
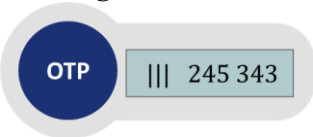



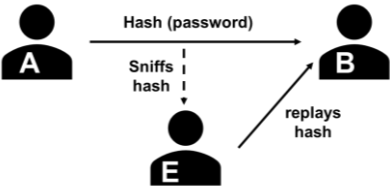




Name	Description
<b>OAuth</b> 	OAuth (Open Authorization) is an open standard for access delegation, commonly used as a way for Internet users to grant websites or applications access to their information on other websites but without giving them the passwords.
<b>One-Time-Password [OTP] generator</b> 	A device that generates a time-limited password (e.g., valid for 2 minutes). After this time, the password is no longer valid and must be generated again.
<b>Password RESET VS RECOVERY</b> 	Password Reset means setting a new password, while password Recovery means that we want to know what our password was (retrieval).
<b>Physical single-factor OTP Generator</b> 	Physical device (similar to a calculator) that generates one-time passwords. In past, some banks had them to enter online banking systems.
<b>Relying parties</b> 	A person or Agency who has received information that includes a certificate and a digital signature verifiable with reference to a public key listed in the certificate, and is in a position to rely on them.
<b>Replay Attack</b> 	Scenario: B requests an authentication password from A. A enters the password and B confirms the login. E intercepts this password (or hash) and presents himself as "A" to B. B accepts E as A, since he knows it from before (but does not know that the password is stolen).
<b>Segregation duties</b> 	In practice, this means that we protect banking systems more strictly than e.g. data on the result of marathon competitors.
<b>Time-based multi-factor OTP token</b> 	In practice, e.g., online banking, the user enters a password and is also provided with a one-time password (e.g., via SMS). This token (or SMS password) is time-limited to one minute.