Applying Cognitive Control Modes to Identify Security Fatigue Hotspots

Simon Parkin, Kat Krol, Ingolf Becker and M. Angela Sasse
University College London
{s.parkin, k.krol, i.becker, a.sasse}@cs.ucl.ac.uk

ABSTRACT

Security tasks can burden the individual, to the extent that security fatigue promotes habits that undermine security. Here we revisit a series of user-centred studies which focus on security mechanisms as part of regular routines, such as two-factor authentication. By examining routine security behaviours, these studies expose perceived contributors and consequences of security fatigue, and the strategies that a person may adopt when feeling overburdened by security. Behaviours and strategies are framed according to a model of cognitive control modes, to explore the role of human performance and error in producing security fatigue. Security tasks are then considered in terms of modes such as unconscious routines and knowledge-based ad-hoc approaches. Conscious attention can support adaptation to novel security situations, but is error-prone and tiring; both simple security routines and technology-driven automation can minimise effort, but may miss cues from the environment that a nuanced response is required.

1. INTRODUCTION

Individuals perform a number of security tasks in their daily lives, both private and professional. These tasks support some primary activity, towards a personal goal such as purchasing an event ticket, or as part of their efforts to comply with an employer's security policies.

There is cognitive – as well as physical – effort associated with each security task. The demands of a task may be excessive or perceived as ill-fitting, promoting the development of *coping strategies* [11]. This avoidance of effort may in fact be rational when limited personal gains are attached to the security task as perceived by the individual [3]. For instance, exhaustively checking characteristics of a website to identify malicious content does not guarantee that the site is benign.

In organisations, security mechanisms and policies are provided to inform secure behaviours. A person might expend security effort for the benefit of others around them and the organisation as a whole [1]. Cumulative effort from burdensome or repetitive security tasks can push an individual past a point where it is then harder for the organisation to encourage a return to good security behaviours. This compliance threshold exemplifies what may be termed *security fatigue*.

Aside from the immediate cognitive and physical demands of security, the consequences of committing effort to both successful and failed security activities can promote avoidance of those same associated personal costs [1]. These costs can include potential embarrassment in the presence of others (should failure occur), and missed opportunities if the security effort associated with a task is excessive.

A number of related studies have directly explored ways to characterise effort associated with security tasks, and the consequences of excessively burdensome security (Section 2). Here we revisit a set of user-centred studies, all driven by a consideration of the tensions between primary tasks and the perceived effort associated with enabling security tasks. These include use of CAPTCHAs (Completely Automated Public Turing test to tell Computers and Humans Apart) [6], and interaction with security policies and security culture in large organisations [1, 4]. Studies are considered as a means to identify the elements of security which are perceived as effortful, both when interacting with individual security mechanisms (Section 3) and combinations of mechanisms (Section 4) as part of day-to-day activities. Studies also allude to the consequences (Section 5), both perceived and actual, of effortful security and security fatigue.

Security tasks can drain individuals' 'energy reservoir' [8] by demanding conscious, laboured cognitive effort. We explore the role of individual performance in security (Section 6), by way of James Reason's model of cognitive control modes [9]. This model differentiates between different families of tasks, which place distinct demands upon the individual's memory and capabilities. These can include routine, unconscious tasks and novel problems which require conscious effort to produce ad-hoc solutions. We reframe this model to consider secondary, security tasks; effortful security can be tiring and error-prone, whereas habitual security routines require experience and training. Here we also consider the impact of cumulative security demands across a collection of security mechanisms and institutional support for the individual (such as IT helpdesks). Conclusions are then drawn in Section 7, summarising recommendations to practitioners and researchers.

Copyright is held by the author/owner. Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee.
Security Fatigue Workshop 2016, June 22, 2016, Denver, Colorado.

2. RELATED WORK

A number of works have explored various dimensions of security effort, and the consequences of that effort when it becomes too great for the individual. These works often use insights from other disciplines to explore security fatigue and its causes.

