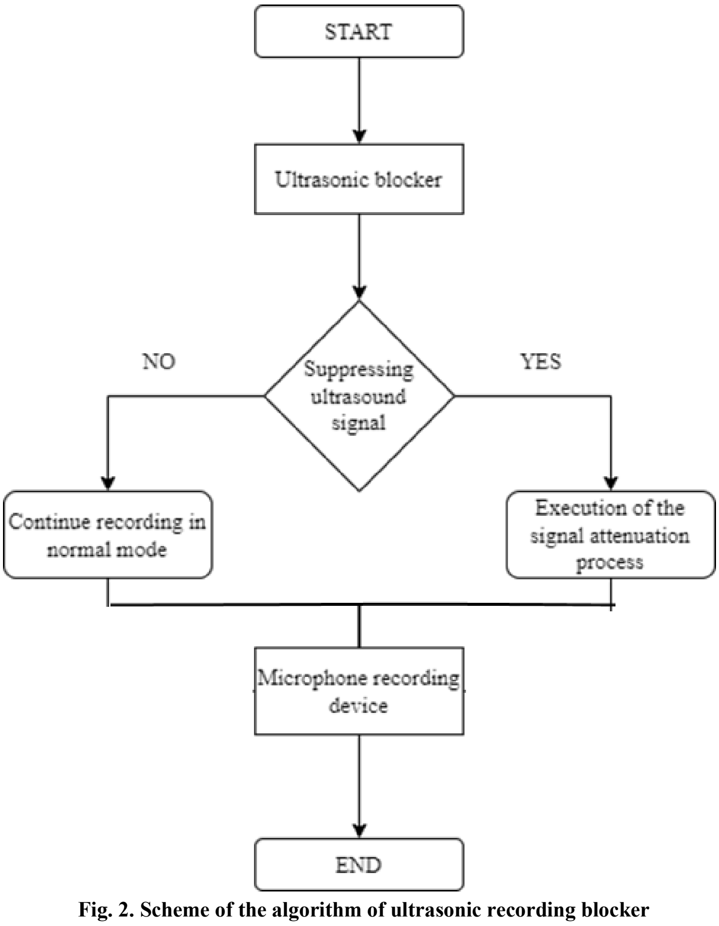
START
Ultrasonic blocker
NO
Suppressing ultrasound signal
YES
Continue recording in normal mode
Execution of the signal attenuation process
Microphone recording device
END

Fig. 2. Scheme of the algorithm of ultrasonic recording blocker

The size of the device is quite small and comfortable, and most importantly invisible, which makes it easy to install in the car showroom or anywhere else.

The next step will be to assess the effectiveness of Dolphin Attack's impact on various factors and methods of protection for them. For a cyberattack, the speed of recognition of different types of voice commands will not differ. Voice assistants such as Siri or Google Assistant are recommended for use in car voice control systems with minimal background noise, as SGCs are sensitive and can lead to incorrect analysis and execution of user-defined voice commands.

As the cyberattack is performed remotely, the level of background noise increases as the distance increases, as previously described, which can lead to incorrect recognition of the voice command. Next, the methods and means of protection in cyber attacks on the voice control system will be evaluated. Both hardware and software methods can be used for protection.

Hardware protection is to improve the SGC microphone and its characteristics. The main reason for a successful cyber attack is that the microphone can receive acoustic commands above 20 kHz, although ideally it should not.

In general, most microphones allow signals above 20 kHz [13], so the microphone should be extended and designed to curb acoustic signals in which the frequency is in the range of ultrasonic commands.

You can add a low-pass filter module to the microphone to detect modulated voice commands and cancel the bandwidth using modulated voice commands. This allows you to detect signals in the frequency range of the ultrasound, showing the modulation characteristics and where to modulate these signals to obtain the main frequency band.

To provide software, you need to use the unique properties of voice commands that distinguish them from the real thing. Figure 3 shows a demodulated cyberattack signal that differs from the original signal and that recorded at high frequencies in the range of 800-2400 Hz.

