A Security Comment on "A Security-Enhanced Authentication and Key Agreement Protocol in Smart Grid"

Dariush Abbasinezhad-Mood

***Abstract*— In smart grid (SG), key agreement protocols (KAPs) are used as one of the most prevalent means to establish secure data transmission channels between smart meters (SMs) and service providers (SPs). Quite recently, Wu et al. [1] have indicated the vulnerability of Hu et al.'s KAP [2] to "key compromise impersonation (KCI)" attack and proposed a security-enhanced one for secure communications of SMs and SPs in SG. Not to undermine the noteworthy contributions of their work, this comment demonstrates that their own KAP, i.e., the proposed one in [1] is still vulnerable to KCI attack. Accordingly, we suggest a simple modification to fix the KCI attack issue. Our attack procedure gives some delicate hints to scholars to protect their schemes against the KCI attack in future researches.**

***Index Terms*— Authentication, Key Agreement Protocol (KAP), Key Compromise Impersonation (KCI) Attack, Smart Grid (SG).**

I. Introduction

In smart grid (SG), key agreement protocols (KAPs) are used as one of the most prevalent means to establish secure data transmission channels between smart meters (SMs) and service providers (SPs) [3], [4]. A desired KAP for SG needs to fulfil certain security properties and must resist specific security attacks. "Key compromise impersonation (KCI)" attack is one of the challenging security threats that may cause devastating consequences [5], [6]. As a result, due to the high importance of KCI attack in the context of SG, quite recently, Wu et al. [1] have argued that the proposed KAP by Hu et al. [2] cannot resist KCI attack. They further suggested a security-improved KAP for SG and mentioned that their proposed one can withstand KCI attack. In their security analysis, they stated that if long-term private values of SM, i.e., $\{ID_{SM_i}, ID_{SP_j}, y_i, X_{ij}\}$, are revealed to attacker $\mathcal{A}$, $\mathcal{A}$ cannot impersonate as SP. Although this statement is completely true and attacker $\mathcal{A}$ cannot impersonate as SP if long-term secrets of SM are disclosed, in this paper, we show that the proposed KAP in [1] is still vulnerable to the KCI attack and if long-term private keys of SP are disclosed to $\mathcal{A}$, $\mathcal{A}$ can easily impersonate as SM and get session key.

II. Synopsis of the Proposed KAP by Wu et al. [1]

In this section, we only briefly explain the "authenticated key agreement (AKA)" phase of the proposed KAP by Wu et al. [1]. For more details, interested readers can refer to the original paper [1]. By the way, it should be mentioned that there are many typos in their proposed KAP that we have tried to correct. Table I shows the steps of key establishment protocol. Details are as follows.

The proposed KAP by Wu et al. [1] is composed of "pre-deployment," "registration," and "AKA" phases. After the registration, SM stores $\{ID_{SM_i}, ID_{SP_j}, y_i, X_{ij}\}$ and SP stores $\{ID_{SP_j}, ID_{SM_i}, y_j, X_{ji}\}$. ID_{SM_i} and ID_{SP_j} are the identifiers of, respectively, the ith smart meter (SM_i) and j^{th} service provider (SP_j), y_i and y_j are the private keys of, respectively, SM_i and SP_j, and $X_{ij} = X_{ji}$ is their shared secret. Furthermore, public keys of SM_i and SP_j are denoted as Y_i and Y_j, respectively. SM_i generates random points M_1 and A_1 (A_1 is the encryption of M_1 for just SP_j, i.e., just SP_j can get M_1), encrypts ID_{SM_i} using M_1 as the key, computes verification token V_1, and submits request $\{V_1, A_1, T_1, EID_{SM_i}\}$ to SP_j.

