Cryptanalysis and Improvement of Anonymous Authentication for Wireless Body Area Networks with Provable Security

Mahender Kumar
School of Computer & Systems Sciences
Jawaharlal Nehru University, India
Mahendjnu1989@gmail.com

Abstract: Recently, He et al. proposed an anonymous authentication for wireless body area networks and prove that their scheme is secure in the random oracle model. In this paper, we cryptanalysis the He et al.'s scheme and design an attack model against their scheme, in which adversary replaces a user's public key with a value of his choice and prove a key replacement attack besides client anonymity. Thus, their scheme is insecure and not suitable for implementing a secure WBAN system. Further, we point out a solution to improve their scheme.

Keywords: Attack model, WBAN, key replacement attack, Anonymous authentication.

1. Introduction

The improvement in medical science and technologies like embedded systems, wireless communication, and sensor technology has driven a significant enhancement in patient's health. Wireless body area networks (WBANs) is an emerging e-monitoring technology that allows real-time monitoring of patient health remotely [1]. It is well-known that the patient data is sensitive, and the nursing of patients relies on the data collected from the sensors to the medical institution. So, any adversarial attack on the data causes a disastrous problem to the patient. Several authentication mechanisms have been discussed to provide security to the WBAN system.

Recently, He et al. [2] proposed an anonymous authentication (AA) for the WBAN system. The scheme reviewed the Lui et al. AA scheme [3] for the WBAN system, and found that it is not suitable for a secure e-health care system as it susceptible to the impersonation attack. Besides, He et al. [2] improve and present an anonymous authentication scheme for the WBAN system and prove their security in the random oracle model. In this paper, we critically analyze the He et al. [2] and propose an attack model, where an adversary replaces the AP's public key with a value of his choice. Thus, we show that He et al. [2] susceptible to key replacement attacks. We also demonstrate that the scheme does not achieve client anonymity and mutual authentication attack, and hence insecure for the WBAN system.

The rest of the paper is organized as follows. Section 2 reviews the He et al. scheme. Section 3 proposes the attack model against He et al. scheme. We suggest an improvement in section 5. The conclusion is given in Section 4.

2. He et al.'s Definition, Security model, and AA scheme

2.1. Formal definition and security model

We give the formal definition and security model, which is the same as He et al.'s scheme [2]. For a complete description, we suggest the readers may refer to the original paper.

2.2. He et al. AA scheme

It involves the three phases: initialization, registration, and Authentication.

Initialization: Suppose an additive group G_1 and a multiplicative group G_2, both with prime order q. Suppose a generator of group G_1 be P and $e: G_1 \times G_1 \rightarrow G_2$ a bilinear pairings. Let two cryptographic hash functions are H and h, where $H: \{0,1\}^* \times G_1 \rightarrow G_1$ and $h: \{0,1\}^* \times G_2 \rightarrow Z_q^*$.

1. Given a security parameter k, network manager (NM) chooses an element as its master key $s_{NM} \in Z_q^*$ and sets pubic key $P_{NM} = s_{NM}P$, and publishes the system parameter $\{e, q, P, G_1, G_2, H, h, P_{NM}\}$.
2. Application provider (AP) chooses an element as its secret key $s_{AP} \in Z_q^*$ and computes public key $P_{AP} = s_{AP}P$.

Registration: The NM registers the client C as follows:

1. On given identity ID, C asks the NM for registration.
2. NM validates the clients ID and defines his right $right$. NM computes $Q_{id} = H(ID||right)$ and private key $S_{id} = s_{NM}\ Q_{id}$ and sends $\{S_{id}, right\}$ to C.
3. C keeps $\{S_{id}, right\}$ secretly.

Authentication: Here, C and AP authenticate each other by executing the following steps.

