Method of Authenticating a User on a Network

Researchers at the University of South Florida have designed a compact and portable authentication/decryption device that incorporates a fingerprint biometric, token and decryption key that attaches to a Universal Serial Bus (USB) port of any computer.

Computer security and identity theft are certainly the most pressing issues of the new information age. Both subjects generate tremendous collective anxiety among executives, IT professionals, and home users alike. The current prevalent solutions to this problem seem focused mostly on the continued efforts to harden security over confidential information contained within enterprise systems. Hence, there is a need for compact portable system which provides highest level of authentication.

Inventors at USF have devised a biometric reader to interpret an individual’s fingerprint and compare with a filed biometric stored previously, a token that generates a password or a PIN and a decryption key that may be required to print the confidential data. These devices may be connected directly to a USB port of any client machine that is attached to an organization’s network and used to access the enterprise systems. This invention may serve as an ideal and cost effective solution that will effectively render any of an organization’s sensitive data that may be lost or stolen entirely useless to any unauthorized recipient.

ADVANTAGES:
- Cost effective
- Can be attached to the USB port of any computer
- Nearly impenetrable level of protection
- Portable token is tamper resistant

Compact and Portable Authentication Device with Biometrics

Tech ID # 05A052 Patent #: 8,127,142