Date of publication MAR-29, 2021, date of current version MAY-19, 2020.
www.computingonline.net / computing@computingonline.net

Print ISSN 1727-6209
Online ISSN 2312-5381
DOI 10.47839/ijc.20.1.2089

Enhancing Security System of Short Message Service for Banking Transaction

I MADE SUNIA RAHARJA[1], AHMAD ASHARI[2]
[1]Jl.Batuyang, Gang PIPIT IIIa No.26, Batubulan, Sukawati, Gianyar, Bali, Indonesia (e-mail: sunia.raharja@gmail.com)
[2]Sekip Utara Kotak Pos Bls 21, Yogyakarta, Indonesia (e-mail: ashari@ugm.ac.id)

Corresponding author: I Made Sunia Raharja (e-mail: sunia.raharja@gmail.com).

ABSTRACT SMS banking still becomes a popular way to make transaction inquiry in Indonesia. The technology protocol used by the service provider is still not secure. The majority of local banks in Indonesia still use non-secure SMS protocols standard. Therefore, an SMS Banking protocol, providing information security service in the transactional message, is urgently in need. Information security can be achieved through some security mechanisms, i.e., encipherment, digital signature, data integrity, and key exchange. These mechanisms are applicable through the implementation of cryptography. SMS Banking security protocol in this research runs through two steps. The first step is the transmission of the transaction request, and the second step is the transaction process. The encipherment is conducted using 3DES symmetric cryptography. Digital signature and data integrity are conducted using ECDSA asymmetric cryptography. The key exchange is conducted using ECDH. The test result showed that the implementation of the protocol could conduct an SMS Banking service and provide protection over the PIN. In general, this protocol has fulfilled X.800 security services.

KEYWORDS security, SMS, banking, Indoneisa, encryption, cryptography.

I. INTRODUCTION

SMS banking still becomes a popular way to make transaction inquiries in a developing country like in Indonesia. SMS Banking in Indonesia is not secure enough, and only a few large banks have adopted encryption to secure SMS Banking services [1]. SMS banking is preferred because it does not require an Internet connection and is very convenient. There are still doubts to submit bank account information to the Internet. Nowadays, lots of hacker attacks are launched via the Internet (Anonymous, Ransomware, Malware, etc.). Although it provides convenience, the technology protocol used by the service provider is still not secure. Most banks in Indonesia are still using non-secure Short Message Services Protocol Standard.

Vulnerability to attacks occurred on the transmission of SMS in GSM network standards that are not voting for good security. Transferring confidential information, for example, user PIN to base stations is known vulnerable to eavesdropping. Thus, information security was required to resolve security vulnerabilities in SMS. Information security can be achieved by providing information security services. X.800 is a standard for information security services. Information security services can be achieved by implementing security mechanisms. Security mechanisms can be implemented using encryption algorithms.

In general, encryption is grouped into Symmetric Encryption and Asymmetric Encryption. Symmetric encryption is often used to conceal the contents of a data block with a certain size such as a message, file, encryption key, and password, while asymmetric encryption is more used for key management in symmetric encryption and digital signatures [17].

One of the symmetric encryption algorithms is 3DES; 3DES is an algorithm that has been recommended to become a data security standard [21]. One example of the asymmetric algorithm that can be used is the ECC algorithm. Elliptic Curve Cryptography (ECC) has the advantage of providing

the same level of security as other asymmetry algorithms (i.e., RSA) but with smaller key sizes [17].

Based on the security issues in the SMS Banking service, the purpose of this research is to develop a more secure SMS Banking protocol by implementing security mechanisms to achieve the X.800 security services standard.

The rest of the paper is organized as follows: the related works and literature review about the topics of this research are considered in Section II, which is followed by the research methodology that is used to conduct this research in Section III. Section IV focuses on protocol testing and analyzes the test result. Section V concludes the paper.

II. LITERATURE REVIEW

This section discusses related works to the topic of security for mobile communication, especially for SMS services. The subsection addresses an overview of the SMS service and a short review of SMS Banking services in Indonesia.

Security for mobile communications has become a popular research topic since the increasing use of handheld devices. Much research is done on the security of SMS communication because, until now, SMS still uses encryption technology that is vulnerable to attack.

