ARTICLE

The Great Authentication Fatigue – And How To Overcome It

M. Angela Sasse[1], Michelle Steves[2], Kat Krol[1], and Dana Chisnell[3]

[1] University College London, Department of Computer Science, London, UK {a.sasse, k.krol}@cs.ucl.ac.uk

[2] U.S. Department of Commerce, National Institute of Standards and Technology,

Gaithersburg, MD, USA michelle.steves@nist.gov

[3] UsabilityWorks, Boston, MA, USA dana@usabilityworks.com

Abstract. We conducted a two-part study to understand the impact of authenti-cation on employees' behaviour and productivity in a US governmental organi-sation. We asked 23 participants to keep a diary of all their authentication events within a 24-hour period, and subsequently interviewed them about their experience with authentication. We found that the authentication tasks employees have to perform not only carry significant workload, but that the way in which authentication disrupts primary tasks reduces productivity and creates frustration. Our participants reported a range of coping strategies, including use of tools and re-organising their work to avoid security. Avoidance meant they logged in less frequently, stopped using certain devices and services. They also reported not pursing innovative ideas because of "the battle with security" that would be required. Our case study paints a picture of chronic 'authentication fatigue' resulting from current policies and mechanisms, and the negative impact on staff productivity and morale. We propose that organisations need to urgently re-think how they authenticate users in a pervasive technology requirement, and advocate a paradigm shift from explicit to implicit authentication.

Keywords: Authentication, usable security, productivity, workload, diary study.

1 Introduction

1.1 Usable security (NOT)

Nearly 20 years ago, Zurko and Simon (1996) argued for ‘user-centred security’ be-cause “mechanisms and models that are confusing to the user will be misused” [p. 32]. Two papers in 1999 demonstrated specific examples of this, and laid the foundation for the discipline now known as ‘usable security’: in “Users Are Not the Enemy” Adams and Sasse (1999) reported why users do not follow password policies, and in “Why Johnny Can’t Encrypt” Whitten and Tygar (1999) showed why even motivated non-technical users trying to encrypt fail. Since then, there have been hundreds of usable security research papers, and authentication has attracted the most attention – several dozen ‘more usable’ authentication mechanisms have been produced. So has there been any change in practice – has authentication become more usable? A study by Inglesant and Sasse (2010) in a corporate environment led the authors to conclude with a resounding ‘no’: despite the introduction of single sign-on (SSO) mechanisms, users still had more passwords than they could manage, and they struggled with the complexity and frequent expiry. Both corporate policies and advice given to consumers keep asking users for more: longer, more complex passwords, which should be changed frequently. This advice is outdated and does not hold in the face of scientific examination (Herley, 2009; 2014).

To round out previous research performed in the private and commercial sectors, we situated the study documented here in the public sector. We sought answers to the following questions: How does authentication fit into employees’ daily activities? and How do staff manage and perceive the costs of authentication and the cumulative impacts, balanced against their perception of the need for security? While the detailed results can be found in Steves at al. (2014), in this paper, we summarise the key insights on how users deal with the authentication burden that many find unmanageable. Combining our results with insights from other recent studies, we diagnose a case of chronic authentication fatigue. Has the time finally come for organisations to acknowledge that the burden of authentication has reached a level that is untenable? When users struggle to manage, they may inadvertently put their own and their organisation’s security at risk levels that are unacceptable; therefore, we argue that a fundamental re-think of authentication is required to safeguard individual and organisational productivity and security.

1.2 Why ‘usable security’ mechanisms don’t work

The ISO standard defines usability as “the extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency, and satisfac-tion in a specified context of use.” (ISO 9241-11) But security mechanisms are cur-rently developed and implemented without reference to any of these three constraints. In particular, security designers and practitioners fail to consider that users encounter authentication in the context of a goal – checking email, paying a bill, etc. The primary goal is what drives users’ behaviour, and the task they carry out to achieve has a certain workload (physical and mental effort); associated with it. The security mechanism presents a secondary task – a hurdle the user has to overcome in order to complete the primary task, and achieve their goal. The workload associated with the security task is often disproportionate to the importance or length of the primary task. Brostoff and Sasse (2000) found users were not willing to spend one minute authenticating if they were planning to only spend a couple of minutes using a system. Security experts generally do not consider user effort (Herley, 2014) or that different primary tasks or physical or social contexts mean you may need a different mechanism.

