"Technology Should Be Smarter Than This!": A Vision for Overcoming the Great Authentication Fatigue

M. Angela Sasse
Professor of Human-Centred Technology
Director, Research Institute for Science of Cyber Security
University College London, Department of Computer Science,
London, United Kingdom
a.sasse@cs.ucl.ac.uk

Abstract: Security researchers identified 15 years ago that passwords create too much of a burden on users. But despite much research activity on alternative authentication mechanisms, there has been very little change for users in practice, and the implications for individual and organisations productivity are now severe. I argue that - rather than looking for alternative 'front-end' solutions, we must re-think the nature of authentication: we must drastically reduce the number of explicit authentication events users have to participate in, and use advanced technologies to implicitly authenticate users, without disrupting their productive activity.

My disciplinary background is in usability, and for a decade, I worked to improve the usability of emerging Internet systems and services. My focus on security (and later privacy, trust and identity aspects) started because an industrial collaborator faced security help desk costs that were spiralling out of control, and asked me to figure out 'why these stupid users cannot remember their passwords'. The resulting study conducted in collaboration with Anne Adams 'Users Are Not the Enemy' [1] published in 1999, the same year as Whitten & Tygar's 'Why Johnny can't Encrypt'. The two papers mark laid the foundation for the research area now referred to as Usable Security. Over the past decade and a bit, this area has flourished: there are now has several conferences and workshops dedicated to the area, and papers on this topic have been accepted to top-tier security and usability conferences alike.

But things have not improved for the average user out there. As Herley [3] put it, most security managers "value users' time at zero". To date, the cost of individual user time and effort spent to what is not their primary goal and activity has been largely hidden. The result, as an intense frustration among users about the burden of security, and the erosion of their personal productivity. Users are acutely aware of this, and stop complying when the friction between the security task and their primary task becomes too high. They introduce workarounds which compromise security, and/or reorganise their primary tasks to minimize their exposure to security [4]. In the context of an organisation, the organisation ultimately pays a high price: the cost of reduced individual and business activity productivity, and that of security breaches which occur as a result of non-compliance. To put it bluntly, most organisations' security at present is an expensive Swiss cheese – to borrow the analogy from the guru of safety research, it is rid-

dled with holes that ever so often align and let the threat through. Unlike good Swiss cheese, the current state of operational security stinks.

Authentication provides a clear example for this. After the publication of "Users are Not The Enemy", we campaigned for changes to reduce the burden of authentication. We had some success: many organisations introduced single sign-on, and reduced the frequency with which passwords expire. But has been no serious attempt to grab the nettle of the password-based infrastructure that is deeply embedded in current systems. In the 2000s, technology (Bill Gates, Bruce Schneier) and usability (Jacob Nielsen) gurus both declared it a non-problem that would be resolved through the introduction of biometrics, which they assumed to be usable by default 'since users don't have to remember anything'. But a decade later, we found that the password burden was still weighing down individuals and organisations alike [6]: single sign-ons, more relaxed policies, and password managers such as LastPass may have reduced the burden somewhat, but the explosive growth in the number of devices, applications and services we use means users still have to manage dozens of passwords. The introduction of self-service re-sets and account recovery mechanisms has increased the burden further: helpdesks staffed by humans to assist other humans a were a visible cost that organisations swiftly moved on – replacing them with a technology-based self-service reminder and re-set mechanisms that create yet more items that users have to think up and remember. In a recent study [7] found additional impact created by "too much" authentication: staff logged in less frequently from home or when travelling, or stopped doing so altogether – meaning colleagues and customers had to wait for information or assistance, which in turn held up their work. Some refused to have a company-owned laptop, or returned it. We also found several examples where staff had identified a business opportunity, but did not pursue it because authentication policies or mechanisms would have to be changed, and they could not face the time and emotional effort that would require. We diagnosed a case of severe Authentication Fatigue, top on the list generated an 'Authentication Hate List':

1. Re- authentication to the same system (e.g. because of 15 min time-outs)
2. Length and complexity makes passwords hard to create, recall and enter – and different rules for different systems compound this
3. Authenticating to infrequently used systems (hard to recall)
4. Password expiry (having to create a new password, interference with the old one, and you have to create 4 passwords a year for a system you only used twice in the same period)
5. Additional credentials for password re-set mechanism

As in previous studies, we found users had created workarounds – to cope with the most hated re-authentication, many users installed mouse-jiggler software to prevent time-outs. Which of, course they forget quite often when they actually do get up and leave their system unattended. So why are we still stuck with high-effort, productivity-zapping authentication mechanisms rendered ineffective by user workarounds? The password nettle is still there, and until we have the courage to grab and remove it, workable mechanisms are hard to realise. In an attempt to reduce the authentication burden, the organisation we studied offered fingerprint sensors to its staff; some used it, and said it was great on a day-to-day basis. But because the underlying authentication infrastructure and policies had not been changed, every 3 months, the underlying password ex-

pired – so they had to find the pieced of paper with the current password, change it, write the new one down, and then re-enrol their fingerprint against the current password. Biometrics have potential to reduce user burden, but do not deliver usability if simply used as an interface solution. Usable security research on authentication to date has largely focused 'user interface' solutions: pictures that are assumed to be more memorable, or password managers (which have been adopted by some users). In an age of ubiquitous computing, the cloud, and touch screen devices, we need to be thinking more broadly and boldly: with cloud computing, even long and complex passwords can be attacked at relatively low cost. The majority of user interactions is now with touch screen devices, rather than keyboards – and entering password of any length and complexity takes at least 3 times longer than doing so on a standard keyboard.