In the beginning, the research on SMS security used symmetric algorithms. In [2], it was proposed a protocol that uses Quasigroup cryptographic for SMS security. The Quasigroup is a stream cipher based symmetric cryptography where each character in the plain text is encrypted simultaneously using different encryption transform at any given time. Applications were created using Java programming languages, J2ME, and CLDC API. SMS usage is increasingly popular, and the research domain started leading to electronic transactions. Authors in [3] made an SMS security application for M-Commerce that was intended specifically for M-Banking service. In this proposed method, the bank maintaining the confidentiality of the SMS transactions used the AES algorithm. The applications were created using .Net programming languages with the Windows Mobile platform. With the same algorithm in [4], the authors implemented the SMS encryption applications by adding the pattern lock method for user authentication and built it using Android programming languages.

Public key (asymmetric) cryptography technology, which is safer, also affects the studies of SMS security. The thesis in [5] used an asymmetric cryptographic scheme with the RSA algorithm. Applications are made in the form of SMS chat using the Microsoft Crypto API. With the same algorithm, authors in [6] implemented SMS encryption, where the encryption process consists of encrypting messages and digital signatures using the RSA algorithm. They used the Symbian programming language for the cryptographic module and Python to program the interface. With a little modification on the same algorithm author in [7] made SMS encryption system based on FPGA for implementing the RSA algorithm.

In contrast to previous research, the research in [8] proposed a digital signature scheme for SMS security using a modified ECDSA algorithm and only focused on the non-repudiation aspect. The author in [9-10] made an SMS security application for M-commerce services. The research in [9] proposed a security method using a combination of digital signatures with public-key RSA cryptography, which was modified. RSA was modified using OAEP (Optimal Asymmetric Encryption Padding) to increase security. In [10] the scheme was proposed using the NTRU algorithm for SMS security on M-commerce services. The algorithm was compared with ECC and RSA algorithms. The comparison shows the NTRU algorithm can perform encryption and decryption operations faster than ECC and RSA.

In addition to using public-key cryptographic systems, there is also research that uses a combination of symmetric and asymmetric systems such as the one carried out in [11] providing SMS security solutions by creating applications in the form of application layer protocol. The concept is to use the elliptic curve-based public key solution to form a secret key in the encryption symmetry algorithm. The symmetry algorithm used is AES. This application is applied to the M-Commerce service, especially for the M-Payment system.

A. GSM NETWORK

GSM network technology (Global System for Mobile Communication) is one of the cellular telecommunication networks that are standardized and regulated by the European Telecommunications Standards Institute (ETSI). The GSM system is built by three subsystems, namely the Mobile Station, the Base Station Subsystem and the Network subsystem. GSM systems use components called SMS centers (SMSC) to implement Short Message Service (SMS). The GSM network architecture with SMSC is shown in Fig. 1.

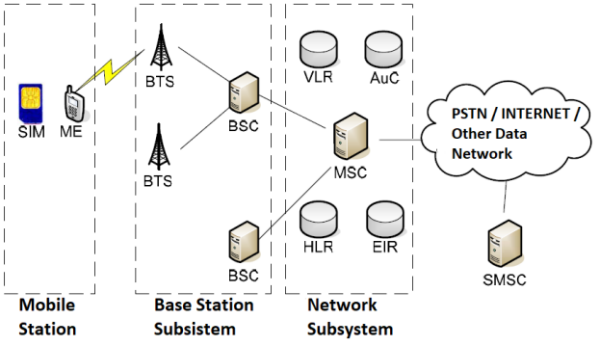


Figure 1. GSM Architecture [12]

Mobile Station (MS) subsystem is Mobile equipment (ME) along with SIM-Card. The main function of the MS subsystem is to transmit and receive sound or data from the GSM system. ME performs signal processing transmitted from BTS, while SIM-cards provide unique identification for each MS.

The Network subsystem has five components that act as the main switching on GSM systems. MSC uses customer data in the VLR along with the Base Station subsystem that

is related to each MS to manage communication between GSM customers and use external networks (such as PSTN) for other network customers. HLR is a database that permanently stores data relating to a specific set of customers, such as identification numbers, authentication parameters, special routing information, and information about VLR used. The AUC component stores information needed for communication security between system components. EIR component is a database that stores the IMEI (Intentional Mobile Equipment Identity) numbers of all MS customers [13].