1.3 Understanding authentication in context

The study presented in this paper was supported by the National Institute of Standards and Technology (NIST) to characterise authentication in modern organisations, and understand the short- and possibly long-term consequences on their behaviour. We asked 23 US government employees to keep an authentication diary for a day, and used the diary entries to ground a subsequent hour-long interview, in which we asked participants to recount the context of the authentication event and how it affected their work. We also probed participants’ experiences with authentication more generally, and what they did to cope with the burden. On average, participants authenticated 23 times on that day and the failure rate was around 10%. The main frustrations they reported were (1) the need to re-authenticate (e.g., after a time-out), (2) managing a large number of credentials for different systems, (3) the workload associated with changing passwords, which expire at differing intervals, (4) logging in to infrequently used systems and (5) struggling with RSA tokens. Participants reported a number of coping strategies, which can be divided into management or avoidance.

In the next section, we briefly review previous authentication and diary studies and their findings. Then we discuss the design of our study and present its results. We then focus on the main problems our participants encountered and how they tried to deal with them. We conclude by giving recommendations for what needs to change in the thinking about authentication and suggest avenues for further research.

2 Background

In the recent years, there have been several studies seeking to understand the authentication effort in a real life context. Florêncio and Herley (2007) looked at the number of passwords and the scale of password reuse through a browser toolbar. They found that on average, users entered 8.1 different passwords per day and had 25 accounts requiring passwords. Two shortcomings arise from the study of authentication events via only one browser: (i) a browser may be used by more than one person; and (ii) users may authenticate with other applications outside of the browser or on multiple devices. Hayashi and Hong (2011) asked participants to fill out an authentication diary for two weeks. They found that for 60% of accounts, participants did not use any memory aids. They preferred to re-use an existing password rather than create a new one and write it down. On contrary, in an organisational context as studied by Inglesant and Sasse (2010), 9 out of 15 participants admitted writing passwords down, especially after having changed it or if they only used it infrequently. In their study, 32 employees in two organisations kept an authentication diary for a week and were later interviewed discussing each password and its context of use. They found that password policies focused on password strength, enforced frequent change and were not designed using principles from the field of Human-Computer Interaction (HCI).

3 Study description

Our study collected two types of data; (1) quantitative data was drawn from self-reports through an authentication diary and (2) qualitative data gathered through an hour-long interview after completion of the diary.

3.1 Participants

Participants were recruited via a call for volunteers throughout the organisation using e-mail. Of the 25 participants who responded, 23 (14 male and 9 female) provided their authentication diary data at the time requested and we were able to interview 22 of them. Age of participants was: 50+ (11), 40s (3), 30s (5) and 20s (3). All partici-pants were knowledge workers, 13 were researchers with computer science related education or job. Three were researchers without a background in computer science (but in physics, cognitive science etc.). Two were IT systems administrators. The remaining two participants were administrative support staff.

3.2 Study set-up

Diary. In the first part of the study, participants were asked to keep an authentication diary for the duration of 24 hours, all of them on the same day. In the briefing session before the commencement of the study, we provided participants with sheets for logging of their authentication events.

Interview. We interviewed each participant within a month of the diary day. The diary data served as a point of departure for the interview which explored the partici-pant’s individual perspective on authentication.

4 Diary results

4.1 Authentication events and errors

In total, participants recorded 528 authentication events during the 24-hour collection period. On average, they authenticated 23 times during that day (min. = 4, max = 40). Out of the total of 528 events, there were problems in the case of 48 (9.1%). The most frequent reason for authentication problems were mistyped (24 occurrences, 50%) and wrong passwords (7, 14.6%).

