Formal Verification of the Authentication and Voice Communication Protocol Security on Device X Using Scyther Tool

Muhamad Al Fikri¹, Kalamullah Ramli, Dodi Sudiana
National Cyber and Crypto Agency, Universitas Indonesia
E-mail: ¹alfikri92@gmail.com

Abstract. In the current era, the ownership of strategic information and the ability to effectively manage it has become a significant advantage. Reflecting on the experience of attacks on strategic communications in Indonesia, including the tapping of the former President Susilo Bambang Yudhoyono's conversation through the cellular network and President Jokowi's official residence, Indonesia has begun paying more attention to security in this sector. Device X is one of the secret strategic communication tools used in Indonesia. The XYZ Agency initiated the use of this device. As of 2020, there have been 1,284 units of Device X widely used by the army, police officers, and other strategic agencies in Indonesia. In its 5 years of operation, the XYZ Agency has researched the algorithm security used in Device X. However, there has never been a study of the security regarding the authentication and communication protocols of this device. This research aims to make a security analysis of voice communication and authentication protocols of Device X. The research was implemented using Scyther Tool as a formal verification approach. The analysis focuses on guaranteeing the confidentiality of information and authentication with four criteria, namely, secrecy, aliveness, synchronization, and agreement. The experimental results demonstrate that the authentication and voice communication protocol of Device X satisfy the secrecy criteria for transmitted confidential information but does not satisfy the criteria of aliveness, synchronization, and agreement on several entities involved in the protocol. Thus, it can be claimed that the authentication and voice communication protocol of Device X is provably secure based on the confidentiality aspect of information but is not secure in terms of authentication.

1. Introduction
From an organizational perspective, information is regarded as a resource that can be vitally utilized for organizational growth and development [1]. In the current era, ownership of strategic information and the ability to effectively manage it remains crucial. An organization is said to be successful if it can continuously update and maintain the authenticity of information to be disseminated to all relevant divisions and integrate it with the latest technology and communication devices. This view is known as the information management perspective. Based on this perspective, dissemination is one of the most vital stages. The purpose of information dissemination is to communicate information from the information maker to the parties in need. Thus, communication is necessary for organizations to conduct their business processes.

More and more experts across disciplines affirm that communication is essential to how an organization is established and designed and to how it survives due to the dynamic, collective nature of continuous interactions among units in the organization itself [2]. Previous research has demonstrated that stakeholders have different ways of responding to these views. This is true in
particular in terms of understanding and interpreting the value of communication, which is then used as the basis for implementing a communication system to achieve organizational goals [3]. Different views in determining communication value have resulted in two general communication classifications, namely, strategic and ordinary communication [3].

Strategic communication is defined as communication that is entirely in line with the organization's communication strategy and aims to improve the organization's strategic position. Effective communication will encourage organizations to convey clear, understandable, and correct information adequately and consistently to each communicating entity. Others have defined strategic communication as communication used to formulate how the organization can achieve its primary goals and then support these efforts in specific and consistent ways for all organizational entities [4].

Considering the substance of strategic communication, which is closely related to the direction of organizational goals, generally, strategic communication is conducted at high-level management or in covert operations. Given the high value of ongoing communication, strategic communication often becomes the target of attacks. This is, of course, a threat because if the content of strategic communication is leaked, it can pose a risk to state security. Several incidents regarding attacks on strategic communications in Indonesia include the tapping of the former President Susilo Bambang Yudhoyono’s conversations through the cellular network in Cikeas in November 2013 by the Australian embassy, which installed devices at the nearest base station [5] [6]. Furthermore, there are also cases of alleged tapping of President Jokowi's official residence, as conveyed by the secretary general of the Indonesian Democratic Party of Struggle, Tjahjo Kumolo, in February 2014 [7].

