IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received February 25, 2019, accepted March 12, 2019, date of publication March 19, 2019, date of current version April 8, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2905731

Questioning Key Compromise Attack on Ostad-Sharif et al.'s Authentication and Session key Generation Scheme for Healthcare Applications

SARU KUMARI[1], PRADEEP CHAUDHARY[2], CHIEN-MING CHEN[3], AND MUHAMMAD KHURRAM KHAN[4], (Senior Member, IEEE)

[1]Department of Mathematics, Chaudhary Charan Singh University, Meerut 250004, India
[2]Department of Statistics, Chaudhary Charan Singh University, Meerut 250004, India
[3]College of Computer Science and Engineering, Shandong University of Science and Technology, Qingdao 266510, China
[4]Centre of excellence in Information Assurance, King Saud University, Riyadh 11653, Saudi Arabia

Corresponding authors: Chien-Ming Chen (chienmingchen@ieee.org) and Muhammad Khurram Khan (mkhurram@ksu.edu.sa)

This work was supported by the Deanship of Scientific Research, King Saud University, through research group under Grant RG-1439-58.

ABSTRACT Recently, Ostad-Sharif *et al.* pointed out the susceptibility of three different authentication schemes themed for telecare medicine/medical information systems to key compromise impersonation attack (KCIA). To further address this issue, they proposed an ECC-based authentication and key generation scheme for healthcare applications. In this paper, we show that Ostad-Sharif *et al.*'s scheme is not only affected with key compromise impersonation attack but also suffers from a key compromise password guessing attack. Several papers have been published by the researchers by applying KCIA on existing authentication protocols. Before any further move in research in this direction, researchers must contemplate about KCIA. We conclude this article with a rigorous analysis of KCIA along with two questions to ponderon for the research community working in this field.

INDEX TERMS Authentication, key-agreement, key compromise password guessing attack, key compromise impersonation.

I. INTRODUCTION

Telecare medicine/medical information systems (TMIS) are systems dedicated to provide online healthcare services. It is playing an important role in upgrading the traditional time consuming healthcare system to a smart healthcare system with the use of information and communication technology (ICT). As these systems are entirely based on Internet, an open medium, security and privacy are major concerns for their viability. The issue of security and privacy is well addressed by the authentication and key agreement schemes.

Recently, Ostad-Sharif *et al.* [1] pointed out key compromise impersonation attack in authentication schemes designed by Giri *et al.* [2], Amin and Biswas [3], and Arshad and Rasoolzadegan [4] for telecare medicine/medical information systems (TMIS). In succession, Ostad-Sharif *et al.* [1] also proposed an authentication scheme for healthcare applications. In this paper, we show that their scheme is also susceptible to key compromise impersonation attack. The worst case is that in their scheme the key compromise impersonation attack leads to password guessing attack.

The associate editor coordinating the review of this manuscript and approving it for publication was Tai-Hoon Kim.

II. NOTATIONS AND PICTORIAL REVIEW OF OSTAD-SHARIF et al.'s SCHEME

A. NOTATIONS AND DESCRIPTION

See Table 1.

B. PICTORIAL REVIEW OF OSTAD-SHARIF et al.'s SCHEME

See Fig. 1.

III. QUESTIONING KEY COMPROMISE ATTACK ON OSTAD-SHARIF et al.'s SCHEME

In this section, we show that Ostad-Sharif et al.'s scheme suffers from key compromise impersonation attack and key compromise password guessing attack.

Patient (p_i)		**Server (S)**
Registration of Patient:		
Chooses id_p, pw_p & r_p, u_p		
$opw_p = h_0((id_m \oplus id_p)\|\|r_p\|\|pw_p)$		
$xpw_p = h_0(u_p\|\|pw_p)P$		
	$\{id_p, id_m, opw_p, xpw_p\}$ →	Checks the validity of id_p, id_m
		$a_p = h_0(id_m\|\|id_p\|\|x)$, $b_p = opw_p \oplus a_p$
		$c_p = h_1(opw_p) \oplus xP$, $d_p = h_1(a_p) \oplus xpw_p$
		Generates random number n_s
		$eid_p = enc_x(id_p\|\|n_s)$
		Stores $\{id_p, id_m, empty, d_p\}$ in its database
	← $\{eid_p, b_p, c_p\}$	
Sets $token_p^{pw} = 0$		
Stores $\{eid_p, b_p, c_p, r_p, u_p, token_p^{pw}\}$ in the mobile device		

