User Authentication Scheme with Key Agreement providing Countermeasure of Impersonation Attack

Jaeyoung Lee

***Abstract*: IoT has expanded into broader areas from convenience and application in existing computing environment. Various threats, other than security issue, have emerged with development, and owing to many limitations in specifications, including device power, memory and communication bandwidth, existing security system cannot be applied. Authentication Scheme, by Mishra et al., employing smartcard with multi-servers, is vulnerable to impersonation, replay and DOS attacks. Authentication scheme which overcame such vulnerability is SIAKAS, yet is vulnerable to impersonation and does not offer message untraceability. The thesis enabled counter-responses against impersonation by attackers, by applying RN_{ij}, a variable recording the number of login request by an adequate user, during message generation of authentication purpose. Furthermore, by exploiting the trait of RN_{ij}, having a different figure every time, untraceability has been granted to message. SIAKAS is vulnerable to impersonation attack by user with smartcard issued, disguising as application server. Attacker can generate a key figure of application server, h(PSK), by using own smartcard data, then execute authentication phase upon login message via the generated h(PSK). Once user authentication is completed, in response to the result, a response message and session key are generated and sent to users, then the user recognizes the message from attacker pretending application server as an adequate application server, thus shares session key with the attacker. The thesis adapted RN_{ij}, which only can be identified by the user on authentication stage and the application server, during login message creation, for improvement, thus the attacker impersonating an application server can no longer use their login message for authentication. SIAKAS cannot offer untraceability on messages. If the application server of receiver is the same, M_4 included in login messages contains the equal figure. If an attacker hijacks login message through tapping, and examines the identity with M4, various data about both the user and application server can be captured. The thesis additionally adapted RN_{ij}, having different figure at every login message creation, into M_4 generation, thus ensured freshness and untraceability of the message. Improving existing Authentication Scheme with Key Agreement, vulnerable to impersonation and not offering traceability to message, the thesis proposes an improved Authentication Scheme with Key Agreement, ensuring untraceability and further anonymity to message and against impersonation attack by user with issued smartcard.**

Index Terms*: *About Key Agreement, Impersonation Attack, IoT, SmartCard, Untracebility, User Authentication.

Revised Manuscript Received on May 23, 2019.

Jaeyoung Lee, Professor, Department of Liberal Education, Semyung University, Jecheon, Republic of Korea

I. INTRODUCTION

As the notion of ubiquitous is practiced and developed, computing environment has rapidly shifted. Not only existing mobile environment, but also various devices which could have never been imagined to be linked to the network, are now being combined and used. Likewise, data, human beings, spaces as well as devices, linked to the network, process, create and store data, and such complex network and computing environment are called Internet of Things. As existing computing environment has gone beyond its convenience and application level, and its volume is consistently being enlarged, its associated, but unexpected and various security threats have emerged. However, devices consisting of IoT have many limitations in computing power, memory and communication bandwidth, hence its existing security system cannot be applied and newly devised security system is required[1]-[4].

IoT must be considered in three aspects – confidentiality, integrity and availability. Confidentiality is to allow access to data only by authorized user and to prevent exposure and disclosure of significant data during intrusion by attacker. Integrity is to prevent non-authorized being from counterfeiting and falsifying data, thus means accuracy, completeness, and effectiveness. Availability is to ensure provision of trustworthy data to legitimately authorized user. For IoT to offer reliable service, resolving confidentiality, integrity and availability issues, security technology such as encryption and mutual authentication is required[5]-[8].

Since 2004, Juang et al. proposed Encryption System based Multi-server Environment Authentication Scheme, various authentication schemes were suggested[9]. Authentication Scheme with Key Agreement by Mishra et al. provides anonymity by employing smartcard in multi-server environment. However, the technique is vulnerable to impersonation, replay and DOS attacks. Improved version of the technique is SIAKAS(Shin's Improved authentication key agreement Scheme)[10]. However, indeed, the technique has had a vulnerable to attack impersonating user and could not offer untraceability to message being sent.