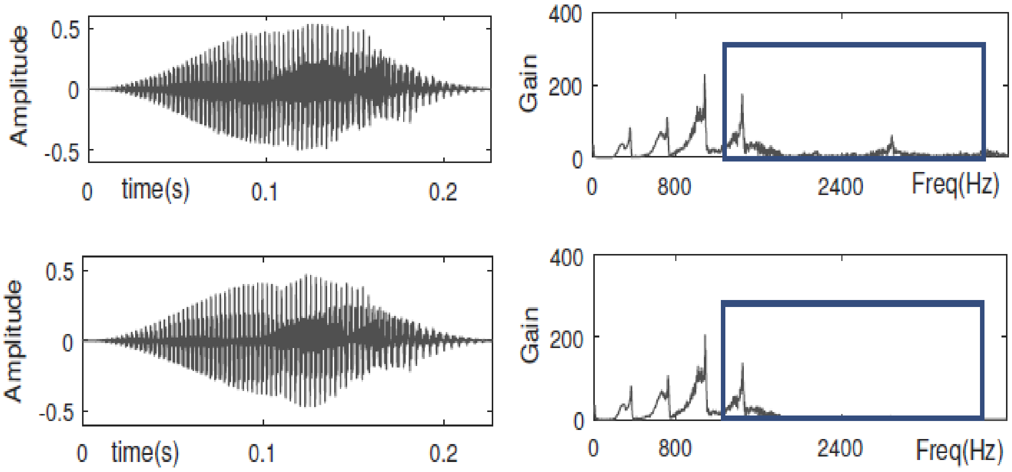

Fig. 3. Difference of demodulated signal from original [14]

The original signal produced by the Google TTS engine has a frequency of 25 kHz for modulation, so it is possible to detect "Dolphin Attack" by performing a frequency analysis in the range from 800 to 2400 Hz. To confirm the feasibility of detecting a cyber attack, the method of reference vectors as a classifier and extraction from audio functions in the frequency and time domain.

Using the created voice commands "Hello, Siri", with the help of special programs for converting text into a voice command, two samples of voice commands were obtained, in which one was recorded and the other was played. In order to teach the classifier on the method of reference values, to detect malicious voice commands, it is necessary to use several recorded audio samples, other samples can be used for testing. The classifier can distinguish restored audio recordings from those recorded with a true positive result and a negative value of one hundred percent.

The result of using a classifier made by the method of reference vectors, shows that this software method of protection can be detected for malicious cyberattacks.

The next method of protection against inaudible cyberattacks will be to search for and detect signs of non-linearity of the signal that is transmitted to the microphone of the voice control system. To do this, you need to understand whether it is possible to identify traces of non-linearity, which the offender will not be able to get rid of. But first you need to understand exactly how acoustic nonlinearity works.

In general, microphones and speakers are designed as linear systems, which means that the output signals are linear combinations of input signals. In the power amplifier used in microphones and speakers, the input audio signal is s (t), then the output signal should ideally be:

$$S_{out}(t) = A_1 s(t)\,, \tag{1}$$

where A_1 is the gain of the amplifier;

In practice, components in microphones can usually be linear only in audible frequency ranges, ie greater than 20 kHz. In ultrasonic bands where the frequency is less than 25 kHz, they do not show linearity [15]. It follows that for ultrasonic signals the output of the amplifier is calculated:

$$s_{out}(t) = \sum_{i=1}^{\infty} A_i s^i(t) = A_1 s(t) + A_2 S^2(t) + A_3 S^3 \cdots \approx A_1 s(t) + A_2 S^2(t) \tag{2}$$

[16] shows how it is possible to reproduce ultrasonic signals that can be recorded by a microphone, but they will be inaudible to humans. In the ultrasonic speaker there is a possibility of reproduction of two inaudible tones:

$s_1(t) = \cos\,(2\pi f_1 t)$ with frequency $f_1 = 38$ kHz i $s_2(t) = \cos\,(2\pi f_2 t)$ with $f_1 = 40$ kHz.