B. GSM SECURITY

In the GSM network system, the unique identity of MS customers is represented by the International Mobile Subscriber Identity (IMSI) number, which is stored in the SIM. The temporary identity numbers are called Temporary Mobile Subscriber Identity (TMSI), which is used to maintain the confidentiality of IMSI. On GSM, IMSI and TMSI are stored in the VLR database. When an active MS radio signal is connected to the coverage area of a particular MSC / VLR, the IMSI is then used to create a TMSI number, which is later used more to communicate with the GSM system. TMSI is only valid in sessions that require customer verification, and it is limited to identity the signal coverage area (Location Area Identification), if the verification has been successfully carried out, the server will send another TMSI for further verification [14].

C. SHORT MESSAGE SERVICE (SMS)

SMS is a communication service in the form of messages provided by the GSM network. In order to transmit messages over the air, the SMS service network uses four important components, namely BTS, MSC, SMSC, and GMSC. GMSC is a component used by SMSC to communicate with TCP / IP networks; in principle, GMSC is an MSC that can receive short messages from SMSC. GMSC interrogates HLRs to get customer routing information and sends messages to MS customers through the relevant MSC. Fig. 2 shows the Architecture of the SMS network [15].

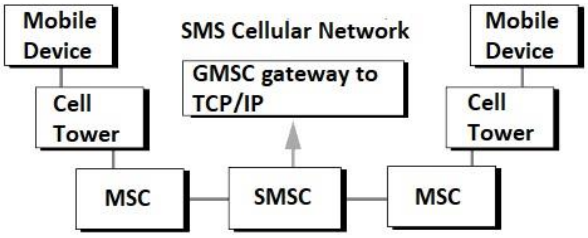


Figure 2. Architecture of SMS Network [15]

D. SMS BANKING

To be able to use the SMS Banking, the account owner must register with the wireless carrier first. The entities involved in carrying out the SMS Banking service are shown in Fig. 3.

The entity is [16]:

- Core banking application that contains account information.
- SMS Mobile banking application that is connected to the SMS network.
- Bulk SMS service provider application that sends SMS to wireless carriers.
- Wireless carriers can transmit messages to mobile phones.
- SMS Mobile Banking Customer that is used by customers to interact with banks.

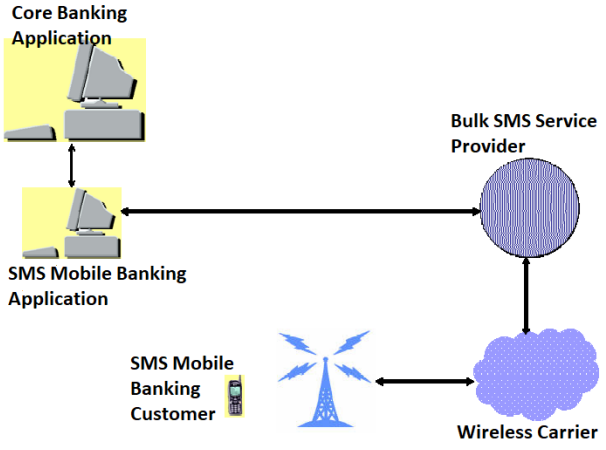


Figure 3. Architecture of SMS Banking service [16]

E. SECURITY SERVICE

The X.800 standard defines services that ensure adequate security for data transmission. X.800 defines security services as being divided into six categories [17].

a) Authentication
Authentication guarantees SMS communication between authentic clients and servers. The function of authentication is to guarantee that the recipient of the SMS is indeed receiving the message from the stated source. Clients and servers must be authentic, both of which are in accordance with what is stated. Services must ensure that SMS communication in a certain way cannot be intervened as a third party that can act as a legitimate party for the purpose of unauthorized transmission.

b) Access Control
Access control is the ability to limit and control access to protocols. Each party involved must be identified and confirmed so that access rights can be adjusted for each individual to achieve the Access Control.

c) Data Confidentiality
Confidentiality Data relates to the confidentiality of the contents of data sent via SMS. The protocol must be able to maintain the confidentiality of data sent by clients and servers. In connection with the SMS Banking, important information sent via SMS must be very difficult for unknown parties to know.

d) Data Integrity
The data sent in the protocol must be protected from modification. In the case of the SMS Banking service,

the SMS message for the transaction cannot be changed by an unauthorized party for an illegal purpose.

e) Non-repudiation
The client and server cannot deny sending SMS Banking messages. So that when the transaction SMS message is sent, the recipient can prove that the sender stated did indeed send the message. Likewise, when a transaction SMS message is received, the sender can prove the recipient who was stated to have indeed received the message.

f) Availability Service
This is the protocol's ability to maintain SMS Banking services that can be used by authorized users. In this case, the SMS Banking protocol can provide SMS services whenever the client makes a transaction via SMS Banking.