1. C chooses an element $x \in Z_q^*$ and timestamp T_c, Now, C computes $X = xP$, $X' = xP_{AP}$, $Q_{id} = H(ID||right)$, $v = H(ID, right, Q_{id}, P_{AP}, X, X', T_c)$, $k = h(X, X', T_c)$, $U = S_{id} + xvQ_{id}$, and encrypts $\{ID, right, U\}$ using $k\ as\ W = E_k(ID, right, U)$. Then, C outputs the data $\{W, X, T_c\}$ to the AP.
2. On given data $\{W, X, T_c\}$, SP ensures the validity of timestamp T_c. If valid, AP computes $X' = s_{AP}X$, $k = h(X, X', T_c)$, and decrypts the W using k to obtain the parameters $(ID, right, U)$. AP generates $Q_{id} = H(ID||right)$, $v = H(ID, right, Q_{id}, P_{AP}, X, X', T_c)$ and checks the parameters using equation $e(U, P)? = e(Q_{id}, P_{NM} + vX)$. If the equation does not holds, it rejects it. Otherwise, AP chooses an element $y \in Z_q^*$, computes $Y = yP$, $K = yX$ and session key $key = h(X, X', Y, K)$ and $Auth = h(W, X, X', Y, K, T_c)$. AP sends $\{Y, Auth\}$ to C.
3. On given parameter $\{Y, Auth\}$, C compute $K = xY$, and session key $key = h(X, X', Y, K)$. Then, AP ensures the validity of $Auth$ by checking $Auth =?\, h(W, X, X', Y, K, T_c)$. If it holds, authentication is completed otherwise, reject.

2.3. Security Model

We suggest the readers may refer to the original paper for complete description of their security model [2].

3. Cryptanalysis of He et al.'s AA scheme

In [2], the authors declare the AP's key pair generation in two positions; one is in the Create (AP) in the security model of section III (Page 4), and the other is in the initialization phase of section V (Page 6). However, the two claims are different. In Create (AP), the authors claim that AP does not generate its key pair. While, in the initialization phase, their description tells that AP generates its key pair and then, unfortunately, has the flaw.

In particular, the AP cannot issue their public and private keys on their own, and without any signature from NM. We show that an attacker can replace the AP's public key in order to break the mutual authentication attack and anonymity attack.

3.1. Attack model

In the registration phase of He et al. scheme, the NM registers each client in the network while it does not register the AP. AP generates its private-public key on its own, but due to the lack of public key certification, we assume that there must be an adversary who can replace AP's public key at his will. Thus, an attacker can fool AP by accepting a signature using a public key that has been supplied by him.

Suppose an adversary A, who replaces the AP public key and not given the master key. Adversary can access the following oracles according to the game played between the challenger Ch and A.

- *Setup*: On given security parameters, challenger Ch generates the pair of master and public parameters of NM. The public parametrs are given to A.
- *Enc([e,d],k,[m,c])*: On given an encryption query Enc(e,k,m), Ch checks if there is an entry of (k,m,c) in list L. If yes, Ch responds c to A; otherwise, Ch chooses a random number c, adds an entry (k,m,c) in list L and responds c to A. Similarly, on given a decryption query Enc(d,k,c), Ch checks if there is an entry of (k,m,c) in list L. If yes, Ch responds m to A; otherwise, Ch chooses a random number m, adds an entry (k,m,c) in list L and responds m to A.
- *RevealSecretKey*: On given an identity $ID \in \{0,1\}^*$, it outputs the corresponding private key of AP, if has been generated previously. Otherwise, abort the process.
- *ReplacePublicKey*: On given an identity ID and AP's public key (upk∗, usk∗), the original AP public/secret key pair of ID is replaced with (upk∗, usk∗) if ID has been created. Otherwise, no action will be taken
- *Send(P_i,m)*: On given query, Ch runs each steps of AA scheme and gives the corresponding message.
- *Reveal(P_i)*: On given query, Ch gives the session key of participant instance P_i to A.
- *Corrupt(P)*: On given query, Ch gives the secret key of participant P to A.
- *Test(P_i)*: On given query, Ch picks a random bit $b \in \{0,1\}$. C session key of participant P_i to A, if b=0. Otherwise, Ch picks a random number and gives it to A.

