UDC 654.15:621.395.721.5:004.056.523 **doi: 10.32620/reks.2024.2.14**

Andrii ASTRAKHANTSEV, Stanislav PEDAN

Department of Information technologies in telecommunications, National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine

IMPROVING USER SECURITY DURING A CALL

The recent development of mobile networks has led to the emergence of new threats and methods of implementing existing ones. Phishing attacks, including robocalls, are causing record losses to both individual users and large corporations. At the same time, existing countermeasures cannot provide protection against such attacks because most existing solutions focus on device authentication, whereas user authentication does not occur during a call. Another problem with mobile networks is that there is no point-to-point encryption, i.e., the speech is encrypted only on the segment from the subscriber to the base station. ***The subject*** *of study in this article is the process of ensuring user security during a call.* ***The purpose*** *of this study is to develop a model of mutual user authentication and end-to-end data encryption in a mobile network during a call. The main* ***objectives*** *are the protection of users from spoofing and vishing and the proposal of a protection method by implementing mutual authentication of users during a call without storing confidential information on the side of a "trusted third party". Method of secure key exchange and end-to-end encryption during a call in the mobile network was proposed. It prevents the interception of calls by the operator for circuit-switched and packet networks. The* ***methods*** *used are mathematical modelling, ontological approach, and multi-criteria optimization models. Because of this research, an algorithm for mutual authentication of users is proposed by introducing biometric authentication methods and modifying the sequence of messages during a call. The proposed approach can be implemented for CS-call and VoLTE/VoWiFi calls. A call cannot be received without user biometric authentication; such as ear pattern or bone conduction methods. Modified SETUP and CONNECT ACK messages are used to inform the other party about the user verification result. This prevents user spoofing, call masquerading, and robocalls. A combination of the proposed asymmetric encryption, a short authentication string, and hashes of previous calls provides a higher level of confidentiality, integrity, and additional resistance to man-in-the-middle attacks.* ***Conclusions****. The scientific novelty of the obtained results is the integration of the above methods into the sequence of call flow messages for providing mutual authentication, end-to-end encryption, and counteraction to the number of network attacks. The proposed methods allow one level to increase the provision of services of privacy and observation groups and can be implemented in the software part of user equipment.*

Keywords: *user authentication during a call; voice encryption; mobile networks; call flow; attack prevention.*

Introduction

Many people receive phone calls from unknown callers, and this is becoming a serious problem. Spam calls continue to deceive people around the world, despite the efforts of operators, telecom companies, mobile operating system developers, smartphone manufacturers, and the pandemic. Truecaller [1] reported 31.3 billion spam calls worldwide from January to October 2022. According to the report [1], in 2021, the average American lost about $502 because of vishing (also known as "voice phishing" or user spoofing), which was up from $351 in 2020.

Vishing is a scam aimed at obtaining sensitive personal information, such as social security information, identification number, and credit card details. Attackers use vishing to illegally obtain data to gain access to bank and social media accounts.

One of the most popular types of vishing is robocall [2]. A robocall is a call that transmits pre-recorded messages using an automatic dialing software.

One of three victims of fraudulent calls picks up the phone because the number sounds familiar. Unknown numbers are the most common, and people do not answer them. This has led fraudsters to adopt a new strategy to get their calls answered. To gain the recipient's trust, they started spoofing the phone numbers of real companies and acting on their behalf. This is called "corporate spoofing" [2].

Thus, to minimize user losses and block the threats associated with vishing, it is necessary to conduct research in this area. In practice, the implementation of the research results will make it impossible to perform vishing attacks based on user spoofing and the use of robocalls. According to reports [2], this will save in average about ~27 million people in the US only. The problems of data leakage are also analyzed in local publications. Article [3] discusses the problem of ensuring the protection of user data in information systems.

The above problems related to the protection of users in mobile networks from vishing, user spoofing, and lack of encryption have been widely covered in the literature due to their importance. Thus, a voice authentication system is proposed in [4]. To increase efficiency, the usage of additional devices in the form of headphones is suggested. However, the issue of authentication during the call remains unresolved because there may be a substitution of the subscriber after voice authentication. This aspect is not analyzed in [4] because it is devoted to the use of a Gaussian mixture for voice authentication, and its further application is not relevant to the purpose of this article. It [5] deals with approaches for user authentication and uses a smartphone as a hardware token, but it does not provide the transmission of user verification information because the authentication process is not considered from the perspective of confirmation during a call. In addition, both methods [4, 5] do not address the issue of data encryption.

Improving user security by using end-to-end encryption is described in [6]. At the same time, the article [7] presents a study of encryption algorithms for mobile devices. The focus is on maintaining the confidentiality of mobile data in the absence of access. AES, DES, RSA, and REA algorithms are studied. The experimental results show that AES is the fastest algorithm and REA is the slowest. Based on the results of [7], the proposed method uses AES (256). The article [8] proposes an effective approach to implement end-to-end encryption through asymmetric encryption and the rejection of a third trusted party. The above publications solve the issue of encrypting data on a mobile device and protecting this data from unauthorized access, but they are not compatible with existing messaging protocols and cannot be used for protection during a call.

Work [9], similar to this article, substantiates the effectiveness of using biometric authentication on a smartphone, but does not provide specific steps for its implementation during a call. A potential reason for this is the need to conduct research in two areas simultaneously: telecommunications and information security.

The article [10] investigated and systematized their end-to-end encryption (E2EE) features, including their underlying authentication ceremonies. The most important part of this research is the analysis and evaluation of a broader set of the most popular E2EE apps and their underlying authentication ceremonies, including during call encryption and authentication. A similar solution for E2EE is presented.

Paper [11] highlights the potential risks and vulnerability of information and control interaction technology in wireless smart systems.

In article [12], we presented a contact-separated triboelectric nanogenerator that allows to mask conversational speech signals through airflow vibrations. This solution protects speech in open space but does not solve the problem of speaker verification confirmation.

In paper [13], a millimeter-wave radar-based voice security authentication system is proposed. This system is highly adaptable and can authenticate designated speakers, resist intrusion by other unspecified speakers and playback attacks, and is secure for smart devices. Extensive experiments have verified that the system achieves a speaker verification accuracy of 93.4% and a misdetection rate of 5.8% for playback attacks.

The study [14] provides evidence that consumer happiness is influenced by voice features (including voice assistant) and shows the role of privacy risk.

For VoIP/VoLTE/VoNR calls, the key protocol is SIP. The paper [15] presents an overview of the authentication and key negotiation schemes proposed for the SIP protocol. It also identifies, classifies, and evaluates various SIP authentication and key negotiation protocols according to their performance and security features, but this overview does not provide encryption and protection against user spoofing.

Given the above, it can be concluded that research aimed at ensuring the protection of users is an important current task, and to protect users, it is necessary to apply effective methods compatible with existing telecommunications protocols.

1. Current Research Analysis

Currently implemented call authentication solutions are mostly based on the presence of a trusted third-party, which should be a service provider. It increases the complexity of the security system. The most widespread solutions are those based on the STIR/SHAKEN protocol [16].