When the combined signal passes through a nonlinear microphone at the output it becomes:

$$\begin{aligned} s_{out}(t) = {} & A_1 s_{hi}(t) + A_2 s_{hi}^2(t) = A_1\big(s_1(t) + s_2(t)\big) + A_2(s_1(t) + s_2(t))^2 \\ & = A_1 \cos(2\pi f_1 t) + A_1 \cos(2\pi f_2 t) + A_2 \cos^2(2\pi f_1 t) + A_2 \cos^2(2\pi f_2 t) \\ & + 2A_2 \cos(2\pi f_1 t) \cos\,(2\pi f_2 t), \end{aligned} \tag{3}$$

This signal has frequency componentsv f_1, f_2, $2f_1$, $2f_{2,}$ $f_2 + f_1$ and $f_2 - f_1$. The microphone before, digital processing and recording uses a low-pass filter to remove components higher than 24 kHz. So frequencies

$$s_{low}(t) = A_2 + A_2 \cos\,(2\pi(f_2 - f_2)t), \tag{4}$$

In general,, $f_2 - f_1 = 2$ kHz з recorded by the microphone, this shows a property that allows you to send an inaudible signal, with the ability to generate a copy of the sound in the middle of the microphone.

Thus we mark the signal of the voice command: "Siri, pave the route…", which was pronounced by the user - $v(t)$, when he will say this command, the expression will be executed:

$$s_h = v(t) + n(t), \tag{5}$$

where $n(t)$- microphone noise;

Let the offender reproduce this voice command using ultrasound, recorded signal s_{atk} look like:

$$s_{atk} = \frac{A_2}{2}(1 + 2v(t) + v^2(t)) + n(t)\,, \tag{6}$$

Figure 4 shows the spectrum of the voice command for the s_h and s_{atk}, as these signals are almost similar in structure, which means that the text converter outputs the same text for the s_h and s_{atk}.

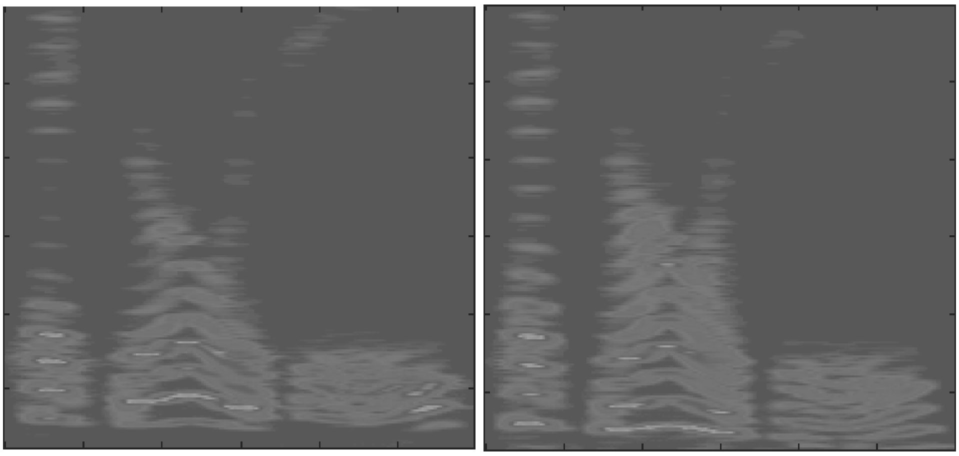

Fig. 4. Spectrogram for signal s_h and s_{atk}k, voice command "Siri, pave route…"

Based on this, we can conclude that for protection you need to check any signal (input) and determine whether it is a low-frequency user-specified, or a copy of the high-frequency cyber attack.

Attack by light commands is similar to cyberattacks by ultrasonic commands, the difference is that it uses a special device (laser) to attack. Hardware and software protection methods are used to protect against this type of attack. The software method of protection is to apply an additional level of authentication to the voice control system. In [17], the authors use an additional step of user authentication, thus trying to protect against the execution of unauthorized conference commands. The method is to use an additional authentication step before executing critical commands and reduce attempts to enter the wrong password if the system supports this feature.

This method can also help if the offender is unable to hear the response of the voice control system because it is far from the attacked device. For example, the system will ask any random question before executing a voice command, to which the offender will not be able to answer, thus stopping the attack.

The next method of protection is to use the operation of sensor algorithms, and use methods of merging them to detect commands entered on the basis of light [18]. Voice assistants often have and use multiple microphones. The essence of the method is that the offender uses one special device (laser) to attack light commands and uses only one microphone that receives the signal, while other microphones do not receive anything. So you can try to detect the attack using comparisons of signals from multiple microphones, ignoring voice commands that are entered using a special device (laser). This method can be effective only when one attacking device is running.

