这是我的第一份 LaTeX 论文文档

杨睿妮 (1416333092@qq.com)
Department of Communication
UESTC, Chengdu, Sichuan, 611731

2021 年 3 月 24 日

Abstract

A user identity anonymity is an important property for roaming services. In 2011, Kang et al. proposed an improved user authentication scheme that guarantees user anonymity in wireless communications. This letter shows that Kang et al.'s improved scheme still cannot provide user anonymity as they claimed.

Keywords: *cryptanalysis, authentication, anonymity, wireless communications, security*

1 Introduction

2 Review of Kang et al.s Scheme

2.1 Initial Phase

Where an MU registers with his/her HA, the MU's identity ID_{MU} is submitted to the HA. After receiving ID_{MU} from MU, HA generates PW_{MU}, r_1 and r_2 as follows.

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

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

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

where N is a secret value kept by HA.HA stores ID_{HA}, r_1, r_2 and $h(\cdot)$ in the smart card of MU and then sends it with PW_{MU} to MU through a secure channel.

2.2 First Phase

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

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

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

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

2.3 Second Phrase

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

3 Anonymity Problem of Kang et al.s Scheme

$$\begin{aligned} n' =& h\left(T'_{MU}\|r_1\right) \oplus r'_2 \oplus PW'_{MU} \\ =& h\left(T'_{MU}\|r_1\right) \oplus h\left(N\|ID'_{MU}\right) \oplus ID_{HA} \\ & \oplus ID'_{MU} \oplus PW'_{MU} \\ =& h\left(T'_{MU}\|r_1\right) \oplus h\left(N\|ID'_{MU}\right) \oplus ID_{HA} \\ & \oplus ID'_{MU} \oplus h\left(N\|ID'_{MU}\right) \\ =& h\left(T'_{MU}\|r_1\right) \oplus ID_{HA} \oplus ID_{MU} \end{aligned} \tag{9}$$

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

4 Conlusions