The thesis would propose Improved Authentication Scheme with Key Agreement having its previous vulnerability resolved. To overcome the vulnerability to attack by user, with smartcard issued,

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

impersonating legitimate application server, a figure only known to user and application server is forced to be utilized for login message generation, and to offer message untraceability, a random number, timestamp and a figure different at every session, shared among application server and user are guided for an adequate use.

The thesis composition as followings. Chapter 2 looks at SIAKAS and analyzes its vulnerability. Chapter 3 suggests Authentication Scheme with Key Agreement having the vulnerability resolved, Chapter 4 analyzes the technique security. Then, eventually, Chapter 5 draws a conclusion.

II. RELATED STUDY

A. SIAKAS

SIAKAS is Key Agreement Authentication Scheme, by Shin, and consists of server registration, user registration, login, authentication and password change stages[11]. Table 1 summarizes the notation of the symbols used in the SIAKAS.

Table 1. Notations

Symbol	Description
i	Remote User i
j	Application server j
RC	Registration center
SC_i	SmartCard of i
ID_i, PW_i, BIO_i	Identity, password, and Bio information of i
SID_i	Identity of i
x	Master key of RC
PSK	Pre-shared key of RC
SK_{ab}	Session key established between a and b
T_i	Timestamp at step i
N_i	Random number at step i
h()	One way hash function
||	Concatenation operation
⊕	XOR operation
ΔT	The maximum of transmission delay time

Server Registration Stager

Application server is registered in RC(Registration Center) for service provision to user. When application server j requests for registration to RC, the RC calculates $h(h(PSK)||SID_j)$ via SID_j, an identifier of application server j and PSK, then send them to the server j. All application server cannot discover the parameter h(PSK) of RC.

User Registration Stage

User should register ID, Password and biometric data to receive service from application server.

1) User i select ID_i and PW_i, input biometrics BIO_i to calculate $W_1=h(PW_i||ID_i)$ and $W2=h(PWi\oplus BIOi)$. User i transmits user registration message $<ID_i, W_1, W_2>$ to RC through a secured channel.

2) When RC receives $<ID_i, W_1, W_2>$, $A_i=h(ID_i||x)$, $B_i=h(A_i)$, $X_i=B_i\oplus W_2$ and $Y_i=h(PSK)\oplus W_1$ are calculated. RC stores $<B_i, X_i, Y_i>$ in smartcard SC_i and send the smartcard SC_i to user i via a secured channel.

User i, with smartcard received, replaces Bi of smartcard SC_i into $C_i=B_i\oplus h(PW_i||ID_i||BIO_i)$, in case of theft and loss of smartcard and of user i verification. At last, $<C_i, X_i, Y_i>$ is stored in smartcard SC_i.

Login Stage

User i, registered in RC, executes login stage if service from application server, j, is desired.

1) User i inserts smartcard in its reader and input ID_i and PW_i. Input BIO_i via sensor.

2) Smartcard generates a random number N_1, and timestamp T_1. Smartcard uses ID_i, PW_i, BIO_i and C_i entered by user to calculate $B_i=C_i\oplus h(PW_i||ID_i||BIO_i)$.

3) Smartcard compares B_i from 2) and $X_i\oplus h(PW_i\oplus BIO_i)$. If they are equal, smartcard certifies user i, otherwise terminate the session.

4) Once user i authentication is successful, smartcard calculate h(PSK) via $Y_i\oplus h(PW_i||ID_i)$, then generate login messages $<M_1, M_2, M_3, M_4, T_1>$. $M_1=N_1\oplus h(B_i)$, $M_2=ID_i\oplus h(N_1)$, $M_3=h(ID_i||N_1||B_i||SID_j||T_1)$ and $M_4=B_i\oplus h(h(PSK)||SID_j)$.

5) Smartcard transfers login messages $<M_1, M_2, M_3, M_4, T_1>$ to application server j via open channel.

Authentication Stage

Application server j, which received $<M_1, M_2, M_3, M_4, T_1>$, certifies user i as followings.