According to the STIR/SHAKEN protocol, a certificate of authenticity must be attached to each call so that service providers can differentiate legitimate from fraudulent calls, such as illegal spoofing, robocalls, or spam calls. If the call does not match the certificate, the customer will see a "spam risk" warning on the caller ID. STIR and SHAKEN are two technologies that stand for Secure Telephony with Identity Re-verification (STIR) and Secure Tokenized Handling of Confirmed Information (SHAKEN). Although STIR technology was designed to be compatible with VoIP calls, it is not compatible with conventional telephone networks. This led to the development of SHAKEN, which performs a similar function to STIR but is compatible with telephone networks that do not depend on an Internet connection [16]. The disadvantages of this approach are that it requires additional time for verification on the side of the "trusted party" and there is no description of the authentication procedure in the case of a CS call in the literature. In addition, the STIR/SHAKEN protocol does not protect against cases when:

- another person calls from a trusted number (in existing solutions, device is authenticated, not the user);
- the phone is picked up on the receiving side by someone other than the owner of the phone, which can lead to a leak of confidential information;
- number of spoofing (substitution) occurs;
- data leakage on the side of the "contact center" - a trusted third party.

One way to protect against vishing is to verify the interlocutors, so the task of user authentication during a call is relevant. In addition to user authentication, increasing user security during a call can be achieved by solving a number of problems, including the following:

- lack of end-to-end encryption in the mobile network;
- user's voice data (including passwords) can be intercepted;
- mobile network subscribers are not protected from sniffing attacks by the operator;
- mobile network subscribers are not protected from fake base station creation and other attacks.

Based on the analysis of the sources, it can be concluded that most of the sources are focused on solving specific issues and do not provide comprehensive user protection. In most cases, the device is authenticated, not the user. In the author’s opinion, this is due to the complexity of making changes to the messaging protocol during a call and the difficulty of conducting experimental studies on a real network. This suggests that it is advisable to conduct a comprehensive user protection study, which would include simultaneous protection against attacks, implementation of end-to-end encryption, and user authentication.

The purpose of this research is to increase the security of mobile network users during a call by protecting them from spoofing attacks, vishing, and interception of the conversation by the operator.

To achieve this goal, the following tasks were set:

- to protect against user spoofing and vishing, to propose a method of protecting against vishing by implementing mutual authentication of users during a call without storing confidential information on the side of a "trusted third party";
- to prevent the interception of conversations by the operator and to propose a method of secure key exchange and end-to-end encryption during a call over a mobile network.

2. Materials and Methods

2.1. Methodology

In accordance with this objective, the object of study is user security during a call. The subject of this study is methods for improving the metrics responsible for the security of mobile network users, as specified in [17], such as confidentiality, integrity, availability, and observability.

The tasks specified in the research objective were achieved by the theoretical development of a new approach followed by mathematical modelling. After determining the characteristics of the proposed approach, a comparative multicriteria analysis was performed using solutions that are currently in use or patented.

The main hypothesis of the study is that during a robocall or user spoofing, the caller’s authentication cannot be confirmed and, accordingly, the call recipient will be warned that the other party is not authenticated and may be a fraudster. This hypothesis is based on the following assumptions:

- most attacks are carried out using robocalls;
- the attack scenario is user spoofing or using a number known to the user (son, daughter, mother);
- biometric authentication is sufficient for reliable confirmation.

For the sake of simplicity, we did not consider hostage scenarios (when a call is received by one person and then another takes over the phone), or "bank" employees (we need to develop a concept for verifying the number of the institution and the users assigned to it).

The following components were chosen as the task statement for the method of mutual authentication of users during a call to prevent spam calls, robocalls, and vishing:

- mutual authentication of users during a call;
- compatibility with 3G/2G (CS calls) and VoIP/SIP (PS calls) calls;
- authentication should be performed automatically, without any additional actions from the user;
- inability to receive a call without user authentication.

To ensure the integrity and confidentiality of users, the method under development had to provide end-to-end encryption, eliminate the impossibility of using the previous session, and block possible attacks from the operator.

Let us now describe the following methods to increase user security during a call.

2.2. A method of protection against vishing by implementing mutual authentication

On the basis of the above requirements, we propose a method for mutual authentication of users during a telephone (CS) or packet (VoIP) call. This method allows users to be confident in the identity of the subscriber on the other side.

The implementation of the mutual authentication method consists of (Fig. 1):

1) obtaining biometric data of the user to be authenticated (registration phase);

2) identification of the user during a call (without additional actions on the part of the user) as a specific authorized user based on biometric data (mutual authentication during the call);

3) in case of positive identification:

– a message with the authentication result will be sent to both parties;

– a screen that displays confirmation of the calling party and the called party;

– a call can be accepted or rejected according to the decision of the authorized user;

4) in case of negative identification:

– an incoming call will be rejected;

– or additional authentication may be requested.

The above sequence is implemented using the method shown in Fig. 1. The improved or newly proposed elements are marked in green.

As shown in Fig. 1, the procedure for using the proposed method consists of the following steps:

1. *Authentication*: at the enrollment phase, the user needs to go through the registration procedure for the first time to authenticate the ear. To do this, the user requests the authentication procedure in the application. After that, the user takes the phone and puts it to the ear several times, during which the algorithm shown in Fig. 2 is executed.

2. *Start an outgoing call* (Fig. 1). After the successful enrollment phase, the user initiates a call through the standard application.

3. *Authentication during an outgoing call* (see Fig. 1). A new proposed element of the algorithm is the use of ear pattern authentication during dialing. Ear pattern authentication was chosen based on the following advantages:

– can be used in the dark;

– there can be no substitution;

– no unusual movements during the call;

– a little time is needed to check the correctness.

In case of failure, acoustic response authentication [18] or fingerprint authentication can be used. The type of authentication is selected depending on the scenario of receiving a call: via a mobile device (smartphone) (Fig. 3) or an additional smart device (e.g., a smartwatch) (Fig. 4).

4. *Communication channel* (see Fig. 1). Typical network procedures related to the transfer of information from user A to user B and vice versa are performed.

5. *Interception of an incoming call* (see Fig. 1). A new proposed element of the algorithm (shown on Fig. 5). It is responsible for authenticating the user receiving the call in accordance with one of the two scenarios below (see Fig. 3, in the case of answering a call using a phone and Fig. 4, in the case of answering a call using a smartwatch).

A message about successful authentication is included in the "*CONNECT*" message and sent to the calling party. In case of unsuccessful authentication, the user is offered another verification method (for example, a fingerprint). The call cannot be accepted and will be rejected until successful authentication.

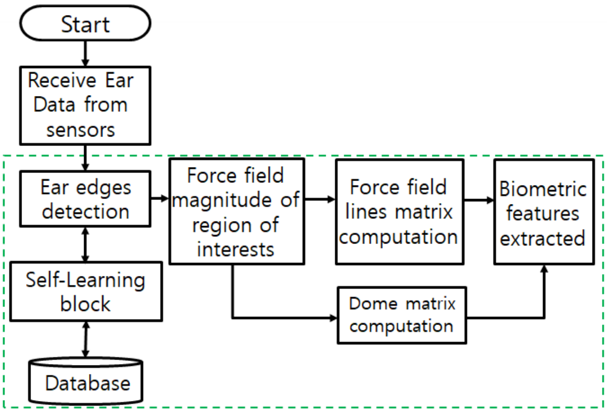

Start
Receive Ear Data from sensors
Ear edges detection
Force field magnitude of region of interests
Force field lines matrix computation
Biometric features extracted
Self-Learning block
Dome matrix computation
Database

Fig. 2. Initial authentication (enrollment phase)

