Users are not ungrateful: Making sense of user resistance to well-intentioned innovation

Frank Stajano

University of Cambridge (United Kingdom)
professor@stajano.com

Abstract. We explore the paradox of users simultaneously complaining about the pain of passwords and at the same time rejecting user-centric prototypes of a more usable and more secure alternative. From our experience with the Pico project we distil unexpected insights about user inertia, mismatched user and researcher expectations, entrenched habits and ecological validity of user studies. The lessons learnt extend beyond authentication to any security usability initiative seeking real-world adoption.

Keywords: passwords · security usability · Pico · ecological validity

1 The pain of passwords

At a party, when they find out you're a doctor, total strangers will ask you about their niggling pain. Similarly, if you're a computer person, you instantly become an IT helpdesk. Around 2010 I noticed that many of the informal helpdesk requests I regularly got from friends and family revolved around passwords. "You're into computer security: can't you do something about it?"
When I started paying attention to the issue I had to admit that we, the computer security geeks, were failing the regular human beings. We were telling them, for their own security, that they were not allowed to write their passwords down, that their passwords had to be hard to guess, and that they had to use a different password for every account. But a moment's thought shows that intersecting these requirements yields the empty set. We were setting people up for failure. Even worse, if their account got compromised, we would, adding insult to injury, blame *them* for having violated those impossible-to-follow directives. I felt this was utterly wrong. We, the security geeks, had a moral duty to do better. So I joined the small but growing group of security researchers who had been trying to build something improve the situation.

My stance was first to get the design right, without worrying (at least initially) about how to make it work in the real world. I gave myself a licence to start from a blank slate and build something that would be (a) easier to use than passwords for non-geeks, even when scaled to thousands of accounts, and then also (b) more secure. The system I came up with would remember, on your behalf, a different public-key-based credential for each of your accounts: I therefore named it Pico [15] after Giovanni Pico della Mirandola, a fifteenth-century philosopher famous for his prodigious memory.

Everyone hated passwords and everyone resonated with the problem on a personal level, so my vision of an easier-to-use and more secure alternative had broad appeal. I was invited to talk about Pico at various workshops and conferences, where audiences embraced the idea enthusiastically, and I even secured an ERC grant to take the Pico vision forward.

2 The challenges of building real prototypes

When assessing claims of usability, the proof of the pudding comes from user studies. But these are difficult, expensive and time-consuming. Some parts of the security usability community embrace Mechanical Turk [13] as a convenient substitute, collecting questionnaire answers from remote correspondents who respond in exchange for a modest payment. This is a good method for producing many papers quickly; but we were always sceptical about the ecological validity of the results thus obtained[1]. For Pico, we stuck to the rather more laborious and inefficient modus operandi of building a prototype, giving it to genuine human beings, letting them use it in their daily life and then debriefing them about their experience [2]. Of course this method does not scale very easily, even though we believe it yields more genuine answers.

At the design stage, as I mentioned, I had ambitiously chosen a blank-slate approach. At the prototyping stage, though, my team and I had to pay its heavy cost: Pico required changing both the client side and the server side. Therefore, even if we built a prototype of a Pico client device, it would not let a user log into a computer or website unless we persuaded the OS or the website operator to adopt our changes. We initially built a software adapter, the Pico lens [16], a browser plugin that made websites appear as if they supported Pico. This allowed us to test and evaluate the Pico interaction method. In a later phase of the project we partnered with Gyazo, a popular image sharing service, which kindly agreed to let a fraction of its existing users log in through Pico. There, instead of a browser plugin, we inserted a proxy web server between the test users and the actual website [2].

Having devoted significant engineering effort to break the "unfair deal" and to provide non-geeks with a better user experience than that offered by passwords,

[1] It is amusing to witness how, since the public release of ChatGPT in November 2022, the people who respond to such questionnaires promptly embraced AI chatbots in order to multiply their own efficiency, further validating our scepticism.

we were disappointed to witness a less-than-enthusiastic adoption of our prototypes from our test subjects. Hey, we were on their side—how come they shunned us? They had all said that passwords were a major pain, so why weren't they grateful that we were building a technology to liberate them from passwords?

