A note on PUF-Based Robust and Anonymous Authentication and Key Establishment Scheme for V2G Networks

Milad Seddigh\textsuperscript{1} and Seyed Hamid Baghestani\textsuperscript{2}

\textsuperscript{1,2}Cyberspace Research Institute, University of Shahid Beheshti, Iran, Tehran
\textsuperscript{1}Milladseddigh7@gmail.com
\textsuperscript{2}se.baghestani@mail.sbu.ac.ir

February 17, 2024

Abstract

Vehicle-to-grid (V2G) provides effective charging services, allows bidirectional energy communication between the power grid and electric vehicle (EV), and reduces environmental pollution and energy crises. Recently, Sungjin Yu et al. proposed a PUF-based, robust, and anonymous authentication and key establishment scheme for V2G networks. In this paper, we show that the proposed protocol does not provide user anonymity and is vulnerable to tracing attack. We also found their scheme is vulnerable to ephemeral secret leakage attacks.

Keywords: Vehicle-to-grid, user anonymity, ephemeral

1 Introduction

After the development of “5G, smart grid (SG), and electric vehicle (EV)” technology, the vehicle-to-grid (V2G) is appearing as an attractive new network paradigm that has grasped the attention of scientific and industrial communities and has aroused their interest in using it \cite{TOD17, YPL+20, KO19}. Besides, V2G provides efficient charging services by creating two-way communication along with two-way electricity transmission between the power grid and electric vehicle (EV). But V2G networks are vulnerable to security threats since an attacker can control and eavesdrop on the transmitted messages in an insecure channel at any time \cite{SGCV17, HX16}.

Recently, Yu \cite{YP24} has proposed a key agreement scheme for the vehicle-to-grid network, in which there are three entities: the electrical vehicle user (\textit{U}_i), the utility service provider (USP), the fog server (FS), and the charging station (CS). USP is responsible for the registration of all participants and generates the secret credentials and parameters for all participants. An ordinary server can only process data from one vehicle at a time. For this reason, V2G requires a CS to perform parallel processing. Also, the FS controls and manages the CS and vehicle in real-time. When the vehicles move out of the smart city, the FS sends a message to the CS to connect to another FS. A user also communicates with CS and USP to be authenticated and obtain a session key. Although the scheme is fascinating, we find it flawed since it fails to maintain user anonymity and is vulnerable to tracing attacks. Also, this protocol cannot resist an ephemeral secret leakage attack \cite{YP24}.

2 Review of the Scheme

USP first selects a master private key \textit{MK}_\text{USP} and comprises the \textit{h(·)}. After that, USP publishes the \textit{h(·)} as public data. In this scheme, before the authentication key establishment (AKE) phase, \textit{U}_i and CS have to be registered with USP to access the useful V2G services and obtain the credential from USP.

The registration phase includes two parts that are performed via a secure channel: CS and \textit{U}_i registration phases.
1. Charging Station Registration Phase: CS generates an identity $ID_{CS}$ and a set of $(C^x_{CS}, R^x_{CS})$. Later on, CS sends $ID_{CS}, (C^x_{CS}, R^x_{CS})$ to the USP via a secure channel. Then, USP computes $Z_j = h(ID_{CS} \parallel ID_{USP} \parallel MK_{USP} \parallel R^x_{CS})$ and $c_j = h(ID_{CS} \parallel MK_{USP})$ and sends it to the CS. Ultimately, USP discards $Z_j$ and $c_j$ and keeps $(C^x_{CS}, R^x_{CS}), ID_{CS}$ in the database (DB). CS also stores $(C^x_{CS}, R^x_{CS}), Z_j, c_j$ securely.