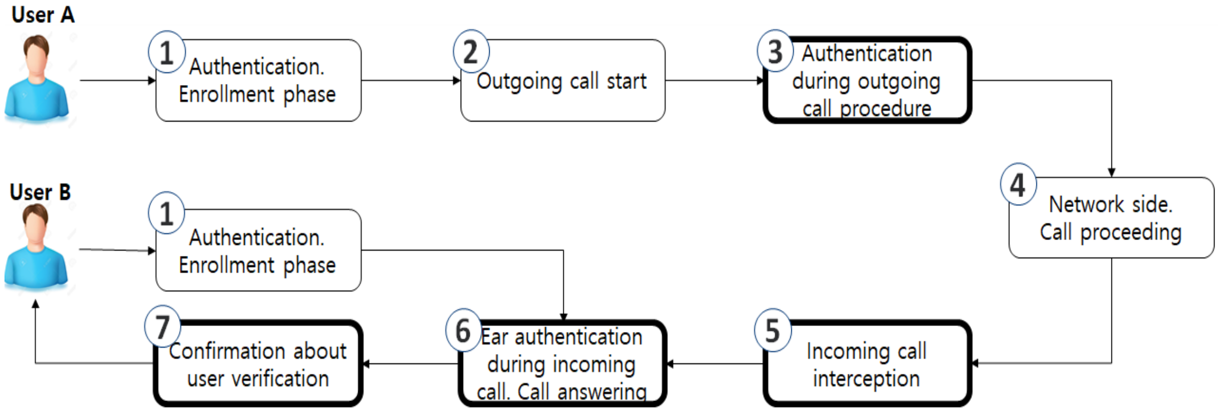

User A
1 Authentication. Enrollment phase
2 Outgoing call start
3 Authentication during outgoing call procedure
4 Network side. Call proceeding
User B
1 Authentication. Enrollment phase
5 Incoming call interception
6 Ear authentication during incoming call. Call answering
7 Confirmation about user verification

Fig. 1. Proposed method for securely answering calls by providing a mutual authentication

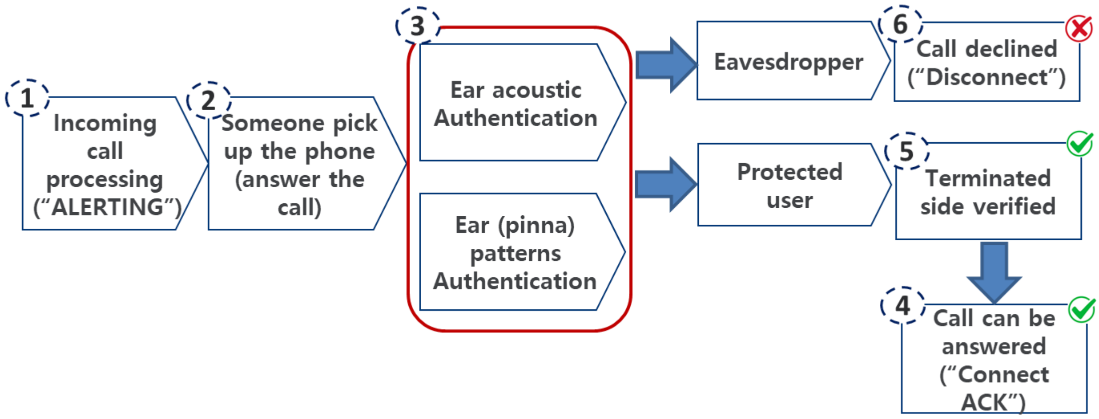

1
Incoming call processing (“ALERTING”)
2
Someone pick up the phone (answer the call)
3
Ear acoustic Authentication
Ear (pinna) patterns Authentication
Eavesdropper
6
Call declined (“Disconnect”)
Protected user
5
Terminated side verified
4
Call can be answered (“Connect ACK”)

Fig. 3. Sequence of actions during user verification when answering a call using a smartphone

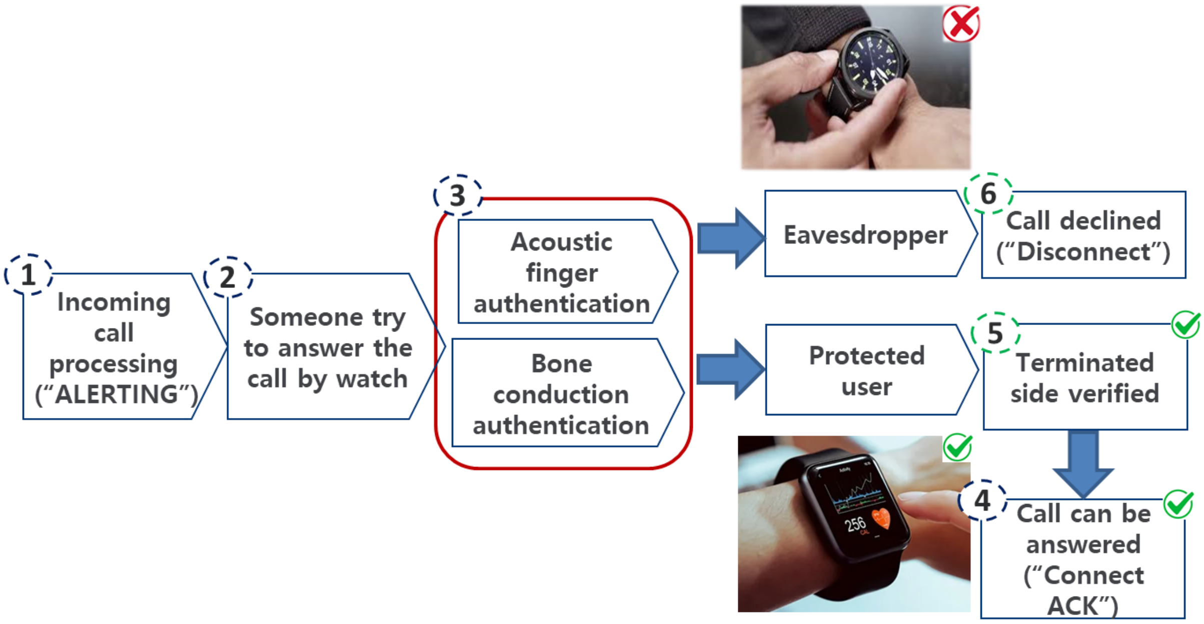

1
Incoming call processing (“ALERTING”)
2
Someone try to answer the call by watch
3
Acoustic finger authentication
Bone conduction authentication
Eavesdropper
6
Call declined (“Disconnect”)
Protected user
5
Terminated side verified
4
Call can be answered (“Connect ACK”)

Fig. 4. Sequence of actions during user verification when answering a call using a smartwatch

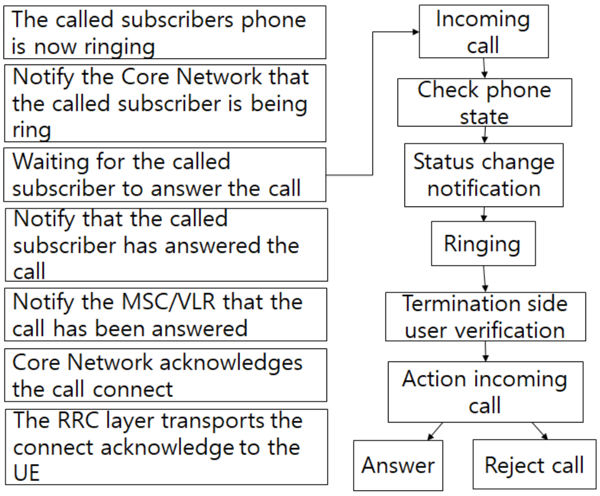

The called subscribers phone is now ringing
Notify the Core Network that the called subscriber is being ring
Waiting for the called subscriber to answer the call
Notify that the called subscriber has answered the call
Notify the MSC/VLR that the call has been answered
Core Network acknowledges the call connect
The RRC layer transports the connect acknowledge to the UE
Incoming call
Check phone state
Status change notification
Ringing
Termination side user verification
Action incoming call
Answer
Reject call

