**سیویلیکا - ناشر تخصصی مقالات کنفرانس ها و ژورنال ها**
گواهی ثبت مقاله در سیویلیکا
CIVILICA.com

## عنوان مقاله:

(Novel Client to Server Password Authentication Key Exchange Protocol (N-C2S-P

## محل انتشار:

سیزهمین کنفرانس دانشجویی مهندسی برق ایران (سال: 1389)

تعداد صفحات اصل مقاله: 5

## نویسنده:

Ali Mackvandi

## خلاصه مقاله:

Up to now, many password authentication key exchange protocols (PAKE) have been proposed. The fundamental security aim of PAKE protocols is providing security against dictionary attacks. These kinds of protocols enable two clients to agree on a common session key, using pre-shared secret key (e.g.password). Unfortunately, most of the proposed protocols are vulnerable to well-known attacks while they are not feasible in the real world. In this paper, we analyze Hitchock et al.'s protocol and show that it is vulnerable to key compromise, ephemeral key compromise impersonation and off-line dictionary attacks. By analyzing the security attributes and performance of our protocol, we show that our proposed scheme can resist against many well-known attacks while it provides better efficiency in .compare with the analyzed protocol

## کلمات کلیدی:

Network security, Authentication, Session Key, Key Exchange, Public Key, Encryption

## لینک ثابت مقاله در پایگاه سیویلیکا:

https://civilica.com/doc/99108