March - April 2020
ISSN: 0193-4120 Page No. 4557 - 4564

User Authentication Scheme offering User Anonymity and Untraceability based on Symmetric Key Cryptographic Algorithm

Jae-young Lee
Assistant Professor,
Department of Liberal Education, Semyung University 65, Semyeong-ro, Jecheon-si, Chungcheongbuk-do, 27136, Republic of Korea, klitie@semyung.ac.kr

Article Info
Volume 83
Page Number: 4557 - 4564
Publication Issue:
March - April 2020

Abstract

Establishment and focus: As network technology has developed, provision of necessary services via network connections has become available at any time and place. Different forms of security threats in the new network environment, unlike the ones in the previous, has emerged and new security techniques is required to respond to the threats. In this thesis, to secure the user anonymity of users transmitting-receiving messages, unilateral hash function is applied to user information so that the information can maintain confidentiality of its login message during transmission. Attackers cannot identify any transmitter-receiver information from the messages with confidentiality maintained. Hence, untraceability is ensured. By using time stamps for session key generation, forward confidentiality is retained. If forward confidentiality is retained, attacks cannot speculate future session keys despite of their acquisitions of sessions keys used in prior.

System: In the user authentication scheme proposed in the thesis, first, users and servers can perform mutual authentication. If users create login messages using their registered information in server and send the messages to the server, the server compares the login message contents and registered user data to identify an authorized user. The server, authenticated a user who received a login message, uses the login message contents and user information stored for generation and transfer of a message including required information for user authentication. The users who received the messages from the server can identify whether the message receiver is an authorized server by referring to the message contents and self-generated data. Second, user anonymity and untraceability are provided. User information in a message needed for login and authentication is included as a figure with a unilateral hash function and the message is transmitted after being encrypted through symmetric-key cryptographic Algorithm. Accordingly, user anonymity is secured as attackers cannot identify any of user information through message tapping, thus untraceability of a message is maintained as the attackers cannot identify any of message transmitters and receivers. Third, users login into smartcards by using ID, password and biometrics. Attackers who captured a smartcard cannot obtain ID, password and biometrics, and cannot login into the smartcard without the data. Fourth, forward confidentiality is maintained. Attackers who acquired previous session keys cannot presume any future session keys to be generated. This thesis proposes a symmetric key cryptographic authentication scheme which is more efficient in arithmetic operations than a public key cryptosystem, and the technique involves mutual authentication, ensures anonymity and untraceability, and secures responses to impersonation attacks and forward confidentiality.

Keywords: *Anonymity, Smartcard, Symmetric-Key Cryptographic, Untraceability, User Authentication.*

Article History
Article Received*: 24 July 2019*
Revised*: 12 September 2019*
Accepted*: 15 February 2020*
Publication*: 26 March 2020*

March - April 2020
ISSN: 0193-4120 Page No. 4557 - 4564

1. Introduction

Due to network technology development and expanded distribution of smartphones, network users have become available for access to system services by connecting networks at any time and place. Moreover, as the number of linking devices to networks increases, relevant services, yet as well as security threats, are constantly being expanded[1]. The network services can be exposed to various attacks as they are transferred via public channels. For secured communication among servers offering services and users to use the services linked with networks, mutual authentication step is necessarily required.

User authentication involves various factors as if Table 1[2]. ID distributed to devices is used for device verification and authentication in the most traditional and universal ID-based authentication scheme. ID-based authentication scheme can be applied to any conditions, however, is vulnerable impersonation attacks from ID exposure. In addition, devices disguising as authorized devices can transmit-receive data without any verification process, the attackers can collect data through impersonation attacks and utilize the collected data for replay attacks. To improve the ID-based authentication scheme, various authentication schemes based on authentication certification, biometrics and smartcards are suggested. Among them, the smartcard-based scheme can use biometrics, knowledge information, ID and password can be used for authentication. Numerous user authentication schemes have been proposed and their complete security safety has been asserted, yet are proved to have vulnerabilities and the vulnerabilities have consistently been improved.[3,4].

In this thesis, to increase efficiency, instead of using multiple servers, a user authentication scheme with a single server as registration center is to be proposed. The proposal authentication scheme enables mutual authentication, enhanced anonymity and untraceability of users, respond to impersonation attacks, and ensures forward confidentiality.