4.2 Memory aids

Of the 528 events reported in the study, 168 (31.8%) involved using some memory aid. The memory aids can be divided into three groups. (I) Participants have the passwords stored for them. Within this group, (i) there are cases where the password is entered for the user: when stored in the client (e.g., in the browser, 13 occurrences) or in a password manager (2); and (ii) there are cases where the password has to be entered by the user but is stored either on paper (11) or in a file (4). (II) There are passwords that users create to be memorable; for example, when a portion of the password stays the same as the previous one (1) or the password is based on a memorable phrase (1). (III) Password entry is replaced with a biometric fingerprint scan (4).

5 Interview results

5.1 Workload perception

We observed a discrepancy between the perceived and actual number of authentica-tion events. In the briefing meetings before data collection, some participants request-ed more diary forms as they were expecting to authenticate more often than what the standard set of forms could hold. After the diary day in the interviews, participants were asked what the biggest surprise about their experience was and several stated that they actually authenticated fewer times than they had expected beforehand. This might be an indication that they perceive authentication as a burden and a nuisance. Clifford Nass, from Stanford, an expert on multi-tasking and task switching told us: “I suspect that unlike multitasking, in which the task switching is voluntary and hence people have an incentive to downplay the costs, authentication is not voluntary, thereby making people aware of the cognitive cost.” (Personal communication, 2012). Other research confirms that task-switching has a ‘ripple effect’ on focus, concentration and efficacy – not only on the next task, but any task for the next 20 to 30 minutes (e.g., Monsell, 2003). The frustration over the disruptive effect of authentication could be due to Zeigarnik effect – humans are more likely to remember tasks that were interrupted and left unfinished. The lack of closure that stems from an interrupted and unfinished primary task promotes some continued task-related cognitive effort which might impact the secondary task of recalling a password (Schiffman & Greist-Bousquet, 1992). In the interviews, P3 complained about the disruptive effect of using RSA tokens: “So actually taking the time away from the computer, I walk to get my bag. Someone else stops me in the hallway. I have a conversation with them. Then soon I go back and I remember to login, but I'm like, "Oh." The strong idea I had in my head of a message that I wanted to send might have become a little more fuzzy, the idea of what I was doing. "Why did I open that other new tab and not go to the..." So there's the little things. I feel like those little things really, when you have an idea of what you want to do next and then you have to deviate from that, I think at least for my brain it throws you off a little bit.”

5.2 Specific problems

We conducted a thematic analysis of the interview transcripts and identified several aspects of authentication employees struggled with.

Frequent re-authentication. Participants reported struggling with re-authentication after a time-out. The computers in the organisation are set to lock after 15 minutes of inactivity (to limit the window of opportunity for an attacker to exploit an unlocked machine while the employee is away). P21 emphasised this causes stress: “You end up having to almost set a timer in your head to go back to the computer and type something within every 10 minutes or so. And some minor studies of productivity I've been involved with indicate that it's better to be focused on a task as opposed to have lots of interruptions throughout the day.”

Multiple passwords, their length and complexity. Participants reported struggling with password creation due to different requirements for each system. They found it hard to come up with strong passwords at frequent intervals.

Infrequently used passwords. Participants reported having problems recalling pass-words they use rarely: “You have to think if you are going to be the responsible per-son, then you have to think of different passwords for everything and it is very frus-trating. So when it gets to those infrequently used passwords, then I get really irritated.” (P11) P17 stressed: “Once again security has gotten in my way and it takes me extra time because now I got to look that one up because I don't use that one often enough.”

Password expiry. Another obstacle to keeping one’s passwords synchronised across applications is that some passwords expire at different intervals – this was certainly the case for many of the organisation’s applications. To address this issue, many participants who synchronised passwords to some degree also used the complementary strategy of updating all their passwords at once.

Interruption of workflow. A number of participants emphasised the disruptive effect authentication has on their work, they felt it had a negative effect on their productivity: “And it gets in the way. It definitely takes way more time out of my day, both just time having to deal with this and then the break in the flow of work.” (P19)

Problems with tokens. Some participants reported struggling with the usability of tokens. They found the RSA token hard to use because (i) the display showing the six-digit code was too small and (ii) the change of number every 60 seconds was making the reading and entering of digits a cumbersome task. At the organisation, RSA tokens are necessary for accessing the VPN (Virtual Private Network) from outside the campus. To authenticate, the user has to enter their username, PIN (Personal Identification Number) and the code given by the token, then their username and password. The problem is that the system needs a few second to process the credentials at both stages and if the code expires before this is completed, the user has to start the authentication process again. P12 also found their token was out-of-sync and sometimes it can take them up to three attempts to log in.

