Cryptanalysis of “Cloud Centric Authentication for Wearable Healthcare Monitoring System”

Chandra Sekhar Vorugunti  
PhD Third Year  
Chittoor - 517520, A.P  
sekar.diiict@gmail.com

Abstract:  
The privacy and security issues of information message dissemination have been well researched in typical wearable sensors. However, cloud computing paradigm is merely utilized for secure information message dissemination over wearable sensors. Sharing encrypted data with different users via public cloud storage is an important functionality. Therefore, many researchers proposed new cloud based user authentication scheme for secure authentication of medical data. Newly A.K.Das et al proposed a new user authentication scheme in which a legal user registered at the BRC will be able to mutually authenticate with an accessible wearable sensor node with the help of the CoTC. Though A.K.Das et al scheme counterattacks key cryptographic attacks, on subsequent in-depth analysis, we validate that their scheme has security downsides such as failure to counterattack ‘privileged insider attack’, which in turn leads to password guessing attack, identity guessing attack, unssr impersonation attack, session specific random number leakage attack etc.

Keywords—Wearable sensors, healthcare, bigdata, cloud computing, authentication, security.

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BRC</td>
<td>Bigdata registration center</td>
</tr>
<tr>
<td>CoTC</td>
<td>Cloud of Things centric</td>
</tr>
<tr>
<td>Ui; SNj</td>
<td>User and wearable sensor, respectively</td>
</tr>
<tr>
<td>SCi</td>
<td>Smart card of Ui</td>
</tr>
<tr>
<td>IDi; IDj</td>
<td>Unique identities of Ui and SNj, respectively</td>
</tr>
<tr>
<td>PWi</td>
<td>Password of Ui</td>
</tr>
<tr>
<td>K</td>
<td>Long-term secret key of the BRC</td>
</tr>
<tr>
<td>MKSNj</td>
<td>Master key of SNj</td>
</tr>
<tr>
<td>p; q</td>
<td>Large distinct secret prime numbers</td>
</tr>
<tr>
<td>n</td>
<td>Modulus, n = p * q</td>
</tr>
<tr>
<td>SKCCSNj</td>
<td>Secret key between CoTC and SNj</td>
</tr>
<tr>
<td>SKUjSN</td>
<td>Secret key between Ui and all wearable Sensors</td>
</tr>
<tr>
<td>SKCCUi</td>
<td>Secret key between CoTC and Ui</td>
</tr>
<tr>
<td>h( )</td>
<td>Cryptographic collision-resistant one way hash function</td>
</tr>
<tr>
<td>SK</td>
<td>Session key among entities Ui &amp; SNj</td>
</tr>
<tr>
<td>i; Rj; a; R2; R3</td>
<td>Random numbers/nonces</td>
</tr>
<tr>
<td>T</td>
<td>Maximum transmission delay</td>
</tr>
<tr>
<td>TCi; TCj1; TCj2</td>
<td>Temporal credentials</td>
</tr>
<tr>
<td>RTSi</td>
<td>Registration timestamp of Ui</td>
</tr>
<tr>
<td>i = j</td>
<td>Checks if the expression i matches with expression j</td>
</tr>
<tr>
<td>ns</td>
<td>Number of wearable sensor devices deployed initially</td>
</tr>
</tbody>
</table>
### User(Uᵢ) vs. Bigdata Registration center(BRC)

**User(Uᵢ):**
- Choose IDᵢ and PWᵢ
- Generate αᵢ, a.
- Calculate HIDᵢ = h(IDᵢ || αᵢ).
- HPWᵢ = h(PWᵢ || αᵢ).
- HPWᵢ₁ = HPWᵢ ⊕ a.
- Generate registration time RTSᵢ for Uᵢ.