Firstly, users had already had to cope with those pesky passwords for long enough that they had developed their own coping mechanisms: they reused passwords across websites, they kept a little notebook or an electronic document with all their passwords, they inflected a base password with some per-website variation, they relied on the "forgot password" facility rather than their own memory, they let their browser remember passwords for them, and so forth. Security-wise, some of these methods were better than others (and some were atrocious) but it was primarily on the basis of usability that individual users generally chose the ones that best suited them. In due course, they got used to their own favourite coping mechanisms. Passwords were indeed a pain but users had found ways to tolerate them. Getting rid of passwords was no longer an existential need, just a nice-to-have.

Secondly, each of our prototypes, besides being a somewhat clunky and unpolished beta version, only worked with a comparatively small subset of the users' accounts. The users still had to use old-fashioned passwords to log into all the others. On specific accounts, our prototypes allowed us to test the user experience of logging in with Pico rather than with a password; but the condition that users could *not* experience in any of our trials was the feeling of having being freed from passwords entirely. Instead, they had to continue to use passwords (and their own personal coping methods) for all their other accounts. Our propaganda ("no more passwords") did not match what we delivered.

With Pico, from that perspective, instead of reducing our users' cognitive burden, we were adding to it. Rather than replacing passwords, Pico was an additional authentication method for them to manage. In rejecting Pico, users were not being ungrateful: they were just being pragmatic.

Angela Sasse's classic paper with Adam Beautement and Mike Wonham on the "compliance budget" [3] helps us frame this phenomenon: it suggests that users have limited capacity to comply with security measures, and must allocate this capacity across competing demands. Adding Pico as an additional authentication method without removing the need for passwords exceeded users' compliance budget. Our own Pico study in collaboration with Angela on user acceptance of security tokens [14] revealed that users' willingness to adopt new authentication mechanisms depends heavily on whether these mechanisms actually reduce burden rather than adding to it.

We learnt that user inertia is a more powerful force than the pain of the current situation. We found that users will tolerate considerable pain in the current unsatisfactory situation if switching would require disrupting established habits without completely solving the problem. Users are not as adventurous or neophiliac as we had hoped. They prefer the devil they know to the angel they do not, especially when that angel requires them to continue dealing with the known devil for other tasks anyway. Besides, users are opportunistic: to be willing to

adopt a new system, they need to perceive a concrete benefit now, rather than the delayed gratification of a possible working solution in the distant future.
This all sounds obvious in retrospect but came as a revelation to us. We thought we were on the side of the users, rescuing them from the unfair predicament of passwords. We thought we would be their heroes. Users, instead, tried our clunky and feature-limited prototype, saw it didn't save them from passwords and deemed the value proposition insufficient. We were disappointed. With the benefit of hindsight, this was not necessarily a criticism of our research ideas or of the Pico architecture (crucial aspects of which have indeed resurfaced in widely adopted systems, as mentioned in section 4) but mainly of our modest initial implementation.

3 Some related work

Angela Sasse's pioneering work on security usability provided a crucial foundation for Pico: her landmark 1999 paper with Anne Adams, "Users are not the enemy" [1], documented how security mechanisms imposed unreasonable burdens on users, who then rationally circumvented them to accomplish their work. This research established that the problem was not user carelessness but rather the inconsiderate design of security mechanisms that failed to account for human capabilities and limitations. Angela warmly encouraged me when I first circulated my user-centric Pico ideas in 2011 and she offered valuable advice on my ERC grant proposal, thus helping me secure the funds to assemble a Pico team. Once the project was underway, we collaborated on several studies, yielding papers that explored user acceptance of security tokens [14] and developed a framework for evaluating the usability of authentication methods [7]. Angela's broader research investigated many other aspects of authentication usability, such as biometrics, and influenced significant policy developments including the UK National Cyber Security Centre's password guidance in 2015.
My Pico vision proposed replacing passwords with a small hardware token that would authenticate users through physical possession and proximity rather than memorized secrets. Communication between the token and the computer would take place over a multi-channel protocol [18] employing both bidirectional radio and a unidirectional visual code for data origin authenticity. Continuous authentication based on proximity would provide both better usability (no memorization, no typing) and better security (strong cryptographic keys, resistance to phishing).
Prior art on trusting only a separate dedicated device for authentication[2] includes at least Ben Laurie and Abe Singer's thought experiment about the "red pill and blue pill" [10].

