cryptStick: Development of a Portable Cryptographic Device for Online Authentication

Schlitt, Aaron (School: Albert-Schweitzer-Schule Kassel)

The use of insecure passwords and growing numbers of security breaches in online services are becoming a bigger threat to both companies as well as people individually. While there are many solutions available to make password-based authentication more secure, these are unable to solve the fundamental problems created by the use of passwords for logging in.   The goal of the cryptStick was to provide a more secure and easier to use solution for online authentication. For this purpose it uses cryptographic algorithms in an external USB device to log in to internet services. The external cryptographic key storage it provides protects from compromised computers and mobile devices. Additional safety measures were implemented to mitigate the concerns that might arise from the use of a physical device for security. In combination with the user's smartphone the stick itself is fully encrypted to prevent physical attacks and to allow for two-factor-authentication. Hardware was chosen to only include easily available and affordable components to make this form of authentication available to as many people as possible at a price of less than 10$. To ensure ease of use, tests were conducted with people with different backgrounds in technology as well as from different age groups. Test results were used to make improvements from one prototype to the next.   Ultimately, I was able to engineer a solution to online authentication that is both easier to use as well as more secure than traditional methods while at the same time keeping it affordable for everyone.