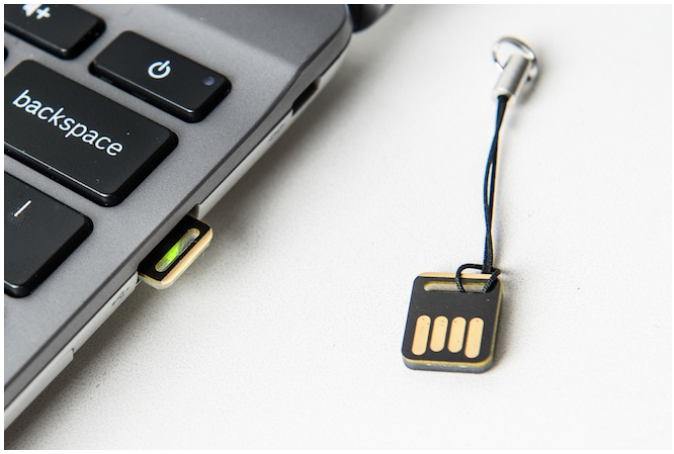
Google does not believe in the password any more-- the search giant is working on a yet unnamed security protocol designed for integration with authentication devices.



In an IEEE Security & Privacy Magazine paper Google security VP Eric Grosse and engineer Mayank Upadhyay outlines plans different means for logging into the websites of the near future, such as SIM cards, authentication keys and NFC-enabled finger rings.

“Along with many in the industry, we feel passwords and simple bearer tokens such as cookies are no longer sufficient to keep users safe,” Grosse and Upadhyay write. “We’ll have to have some form of screen unlock, maybe passwords but maybe something else... But the primary authenticator will be a token like this or some equivalent piece of hardware.”

The problem with such a security system is getting other websites to adopt the Google approach. Grosse and Upadhyay insist the security protocol they describe is Google-independent, and only requires a browser update from the user's side.

Google already has at least one partner-- Yubikey cryptographic device maker Yubico. Such devices connect to PCs via either USB or NFC and require a single password to handle multiple systems.

Currently the Google security proposals are in testing, but should the industry agree with the search giant we might see an end to increasingly long and complicated passwords. Until then, Google also offers a 2-step authentication process...

Go Google Protocol & Yubico Identity Vision

Go IEEE Security & Privacy Magazine