Kuo-Hui Yeh, 2015. A lightweight authentication scheme with user untraceability. *Frontiers of Information Technology & Electronic Engineering*, **16**(4):259-271. [doi:10.1631/FITEE.1400232]

A lightweight authentication scheme with user untraceability

Key words: Authentication, Privacy, Security, Smart card, Untraceability

Contact: Kuo-Hui Yeh
E-mail: khyeh@mail.ndhu.edu.tw
ORCID: http://orcid.org/0000-0003-0598-761X

Introduction

- With the rapid growth of electronic commerce and associated demands on variants of Internet based applications, a variety of authentication schemes have been proposed to guarantee robust security and computational efficiency for service retrieval.

- Chang *et al*. (2014) introduced a formally provable secure authentication protocol with the property of user-untraceability. Unfortunately, the proposed scheme fails to provide the property of user-untraceability as claimed, and is insecure against user impersonation attack, server counterfeit attack, and man-in-the-middle attack.

The proposed method: login and authentication phase

$h(h(y\|\|r_2))^*$
$h(h(y\|\|r_2))^1$
$h(h(y\|\|r_2))^2$
…
$h(h(y\|\|r_2))^n$

Compute

$A=M_i \oplus h(PW_i||r_1)=h(y||r_2)$

$D=r_3 \oplus h(A)$

$B=N_i \oplus h(PW_i||r_1)=h(ID_i||x)$

$N_i'=N_i \oplus h(h(A)||r_3)$

$CID_i=ID_i \oplus h(N_i||h(A)||r_3)$

$C=h(N_i||h(A)||B||r_3)$

D, CID_i, N_i', C →

For each $h(h(y||r_2))^*$ *in* T, compute

$r_3^*=D \oplus h(h(y||r_2))^*$

$N_i^*=N_i' \oplus h(h(h(y||r_2))^*||r_3^*)$

$ID_i^*=CID_i \oplus h(N_i^*||\ h(h(y||r_2))^*||r_3^*)$

$B^*=h(ID_i^*||x)$

$C^*=h(N_i^*||h(h(y||r_2))^*||B^*||r_3^*)$

Check $C^*=C$?

Check the freshness of r_3^*

Check the validity of request

Compute $a=h(B^*||h(h(y||r_2))^*||r_4)$

← a, r_4

Check the freshness of r_4

Compute $a^*=h(B||h(A)||r_4)$

Check $a^*=a$?

Comparison results: security

Table 2 Security comparison of our proposed protocol and other schemes

Performance	Proposed scheme	Chang *et al.*, 2014	Tsai *et al.*, 2013
Freedom to choose and change password	Yes	No	Yes
User anonymity	Yes	No	Yes
Mutual authentication	Yes	Yes	Yes
Resistance to user impersonation attack	Yes	No	No
Resistance to server counterfeit attack	Yes	No	Yes
Resistance to man-in-the middle attack	Yes	No	Yes
Resistance to replay attack	Yes	Yes	Yes

Comparison results: performance

Number of operations			
Proposed scheme	Chang *et al.*, 2014	Kumari and Khan, 2013	Tsai *et al.*, 2013
19 HF+14 XOR	23HF+13 XOR	7 HF+9 MM+7 ME+ 11 XOR+5 E/D	14 HF+4 PM+ 9 XOR

HF: hash function; MM: modular multiplication;

ME: modular exponentiation; PM: ECC point multiplication; E/D: encryption/decryption

Conclusions

- Designing a secure but lightweight authentication scheme is a particular challenge owing to the difficult trade-off between security requirements and computation efficiency.
- We propose a lightweight authentication scheme with user untraceability.
- Our formal analysis and performance comparison have established that the security robustness and computation efficiency of our proposed authentication protocol can be guaranteed.