This thesis consists of followings. Chapter 2 observes the previous model of user authentication scheme and analyzes its weaknesses. Chapter 3 proposed its reinforced model with the weaknesses improved and Chapter 4 analyzes security and efficiency of the proposal model. Then, Chapter 5 draws a conclusion.

2. Related Study

Recently proposed user authentication schemes has following features. Lu et al.' scheme[5] improved the vulnerability to password guessing attacks from Arshad et al.'s[6], suggesting use of biometrics as an authentication instrument and decreased the level of calculation complexity by using dot product.

Table 1. Authentication Method[2]

Element	Description	Technology
Knowledge	Something you know	ID, Password, PIN
Possession	Something you have	Token, Smartcard, OTP, SMS
Existence	Something you are	Fingerprinter, Iris, Retina, Face, Palm pattern, Vein
Behavior	Something you do	Sign, Gait, Voice, Keyboard input

K. C. Shin's[7] proposal scheme cannot ensure anonymity, and Lu et al.'s scheme is vulnerable impersonation attacks. Huang et al.'s[8] is based on RSA cryptographic Algorithm and suggested dual element remote authentication using time-stamps. Amin et al.'s[9] proved the Huang et al.'s to be vulnerable to impersonation, password guessing and insider attacks and to have errors in password changing phase and suggested an user authentication scheme based on an improved RSA password system. Furthermore, in 2018, Xu et al.'s[10] indicated Amin et al.`s vulnerability to impersonation attacks with no forward confidentiality and untraceability ensured, and proposed a ECC-based multi-server authentication scheme.

2.1 Lu et al.' s Proposal User Authentication Scheme

Signs used in Lu et al. ' s proposal user authentication scheme as Table 2.

Table 2. Notation

Symbol	Description
Ui, Sj	User, Server
ID, PW, BIO	Identity, password, Bio
h(),h1(),h2()	Hash function
x	Secret key of the server
y	Secret Number
⊕, ‖	XOR operation, Concatenation operation
Ek, Dk	Encryption/Decryption with k
T	timestamp
SK	Session key

Registration Stage

Users register into a server to issue smartcards.

1) User selects their IDi and PWi and creates BIOi.

2) User calculates BPWi=PWi⊕h(BIOi) by using password PWi and biometrics BIOi, then transmit {IDi, BPWi} to the server via a secured channel.

3) Server with IDi and BPWi received calculates AIDi=IDi⊕h2(x) and Vi=h1(IDi||BPWi) by using secret key x, stores {AIDi, Vi, h1(), h2(), h()} in smartcards and transmits it to the users..

Login Stage

Users create a login message to request a server login.

1) Users insert their smartcards received from servers into card readers, then input IDi, PWi, and BIOi. Smartcards performs calculation of BPWi*=PWi⊕h(BIOi) with the input data and of Vi*=h1(IDi||BPWi) with BPWi*. The calculated Vi* and Vi stored in smartcards are compared

2) If the comparison results in not being equal, the login message is rejected. If the two are equal, smartcards select a random number Ri. Using the Ri, timestamp T1, stored data in smartcards and input data by users, K=h1(IDi||IDi⊕AIDi), M1=K⊕Ri and M2=h1(IDi||Ri||T1) are calculated. Login message {M1, M2, AIDi, T1} is created and transmitted to the server

Authentication Stage

Server which received the login message from users, performs authentication upon the users and practices authentication stage to create a session key.

1) Server with login {M1, M2, AIDi, T1} received create a timestamp Tc. Using the Tc created and message timestamp T1, validity of login message is verified. $|Tc-T1| \leq \Delta T$

2) Once the validity is verified, for the server to extract the user ID, IDi*=AIDi⊕h2(x) is calculated by using AIDi from the message and private key x from the server. Using the extracted user IDi* and received AIDi,

March - April 2020
ISSN: 0193-4120 Page No. 4557 - 4564

K*=h1(IDi*||IDi*⊕AIDi) is calculated, then a random number of the user, Ri*=K*⊕M1, is calculated by using the calculated figures and timestamp T1. M2* is compared with M2 within the login message.

3) If the two values are equal, the entity that transmitted a login message is confirmed to be a user. The server creates a random number Rs and timestamp T2. Using the Rs and T2, M3=K⊕Rs, SK=h(Ri||Rs), and M4=h1(K||Ri||SK||T2) are calculated, then the message {M3, M4, T2} is transmitted to the user.