Upon receiving the request, SP_j checks time, decrypts A_1 using its private key to get $M_1^{'}$, decrypts $EID_{SM_i}^{'}$ by $M_1^{'}$ and gets $ID_{SM_i}^{'}$ and checks the verification token to ensure the authenticity of SM_i and integrity of received message. Following, SP_j generates random points M_2 and A_2 (A_2 is the encryption of M_2 for just SM_i, i.e., just SM_i can get M_2), encrypts ID_{SP_j} using M_2 as the key, computes $SS^{'} = ((r_2 y_j)\ mod\ p) \cdot M_1^{'}$, $K = K_1 \| K_2 = KDF(ID_{SM_i}^{'} \| ID_{SP_j} \| SS^{'})$, and $V_2 = HMAC(K_1, ID_{SP_j} \| ID_{SM_i}^{'} \| T_2 \| M_1^{'} \| M_2 \| SK)$. It should be mentioned that "KDF" is a key derivation function that outputs K_1 and K_2 from shared secret $SS^{'}$. K_1 is used as the "HMAC" key and K_2 is the session key (SK). Finally, SP_j computes verification token V_2 and submits response $\{V_2, T_2, A_2, EID_{SP_j}\}$ to SM_i.

Upon receiving the response, SM_i checks time, decrypts A_2 using its private key to get $M_2^{'}$, decrypts $EID_{SP_j}^{'}$ by key $M_2^{'}$ and gets $ID_{SP_j}^{'}$, computes $SS^{'} = ((r_1 y_i) mod p) \cdot M_2^{'}$ and $K = K_1 \| K_2 = KDF(ID_{SM_i} \| ID_{SP_j}^{'} \| SS^{'})$, and checks verification token V_2. If the verification holds, it computes acknowledgement token $Ack = HMAC(K_1, ID_{SM_i} \| ID_{SP_j}^{'} \| T_3)$ and sends $\{Ack, T_3\}$ to SP_j.

Upon receiving the response, SP_j checks time and verifies the equality of $Ack \stackrel{?}{=} HMAC(K_1, ID_{SM_i}^{'} \| ID_{SP_j} \| T_3^{'})$ and if so, it accepts session key.

Dariush Abbasinezhad-Mood is with Computer Engineering Department, Imam Reza International University, Mashhad, Iran, e-mail: dariush.abbasinezhad@imamreza.ac.ir.

TABLE I
PROPOSED KAP BY WU ET AL. [1]

