Technology Profile Fact Sheet

Title: Tokeneer Password Modification

Aliases: Tokeneer

Technical Challenge: Provide a technique that will enhance identification and authentication mechanisms by upgrading existing password-based or biometric-based logon schemes to utilize token-based technology, resulting in use of a one-time password for each logon.

Description: This scheme provides enhancements to upgrade current logon schemes to utilize token-based technology. If a password is used, the password is sent directly to a token (e.g. smart-card). If a biometric verification is used, then the system performs a biometric verification on the user; if the user verifies, then a system-wide password is sent to the token.

In either case, the token encrypts the password using a previously stored key and a newly created key (known as the Modified and Next passwords respectively). These passwords are sent back to the Logon script. The Logon script then commands the card to destroy the key that made the modified password and labels the key used to make the next password as the key to make the modified password. When this procedure is performed, the password sent to the system changes with every logon.

Demonstration Capability: No.

Potential Commercial Application(s): Operating system logon products and user authentication functions that get embedded in any application.

Patent Status: A patent application has been filed with USPTO.

Reference Number: 1180