The imperfections of specialized computer systems with voice control of the car, namely with the problems of authentication or lack thereof in general, allow criminals to access various functions and capabilities of the car. Using various types of cyberattacks, such as attacks by light commands, or the introduction of inaudible (ultrasonic) commands, with the help of special devices aimed at microphones of voice control of the car, will allow criminals to bypass the imperfections of the driver authentication system.

The previously described protection methods allow to ensure the reliability of the car's voice control systems, quite effectively, but not as much as possible. As a result of the review of the original sources of the authentication system of different cars, the material obtained, the analysis of which led to the conclusion that to ensure the reliability of the car voice control system, you need to use an additional authentication system that will allow only the driver or proxies. system management and more. To solve the problem of additional authentication, an autonomous security system will be created, with the possibility of direct authentication using the fingerprints of the car owner or proxies. The main components of the system will be the Arduino UNO board, fingerprint scanner, LCD display, servomotor. The Arduino IDE will be used to download code and program the Arduino UNO board. The algorithm of the system (Figure 5) shows that if the user is not authenticated correctly, the system will not be able to provide access to the car's functions.

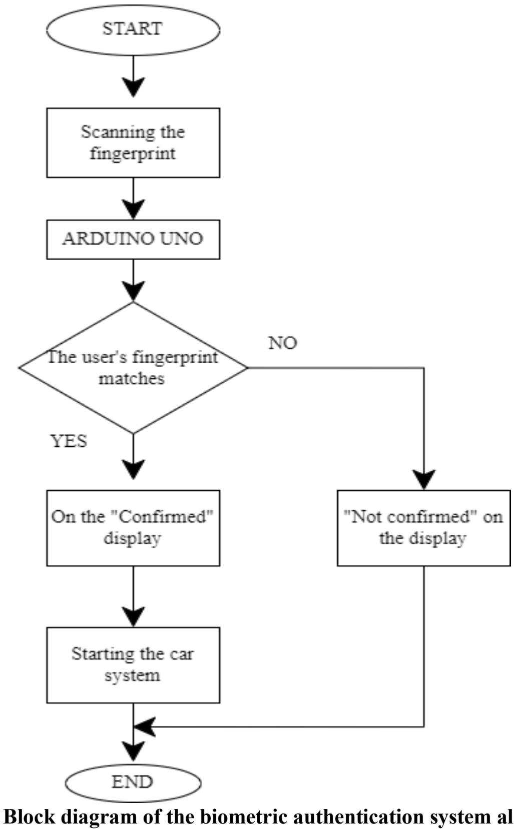
START
Scanning the fingerprint
ARDUINO UNO
The user's fingerprint matches
NO
YES
On the "Confirmed" display
"Not confirmed" on the display
Starting the car system
END

Fig. 5. Block diagram of the biometric authentication system algorithm

Biometric fingerprint recognition technology is a new and modern method for ensuring reliability and protection for security systems. This method uses the physical presence of the user to authenticate the user. Today, fingerprint recognition is widely used in various biometric systems, such as telephones, smart devices, biometric locks, bank payments and more [19]. The use of biometric authentication as a personal code as a personal code is considered a traditional method.

The use of this biometric authentication system will be quite reliable and will allow the user to provide reliability for specialized computer systems of the car, and block the criminal's access to the voice control system, which in turn will prevent various methods of cyberattacks

Known approaches to solving this problem are based on the work [20], which states that biometric security technologies are one of the most effective protection systems, and are increasingly becoming everyday attributes in the lives of ordinary people. In recent years, these systems have become widespread in the production of mobile technology, ie smartphones are built-in fingerprint scanners, voice recognition and more.

Particular attention is paid to the problem of authentication, related to the development of methods and tools to ensure the reliability of the car's SCS. That is, through the process of authentication of a person, using the comparison of its characteristics with the characteristics that were previously entered into the system, it is possible to determine as accurately as possible whether the user has appropriate access to the requested information or not. This makes it possible to ensure the reliability of the current problem of information security.