i^{th} Smart Meter (SM_i)	j^{th} Service Provider (SP_j)
Stored parameters: $\{ID_{SM_i}, ID_{SP_j}, y_i, X_{ij}\}$	Stored parameters: $\{ID_{SP_j}, ID_{SM_i}, y_j, X_{ji}\}$
Generates T_1 and selects random $r_1 \in Z_q^*$ $M_1 = ((r_1 y_i) \bmod p) \cdot P$ $A_1 = ((r_1 y_i) \bmod p) \cdot Y_j \bigoplus h(X_{ij} \| T_1)$ $EID_{SM_i} = ID_{SM_i} \bigoplus h(M_1)$ $V_1 = h(ID_{SM_i} \| ID_{SP_j} \| T_1 \| M_1)$	
$\xrightarrow[msg_1]{\{V_1, A_1, T_1, EID_{SM_i}\}}$	
	Generates T_2 and verifies $\|T_2 - T_1^{'}\| \leq \triangle T$ $M_1^{'} = (y_j^{-1} \bmod p) \cdot (A_1^{'} \bigoplus h(X_{ji} \| T_1^{'}))$ $ID_{SM_i}^{'} = EID_{SM_i}^{'} \bigoplus h(M_1^{'})$ $V_1^{'} \stackrel{?}{=} h(ID_{SM_i}^{'} \| ID_{SP_j} \| T_1^{'} \| M_1^{'})$ Selects random $r_2 \in Z_q^*$ $M_2 = ((r_2 y_j) \bmod p) \cdot P$ $A_2 = ((r_2 y_j) \bmod p) \cdot Y_i \bigoplus h(X_{ji} \| T_2)$ $EID_{SP_j} = ID_{SP_j} \bigoplus h(M_2)$ $SS^{'} = ((r_2 y_j) \bmod p) \cdot M_1^{'}$ $K = K_1 \| K_2 = KDF(ID_{SM_i}^{'} \| ID_{SP_j} \| SS^{'})$ $V_2 = HMAC(K_1, ID_{SP_j} \| ID_{SM_i}^{'} \| T_2 \| M_1^{'} \| M_2 \| SK)$
	$\xleftarrow[msg_2]{\{V_2, T_2, A_2, EID_{SP_j}\}}$
Generates T_3 and verifies $\|T_3 - T_2^{'}\| \leq \triangle T$ $M_2^{'} = (y_i^{-1} \bmod p) \cdot (A_2^{'} \bigoplus h(X_{ij} \| T_2^{'}))$ $ID_{SP_j}^{'} = EID_{SP_j}^{'} \bigoplus h(M_2^{'})$ $SS^{'} = ((r_1 y_i) \bmod p) \cdot M_2^{'}$ $K = K_1 \| K_2 = KDF(ID_{SM_i} \| ID_{SP_j}^{'} \| SS^{'})$ $V_2 \stackrel{?}{=} HMAC(K_1, ID_{SP_j}^{'} \| ID_{SM_i} \| T_2^{'} \| M_1 \| M_2^{'} \| SK)$ $Ack = HMAC(K_1, ID_{SM_i} \| ID_{SP_j}^{'} \| T_3 \| M_2^{'})$	
$\xrightarrow[msg_3]{\{Ack, T_3\}}$	
	Generates T_4 and verifies $\|T_4 - T_3^{'}\| \leq \triangle T$ Verifies $Ack \stackrel{?}{=} HMAC(K_1, ID_{SM_i}^{'} \| ID_{SP_j} \| T_3^{'} \| M_2)$

Note that $M_2^{'}$ is added to the computation of Ack as a remedy to fix the KCI attack issue. Red texts show the corrected typos.

III. KCI ATTACK ON THE KAP BY WU ET AL. [1]

In an authenticated KAP that resists the KCI attack, if long-term private keys of participant A are disclosed to attacker $\mathcal{A}$, $\mathcal{A}$ is not able to impersonate as participant B, i.e., one communicating with A [5], [7]. This property must be checked for the both sides. In the other words, in order to resist the KCI attack, when long-term private keys of participant A is disclosed, $\mathcal{A}$ must not be able to impersonate as participant B and when long-term private keys of participant B is disclosed, $\mathcal{A}$ must not be able to impersonate as participant A. In the proposed KAP by Wu et al. [1], if long-term private keys of SM_i are disclosed, $\mathcal{A}$ cannot impersonate as SP_j; however, $\mathcal{A}$ can easily impersonate as SM_i if long-term private keys of SP_j are disclosed. Details are as follows.

Table II shows the KCI attack on the proposed KAP by Wu et al. [1]. When long-term secrets of SP_j, i.e. $\{ID_{SP_j}, ID_{SM_i}, y_j, X_{ji}\}$ are disclosed to attacker $\mathcal{A}$, he/she performs the following steps to impersonate as SM_i. Attacker $\mathcal{A}$ generates T_1 and selects random $r_{\mathcal{A}} \in Z_q^*$, computes $M_{\mathcal{A}} = ((r_{\mathcal{A}} y_j^{-1}) \bmod p) \cdot Y_i$, $A_{\mathcal{A}} = (r_{\mathcal{A}} \bmod p) \cdot Y_i \bigoplus h(X_{ji} \| T_1)$, $EID_{\mathcal{A}} = ID_{SM_i} \bigoplus h(M_{\mathcal{A}})$, and $V_{\mathcal{A}} = h(ID_{SM_i} \| ID_{SP_j} \| T_1 \| M_{\mathcal{A}})$, and submits request message $\{V_{\mathcal{A}}, A_{\mathcal{A}}, T_1, EID_{\mathcal{A}}\}$ to SP_j.