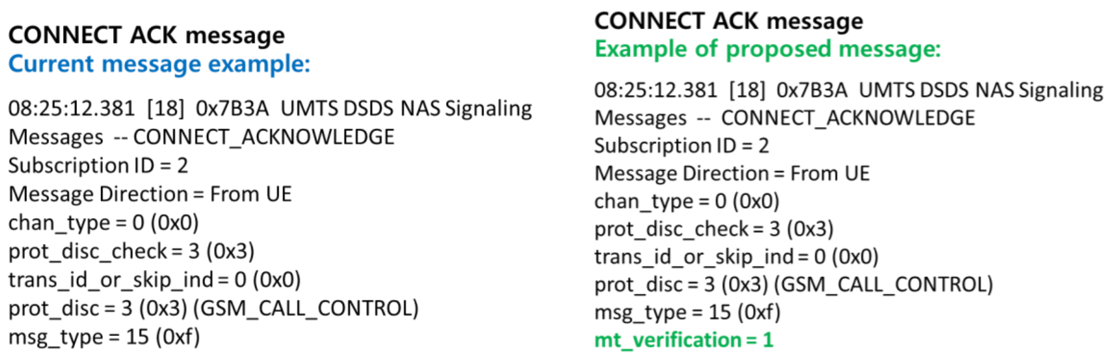
Fig. 5. Proposed call interception procedure

6. *Answering an incoming call* is allowed only after successful authentication.

7. *User verification* is confirmed after successful authentication during the call. Confirmations for both users will be delivered using the *"SETUP"* and *"CONNECT ACK"* messages. An example of the initial and modified *"CONNECT ACK"* message is shown in Fig. 6.

The final message exchange protocol showing the entire call process with the modified elements (highlighted) is shown in Fig. 7.

As can be seen from Fig. 7, the information about the authentication of the call originating side is transmitted with the message *"SETUP"* and the user to whom the call is made already knows whether the user



```
CONNECT ACK message
Current message example:

08:25:12.381  [18]  0x7B3A  UMTS DSDS NAS Signaling
Messages  -- CONNECT_ACKNOWLEDGE
Subscription ID = 2
Message Direction = From UE
chan_type = 0 (0x0)
prot_disc_check = 3 (0x3)
trans_id_or_skip_ind = 0 (0x0)
prot_disc = 3 (0x3) (GSM_CALL_CONTROL)
msg_type = 15 (0xf)
```

```
CONNECT ACK message
Example of proposed message:

08:25:12.381  [18]  0x7B3A  UMTS DSDS NAS Signaling
Messages  --  CONNECT_ACKNOWLEDGE
Subscription ID = 2
Message Direction = From UE
chan_type = 0 (0x0)
prot_disc_check = 3 (0x3)
trans_id_or_skip_ind = 0 (0x0)
prot_disc = 3 (0x3) (GSM_CALL_CONTROL)
msg_type = 15 (0xf)
mt_verification = 1
```

Fig. 6. Proposed modification of “*Connect ACK*” message

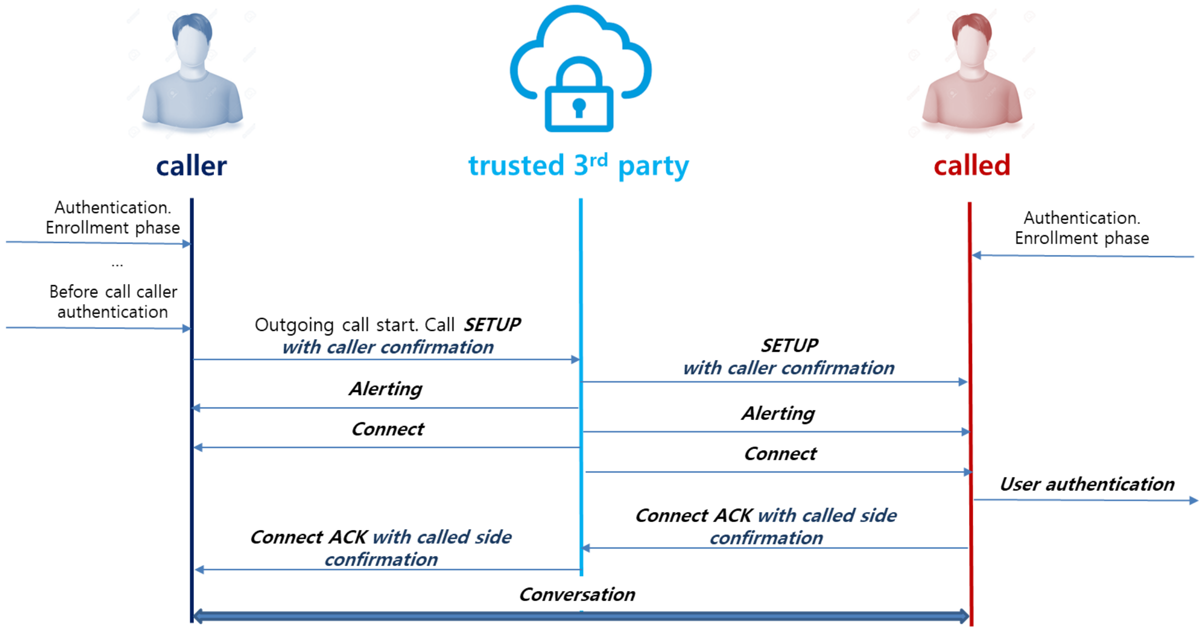

caller
trusted 3rd party
called
Authentication. Enrollment phase
...
Before call caller authentication
Outgoing call start. Call SETUP with caller confirmation
Alerting
Connect
Connect ACK with called side confirmation
SETUP with caller confirmation
Alerting
Connect
Connect ACK with called side confirmation
Authentication. Enrollment phase
User authentication
Conversation

Fig. 7. Modified call flow sequence during a voice call conversation

on the other side is corresponding. In turn, information about the verification of the called party is transmitted with the message "*CONNECT ACKNOLEDGEMENT*", which allows the originating side to see who received the call.

Because there are no existing solutions that would provide mutual authentication of users rather than devices during a call, the proposed method of secure call answering was compared with other patented solutions. For comparison, a multi-criteria analysis was performed based on the following criteria: the possibility of using the device during a call, the availability of mutual authentication, and the possibility of using the device without authentication. The results of a comparative analysis of the effectiveness of the proposed and existing methods are presented in Table 1.

The proposed method protects against vishing and user spoofing attacks and increases the level of sender and receiver authentication services, according to [17].

2.3. Proposed method of secure key exchange and end-to-end encryption during a call

In 2G/3G networks, the challenge and response protocol is used during the handover (Fig. 8). In this protocol, the user equipment (UE) has to prove that it recognizes the key, and only in rare cases does the UE authenticate the home network. This leaves the possibility of creating a fake connection (fake base station) and intercepting user traffic [23].

To overcome these problems and increase the level of privacy, a method of increasing user privacy that differs from the existing methods (Fig. 9) was proposed (Fig. 10):

– Diffie-Hellman protocol for secure key exchange;

– Short Authentication String (SAS) to counteract the man-in-the-middle attack;

– a pre-call hash to counteract phone number spoofing;

– modern symmetric encryption of speech using the AES (256) algorithm to counteract eavesdropping and increase confidentiality in the exchange [17].

