ENCRYPTED CLASSIFIED VOICE INFORMATION AND THE MANAGEMENT OF ITS SUSTAINABILITY

Elxan SABZİEV
Azad BAYRAMOV
Rahila SADIGOVA

Azerbaijan National Academy of Sciences,
Control Systems Institute, Baku, Azerbaijan

The problem of management of the reliable information security is one of the most important problems of our time. The problem of protecting information from unauthorized intervention and external impact is always topical and seriously investigated. A modification of the encryption algorithm related to the symmetric encryption method during the transmission of classified voice information is consudered in the paper. A management of the assessnent of a level of protection of encrypted classified voice information against cryptographic attacks is investigated by using of calculation of the keys number of encrypted data. This method is based on the rule of reflected sliding encrypted voice information.

Key words: *voice information, symmetric encryption, decryption, calculation method.*

1. INTRODUCTION

The problem of protecting information from unauthorized intervention and external impact is always topical and seriously investigated. In this regard, the value of the concept of information security is growing in connection with the development of human society, the emergence of private property and the further expansion of the scope of human activity. The emergence of personal computers, local and global networks, satellite communication channels, an effective technical reconnaissance and confidential classified information has significantly exacerbated the problem of information protection. Thus, the problem of management of the reliable information security has become one of the most important problems of our time [Sichev:2007, p.9].

Currently, the main target of cyberattacks is information exchange systems between users - sources. In this sense, Azerbaijan pays

special attention to the protection of the confidentiality of national information sources and the security of military information. To ensure information security in the public and private sectors of the country, normative legal acts have already been prepared, the articles of the Criminal Code on the prevention of cyber attacks have been improved. Laws on protection of state secrets have been amended and other important steps have been taken.

Voice information (speech) has a special place among the information required for secure exchange. Numerous objective and subjective factors influence the expansion and development of the technical arsenal used for the protection of voice information. From this point of view, considered to be taken into account during the study of the issue of ensuring confidentiality in the process of transmission of the conversation the following opinions have been formed:

- Human speech and hearing aids are considered to be a perfectly adapted and obstacle-resistant system, in this regard, small distortions in speech do not prevent its understanding [Kravchenko: 1999; Tsviker & Feld-keller:1971].
- Devices and communication systems involved in the processing and transmission of voice information are constantly progressing and developing. For mobile devices and computers, the speech interface is considered the most convenient way to exchange information. Appropriate changes affect leaks of speech information, as well as methods of unauthorized access to this information. This process requires an adequate approach to the development of defense strategies and the improvement of methods for the protection of speech signals.
- In principle, new automated and computerized processing systems are becoming more widespread. These systems process, collect, and store large amounts of information, including speech. In this regard, the development of new technologies and methods of protection management of speech information is required [Grishin: 2008].

The choice of methods of encrypting and decrypting the transmitted data in order to secure it is, as always, relevant in modern times. The purpose of choosing these methods is to prevent outside interference in the transmitted

information. Encryption has always been the target of encryptors. Once encryptors have created tools that can detect vulnerabilities in encryption, it makes no sense to use this encryption rule.

The proposed encryption methods for transmitting information are reflected in many articles [Bauer & Friedrich:2007; Encyclopedia:2005; Shayer:2003; Singh:2006; Pashaev et.al: 2016a; Pashaev:2016b; Hasanov:2019]. Which of the proposed methods is preferred depends on both the type of information being collected and the area to which it relates. The complexity of the encryption process can make it difficult to decrypt. New algorithms are added to the encryption process to protect against crypto attacks.

The application of floating-point encryption to voice data encryption is described in detail in [Hasanov:2019a]. During the investigation, some technical problems were encountered in solving the problem. In order to eliminate these problems, or not to encounter them again, it is necessary to add innovations in the process of data encryption. Therefore, it is necessary to take other measures. These problems include the fact that the length of the keyword plays a special role in the encryption of voice data, and the closeness of the data obtained without encryption with similar keywords.

2. PROBLEM STATEMENT

Let's take another look at the method of encrypting voice data [Hasanov:2019b]. It is believed that the encryption operation is carried out by using of a program controlled by the operator. Like text-based information, voice information is also vulnerable to cyberattacks. To protect such information, the article [Hasanov:2019b] provides an algorithm for generating a second keyword using the primary keyword and an encryption algorithm using a second keyword. Voice information protected in this way requires an investigation into the reliability of encryption during a cyber attack.