1) Application server j identifies freshness of login message and legality of user i. Freshness of login message is identified through t_1, the time of login message reception and T_1 from login message, measuring t_1-T_1. If the figure is larger than Δt, login request by user i is denied. $(t_1-T_1)\geq\Delta t$

2) Once freshness of login message is identified, application server j calculates $h(h(PSK)||SID_j)$ to estimate B_i from M_4. $B_i=M_4\oplus h(h(PSK)||SID_j)$ is calculated, $N_1=M_1\oplus h(B_i)$ is calculated with the measured B_i and M_1, then $ID_i=M_2\oplus h(N_1)$ is calculated through M_2 and $h(N_1)$. At last, $h(ID_i||N_1||B_i||SID_j||T_1)$ is measured. Checking whether the calculation result and M_3 from login message are equal, if they are, application server j certifies user i.

3) Once user i certification is completed, application j generates a random number N_2, calculates $SK_{ij}=h(ID_i||SID_j||B_i||N_1||N_2)$, $M_5=N_2\oplus h(ID_i||N_1)$, $M_6=h(SK_{ij}||N_1||N_2||T_2)$ and $M_7=SID_j\oplus h(h(PSK)||SID_j)$, then send $<M_5, M_6, M_7, T_2>$ to user i.

4) Smartcard SC_i, having message received, calculates t_2-T_2 through using t_2, the time of message reception and T_2 of message to confirm the message freshness. If the figure is larger than Δt, terminate the session. $(t_2-T_2)\geq\Delta t$.

5) Once the freshness is confirmed, $N_2=M_5\oplus h(ID_i||N_1)$ is calculated via M_5 of the message received, then session key $SK_{ij}=h(ID_i||SID_j||B_i||N_1||N_2)$ is calculated via N_2. Using the measured figures, $h(SK_{ij}||N_1||N_2||T_2)$ is measured and compared with M_6. If the figures are equal, smartcard SC_i certifies application server j.

6) Once application server j is successfully certified, smartcard calculates $M_8=h(SK_{ij}||N_1||N_2)$ and transmits the figure to application j.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

7) Application server j compares the received M_8 and calculated M_8, then identifies legitimate user i and session key SK_{ij}.

Password Change Stage

Password change can freely be performed by user without any help from RC.

1) User inserts smartcard into reader, enter ID_i, PW_i, and BIO_i. Smartcard calculates $B_i=C_i \oplus h(PW_i||ID_i||BIO_i)$ and $W_2 \oplus X_i$ to check their identity for smartcard holder certification. If the authentication is successfully completed, new password PW_{inew} is entered.

2) Set X_i as X_{inew} after Smartcard calculates $W_2=h(PW_i \oplus BIO_i)$, $W_{2new}=h(PW_{inew}||BIO_i)$ and $X_{inew}=X_i \oplus W_2 \oplus W_{2new}$.

B. SIAKAS Security Vulnerability

Vulnerable to Impersonation attack by legitimate user impersonates application server j

SIAKAS is vulnerable to attack by legitimate user, with smartcard SC_a issued from RC, impersonating application server j through using own smartcard. When user i transmits $<M_1, M_2, M_3, M_4, T_1>$ to attacker a impersonating application server j, attacker a, who received login message, performs followings for authentication stage, in order for calculation of h(PSK) via data in ID_a, PW_a, BIO_a and smartcard SC_a and for impersonating application server j.

Authentication Stage 1) Attacker a identifies freshness and legitimacy of login message transmitted from user i. Attacker a uses t_1, the time of login message reception and T_1 of login message to calculate t_1-T_1. If the figure is larger than Δt, login request by user i is denied. $(t_1-T_1) \geq \Delta t$

Once the freshness of login message is confirmed, attacker a calculates $h(h(PSK)||SID_j)$ to estimate B_i from M_4. $B_i=M_4 \oplus h(h(PSK)||SID_j)$. Furthermore, proceed calculation of $N_1=M_1 \oplus h(B_i)$ via calculated B_i and M_1, then perform $ID_i=M_2 \oplus h(N_1)$ calculation with M_2 and $h(N_1)$. Lastly, execute calculation of $h(ID_i||N_1||B_i||SID_j||T_1)$. Confirm whether the result and M_3 of login message are equal, and if they are, attacker a certifies user i. Once authentication on user i is successful, attacker a generates a random number N_2, calculates $SK_{ij}=h(ID_i||SID_j||B_i||N_1||N_2)$, $M_5=N_2 \oplus h(ID_i||N_1)$, $M_6=h(SK_{ij}||N_1||N_2||T_2)$ and $M_7=SID_j \oplus h(h(PSK)||SID_j)$, then send $<M_5, M_6, M_7, T_2>$ to user i.