Also using PIV cards has posed some challenges. This type of card is normally in-serted to the computer to authenticate using a PIN. However, the card is also used to open doors, and P19 reported often leaving the card in the computer, exiting the room and then being locked out: “So I would forget this every single time. And I've been locked out of the building. I've been locked out of the floor. I've been reprimanded for leaving this in the computer. And there's nothing I could have done other than somehow setting reminders every two minutes to don't forget this.” (P19)

Lack of integration. Four employees reported using a biometric fingerprint reader for some logins. Biometrics are considered to be “usable by default” because they do not require recalling a password or carrying a token (Fairhurst et al., 2003). However, there were physical usability problems for one of the participants, who needed to use moisturiser to make the prints readable: “This is worse, because it works by a bio-metric, and my finger doesn't read very well. I have to smear it with moisturizer, and then I forget what the actual password is. When it really just won't read my finger, I can't unlock it and I can't remember." (P2) And in this organisation, the underlying infrastructure and policies had not been adjusted – the underlying password – which users avoid by using the fingerprint reader – expires every 90 days. When this hap-pens, the user has to find their current password (usually written on a piece of paper kept in the drawer), change the old password, write the new one down, and enrol their fingerprint. This illustrates how the usability of authentication cannot be assured by simply replacing the 'front-end' but keeping the underlying policies and technology infrastructure the same.

6 Employees' coping strategies

Our participants reported a number of strategies for coping with unmanageable authentication workload. The coping strategies fell into two groups: participants either tried to manage and be in control of their authentication effort, or avoid authenticating altogether. The two ways to cope are best summarised by P17: "Yes, I'm trying not to log in that often. And also, if I am logged in, I'll keep going in. Hitting 'check mail' just to make sure it doesn't time me out."

6.1 Management : Trying to stay efficient

Centralising. Most participants attempted to reduce their authentication effort by employing password managers or synchronising passwords across multiple systems: "centralizing it and creating the strongest password for centrally possible has been my tactic. Try to get it all in one bucket." (P3) Most had no awareness of the potential risks of doing so, others were aware but felt they had no choice – it was this, or constantly floundering when a password was needed. The other strategy was employing a password manager (such as LastPass) and storing all their passwords in it.

Batching and proactive authentication. Another common coping strategy for man-aging authentication was batching of primary tasks: employees reported that they try to group several tasks that required access to the same system together, so they only needed to login once. Thus, the secondary security cart is driving the primary task horse, and this has implications for organisational productivity, since it delays com-pletion of tasks. Participants also reported planning ahead and 'authenticating in advance' if they expected a message or file they needed for their work, so they could access it without being delayed by authentication.

6.2 Avoidance: Not using devices or services

Giving up on devices. A number of participants reported that they cope with authen-tication by limiting the number of devices they authenticate to; P19 stated: "If I had a laptop I would have to log in twice, once when you turn it on because the hard drive's encrypted, and then again to actually get into Windows or the operating system. […] So I never wanted an agency laptop for that reason. I don't want to have to log in more times than I need to. That goes to the whole password security policy that we have here, is everything that leaves the agency has to be encrypted." Those participants who refused to have an agency laptop were now incommunicado during business trips, meaning colleagues had to wait several days for response required to complete their own work.

Preventing log-out. Others reduced the frequency of authentication by avoiding re-authentication, they kept the screen active by moving their mouse or joked about installing “mouse jiggler” software.

Logging in less frequently. Participants also reported that they would turn around their email faster if it were not for the authentication burden. They reported that they particularly reduced the frequency with which they logged in remotely (e.g., from home), because this required additional security steps.