In Indonesia, Device X is one of the devices used for strategic communication. Device X is used by the Indonesian National Army (TNI), the Indonesian National Police (POLRI), and strategic civilian agencies. The XYZ Agency defines device X as classified tactical communication equipment provided by the XYZ Agency. The device's designation is set according to request or analysis of the need for cybersecurity in government agencies or in local governments [8]. Device X by the XYZ agency has been used since 2015 in government agencies and local governments. Although it is not the primary secret communication device, the demand for this device is relatively high. Based on data from Directorate A of the XYZ Agency, 1,284 pieces of Device X have been distributed throughout Indonesia [8].

Device X is used for strategic communication needs with confidential content. Information security usually focuses on three main aspects: confidentiality, integrity, and information availability [9] [10] [11]. To provide information security assurance, Device X applies cryptographic techniques, such as encryption and hash functions [9] [12]. Since the use of Device X is associated with strategic information with confidential content, the ability of Device X to provide information security assurance must be ensured. To determine Device X’s information security assurance, an analyst can perform security analysis. In the context of secret communication, cryptographic security analysis of communication algorithms and protocols can be used as an approach to determine whether the security features provided by Device X are as expected [13] [14].

Based on in-depth analysis, Device X, which has been distributed throughout Indonesia, has previously undergone a modification process by embedding a proprietary encryption algorithm from the XYZ Agency. The modification was made based on the results of a study conducted by the XYZ Agency regarding the security of the built-in encryption algorithm for Device X. However, there has been no review within 5 years on the operation of the communication protocol security for Device X.

![Device X's encryption mechanism.](image-url)
Cryptographic protocol security analysis usually focuses on cryptographic features used to ensure the security of both the confidentiality and integrity of the information transmitted and the non-denial and authentication criteria of the parties involved in the communication [14]. Cryptographic protocol analysis is generally conducted in two ways: direct observation and formal verification, which includes either the use or non-use of tools [15] [16]. In response to these conditions, in this current study, we are encouraged to perform a security analysis of the communication and authentication protocol of Device X to complete the security study of Device X as one of the secret strategic communication devices in Indonesia.

2. Device X

2.1. Device X Overview
Device X is a type of secret strategic communication tool used in Indonesia. It is a DMR-based handy talky. Device X is used by the Indonesian National Army (TNI), the Indonesian National Police (POLRI), and strategic civilian agencies. The XYZ agency defines device X as a classified tactical communication device. According to a request or analysis of the need for cybersecurity in government agencies or local governments [8], the devices’ designation plan was formulated. Device X by the XYZ Agency has been used in government agencies and local governments in Indonesia since 2015. Although Device X is not the primary secret communication tool, this device’s need is relatively high. It has been established that as of 2019, based on data from Directorate A in XYZ Agency, 1,284 pieces of Device X have been distributed throughout Indonesia [8].

2.2. General System Overview
Because Device X is used for confidential communication, encryption is used as a security measure. During communication, every voice message is sent in an unencrypted form to the module. Digital voice messages in each frame will be operated using the XoR function with the crypto worm and will generate encrypted voice messages. Crypto worm is an output from a computational process using an algorithm with a key and an initial vector as the input. The encryption process during the sending process (TX) is depicted in Figure 1.

As with the encryption process during the sending process, the decryption during the receiving process is also carried out in the module. In this process, every encrypted voice message is sent to the module. The decryption process is performed to obtain voice messages from the encrypted voice messages received. The decryption process is conducted by performing an XoR operation between encrypted voice messages and the crypto worm. The crypto worm used in the decryption process is the same crypto worm used in the encryption process. Close attention needs to be paid to the initial vector used at the time of this message encryption-decryption process. IV is generated when communication is established. A new 56 bits (7 Bytes) IV will be generated and transmitted every 720 ms (12 voice frames) as depicted in Figure 2.

