Kuo-Hui YEH, Kuo-Yu TSAI, Jia-Li HOU
Journal of Zhejiang University-SCIENCE C (Computers & Electronics),
2013, **14**(12):909-917. [doi:10.1631/jzus.C1300158]

Analysis and design of a smart card based authentication protocol

智慧卡身分鉴别的分析与设计

Key words: Authentication, Privacy, Security, Smart card

关键词：身分鉴别，隐私，安全，智慧卡

Security Requirements for Authentication

- Mutual authentication
- Session key agreement
- Resistance to replay attack, server spoofing attack, user impersonation attack, and man-in-the-middle attack
- Robust properties of session key security, forward secrecy, and known-key security
- No timestamp
- Freely chosen password
- Single registration
- Low communication and computation cost

Security Proof of the Proposed Protocol

Theorem 1 Let A be an adversary of the authenticated key exchange (AKE) security of the proposed protocol with fewer than q_s interactions with the communication entities, also asking q_h public one way hash-queries, i.e., $h(\ )$, and q_H private one-way hash-queries, i.e., $H(\ )$. Then

$$\mathrm{Adv}_P^S(A) \le \frac{q_s+q_h+{q_h}^2}{2^{l+1}} + \frac{{q_H}^2}{2^{k+1}} + \frac{q_s+q_H}{\Lambda_{AH}2^{k+1}}.$$

Improvement 1/2

Type of security	Chang and Cheng (2011)'s scheme	Our proposed protocol
Data confidentiality	No	Yes
Session key security	No	Yes
Forward security	No	Yes
Known-key security	No	Yes
Resistance to replay attack	Yes	Yes
Resistance to server spoofing attack	No	Yes
Resistance to user impersonation attack	No	Yes
Resistance to session key disclosure	No	Yes

Improvement 2/2

Phase	Computation cost	
	Chang and Cheng (2011)'s scheme	Our proposed protocol
Registration	2 Hash+1 XOR	3 Hash+3 XOR
Login	3 Hash+4 XOR	3 Hash+6 XOR
Authentication	14 Hash+17 XOR	14 Hash+19 XOR
Total	19 Hash+22 XOR	20 Hash+28 XOR

Note that some computations can be reused in our protocol