2. User Registration Phase: Before AKE phase, $U_i$ registers within USP to access the useful V2G services and obtains the credential from USP. First, $U_i$ generates $ID_i$ and $PW_i$ and imprints BIO. Later on, $U_i$ selects a set of $(C^y_{U}, R^y_{U})$ and computes $RID_i = h(ID_i \parallel BIO)$ and $RPW_i = h(PW_i \parallel BIO)$ and then transmits $RID_i, RPW_i, (C^y_{U}, R^y_{U})$ to the USP. Then, USP calculates $X_i = h(RID_i \parallel MK_{USP} \parallel R^y_{U}), Q_i = X_i \oplus h(RID_i \parallel R^y_{U}) \oplus RPW_i$, and $W_i = h(RID_i \parallel R^y_{U} \parallel X_i \parallel RPW_i)$. After that, USP keeps $Q_i, W_i$ in the SC and sends the SC to the $U_i$. Then, $U_i$ calculates $E_i = X_i \oplus ID_{USP} \oplus MK_{USP}$ and stores $E_i, (C^y_{U}, R^y_{U})$ in the DB [YP24].

After the registration phase, $U_i$ must have a mutual authentication with USP via CS and establish a session key (SK) among $U_i$, CS, and USP. This authentication key establishment (AKE) phase is performed over an insecure channel (Table 1).

### 3 The Loss of Anonymity and Untraceability:

The goal of anonymity is that an attacker cannot extract the ID of the electrical vehicle user by intercepting messages transmitted in an insecure communication channel, and at a higher level, the attacker may not even be capable of finding any relation between two specific sessions. [YP24] claim that the attacker that eavesdrops on the exchanged messages during the AKE phase is unable to extract the real ID of the electrical vehicle user without knowing the “biometric (BIO), secret credentials ($X_i$), and PUF secret value $R^1_U$.

We find the claim unsound and misleading. In fact, an attacker can directly retrieve the pseudo-identity RID by capturing messages transmitted via the insecure channel. Note that the pseudo-identity is sent by the user in the registration phase and is unchanged in various sessions. Thus, the attacker can attribute different sessions created by the user $U_i$ to the pseudo-identity RID (Figure 1). Although the attacker cannot recover $ID_i$ from the equation $RID_i = h(ID_i \parallel BIO)$, the exposure of $RID_i$ cannot cause the anonymity of the user. In other words, identifier $ID_i$, characteristics of electrical vehicle user, uniquely corresponds to the pseudo-identifier $RID_i$, and the attacker can recognize the identity of the user by obtaining $RID_i$. As a result, after obtaining RID, the attacker can relate between the sessions and trace the user. In order to prevent this attack, the identity of the user must be changed and unique for each session.
Table 1: Summary of Authentication and Key Establishment Phase of R2AKE-V2G \cite{YP24}

<table>
<thead>
<tr>
<th>Phase</th>
<th>Protocol Inputs</th>
<th>Protocol Outputs</th>
<th>Protocol Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Initialization</td>
<td>$ID_U, PW_U$, and imprints BNO on SC</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Charging Station (CS)</td>
<td>$RBID, PW_{RB} = h(ID_{RB})$</td>
<td>$R, W, T_2$</td>
<td>Generates a random nonce $R_1$ and a timestamp $T_1$</td>
</tr>
<tr>
<td>3. Vehicle (V)</td>
<td>$X = h(ID_U</td>
<td></td>
<td>RBID</td>
</tr>
</tbody>
</table>

4 Ephemeral Secret Leakage Attack

A protocol is resistant to an ephemeral secret leakage attack if all random session numbers are leaked and all of the sensitive session parameters, such as the session key, remain secure. However, the Yu et al. \cite{YP24} scheme cannot resist an ephemeral attack. In the CK model, when all random session numbers such as $R_1$, $R_2$, and $R_3$ are leaked, the session key ($SK = h(R_1 || R_2 || R_3)$) remains insecure.

5 Conclusion

In this article, the protocol presented by Sungjin Yu et al. \cite{YP24} was analyzed, and the security analysis of the protocol demonstrated that their scheme is vulnerable to tracing attacks (loss of anonymity) and ephemeral secret leakage attacks. Since it does not meet proper anonymity standards, it is not optimal to implement on vehicle-to-grid networks.

References


