Project Documentation

122294 Seung-jae Park

16011132 Hyun-min Ko

Our team project is improving an open source, "Google Authenticator Libpam" application. This application is a software token that implements two-step verification services using the Time-based One-time Password Algorithm (TOTP) and HMAC-based One-time Password Algorithm (HOTP), for authenticating users of applications by Google. This is a pluggable authentication module program which provides a six-digit one-time password which users must provide in addition to their username and password to log into Google services or other sites.

Typically, a user installs the Authenticator Libpam app on a device. To log into a site or service that uses two-factor authentication, the user provides user name and password to the site and runs the Authenticator Libpam app. The app displays an additional six-digit one-time password. The same password is independently generated by the site, which asks the user for it. The user enters it, thus authenticating the user's identity. For this to work, a set-up operation has to be performed ahead of time: the site provides a shared secret key to the user over a secure channel, to be stored in the Authenticator Libpam app. This secret key will be used for all future logins to the site. With this kind of two-factor authentication, mere knowledge of username and password is not sufficient to break into a user's account. The attacker also needs knowledge of the shared secret key or physical access to the device running the Authenticator Libpam app.

But the app's encryption algorithm is based on SHA-1, which is old and is considered not safe anymore. Recent trend of IT is altering SHA-1 to stronger one. So we will substitute encryption algorithm to much safe algorithm, such as SHA-256. And we'll demonstrate if it is working correctly.