Consider the Diffie-Hellman (DH) key exchange protocol (Fig. 9) [25].

According to Fig. 9, Alice chooses a and sends A=g^a, while Bob chooses b and sends B=g^b. Both parties compute g^ab and generate a message authentication code (HMAC) based on this value, along with many other parameters, to obtain a temporary session key CK(i). The parties then calculate the 32-bit Short Authentication String (SAS) value as a function of CK(i) and compare them.

The new session key "*Total_key*" is calculated as the value of g^{ab} and the hash function of the previous call's hash (from the old session). Signed certificates or verified SAS can also be used.

Table 1

Comparative analysis of the proposed method for secure call answering with existing solutions

Existing solution	1	2	3	4	5
US9197 746B2 [19]	Yes	Trusted party–network. Device is checked	No info	Malware traffic, phishing, farming, web-spoofing	No need, network makes all decisions
CN10518 7672A [20]	Yes	3rd-party makes decision	Smart-phone only	User spoofing	Preliminary authentication required, works for existing contacts only
US859 4287B2 [21]	No, bef. call only	One party only	Smart-phone and computer	User not identified	Every user settings required before first call
US202 00184 057A1 [22]	No	One party only	Head set	Non-authorized user	–
Proposed method	Yes	Two parties	Smart-phone, head set	vishing, user spoofing	Preliminary authentication required

The following notations are used in Table 1: 1 – possibility of usage during a call; 2 – ability to authenticate both parties; 3 – ability to answer the call; 4 – list of attacks against which the solution protects; 5 – the need for preliminary settings.

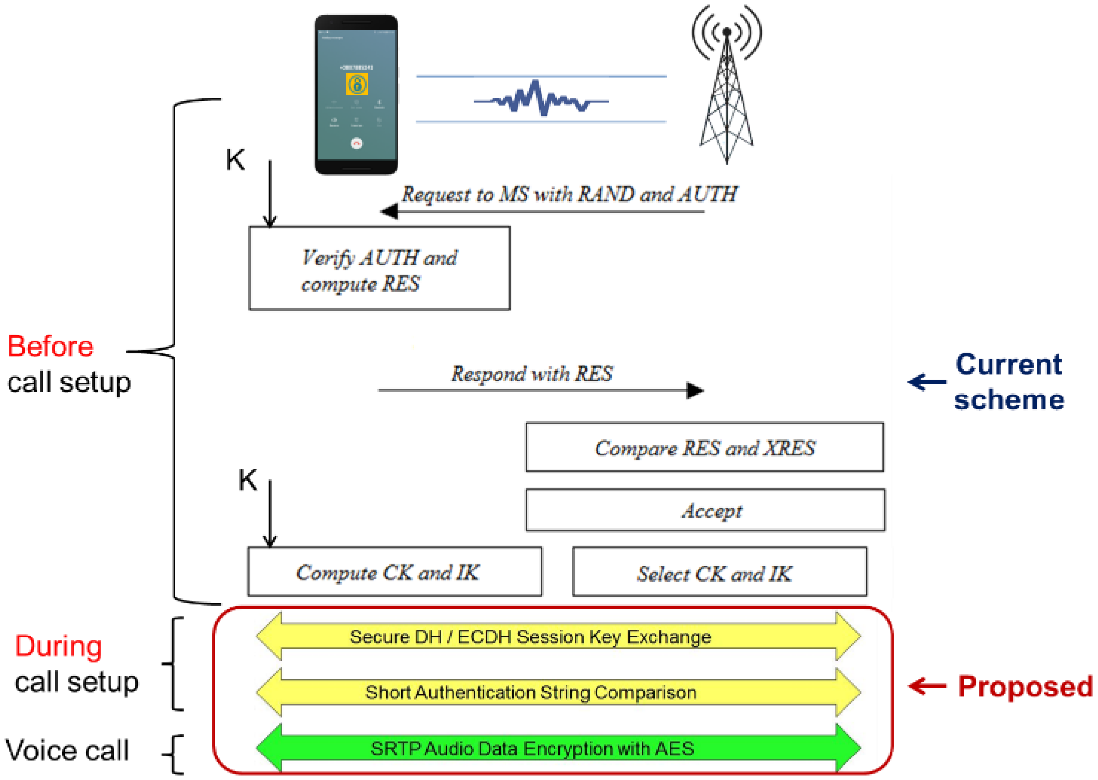

K
Request to MS with RAND and AUTH
Verify AUTH and compute RES
Before call setup
Respond with RES
Current scheme
Compare RES and XRES
K
Accept
Compute CK and IK
Select CK and IK
During call setup
Secure DH / ECDH Session Key Exchange
Short Authentication String Comparison
Proposed
Voice call
SRTP Audio Data Encryption with AES

Fig. 8. Improved procedure for ensuring subscriber privacy

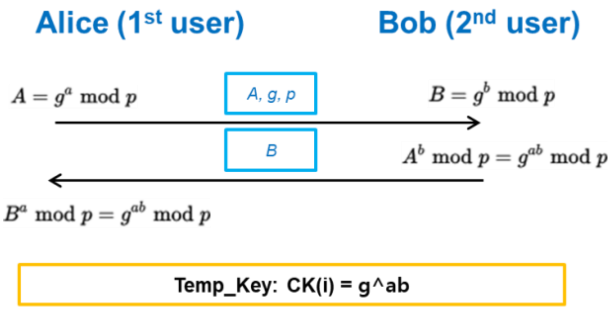


Fig. 9. DH key exchange protocol

To implement the above protocol, we proposed a modification of the *"SETUP"* and *"CONNECT"* messages in the traditional call flow sequence during call establishment. The modified call flow sequence is shown in Fig. 10.

Diffie-Hellman key exchange alone does not provide protection against a man-in-the-middle attack. To ensure that the attacker is not really present in the first session (when there are no shared secrets), the Short Authentication String (SAS) method [24, 25] is used (Fig. 11).

The advantages of the short authentication string include the absence of the need for a "trusted third-party". The most effective cases when the use of a short authentication string is necessary are as follows:

- user certificates are missing, revoked or expired;
- there is no hash of the previous call;
- an unsigned Diffie-Hellman protocol is used.

The sequence of actions during the calculation and use of SAS is shown in Fig. 11. The proposed differences are marked in red.

The effectiveness of counteracting man-in-the-middle attacks is achieved by implementing a second level of authentication based on key continuity. For this purpose, some hashed key information is stored in the TrustZone for use in the next call, which will be mixed with the shared DH secret of the next call, giving it key continuity properties similar to those of the SSH protocol (Fig. 12).

Thus, the essence of the proposed method can be described as follows:

- computing a temporary key for the first user from the first user's key material and random cryptographic data via TrustZone for a secure mobile call;
- sending the key material to the second user;
- generating a session key from the temporary keys of the first and second users to encrypt a mobile voice call between the first and second users;
- use of a short authentication string (SAS) to protect against man-in-the-middle (MitM) attacks;
- storing a hash value for past secure calls in memory;
- supplementing the cryptographic key material during the second communication session between the first user and the second user with the cryptographic key material from the first communication session.