4) User with message {M3, M4, T2} received creates a timestamp Tc, then verifies the message validity by using T2 from the message and Tc. $|Tc-T2| \leq \Delta T$

5) Once the validity is verified, the user calculates Rs*=K⊕M3 by using K and M3 from the message, then calculates SK*=h(Ri||Rs*) with the calculated Rs*. Using the calculated values and received values, performs calculation of M4*=h1(K||Ri||SK*||T2) and comparison between the M4* and M4 from the message.

6) If the two are equal, the user creates a timestamp T3, calculates M5=h1(K||Rs||SK||T3) and transmits {M5, T3} to the server.

7) Server with {M5, T3} received creates a timestamp Tc, then practices verification of server validity with T3 from the message and Tc. $|Tc-T3| \leq \Delta T$

Once the validity is verified, M5*=h1(K|Rs||SK|T3) is calculated, then compares it with M5 from the message. If the two are equal, user is authenticated, and SK is approved through a session key.

2.2 Vulnerabilities in Lu et al.'s Proposal User Authentication Scheme

Vulnerable to User Impersonation Attacks

If an attacker who tapped a login message {M1, M2, AIDi, T1} transmitted from user Ui to the server is the user Ua with a smartcard legitimately issued from the server, the attacker can identify the ID of user Ui from the login message sent by user Ui.

All users with smartcard {AIDx, Vx, h1(), h2(), h()} issued from the server can calculate h2(x)=AIDx⊕IDx by using AIDx and their own IDx. If an attacker Ua taps a login message and calculates AIDi⊕h2(x) via h2(x) calculated and AID from the login message {M1, M2, AIDi, T1}, the attacker can extract the ID of user Ui who transmitted-received a login message. Attacker Ua can disguise as user Ui by using IDI of user Ui, the smartcard owner, and can perform mutual authentication with the server and session key creation.

Vulnerable to Server Impersonation Attacks

User Ua who legitimately issued a smartcard can disguise as the server. Attacker, who tapped a login message {M1, M2, AIDi, T1} being transmitted from user Ui to the server, can extract user ID by calculating AIDi⊕h2(x) from h2(x), calculate K=h1(IDi*||IDi*⊕AIDi) by using the extracted IDi and AIDi from a tapped message, and a random number Ri=K⊕M1 of the user Ui by using M1 from the login message and calculated K. Attacker Ua selects a random number Ra, creates a timestamp T2, calculates M3=K⊕Ra, SK=h(Ri||Ra), M4=h1(K||Ri||SK||T2), and transmits a message {M3, M4, T2} to user Ui.

User Ui who received the message {M3, M4, T2} from user Ua disguising itself as the server identifies the T2 validity, then calculates Ra from M3⊕K and SK from h(Ri||Rs). Using Ra, SK, T2 and its own random number Rj, M4 is calculated and then the value is compared with the M4 in the message from attacker Ua for further verification of the attacker Ua as an authorized server.

3. Proposal User Authentication Scheme

This thesis suggests an improved model from the previous user authentication scheme vulnerabilities.

Registration Stage

1) User Ui selects identifier IDi, password PWi, biometrics BIOi and a random number Ri, then performs calculation of h(BIOi)와, RPWi=h(PWi||Ri). Registration message {IDi, RPWi, h(BIOi)} is transmitted to the server Sj via a secured channel.

2) The server Sj with registration message {IDi, RPWi, h(BIOi)} received uses a shared secret key xi with user Ui to calculate Vi=h(xi), CIDi=h(IDi||Vi||h(BIOi)) and DIDi=h(IDi||h(BIOi)). Using the calculated Vi and CIDi, Yi=RPWi⊕CIDi is calculated. Server Sj stores IDi, DIDi, DIDI and Vi of the user Ui into the database.

3) Server Sj stores Yi and DIDi into smartcards and transmits them to user Ui through a secured channel.

4) The User Ui with a smartcard received calculates Ai=Ri⊕h(IDi||PWi), and calculates CIDi*=Yi⊕RPWi by using RPWi. Using the calculated CIDi, Bi=h(Ri||CIDi*||h(IDi||PWi), Ci=h(xi)⊕h(IDi||PWi) are calculated then, Ai, Bi, Ci are additionally stored into the smartcards. SCi={Yi, DIDi, Ai, Bi, Ci}

Login and Authentication Stage

1) User Ui inserts a smartcard into a card reader, then input IDi, PWi, and BIOi.