Upon receiving the request, SP_j checks time, computes $M_{\mathcal{A}}^{'} = (y_j^{-1} \bmod p) \cdot (A_{\mathcal{A}}^{'} \bigoplus h(X_{ji} \| T_1^{'})) = ((y_j^{-1} r_{\mathcal{A}}) \bmod p) \cdot Y_i$ and $ID_{SM_i}^{'} = EID_{\mathcal{A}}^{'} \bigoplus h(M_{\mathcal{A}}^{'})$, and verifies the equality of $V_{\mathcal{A}}^{'} \stackrel{?}{=} h(ID_{SM_i}^{'} \| ID_{SP_j} \| T_1^{'} \| M_{\mathcal{A}}^{'})$, which certainly holds. In other words, the fabricated message by $\mathcal{A}$ has successfully passed the verification. Following, SP_j selects random $r_2 \in Z_q^*$ and computes $M_2 = ((r_2 y_j) \bmod p) \cdot P$, $A_2 = ((r_2 y_j) \bmod p) \cdot Y_i \bigoplus h(X_{ji} \| T_2)$, $EID_{SP_j} = ID_{SP_j} \bigoplus h(M_2)$, and $SS^{'} = ((r_2 y_j) \bmod p) \cdot M_{\mathcal{A}}^{'}$. The computed $SS^{'}$ by SP_j is equal to $SS^{'} = ((r_2 y_j) \bmod p) \cdot M_{\mathcal{A}}^{'} = ((r_2 y_j) \bmod p) \cdot (((y_j^{-1} r_{\mathcal{A}}) \bmod p) \cdot Y_i) = ((r_2 r_{\mathcal{A}}) \bmod p) \cdot Y_i$. Next, SP_j computes $K = K_1 \| K_2 = KDF(ID_{SM_i}^{'} \| ID_{SP_j} \| SS^{'})$ and $V_2 = HMAC(K_1, ID_{SP_j} \| ID_{SM_i}^{'} \| T_2 \| M_{\mathcal{A}}^{'} \| M_2 \| SK)$ and submits response $\{V_2, T_2, A_2, EID_{SP_j}\}$ to SM_i.

Upon receiving the request, attacker $\mathcal{A}$ checks time and computes $SS^{'} = ((r_{\mathcal{A}} y_j^{-1}) \bmod p) \cdot (A_2^{'} \bigoplus h(X_{ji} \| T_2^{'}))$. Evidently, the computed $SS^{'}$ by attacker $\mathcal{A}$ is identical to the computed one by SP_j, i.e., $SS^{'} = ((r_{\mathcal{A}} y_j^{-1}) \bmod p) \cdot (A_2^{'} \bigoplus h(X_{ji} \| T_2^{'})) = ((r_{\mathcal{A}} y_j^{-1}) \bmod p)((r_2 y_j) \bmod p) \cdot Y_i = ((r_{\mathcal{A}} r_2) \bmod p) \cdot Y_i$. In other words, attacker $\mathcal{A}$ has successfully achieved $SS^{'}$. Following, he/she computes $K = K_1 \| K_2 = KDF(ID_{SM_i} \| ID_{SP_j}^{'} \| SS^{'})$, can optionally check V_2, computes acknowledgment token $Ack = HMAC(K_1, ID_{SM_i} \| ID_{SP_j}^{'} \| T_3)$, and submits message $\{Ack, T_3\}$ to SP_j.

