OTPass-One Time Password As Service

Abstract:

—Conventional password-based authentication is considered inadequate by users as many online services started to affect each other. Online credentials are used to recover other credentials and complex attacks are directed to the weakest one of many of these online credentials. As researchers are looking for new authentication techniques, one time passwords, which is a two-factor authentication scheme, looks like a natural enhancement over conventional username/password schemes. The manuscript places the OTP verifier to the cloud to ease adoption of its usage by cloud service providers. When the OTP verifier is placed on the cloud as a service, other cloud service providers could outsource their OTP deployments as well as cloud users could activate their respective account on the OTP provider on several cloud services. This enables them to use several cloud services without the difficulty of managing several OTP accounts for each cloud service. On the other hand, OTP service provision saves inexperienced small to medium enterprises from spending extra costs for OTP provisioning hardware, software and employers. The paper outlines an architecture to build a secure, privacy friendly and sound OTP provider in the cloud to outsource the second factor of authentication. Cloud user registration to OTP provider, service provider activation and authentication phases are inspected. The security and privacy considerations of the proposed architecture are defined and analyzed. Attacks from outsiders, unlinkability properties of user profiles, attacks from curious service providers or OTP verifiers are mitigated within the given assumptions. The proposed solution, which locates the OTP provider in the cloud, is rendered robust and sound as aresult of the analysis.