The Compliance Budget [1] applies security economics principles to consider the costs and benefits for employees in expending effort for the benefit of the organisation. This encapsulates the challenge for organisations to moderate the security demands placed upon employees, to encourage compliance and commit resources to support that compliance. Individuals expend effort altruistically for the benefit of the organisation, but security policies should consider that there is almost a fixed amount of goodwill available before the *compliance threshold* is passed; security that is effortful, repeated over and over during the day, or generally does not adequately consider the user will drain the budget more. Upon reaching what we might refer to here as 'compliance fatigue', the individual may resort to workarounds and coping strategies with greater frequency, and the organisation must invest ever greater resources to promote secure working practices. Here we explore similar thresholds as a trigger to less secure routines.

Cranor [2] devises a framework which considers usability requirements as part of security design; if human participation is necessary for security, there are factors to account for to support a successful outcome. Factors such as interference to tasks and switching attention between tasks can impact the user, making it more difficult to avoid security breaches. Here we consider the impact of cumulative effort upon the individual, where a fatigued state can result in insecure outcomes.

Work by Pfleeger et al. [8] leverages behavioural sciences concepts, such as moral values and habit formation; here we have considered complementary works from the domain of safety. Pfleeger et al. consider habit formation and related constructs as a means to improve provisioning of security awareness support for individuals. Development of more effective security routines is seen as one means of improving individual security behaviour. Relating to the intentions of this paper, Pfleeger et al. allude to "user's energy" and how tasks should be arranged so as to make best use of it.

Renaud [10] considers that security policies in organisations have an effect of placing unrealistic demands upon employees. A survey of 328 employees of the UK National Health Service (NHS) found that the majority of employees would feel stress and an inability to cope should security policies require them to change their routines. Survey respondents perceived that policies did not recognise the demands placed upon them. Here we consider that security effort should be expected in the right way at the right time, in order to limit the emergence of security fatigue.

3. INDIVIDUAL SECURITY ROUTINES

The authors have been variously involved with a number of related security usability studies. Each study examined the ease-of-use of existing security mechanisms. Studies also explored participants' perception of effort related to use of security technologies to support particular primary tasks. The studies include:

- A diary study exploring the burden of authentication tokens upon employees in a large governmental organisation [12, 13].
- Interviews and a diary study with members of the public, exploring how individuals manage authentication tokens for online banking [7].
- Usage scenarios and follow-on interviews looking at human verification technologies such as CAPTCHAs, and candidate replacement technologies including a game and a face recognition solution [6].

Here we revisit the original study results, to consider themes relating to security fatigue, the cognitive and physical demands that are associated with each mechanism, and how individuals respond to excessive security expectations.

3.1 Two-factor authentication

Diary studies of authentication [12, 13] showed that participants disliked one-time credentials as they made the login procedure disruptive, since the password entry could not be automated. P11 explained:

> *"And it's not something that you just have memorized that you just can do automatically. Again, it's that sort of effortful, I have to get the device. I have to look at it. I have to copy what it says into my computer, and then enter my password. If it was just me entering my password it wouldn't be as big of a deal. [...] It's that deliberate effortful, conscientious... I really have to stop what I'm doing and think about it. Whereas if you're just doing something from muscle memory, you don't really even have to think about that."*

The study found that employees would variously batch tasks to avoid interaction with security, or avoid security tasks – and the actual services they support – altogether. This had an impact on productivity as P6 explained:

> *"To me, the way that security impacts work is not that I waste a few seconds typing in a password, but it is these things that you just can't do because of the limitations of security policy. [...] I can think of cases when I have thought it would be really nice to include some person at another university on a software development project, but then I realize it is going to be such a tremendous pain to organize that."*

Fatigue can also occur when users feel that the level of security is not appropriate to the level or risk and the related effort is thus excessive. P19 noted:

> *"If you're working for the CIA or a hospital with patient records, maybe I could understand that. [...] Nothing we do is sensitive. Everything is public, so they can get it anyways. It doesn't make any sense."*

These themes are echoed in interviews with customers who have used security features of online personal banking [7]. One participant found online banking authentication procedures to be excessive compared to offline transactions where a four-digit PIN is needed to authorise a card payment; as another participant explained:

> *"It feels like if you add that step, or another machine or a special card reader, it feels like when does it end?"*

As in the previous study, some participants felt that hardware tokens were added to online banking not to improve actual security, but perceived security, P01 explained:

