Password security relies heavily on the choice of password by the user but also on the one-way hash functions used to protect stored passwords. To compensate for the increased computing power of attackers, modern password hash functions like Argon2, have been made more complex in terms of computational power and memory requirements. Nowadays, the computation of such hash functions is performed usually by the server (or authenticator) instead of the client. Therefore, constrained Internet of Things devices cannot use such functions when authenticating users. Additionally, the load of computing such functions may expose servers to denial of service attacks. In this work, we discuss client-side hashing as an alternative. We propose Clipaha, a client-side hashing scheme that allows using high-security password hashing even on highly constrained server devices. Clipaha is robust to a broader range of attacks compared to previous work and covers important and complex usage scenarios. Our evaluation discusses critical aspects involved in client-side hashing. We also provide an implementation of Clipaha in the form of a web library and benchmark the library on different systems to understand its mixed JavaScript and WebAssembly approach's limitations. Benchmarks show that our library is 50% faster than similar libraries and can run on some devices where previous work fails.

And the authors:
Francisco Blas Izquierdo Riera Chalmers
Magnus Almgren Chalmers
Pablo Picazo-Sanchez Halmstad
Christian Rohner Uppsala