Upon receiving the response, SP_j checks time and verifies

TABLE II
KCI ATTACK ON THE PROPOSED KAP BY WU ET AL. [1]

Attacker $\mathcal{A}$ (Impersonates as SM_i)	j^{th} Service Provider (SP_j)
Disclosed parameters of SP_j: $\{ID_{SP_j}, ID_{SM_i}, y_j, X_{ji}\}$	Stored parameters: $\{ID_{SP_j}, ID_{SM_i}, y_j, X_{ji}\}$
Generates T_1 and selects random $r_{\mathcal{A}} \in Z_q^*$	
$M_{\mathcal{A}} = ((r_{\mathcal{A}} y_j^{-1}) \bmod p) \cdot Y_i$	
$A_{\mathcal{A}} = (r_{\mathcal{A}} \bmod p) \cdot Y_i \bigoplus h(X_{ji} \| T_1)$	
$EID_{\mathcal{A}} = ID_{SM_i} \bigoplus h(M_{\mathcal{A}})$	
$V_{\mathcal{A}} = h(ID_{SM_i} \| ID_{SP_j} \| T_1 \| M_{\mathcal{A}})$	
$\xrightarrow[msg_1]{\{V_{\mathcal{A}}, A_{\mathcal{A}}, T_1, EID_{\mathcal{A}}\}}$	
	Generates T_2 and verifies $\|T_2 - T_1^{'}\| \leq \triangle T$
	$M_{\mathcal{A}}^{'} = (y_j^{-1} \bmod p) \cdot (A_{\mathcal{A}}^{'} \bigoplus h(X_{ji} \| T_1^{'})) = ((y_j^{-1} r_{\mathcal{A}}) \bmod p) \cdot Y_i$
	$ID_{SM_i}^{'} = EID_{\mathcal{A}}^{'} \bigoplus h(M_{\mathcal{A}}^{'})$
	$V_{\mathcal{A}}^{'} \stackrel{?}{=} h(ID_{SM_i}^{'} \| ID_{SP_j} \| T_1^{'} \| M_{\mathcal{A}}^{'})$
	Selects random $r_2 \in Z_q^*$
	$M_2 = ((r_2 y_j) \bmod p) \cdot P$
	$A_2 = ((r_2 y_j) \bmod p) \cdot Y_i \bigoplus h(X_{ji} \| T_2)$
	$EID_{SP_j} = ID_{SP_j} \bigoplus h(M_2)$
	$SS^{'} = ((r_2 y_j) \bmod p) \cdot M_{\mathcal{A}}^{'}$
	$= ((r_2 y_j) \bmod p) \cdot (((y_j^{-1} r_{\mathcal{A}}) \bmod p) \cdot Y_i)$
	$= ((r_2 r_{\mathcal{A}}) \bmod p) \cdot Y_i$
	$K = K_1 \| K_2 = KDF(ID_{SM_i}^{'} \| ID_{SP_j} \| SS^{'})$
	$V_2 = HMAC(K_1, ID_{SP_j} \| ID_{SM_i}^{'} \| T_2 \| M_{\mathcal{A}}^{'} \| M_2 \| SK)$
	$\xleftarrow[msg_2]{\{V_2, T_2, A_2, EID_{SP_j}\}}$
Generates T_3 and verifies $\|T_3 - T_2^{'}\| \leq \triangle T$	
$SS^{'} = ((r_{\mathcal{A}} y_j^{-1}) \bmod p) \cdot (A_2^{'} \bigoplus h(X_{ji} \| T_2^{'}))$	
$= ((r_{\mathcal{A}} y_j^{-1}) \bmod p)((r_2 y_j) \bmod p) \cdot Y_i$	
$= ((r_{\mathcal{A}} r_2) \bmod p) \cdot Y_i$	
$K = K_1 \| K_2 = KDF(ID_{SM_i} \| ID_{SP_j}^{'} \| SS^{'})$	
$V_2 \stackrel{?}{=} HMAC(K_1, ID_{SP_j} \| ID_{SM_i}^{'} \| T_2 \| M_{\mathcal{A}}^{'} \| M_2 \| SK)$	
$Ack = HMAC(K_1, ID_{SM_i} \| ID_{SP_j}^{'} \| T_3)$	
$\xrightarrow[msg_3]{\{Ack, T_3\}}$	
	Generates T_4 and verifies $\|T_4 - T_3^{'}\| \leq \triangle T$
	Verifies $Ack \stackrel{?}{=} HMAC(K_1, ID_{SM_i}^{'} \| ID_{SP_j} \| T_3^{'})$