The problem that a third party will encounter when attacking this information will be to set the primary keyword encrypted by a special algorithm. Exploring the different options for assigning such a keyword will certainly take a long time. It should be noted that the importance of a number of characters in the primary keyword is large. The greater the number of characters that make up a keyword, the longer the time it takes to identify it. The problem statement is to estimate the amount of time it takes to decrypt a data in a cyberattack, depending on the number of characters in the keyword.

3. VOICE DATA ENCRYPTION MECHANISM

Before solving this problem, let's recall in detail the mechanism of the method of sliding imaging encryption of voice information [Hasanov:2019b].

Normally, in order to transmit voice information expressed by "0" and "1", it is digitized from a microphone or received from files with audio content, divided into parts called "chunk", and then transmitted on the basis of protocols based on appropriate rules. For such transmission, it is important that the transmitter and receiver operate on the same protocol. The mechanism for sliding imaging encryption of voice data is that the parts of the data are chunked and encrypted with the known keyword. This encryption procedure can be described in more detail as follows: For the first chunk, its digits "0" and "1" are added to the beginning of the keyword of the same length, and the next "0", which forms the keyword for encrypting the next chunk. or a sequence of numbers "1" is applied. This process is repeated for each subsequent chunk. If the number of characters in the keyword is not enough for any "chunk", then the key is returned to the beginning of the word and applied to the missing part in the previous order.

The decryption procedure was the complete opposite of the encryption procedure. It is necessary to deduce from the accepted "chunk" the parts of the keyword expressed by "0" and "1". In essence, encryption means that the part of the keyword that is involved in the conversion imaging process is shifted along the word to "chunk" each time.

In order to complicate the decryption process during a cyber attack, in addition to the procedure given in [Hasanov:2019a] in the process of encrypting voice data, two more algorithms [12] had been proposed for performing the procedure.

In order to complicate the decryption process during a cyber attack, in addition to the procedure given in [Hasanov:2019a] in the process of encrypting voice data, [Hasanov:2019b] proposed two more algorithms for performing the procedure. The problems can be solved by implementing two additional measures - the procedure, in addition to the operation of collecting codes during the application of this encryption algorithm. In order to complicate the decryption process during a cyber attack, in addition to the procedure given in [Hasanov:2019a] in the process of encrypting voice data, [Hasanov:2019b] proposed two more algorithms for performing the procedure.

The problems can be solved by implementing two additional measures - the procedure, in addition

to the operation of collecting codes during the application of this encryption algorithm.

The purpose of this algorithm is to bring the volume of the entered primary keyword into a "chunk" order. So, to get an "extended keyword", you need to make an additional "extension" to the original keyword, which differs from each other many times and is not repeated. The mathematical algorithm of this procedure can be interpreted as follows (Algorithm 1): after dividing the length of 1 "chunk" (1600 bytes) by the length of the primary keyword consisting of k characters, the number of additions required to extend it is found. This number is denoted by N. Then the codes of the characters in which the keyword is composed are calculated by multiplying their numbers by 2 and N + 1, respectively, and these examples are placed side by side to obtain an "extended keyword".

In data obtained from reflected sliding encrypted data using similar keywords that differ by several characters, the characters that differ from each other form a set with a very small density in the sequence of all characters in the information. Due to the robustness of the auditory organ, a person perceives the elements of this set as noise, but the low density of this set in the general flow of audio information does not prevent it from being understood well enough. To solve this problem, it is proposed to use a procedure in which each character of the keyword participates in the encryption of all characters of voice information. This algorithm can be expressed, for example, as follows: a "derivative keyword" can be obtained by performing the following mathematical operations on a primary keyword consisting of k characters:

$$B_j = \sum_{i=1}^{k} (i + j) \times A_i, \quad j = 1,2, \dots, k.$$

Here, $A_i, i = 1, 2, \dots, k$ are the characters that make up the primary keyword, B_j, $j = 1, 2, \dots, k$ are the characters that make up the "derivative keyword". It is easy to see that changing any character in the sequence $A_1 A_2 A_3 \dots A_k$ of the "primary keyword" causes all the characters changing of the "derivative keyword".

4. EVALUATION OF THE RESISTANCE OF ENCRYPTION ALGORITHM TO CYBER ATTACKS

In order to apply the full counting rule to all possible keys, it is necessary to know which the crypto-analyst of cryptographic system is used. This method is used much because it is available easy [Dudenko:2002]. It should be noted that due to the rapid development of

information technology, increasing the size of computer memory and increasing the frequency of operations, the duration of resistance to cryptocurrencies can be reduced by the full counting of keys. While the similarities in the application of the full counting rule for all possible keys to the disclosure of text-to-text information and voice-to-voice information are that all possible keys are considered [Pashaev: 2016b], the principles governing the decryption of each key are different.