> *"I think at the time there has been a lot of fear of online banking – and a lot of people were afraid of getting their account compromised [. . .] I think that it was done to give the appearance to those using online banking, or all those new to online banking that it was secure."*

3.2 Human verification

Similarly in the study of candidate CAPTCHA replacement mechanisms [6], a participant was annoyed with a security measure if they felt it was excessive:

> *"it's not important enough for just contributing to an online forum, if you start adding stats for everything you're not going to enjoy your experience of the Internet... it's already annoying when Facebook tells me you are connecting from another computer, I think – Just let me be!"* (P15)

A face biometric alternative was also assessed – participants did not feel that they could influence the outcome of the process, regardless of how much effort they may exert, creating a stressful situation. It was perceived that individuals had control over CAPTCHAs and that they can always 'try harder' to read characters correctly. If an individual feels that reaching their goal is not guaranteed, they may switch to a procedure where they are more able to influence the perceived outcome.

Fatigue happens when users need to engage in tasks repeatedly while believing that these tasks should be automated, essentially that "The computer should know it's me." Similarly, in the authentication study conducted in a governmental organisation [12, 13], P18 explained:

> *"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. [. . .] That's too much, because you shouldn't have to do extra work to authenticate."*

4. FATIGUE ACROSS COMPETING ROUTINES

A number of studies conducted by the authors have also examined security effort in environments where individuals must manage many security controls as part of their regular activities, and the associated competing demands.

The study examining use of authentication tokens for online banking [7] (as discussed in the previous section) considered the impact of managing multiple bank accounts. These accounts were found to differ so much in their definition and use of authentication terminology and devices that moving attention between accounts was burdensome for individuals. The need to provide multiple credentials also limited how much individuals were able to develop automated banking authentication habits; one consequence of this was that at least one participant moved their banking to another provider. In this case, it took too much conscious effort to be prepared for interacting with – and switching between – a number of tasks which are in essence repetitive. P14 complained logging in to online banking required conscious effort and an attention switch:

> *"I'll have to get myself together mentally and let's say: 'Focus! Whatever is in your mind, forget it.' "*

Large organisations often use security policies to dictate how security should be managed for provisioned IT systems. This extends to the expectations placed upon employees, in terms of how they should use the infrastructure. An organisation normally also provides support for use of IT, and policies will describe how and when support mechanisms should be called upon. An analysis of more than 100 interviews with employees in various roles in a large organisation uncovered many sources of security burden [5]. Proscribed security tasks which distracted from the main work activity would be circumvented, but notably replaced with lower-impact alternatives, sourced from within and outside the organisation, which could be more easily adopted as part of less effortful routines by the individual (e.g., maintaining local copies of files if VPN services were too cumbersome).

At times, the support the organisation had put in place was not adequate, meaning that any and all effort a person could exert to reach a successful outcome would be for nothing:

> *"I've actually had to go home because there was no one in the building I knew to let me in... we could do with say a sign-in procedure or an alternative approach. It was just too much hassle."*

In other cases, high cognitive load related to managing passwords for multiple corporate accounts resulted not only in passwords being recorded to aid future recall, but effort then being exerted to provide some approximation of security for those same records (e.g., a password-protected text file). Employees were conscious of a need for security, and developed solutions based upon their own approximation of good security practices, sometimes without the awareness or active involvement of the security function, referred to as *shadow security* practices. Security mechanisms may otherwise outright block the main work activity, whereas workarounds were not without effort demands of their own, such as renaming files to circumvent restrictions on file access. Critically, individuals are exerting effort to simplify the task and maintain a sense of control towards a particular

outcome, while also preserving some sense that productive tasks are still being conducted securely.

5. IMPLICATIONS OF SECURITY FATIGUE

5.1 Sources of fatigue

The previous two sections – and the studies they touch upon – have demonstrated that there are a number of sources of perceived security fatigue:

- **Excessive cognitive load.** Recalling passwords, recalling the steps of a complicated security process.
- **Excessive physical load and preparedness.** Remembering in advance to carry an authentication token, and coordinating its timely use as a part of a security process [12, 7].
- **Distraction from time-sensitive tasks.** Work pressures can make security demands seem more burdensome [1].
- **Blocking of tasks and missed opportunities.** Waiting for IT support to resolve issues, avoiding new business partnerships because setting up secure IT access seems too troublesome [12].
- **Potential embarrassment.** The possibility of being unable to access data in the presence of a client adds excessive stress to the process [1].