$Ack \stackrel{?}{=} HMAC(K_1, ID_{SM_i}^{'} \| ID_{SP_j} \| T_3^{'})$, which certainly holds so SP_j accepts the session key. Doing so, attacker $\mathcal{A}$ has successfully forged messages $\{V_{\mathcal{A}}, A_{\mathcal{A}}, T_1, EID_{\mathcal{A}}\}$ and $\{Ack, T_3\}$ and established session key with SP_j.

IV. KCI ATTACK FIX FOR THE PROPOSED KAP BY WU ET AL. [1]

The main reason for why $\mathcal{A}$ cannot impersonate as SP_j is the usage of $M_1^{'}$ in the computation of V_2. This is because $M_1^{'}$ can only be obtained by the private key of SP_j, i.e., y_j. In a similar manner, to fix the KCI attack, as shown in Table I, it would suffice to include $M_2^{'}$ in the computation of Ack. Doing so, having access to long-term private keys of SP_j, without private key of SM_i, i.e., y_i, $\mathcal{A}$ cannot impersonate as SM_i.

V. CONCLUSION

Quite recently, Wu et al. [1] have indicated the susceptibility of Hu et al.'s KAP [2] to KCI attack and proposed a security-enhanced one for secure communications of SMs and SPs in SG. In this paper, we have shown that their own KAP, i.e., the proposed one in [1], is still vulnerable to KCI attack. Accordingly, we suggest a simple modification to fix the KCI attack issue and corrected typos of their protocol. Our attack procedure gives some delicate hints to scholars to protect their schemes against the KCI attack in future researches.

REFERENCES

[1] Y. Wu, H. Guo, Y. Han, S. Li, and J. Liu, "A security-enhanced authentication and key agreement protocol in smart grid," *IEEE Transactions on Industrial Informatics*, 2024.

[2] S. Hu, Y. Chen, Y. Zheng, B. Xing, Y. Li, L. Zhang, and L. Chen, "Provably secure ECC-based authentication and key agreement scheme for advanced metering infrastructure in the smart grid," *IEEE Transactions on Industrial Informatics*, vol. 19, no. 4, pp. 5985–5994, 2022.

[3] D. Abbasinezhad-Mood, A. Ostad-Sharif, M. Nikooghadam, and S. M. Mazinani, "A secure and efficient key establishment scheme for communications of smart meters and service providers in smart grid," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 3, pp. 1495–1502, 2019.

[4] D. Abbasinezhad-Mood and M. Nikooghadam, "Efficient design and extensive hardware evaluation of an anonymous data aggregation scheme for smart grid," *Security and Privacy*, vol. 1, no. 2, p. e24, 2018.

[5] A. Shahidinejad and J. Abawajy, "An all-inclusive taxonomy and critical review of blockchain-assisted authentication and session key generation protocols for IoT," *ACM Computing Surveys*, vol. 56, no. 7, pp. 1–38, 2024.

[6] D. Abbasinezhad-Mood, S. M. Mazinani, M. Nikooghadam, and A. Ostad-Sharif, "Efficient provably-secure dynamic ID-based authenticated key agreement scheme with enhanced security provision," *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 2, pp. 1227–1238, 2020.

[7] B. LaMacchia, K. Lauter, and A. Mityagin, "Stronger security of authenticated key exchange," in *Provable Security: First International Conference, ProvSec 2007, Wollongong, Australia, November 1-2, 2007. Proceedings 1*. Springer, 2007, pp. 1–16.