Revocable, Interoperable and User-Centric (Active) Authentication Across Cyberspace

Yan Sui, Computer Science Dept. IUPUI
Xukai Zou, Computer Science Dept. IUPUI
Eliza Y. Du, Qualcom, (Formal faculty at ECE, IUPUI)
Feng Li, Computer and Information Technology Dept. IUPUI

This work addresses fundamental and challenging user authentication and universal identity issues and solves the problems of system usability, authentication data security, user privacy, irrevocability, interoperability, cross-matching attacks, and post-login authentication breaches associated with existing authentication systems. It developed a solid user-centric biometrics based authentication model, called Bio-Capsule (BC), and implemented an (active) authentication system. BC is the template derived from the (secure) fusion of a user's biometrics and that of a Reference Subject (RS). RS is simply a physical object such as a doll or an artificial one, such as an image. It is users' BCs, rather than original biometric templates, that are utilized for user authentication and identification. The implemented (active) authentication system will facilitate and safely protect individuals' diffused cyber activities, which is particularly important nowadays, when people are immersed in cyberspace.

User authentication is the first guard of any trustworthy computing system. Along with people's immersion in the penetrated cyber space integrated with information, networked systems, applications and mobility, universal identity security& management and active authentication become of paramount importance for cyber security and user privacy. Each of three typical existing authentication methods, what you KNOW (Password/PIN), HAVE (SmartCard), and ARE (Fingerprint/Face/Iris) and their combinations, suffer from their own inherent problems. For example, biometrics is becoming a promising authentication/identification method because it binds an individual with his identity, is resistant to losses, and does not need to memorize/carry. However, biometrics introduces its own challenges. One serious problem with biometrics is that biometric templates are hard to be replaced once compromised. In addition, biometrics may disclose user's sensitive information (such as race, gender, even health condition), thus creating user privacy concerns. In the recent years, there has been intensive research addressing biometric template security and replaceability, such as cancelable biometrics and Biometric Cryptosystems. Unfortunately, these approaches do not fully exploit biometric advantages (e.g., requiring a PIN), reduce authentication accuracy, and/or suffer from possible attacks. The proposed approach is the first elegant solution to effectively address irreplaceability, privacy-preserving, and interoperability of both login and after-login authentication. Our methodology preserves biometrics' robustness and accuracy, without sacrificing system acceptability for the same user, and distinguishability between different users. Biometric features cannot be recovered from the user's Biometric Capsule or Reference Subject, even when both are stolen. The proposed model can be applied at the signal, feature, or template levels, and facilitates integration with new biometric identification methods to further enhance authentication performance. Moreover, the proposed active, non-intrusive authentication is not only scalable, but also particularly suitable to emerging portable, mobile computing devices. In summary, the proposed approach is (i) usercentric, i.e., highly user friendly without additional burden on users, (ii) provably secure and resistant to attacks including cross-matching attacks, (iii) identity-bearing and privacy-preserving, (iv) replaceable, once Biometric Capsule is compromised, (v) scalable and highly adaptable, (vi) interoperable and single signing on across systems, and (vii) cost-effective and easy to use.