Seamless Authentication with Pico

Kat Krol, Seb Aebischer, David Llewellyn-Jones, Claudio Dettoni, and Frank Stajano
Computer Laboratory, University of Cambridge
Email: firstname.lastname@cl.cam.ac.uk

In this talk, we present seamless authentication as a challenge in terms of anticipating user preferences and offering them options to balance their need for convenience, security, and control. We describe our ongoing trial of the Pico password replacement scheme in which we explore user experiences with different options for a seamless login using Bluetooth.

These days, the industry strives for seamless interactions – content sharing at the press of a button, devices reacting to voice and gestures, cars driving themselves. Security, and authentication more specifically, has been at odds with this. Authentication used to be based on the *interrupt–authenticate* model, where the user is interrupted in whatever they are doing and asked to enter a password – otherwise they are prevented from continuing with their tasks. Luckily, this approach to authentication is slowly changing. Notable examples of more seamless logins include behavioural biometrics where the user is authenticated based on voice, typing rhythm etc. [1]. Although the proposition of a seamless login is very promising, it might go against user expectations. Recent research has shown that users translate difficult security to mean good security [2] according to the saying "If it's not hurting, it's not helping." The visibility of a security-related process gives users reassurance that things are done right [3].

Important factors to ensure user acceptance are accuracy and privacy/security [4]. A system providing seamless authentication would need to be accurate because false positives (inadvertent logins) would undermine users' security and privacy and false negatives (failure to log in) would result in a lack of availability. Both cases would undermine user acceptance of the system. Previous research shows that automated processes can also leave the user outside control as users worry that if "The computer says *no*", they would be left stranded without access [5]. Although this is no different to using a password, users there have the perception or illusion that they can attribute failure to log in to their own actions and regain access. They do not feel this way when security processes are automated and opaque.

The Pico Team at the University of Cambridge Computer Laboratory [6] is working on a password replacement scheme called *Pico* [7]. One of its aims is to reduce the cognitive and physical burden of entering credentials. Although first conceived as a hardware token, we are currently working on its implementation as a smartphone app. At the moment, the Pico app offers two modalities of login: scanning a QR code or using Bluetooth. Bluetooth-based login with Pico has the potential to offer seamless continuous authentication: the user would be logged out when their phone leaves the Bluetooth range of their computer, and logged back in upon return. We are currently conducting a user trial to explore user perceptions of and experiences with these three login modes over Bluetooth:

- *On/off permanently*: The user can choose to always be automatically logged in when their phone is in range.
- *Show notification*: When the user's phone is within range, Pico puts up a notification that the user taps on to be logged in.
- *One-off login*: Each time they want to log in, the user has to press a button inside the app.

These three options vary in how much control, security and convenience they give to the user. For example, while *on permanently* logs them in whenever their phone is within the Bluetooth range of their computer, a *one-off login* logs them in only once when they express the desire to authenticate. The *show notification* mode is meant to give the user the convenience of being alerted when there is a computer within range but leaves them the choice if they want to be logged in to it. In our eight-week trial, we ask study participants to use each login mode for two weeks and then choose their preferred one for the final two weeks. Through our study, we seek to explore user perceptions of seamless authentication, and at the same time choose a suitable default setting for the release of the Pico app.

References

[1] K. S. Killourhy, R. Maxion *et al.*, "Comparing anomaly-detection algorithms for keystroke dynamics," in *IEEE/IFIP International Conference on Dependable Systems & Networks*. IEEE, 2009, pp. 125–134.
[2] K. Krol, C. Papanicolaou, A. Vernitski, and M. A. Sasse, " 'Too Taxing on the Mind!' Authentication Grids are not for Everyone," in *Human Aspects of Information Security, Privacy, and Trust (HAS), HCI International 2015*, vol. LNCS 9190, 2015, pp. 71–82.
[3] S. Ruoti, N. Kim, B. Burgon, T. van der Horst, and K. Seamons, "Confused Johnny: When automatic encryption leads to confusion and mistakes," in *Symposium on Usable Privacy and Security (SOUPS)*. ACM, 2013.
[4] K. Krol, E. Philippou, E. De Cristofaro, and M. A. Sasse, " 'They brought in the horrible key ring thing!' Analysing the Usability of Two-Factor Authentication in UK Online Banking," in *NDSS Workshop on Usable Security (USEC 2015)*, 2015.
[5] K. Krol, S. Parkin, and M. A. Sasse, "Better the Devil You Know: A User Study of Two CAPTCHAs and a Possible Replacement Technology," in *NDSS Workshop on Usable Security (USEC)*, 2016.
[6] The Pico Project, "Pico: No more passwords!" https://mypico.org/, 2017.
[7] F. Stajano, "Pico: No more passwords!" in *Security Protocols XIX*. Springer, 2011, pp. 49–81.

The Pico Project is generously funded by the European Research Council (ERC), grant number: StG 307224 (Pico).