**Bigdata Registration center (BRC):**
- Choose random number Rᵢ.
- {HIDᵢ, HPWᵢ₁} → Generate registration time RTSᵢ for Uᵢ.
- Choose random number Rᵢ.
- Compute Regᵢ = h((IDᵢ || Rᵢ).
- Aᵢ = Rᵢ ⊕ HIDᵢ ⊕ HPWᵢ₁
- TCᵢ = h(SKᵢ⁻¹ || HIDᵢ || RTSᵢ)
- Store {HIDᵢ, Rᵢ} into the database of CoTC.
- SCᵢ = {Aᵢ, SKᵢ⁻¹, Regᵢ, TCᵢ, n, h(.)}

**Compute:**
- Aᵢ₁ = Aᵢ ⊕ a.
- Regᵢ₁ = h(Regᵢ || PWᵢ).
- TCᵢ₁ = TCᵢ ⊕ h(PWᵢ || IDᵢ || αᵢ).
- βᵢ = αᵢ ⊕ h(IDᵢ || PWᵢ).
- SKᵢ⁻¹ = SKᵢ⁻¹ ⊕ h(αᵢ || PWᵢ)
- Replace Aᵢ, Regᵢ, SKᵢ⁻¹ and TCᵢ
- With Aᵢ₁, Regᵢ₁, SKᵢ⁻¹
- And TCᵢ₁, respectively.
- Store βᵢ into SCᵢ.
- Finally SCᵢ₁ = {Aᵢ₁, Regᵢ₁, SKᵢ⁻¹, TCᵢ₁, βᵢ, n, h(.)}.

**Fig.3. Summary of user registration phase**
Fig. 4. Summary of login and authentication phases
Choose $ID_i$ and $PW_i$.

1. $\{ ID_i, PW_i \}$

Compute

- $\alpha_i = \beta_i \oplus h(ID_i \parallel PW_i)$,
- $HID_i = h(ID_i \parallel \alpha_i)$,
- $HPW_i = h(PW_i \parallel \alpha_i)$,
- $TC_i = TC_i \oplus h(PW_i \parallel ID_i \parallel \alpha_i)$,
- $R_i^* = A_i^1 \oplus (HPW_i \oplus HID_i)$,
- $Reg_i^* = h(HID_i \parallel R_i^*)$.

Verify $Reg_i^* = h(Reg_i^* \parallel PW_i)$.

If so, ask $U_i$ to provide new password.

Select new Password $PW_i^{new}$

1. $\{ PW_i^{new} \}$

Compute $HPW_i^{new} = h(PW_i^{new} \parallel \alpha_i)$,
- $A_i^{new} = R_i^* \oplus (HPW_i^{new} \oplus HID_i)$,
- $Reg_i^{new} = h(Reg_i^* \parallel PW_i^{new})$,
- $TC_i^{new} = TC_i \oplus h(PW_i^{new} \parallel ID_i \parallel \alpha_i)$,
- $\beta_i^{new} = \alpha_i \oplus h(ID_i \parallel PW_i^{new})$,
- $SK_{U_i-SN}^{new} = SK_{U_i-SN}^{new} \oplus h(\alpha_i \parallel PW_i) \oplus h(\alpha_i \parallel PW_i^{new})$.

Replace $A_i^1$, $Reg_i^*$, $SK_{U_i-SN}$, $TC_i^1$ & $\beta_i$ with $A_i^{new}$, $Reg_i^{new}$, $SK_{U_i-SN}^{new}$, $TC_i^{new}$ & $\beta_i^{new}$ in $SC_i$, respectively.

Fig.5. Summary of password change/update phase

| User($U_i$) | Bigdata Registration center(BRC) |
I. Cryptanalysis of A.K. Das et al.’s Scheme

In this segment, we demonstrate that A.K. Das et al.’s authentication system is susceptible to several key cryptographic vulnerabilities, mainly privileged insider attack. We explained in following subdivisions.

In this segment, we cryptanalyze A.K. Das et al.’s system [4] and prove that A.K. Das et al. system is susceptible to security attacks. According to the threat model discussed above and depicted in [1,2,3,4], an attacker ‘E’ can intercept, eavesdrop and alter any message transmitted in the public communication channel. As discussed in [1,2,3,4], the attacker by carrying out power consumption analysis, can excerpt all the parameters deposited in the smart card [1,2]. Built on these two well accepted assumptions, the A.K. Das et al. system is vulnerable to subsequent cryptographic outbreaks.