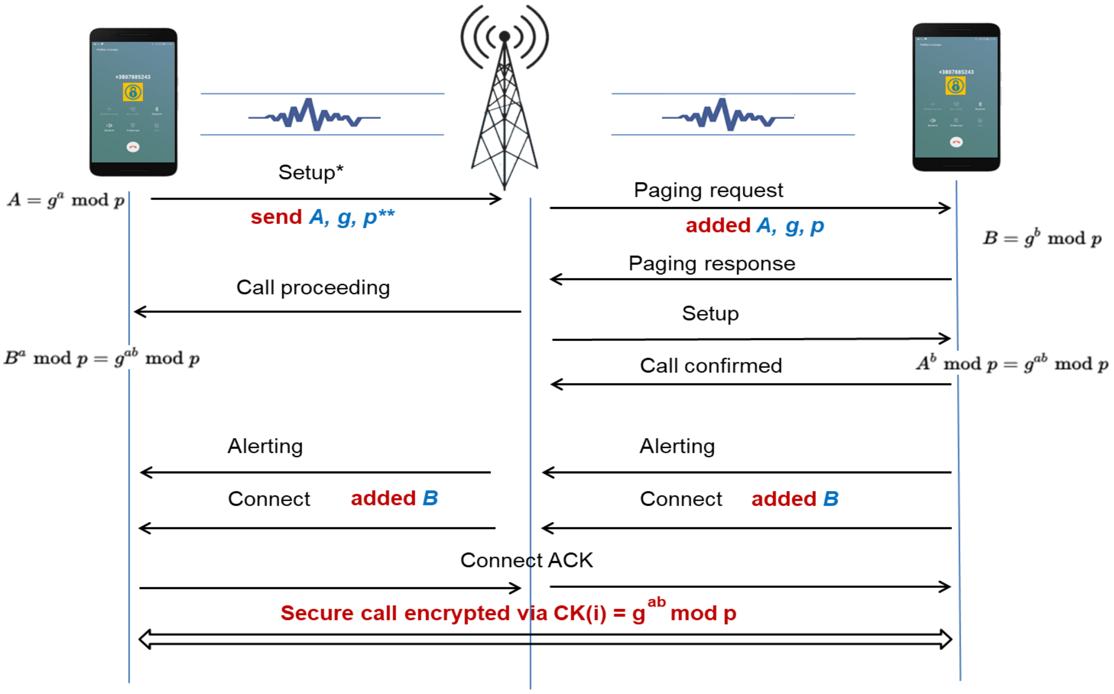


Fig. 10. Implementation of the Diffie-Hellman key exchange protocol in the messaging protocol (*current sequence, **proposed elements)

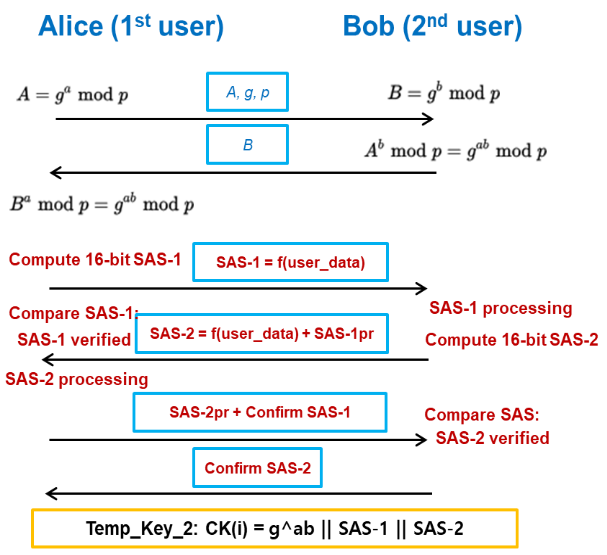


Fig. 11. Sequence of actions when calculating and using SAS

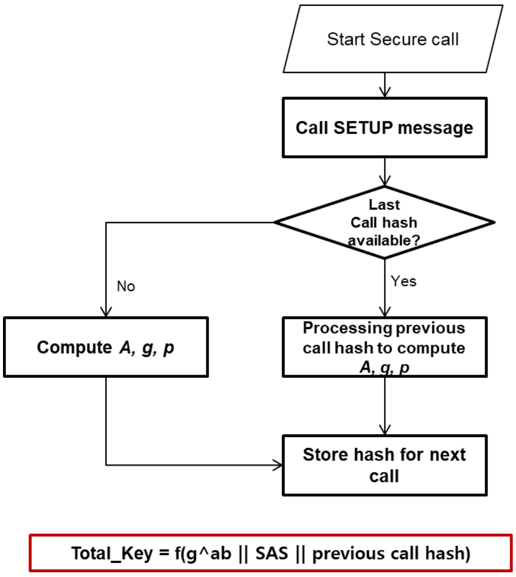

Start Secure call
Call SETUP message
Last Call hash available?
No
Yes
Compute A, g, p
Processing previous call hash to compute A, g, p
Store hash for next call
Total_Key = f(g^ab || SAS || previous call hash)

Fig. 12. Algorithm for calculating the key data

Table 2

Comparison with prior-arts

Prior-art	Call hash usage	SAS usage	Additional auth. conf.	Coordination with network	Protection against attacks from operator side
ZRTP [26]	Yes	Yes	Yes	Partially	Yes
US 2007015 7026A1 [27]	Yes	No	Yes	VoIP only	Yes
US 8462942 B2 [28]	No	No	Key from user	No	No
US 9596079 B1 [29]	No	No	No	No info	No
Proposed method	Yes	Yes	No	Yes	Yes

The secure key exchange and end-to-end encryption method was also compared with other patented solutions. The comparison criteria included the ability to protect against operator attacks, the complexity of the method's implementation (the degree of its consistency with the network), the use of a call hash, and a short authentication string for protection.

The comparison results are shown in Table 2.

3. Results and Discussion

The obtained results of the secure key exchange and end-to-end encryption method are explained by the improvements shown in Figs. 9, 11, and 12, which illustrate the key features of the proposed method. The results of the secure call answering method are explained in Figs. 2 and 7, which illustrate the elements of novelty of the proposed approach.

According to Table 1, the closest to the proposed idea are solutions [19, 20], which also allow performing mutual authentication; however, their disadvantage is the need for additional actions by the user. In addition, these solutions work only with previously known contacts and do not describe how the user's verification information will be transmitted to the other party. Unlike these solutions, the proposed method solves this problem by modifying certain fields in the messaging protocol. Another disadvantage of these solutions, compared to the proposed method, is the need for a trusted third-party. The solutions [4, 5, 9, 10, 21, 22] provide user authentication, but there is no secure protocol for exchange between the parties that would implement the transfer of authentication results and, as a result, mutual authentication of users. In contrast, the proposed solution provides an exchange protocol for this purpose by transmitting this information in the modified fields of the "SETUP" and "CONNECT ACK" messages.

This becomes possible either after being introduced into the IEEE specification or when a mobile phone vendor (e.g., Samsung) makes such changes to its models, allowing mutual user authentication as an additional feature.

Unlike the solutions presented in Table 1 [6, 7, 26, 27, 28, 29], the proposed method of secure key exchange and end-to-end encryption does not require additional key storage and protects against attacks from the mobile network operator. This becomes possible by using TrustZone and the use of the previous call hash. The advantages of the proposed solution include the fact that the secure channel is prepared at the initial stage (before the call). The proposed method does not require voice confirmation or an additional password; it is protected from a man-in-the-middle attack on the operator's side and is compatible with various mobile network technologies (2G, 3G, 4G, 5G inclusive).

Let's consider how the proposed methods cover the described disadvantages.

The method of mutual authentication of users during a call allows avoiding user spoofing on the other side and verifying the user by using various types of biometric authentication and by transmitting this information in the modified fields of the "*SETUP*" and "*CONNECT ACK*" messages.

The secure key exchange and end-to-end encryption method provides these benefits because the Diffie-Hellman protocol implements secure key exchange and a short authentication string counteracts the man-in-the-middle attack. A hash of the previous call is used to prevent spoofing of phone numbers, and symmetric encryption is used to counteract eavesdropping.