F. NETWORK SECURITY PROTOCOL

Security applied to computer networks aims to provide computer security services. A protocol combined with cryptographic algorithms is to solve a problem. Encryption algorithms are used in implementing computer security mechanisms, while protocols help provide rules, definitions, and statements for certain situations and conditions.

A protocol is a series of steps involving two or more parties and designed to complete certain tasks. A series of steps means the protocol must be run from the start (begin) to the end (finish). Each step is executed in the order, and there are no steps that can be executed if the previous step has not been completed. Involving two or more parties means that at least two parties are needed to complete the protocol. In this case, not only has one party completed a series of protocol steps, but also there is another who also completes the steps in the protocol. Completing a certain assignment means that the tasks assigned to the protocol must be completed.

Several other protocol characteristics [18]:

- Each party involved in the protocol must know the protocol, and each step that will be carried out.
- Each party involved must agree to carry out each specified step.
- The protocol must not be ambiguous; each step must be well defined. There must be no misunderstanding.
- The protocol must be resolved; there must be specific actions for each situation that might occur.

The specifications of a protocol consist of five protocol elements, namely [19]:

- Service must be provided by the protocol.
- There are assumptions about the environment in which the protocol was executed.
- There are the vocabulary messages used for protocol implementation.
- There should exist Encoding (format) for every message in the vocabulary.
- The protocol uses rules and procedures in exchanging messages.

III. RESEARCH METHOD

This section describes how research is carried out through the stages of research methods. The stages of conducting this research are Data Analysis, Protocol Design, and Protocol Implementation.

A. DATA ANALYSIS

The protocol in this research uses two components, namely Client/Mobile-phone and Server/Bank-server. Security protocols in this research are expected to meet the X.800 security services consisting of authentication, control access, data confidentiality, integrity, non-repudiation, and availability services. The protocol should implement some mechanism to meet the security services. The mechanism is encipherment, which is implemented using the 3DES algorithm, digital signature, and data integrity mechanism using the ECDSA algorithm. And the key exchange mechanism, which is implemented using the ECDH algorithm.

The protocol on the mobile-phone side has the functional specification that processes the transaction request message, the digital signatures process for the security of the transaction message, and the encryption process for approval transaction message. Meanwhile the bank server side has the functional specifications, that is, transaction request handling process, digital signatures for the security of the transaction message, decryption, and approval transaction message handling process.

The data required by the protocol include savings account data, SMS Banking account data, and transaction data.

B. SECURITY PROTOCOL DESIGN

The design of proposed security protocols for SMS Banking is shown in Fig. 4.

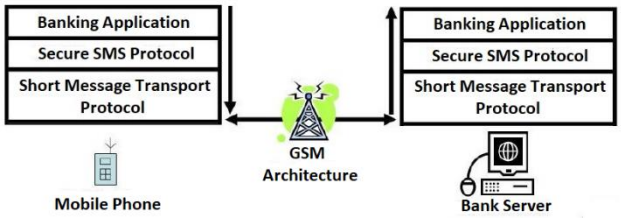


Figure 4. Design of security protocol for SMS Banking

The focus of this research is to design the banking application layer and Secure SMS Protocol layer, which resides either on the Mobile-phone side and the Server bank side.

- The Banking Application layer serves to process the input data from the user transformed into a secure transaction message. The banking application layer resides either on the Mobile-phone side and server bank side.
- The Secure SMS Protocol layer shows the place where the security mechanism is implemented for sending the transaction message.

- The Short Message Transport Protocol is the standard SMS service layer for sending SMS via GSM cellular networks. This layer resides either on the Mobile-phone side and server bank side.