Patient(p_i) /Mobile Device(md_i)		**Server (S)**
***Login and Authentication*:**		
p_i: Inserts id_p, pw_p		
md_i: Retrieves r_p, b_p		
$opw_p = h_0((id_m \oplus id_p)\|\|r_p\|\|pw_p)$		
$a_p = opw_p \oplus b_p$, $Q = xP = h_1(opw_p) \oplus c_p$		
Generates random number n_p		
$X_p = h_0(id_m\|\|id_p\|\|n_p)P$		
$v_p = h_0(a_p\|\|X_p\|\|Q\|\|t_p\|\|token_p^{pw})$		
For $token_p^{pw} >= 1$		
$xpw_p = h_0(u_p\|\|pw_p)P$		
$v_p^{pw} = h_0(a_p\|\|X_p\|\|Q\|\|t_p\|\|xpw_p\|\|token_p^{pw})$		
	$\{token_p^{pw}, eid_p, X_p, v_p, v_p^{pw}, t_p\}$ →	For fresh t_p , $(id_p\|\|n_s) = dec_x(eid_p)$
		For valid id_p , Retrieves id_m and d_p
		$a_p = h_0(id_m\|\|id_p\|\|x)$, $xpw_p = h_1(a_p) \oplus d_p$
		For $token_p^{pw} = 0$, verifies if
		$h_0(a_p\|\|X_p\|\|Q\|\|t_p\|\|token_p^{pw}) =? v_p$
		For $token_p^{pw} >= 1$, verifies if
		$h_0(a_p\|\|X_p\|\|Q\|\|t_p\|\|xpw_p\|\|token_p^{pw}) = ? v_p^{pw}$
		Else, $\{xpw_p^{old} = h_1(a_p) \oplus d_p^{old}$
		$h_0(a_p\|\|X_p\|\|Q\|\|t_p\|\|xpw_p^{old}\|\|token_p^{pw}) = ? v_p^{pw}\}$
		Generates random number n_{ss}
		$k = (x + h_0(id_x\|\|n_{ss}))(xpw_p + X_p)$, $sk = h_2(t_p\|\|k)$
		Generates random number n_s^{new}
		$eid_p^{new} = enc_s(id_p\|\|n_s^{new})$, $oeid_p^{new} = eid_p^{new} \oplus h_3(sk)$
		$v_s = h_0(a_p\|\|X_s\|\|eid_p^{new}\|\|sk)$
	← $\{oeid_p^{new}, X_s, v_s\}$	
$k = (h_0(u_p\|\|pw_p) + h_0(id_m\|\|id_p\|\|n_p))(Q + X_s)$		
$sk = h_2(t_p\|\|k)$, $eid_p^{new} = oeid_p^{new} \oplus h_3(sk)$		
$h_0(a_p\|\|X_s\|\|eid_p^{new}\|\|sk) = ? v_s$		
$eid_p^{new} \leftarrow eid_p$		
Sets $token_p^{pw} = 0$		

FIGURE 1. User registration, login & authentication phases of Ostad-Sharif et al.'s scheme.

A. KEY COMPROMISE IMPERSONATION ATTACK

An attacker E possessing the secret key x of the server S intercepts the login message $\{token_p^{pw}, eid_p, X_p, v_p, v_p^{pw}, t_p\}$ of p_i from public channel and reads the value of $token_p^{pw}$. E computes $(id_p||n_s) = dec_x(eid_p)$ and uses the retrieved id_p to obtain user specific details $\{id_p, id_m, d_p\}$ from the stolen registration table of the database of S. E computes $a_p = h_0(id_m||id_p||x)$, generates a random number n_{ep} and computes $X_{ep} = h_0(id_m||id_p||n_{ep})P$ where P is public value. For $token_p^{pw} = 0$, E computes $v_{ep} = h_0(a_p||X_{ep}||xP\ ||t_{ep}||token_p^{pw})$ with current timestamp t_{ep}. For $token_p^{pw} >= 1$, E computes $xpw_p = d_p \oplus h_1(a_p)$ and $v_{ep}^{pw} = h_0(a_p||X_{ep}||xP\ ||t_{ep}||xpw_p||token_p^{pw})$. E sends $\{token_p^{pw}, eid_p, X_{ep}, v_{ep}, v_{ep}^{pw}, t_{ep}\}$ as a login message to S in order to act as the legal user p_i. Clearly, the login message $\{token_p^{pw}, eid_p, X_{ep}, v_{ep}, v_{ep}^{pw}, t_{ep}\}$ will be entertained by S as

TABLE 1. The notations with description.