6.3 Learning about workload

Our participants developed the coping strategies to consolidate the effort associated with security, and minimise disruption of the primary tasks. To understand the work-load they faced, we conducted an analytical assessment of the workload certain authentication events would pose using the GOMS-KLM modelling technique (Card, Moran, & Newell, 1980). GOMS (Goals, Operators, Methods and Selection rules) and KLM (Keystroke-level Modelling) decompose the interaction between a human and a computer to basic physical and cognitive actions – such as recalling a password (GOMS) or clicking a button (KLM). Once a given task has been decomposed into steps, standard times a practiced user needs to complete each step can be assigned. A GOMS-KLM analysis is traditionally done as a paper-and-pencil analysis, but can be carried out automatically using CogTool (2014).

We used both methods and calculated how long authentication tasks would take our participants. Authentication with the username and policy-compliant pass-word takes 10 seconds. Using LastPass reduces this time to around 4 seconds. This number may not look like a huge saving, but using LastPass posed significantly less of a disruption to the primary task – which means the cost associated with re-starting the primary task was significantly lower.

A few participants said they preferred to keep a piece of paper with the pass-word written on, even if it took several minutes to locate, rather than try to recall their password. This shows a fundamental truth from the field of HCI – users prefer extra physical to extra cognitive effort. In the specific case of authentication, authentication is a hurdle dropped in the path of task completion. If the authentication task requires cognitive resources, it can interfere with the cognitive effort of the primary task. Our participants reported having authenticated, only to find they could not recall what they wanted to do – and needing significant time to backtrack in the task and resume work. Our GOMS-KLM shows the password manager minimises disruption caused by password recall and entry.

7 The cumulative burden of authentication

So authentication takes time, is a burden, disrupts primary tasks and reduces produc-tivity. Among our participants, there was measurable authentication effect and the experience shaped their perception of, and attitudes to, security. Inspired by several participants’ telling us they were ‘tired’ with some aspects of authentication, we call this effect ‘authentication fatigue’.

7.1 Implications for organisations

A previous study (Inglesant & Sasse 2010) found that staff re-organised their work to minimise authentication effort. In the study presented here, we collected further ex-amples of long-term consequences: some participants reported they had returned devices, others stopped to taking it when travelling for work.

Several participants said they had reduced the amount of additional work they did outside of regular office hours because of the authentication burden. Staff avoided logging in or did so less frequently from home or when travelling: “Things get put off until when it's, ‘OK, I have a block of time. It's worth it for me to get the token, to log in and to sit there and do like an hour's worth of work or half an hour or something like that." […] But if it's for like fleeting little, ‘Oh, I have this great idea’ or ‘I want to send this e-mail’ or something, then I'm more likely to put it off until I have that sort of block of time where a log in is worth it. […] especially if it's something that wasn't actually due. It's after hours. You've already put in your nine hours or however many hours you're doing and then you think of something at home, it definitely is less likely that you're going to get online to actually do that thing that you're thinking of. You're just going to wait until the next day.” (P11) So colleagues and customers need to wait for information or assistance, which in turn holds up their work, and that great idea might have been forgotten by the next time our participant logged in.

The security policies that frustrated our participants are arguably not keeping up with technology development and modern ways of working. The authentication burden escalated for employees who used touch screen devices, where entry of cre-dentials took longer and failed more often. The consequences of authentication can embarrass staff in front of customers and peers: “I'd have 150 people waiting for a presentation. I'm waiting for 15 minutes for that sucker to boot up, so I can actually use it. Then, because I'm not admin and I can't change any setting on that box, when the screensaver kicks in, then I've got to log in all over again and reinitialize every-thing and start my presentation all over again and figure out where I was in the 120 slides that I use and make my way there. All the time the audience is right? That's a combination of security and other miscellaneous things. But, like I said, it gets in the way. You're trying to do something, which should be straightforward, but you can't.” (P17) It is not surprising that employees try to avoid such problems or create worka-rounds, that while within existing policy, may inadvertently undermine security.