![Figure 2. New IV generation and distribution.](image)

3. Scyther Tool

3.1. Scyther Tool Overview
The Scyther Tool is the result of Cas Cremers' research in 2006. During that time, Cas Cremers published his research related to a methodology for formal analysis and verification of a cryptographic
protocol in the form of an analysis tool known as the Scyther Tool. This tool can analyze the confidentiality (secrecy) and authentication property in a cryptographic protocol. With the Scyther Tool, the objectivity of a formal protocol verification can be guaranteed.

3.2. Security Claims on Scyther Tool

The claim event is used by the role to model the security properties in question. There are two security properties, including secrecy (confidentiality) and authentication.

1) **Secrecy**. A Secrecy claim states that certain information was not disclosed to the attacking party even though the data was communicated over an untrusted network.

2) **Authentication**. Authentication exists to ensure the existence of the communicating parties. There are three criteria for authentication, namely, aliveness, synchronization, and agreement. The authentication criteria are hierarchical in that the synchronization criteria can be met only if the aliveness criteria have been met. Furthermore, the agreement criteria will be met only if synchronization and aliveness have been met [17]. The explanation of the authentication criteria on Scyther Tool is as follows:

a) **Aliveness**: Aliveness is a form of authentication that aims to ensure that the communicating party has performed several events, which indicates that the party is ‘alive’.

b) **Synchronization**: Synchronization requires that the message has been sent or received by the communicating parties. Synchronization only reviews content and sorts the messages. This criterion implies that each entity has sent and received messages. There are two types of synchronization, namely, injective and non-injective synchronization. Non-injective synchronization ensures that the protocol is executed in the absence of an attacker, leaving the protocol vulnerable to replay attacks. Furthermore, injective synchronization prevents replay attacks, meaning the recipient can only communicate once for the same message.

c) **Agreement**: This form of authentication focuses on the data agreement exchanged between agents, which requires that the content of the message received matches the message sent as determined by the protocol.

4. Research Methodology

In this research, we utilized a literature review and experimental methods for investigation. The literature review analyzed theories and concepts related to DMR, SDR, security requirements and threats to SDR, Device X, authentication and voice communication protocols, and Scyther Tool. Sources used for the literature review in the current study included books, papers, theses, standards, official documentation, and other sources supporting this research. The experimental method was conducted by simplifying the authentication and voice communication protocol before modelling it using a Scyther Tool-appropriate programming language. After that, the model was tested and analyzed. The analysis results were used to make recommendations for the protocol weaknesses.

The research stages are illustrated in the research flow depicted in Figure 3. The explanation of each stage is as follows:

1) **Literature Review**

A literature review was conducted of theories, references, and concepts regarding DMR, SDR, security requirements and threats to SDR, Device X, authentication and voice communication protocols, and the Scyther Tool. The primary sources of reference in this literature review included the ETSI TS 102 361-1 Standard, ETSI TS 102 361-2, ETSI TS 102 361-4, and Device X documentation. The result of this process was a general description of Device X authentication and voice communication protocols.

2) **Experiment**

a) **Protocol Simplification**: The next step was protocol simplification based on the general description of Device X authentication and voice communication protocols obtained from the literature review. Simplification was made based on the research focus. The simplification results only included relevant protocol data units (PDUs) to the research...
focus. The protocol was described with the assumption that all requests sent by the device during the authentication and communication processes were received without experiencing time outs, misidentification of address, or other errors.

After protocol simplification, the next step included validation. Validation was conducted by scanning using RTL-SDR, DSR # v.1.0.0.1635, and DSD+ software. Validation aims to see whether the PDUs described in the simplification results referring to the ETSI TS 102 361 Part 1, Part 2, and Part 4 standards is true.

b) Modelling: The second experimental stage was modelling. At this stage, the simplified authentication and voice communication protocols of Device X were modelled using Scyther Tool proprietary programming language. Modelling was made by referring to the rules determined in the Scyther Tool. The model was then validated using two approaches. Component Checklist: This approach was performed using a checklist table containing information on each component in the modelling, including role, atomic term, event, and claim. Model Checking in Scyther Tool: This approach follows the modelling requirements in Scyther Tool. Checks were performed automatically by the Scyther Tool.