Notations	Description
p_i	Patient
S	Server
E	Attacker
id_p, pw_p	Identity/password of patient
id_m	Identity of patient's mobile device
x	Server's master secret key
r_p, u_p	Random numbers generated at the patient end during registration phase
n_s	Random number generated at the server end during registration phase
n_p	Random number generated at the patient end during login-authentication phase
n_{ss}, n_s^{new}	Random numbers generated at the server end during login-authentication phase
t_p	Current timestamp at the patient side
sk	Session key agreed between patient and server
P	Base point on a suitably chosen elliptic curve
$h_0(.)$, $h_1(.)$, $h_2(.)$	One-way hash functions
$\oplus$	Bitwise XOR operator
$\|\|$	Concatenation operator

t_{ep} is the current timestamp; eid_p contains the valid identity id_p of p_i; X_{ep} contains the valid identity id_p of p_i, the valid identity id_m of the mobile device of p_i, and fresh random number n_{ep}; further v_{ep} and v_{ep}^{pw} are computed with the exact session key x of S,valid value of a_p and also according to the value of $token_p^{pw}$ being sent. Thus, the server will believe that the received message is from the legitimate patient p_i and hence the attacker is able to impersonate as patient.

B. KEY COMPROMISE PASSWORD GUESSING ATTACK

Suppose that an attacker E, possessing the compromised secret key x of the server, obtains the mobile device of patient p_i. E can procure the parameters $\{eid_p, b_p, c_p, r_p, u_p, token_p^{pw}\}$ stored inside the mobile device [5], [6]. Then E can guess the password of p_i in any of the following ways.

E computes $(id_p||n_s) = dec_x(eid_p)$ to obtain id_p, makes a guess id_m^* for identity of the mobile device of p_i and computes $a_p^* = h_0(id_m^*||id_p||x)$, $opw_p^* = b_p \oplus a_p^*$, $h_1(opw_p^*)$, $h_1(opw_p) = c_p \oplus xP$, whence P is public parameter. Compares $h_1(opw_p^*)$ and $h_1(opw_p)$, equality of these two values guarantees the correctness of the guessed id_m^*, else, E attempts with some other guess. It is clear from the aforementioned computations that if E possesses the correct id_m then it also possesses the correct opw_p and a_p. Then E guesses pw_p^* for possible password of p_i and computes $opw_p^{**} = h_0((id_m \oplus id_p)||r_p||pw_p^*)$ whence r_p is available from the mobile device. Equality of opw_p^{**} and opw_p guarantees the correctness of the guessed pw_p^*, else, E attempts with some other guess.

Alternately, E can also obtain the exact value of id_m corresponding to the patient p_i from the database of the server S since S stores $\{id_p, id_m, empty, d_p\}$ in its database as the explanation follows. Since id_p is available in the database entry of p_i. The attacker E possessing id_p via computation $(id_p||n_s) = dec_x(eid_p)$, can easily pick the entry $\{id_p, id_m, d_p\}$ corresponding to p_i from the stolen registration table of the database of S. Then E guesses pw_p^* for possible password of p_i, computes $a_p = h_0(id_m||id_p||x)$, $opw_p = b_p \oplus a_p$. E computes $opw_p^* = h_0((id_m \oplus id_p)||r_p||pw_p^*)$ whence r_p is available from the mobile device. E compares opw_p^* and opw_p, the equality of these two values ensures the correctness of the guessed pw_p^*, else, E attempts with some other guess. E can also compute $xpw_p = d_p \oplus h_1(a_p)$, $xpw_p^* = h_0(u_p||pw_p^*)P$, whence r_p is available in the mobile device. E compares xpw_p^* and xpw_p, the equality of these two values ensures the correctness of the guessed pw_p^*, else, E attempts with some other guess. In this way, the attacker E can guess the password of p_i.

IV. CONCLUSION

Given any authentication scheme, if the secret key of the server is compromised and comes in the knowledge of an attacker then the scheme will surely be exposed to various types of attacks. In fact, leakage of server's secret key is very rare and this is a very strong assumption to apply attacks on an existing scheme. The reason is that the server is the most trusted authority in the scenario of authentication schemes, thereby; there are substantial security provisions to maintain the security of server's secret key.

We observed that Ostad-Sharif et al.'s scheme suffers from key compromise impersonation attack as well as key compromise password guessing attack although they would have definitely tried their best to avoid the possibility of key compromise attack on their scheme as they themselves mounted this attack on the target schemes in their work, and in the process of seeking a solution to this attack they designed and presented a new scheme. Thus, it is hardly possible for an authentication scheme to defy this attack. Moreover, once the secret key of the server comes in the knowledge of an attacker E, he/she can act as the legitimate server. In sensitive application scenario of healthcare, the attacker sitting as a valid server can collect sensitive data of patients that can be misused for various purposes. In addition, the attacker acting as the legitimate server can also provide false reply to patients' queries thereby creating problems in their treatment with an intention to corrupt the online healthcare system. Therefore, key compromise attack is detrimental for sensitive applications such as healthcare services and it may lead to public unrest and disinterest in online services.