Suppose P(A) be the probability that A guess the correct bit b in the Test query. The advantage of A violates the indistinguishability of the AA scheme is defined as

$$Adv_{AA}^{AKE}(A) = |P(A) - \frac{1}{2}| \geq \varepsilon$$

3.2. AP's Public Key replacement attack

Suppose an adversary A is an insider of AP or a powerful attacker that computes the public/private key (P_{AP}^*, t). We demonstrate that the adversary A could impersonate client *C* that he is AP by replacing the original public key P_{AP} of AP with public key P_{AP}^*. Now A and client C run the following steps:

1. C chooses an element $x \in Z_q^*$ and timestamp T_c, Now, C computes $X = xP$, $X'^* = xP_{AP}^*$, $Q_{id} = H(ID||right)$, $v^* = H(ID, right, Q_{id}, P_{AP}^*, X, X'^*, T_c)$, and $k^* = h(X, X'^*, T_c)$. C computes $U^* = S_{id} + xv^*Q_{id}$ to give the forged signature on v^* under P_{AP}^*. Now, C encrypts forged signature ass $W^* = E_{k^*}(ID, right, U^*)$ under k^*. C outputs the parameter $\{W^*, X, T_c\}$ to the A.

2. On given data $\{W^*, X, T_c\}$, adversary A computes $X'^* = tX = \mathrm{t}xP = xP^*_{AP}$, $k = h(X, X'^*, T_c)$, and decrypt the W^* using k to obtain the parameters $(ID, right, U^*)$. A generates $Q_{id} = H(ID||right)$, $v^* = H(ID, right, Q_{id}, P^*_{AP}, X, X'^*, T_c)$. The parameter $\{U^*, v^*\}$ must satisfied the equation $e(U^*, P)? = e(Q_{id}, P_{NM} + v^*X)$. Now, A chooses an random element $b \in Z_q^*$, computes $Y^* = bP$, $K^* = bX = xbP$ and session key $key^* = h(X, X'^*, Y^*, K^*)$ and $Auth^* = h(W^*, X, X'^*, Y^*, K^*, T_c)$. A sends $\{Y^*, Auth^*\}$ to C.

   Now, we show that the data $\{U^*, X, T_c\}$ could pass the verification. Since $U^* = S_{id} + xv^*Q_{id}$, we check

$$\begin{aligned}
&e(U^*, P)\\
&= e(S_{id} + xv^*Q_{id}, P)\\
&= e(s_{NM}\, Q_{id} + xv^*Q_{id}, P)\\
&= e(Q_{id}(s_{NM} + xv^*), P)\\
&= e(Q_{id}, s_{NM}P + xv^*P)\\
&= e(Q_{id}, P_{NM} + v^*X)
\end{aligned}$$

   Now, A will get the parameter $\{W^*, X, T_c\}$ that will pass the validation using equation $e(U^*, P)? = e(Q_{id}, P_{NM} + v^*X)$ and adversary could successfully impersonate the C.

3. On given parameter $\{Y^*, Auth^*\}$, C compute $K^* = xY^*$, and session key $key = h(X, X', Y, K^*)$. Then, AP ensures the validity of $Auth$ by checking $Auth^* =? h(W^*, X, X'^*, Y^*, K^*, T_c)$. If it holds, authentication is accomplished, otherwise, reject it.

In this case, an adversary replaces the original public key with fraud public key P^*_{AP} and impersonates the client as an AP. Now, the client C sends the login message $\{W^*, X, T_c\}$ corresponding to the fraud public key P^*_{AP} to the A. The adversary receives the login message and generates the response message $\{Y^*, Auth^*\}$ and sends it to the client C where to check the validity of response and compute the session key. In Lemma 2 of the AA scheme [2], the probability E^{AP2C} (denotes the event that adversary A violates AP to C authentication) become 1 as A forge a response $\{Y^*, Auth^*\}$ after intercepting the login message $\{W^*, X, T_c\}$ corresponding to fake public key P^*_{AP}. Thus, He et al. AA scheme for WBAN is MA insecure.