2) Using the input values and stored values, Ri*=Ai⊕h(IDi||PWi) is calculated, and using Ri*, CIDi*=Yi⊕h(PWi||Ri*) is calculated. Using the calculated Ri* and CIDi*, Bi*=h(Ri*||CIDi*||h(IDi||PWi) is calculated and is compared with stored Bi. If the two values are equal, the smartcard confirms the user who input IDi, PWi, BIOi as the smartcard owner.

3) User selects a random number N1 and creates a timestamp T1. h(xi)*=Ci⊕h(IDi||PWi) is calculated and a secret key k=h(h(xi)⊕T1) is created by using the calculated h(xi)* and T1.

4) Using the secret key k, a cryptograph Li=Ek(IDi||N1||h(BIOi))is created.

5) User transmits a login message {Li, T1, DIDi} to the server.

6) The serve which received the login message {Li, T1, DIDi} creates a timestamp Tc. Using the timestamp Tc and login message timestamp T1, validity of login message is verified. $|Tc-T1| \leq \Delta T$

7) Once the validity is verified, the server searches for DIDi from the database of login messages. Vi is selected from the searched DIDi. Using the selected Vi and T1 of the message, k=h(Vi)⊕T1) is created, then Li is descrambled with the secret key k.

8) Using the extracted IDi from descrambling and h(BIOi), CIDi*=h(IDi||Vi||h(BIOi)) is calculated, then the value is compared with CIDi stored in a database. If they are equal, the user who transmitted-received a login message is confirmed to be a legitimate user.

9) Using CIDi, CIDi'=CIDi⊕k is calculated, and a timestamp T2 is created. With the calculated CIDi' and N1 of login message and timestamps T1 and T2, a session key SK=h(CIDi'||N1||T1||T2) is created then, Yj=h(IDi||SK||T2) is calculated.

10) The server transmits the message {Yj, T2} to the user.

11) The user who received the message {Yj, T2} from the server creates a timestamp Tc, then verifies the message validity by using the Tc and T2 from the message. $|Tc-T2| \leq \Delta T$

March - April 2020
ISSN: 0193-4120 Page No. 4557 - 4564

12) Once the validity is verified, the user calculates CIDi'*=CIDi⊕k and a session key SK*=h(CIDi'*||N1||T1||T2), then Yj*=h(IDi||SK*||T2) by using the calculated session key. If the calculated Yj* and Yj are equal, the user confirms the server which transmitted the message as an authorized server

4. Safety Analysis of Proposal User Authentication Scheme

4.1 Mutual Authentication

The server with the login message {Li, T1, DIDi} receives from user Ui searches DIDi in the database and extracts Vi from the searched values. With the extracted Vi and T1 from login message, a secret key k is created, then Li is descrambled by using the created secret key. As a result of descrambling, IDi, random number N1 and h(BIOi) are extracted, and CIDi is calculated by using the extracted figures. If the CIDi is found from the database, the user Ui who transmitted-received the login message is authenticated. The server which authenticated the user creates a message {Yj, T2} and sends it to the user, then the user who received the message can calculate CIDi' by using CIDi and secret key k and can generate a session key SK from the figures. The user Ui who calculated Yj by using the calculated CIDi' and session key SK, verifies the transmitting-receiving server of message {Yj, T2} as a legitimately authorized server if the calculated Yj and Yj from the received message are equal.

4.2 Provision of User Anonymity and Untraceability

If user Ua who legitimately issued a smartcard by performing a registration stage can identify IDi of user Ui and the shared secret key h(xi) among the server and the user Ui by tapping a message transmitted-received between user Ui and the server or by using the stored data in tis own smartcard, the user anonymity cannot be ensured and the data can be used by attackers to commit impersonation attacks. However, in the user authentication scheme proposed in this thesis, the data regarding users is included in Li of the login message {Li, T1, DIDi}, and Li is encrypted with secret key k. Moreover, DIDi=h(IDi||h(BIOi)) cannot be created, if IDi and h(BIOi) of user Ui is not identifiable. Thus, even if the attacker taps a login message, no data upon the transmitter and the receiver can be discovered.