An important point for research in automotive authentication systems is the fact that in today's world there is a high demand for reliable and safest systems in vehicles. Thus, the design and development of hardware and software biometric security system using fingerprint technology to prevent unauthorized access to the car is simple and useful to use. The hardware and software implementation of the system will use an additional method of user authentication, which will be based on the ability to start the car's ignition system, which in turn will use its functionality and prevent its use in case of incorrect biometric authentication with fingerprint.

Fingerprint sensor, allows you to match the image of the user's fingerprint with what is stored in the system memory of the sensor. The research program focuses on a tool to obtain answers and follow instructions according to the results obtained, using the Android Uno microcontroller and includes the following security issues. Who use the analysis of the obtained results and check whose fingerprints can get access rights to turn on a specialized computer system of the car.

Experimental results and analysis of an additional user authentication system

Checking access to the car's biometric authentication system can be considered successful if the user turns on the car's system using their own fingerprint, which is registered in the device's memory. If the user registered in the system is unable to do so, the system may be considered defective.

The experiment is performed by detecting fingerprints for the system, aimed at finding the value of the success rate of other fingerprints that have not been entered into the scanner database. The experiment is performed by setting the fingerprint of the user, and then continuing to establish the fingerprint of the second user. To determine the percentages, changes in the ten right fingerprints of users that were used using another person's scan pattern that was not registered in the fingerprint sensor scanner will be checked.

An important point for the study is the position that the scanner is very sensitive to the placement of the user's fingerprints. The location of the fingerprint should be exactly on the layer of the scanner glass so that the fingerprint is read clearly and in accordance with the input and stored in the system. The results of the study of the fingerprint module are shown in table 2.

Table 2 shows the matrix of test results. The matrix displays the actual and incorrect number of predictions in the matrix test data. The input data of the matrix have the following values:

- positive (true) - is the number of fingerprints of users using a scanner;
- negative (true) for the number of prints of other users that are detected incorrectly;
- false-positive fingerprint results of another user being entered, verified and correct;
- false-negative when the fingerprint scanner module indicates that the car startup system could not be accessed.

Table 2

Study of the fingerprint scan of the user of the car's biometric system

Fingerprint	Positive (real)	Negative (real)	False-positive	False-negative	Car system
1	1	0	0	0	included
2	1	0	0	0	included
3	1	0	0	1	excluded
4	1	0	0	0	included
5	1	0	0	0	included
6	1	0	0	0	included
7	1	0	0	1	excluded
8	1	0	0	0	included
9	1	0	0	0	included
10	1	0	0	0	included

Based on the above results, it can be concluded that the success rate of the fingerprint of the user who can access the car is 90 percent.

Similar works

There are many articles on this topic, for example, a scientific article [21] presented the results of user interaction with a specialized computer system "Android Auto". The study examined the interaction of drivers with the functions of the voice control system and the safety of their control on the road. The results of the study showed that using the "Android Auto" system is quite safe.

McAfee and its partners have published a report called "Precautionary Software" [22], in which they analyzed the new threats and risks in the automotive specialized computer system that are present in modern cars. In

[23-24], the authors show a comprehensive approach to show that the safety of modern cars may be compromised due to interference and interference with the passage of Bluetooth and Wi-Fi signals. In some articles, such as [25], security and privacy issues in car voice control systems are solved using different cryptographic methods, or using different secure development environments [26].

Conclusions

As a result of summarizing the literature to ensure the reliability of a specialized computer voice control system, a number of problems have been identified, the main of which is the imperfection of the user authentication system.

To implement the solution to this problem, a hardware and software product of an additional biometric automotive user authentication system was created and developed. The system was created to ensure the reliability of cyber attacks on the voice control system.

An experiment with a biometric authentication system found that the success rate for a registered fingerprint user who can access the car is ninety percent.

References

1. What is a computer system? - definition from technopedia. URL: https://uk.theastrologypage.com/computer-system (Accessed on: 06.11.2021).

2. Theology voice control. URL: http://tehnology.com (Accessed on: 22.11.2021).

3. S.Mohith., S.Santhanalakshmi., M.Sudhakaren. Gesture and Voice Controlled Robotic Car using Arduino.2018., pp 3392-3396.

4. What is Android Auto? And how it works. URL: http://www.rcd330.com.ua/ chto-takoe-android-auto (Accessed on: 05.12.2021).