c) Testing: Testing was conducted by verifying the protocol security on the Scyther Tool. The verification performed was based on the assumptions included in the Scyther Tool. Testing on the Scyther Tool was performed to prove two things: the possibility of an attack pattern on the protocol and claims of the confidentiality of information and authentication of the parties involved in the communication. The confidentiality aspect was represented by secrecy criteria, whereas authentication aspects were represented by aliveness, synchronization, and agreement criteria.

d) Analysis: The current study included two analyses: the security analysis and the Scyther Tool's output analysis. The security analysis was conducted by considering the security aspects of SDR that also applied to Device X. The Scyther Tool output analysis was performed by examining possible attack patterns and ensuring that each claim was met as expected.

Figure 3. Research flow diagram.

5. System and Simplified Protocol Description
The general illustration of the existing system on Device X is depicted in Figure 4. Two devices, Mobile Station A (MSA) and Mobile Station B (MSB), were used to communicate. Prior to communication, each MSA and MSB was registered to Trunk Station Control Channel (TSCC). After the registration process was completed, communication occurred from MSA to MSB.
For each component, the MSA, MSB, and TSCC were instrumented with a security system as follows:

1) TSCC was instrumented with RC4 and maintained a database that contained information about authorized devices instrumented with each device's authentication key.

2) MSA and MSB were each instrumented with two modules, namely, the default module and the custom module. The default module was instrumented with RC4 and the respective device authentication key, which was set by the factory. Furthermore, the custom module was instrumented with a high-level encryption system used in the communication process.

Based on Figure 4, it can be seen that the device has two types of pre-installed keys: one used for authentication and one used for communication. The pre-installed key used for authentication is specified in the 56-bit long device creation process. Furthermore, the pre-installed key used for communication is determined by the user and entered into a customizable module. There are differences in security systems in the authentication process and device voice communication. The use of more complex algorithms and longer key makes the security system in the communication process more secure than the security system in the authentication process.

The protocol simplification in this research was made according to the research focus to test the security requirements of the aspects of confidentiality of information and authentication. The confidentiality of information focused on confidential information. Thus, PDUs or information that did not contain confidential information was not described. Additionally, authentication focused on the parties or entities that communicate in the protocol. In the simplified protocol, only the main communicating entities at the highest layer were described. These entities included MS or Device X and TSCC. The simplification results are depicted in Figure 5.

![Figure 4. System overview of Device X.](image)

Based on Figure 5, there are eight stages to complete the MSA and MSB authentication process on the TSCC. The necessary PDUs in the authentication process are C_RAND, C_AHOY, C_ACKU, and C_ACKD. Each PDU is a collection of information elements. The following process was used to perform device authentication:

1) MS, who will register to TSCC, sends C_RAND PDU along with CC.

2) After receiving the C_RAND PDU from the registering device, TSCC will perform an authentication process using a challenge-response mechanism that uses known information about the device by sending the C_AHOY PDU along with the CC.

3) When the registering MS receives C_AHOY PDU, the MS will calculate the response to the received challenge. When finished, the MS sends a response with C_ACKU PDU along with CC.
After receiving C_ACKU PDU, TSCC will perform calculations with the same information and algorithms, then match the results. If the information received is the same, TSCC will send C_ACKD PDU along with CC, indicating that the device registration was successful.

Figure 5. Device X’s simplified authentication and voice communication protocols.

The communication process includes some crucial pieces of information, namely, device identifier (Ida and Idb), message (M), symmetric key shared between devices A and B (K_{ab}), an Initial Vector (IV) of the voice frame. The Id is the address and destination marker of the communicating device. Messages are sound transmitted via radio waves. Symmetric key and IV are the parameters used as input for the encryption algorithm to secure the message. The following process was used to perform voice communication:

1) MSA sends a series of signals consisting of Id_a as the source address, Id_b as the destination address, \{M_1\} K_{ab} as the M_1 message which is encrypted with K_{ab}, IV_0 as the parameters used to increase the configuration aspect of the encryption result.