As user i, with message received from attacker a, successfully perform authentication stage, attacker a is certified as application server j. Reason for attacker a being able to be certified as application server j is because, significant data of RC, h(PSK) can be generated by any user with smartcard issued.

Session Traceability Attack

Anonymity and traceability of communication session in information society are important issues directly related to security and privacy[2]. Reason for uses of a random number and timestamp in security technique is to respond against replay attack by ensuring message freshness and to offer untraceability. However, assuming that M4 generated from login phase 3 of SIAKAS is reformed into $B_i \oplus h(h(PSK)||SID_j)$ and the B_i is $h(h(ID_i||x))$, M_4 is always identically created under the same conditions of the same user and application server. If attacker hijacks login message through tapping and examine identity of M_4, the data can diversely be utilized through traffic analysis.

III. PROPOSAL OF AUTHENTICATION SCHEME WITH KEY AGREEMENT

The thesis proposes an improved Authentication Scheme with Key Agreement from security vulnerability of SIAKAS. The proposal technique also equally consists of server registration, user registration, login, authentication and password change stages.

Server Registration Stage

Once application server j requests RC for registration, RC uses identifier SID_j of application server j and PSK to calculate $h(h(PSK)||SID_j)$, then sends it to server j. h(PSK) of RC is not known to any application server.

User Registration Stage

User i should be registered into RC to receive service by application server j.

1) User i selects ID_i and PW_i, inputs biometrics BIO_i into sensor, then calculates $W_1=h(PW_i \oplus BIO_i)$. User i transmits user registration message $<SID_j, ID_i, W_1>$ to RC via secured channel.

2) Once RC receives user registration message $<SID_j, ID_i, W_1>$, $A_i=h(ID_i||x)$, $X_i=A_i \oplus W_1$ and $Y_i=h(h(PSK)||SID_j) \oplus W_1$ are calculated, then stores $<A_i, X_i, Y_i>$ in smartcard SC_i for transfer to user i via secured channel.

3) RC sends ID_i of User i to application server j. Application server j check if the ID exists in the user management list. User list of application server j stores user ID from service request and RN_{ij} variable recording the number of service request by the user. If the ID is not confirmed from the user list, the ID and RN_{ij} of the user i are added into the list. Initial figure of RN_{ij} is 0.

User i, with smartcard received, replaces A_i of smartcard SC_i into $B_i=A_i \oplus h(PW_i||ID_i||BIO_i)$, in case of theft and loss of smartcard and of user i verification. At last, $<B_i, X_i, Y_i>$ is stored in smartcard SC_i.

Login Stage

User i initiates login stage to receive service of application server j.

1) User i inserts smartcard SC_i into reader. ID_i and PW_i are input, and biometrics BIO_i is entered via sensor.

2) Smartcard generates a random number N_1 and time stamp T_1. Then, renew RN_{ij} variable recording the number of service request to application server j. IF it is an initial, RN_{ij}=0, if not, $RN_{ij}=RN_{ij}+1$. Smartcard calculates $A_i=B_i \oplus h(PW_i||ID_i||BIO_i)$ by using ID_i, PW_i and BIO_i entered by user and B_i.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

3) Smartcard compares calculated A_i and $X_i \oplus W_1$. If they are equal, smartcard certifies SC_i, otherwise terminates the session. Once smartcard successfully perform user authentication, $Y_i \oplus W_1$ is calculated to generate $h(h(PSK)||SID_j)$ and login message <M_1, M_2, M_3, M_4, T_1>.
$M_1=N_1 \oplus h(A_i)$,
$M_2=ID_i \oplus h(RN_{ij})$,
$M_3=h(ID_i||N_1||A_i||SID_j||T_1||RN_{ij})$,
$M4=A_i \oplus h(h(PSK)||SID_j) \oplus h(RN_{ij})$.

