A Secure Authentication Scheme for a Public Terminal Before a Transaction

Chin-Ling Chen[1], Yu-Yi Chen[2], and Jinn-Ke Jan[3]

[1] Department of Computer Science and Information Engineering,
Chaoyang University of Technology, Taichung, Taiwan 413, ROC
clc@mail.cyut.edu.tw
[2] Department of Management Information Systems,
National Chung Hsing University, Taichung, Taiwan 402, ROC
chenyuyi@nchu.edu.tw
[3] Department of Computer Science, National Chung Hsing University,
Taichung, Taiwan 402, ROC
jkjan@cs.nchu.edu.tw

Abstract. Due to the fast progress of the Internet, and with the increasing numbers of public terminals spread everywhere, people can access personal sensitive data or perform transactions easily through these public terminals. Identifying these public terminals is therefore a most urgent topic. We propose an efficient and secure scheme that meets real environmental conditions for authenticating these public terminals before conducting a transaction.

Keywords: Cryptography, security, public terminal, kiosk.

1 Introduction

Today, people can access personal sensitive data or perform financial transactions through public Internet kiosks that are located at malls, airports, hospitals, government agencies, etc.. Unverified kiosks are problematic for secure Internet services, as all service data is available in unencrypted form to the kiosk. Before performing personal data access or a transaction, people are required to enter their password or PINs to reliably authenticate themselves to the backend service server. However, using a public Internet access terminal creates an opportunity for persons with criminal intent to use a fake-terminal to cheat users. Currently, a counterfeit public terminal can keep users completely in the dark. The fake-terminal usually reports some plausible error messages to the users after the sensitive information has been revealed.

In accordance with these problems, in 1999, Asokan et al. [1] proposed solutions for different scenarios that correspond to different situations where the users are equipped with devices of different capacity, such as a personal trusted device with its own display, a smart card without a display, or a memory card. The Asokan et al.'s working model is shown in Fig. 1. Asokan et al.'s solutions assume the use of suitable existing authentication protocols such as Secure Sockets Layer (SSL) [5], KryptoKnight [2],

T. Enokido, L. Barolli, and M. Takizawa (Eds.): NBiS 2007, LNCS 4658, pp. 118–126, 2007.

and Kerberos [8] Later, Cheng et al. [4] modified part of Asokan et al.'s work using the public key algorithm concept. However, in a general and comprehensive pre-view, these solutions are not perfect because many interactive steps are necessary.

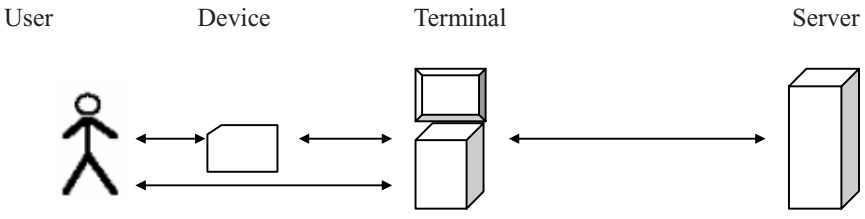

Fig. 1. Asokan et al.'s working model

In their proposals [1, 4], there were only four parties in their working model: the user, the personal trusted device, the public terminal and the server. Any public terminal can be activated by the user's trusted device to access various services from the server. These public terminals are susceptible to the fake-terminal attack: the attackers set up a fake terminal and steal the unsuspecting users' sensitive information, such as passwords, PINs or private e-mails, when the users attempt to use these fake terminals. Because unverified terminals are problematic for secure Internet service, all users will intend to authenticate the secure authenticated channel between the terminals and the server has already been set up before performing any transactions.

In consideration of the real environment, there should be a *PoC* (Point-of-Contact) server to handle all communications with kiosks [3, 6]. This concept was proposed by Laufmann [9] and the architecture was sketched as Fig. 2.

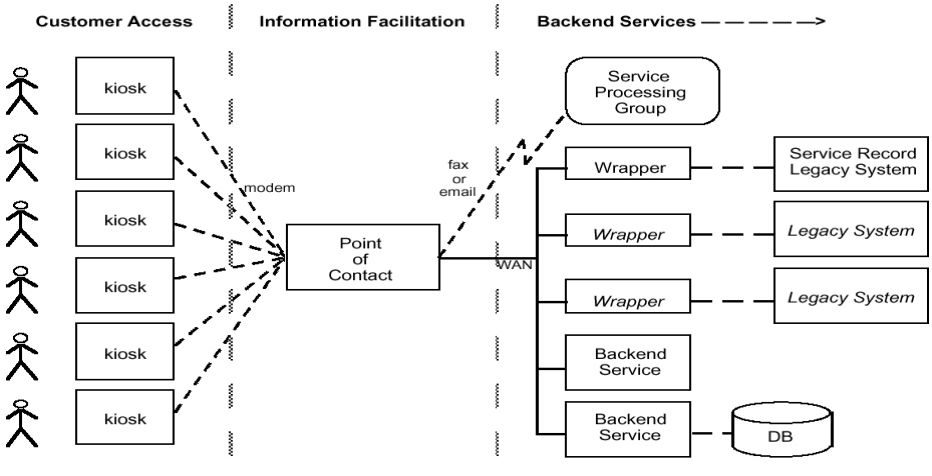

Fig. 2. Kiosk Support Service Architecture [9]