Thus, if the fact of decoded text-type information is explained by the fact that the received expressions are in the existing dictionary, the fact of decodeding the spoken speech information can be determined by the presence of a sufficient number of speech breaks indicating that it consists of separate parts. In consideration of that this criterion is used for crypto-attacks, the resistance to such an attack can be assessed as follows.

Let's denote the number n by all the characters of the alphabet used in the encryption system. It is believed that the length of the keyword is limited from below and above. Let's denote the minimum number of characters that make up the keyword as , the maximum number as . Then the number of keys that can be corrected using the number m of all characters of the alphabet is . It is estimated that at least half of the combinations must be verified to verify that they have a decryption key. Let's denote the check period t of a key by according to the rule of full counting of keys. Then the time required to find the key in this way is calculated as follows:

$$T = \frac{t}{2} \sum_{m=m_0}^{m_n} n^m \quad (1)$$

It should be noted that the length of the keyword is usually 15-25 characters. For example, in [Yaglom & Yaglom:2007] the number of alphabetic characters is $n = 35$ and the time taken to verify a key is $t = 2$ seconds. Then, depending on whether the secret key consists of $m = 3,4,5$ characters, the following evaluation table is obtained for the average decoding time according to the formula (1) (Table 1):

Table 1. Decryption time depending on the number of characters

The length of a secret key (number of characters)	m	3	4	5
The time required to find the key (necessary number of days)	T	0,5	18	626

The formula (1) allows you to determine the minimum length of a keyword, depending on the degree of relevance and relevance of the information being transmitted. For example, based on Table 1, it can be said that a 3-character keyword can be used to encrypt the information transmitted over a conversation only if the urgency of protecting the information is measured in hours. If the relevance of the information is measured in years, the number of characters in the keyword should be 5 or more characters, depending on the time period.

5. CONCLUSION

Thus, the presented paper considers the issue of assessing the resistance to attempts cyber attacks in order to decrypt encrypted voice information using sliding encrypted encryption method. To assess the continuity of decryption of speech-type voice information, a formula is given that determines the average time of decryption based on the verification period of a key in accordance with the rules of full counting of keys. This formula allows you to determine the minimum number of characters in the key used to encrypt information, depending on the degree of relevance.

REFERENCES

[1] Dudenko S.V. Evaluating the parameters of a cryptographic system key // Information development system, vol,, 3(19), 2002, p.155-157.

[2] *Encyclopedia of Cryptography and Security*. Edited by Henk C.A. van Tilborg., Springer Science+Business Media, Inc., Printed in the USA, 2005, 684 p.

[3] Grishin A.M. *Methods for protecting speech information* // Applied discrete mathematics, Mathematical basis of computer security. 2008, №2(2).

[4] Hasanov A.N., Sabziev E.N., Talibov A.M. Sliding encryption of voice information in a military control system // Information safety. 2019, №1, p. 11-17.

[5] Hasanov A.N., Sabziev E.N. Analysis and solutions to voice data encryption problems // National safety and military sciences, 2019, №2, p. 13-16.

[6] Kravchenko V.B. Defence of spoken information in communication chanels // Special texnics. 1999. №4. p.2-9.

[7] Pashaev A.B., Sabziev E.N., Hasanov A.N., Abdullaeva G.V., Talıshinski M.M. About one method of text coding // National safety and military sciences. Baku, 2016, №2(2), p. 123-128.

[8] Pashaev A.B., Sabziev E.N., Hasanov A.N. Assessing the difficulty of decrypting encrypted text using a modified encryption method // National safety and military sciences, 2016, №3(2), p.22-26.

[9] Shayer B. *Applied cryptography. Protocols, algorithms, source texts in the CI-language*. Moscow. Triumf, 2003, 806 p.

[10] Sichev Y.N. *Basis of information safety*. Moscow. 2007, Pbl. Center EAOI, 300 p.

[11] Singh S. *Book of codes. The secret history of codes and their decryption*. Moscow. Akt, Aktrel, 2006. 447 p.

[12] Tsviker E., Feldkeller R. *The ear as a receiver of information* //Ed. I.G. Belkina. Moscow. Svaz, 1971.

[13] Yaglom A.M., Yaglom I.M. *Probability and information* // Moscow. КомKniga, 2007, 512 p.