[2] A principled security stance from which Pico later receded—as did the many banks that, during the 2010s, moved from proprietary login tokens to mobile apps that trusted the secure enclave of modern smartphone platforms, for the sake of not losing customers to competitors who had already switched to this more practical alternative that did not require carrying one more gadget around.

Prior art on continuous authentication includes at least Roy Want and Andy Hopper's Active Badge [17], Carl Landwehr's RFID-based secure identification system [8,9] and Mark Corner and Brian Noble's zero-interaction authentication [5,12].

Prior art on using a visual code for authentication includes at least Jon McCune, Adrian Perrig and Mike Reiter's pioneering "Seeing is believing" [11] as well as, years later but still before Pico, the photoTAN[3] of Cambridge start-up Cronto, of which Steven Murdoch was the Chief Security Architect. Cronto's well-deserved commercial success stemmed partly from focusing on a narrower problem (banking authentication rather than a universal cure for all passwords) and partly because their clients had the luxury of being in control of both the client and server sides of the authentication protocol.

A rather more extensive survey of related work is in the post-proceedings version of my Pico paper [15]; but at the time, as I wrote and rewrote it, I felt that even that was incomplete. Therefore I teamed up with Cormac Herley, Joseph Bonneau and Paul van Oorschot to develop a comprehensive rating and evaluation methodology of password replacement schemes [4]. Extending the criteria I had originally developed for the Pico paper, we rated 35 schemes on whether they provided any of 25 benefits in the broad categories of usability, security and deployability. Our framework became a widely adopted reference in authentication research. We noted that no proposed alternative scheme provided all the desired benefits, and that none retained all the benefits of passwords. We thus predicted that, despite best efforts by many researchers and organisations, ourselves included, passwords would continue to survive for a long time—as indeed they have.

4 Lessons and legacy

Several lessons emerge for researchers wishing to develop solutions to security usability problems. First, users often develop their own coping strategies for any nagging problems: any new solution will be compared not against the raw problem but against these existing workarounds. Second, partial solutions that require users to maintain both old and new systems simultaneously may be rationally rejected as even more burdensome than the status quo, however flawed. Third, users are pragmatic: they adopt solutions on the basis of their immediate utility, not on the basis of their future potential.

Understanding and accommodating what users are willing to do is necessary in order to design and implement systems that will actually be adopted.

Although Pico did not achieve commercial success, its intellectual legacy may be its greatest contribution. Its core concepts have been adopted or rediscovered by authentication systems that are now widely deployed. Modern passkeys [6], standardized by the FIDO Alliance, embody many of Pico's principles—they do

[3] I would have loved to add a reference to a technical write-up, but was not able to find one.

not require the user to remember any secrets and they use a different public-key-based credential for every account, securely stored on the user's device. The ability to unlock a computer using a smartwatch, now offered by both macOS and Windows, implements Pico's vision of seamless authentication through a device carried by the user. The ability to unlock a smartwatch by authenticating to a paired smartphone in order to save the user from having to type a PIN on the smartwatch, as offered in the Apple ecosystem, is reminiscent of the Picosiblings [15]. Pico (2011) predates both the formation of the FIDO Alliance (2012) and the release of the first Apple watch (2015).

These systems succeeded where Pico did not, largely because they had the backing of major technology companies capable of deploying authentication changes across the entire ecosystem, upgrading both the client and the server simultaneously. A small academic research group, with limited resources, has little hope to change the entrenched behavior of millions of websites and users. Successful deployment of security mechanisms requires either broad industry standardization (as with passkeys) or integration by a dominant platform vendor (as with smartwatch authentication). The humbling lesson here is that academic research may well invent new ideas, develop concepts and demonstrate viability, but translating those concepts into mass adoption is a whole 'nother story.