The proposed Secure SMS Protocol consists of two stages, the first stage is the request transaction, and the next stage is the process transaction. Following is the notation used to explain the protocol design:

Table 1. Notation for the protocol design

Notation	Description
S	Server/Bank-server
C	Client/Mobile-phone
PIN	PIN code from user
Req	Request transaction data
Konf	Reply from Bank-server about the transaction confirmation
Hasil	Reply from Bank-server about the transaction result
SS_{priv}	A digital signature using Bank-server private key
SC_{priv}	A digital signature using Mobile-phone private key
S_{ECDH}	Server/Bank-server ECDH value
C_{ECDH}	Client/Mobile-phone ECDH value

The protocol P consists of two, namely Request Transaction (RT) and Process Transaction (PT):

$$P = RT + PT. \quad (1)$$

More detail for RT stage:

M1 : C→S: [SCpriv(CECDH || Req)] : Request transaction message

M2 : S→C: [SSpriv(SECDH || Konf)] : Transaction confirmation message

More detail for PT stage:

M3 : C→S: [SCpriv(EKs(PIN))] : Request transaction message

M4 : S→C: [SSpriv(Hasil)] : Transaction confirmation message

The two stages of the protocol must be run in order. The PT stage cannot be run if it does not run the RT stage, the stages for each message delivery.

M	Message delivery detail
M1	C compiles a transaction request message consisting of the ECDH public key ECDH(C_{ECDH}) and the transaction request data (Req). This message is then signed using the private key of the Mobile-phone (SC_{priv}(C_{ECDH} || Req)). The signed message is then sent to the Bank-server (C→S: [SC_{priv}(C_{ECDH} || Req)]).
M2	S receives the M1 message then checks the digital signature using the public key of the Mobile-phone stored on the Bank-server. If invalid, the request message will be deleted immediately, whereas if valid, the request message will be processed. The request message is processed so that it can be used for the next part of the protocol. The Bank-server generates a secret key (K_s) using C_{ECDH} from M1 and the private value of ECDH owned by the Bank-server, this secret key will be used for the next part of the protocol. Transaction request messages will be returned with a transaction confirmation message to request approval of the transaction process to the customer. Together with the S_{ECDH} value, the transaction confirmation is signed Ss_{priv}(SS_{priv}(S_{ECDH} || Konf)) and then sent to the client (S→C: [SS_{priv}(S_{ECDH} || Konf)]).
M3	C receives M2 messages and checks the message signatures using the Bank-server public key stored on the Mobile-phone. If the signature is invalid, the message cannot be used to approve the transaction, whereas if valid, the message will be processed by means of; Mobile-phone takes S_{ECDH} value, and then together with the private value of ECDH owned by the Mobile-phones, a secret key was generated (K_s). This will be used to encrypt(EK_s) the transaction confirmation message. The transaction confirmation message is approved by the client by sending a transaction approval message containing a PIN code that is encrypted using the secret key (Ek_s(PIN)). An encrypted transaction approval message is signed again by Mobile-phone and sent back to the Bank-server (C→S: [SC_{priv}(Ek_s(PIN))]).
M4	S receives the M3 transaction approval message and checks the digital signature using the Mobile-phone public key. If it is invalid, the message will be deleted, while the valid transaction approval message is decrypted using the secret key (Ks) generated at M2. Decrypted messages are used to process transactions. The results of the transaction process will be signed by the Bank-server (SSpriv(Hasil)) and sent to the Mobile-phone as a transaction message result(S→C: [SSpriv(Hasil)]).

C. SECURITY PROTOCOL IMPLEMENTATION

The client / Mobile-phone side is implemented using Android and SQLite for the database, while Server / Bank-side is implemented on a PC server that is connected to a cellular network using a GSM modem.

IV. RESULT AND DISCUSSION

This section focuses on the security testing of proposed protocols and the analysis of the results. The testing scenario is in the form of a Man-in-the-middle attack where the attacker is between Client and Server Side. The condition is that an attacker can tap into the cellular network that is used to send transaction messages.

Analysis of the results of security testing is done by observing whether the protocol meets X.800 security standards and comparative analysis with existing conditions that do not yet have a security mechanism.

A. PROTOCOL SECURITY TEST

Protocol security test use attack models defined by Emanuel [20], Attacks on SMS Banking can occur with the attempt shown in Fig. 5.

The attack is made by tapping on the transmission of SMS among the Mobile-phone and the Bank-server.

The purpose of the attack on the protocol is to get an SMS Banking PIN code. The process of attack to get the PIN is shown by the attack tree model for the protocol in Fig. 6.