8 Recommendations

8.1 Consolidating authentication: SSO

The organisation in which our participants worked had SSO, but as in Inglesant and Sasse (2010), most participants reported that they had credentials for a system on which it had not been implemented. Participants said they would prefer one complex and longer password rather than many passwords with different requirements as they do right now. P11 shared with us his dream to only have one password: “I guarantee for me I would sit down and practice that thing and practice that thing and practice that thing until it's automatized and I wouldn't forget it and I would be totally happy to enter a 20 digit password if I could use the same one and not have to go through this hullabaloo of calling and resetting.”

SSO could also solve the problem that participants in our study sometimes did not know which password to use to access which system. But it seems that, in practice, organisations find it difficult to consolidate all credentials behind a single gateway.

Federated identity (a solution where users can use credentials from one pro-vider to log into a multitude of services) offers another potential way of reducing the number of authentication credentials individuals have to manage. But from a security perspective, many organisations will be unwilling to outsource authentication of their own staff. Furthermore, a recent study found that users can be confused and alarmed when being re-directed to an external identity provider (Brostoff et al., 2013).

8.2 "Technology should be smarter than this!"

Compared to the speed with which new devices are being developed, the masses of data we generate when we use them, and the explosion of apps and services which track our every move, the security policies and mechanisms we interact with seem frozen in time. When computer passwords were first introduced in the 60s, they were a badge that gave members of a technical elite access to a rare and expensive piece of equipment – so you had only one password, it was short, didn't expire, and nobody minded if you used the name of your dog or favourite Star Trek character. 50 years later, security clings to the same mechanism even though we now interact with a much larger number of devices and services, and more complex credentials.

In an age where commercial companies are able to use the masses of data we produce to identify and profile us with what many think is a frightening degree of accuracy (e.g., Nikiforakis et al., 2013), it is bizarre that users' activity is constantly disrupted by systems insisting that we prove who we are. In an age where there is so much emphasis on interactions being seamless and sleek and delivering users the best possible experience, users are still bothered with authentication which causes frustra-tion and affects their productivity. The aim of the usable security community should be to learn from both the identifying capabilities of commercial companies and the sleek interaction tips from the user experience (UX) design community.

8.3 Shifting from implicit to explicit authentication

As cloud computing is becoming more and more powerful, even long and seemingly strong passwords need less time to be cracked. In this situation, companies push for 2-factor authentication to achieve better security. It is predominantly tokens, smart-cards or mobile phones that are used to create the second factor. Although the solution may appear plausible, it is rather error-prone and creates additional work for the user. They have to remember to have the token with them and it can pose usability challenges as we have seen in our study. In other contexts of use, for example the case of mobile phone-based 2-factor authentication, one has to remember to have the phone with them and wait for the credential to arrive. But what if the phone is out of battery or there is no reception? This highlights a few of the shortcomings of the state-of-the-art 2-factor authentication. Because of this, we call for a paradigm shift from explicit to implicit authentication.

0-effort, 1-step, 2-factor authentication. P18 mentioned in the interview: "Well, I think that if I just logged in, then it should be able to understand that I just logged in and not ask me for the password again. […] You shouldn't have to do extra work to authenticate. Because yeah, it can just pick up what you do." and this best summarises the shape we believe authentication should take in the future. Computers could authenticate users based on what they do as part of their work. A good way of doing this is through the use of biometrics and in particular behavioural biometrics such as typing rhythm or voice. It has been suggested in the past (Thorpe et al. 2005) that users could be authenticated based on their thoughts. What sounded like a far-fetched idea a decade ago, appears to be a plausible alternative today due to the emergence of brain-computer interfaces such as the Emotiv EPOC (Emotiv, 2014) headset. Introduced to enhance the UX, the Emotiv headset was meant to provide a faster input method for games. The idea behind this EEG-based technology is to steer games by the player's thoughts and facial expressions. The fact that the headset is relatively low-cost and increasingly more popular could make it possible for the user to think their password or any other credential rather than having to enter it explicitly.

Shi et al. (2011) explored the possibility of implicit authentication through observations of user behaviour (location and patterns of messaging, browsing etc.). Roy Maxion's work on keystroke dynamics shows that users can be recognised by the way the type with high levels of accuracy (Killourhy & Maxion, 2009). Also in the age of touch screens and gesture-based interaction, systems could authenticate users based on the way in which they gesture or interact with touch-screens as part of their primary task. In this way, we could achieve 0-effort, 1-step, 2-factor authentication.