2) After receiving the message, MSB will send a series of signals consisting of Id_b as the source address, Id_a as the destination address, \{M_2\} K_{ab} as the M_2 message that is encrypted with K_{ab}, IV_0 as the parameters used to increase the configuration aspect of the encryption result.

To ensure that the PDU contained in the simplified protocol is correct, a simple experiment was conducted using the RTL-SDR and the DSR # v.1.0.0.1635 and DSD+ software. The tools used in this experiment were RTL-SDR (DVB-T Dongle with RTL2832U chipset), an antenna with MCX female and MCX male connectors, DSD+ software, Windows computers, and two units of Device X.

Using DSD+, researchers monitored encrypted communication between two devices, namely the X-1 and the X-2. It can be seen that based on monitoring results, the PDU Devices Identifier (Ida and Idb), Color Code (CC), and encrypted messages ([M]Kab) were captured. Although there was no information explaining the initial vector (IV), the IV-sent information was considered valid based on the information in the official documentation from Device X owned by the XYZ Agency. Based on the findings and supporting data above, the authentication and voice communication protocol of Device X resulting from the simplification was considered valid to represent the transmitted PDU.

6. Modelling and Testing
Device X’s authentication and voice communication protocols were developed in two separate models to simplify the data presentation. Even though they were manufactured separately, the entities involved in the protocol and the transmitted PDUs in the protocol still followed the configuration depicted in Figure 5.

The modelling of the authentication and voice communication protocols for Device X was performed by compiling the protocol MSC following the Scyther Tool provisions. In the authentication protocol, the two MSA and MSB entities acted as initiators in the device registration process. However, in the voice communication protocol, MSA acted as a communication initiator.
The protocol model’s validity was tested using two approaches, namely, the component checklist and model checking. Device X’s authentication protocol model was verified on Scyther Tool. As depicted in Figure 6, the model was promptly validated with the output of protocol verification based on the model checking approach. The component checklist was performed by creating a control table according to the protocol specifications. The results demonstrated that the model made with the Scyther Tool’s local programming language followed Device X’s authentication protocol specifications.

After creating the model, the next step was to test its verification. Verification was done using the Verify ➔ Verify Protocol menu. Figure 13 depicts the verification results of Device X’s authentication protocol. Of the nine claims, three were declared valid or OK, and six claims were declared as failed or FAIL. Figure 14 illustrates the verification results of Device X’s voice communication protocol. Of the 13 claims, 10 were declared valid or OK, and three claims were declared failed or FAIL.

7. Analysis
The analysis was divided into two: an analysis of the Scyther Tool output and an analysis of the relevant SDR security requirements for this research.

7.1. Scyther Tool Output Analysis
The Scyther Tool analysis included two components: the interpretation of test results and analysis of potential attack patterns in the protocol. The interpretation of the test results provides an overview of the protocol’s overall condition according to the claims made. Analysis of attack patterns demonstrates attacks that resulted in unfulfilled protocol security claims. Table I and Table II provides a summary of Device X’s authentication and voice communication verification results.

![Figure 6. Device X’s authentication protocol (a) and voice communication protocol (b) verification results.](image)

| Claim          | Confidentiality          | Authentication          |
|----------------|--------------------------|-------------------------|
| **OK**         | Role MSA: -              | Role MSA: -             |
|                | Role TSCC: -             | Role TSCC: Aliveness, Nisynch, and Niagree |
|                | Role MSB: -              | Role MSB: -             |
| **FAIL**       | Role MSA: -              | Role MSA: Aliveness, Nisynch, and Niagree |
|                | Role TSCC: -             | Role TSCC: -            |
|                | Role MSB: -              | Role MSB: Aliveness, Nisynch, and Niagree |

In Table 1, the claim is not fulfilled because there is at least one possible type of attack against the device authentication protocol based on the test results. As the initiator, each MSA and MSB experienced the same failure in fulfilling all security criteria on authentication type claims, namely,
aliveness, synchronization, and agreement. The possible attack patterns against these criteria on each device were the same as illustrated in Figure 7 (a).