5.2 Responses to fatigue

Related studies also identified potential responses to security fatigue. These responses may inspire changes to habits should security effort cross a threshold and be perceived as too much to justify maintaining proscribed behaviour:

5.2.1 Types of compliance

- **Continued goodwill.** This is the starting position, which in an organisation can be regarded as altruism for the greater good of all individuals in that organisation [1]. An appropriate number of tasks to perform, that support *diligence*. The individual will do what they are asked to do in the name of security, by rote, because it is reasonable and achievable.
- **Grudging compliance.** Continued, visible compliance with security expectations, but only because technology is constraining behaviour. Critically, this behaviour may be *indistinguishable* from security goodwill if the impact on productivity is not also visible [1] (an individual appears to be complying with policy, but their productive tasks are suffering an impact elsewhere).
- **Shadow security.** Where policy or guidance is not visible – or is not descriptive enough to guide behaviour – individuals may create security solutions of their own. These solutions leverage individuals' own existing knowledge of security, and may develop in response to immediate needs or persistently effortful security that is imposed upon them. Crucially, shadow security [4] happens because people want to behave securely, but take action on their own (or collectively in groups) to manage security fatigue and develop workable, repeatable solutions that can be called upon to address recurring security challenges. Rather than being an act of pushing back against security, shadow security is an attempt to match security effort to the task in the absence of external support.
- **Sub-optimal compliance.** Examples focus on 'batching' of tasks [13, 12] as further described in 5.2.2. Productive tasks are performed at times which are sub-optimal, to reduce the need to carry out effortful security routines that are wrapped around any one access to a particular system. Technically compliant with security, but the value of security for the process is diminished – an example would be logging in to a system at the end of the day to perform multiple data entry tasks which could have been carried out at any time, meaning data enters the system later than it normally would.
- **Learned resignation.** Too few tasks to perform. It may not be appropriate to limit individuals' involvement in their own security [14]. Waiting for face recognition technology to decide whether a person is a human or not is one example [6]. This has the same fundamental dilemma as potential embarrassment, where here a person may experience stress at the possible outcome for lack of being able to do anything else to influence the end result.

5.2.2 Coping strategies and workarounds

Users develop coping strategies and workarounds to manage the security effort required from them. Users modify characteristics of the task to make repeated application of a routine that is known to support reaching the primary goal without risk of their work being blocked by security. Coping strategies mean that users reorganise their work and security task through for example batching logins. When batching logins, users do not log in to a system as they need it for their work but batch multiple activities that need to be done on a system to reduce the number of login procedures required. One type of a coping strategy can be disengagement where individuals abandon or avoid the use of technologies or services altogether [13]. This can include workarounds, and indeed avoidance of the productive task that security was intended to support.

An example of a workaround is when users decide to switch to an alternative to the advocated technology. This can include other security mechanisms (e.g., transfer files on an encrypted USB stick instead of via a file-share), or 'homemade', *shadow security* solutions leveraging a personal approximation of security [4] (such as a password-protected record of passwords, kept on a personal machine which never leaves the office). These may be workarounds, but also appropriations of other technologies advocated in policy. Banking customers may use an account less often or switch to a different provider altogether [7].

6. COGNITIVE CONTROL MODES AND SECURITY FATIGUE

Many of the sources of security fatigue are cognitive. Individuals will act to automate security, or otherwise develop workable, repeatable security habits which are ensured to reach a successful outcome.

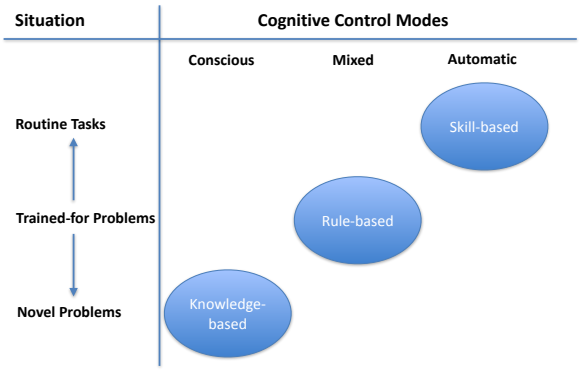

Figure 1: Three levels of performance control (adapted from Reason [9]).