4) Smartcard sends login message <M_1, M_2, M_3, M_4, T_1> to application server j via open channel.

Authentication Stage

Application Server with <M_1, M_2, M_3, M_4, T_1> received certifies user i.

1) To identify freshness of login message, application server j measures t_1-T_1 by using t_1, the time of login message reception and T_1 of message. If the figure is larger than Δt, the login request should be denied. $(t_1-T_1) \geq \Delta t$

2) Once login message freshness is confirmed, application server j identifies legitimacy of user i. Server j searches for ID_i and RN_{ij} that satisfies M_2 conditions of login message in user list. If no figure is appropriate, terminate the session. Otherwise, calculate $A_{i=}M_4 \oplus h(h(PSK)||SID_j) \oplus h(RN_{ij})$, using M_4 of login message, $h(h(PSK)||SID_j)$ and RN_{ij}. Furthermore, calculate $N_1=M_1 \oplus h(A_i)$ via M_1 and calculated A_i, and lastly, calculate $M_3=h(ID_i||N_1||A_i||SID_j||T_1||RN_{ij})$, then confirm if the figure and M_3 of login message are equal. If they are, application server j certifies user i as legitimate.

3) Once user is certified, application server j generates a random number N_2, calculates $SK_{ij}=h(ID_i||SID_j||A_i||N_1||N_2||RN_{ij})$, $M_5=N_2 \oplus h(ID_i||N_1) \oplus h(RN_{ij})$ and $M_6=h(SK_{ij}||N_1||N_2||T_2)$, then send <$M_5$, M_6, T_2> to user i.

4) User i, who received message, uses t_2, the time of message reception, and T_2 of message to check freshness, then measure t_2-T_2. If it is larger than Δt, terminate the session. $(t_2-T_2) \geq \Delta t$.

Once message freshness is confirmed, $N_2=M_5 \oplus h(ID_i||N_1) \oplus h(RN_{ij})$ is calculated via M_5, then measure session key SK_{ij} by using N2 calculated. $SK_{ij}=h(ID_i||SID_j||A_i||N_1||N_2||RN_{ij})$. By means of the calculated figure, measure M_6, then compare with the M_6 with other M_6 from the received message. If they are equal, application server j is certified as legitimate.

5) When application server j is successfully certified, smartcard calculates $M_7=h(SK_{ij}||N_1||N_2)$ and send it to server j.

6) Application server j compares M_7 received and own M_7 estimated, thus to identify a legitimate user i and session key SK_{ij}.

Password Change Stage

Password change can freely be performed by user without any help from RC.

1) User inserts smartcard into reader, enter ID_i, PW_i, and BIO_i. Smartcard calculates $B_i=C_i \oplus h(PW_i||ID_i||BIO_i)$ and $W_2 \oplus X_i$ to check their identity for smartcard holder certification. If the authentication is successfully completed, new password PW_{inew} is entered.

2) Set X_i as X_{inew} after Smartcard calculates $W_2=h(PW_i \oplus BIO_i)$, $W_{2new}=h(PW_{inew}||BIO_i)$ and $Xi_{new}=X_i \oplus W_2 \oplus W_{2new}$.

IV. SECURITY ANALYSIS

A. Counter-response against Impersonation Attack

Proposal of Authentication Scheme with Key Agreement is secured from attack by user a, with smartcard issued, impersonating application server j. To impersonate server j, attacker a must be able to generate <M_5, M_6, T_2> during authentication stage. M_5, being generated from calculation of $N_2 \oplus h(ID_i||N_1) \oplus h(RN_{ij})$, can only be calculated when RN_{ij} is known. RN_{ij}, a shared figure among user i and application server j, is a variable recording the number of service request from user i to server j, thus is a figure which cannot be captured by attacker a.

B. Provision of Untraceability

In Proposal of Authentication Scheme with Key Agreement, user i and application server j confirm message freshness and legitimacy of user and of application server via <M_1, M_2, M_3, M_4, T_1>, <M_5, M_6, T_2> and <M_7> during authentication stage. Appropriately exploiting a random number, time stamp, RN_{ij}, having different figure at every session, included in message generated from the proposal technique, message freshness and untraceability have become available for provision.