The first failure was in the aliveness criteria. Referring to the definition, Device X’s authentication protocol was stated as guaranteeing the MSA/MSB entity’s aliveness if another entity communicating with MSA/MSB, namely TSCC, can be assured the existence of MSA/MSB. Many protocols failed to meet this authentication criterion despite simple attacks. As with most cases, an attacker can mirror attack by returning the message sent by entity A back to him. This is illustrated by the attack patterns that fail MSA and MSB’s aliveness criteria as depicted in Figure 7 (a).

![Figure 7. Attack scenarios that fail the aliveness-type authentication claims by role MSA in the authentication protocol (a) and in the voice communication protocol (b).](image)

The second failure was in the synchronization criteria. The aliveness criterion only requires that some events be executed by the real communication partner entity when the communication takes place without limiting the content of the messages exchanged. Synchronization has higher authentication requirements. Synchronization requires that the communication partner send all messages received and that the communication partner receive the messages sent. This condition conforms to the requirement that the actual message exchange has occurred precisely as specified by the protocol description. However, in Figure 7 (a), the attack pattern proves that there is no guarantee that the message MSA receives is actually from TSCC. In Device X’s authentication protocol, some parties can pretend to be communication partners, thereby eliminating the guarantee of the communication partner’s correctness.

The third failure was in the agreement criteria. The synchronization criteria ensure that the protocol can behave according to predefined descriptions even in an attacker’s presence. The agreement is another criterion of authentication that focuses on the agreement on exchanged between entities. The idea behind the agreement criteria is that after executing the protocol, the parties agree on certain variables' values. The agreement is defined as a criterion that requires that the message's content is following the message sent as determined by the protocol. As a result, after the protocol has been run, the variables' contents will be precise as defined by the protocol. In that sense, there is no possibility of changing the content of the message. If it happens, then it can be known. Under the Device X authentication protocol, there was no guarantee of the contents of the messages sent.

In Table 2, the claim was not fulfilled because there is at least one possible type of attack against the device authentication protocol based on the test results. As the initiator, each MSA experienced the same failure in fulfilling all security criteria on authentication type claims, namely, aliveness, synchronization, and agreement. The possible attack patterns against these criteria on each device are the same as depicted in Figure 7 (b).
Table 2. Recapitulation of device X’s voice communication protocol verification result.

| Claim | Confidentiality | Authentication |
|-------|-----------------|----------------|
| OK    | Role MSA: M1    | Role MSA: -    |
|       | Role TSCC: M1 and M2 | Role TSCC: Aliveness, Nisynch, and Niagree |
|       | Role MSB: M2    | Role MSB: Aliveness, Nisynch, and Niagree |
| FAIL  | Role MSA: -     | Role MSA: Aliveness, Nisynch, and Niagree |
|       | Role TSCC: -    | Role TSCC: -    |
|       | Role MSB: -     | Role MSB: -     |

As a communication initiator, MSA failed to fulfil all security criteria on authentication type claims. The cause of failure of Device X’s voice communication protocol resembled that of Device X’s authentication protocol failure.

The first failure was in the aliveness criteria. Device X voice communication protocol is stated to guarantee the MSA entity's aliveness if another entity communicating with MSA, namely TSCC and MSB, can be assured of the existence of MSA. The mirror attack is illustrated by the attack patterns that fail MSA's aliveness criteria as depicted in Figure 7 (b).