Based on the above analysis and discussion we put forward two questions for the researchers working in this field. First question is whether the key compromise attack should be designated as a valid attack or an invalid attack. That is, researchers should provide either validity or invalidity to this attack. Second question is that if the researchers provide validity to this attack then they should provide a concrete solution to it which is an open challenge.

CONFLICT OF INTEREST

Authors have no conflict of interest.

REFERENCES

[1] A. Ostad-Sharif, D. Abbasinezhad-Mood, and M. Nikooghadam, "A robust and efficient ECC-based mutual authentication and session key generation scheme for healthcare applications," *J. Med. Syst.*, vol. 43, p. 10, Jan. 2019, doi: 10.1007/s10916-018-1120-5.
[2] D. Giri, T. Maitra, R. Amin, and P. D. Srivastava, "An efficient and robust RSA-based remote user authentication for telecare medical information systems," *J. Med. Syst.*, vol. 39, no. 1, p. 145, Jan. 2015, doi: 10.1007/s10916-014-0145-7.
[3] R. Amin and G. P. Biswas, "An improved RSA based user authentication and session key agreement protocol usable in TMIS," *J. Med. Syst.*, vol. 39, no. 8, p. 79, 2015.
[4] A. Hamed and A. Rasoolzadegan, "Design of a secure authentication and key agreement scheme preserving user privacy usable in telecare medicine information systems," *J. Med. Syst.*, vol. 40, no. 11, p. 237, 2016.
[5] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Proc. Annu. Int. Cryptol. Conf.*, 1999, pp. 388–397.
[6] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Examining smart-card security under the threat of power analysis attacks," *IEEE Trans. Comput.*, vol. 51, no. 5, pp. 541–552, May 2002.

SARU KUMARI received the Ph.D. degree in mathematics from Chaudhary Charan Singh University, Meerut, India, in 2012, where she is currently an Assistant Professor with the Department of Mathematics. She has published more than 133 research papers in reputed International journals and conferences, including 115 publications in SCI-Indexed Journals. Her current research interests include information security and applied cryptography. She is a Technical Program Committee Member for many International conferences. She served as a Lead/Guest Editor of four Special Issues in SCI Journals of Elsevier, Springer, and Wiley. She is on the Editorial Board of more than 12 Journals of International repute including seven SCI Journals.

PRADEEP CHAUDHARY received the M.Sc. (Hons.), M.Phil. (Hons.), and Ph.D. degrees in statistics from Chaudhary Charan Singh (CCS) University, Meerut, India, in 1996, 1998, and 2004, respectively. He has also served as a Research Assistant, the Directorate of the Institutional Finance and Sarvhit Bima, Government of U.P., India, and as an Assistant Director of the State Institute of Rural Development, Rural Development Department, Government of U.P. He is currently an Assistant Professor with the Department of Statistics, CCS University. His current research interests include reliability and applied cryptography.

CHIEN-MING CHEN received the Ph.D. degree from National Tsing Hua University, Taiwan. He is currently an Associate Professor of the Shandong University of Science and Technology, China. He also serves as an Associate Editor of the IEEE Access. His current research interests include network security, the mobile Internet, the IoT, and cryptography. He serves as an Executive Editor of the *International Journal of Information Computer Security*.

MUHAMMAD KHURRAM KHAN is currently a Full Professor with the Center of Excellence in Information Assurance (CoEIA), King Saud University, Saudi Arabia. He is one of the founding members of CoEIA and has served as the Manager R&D, from 2009 to 2012. He has published more than 325 research papers in the journals and conferences of international repute. In addition, he is an inventor of ten US/PCT patents. He has edited seven books/proceedings published by Springer–Verlag and IEEE. His research interests include cybersecurity, digital authentication, biometrics, multimedia security, and technological innovation management. He has secured an outstanding leadership award at IEEE International Conference on Networks and Systems Security 2009, Australia. He received the Gold Medal for the Best Invention & Innovation Award at 10th Malaysian Technology Expo 2011, Malaysia. Moreover, his invention recently got a Bronze Medal at '41st International Exhibition of Inventions', Geneva, Switzerland, in 2013. In addition, he received the Best Paper Award from the *Journal of Network & Computer Applications* (Elsevier), in 2015. He was a recipient of the King Saud University Award for Scientific Excellence (Research Productivity), in 2015. He was also a recipient of the King Saud University Award for Scientific Excellence (Inventions, Innovations, and Technology Licensing), in 2016. He is the Editor-in-Chief of a well-esteemed international journal *Telecommunication Systems* (Springer-Verlag, since 1993) with an impact factor of 1.542 (JCR 2017). He is also the full-time Editor/Associate Editor of several international journals/magazines. He has also played role of the guest editor of several international ISI-indexed journals of Springer–Verlag and Elsevier Science. Moreover, he is one of the organizing chairs of more than five dozen international conferences and member of technical committees of more than ten dozen international conferences.