Evaluation of Encryption Procedure for User Attestation System Using a Cellular Phone

Noriyasu Yamamoto, Fukuoka Institute of Technology, Japan
Toshihiko Wakahara, Fukuoka Institute of Technology, Japan

ABSTRACT

To provide a low-cost and simple user attestation method, the authors previously proposed a method with strong authentication using the digital camera of a cellular phone. This method used 2D color code, and as such, there are some process costs like create and decode 2D color code. In this paper, the authors present an improved attestation system using a cellular phone and 2D color code. They compare the performance of the encryption methods and the efficiency of the proposed attestation method, which is confirmed using an experimental prototype system.

Keywords: Cellular Phone, Digital Camera, Password, Two-Dimensional Code, User Attestation System

INTRODUCTION

With the explosive growth of the Internet, many web sites, such as shopping sites and online banking sites have been globally setup and managed by Web 2.0 technology. In the network-based services and systems, a user attestation system is needed for identifying the right user. As the user attestation system, a popular reusable password method which was used in the early days of the Internet is still widely used despite the danger (Figure 1). This is because the reusable password method is simple and cost-effective.

However, this reusable password method is vulnerable to be used as a user attestation mechanism. With the increase of number of sites and services that require authentication, this system has many problems. Because it is managed by many one-password users, this system can be easy accessed by intrusion or improper password management.

In order to deal with these problems, we propose a new simple user attestation system using 2-Dimensional (2D) color code. The prototype system using the Quick Response (QR) code and cellular phone was implemented and the validity of the system was confirmed by experiments (Yamamoto & Wakahara, 2009). The system is easily realized by simply adding a
few lines in the server program and utilizing the cellular phone equipped with QR code reading function. But still remain some problems such as steal monitoring of the network and spy a cellular phone screen.

In another previous work, we proposed a new low cost and simple attestation system using 2D color code which solves the above vulnerability of reusable password and steal monitoring (Yamamoto & Wakahara, 2010). The efficiency of the system was confirmed by the experiments. But, there are still some problems such as process costs for 2D color code (Yamamoto & Wakahara, 2011).

In this paper, we propose an improved attestation system using 2D color code, which solves the process costs for 2D color code.

The paper structure is as follows. In the next section, we introduce the first user attestation system using a cellular phone. Then, we show some problems such as process time for 2D color code. After that, in order to deal with these problems, we present a new user attestation procedure. Then, we discuss system evaluation. Finally, conclusions are given.

USER ATTESTATION SYSTEM USING A CELLULAR PHONE

User Attestation System

The reusable fixed password system is widely used as a user attestation system between the server and client terminals. As this system is easily handled and has low cost, it has been widely used in previous systems. But this system has many security problems, because the user can lose the password and user password can be intercepted. Moreover, there are serious problems caused by confusing of many passwords requested in the most website and improper management of security operation with the recent development of the Internet. As the solutions for the vulnerabilities reusable password systems, many new systems such as one-time password system, IC card authentication or biometric authentication system, have been developed and operated (Davaanaym, Lee, Lee, Lee, & Lim, 2009; Thinn, 2009; Kumar, Hanmandlu, Madasu, & Lovell, 2009; Qu, Wang, Zheng, & Liu, 2010; Vetter, 2010).

One-time password system can deal with system vulnerabilities caused by the password theft and can reduce the complexity of password management. However, a mechanism for generating new disposable password is necessary.

In IC card authentication system, because it is difficult to replicate the same IC cards, strong authentication characteristics can be achieved. However, considerable cost is needed to introduce an IC card and IC card reader is also necessary in the user client. Then biometric authentication system is often used to realize the strong access control. Many people do not feel comfortable to the authentic systems based they need human characteristics, such as fingerprint, iris, and voiceprint. Also, the system needs a special hardware, which increases the cost and complexity of the authentication system.

In our study, the goal is to realize a strong authentication system the same as the existing fixed one-time password scheme with minimal
10 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the product's webpage:

www.igi-global.com/article/evaluation-encryption-procedure-user-attestation/67555?camid=4v1

This title is available in InfoSci-Journals, InfoSci-Journal Disciplines Computer Science, Security, and Information Technology. Recommend this product to your librarian:

www.igi-global.com/e-resources/library-recommendation/?id=2

Related Content

A Dynamic Load Balancing Strategy with Adaptive Thresholds (DLBAT) for Parallel Computing System
www.igi-global.com/article/a-dynamic-load-balancing-strategy-with-adaptive-thresholds-dlbate-for-parallel-computing-system/104764?camid=4v1a

Dynamic Dependent Tasks Assignment for Grid Computing
www.igi-global.com/article/dynamic-dependent-tasks-assignment-grid/54195?camid=4v1a

Securing Real-Time Interactive Applications in Federated Clouds
www.igi-global.com/chapter/securing-real-time-interactive-applications/55247?camid=4v1a
Supervised and Unsupervised Information Granulation: A Study in Hyperbox Design
www.igi-global.com/chapter/supervised-unsupervised-information-granulation/44699?camid=4v1a