The second failure was in the synchronization criteria. Synchronization requires that the communication partner indeed sends all messages received on Device X's voice communication protocol and that the communication partner indeed receives the messages sent. This conforms to the requirement that the actual message exchange has occurred precisely as specified by the protocol description. However, the attack pattern in Figure 7 (b) proves that there is no guarantee that the message MSA receives is actually from the TSCC. In Device X’s authentication protocol, a party can pretend to be a communication partner, thereby eliminating the guarantee of truth from the communication partner.

The third failure was in the agreement criteria. The agreement criterion requires that the content of the message received matches the message sent as determined by the protocol. As a result, after the protocol has been run, the variables’ contents will be precisely as defined by the protocol. In that sense, there is no possibility of changing the content of the message. In Device X’s voice communication protocol, there is no guarantee for the contents of the message sent as the possibility is illustrated in Figure 7 (b). The absence of such a guarantee invalidates the agreement claim in the communication.

7.2. Security Analysis

Referring to the definition of security requirements from the International Telecommunications Union, security requirements have eight aspects of security requirements as follows:

1) Access control to resources: The system must ensure that actors are prevented from gaining access to information or resources that do not comply with their authority.

2) Robustness: The system must provide the necessary communication services following a specific service level agreement (SLA). For example, the SLA can determine the Quality of Service (QoS) or traffic capacity required. This requirement relates to the system's ability to deal with threats that aim to thwart one or more system services.

3) Protection of confidentiality: The system must provide the ability to ensure the confidentiality of data stored and communicated.

4) Protection of system integrity: The system must guarantee the integrity of the system and its components.

5) Protection of data integrity: The system must guarantee the integrity of the data stored and communicated.

6) Compliance with the regulatory framework: The system must be able to ensure compliance with existing regulations in the area where the system operates.

7) Accountability: The system must ensure that an entity cannot deny responsibility for the actions taken. In this context, accountability is used as a synonym for non-denial.
8) Identity verification: The telecommunications network must provide the ability to establish and verify the identity of any authorized user.

Following research that focuses on secrecy and authentication, the other six security aspects are not discussed. According to references from ITU and the definitions of Scyther Tool's criteria, the relevant aspects of the safety requirements are detailed in points 3, 5, and 8.

The results from testing and analyzing Scyther Tool have demonstrated that the confidentiality aspect of information has been guaranteed both for the authentication protocol and the voice communication of Device X. This aspect of confidentiality can be achieved by applying the encryption of confidential information. In the protocol description, the classified information is denoted as M1 and M2.

Nevertheless, unfortunately, data integrity and identity verification aspects are not fulfilled in several parts of the authentication and voice communication protocols of Device X. This is because the authentication and voice communication protocols of Device X have not guaranteed the following:

1) the presence (aliveness) of several entities in the protocol for its communication partners;
2) that the message received was sent by the communication partner and that the message sent was received by the communication partner;
3) and that the contents of the message received can be guaranteed its integrity.

8. Recommendations

It should be borne in mind that the protocol that is used as the object of this research is run on a radio device that has limitations in terms of hardware capacity for implementation. On the one hand, the hardware limitation is a plausible explanation for any flaws in the system. The flaw in question can be seen in terms of the system (e.g., unstandardized encryption algorithms) or the weakness of the implemented cryptographic protocols. However, from a theoretical perspective, the security aspect, which has been proven to have weaknesses, cannot be ignored. Rather than being seen as an excuse to justify using a less secure system, hardware limitations are better viewed as a challenge to create a lightweight but robust system.

Concerning the results, the weaknesses found can be overcome by using existing cryptographic techniques such as the following:

1) the use of a timestamp as a marker to guarantee the timeliness and uniqueness of a message;
2) the use of a hash function to ensure the authenticity of the message received;
3) and use of a variety of signature techniques, such as blind signatures and public-key mechanisms, to verify the identity of the entities involved in communication.