As Harry Truman famously observed: "It is amazing what you can accomplish if you do not care who gets the credit". Some of the ideas developed in the Pico project are now found in authentication systems used by millions of people. On that basis, there is much to celebrate in what we accomplished.

Acknowledgments. Thanks to Angela Sasse for her valuable input on the original Pico grant proposal and for our subsequent collaboration on Pico leading to joint papers. Thanks to all my other external co-authors on various Pico-related papers: Joseph Bonneau, Cormac Herley, Paul C. van Oorschot, Bruce Christianson, Mark Lomas, Ian Goldberg, Brian Glass, Yuqi Liu. Thanks to all my University of Cambridge collaborators who contributed to building Pico: to my employees / developers / researchers (Quentin Stafford-Fraser, Max Spencer, Chris Warrington, Jeunese Payne, Graeme Jenkinson, David Llewellyn-Jones, Kat Krol, Claudio Dettoni, Seb Aebischer, David Harrison, Robert Irvine, Matthew Wahab); to my summer interns (Alex Dalgleish, Agnes Cameron, Fin Brown); to my undergraduate students (Bo Tian, Oliver Stannard, Jonathan Millican, Daniel Low, Spencer Thang, Antoanela Siminiuc, James Brashko, Adam Roberts) and master students (Anders Bentzon, Cristian Toader, Fabian Krause) who did their project dissertation on Pico; and to visiting scientists Toshiyuki Masui and Jiny Bradshaw. A second thank you to David Llewellyn-Jones for co-founding Cambridge Authentication and riding the bumpy but exhilarating start-up road with me. Institutionally, thanks to the European Research Council (ERC) for funding the project [StG 307224, Pico] and to the Engineering and Physical Sciences Research Council (EPSRC) for funding Toshiyuki's visits to Cambridge [EP/M019055/1, Future authentication systems]; to ICURe, CyLon and Cambridge Enterprise for seed investment and business mentorship to Cambridge Authentication; and to Gyazo and Innovate UK for hosting Pico trials.

