New Authentication Scheme Based on a One-Way Hash Function and Diffie-Hellman Key Exchange

Eun-Jun Yoon and Kee-Young Yoo

Department of Computer Engineering, Kyungpook National University,
Daegu 702-701, South Korea
ejyoon@infosec.knu.ac.kr, yook@knu.ac.kr

Abstract. In 2004, Wu-Chieu proposed improvements to their original authentication scheme in order to strengthen it to withstand impersonation attacks. In 2005, Lee-Lin-Chang proposed improvements on Wu-Chieu's original scheme so that not only could it withstand a forgery attack, but it required less computational costs and it was suitable for mobile communication. The current paper, however, demonstrates that Wu-Chieu's improved scheme is vulnerable to an off-line password guessing attack and an impersonation attack by the use of a stolen smart card. Also, we demonstrates that Lee-Lin-Chang's scheme is vulnerable to a forgery attack. Furthermore, we present a new authentication scheme based on a one-way hash function and Diffie-Hellman key exchange in order to isolate such problems and to provide mutual authentication between the user and the remote system.

Keywords: Authentication, Password, Guessing attack, Smart card.

1 Introduction

User authentication is an important part of security, along with confidentiality and integrity, for systems that allow remote access over untrustworthy networks, like the Internet. As such, a remote password authentication scheme authenticates the legitimacy of users over an insecure channel, where the password is often regarded as a secret shared between the remote system and the user. With knowledge of the password, the user can use it to create and send a valid login message to a remote system in order to gain access. Meanwhile, the remote system also uses the shared password to check the validity of the login message and to authenticate the user. ISO 10202 standards have been established for the security of financial transaction systems that use integrated circuit cards (IC cards or smart cards). The smart card originates from the IC memory card which has been in the industry for about 10 years [1][2]. The main characteristics of a smart card are its small size and low-power consumption. In general, a smart card contains a microprocessor which can quickly manipulate logical and mathematical operations, RAM, which is used as a data or instruction buffer,

Y.G. Desmedt et al. (Eds.): CANS 2005, LNCS 3810, pp. 147–160, 2005.

and ROM which stores the user's secret key and the necessary public parameters and algorithmic descriptions of the executing programs. The merits of a smart card regarding password authentication are its simplicity and its efficiency in terms of the log-in and authentication processes.

In 1981, Lamport [3] proposed a remote password authentication scheme using a password table to achieve user authentication. In 2000, Hwang and Li [4] pointed out that Lamport's scheme suffers from the risk of a modified password table. Also, there is the cost of protecting and maintaining the password table. Therefore, they proposed a new user authentication scheme using smart cards to eliminate risks and costs. Hwang and Li's scheme can withstand replay attacks and it can also authenticate users without maintaining a password table. Later, Sun [5] proposed an efficient smart card-based user authentication scheme to improve the efficiency of Hwang and Li's scheme. In 2003, Wu-Chieu [6] proposed an improvement on Sun's scheme to make the protocol a user-friendly remote authentication scheme, through which the user can choose and change their password based on a secure channel. They claimed that their scheme provided effective authentication and also eliminated the drawback of Sun's scheme that required lengthy passwords.

In 2004, Wu-Chieu, [7], however, pointed out that their original scheme is vulnerable to an impersonation attack. They proposed an improvement to their original scheme in order to protect the scheme from an impersonation attack. At the same time, Yang-Wang [8] also pointed out Wu-Chieu's original scheme [6] is susceptible to a forgery attack. Thereafter, in 2005, Lee-Lin-Chang [9] proposed improvements to Wu-Chieu's original scheme so that not only could it withstand a forgery attack, but it required less computational costs and it was suitable for mobile communication. Lee-Lin-Chang claimed that their scheme provided effective authentication and it also eliminated the drawbacks of Wu-Chieu's original scheme.

The current paper, however, demonstrate that Wu-Chieu's improved remote authentication scheme [7] is vulnerable to an off-line password guessing attack [10], where an attacker can easily guess a legal users's password and can impersonate an legal users by using a stolen smart card. Also, we demonstrate that Lee-Lin-Chang's scheme is vulnerable to a forgery attack, where an attacker can easily masquerade as another legal users in order to access the resources of a remote system. Furthermore, we present an improved authentication scheme based on a one-way hash function and Diffie-Hellman key exchange to the schemes, in order to isolate such problems. As a result, the proposed scheme is more secure than Wu-Chieu's improved scheme and Lee-Lin-Chang's scheme. Also, it provides mutual authentication between the user and remote system and it has the same advantages as the other schemes. In addition, the proposed scheme does not require time synchronization or delay-time limitations between the user and remote system, unlike the other schemes. A timestamp-based authentication scheme is suitable for tightly synchronized system clocks, such as local area networks (LAN). For a large network where clock synchronization is difficult to work, such as wide area networks (WAN), mobile communication networks, and