Implementation of the proposed solution becomes possible if the above fields are modified during connection establishment, which is a novelty of the approach and allows for compatibility with various mobile network technologies.

The implementation of the described approach allows increasing the levels of "confidentiality in exchange" and "integrity in exchange" services [17], which ensures an increase in the overall level of confidentiality.

The disadvantages of this study are that the proposed solutions are only submitted as patent applications and there is no testing on a real network. The lack of testing, in turn, is related to the restrictions imposed by certain authorities on the activities of network operators. This restriction determines the requirements for traffic encryption and user privacy.

Conclusion

For the first time, a method of mutual authentication of users during a call is proposed by modifying the "SETUP" and "CONNECT ACK" message fields and using various types of biometric authentication (depending on the scenario). The implementation of the method allows avoiding user substitution on the other side, providing access to services to the authorized user only, and increasing the level of service provision to confidentiality, integrity, and observability groups. The scientific novelty lies in the fact that user authentication occurs directly during the call and does not require any additional actions from the user. This is achieved using Continuous Authentication or biometric authentication based on the ear pattern/acoustic response.

The method of end-to-end encryption and key exchange in mobile networks has been improved. Its key differences are the use of the Diffie-Hellman protocol for secure key exchange and a short authentication string to counteract a man-in-the-middle attack. Adding a pre-call hash also provides anti-spoofing, while symmetric AES (256) encryption prevents eavesdropping. The key difference of the method is that to implement these features, we propose a modification of the "*SETUP*" and "*CONNECT*" messages in the traditional sequence of messages during call establishment.

The scientific novelty of the approach lies in the proposed modifications to the sequence of call messages, which allows the implementation of authentication and encryption methods and provides counteraction to peer-to-peer attacks.

Future research development. The practical implementation of the described methods and the numerical results obtained during its testing in a real network can be a further development of the study.

Contributions of authors: conceptualization, methodology – **Andrii Astrakhantsev**; formulation of tasks, analysis – **Andrii Astrakhantsev**, **Stanislav Pedan**; development of model, verification – **Andrii Astrakhantsev**, **Stanislav Pedan**; analysis of results, visualization – **Stanislav Pedan**; writing – original draft preparation – **Andrii Astrakhantsev**, writing – review and editing – **Andrii Astrakhantsev**, **Stanislav Pedan**.

Conflict of Interest

The authors declare that they have no conflict of interest in relation to this research, whether financial, personal, authorship or otherwise, that could affect the research and its results presented in this paper.

Financing

This study was conducted without any financial support.

Data Availability

Data will be made available upon reasonable request.

Use of Artificial Intelligence

The authors confirm that they did not use artificial intelligence methods while creating the presented work.

All the authors have read and agreed to the published version of this manuscript.

References

1. *Truecaller. Truecaller insights 2021. U.S. spam & scam report.* Available at: https://www.truecaller.com/blog/insights/us-spam-scam-report-21 (accessed 12.03.2024).

2. Leonhardt, M. *Americans lost $29.8 billion to phone scams alone over the past year.* Available at: https://www.cnbc.com/2021/06/29/americans-lost-billions-of-dollars-to-phone-scams-over-the-past-year.html (accessed 12.03.2024).

3. Zadereyko, O., Trofymenko, O., Prokop, Y., Loginova, N., Dyka, A., & Kukharenko. S. Research of potential data leaks in information and communication systems. *Radioelectronic and computer systems*, 2022, no. 4, pp. 64-84. DOI: 10.32620/reks.2022.4.05.

4. Perdana, N. J., Herwindiati, D. E., & Sarmin, N. H. Voice Recognition System for User Authentication Using Gaussian Mixture Model. *International Conference on Artificial Intelligence in Engineering and Technology (IICAIET)*, 2022, Malaysia, IEEE, pp. 1-5. DOI: 10.1109/IICAIET55139.2022.9936856.

5. Lee, M.-K., Kim, J. B., & Song, J. E. Smartphone user authentication using audio channels. *Proceedings of the 2012 International Conference on Consumer Electronics (ICCE)*, 2012, USA, IEEE, pp. 735-736. DOI: 10.1109/ICCE.2012.6162060.

6. Shaofeng, L., Chaoping, G., Lin, N., Wanli, K., & Minjiao, Z. The Research of Encryption Algorithm for Voice Communication of Mobile Station. *Proceedings of the 2015 International Conference on Intelligent Transportation, Big Data and Smart City*, 2015, Vietnam, pp. 898-901. DOI: 10.1109/ICITBS.2015.228.

7. Rouaf, M. T., & Yousif, A. Performance Evaluation of Encryption Algorithms in Mobile Devices. *Proceedings of the 2020 International Conference on Computer, Control, Electrical, and Electronics Engineering (ICCCEEE)*, 2021, Sudan, pp. 1-5. DOI: 10.1109/ICCCEEE49695.2021.9429673.

8. Eltengy, A. H. Encryption Of Voice Calls Using CryptoBin Algorithm. *Proceedings of 2021 International Telecommunications Conference (ITC-Egypt)*, 2021, Alexandria, Egypt, pp. 1-5. DOI: 10.1109/ITC-Egypt52936.2021.9513963.

9. Irvan, M., Nakata, T., & Yamaguchi, R. S. User authentication based on smartphone application usage patterns through learning classifier systems. *Proceedings of 2020 International Conference on Big Data (Big Data)*, 2020, Atlanta, GA, USA, IEEE, pp. 4462-4466. DOI: 10.1109/BigData50022.2020.9378172.

10. Alatawi, M., & Saxena, N. SoK: An Analysis of End-to-End Encryption and Authentication Ceremonies in Secure Messaging Systems. *WiSec 2023 - Proceedings of the 16th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, 2023, pp. 187–201. DOI: 10.1145/3558482.3581773.

11. Pevnev, V., & Kharchenko, V. Cyber security of wireless smart systems: channels of intrusions and radio frequency vulnerabilities. *Radioelectronic and computer systems*, 2020, no. 4, pp. 79-92. DOI: 10.32620/reks.2020.4.07.

12. Li, J., Shi, Y., Chen, J., Huang, Q., Ye, M., & Guo, W. Flexible Self-Powered Low-Decibel Voice Recognition Mask. *Sensors*, 2024, vol. 24, no. 10, article no. 3007. DOI: 10.3390/s24103007.

13. Hao, Z., Peng, J., Dang, X., Yan, H., & Wang, R. mmSafe: A Voice Security Verification System Based on Millimeter-Wave Radar. *Sensors*, 2022, vol. 22, no. 23, article no. 9309. DOI: 10.3390/s22239309.

14. Mo, L., Zhang, L., Sun, X., & Zhou, Z. Unlock Happy Interactions: Voice Assistants Enable Autonomy and Timeliness. *J. Theor. Appl. Electron. Commer. Res*, 2024, vol. 19, no. 2, pp. 1013-1033. DOI: 10.3390/jtaer19020053.

15. Kilinc, H. H., & Yanik, T. A Survey of SIP Authentication and Key Agreement Schemes. *IEEE Communications Surveys & Tutorials*, 2024, vol. 16, no. 2, pp. 1005-1023. DOI: 10.1109/SURV.2013.091513.00050.

16. James, T. Yu. An Analysis of Applying STIR/SHAKEN to Prevent Robocalls. *Advances in Security, Networks, and Internet of Things*, 2021, pp. 277-290. DOI: 10.1007/978-3-030-71017-0_20.

