Cryptology ePrint Archive: Report 2013/167

Single Password Authentication

Tolga Acar and Mira Belenkiy and Alptekin Küpçü

Abstract: Users frequently reuse their passwords when authenticating to various online services. Combined with the use of weak passwords or honeypot/phishing attacks, this brings high risks to the security of the user's account information. In this paper, we propose several protocols that can allow a user to use a single password to authenticate to multiple services securely. All our constructions provably protect the user from dictionary attacks on the password, and cross-site impersonation or honeypot attacks by the online service providers.

Our solutions assume the user has access to either an untrusted online cloud storage service (as per Boyen [14]), or a mobile storage device that is trusted until stolen. In the cloud storage scenario, we consider schemes that optimize for either storage server or online service performance, as well as anonymity and unlinkability of the user's actions. In the mobile storage scenario, we minimize the assumptions we make about the capabilities of the mobile device: we do not assume synchronization, tamper resistance, special or expensive hardware, or extensive cryptographic capabilities. Most importantly, the user's password remains secure even after the mobile device is stolen. Our protocols provide another layer of security against malware and phishing. To the best of our knowledge, we are the first to propose such various and provably secure password-based authentication schemes. Lastly, we argue that our constructions are relatively easy to deploy, especially if a few single sign-on services (e.g., Microsoft, Google, Facebook) adopt our proposal.

Category / Keywords: cryptographic protocols / Password-based authentication, dictionary attacks, malware, honeypots, privacy, mobile

Publication Info: under submission

Date: received 22 Mar 2013

Contact author: akupcu at ku edu tr