C. Provision of Anonymity

In Proposal of Authentication Scheme with Key Agreement, ID_i of user i cannot be identified from message being sent or received among user i and application server j. Associated figure with ID_i of user i is $M_2=ID_i \oplus h(RN_{ij})$. Discovering RN_{ij}, being shared only by user i and application server j, is necessary to identify identifier ID_i of user i through M_2, however attacker cannot measure RN_{ij}.

Table 2 is a comparison of the safety of SIAKAS and Proposal of Authentication Scheme with Key Agreement.

Table 2. Comparison of security features

Features	SIAKAS	Proposal of Authentication Scheme with Key Agreement
Password guessing	O	O
Impersonation	X	O
Replay	O	O
User anonymity	O	O
Untraceability	X	O

V. CONCLUSION

The thesis proposed an improved Authentication Scheme with Key Agreement from existing SIAKAS, by identifying its security vulnerability.

The proposed Authentication Scheme with Key Agreement uses a figure, only known to the user and application server, during login message creation, hence enabled counter-responses against impersonation by users with smartcard issued, exploiting own data, and allowed provision of freshness and untraceability of messages through an adequate uses of a random number, time-stamp and the shared figure among the users and the application server.

REFERENCES

1. H. W. Kim, "A Design of mutual authentication protocol between heterogeneous services in the internet of things Environment", Graduate School of Soongsil University, 2017.
2. K. W. Choi, "A Study on Improved User Authentication and Key Agreement In WSN Environment", Graduate School of Soonchunhyang University, 2018.
3. S. G. Park, "An Efficient Key management for Wireless Sensor Network", Journal of Digital Contents Society, 2012 Mar, 13(1), 129-39. DOI :10.9728/dcs.2012.13.1.129.
4. Y. S. Lee, "Authentication Method for Safe Internet of Thing Environment", Journal of Korea institute of information, electronics, and communication technology, 2015 Feb, 8(1), pp.51–58. DOI:10.17661/jkiiect.2015.8.1.051.
5. https://terms.naver.com/entry.nhn?docId=3431828&cid=58437&categoryId=58437, 2019.
6. J. H. Moon, D. H. Won, "An Enhanced Symmetric Key-Based Remote User Authentication Scheme with Forward Secrecy", Journal of Korea Multimedia Society, 2017 Mar, 20(3), pp.200-10. DOI:10.9717/kmms.2017.20.3.500.
7. M. O. Park, "Weaknesses Cryptanalysis of Khan's Scheme and Improved Authentication Scheme preserving User Anonymity", Journal of the Korea Society of Computer and Information. 2013 Feb, 18(2), pp.87-94. UCI:G704-001619.2013.18.2.007.
8. H. W. Choi, H. S. Kim, "Impersonation Attacks on Anonymous User Authentication and Key Agreement Scheme in Wireless Sensor Networks", Journal of Digital Convergence. 2016 Oct, 14(10), pp.287-93. DOI:10.14400/JDC.2016.14.10.287.
9. W. S. Juang, "Efficient multi-server password authenticated key agreement using smart card", IEEE Transactions on Consumer Electronics. 2004 Jan, 50(1), pp.251-55. DOI:10.1109/TCE.2004.1277870.
10. D. Mishra, A. K. Das, S. Mukhopadhyay, "A secure user anonymity-preserving biometric-based multi-server authenticated key agreement scheme using smart cards", Expert System with Applications. 2014, 41(18), pp.8129-42. DOI:10.1016/j.eswa.2014.07.004.
11. K. C. Shin, "Analysis and security improvements to Mishra et al.'s authentication", Journal of Security Engineering. 2016 Jul, 13(4), pp.261-78. DOI:10.14257/jse10.14257/jse.2016.0810.14257/jse.2016.08.01

AUTHORS PROFILE

Jaeyoung Lee received the Ph. D. from Chungbuk National University, Cheongju, Republic of Korea. She is an Assistant Processor in Department of Liberal Education at Semyung University, Jecheon, Republic of Korea. Her main areas of research interest are Network Security.