3.3. Anonymity attack.

Here, we show that an attacker can know the identity of client C by replacing the original public key P_{AP} of AP with public key P^*_{AP}. Like key replacement attack, A can obtain the parameter $\{W^*, X, T_c\}$. A computes the computes $X'^* = s^*_{AP}X = s^*_{AP}xP = xP^*_{AP}$, $k = h(X, X'^*, T_c)$, and decrypt the W^* using k in order to obtain the parameters $(ID, right, U^*)$. Thus, He et al. scheme is insecure against client's anonymity attack.

3.4. Calculation Infeasibility

In He et al. scheme, if the cryptographic hash function $h: \{0,1\}^* \times G_2 \rightarrow Z_q^*$ that takes input string of any length with G_2 and outputs an integer in Z_q^*, then how to compute $k = h(X, X', T_c)$, $key = h(X, X', Y, K)$ and $Auth = h(W, X, X', Y, K, T_c)$.

4. Improvement of He et al.'s scheme

This section gives the improvement to withdraw the limitation of He et al. AA scheme. The improved Anonymous authentication scheme consists of three entities: NM, client and AP. It includes three phases: system initialization, registration and authentication and key establishment.

Initialization: Suppose an additive group G_1 and a multiplicative group G_2, both with prime order q. Suppose a generator of group G_1 be P and $e: G_1 \times G_1 \to G_2$ a bilinear pairings. Let two cryptographic hash functions are H and h, where $H: \{0,1\}^* \times G_1 \to G_1$ and $h: \{0,1\}^* \times G_2 \to Z_q^*$.

1. Given a security parameter k, network manager (NM) chooses an element as its master key $s_{NM} \in Z_q^*$ and sets pubic key $P_{NM} = s_{NM}P$, and publishes the system parameter $\{e, q, P, G_1, G_2, H, h, P_{NM}\}$.

Registration: The NM registers the client C and AP as follows:

1. On their identities, C and AP asks to the NM for registration.
2. NM validates the clients ID_C and defines his right $right$. NM computes $Q_C = H(ID_C||right)$ and private key $S_C = s_{NM}Q_C$ and sends $\{S_C, right\}$ to C.
3. NM validates the AP's ID_{AP} and computes $Q_{AP} = H(ID_{AP})$ and private key $S_{AP} = s_{NM}Q_{id}$ and sends S_{AP} to C.

Authentication: This algorithm enables C and AP to authenticate each other using their private keys and identities. The authors will give the complete implementation in future work.

5. Conclusion

In this paper, we analyze the He et al.'s AA scheme and show that their scheme is susceptible to key replacement attack by designing an attack model, where an attacker can replace the AP's public key with his public key. We also demonstrate that their scheme does not provide mutual authentication. Moreover, we point out the mistake in the proof of their scheme. Thus, their anonymous authentication scheme for secure WBAN is insecure. In the end, we give the improvement to withdraw the limitation of the He et al. AA scheme. In the future, the author will present the complement implementation.

References

[1] S. Movassaghi, M. Abolhasan, J. Lipman, D. Smith, and A. Jamalipour, "Wireless body area networks: A survey," *IEEE Commun. Surv. Tutorials*, vol. 16, no. 3, pp. 1658–1686, 2014.

[2] D. He, S. Zeadally, N. Kumar, and J.-H. Lee, "Anonymous authentication for wireless body area networks with provable security," *IEEE Syst. J.*, vol. 11, no. 4, pp. 2590–2601, 2017.

[3] J. Liu, Z. Zhang, X. Chen, and K. S. Kwak, "Certificateless remote anonymous authentication schemes for wirelessbody area networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 2, pp. 332–342, 2014.