

Title: User authentication method and user authentication system
Patent Application ID: US 20050160297
Filing Date: February 13, 2003
Priority Data: February 13, 2002
Patent ID: KR 716082
Patent ID: JP 3809441

ABSTRACT

The present invention is a user verification method and a user verification system, in which a password derivation pattern for each user is pre-registered into a verification server, and when a user is to use the system, the verification server generates a presented pattern and presents this to the user, the user inputs a password corresponding to the user's own password derivation pattern for the presented pattern, the verification server performs verification of the inputted password based on the presented pattern and the user's own password derivation pattern that was registered, and a verification result is then notified to the usage target system.

BACKGROUND

The present invention relates to a user verification method, and a user verification system for realizing the same.

In recent years, various information apparatuses, of which computers are representative, have become widespread. In particular, mobile phones provided with electronic mail functions and internet connection functions have spread extremely quickly, and have become necessary information items for people.

As this information society advances, illegitimate access to systems, and other such security problems, are becoming extremely important. In order to prevent illegitimate access to systems, traditionally, a common method is to use a pre-registered user ID and password to perform user verification. However, in order to answer to a need for even stronger security levels, proposals have been made for various user verification methods adapted to usage environments and objectives.

One of these is user verification system which limits terminal devices that can access a system. This method rests on a premise that the person who owns the terminal device is the person using it. For example, when accessing a given system from a mobile phone, a per-unit identification number that is assigned to that mobile phone can be used to achieve more secure user verification.

Furthermore, user verification using a random number table is also known. In this user verification using the random number table, random number table cards with random number tables written thereon are issued in advance to each user, and each time the user verification is performed, the system designates a character at a freely chosen position in the random number table, and has the user input it. Accordingly, since the inputted character changes each time, this method is effective against "eavesdropping".

In user verification performed on the system, leaking ("eavesdropping") of the password being used there results in causing extremely serious security problems. Therefore, management of the password by the user is extremely important, and each of the users having "responsibility" in their own actions is fundamental when considering the security problems of the system.

In general, different passwords used for the user verification are required for each system, and the formats thereof are varied. As such, users who use many systems must manage

many passwords, and password management becomes a burden for the user. The user, because of the nature of passwords, should strive to maintain the password in his or her memory, but when managing many passwords, it is not rare to write these down in a notebook or the like. Furthermore, users who find password management troublesome have set their passwords with characters that are easy to remember, or have set the same characters for the password for each system to manage them in an integrated fashion.

However, such actions by the user with respect to password management mean that the system is exposed to security risks. As long as the user acts in this way, the originally intended user verification with the password has essential security problems.

Furthermore, even when the user pays careful attention when managing the password, for example, there were still security problems, such as when the password being inputted into a terminal device in a shop is illegitimately observed, or when an "eavesdropping" mechanism gets built into the terminal device itself, whereby the password leaks to a third party.

Furthermore, even in user verification as described above where the mobile phones that can access the system are limited, when a user loses a mobile phone or it is stolen or comes into the possession of a third party, there is only the security level equivalent to when traditional user verification is performed, and thus this type of user verification had difficulties effectively preventing illegitimate access to the system. This was similar even in user verification using the random number tables.