If we use passwords at all, they have to be memorable and quick and easy to enter – that means using some form of 2 factor authentication is inevitable. Most organisations adopt 2 factor authentication for security reasons, and opt for token-based authentication in form of special devices, smartcards, software tokens, or phones to send additional codes (as Google, for instance, does). But these solutions may, at first glance, offer an improvement in security, they create yet more burden on users, who have to remember to carry tokens, or wait for and enter further credentials. And remember to obtain a credential in advance when travelling somewhere without phone reception.

What we need is a shift from repeated explicit to implicit authentication: in an age where commercial companies are able to use the masses of data we emit to identify and profile us with what many think is a frightening degree of accuracy [e.g.8] it is bizarre that users' activity is constantly disrupted by systems insisting that we prove who we are. The 'wall of authentication' [7] users currently face is the legacy of old-style command-and-control, perimeter-based security thinking, where it was acceptable to create big obstacles to keep attackers out of systems, and make it almost as difficult for legitimate users to get in. That approach is not sustainable, and we hear users [in 7, but also a range of other studies we conducted shouting in collective frustration that "technology should be smarter than this!" And consumer-based parts of the industry are beginning to move – the FIDO alliance [9], which numbers Google and Paypal amongst its members, is the example of a framework that replaces passwords altogether. It shows how smarter use of the information we have on users – their devices, location, biometrics, patterns of use – can be leveraged to provide low-effort authentication. The final step is to shift towards implicit authentication: application of usability principles to leverage user activity on the primary task, rather than create an explicit, secondary security task – making security not entirely transparent, but making it "zero perceived effort". Biometrics that have been developed to deliver high levels of accuracy (building on Roy Maxion's work keystroke recognition [11]) can recognise users from the way they type, touch – and perhaps even sing [12] or think [13] a simple knowledge-based credential – as part of their main activity to deliver 0 Effort, 1 Step, 2 Factor Authentication. I have to admit to having dismissed the authentication described in [12] and [13] as impractical in the past, but the emergence of low-cost smart technology such as the Emotiv helmet [14], developed to provide faster input for gaming, brings the idea of users 'thinking their password' and having it entered at the same time into the realm of the possible. Authentication is only one security mechanism that needs a radical re-think and re-design – users are suffering from outdated and unworkable access control mechanisms, slow and

timewasting CAPTCHAs and incomprehensible security warnings. We need to start designing security that starts with protecting what users do and value.

References

1. Adams, A., and Sasse, M. A. "Users are not the enemy." In Communications of the ACM 42, no. 12 (1999): 40-46.
2. Whitten, A., and Tygar, J.D. Why Johnny can't encrypt: a usability evaluation of PGP 5.0. In Proceedings of the 8th conference on USENIX Security Symposium - Volume 8 (SSYM'99), Vol. 8. USENIX Association, Berkeley, CA, USA, 14-14 (1999).
3. Herley, C. So long, and no thanks for the externalities: The rational rejection of Security advice by users. In Proceedings of the New Security Paradigms Workshop 2009, pages 133-144 (2009).
4. Beautement, A., Sasse, M. A., and Wonham, M. The compliance budget: managing security behaviour in organisations. In NSPW '08: Proceedings of the 2008 workshop on New security paradigms, pages 47-58 (2008).
5. Reason, J. T. The human contribution: Unsafe acts, accidents and heroic recoveries. Ashgate Publishing, Ltd., 2008.
6. Inglesant, P. G., and Sasse, M. A. "The true cost of unusable password policies: password use in the wild." In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 383-392. ACM (2010).
7. Steves, M., Chisnell, D., Sasse, M. A., Krol K. & Wald H. 'Report: Authentication Diary Study', National Institute of Standards and Technology, Gaithersburg, MD USA, NISTIR <publication TBA> (2013)
8. Nikiforakis, N., Kapravelos, A., Joosen, W., Kruegel, C., Piessens, F., & Vigna, G. Cookieless monster: Exploring the ecosystem of web-based device fingerprinting. In IEEE Symposium on Security and Privacy. (2013)
9. Kirlappos, I., Beautement, A., & Sasse, M. A. "Comply or Die" Is Dead: Long live security-aware principal agents In USEC 2013
10. FIDO alliance www.fidoalliance.org/
11. Killourhy, K. S., & Maxion, R. A. Comparing anomaly-detection algorithms for keystroke dynamics. In Dependable Systems & Networks, 2009. DSN'09. IEEE/IFIP International Conference on (pp. 125-134). IEEE. (2009)
12. Gibson, M., Renaud, K., Conrad, M., & Maple, C. Musipass: authenticating me softly with my song. In Proceedings of the 2009 workshop on New security paradigms workshop (pp. 85-100). ACM. (2009)
13. Thorpe, J., van Oorschot, P. C., & Somayaji, A. Pass-thoughts: authenticating with our minds. In Proceedings of the 2005 workshop on New security paradigms (pp. 45-56). ACM. (2005)
14. www.emotiv.com/