5. How to set up Apple CarPlay in your car (manual). URL: https://uk.vemprarua.org/how-setup-apple-carplay-your-car (Accessed on: 15.12.2021).

6. A Voice Identification System using Hidden Markov Model T. K. Das., Khalid M.O., Nahar SITE, VIT University, Vellore – 632014, Tamil Nadu, India; Department of Computer Science, Yarmouk University, Irbid – 21163, Jordan.

7. V. N. Shmatkov, P. Bonkowski, D. S. Medvedev [et al.] Interact with IOT devices using the voice interface // Scientific and technical Bulletin of information technologies, mechanics and optics, 2019

8. Nicholas Carlini., Pratyush Mishra., Tavish Vaidya., Yuankai Zhang., Micah Sherr.,Clay Shields., DavidWagner.,Wenchao Zhou. 2016. Hidden Voice Commands. In 25th USENIX Security Symposium (USENIX Security 16). USENIX Association, Austin, TX, 513–530.

9. Collection of scientific works. Center for Strategic Studies of the National University of Defense of Ukraine named after Ivan Chernyakhovsky. 2018. № 3(64). C. 149.

10. Chaouki Kasmi and Jose Lopes Esteves. 2015. IEMI threats for information security: Remote command injection on modern smartphone

11. Nicholas Carlini, Pratyush Mishra, Tavish Vaidya, Yuankai Zhang, Micah Sherr, Clay Shields, David Wagner, and Wenchao Zhou. 2016. Hidden voice commands. In Proceedings of the USENIX Security Symposium.

12. Dibya Mukhopadhyay, Maliheh Shirvanian, and Nitesh Saxena. 2015. All your voices are belong to us: Stealing voices to fool humans and machines. In Proceedings of the European Symposium on Research in Computer Security. Springer, 599–621.

13. STMicroelectronics. 2016. MP34DB02 MEMS audio sensor omnidirectional digital microphone. http://www.mouser.com/ds/2/389/mp34db02-955149.pdf. 2016.

14. Yitao He, Junyu Bian, Xinyu Tong, Zihui Qian, Wei Zhu, Xiaohua Tian, Xinbing Wang. Canceling Inaudible Voice Commands Against Voice Control Systems. 2019. Article No.: 28. Pages 1-15.

15. DOBRUCKI, A. Nonlinear distortions in electroacoustic devices. Archives of Acoustics 36. 2 (2011). 437–460.

16. Nirupam Roy, Sheng Shen, Haitham Hassanieh, Romit Roy Choudhury University of Illinois at Urbana-Champaign. Inaudible Voice Commands: The Long-Range Attack and Defense.

17. Takeshi Sugawara, The University of Electro-Communications; Benjamin Cyr, Sara Rampazzi, Daniel Genkin, and Kevin Fu, University of Michigan. Light Commands: Laser-Based Audio Injection Attacks on Voice-Controllable Systems August 12–14. 2020.

18. D. Davidson, H. Wu, R. Jellinek, T. Ristenpart, and V. Singh, “Controlling UAVs with sensor input spoofing attacks,” in USENIX WOOT, 2016.

19. Omidiora E. O., Fakolujo O. A., Arulogun O. T., Aborisade D. O. 2011. A Prototype of a Fingerprint Based Ignition Systems in Vehicles. 62(2): 164-171.

20. Tomas Trainys, Algimantas Venčkauskas. Encryption Keys Generation Based on Bio- Cryptography Finger Vein Method. CEUR Workshop Proceedings 2145 (2018) 106-111

21. R Ramnath., N Kinnear., S Chowdhury., THyatt. Interacting with Android Auto and Apple CarPlay when driving: The effect on driver performance. 2020. pp 12-17.

22. Stuart McClure. Caution: malware ahead. Vision Zero International. 2013.

23. Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, Stefan Savage, Karl Koscher, Alexei Czeskis, Franziska Roesner, Tadayoshi Kohno, et al. 2016.

24. Charlie Miller., Chris Valasek. Remote exploitation of an unaltered passenger vehicle. Black Hat. 2015.

25. Ramon de Graaff. 2015. Controlling your Connected Car. 2015.

26. Yunhan Jack Jia., Ding Zhao., Qi Alfred Chen.,Z Morley Mao.Towards Secure and Safe Appified Automated Vehicles. 2017.