Public-key Based Authentication with WebAuthn and FIDO

Martiño Rivera-Dourado, Marcos Gestal, José M. Vázquez-Naya

Authentication is the process of validating the user identity in a system for them to be authorized accordingly. Nowadays, passwords are the most used authentication method in information systems, including critical ones such as those holding medical data. However, passwords entail many security problems and are threatened by attacks like phishing and the installation of keyloggers, which allow an attacker to obtain the secret password that authenticates a user and, therefore, eventually getting access to the system.

For this reason, there is a need for new advanced authentication protocols that complement or even replace passwords. During the last years from 2014, the FIDO Alliance and the W3C have developed FIDO CTAP and W3C WebAuthn API that constitute a new authentication method that makes use of hardware devices known as security keys or authenticators. These devices allow a user to benefit from public-key cryptography to authenticate in a system only by pressing a button.

In this context, we have developed a debugging tool for the protocol, and we have designed two scenarios in the Network Access Control field: using WebAuthn API together with a Captive Portal and using FIDO CTAP together with the Extensible Authentication Protocol framework to allow users to use security keys to connect to an IEEE 802.11 or IEEE 802.3 Local Area Networks.