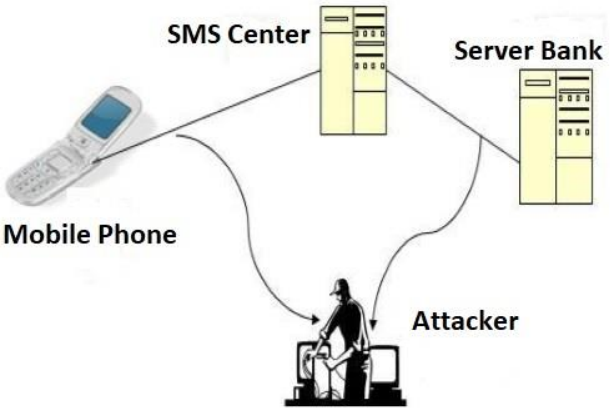
The attack tree shows that an attacker can read all the messages transmitted between the mobile phone and the server.

After reading the transaction request message, the attacker can also falsify the transaction request message. In this attack, the attacker will forge a transaction confirming message so that the attacker can forge a secret key used for encrypting user PIN.

This fake secret key is used to decrypt the PIN ciphertext existing in the transaction approval message and get the user PIN code. This attack cannot be performed because the attacker does not have a private key ECDSA that is used for digital signatures by the server. False transaction

confirmation messages could not be validated by the Mobile-phone, so the transaction confirmation messages cannot be processed.

Attacks originating from the SMS server center has the resources to hack into bank server in order to get the server ECDSA private key that can falsify a transaction confirmation messages. The attacks on the bank server are not possible because the bank has excellent security technology.



existing

est

Figure 5. Attack on the SMS Banking message transmission [20]

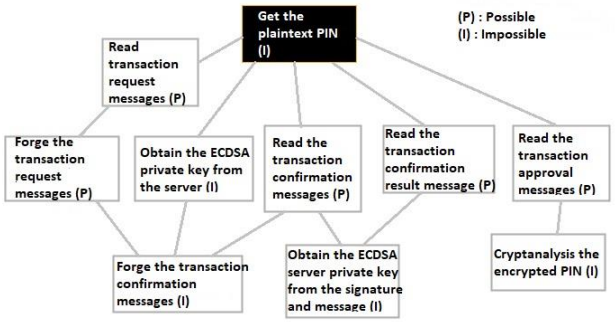


Figure 6. Attack tree to the proposed protocol to get the PIN code

Another way to get the customer's PIN code is to read the agreement message for the transaction sent by the user, that contains the ciphertext PIN and do the cryptanalysis of the ciphertext. This protocol uses the 3DES / TDEA encryption algorithm, which is an encryption algorithm recommended by NIST [21], according to Hamdan and Zaidan [22], the time needed to carry out a brute force attack is 800 days, with a speed of 50 million keys per second. Besides that, the secret key made in this protocol is a one-time password, which only applies to one transaction.

All attacks on the leaf node are not possible, so it is known that it is not possible to obtain a user's PIN code through several defined protocol attacks.

If we compared to the existing SMS Banking service, the attack tree is shown in Fig. 7.

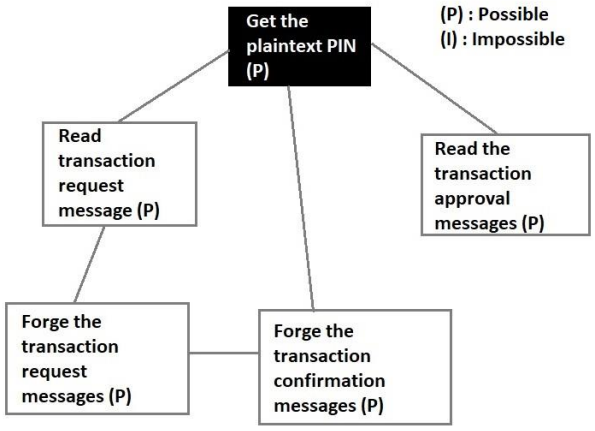


Figure 7. Attack tree to the existing SMS banking service to get the PIN code

Because the existing SMS banking service does not have a security mechanism, the attacker can easily read the text message sent. Attackers can get a user PIN in two ways.