17. *ND TZI 2.5-004-99. Kryteriyi otsinky zakhyshchenosti informatsiyi v komp'yuternykh systemakh vid nesanktsionovanoho dostupa*. [State standard 2.5-004-99 criteria for assessing the security of information in computer systems against unauthorized access]. Kyiv, 1999. 60 p. Available at: https://tzi.com.ua/downloads/2.5-004-99.pdf (accessed 12.03.2024).

18. Sim, J. Y., Noh, H. W., Goo, W., Kim, N., Chae S.-H., & Ahn, C.-G. Identity Recognition Based on Bioacoustics of Human Body. *IEEE Transactions on Cybernetics*, 2021, vol. 51, no. 5, pp. 2761-2772. DOI: 10.1109/TCYB.2019.2941281.

19. Kurapati, S., Mohan, R., Sadhasivam, K., & Tyagi, S. System, method and apparatus for authenticating calls. US Patent, no. US9197746B2,

2009. Available at: https://patents.google.com/patent/US9197746B2/en (accessed 12.03.2024).

20. Zhang, G., Rong, W., Zhou, K., Wang, D., & Xu, Y. Incoming call answering method and mobile terminal. CN Patent, no. CN105187672A, 2015. Available at: https://patents.google.com/patent/CN105187672A/en (accessed 12.03.2024).

21. Dolan, R. A., Hofstatter, D. F., & Kirchhoff, L. Methods and apparatus for providing expanded telecommunications service. US Patent, no. US8594287B2, 2010. Available at: https://patents.google.com/patent/US8594287B2/en (accessed 12.03.2024).

22. Mukund, S. K. Headset for Acoustic Authentication of a User. US Patent, no. US20200184057A1, 2020. Available at: https://patents.google.com/patent/US20200184057A1/en (accessed 12.03.2024).

23. *3GPP TS 33.102 version 11.5.1 Release 11. Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); 3G security; Security architecture*. 2013. 77 p. Available at: https://www.etsi.org/deliver/etsi_ts/133100_133199/133102/11.05.01_60/ts_133102v110501p.pdf (accessed 12.03.2024).

24. Khalfaoui, S., Leneutre, J., Villard, A., Ma, J., & Urien, P. Security Analysis of Out-of-Band Device Pairing Protocols: A Survey. *Wireless Communications and Mobile Computing*, 2021, pp. 1-30. DOI: 10.1155/2021/8887472.

25. Miers, I., & Green, M. Short Authentication Strings for TLS, 2014. 6 p. Available at: https://tools.ietf.org/html/draft-miers-tls-sas-00 (accessed 12.03.2024).

26. Bresciani, R., & Butterfield, A. ProVerif Analysis of the ZRTP Protocol. *International Journal for Infonomics (IJI)*, 2010, vol. 3, iss. 3, pp. 306-313. DOI: 10.20533/iji.1742.4712.2010.0033 (accessed 12.03.2024).

27. Zimmermann, P. R. *Method and system for key management in voice over internet protocol*. US Patent, no. US7730309B2, 2006. Available at: https://patents.google.com/patent/US7730309B2/en (accessed 12.03.2024).

28. Berggren, D. E., & Belczyk, S. E. *Method and system for securing packetized voice transmissions*. US Patent, no. US8462942B2, 2009. Available at: https://patents.google.com/patent/US8462942B2/en (accessed 12.03.2024).

29. Kasabwala, D. R., & Leavy, T. M. *Secure telecommunications*. US Patent, no. US9596079B1, 2016. Available at: https://patents.google.com/patent/US9596079B1/en (accessed 12.03.2024).

Received 13.03.2024, Accepted 15.04.2024

ПІДВИЩЕННЯ ЗАХИЩЕНОСТІ КОРИСТУВАЧІВ ПІД ЧАС ДЗВІНКА

А. А. Астраханцев, С. І. Педан

Розвиток мобільних мереж призвів до появи нових загроз і нових методів реалізації вже існуючих. Фішингові атаки, включаючи роботизовані автодзвінки наносять рекордну шкоду як окремим користувачам так і великим корпораціям. При цьому, існуючі методи протидії не можуть забезпечити захист від таких атак, оскільки більшість існуючих рішень сконцентровані на автентифікації пристрою, при цьому автентифікація користувача під час відповіді на дзвінок не відбувається. Ще однією проблемою мобільних мереж є те, що немає шифрування точка-точка, тобто мова шифрується лише на відрізку від абонента до базової станції. **Предметом** вивчення в статті є процеси забезпечення захищеності користувача під час дзвінка. **Метою** є розробка моделі взаємної автентифікації користувачів та наскрізного шифрування даних в мобільній мережі під час дзвінка. **Завданнями** є захист користувача від його підміни та вішингу, пропозиція методу захисту шляхом впровадження взаємної автентифікації користувачів під час дзвінка без зберігання конфіденційної інформації на боці «довіреної третьої сторони». Для недопущення перехоплення розмов по мобільній мережі з боку оператора, як через мережу з комутацією каналів так і пакетну мережу, запропонувати метод безпечного обміну ключами і наскрізного шифрування під час дзвінка по мобільній мережі. Використовуваними **методами** є: математичні методи моделювання, онтологічний підхід, моделі багатокритеріальної оптимізації. Отримані такі **результати**. Запропонована алгоритм взаємної автентифікації користувачів шляхом впровадження біометричних методів автентифікації і модифікації послідовності повідомлень під час дзвінка. Прийом дзвінка унеможливлюється до проходження автентифікації користувача, яка відбувається без додаткових дій з боку користувача (запропонована біометрична по рисунку вуха та кісткової провідності). Для інформування протилежної сторони про результат верифікації користувача використовуються модифіковані повідомлення SETUP, CONNECT ACK. Це унеможливлює підміну користувача, «маскарад» під час дзвінка та рободзвінки. Запропоновано поєднання асиметричного шифрування, короткого автентифікаційного рядка і хешів попередніх дзвінків для підвищення конфіденційності, цілісності і протидії атакам «зловмисника посередині». **Висновки.** Наукова новизна отриманих результатів полягає в інтеграції наведених методів в послідовність повідомлень дзвінка, що дозволяє реалізувати методи взаємної автентифікації, наскрізного шифрування і забезпечити протидію ряду атак. Запропоновані методи можуть бути реалізовані у програмному забезпеченні обладнанні користувача.

Ключові слова: автентифікація користувачів під час дзвінка; шифрування голосу; мобільні мережі; протокол з’єднання; протидія атакам.

Астраханцев Андрій Анатолійович – канд. техн. наук, доц. каф. Інформаційних технологій в телекомунікаціях, Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Київ, Україна.

Педан Станіслав Ігорович – канд. техн. наук, старш. викл. каф. Інформаційних технологій в телекомунікаціях, Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Київ, Україна.

Andrii Astrakhantsev – PhD in Radio Engineering Devices and Telecommunications Equipment, Associate Professor, Associate Professor at the Department of Information Technologies in Telecommunications, National Technical University of Ukraine “Igor Sikorsky Kyiv Polytechnic Institute”, Kyiv, Ukraine,
e-mail: andrii.astrakhantsev@nure.ua, ORCID: 0000-0002-6664-3653.

Stanislav Pedan – PhD in Information Technologies, Senior Lecturer at the Department of Information Technologies in Telecommunications, National Technical University of Ukraine “Igor Sikorsky Kyiv Polytechnic Institute”, Kyiv, Ukraine,
e-mail: stas.pedan@gmail.com, ORCID: 0009-0007-8790-6962.