4.3 Response to Smartcard Thefts

When smartcard is lost or stolen, impersonation attacks using stored data is available. In the user authentication scheme of this thesis, {Yi, DIDi, Ai, Bi, Ci} is the data stored in smartcards. All values stored in smartcards consists of values which cannot be used for extraction of any figures including IDi, PWi, BIOi, random number Rj and unique key xi,. Furthermore, no data can be obtained about users from any message in transmission-reception among servers and users.

4.4 Forward Confidentiality

Session key and secret key k to encrypt login message are generated as h(CIDi'||N1||T1||T2) and h(h(xi)||T1) respectively. Involving different timestamps at each session key and secret key creation, even if session key used previously is exposed to attackers, the data in exposed session keys cannot be used for guessing future session key.

5. Conclusion

In the user authentication scheme in this thesis proposal, first, users and servers can perform mutual authentication. Users registered to the server create login message by using their registered data, transmits the created message to the server, then the server compares the login message content and registered user information to authenticate the user.

March - April 2020
ISSN: 0193-4120 Page No. 4557 - 4564

Table 3. Comparison of security features

Features	Lu	Proposal User Authentication Scheme
Key Agreement	O	O
Forward Confidentiality	O	O
Untracebility	X	O
Smart-card Loss Attack	X	O
User Anonymity	X	O
mutual authentication	X	O

The server uses the login message content and the stored information to create authentication message after the completion of authentication process and transmits the message to the user.

The user who received the authentication message from the server uses the message content and the data previously input to identify whether the server is legitimately authorized. Second, user anonymity and untraceability are ensured. Messages transmitted-received among the server and users are not transmitted in plain texts, hence attackers cannot identify the user information despite of their tapping attempts. As no data of transmitter and receiver can be captured from messages, untraceability is ensured. Third, the system can respond to smartcard thefts. Attackers who acquired a lost smartcard by a legitimate user can use the smartcards can create login or authentication messages by obtaining ID, password and biometrics of the smartcard owners. However, creation of login or authentication messages is unavailable through stored figures in smartcards in the authentication scheme of this thesis proposal. Fourth, forward confidentiality I ensured. Having a timestamp at each session key or secret key generation allowed used session or secret key at previous session has no use for guessing future session or secret key from its containing information despite of being exposed to attackers.

References

[1] Keum DG. IoT Device Authentication And Security Using Blockchain [dissertation]. University of soonsil;2019.

[2] https://m.post.naver.com/viewer/postView.nhn?volumeNo=5667570&memberNo=3185448&vType=VERTICAL.

[3] Sambasiva Rao K, Kameswara Rao M. A lightweight digital signature generation mechanism for authentication of IoT devices. International Journal of Recent Technology and Engineering (IJRTE). 2019 Mar;7(6): 1862-1866.

[4] Shin KC. Remote Mutual Authentication Scheme for Anonymity and Un_Traceability Based on Biometric Information Using Public Key Cryptography. Journal of Knowledge Information Technology and Systems(JKITS). 2019 Oct; 14(5): 479-489.

[5] LU Y, Li L, Pent H, Yang Y. An enhanced biometric-based authentication scheme for telecare medicine information system using elliptic curve cryptosystem. Journal of Medical Systems. 2015 Feb; 39(32): 1-9.

[6] Arshad H, Nikooghadam M. Three-factor anonymous authentication and key agreement scheme for telecare medicine information systems. J. Med. Syst. 2014; 38(12): 1-12.

[7] Shin KC. A study on design of robust remote user authentication scheme with enhanced for anonymity and confidentiality. Journal of Knowledge Information Technology and Systems(JKITS). 2019 Feb; 14(1): 11-24.

[8] Huang HF, Chang HW, Yu PK. Enhancement of timestamp-based user authentication scheme with

March - April 2020
ISSN: 0193-4120 Page No. 4557 - 4564

smart card. International Journal of Network Security. 2014 Jan;6(6): 463-467.

[9] Amin R, Maritra T, Giri D, Srivastava PD. Cryptanalysis and improvement of an RSA based remote user authentication scheme using smart card. Wirel. Pers. Commun. 2017.

[10] Xu G, Qiu S, Ahmad H, Xu G, Guo Y, Zhang M, et al. A multi-server two-factor authentication scheme with un-traceability using elliptic curve cryptography, Sensors (Basel). 2018 Jul;18(7). pii: E2394. doi: 10.3390/s18072394.