A more secure way of fingerprint authentication

Popular Science Summary
Michaela Bergman

Today, many users of web services believe that placing their fingerprint on a fingerprint sensor is the safest way to protect their data or service from being misused by others. However, if the fingerprint data leaves the device it can be exposed to attacks and, if it looses its unique binding to a person, it will no longer be safe to use in any authentication process. This problem is one of the problems we investigate in this project. The result of this project is a multi-factor authenticator that includes fingerprint scanning, but it is combined with a time-based one time password to mitigate the risk of a fingerprint being compromised. The multi-factor authenticator is a part of the code flow defined in the OpenID Connect protocol, a widely used industry-standard protocol. The OpenID Connect protocol is a protocol that is an extension to OAuth 2.0, which is another popular protocol. To be able to easily integrate a system with another system (if needed), there are benefits with using industry-standard protocols for authorization and authentication, i.e., OAuth 2.0 and OpenID Connect. Therefore, the project also gives a summary of the OAuth 2.0 and the OpenID Connect protocols and how they are related to the implemented multi-factor authenticator.

The process of authentication is typically a part of the login process to any web service. The user presents a username or an email address to a security system to identify, and a password to verify its claimed identity. There are different authentication factors that can be used successively and the use of more than one factor is referred to as multi-factor authentication. Examples of authentication factors are *something that the user knows* (password, PIN), *something that the user has* (smartphone, ID card, one-time passwords), and *something that the user is* (fingerprint, iris, facial characteristics). If a user's password gets compromised by an attacker and multi-factor authentication is used, the attacker will still not be able to access the protected resources, since at least one more authentication factor is required. Hence, multi-factor authentication provides a higher level of security than single factor authentication. This project describes a multi-factor authenticator that includes a knowledge factor (username/password), an ownership factor (smartphone), a biometric factor (fingerprint), as well as another knowledge factor (time-based one-time password).

The main security advantage of the authenticator methods based on biometric factors is that there is a strong relationship between the user and its biometric data. However, it is important to emphasize the importance of the "fallback authenticator". If a user loses its smartphone, there should

be a way for the user to authenticate without it. If another authentication factor than biometric is used for the fallback authenticator, the fallback authenticator (and the original multi-factor authenticator) will not bring the same level of security. Hence, to maintain the security that the biometric factor of this multi-factor authenticator brings, the fallback authenticator must include a biometric factor. If the smartphone device with the fingerprint application is lost, there must be another biometric sensor (another smartphone or hardware device) available to the user.

Master's Thesis project: *Login hardening with Multi-factor Authentication*