Unknown Key Share Attack on STPKE' Protocol

R. Padmavathy[1] and Chakravarthy Bhagvati[2]

[1] Department of Computer Science and Engineering,
National Institute of Technology, Warangal, India
r_padma3@rediffmail.com
[2] University of Hyderabad, Hyderabad, India
chakcs@uohyd.ernet.in

Abstract. Three-party authenticated key exchange protocol is an important cryptographic technique in the secure communication areas, by which two clients, each shares a human-memorable password with a trusted server, can agree a secure session key. Recently, Lu and Cao proposed a simple three party password-based key exchange protocol (STPKE protocol). They claimed that their protocol is secure, efficient and practical. Unlike their claims, Kim & Choi proved that the STPKE protocol is vulnerable to Undetectable on-line password guessing attacks, and suggested an enhanced protocol (STPKE' protocol). In this paper, an Unknown key share attack on STPKE' protocol is demonstrated. The attack is implemented using a comprehensive set of experiments and reported. Additionally, the countermeasures to resist the above attack are discussed.

Keywords: STPKE' protocol, Unknown Key share attack, STPKE protocol.

1 Introduction

To communicate securely over an insecure public network, it is essential that secret session keys be securely exchanged. The shared session key may be subsequently used to achieve some cryptographic goals such as confidentiality or data integrity. Password-authenticated key exchange (PAKE) protocols [1,2] allow two or more specified parties to share a secret session key using only a human-memorable password. Password-based authenticated key exchange protocols, however, are vulnerable to password guessing attacks [3] since users usually choose easy-to-remember passwords. The goal of the attacker, is to obtain a legitimate communication party's password, can be achieved within a reasonable time. Thus, the password guessing attacks on password-based authenticated key exchange protocols should be considered realistic.

In general, the password guessing attacks can be divided into three classes [3].

Recently, Lu and Cao [4] proposed a simple three-party key exchange (STPKE) protocol based on the chosen-basis computational Diffie-Hellman (CCDH) assumption. They claimed that their protocol can resist various attacks and is superior to similar protocols with respect to efficiency. Kim and Choi [5] found that the STPKE protocol is vulnerable to undetectable on-line password guessing attacks by using formal description and proposed an alternative protocol (STPKE' protocol).

V.V Das et al. (Eds.): BAIP 2010, CCIS 70, pp. 605–608, 2010.

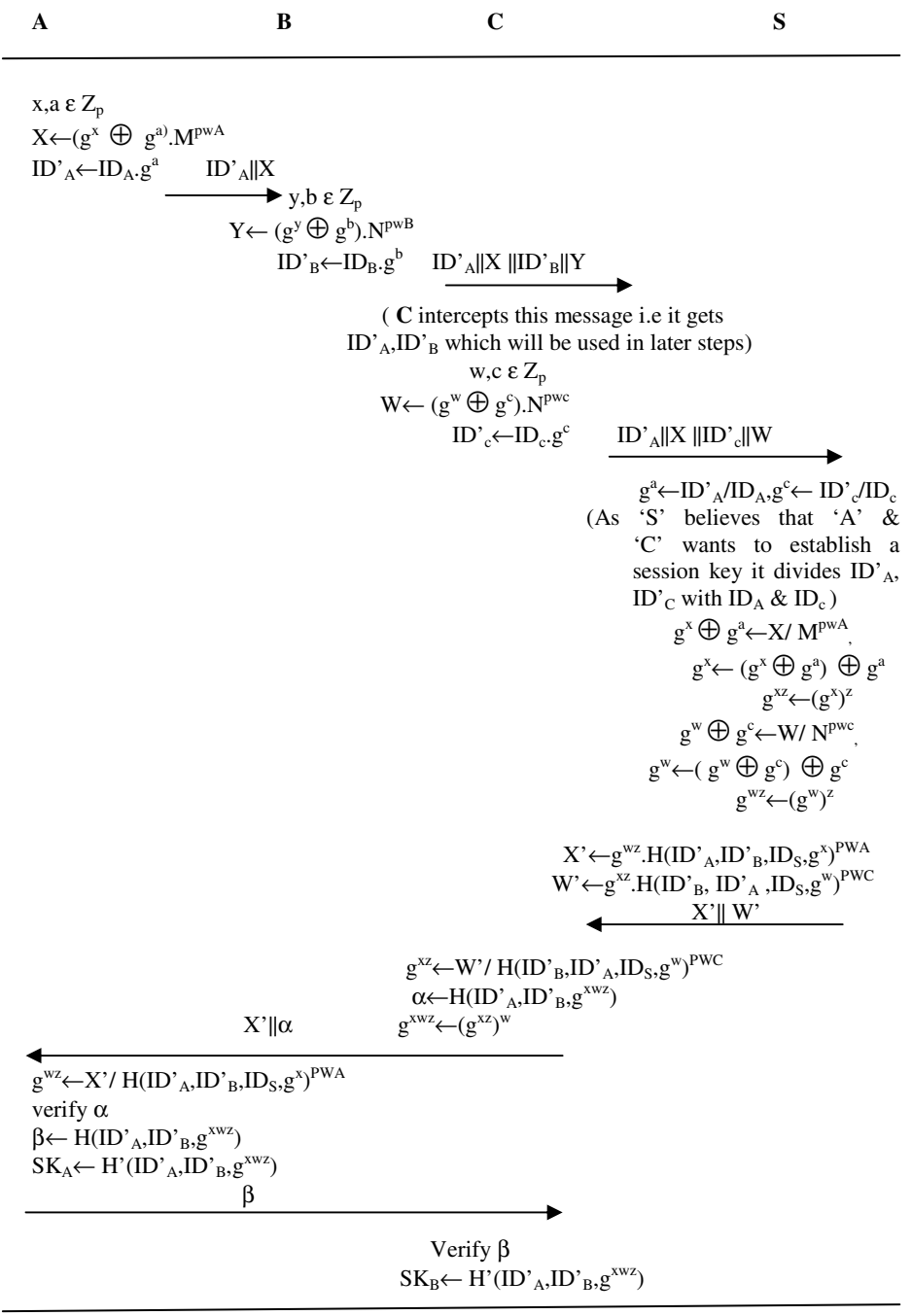

Fig. 1. Unknown key share attack on STPKE' protocol