Efficient Multi-Factor Authenticated Key Exchange Scheme for Mobile Communications

Abstract:

Authenticated key exchange (AKE) is one of the most important applications in applied cryptography, where a user interacts with a server to set up a session key where pre-registered information (aka. authentication factor), such as a password or biometrics, of the user is stored. While single-factor AKE is widely used in practice, higher security concerns call for multi-factor AKE (MFAKE) schemes, e.g. combining both passwords and biometrics simultaneously. However, in some casually designed schemes, security is even weakened in the sense that leakage of one authentication factor will defeat the whole MFAKE protocol. Furthermore, an inevitable by-product arise that the usability of the protocol often drop greatly. To summarize, the existing multi-factor protocols did not provide enough security and efficiency simultaneously. In this paper, we make one step ahead by proposing a very efficient MFAKE protocol. We define the security model and give the according security analysis. We also implement our protocol on a smartphone and a cloud server. The theoretic comparisons and the experimental results show that our scheme achieves both security and usability

Introduction:

User authentication is a very important part for many information systems. In practice, it is often done via the following methods: — Password-Based Authentication: which is the most popular way, while quite insecure in some cases. E.g., in the Worst Password List compiled by SplashData, among 3.3 million passwords used for test, almost 20,000 were in fact ”123456”. The statistics show that most passwords in use are not so hard to guess. — Hardware-Based Authentication:With storage space for long secret keys and computation power for authentication, hardware provides higher security than password. But if it was stolen or lost, which happens in daily life occasionally, the authentication fails completely. — Biometrics-Based Authentication: which utilizes the unique and life-long invariant property of the biometrics. But it is not so reliable, e.g., biometric characteristics such as fingerprint can be easily “copied” without the awareness of the owner. Single-factor authentication only provides limited security, then combining these methods together

is considered as a good way to achieve higher security. But, in fact, many exiting multi-factor authentication schemes are quite insecure. For instance, in practice, SMS-based two-factor authentication was widely adopted and has been used in many applications, e.g., Gmail. But in the latest draft of the Digital Authentication Guideline, NIST announced its opinion, ". . . using SMS is deprecated, and may no longer be allowed in future releases of this guidance".