1. Privileged Insider Attack

A.K. Das et al. in their prior work [2,3] cryptanalyzed few authentication schemes like Jiang et al. [1] by adopting privileged insider attack. In this attack, we assume that an insider of the Gate Way Node (GWN) / Bigdata Registration center (BRC) is having access to registration information sent by the legal user Ui, inside database (any data stored in BRC data base) and the lost/stolen smart card of the legal user Ui.
i.e The insider being an attacker tries to get the information from legal user $U_i$ and tries to perform various cryptographic attacks as described below:

Step 1: The insider ‘I’ as an attacker is having access to: $\{\text{HID}_i, R_i\}$ (U_i specific data stored in database of CoTC. $U_i$ submits $\{\text{HID}_i, \text{HPW}_i\}$). Finally the smart card contents $SC_i = \{A_i, \text{Reg}_i, SK_{U_i-SN_i}, TC_i, B_i, n, h(\cdot)\}$.

Step 2:

2.a) from $\{\text{HID}_i, R_i\}$ computes $\text{Reg}_i = h(\text{HID}_i || R_i)$.
2.b) from the S.C $\text{Reg}_i = h(\text{Reg}_i || \text{PW}_i)$, from above computed $\text{Reg}_i$, peform the password guessing attack on $\text{Reg}_i = h(\text{Reg}_i || \text{PW}_i)$, as only unknown parameter in $\text{Reg}_i$ is $\text{PW}_i$.

2.b.1) Pick a guessed password $\text{PW}_i^*$, and compute $\text{Reg}_i^* = h(\text{Reg}_i || \text{PW}_i^*)$.
2.b.2) Check if $\text{Reg}_i^* = \text{Reg}_i$. If there is a match, the insider is successful in finding the correct password $\text{PW}_i$ of the user $U_i$ and terminates the procedure. Otherwise, the insider discards this guessed password and guesses a new password, and goes to Step 2.b.1

It is thus clear that an insider of the CoTC/ BRC is successful in deriving the correct password $\text{PW}_i$ of a legal user $U_i$ in a relatively small dictionary. Hence, A.K Das et al.’s scheme fails to achieve password guessing attack.

Step 3: from the equation, $\beta_i = \alpha_i \oplus h(\text{ID}_i || \text{PW}_i)$, ($\beta_i$ is stored in $U_i$ S.C and is accessible to ‘I’). ‘I’ knows $\text{PW}_i$, $\beta_i$. $\beta_i$ can be rewritten as

3.1) $\alpha_i = \beta_i \oplus h(\text{ID}_i || \text{PW}_i)$.
3.2) $\text{CID}_i = (\text{HID}_i || R_i || h(\text{TC}_i || T_i))^2$ (mod n).

3.3) From $\text{TC}_i = \text{TC}_i \oplus h(\text{PW}_i || \text{ID}_i || \alpha_i) = \Rightarrow \text{TC}_i = \text{TC}_i \oplus h(\text{PW}_i || \text{ID}_i || \alpha_i)$ replacing $\text{TC}_i$ in above equation (3.2).

3.4) $\text{CID}_i = (\text{HID}_i || R_i || h(\text{TC}_i \oplus h(\text{PW}_i || \text{ID}_i || \alpha_i) || T_i))^2$ (mod n).
3.5) Guess an identity $\text{ID}_i^*$ and compute $\alpha_i^* = \beta_i \oplus h(\text{ID}_i^* || \text{PW}_i)$.
3.6) Substitute $\text{ID}_i^*$ and $\alpha_i^*$ in 3.4 to get $\text{CID}_i^* = (\text{HID}_i || R_i || h(\text{TC}_i \oplus h(\text{PW}_i || \text{ID}_i^* || \alpha_i^*) || T_i))^2$ (mod n). Check $\text{CID}_i^* = \text{CID}_i$ if it holds, the attacker find out the identity $\text{ID}_i$ and the random value $\alpha_i$.

It is thus clear that an insider of the CoTC/ BRC is successful in deriving the correct identity $\text{ID}_i$, $\alpha_i$ of a legal user $U_i$ in a relatively small dictionary. Hence, A.K Das et al.’s scheme fails to achieve preserving anonymity attack.

Step 4: Based on the above discussion, the attacker ‘I’ can compute the Message1 = $\{\text{CID}_i, \text{ID}_i, \text{SN}_{ij}, P_I, T_I\}$. Therefore, we can prove that A.K.Das et al is vulnerable to user impersonation attack.

Step 5: **Known session-specific temporary information attack**

The reveal or leakage of a session specific random numbers should not reveal the session key generated [1,2,3,4]. Despite, in A.K.Das et al system, if session specific random numbers i.e. R2 and R3 are leaked, the attacker can frame the session key.

REFERENCES