The first way, the attacker acts as a fake Bank-server. The attacker intercepts and forge the transaction request messages, forging the transaction messages, in this case, it can be in the form of changing the contents of transaction request messages (e.g., changing the destination of the transaction to the attacker's bank account), this transaction request message is sent to the actual Bank-server, so the Bank server will send a transaction confirmation message.

The transaction confirmation message sent by the Bank-server is then intercepted and forged again by the attacker (changed to the correct transaction data) so that the user will not notice anything wrong with the transaction. In order for a transaction to be processed, the user must send a transaction approval message in the form of a PIN. So that the PIN sent can be intercepted and read by the attacker and processing wrong transactions (i.e., the money is sent to the attacker's bank account).

The second way is that the attacker can only tap transaction approval messages and read the PIN directly.

All attacks on the leaf node are possible, so it is known that it is possible to obtain a user's PIN code through several defined attacks.

B. RESULTS ANALYSIS

From the results of security testing for the protocol, it is known that the protocol has been built to protect the confidentiality of the PIN from several attacks. From the result of the security testing also can be seen that the protocol is compliant with X.800 data security services, namely:

a. Authentication
The combined use of SMS Banking PIN and phone numbers provide customer authentication because Reonly customers who know the PIN code.
b. Access Control
The servers can be identified through the digital signature, and the mobile-phone can be identified based on a phone number and a digital signature. Parties who only have a valid signature have access to the protocol.
c. Data Confidentiality
The very important and confidential data is the customer's PIN, encryption PIN is already using a strong encryption algorithm with a secret key which is a one-time password that provides more strong confidentiality.
d. Data Integrity
The digital signature mechanism implements the hash function that produces a message digest; if the message is changed, then it will produce a different digest value that becomes invalid signatures.
e. Non-repudiation
The protocol is built using SMS Banking PIN to execute transactions, PIN known only to the customer so that the customer cannot deny approving the transaction.
f. Availability Service
SMS Banking service availability can be plagued by a denial-of-service (DoS) attack. DoS attacks can be prevented by utilizing the structure of the message and the digital signature. Messages with a version that does not fit and messages with invalid signatures will be deleted by the server, thus will not burden further computing.

The existing SMS Banking service only meets the Authentication aspect, where only a combination of the PIN with phone number is used to process transactions. It is assumed that the combination of a confidential PIN and a unique phone number is secure enough. But, the existing SMS Banking service does not meet the other X.800 security aspects.

V. CONCLUSION

A security protocol for SMS Banking can be created with transaction SMS delivery mechanism in two stages where this is done by sending a request transaction first, and then the next stage sends the transaction approval to process the transaction. Additionally, a transactional message delivery mechanism can be combined with the security mechanisms; namely encipherment mechanism can be done through the symmetric encryption process using 3DES algorithms. The secret key used for encryption is obtained through the key exchange mechanism using ECDH algorithm, and implement the digital signature and data integrity mechanisms using ECDSA. Protocol security testing shows that the proposed security protocol can protect the confidentiality of a PIN code and meet X.800 security standards.