For hardware limitations, implementation can be done by implementing lightweight algorithms or schemes. In the future, if no algorithm or scheme is considered qualified, this will be an opportunity and a challenge for researchers in the information security field to develop algorithms and lightweight schemes that can better meet security criteria for the specific case.

9. Conclusion

Based on the analysis result, the following can be concluded that Device X’s authentication and voice communication protocols have fulfilled the secrecy criteria for the transmitted confidential information but has not fulfilled the criteria of aliveness, synchronization, and agreement on several entities involved in the protocol. Thus, Device X’s authentication and voice communication protocols are considered to be provably secure based on the confidentiality aspect, but not based on the authentication aspect.

10. Future Work

Future work that can be developed from this research includes the following:

1) a possible updating of the security review document for Device X according to the research results by the XYZ agency;
2) research to apply cryptographic techniques to the recommendations for improvement in this research to overcome Device X’s identified weaknesses;
3) and research that examines more deeply Device X’s vulnerability to eavesdropping and cloning.

References
[1] Eroğlu Ş and Çakmak T 2018 Information as an organizational asset: assessment of a public organization’s capabilities in Turkey Information Development 36(1) pp 58–77
[2] Cooren F, Kuhn T, Cornelissen J P and Clark T 2011 Communication, organizing and organization: an overview and introduction to the special issue Organization Studies 32(9) pp 1149–70
[3] Johansson C and Ottestig A T 2011 Communication executives in a changing world J. of Communication Management 15(2) pp 144–64
[4] Hirsch P 2000 Book reviews: corporate communication 2nd edition by Paul A. Argenti Business Communication Quarterly 63(1) pp 111–3
[5] BBCIndonesia 2013 BIN: Australia Menyadap Indonesia Sejak 2007 Retrieved on 1 June 2020 from https://www.bbc.com/indonesia/berita_indonesia/2013/11/131120_bin_sadap_australia
[6] BIN 2013 Kepala BIN: Evaluasi Sistem Keamanan Komunikasi Retrieved on 1 June 2020 from http://www.bin.go.id/nasional/detil/255/1/29/11/20%2013/kepala-bin-evaluasi-sistem-keamanankomunikasi
[7] Tempo.co 2014 4 Kasus Penyadapan Besar di Indonesia Retrieved on 1 June 2020 from https://nasional.tempo.co/read/556304/4-kasus-penyadapan-besar-di-indonesia
[8] XYZ Agency 2019 Device X Unpublished
[9] Menezes A J, van Oorschot P C and Vanstone S A 2018 Handbook of Applied Cryptography (Florida: CRC Press)
[10] Shim J 2013 The International Handbook of Computer Security (New York: Routledge)
[11] Komperda T and Boudriga N 2013 Telecommunications and network security: communications and network security Information Security Management Handbook 6th Edition ed R O’Hanley and J S Tiller (New York: Routledge) chapter 1
[12] Michael K 2012 The basics of information security: understanding the fundamentals of InfoSec in theory and practice Computers & Security 31(4) pp 634–5
[13] ISO 2916 Information Technology – Security Techniques– Cryptographic Algorithms and Security Mechanisms Conformance Testing Retrieved from https://www.sis.se/en/produkter/information-technology-office-machines/it-security/isoiec183672016/
[14] Chen Q, Zhang C and Zhang S 2008 Overview of security protocol analysis Lecture Notes in Computer Science vol 5111 pp 17–72
[15] Avalle M, Pironti A and Sisto R 2012 Formal verification of security protocol implementations: a survey Formal Aspects of Computing 26(1) pp 99–123
[16] Chadha R, Cheval V, Ciobăcă Ş and Kremer S 2016 Automated verification of equivalence properties of cryptographic protocols ACM Transactions on Computational Logic 17(4) pp 1–32
[17] Lowe G 1997 A hierarchy of authentication specifications Proc. 10th Computer Security Foundations Workshop pp 31–43