Abstract

The focus of this thesis is to investigate solutions that shall enhance the security of remote client authentication for mCommerce applications on phones such as Smartphones or Tablet-PCs. This thesis details three innovative authentication schemes developed during the course of this study. These schemes are based on the use of localisation and obfuscation techniques in combination with multi-factor authentication to enforce the knowledge of "who, when, where and how" necessary for any remote client authentication attempt. Thus, assuring the mCommerce service provider about the genuine client as well as ensuring correct capturing and processing of the client's authentication data on the remote phone. The author of this thesis believes that these schemes, when developed on commercial mCommerce applications, shall enhance the service provider's trust into the received client data and therefore shall encourage more service providers to offer their mCommerce services via phone applications to their clients.

The first proposed scheme, called MORE-BAILS, combines multiple authentication factors into a One-Time Multi-Factor Biometric Representation (OTMFBR) of a client, so to achieve robust, secure, and privacy-preserving client authentication. Tests and trials of this scheme proved that it is viable for use in the authentication process of any type of mCommerce phone applications.

The second and third schemes, called oBiometrics and LocAuth respectively, use a new obfuscated-interpretation approach to protect the mCommerce application against misuse by attackers as well as to ensure the real-time and one-time properties of the client's authentication attempt. The novelty of combining biometric-based keys with obfuscated-interpretation tightly binds the correct mCommerce application execution to the genuine client. Furthermore, integration of the client's current location and real-time in the LocAuth challenge / response scheme eliminates the risk that an attacker can illegitimately re-use previously gathered genuine client authentication data in a replay attack.

Based on appropriate criteria, the MORE-BAILS, oBiometrics and LocAuth levels of security, user-friendliness and algorithms' ease-of-implementation are proven in experiments and trials on state-of-the-art Android-based Smartphones.