这是任振华的第一份LaTeX文档

任振华
2452503780@qq.com
计算机学院
数据科学与大数据专业
UESTC,Chengdu,Sichuan,611731

2020年2月28日

摘要

A user identity anonymous is am important propetry.

Keywords: LaTeXsdfsd

1 Introduction

In 2004,Zhu and Ma [1] proposed an authentication scheme with anonymity for wireless communication environ-ments. Later, Lee et al. [2] showed several security flaws of Zhu-Ma's scheme and then improved it.However, in2008,Wu et al.[3] showed that both Zhu-Ma's scheme and Lee et al.'s scheme still cannot provide anonymity andthen proposed an improvement to preserve anonymity. Nevertheless Zeng et al.[4] and Lee et al.[5] showed that Wuet al.'s scheme also cannot provide anonymity,respectively.

In 2011,Kang et al. [7] proposed an improved user authentication scheme based on both Wu et al.'s and Wei etal.'s scheme[3], [6] that guarantees strong user anonymity in wireless communications. However, this letter shows that the Kang et al.'s improved scheme also cannot provide user anonymity as they claimed.

2 Review of Kang et al.s Scheme

2.1 Initial Phase

When an MU registers

$$PW_{MU} = h(N \| ID_{MU}) \tag{1}$$

$$r_1 = h(N \| ID_{HA}) \tag{2}$$

$$r_2 = h(N \| TD_{MU}) \oplus ID_{NA} \oplus ID_{MU} \tag{3}$$

2.2 First Phase

$$n = h(T_{MU} \| r_1) \oplus r_2 \oplus PW_{MU} \tag{4}$$

$$L = h(T_{MU} \oplus PW_{MU}) \tag{5}$$

$$ID_{MU} = h(T_{MU} \| h(N \| ID_{HA})) \oplus n \oplus ID_{HA} \tag{6}$$

$$\begin{aligned} k &= h(h(h(h\Phi N \| ID_{MU})) \| x \| x_0) \\ &= h(h(PW_{MU})) \| x \| x_0 \end{aligned} \tag{7}$$

2.3 Second Phase

$$k = h(h(h(h(N \| ID_{MU})) \| x \| x_{i-1} \tag{8}$$

3 Anonymity Problem of Kang et al.s Scheme

$$\begin{aligned} n' =& h(T'_{MU} \| r_1 \oplus PW'_{MU} \\ =& h(T'_{MU} \| h(N \| ID'_{MU}) \oplus ID_{HA} \\ & \oplus ID'_{MU} \oplus PW'_{MU} \\ =& h(T'_{MU} \| r_1) \oplus h(N \| ID'_{MU} \oplus ID_{HA}) \\ & \oplus ID'_{MU} \oplus h(N \| ID'_{MU}) \\ =& h(T'_{MU} \| r_1) \oplus ID_{HA} \oplus ID_{MU} \end{aligned} \tag{9}$$

表 1: Notations

HA	Home Agent of a mobile user
FA	Foreign Agent of the network
MU	Mobile User
PW_{MU}	A password of MU
N	A strong secret key of HA
ID_A	Identity of an entity A
T_A	Timestamp generated by an entity A
$Cert_A$	Certiface of an entity A
$(X)_K$	Encryption of message X using symmetric key K
$E_{P_A}(X)$	Encryption of message X using public key A
S_{S_A}	Encryption of message X using private key A
$h(-)$	A one-way hash function
$\|$	Concatenation
$\oplus$	Bitwise exclusive-or opertaion

$$\begin{aligned}
ID'_{MU} =& n' \oplus (T'_{MU} \| r_1) \\
=& h(T'_{MU} \| r_1) \oplus ID_{HA} \oplus ID'_{MU} \\
& \oplus ID_{HA} \oplus h(T'_{MU} \| r_1) \\
=& ID'_{MU}
\end{aligned} \tag{10}$$

4 Conclusions

Acknowledgements