Intelligent and Robust Multi-Factor Authentication Technology Available for Licensing

Multi-Factor Authentication (MFA) is the current trend to genuinely identify authorized users through the active authentication process using passwords, biometrics, cognitive behavior and others. As new authentication modalities are becoming available, they broaden the options for security researchers to devise more secure solutions to continuously authenticate to users of online systems. This invention focuses on describing a framework for continuous authentication where authentication factors are selected adaptively by sensing the users' operating environment (the devices, communication media, and surrounding conditions). This adaptive multi-factor decision support technique is available for exclusive licensing from the University of Memphis.

Applications

- Continuous, high – confidence, identity authentication for
  - Banking, including online funds transfer
  - Online testing in education and training settings
  - Secure access to Electronic Medical Records
- Deployable at different levels of Internet Computing
  - Application level (financial applications, email/business/personal applications, social applications)
  - User level (root user, administrators, guest users)
  - Document level (pdf containing application form, resume, document containing proprietary information, image/video containing confidential and sensitive footage)

Advantages

- Adaptive to changes in operational conditions
- Assures user identity during an interactive session and beyond the initial log-in
- If an authentication modality is compromised the system can adjust to using the remaining non-compromised modalities
- Scalable: New modalities can be added to the existing sets of modalities.
- Flexible enough to allow generating the operating/configuration parameters for the added authentication modalities as they become available.

The novel aspect of the invention lies in the development of an adaptive multi-factor authentication framework for secure and trustworthy access to data and services, and in the design of algorithms for determining the optimal authentication metrics and multi-factor authentication modalities. More specifically, this invention addresses the challenges of integrating the operating devices, surrounding conditions, types of applications, and differing modes of communication to adaptively select a subset of authentication modalities (biometric and non-biometric, active and passive) that are the most secure and trustworthy for the given operational conditions.

For further information on licensing this technology, please contact Kevin Boggs at kpboggs@memphis.edu or 901-678-1712