References

1. Adams, A., & Sasse, M. A. (1999). Users are not the enemy. Communications of the ACM, 42(12), 40-46.
2. Brostoff, S., Jennett, C., Malheiros, M., & Sasse, M. A. (2013). Federated identity to access e-government services: Are citizens ready for this? In 2013 Workshop on Digital Identity Management (pp. 97-108). ACM.
3. Brostoff, S., & Sasse, M. A. (2000). Are Passfaces™ more usable than passwords? A field trial investigation. In People and Computers XIV—Usability or Else! (pp. 405-424). Springer London.
4. Card, S. K., Moran, T. P., & Newell, A. (1980). The keystroke-level model for user performance time with interactive systems. Communications of the ACM, 23(7), 396-410.
5. CogTool (2014). http://cogtool.hcii.cs.cmu.edu/
6. Emotiv (2014). http://www.emotiv.com/
7. Fairhurst, M. C., Guest, R. M., Deravi, F., & George, J. (2003). Using biometrics as an enabling technology in balancing universality and selectivity for management of information access. In Universal Access Theoretical Perspectives, Practice, and Experience (pp. 249-259). Springer Berlin Heidelberg.
8. Florêncio, D., & Herley, C. (2007). A large-scale study of web password habits. In 16th International Conference on World Wide Web (pp. 657-666). ACM.
9. Hayashi, E., & Hong, J. (2011). A diary study of password usage in daily life. In SIGCHI Conference on Human Factors in Computing Systems (pp. 2627-2630). ACM.

10. Herley, C. (2009). So long, and no thanks for the externalities: the rational rejection of security advice by users. In 2009 Workshop on New Security Paradigms (pp. 133-144). ACM.
11. Herley, C. (2014). More is Not The Answer. IEEE Security & Privacy, 12(1), 14-19.
12. Inglesant, P.G., & Sasse, M. A. (2010). The true cost of unusable password policies: password use in the wild. In SIGCHI Conference on Human Factors in Computing Systems (pp. 383-392). ACM.
13. ISO 9241-11 (1998). Ergonomic requirements for office work with visual display terminals (VDTs)-Part 11-Guidance on usability. International Organisation for Standardisation.
14. Killourhy, K. S., & Maxion, R. A. (2009). Comparing anomaly-detection algorithms for keystroke dynamics. In 2009 Dependable Systems & Networks. (pp. 125-134). IEEE.
15. Monsell, S. (2003). Task switching. Trends in cognitive sciences, 7(3), 134-140.
16. Nikiforakis, N., Kapravelos, A., Joosen, W., Kruegel, C., Piessens, F., & Vigna, G. (2013). Cookieless monster: Exploring the ecosystem of web-based device fingerprinting. In IEEE Symposium on Security and Privacy.
17. Schiffman, N., & Greist-Bousquet, S. (1992). The effect of task interruption and closure on perceived duration. Bulletin of the Psychonomic Society, 30(1), 9-11.
18. Shi, E., Niu, Y., Jakobsson, M., & Chow, R. (2011). Implicit authentication through learning user behavior. In Information Security (pp. 99-113). Springer Berlin Heidelberg.
19. Steves, M., Chisnell, D., Sasse, A., Krol, K., Theofanos, M. & Wald, H. (2014). Report: Authentication Diary Study. NISTIR 7983. http://dx.doi.org/10.6028/NIST.IR.7983
20. Thorpe, J., van Oorschot, P. C., & Somayaji, A. (2005). Pass-thoughts: Authenticating with our minds. In 2005 Workshop on New Security Paradigms (pp. 45-56). ACM.
21. Whitten, A., & Tygar, J. D. (1999). Why Johnny can’t encrypt: A usability evaluation of PGP 5.0. In 8th USENIX Security Symposium (Vol. 99). McGraw-Hill.
22. Zurko, M. E., & Simon, R. T. (1996). User-centered security. In 1996 Workshop on New Security Paradigms (pp. 27-33). ACM.