References

1. Adams, A., Sasse, M.A.: Users are not the enemy. Commun. ACM **42**(12), 40–46 (December 1999). https://doi.org/10.1145/322796.322806
2. Aebischer, S., Dettoni, C., Jenkinson, G., Krol, K., Llewellyn-Jones, D., Masui, T., Stajano, F.: Deploying authentication in the wild: Towards greater ecological validity in security usability studies. Journal of Cybersecurity (2020). https://doi.org/10.1093/cybsec/tyaa010
3. Beautement, A., Sasse, M.A., Wonham, M.: The compliance budget: managing security behaviour in organisations. In: Proc. New Security Paradigms Workshop 2008. pp. 47–58. ACM (2008). https://doi.org/10.1145/1595676.1595684, https://www.nspw.org/papers/2008/nspw2008-beautement.pdf
4. Bonneau, J., Herley, C., van Oorschot, P.C., Stajano, F.: The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In: Proc. IEEE Symp. on Security and Privacy. pp. 553–567 (2012). https://doi.org/10.1109/SP.2012.44, http://www.cl.cam.ac.uk/~fms27/papers/2012-BonneauHerOorSta-password.pdf
5. Corner, M.D., Noble, B.D.: Zero-interaction authentication. In: Proc. ACM MobiCom 2002. pp. 1–11 (2002). https://doi.org/10.1145/570645.570647
6. Daffalla, A., Bhattacharya, A., Wilder, J., Chatterjee, R., Dell, N., Bellini, R., Ristenpart, T.: A framework for abusability analysis: the case of passkeys in interpersonal threat models. In: Proceedings of the 34th USENIX Conference on Security Symposium. SEC '25, USENIX Association, USA (2025), https://www.usenix.org/system/files/usenixsecurity25-daffalla.pdf
7. Glass, B., Jenkinson, G., Liu, Y., Sasse, M.A., Stajano, F.: The usability canary in the security coal mine: A cognitive framework for evaluation and design of usable authentication solutions. In: Proc. EuroUSEC 2016. p. (11 pages). Internet Society (Jul 2016). https://doi.org/10.14722/eurousec.2016.23007, http://www.cl.cam.ac.uk/~fms27/papers/2016-GlassJenLiuETAL-canary.pdf
8. Landwehr, C.E.: Protecting unattended computers without software. In: Proceedings of the 13th Annual Computer Security Applications Conference. pp. 274–283. IEEE Computer Society, Washington, DC, USA (Dec 1997). https://doi.org/10.5555/872015.872112
9. Landwehr, C.E., Latham, D.L.: Secure identification system (1999), uS Patent 5,892,901, filed 1997-06-10, granted 1999-04-06.
10. Laurie, B., Singer, A.: Choose the red pill and the blue pill: a position paper. In: Proc. New Security Paradigms Workshop 2008. pp. 127–133. ACM (2008). https://doi.org/10.1145/1595676.1595695, http://www.links.org/files/nspw36.pdf
11. McCune, J.M., Perrig, A., Reiter, M.K.: Seeing-is-believing: Using camera phones for human-verifiable authentication. In: Proc. IEEE Symposium on Security and Privacy 2005. pp. 110–124. https://doi.org/10.1109/SP.2005.19, https://www.jonmccune.net/papers/mccunej_believing.pdf, updated version in *Int. J. Security and Networks* **4**(1–2):43–56 (2009) DOI 10.1504/IJSN.2009.023425 https://www.jonmccune.net/papers/mccunej_ijsn4_1-2_2009.pdf
12. Nicholson, A., Corner, M.D., Noble, B.D.: Mobile device security using transient authentication. IEEE Transactions on Mobile Computing **5**(11), 1489–1502 (Nov 2006). https://doi.org/10.1109/TMC.2006.169
13. Paolacci, G., Chandler, J., Ipeirotis, P.G.: Running experiments on amazon mechanical turk. Judgment and Decision Making **5**(5), 411–419 (2010). https://doi.org/10.1017/S1930297500002205

14. Payne, J., Jenkinson, G., Stajano, F., Sasse, M.A., Spencer, M.: Responsibility and tangible security: Towards a theory of user acceptance of security tokens. In: Proc. USEC 2016 (Feb 2016). https://doi.org/10.14722/USEC.2016.23003, http://www.cl.cam.ac.uk/~fms27/papers/2016-PayneJenStaSasSpe-tokens.pdf
15. Stajano, F.: Pico: No more passwords! In: et al., B.C. (ed.) Proc. Security Protocols Workshop 2011. LNCS, vol. 7114, pp. 49–81. Springer (Mar 2011). https://doi.org/10.1007/978-3-642-25867-1_6, http://www.cl.cam.ac.uk/~fms27/papers/2011-Stajano-pico.pdf
16. Stajano, F., Jenkinson, G., Payne, J., Spencer, M., Stafford-Fraser, Q., Warrington, C.: Bootstrapping adoption of the pico password replacement system. In: et al., B.C. (ed.) Proc. Security Protocols Workshop 2014. LNCS, vol. 8809, pp. 172–186. Springer (Apr 2014). https://doi.org/10.1007/978-3-319-12400-1_17, http://www.cl.cam.ac.uk/~fms27/papers/2014-StajanoJenPayETAL-bootstrapping.pdf
17. Want, R., Hopper, A., Falcão, V., Gibbons, J.: The active badge location system. ACM Transactions on Information Systems **10**(1), 91–102 (Jan 1992). https://doi.org/10.1145/128756.128759
18. Wong, F.L., Stajano, F.: Multi-channel protocols. In: et al., C. (ed.) Proc. Security Protocols Workshop 2005. LNCS, vol. 4631, pp. 112–127. Springer-Verlag (Apr 2005), http://www.cl.cam.ac.uk/~fms27/papers/2005-WongSta-multichannel.pdf, updated version in *IEEE Pervasive Computing* **6**(4):31–39 (2007) https://doi.org/10.1109/MPRV.2007.76