Cryptanalysis of a New Authentication Scheme with Anonymity for Wireless Environments

Chu-Hsing Lin and Chia-Yin Lee

Abstract

In 2004, Zhu and Ma proposed an authentication scheme with smart cards for wireless environments. Their scheme provides the anonymous feature for mobile users. In this article, we present a possible attack on their scheme to obtain the identity and the password of a legal user. Thus, the attacker can forge the legal user to visit a foreign network.

1. Introduction

User authentication is an important issue for wireless environments and there are many authentication schemes have been proposed in the literature. In 2004, Zhu and Ma [1] proposed an authentication scheme with smart cards for wireless environment. Their scheme provides the anonymous feature for mobile users. However, we will point out that their scheme suffers from the forge attack. An attacker can collect the transmission messages to obtain both of the identity and the password of a legal user.

2. Review of Zhu-Ma Scheme

In the Zhu-Ma’s user authentication scheme, there are three entities in the wireless environment: \( MN \) indicates a mobile user, \( HA \) indicates the home agent of the mobile use, and \( FA \) indicates the agent of a foreign network. When \( MN \) visits a new foreign network, \( FA \) needs to authenticate the mobile user through the user’s home agent \( HA \). The authentication protocol is described briefly as follows.

In the registration phase, a new user \( MN \) submits his \( ID_{MN} \) to the home agent \( HA \) for registration. \( HA \) generates a password for \( MN \) by computing \( PW_{MN} = h(N \| ID_{MN}) \), where \( N \) is \( HA \) ’s secret key. Then, \( HA \) issues a smart card, which contains \( r \), \( ID_{HA} \), and a strong one-way hash function \( h \), where \( r = h(N \| ID_{HA}) \oplus h(N \| ID_{MN}) \oplus ID_{HA} \oplus ID_{MN} \) and \( ID_{HA} \) is \( HA \) ’s

---

1 Department of Computer Science and Information Engineering, Tunghai University, 407 Taichung, Taiwan
identity. *HA* delivers the smart card and the password $PW_{MN}$ to the user through a secure channel.

When a user *MN* visits a new foreign network, *MN* begins the following steps for the login request.

1) *MN* enters the password $PW_{MN}$ to the device, then the device generates a secret random number $x_0$.
2) *MN* computes $n = r \oplus PW_{MN}$ and uses the current timestamp $T_{MN}$ to generate the temporary key $L$ by computing $L = h(T_{MN} \oplus PW_{MN})$.
3) *MN* encrypts $x_0$ with the key $L$ using a symmetric cryptosystem, indicated as $(x_0)_L$.
4) *MN* sends the message $\{n, (x_0)_L, ID_{HA}, T_{MN}\}$ to *FA*.

After receiving the login request from the user *MN*, *FA* first checks the timestamp $T_{MN}$ with current date and time. If the timestamp is valid, *FA* starts the following steps.

1) Generate a random number $b$, and compute its signature by computing $\text{signature}_{FA} = E_{KR_{FA}}(h(b, n, (x_0)_L, T_{MN}, \text{Cert}_{FA}))$, where $KR_{FA}$ is *FA*’s private key.
2) Generate the timestamp $T_{FA}$, and send the message $\{b, n, (x_0)_L, T_{MN}, \text{signature}_{FA}, \text{Cert}_{FA}, T_{FA}\}$ to *HA*, where *Cert*$_{FA}$ is *FA*’s certificate defined in X.509.

Receiving the message from *FA*, *HA* verifies the timestamp $T_{FA}$ and the certificate *Cert*$_{FA}$. If the timestamp and certificate are valid, *HA* computes the following steps.

1) Obtain *MN*’s identity by computing $ID_{MN} = h(N \parallel ID_{HA}) \oplus n \oplus ID_{HA}$.
2) Then *HA* verifies whether *MN* is a legal user or not. If the verification result is not true, *HA* sends the message “This user is an illegal user.” Otherwise, *HA* continues the next step.
3) Compute $L = h(T_{MN} \oplus h(N \parallel ID_{MN}))$.
4) Use $L$ to obtain $x_0$ by decrypting the message $(x_0)_L$.
5) *HA* generates a random number $c$, and generates its signature by computing $\text{signature}_{HA} = E_{KR_{HA}}(h(b, c, E_{KU_{FA}}(h(ID_{MN} \parallel x_0), \text{Cert}_{HA})))$, where $KR_{HA}$ and $KU_{FA}$ are the *HA*’s private key and *FA*’s public key, respectively.
6) Generate the timestamp $T_{HA}$, and send the message $\{b, c, E_{KU_{FA}}(h(ID_{MN} \parallel x_0)), \text{signature}_{HA}, \text{Cert}_{HA}, T_{HA}\}$ to *FA*.
After receiving the message, \( FA \) will verify the timestamp \( T_{FA} \) and the certificate \( Cert_{FA} \). If \( T_{FA} \) and \( Cert_{FA} \) are valid, \( FA \) knows that \( MN \) is a legal user. Then, it continues the following steps.

1) Issue a temporary certificate \( TCert_{MN} \) to \( MN \), and compute \( k = h(ID_{MN}) \oplus x_0 \).
2) Send \( \{(TCert_{MN})_k\} \) to \( MN \).

So far, \( FA \) has finished the process of authentication to \( MN \) and established the session key. After receiving the message from \( FA \), \( MN \) computes the session key \( k = h(ID_{MN}) \oplus x_0 \) and decrypts \( (TCert_{MN})_k \) to get \( TCert_{MN} \).

3. Cryptanalysis

By collecting the transmission messages, we present a possible attack on Zhu and Ma’s authentication protocol. We assume that a legal user \( MN \) wants to forge another legal user \( MN^* \). By using the following steps, the attacker can forge the legal user successfully if his/her smart card can be obtained.

1) Due to \( MN \) is a legal user of the home network so that \( MN \) can obtain \( h(N \| ID_{HA}) \) from the equation \( n = r \oplus PW_{MN} = h(N \| ID_{HA}) \oplus ID_{HA} \oplus ID_{MN} \).
2) By collecting an old login message \( n^* = h(N \| ID_{HA}) \oplus ID_{HA} \oplus ID_{MN^*} \), \( MN \) can obtain the legal user’s identity \( ID_{MN^*} \) from computing \( ID_{MN^*} = n^* \oplus h(N \| ID_{HA}) \oplus ID_{HA} \).
3) Having \( MN^* \)’s identity \( ID_{MN^*} \) and smart card, the attacker can enter the password \( PW_{MN^*} = 0 \) to obtain the value \( r^* \) by computing \( n^* = r^* \oplus PW_{MN^*} = r^* \oplus 0 \).
4) After knowing \( h(N \| ID_{HA}) \), \( ID_{MN^*} \) and \( r^* \), the attacker can obtain the real password of \( MN^* \), by computing \( PW_{MN^*} = r^* \oplus h(N \| ID_{HA}) \oplus ID_{HA} \oplus ID_{MN} \).
5) After that, the attacker can forge the legal user \( MN^* \) by using his/her password \( PW_{MN^*} \) to visit a foreign network.
4. Conclusion

From the above analysis, we know that the Zhu-Ma scheme suffers from the forge attack. The attacker can obtain a legal user’s identity and password easily. It means that the Zhu-Ma scheme is not secure enough for some applications with serious security requirement.

References