References

[1] CISSReC, *Cegah Pencurian Dana Nasabah, Perbankan Harus Perkuat Keamanan SMS Banking*, 2015. [Online]. Available at: http://bit.ly/2XiRz53. (in Indonesian)
[2] M. Hassinen, S. Markovski, *Secure SMS Messaging using Quasigroup Encryption and Java SMS API*, in P. Kilpeläinen & N. Päivinen, ed., 'SPLST,' University of Kuopio, Department of Computer Science, 2003, pp. 187.
[3] V. Manoj, Bramhe, "SMS based secure mobile banking," *International Journal of Engineering and Technology*, vol. 3, pp. 472–479, 2011.
[4] R. Rayarikar, S. Upadhyay, P. Pimpale, "SMS encryption using AES algorithm on Android," *Foundation of Computer Science*, vol. 50, no. 9, pp. 12-17, 2012. https://doi.org/10.5120/7909-1038.
[5] Y. L. Ng, *Short Message Service (SMS) Security Solution for Mobile Devices*, Nanyang Technological University, Singapore, pp. 1-4, 2006.
[6] D. Lisoněk, M. Drahanský, "SMS encryption for mobile communication," *Proceedings of the International Conference on Security Technology*, 2008, pp. 198-201. https://doi.org/10.1109/SecTech.2008.48.
[7] N. Qi, J. Pan, Q. Ding, "The implementation of FPGA-based RSA public-key algorithm and its application in a mobile-phone SMS encryption system," *Proceedings of the International Conference on Instrumentation, Measurement, Computer, Communication and Control*, 2011, pp.700-703. https://doi.org/10.1109/IMCCC.2011.178.
[8] N. Saxena, N.S. Chaudhari, "A secure digital signature approach for SMS security," *International Journal of Computer Aplication (IJCA)*, vol. 1, pp. 98–102, 2011.
[9] N. Saxena, A. Payal, "Enhancing security system of short message service for M-Commerce in GSM," *International Journal of Computer Science & Engineering Technology (IJCSET)*, vol. 2, pp. 126–133, 2011.
[10] A.K Nanda, L.K. Awasthi, *SMS Security Using NTRU Cryptosystem for M-Commerce*, Research Scholar, CSE Department National Institute of Technology, 2012, 17 p.
[11] M. Toorani, A.A. Beheshti, "SSMS – A secure SMS messaging protocol for the M-Payment systems," *Proceedings of the 13th IEEE Symposium on Computers And Communications* (ISCC'08), 2008, pp. 700–705. https://doi.org/10.1109/ISCC.2008.4625610.
[12] Y.L. Ng, *Short Message Service (SMS) Security Solution for Mobile Devices*, Nanyang Technological University, Singapore, 2006, pp. 5-6.
[13] A. Mehrotra, *GSM System Engineering*, Artech House, London, 1997, 472 p.
[14] M.K. Chong, *Security of Mobile Banking: Secure SMS Banking*, Data Network Architectures Group Department of Computer Science University of Cape Town, Private Bag, Rondebosch 7701, South Africa, 2006, 69 p.
[15] T. Clements, *SMS – Short but Sweet*, 2003, [online]. Available at: http://tinyurl.com/bvk6qoh.
[16] K. Kohli, *SMS in Banking Mitigating the Risks*, Paladion Networks, Paladion Knowledge Series, 2004, 9 p.
[17] W. Stallings, *Cryptography and Network Security Principles And Practice Fifth Edition*, Prentice Hall, New York, 2011, 752 p.
[18] B. Schneier, *Applied Cryptography Protocols, Algorithms, and Source Code in C, 2nd ed*, John Wiley & Sons, inc., New York, NY, USA, 1995, 758 p.
[19] G.J. Holzmann, *Design and Validation of Computer Protocols*, Prentice, Hall Software Series, Upper Saddle River, NJ, USA, 1991, 512 p.
[20] A. Emmanuel, *Mobile Banking in Developing Countries: Secure Framework for Delivery of SMS-banking Services*, The Netherlands. Security of Systems, Radboud University Nijmegen, 2007, 53 p.
[21] W.C. Barker, *Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher*, National Institute of Standards and Technology, Gaithersburg, 2012, MD 20899-8, 35 p. https://doi.org/10.6028/NIST.SP.800-67r1.
[22] O.A. Hamdan, B.B. Zaidan, A.J. Hamid, M. Shabbir, Y. Al-Nabhani, "New comparative study between DES, 3DE, and AES within nine factors," *Journal of Computing*, vol. 2, issue 3, pp. 152-157, 2010.

I MADE SUNIA RAHARJA, *S. Kom., M. Kom. The author took a Bachelor of Computer Science from Udayana University, Bali, Indonesia and the Master's degree in Computer Science from Gajahmada University, Yogyakarta, Indonesia, the research for his thesis is the study of security protocol. He was a lecturer in STIKOM Bali and STIKI Indonesia from 2014 until 2015, teaching Computer Networking and Data Communication, now he works as a lecturer at Information Technology Udayana University teaching programming and soft computing. Research interest is on network security, security algorithm cryptography, AI, and Smart Technology.*

Dr. techn. AHMAD ASHARI, *M. Kom. The author took Bachelor of Physics from Gajahmada University, Yogyakarta, Indonesia and a Master's degree in Computer Science from the University of Indonesia, Indonesia, the main field of his research thesis is the network and computer architecture. He took Doctoral degree on the informatics field at Vienna University of Technology, in Austria. He is a lecturer in Gajahmada University from 1989 until now, he teaches Computer Networking and Data Communication, Internet Network and World Wide Web, Distributed System and Parallel Computation.*