James Reason has previously defined a framework (see Figure 1) to explain how individuals apply cognitive effort towards completion of tasks. Given a focus on safety and the reduction of errors in practice, the framework considers the consequences when badly-fitting tasks place improper demands upon an individual's memory. This model can frame how an individual rationally moves to a different default response to minimise the sense of fatigue and reach a successful outcome for the primary task, especially within the security domain (a range of default positions were explored in the previous section).

Knowledge-based performance applies conscious attention to a task. This approach is adaptive to the situation, but effortful, tiring, and – critically for creating a consistent, workable security environment – it is not what humans typically prefer to do, and can be extremely error-prone. In novel situations where there is no clear advice or known solution, knowledge-based performance may be the only approach available.

Skill-based performance supports conscious pursuit of goals with automatic actions, such that the enabling activity is near-unconscious. Automatic habits reduce the need to expend cognitive effort in the completion of a range of tasks; however, absent-mindedness can still occur if the circumstances of the setting do not fit application of the learned behaviour. Application of learned behaviours may be challenged in times of increased pressure, such as time-sensitive tasks (as in Section 5).

Rule-based performance considers circumstances specific to the activity, then selecting a pre-packaged solution that applies to those circumstances. This is supported by experience and training; for security, if bad habits develop which nonetheless manage burden and fatigue, they then become part of the repertoire of solutions that a person can call upon in the future. The need to apply rules can also be missed; this may occur if the role of security in the main activity has not been made clear. Similarly, if a person is not adequately prepared for the situation, they have to resort to effortful, tiring conscious thought.

6.1 Security fatigue across performance levels

Reflecting upon the model of cognitive control modes, Reason builds an argument that fatigue contributes to task errors. It is then important to ensure that security effort fits the task, otherwise individuals are likely to be placed in a situation where they are more likely to make a mistake. Conversely, habits may develop to reach a desired goal, and the habit hardly revisited to determine if it requires rules or knowledge. An example would be regarding browser warnings as a routine (clicking through all prompts) when the process is intended as a trained-for problem, albeit lacking the training that would normally prepare a person with established routines to call upon. An insecure skill-based approach is hard to shift, so it is necessary to establish good security habits which will genuinely prepare the individual for the situation in which they are applied, but which will also moderate security effort from first application onwards.

Reason argues that the human mind will defer to automatic practices whenever possible, which is then error-prone in itself. Solutions will fall between treating a situation like a similar one, and deferring to the most often used solution. Stressful situations promote use of reliable approaches which were felt to work well in the past – in this sense, security tasks which may create embarrassment or inconsistent outcomes should be re-evaluated, as should tasks which leave users uninformed and disconnected from what is happening during the process. Considering collections of tasks (Section 4), if all security tasks demand conscious effort, a person may become tired more rapidly.

Use of passwords as an authentication credential is in some sense intended to be simple and effortless, in essence a skill-based task. However, this does not scale as it requires rule-based thinking for an individual to recall their password composition strategies and simply which password applies to which account. Knowledge-based approaches may even be required if a password strategy cannot be recalled; ad-hoc solutions can include borrowing another person's account credentials, or embarking on an unfamiliar password-resetting process.

Security technology may at times serve to automate effort on behalf of the user, akin to how humans may themselves automate a task. Automation of security effort in technology may seem like a virtuous solution, taking burden away from the individual. However, if the automation does not for instance support rule-based performance, the completion of trained-for problems is made more difficult; the individual may assess a situation as requiring input on their part, but the act of putting cognition into action is removed from them – conscious effort will not change the result. This can for example include the need to call on IT support to resolve an issue; if the support is not timely, there is nothing the individual can do, and they may avoid tasks which require particular technologies.

Reason's framework also illustrates that some effort is necessary and acknowledged in the way that tasks leverage memory and situational cues. Different modes of performance can be employed to guarantee a satisfactory (read, secure) outcome with a level of conscious effort that fits the task.

Fatigue is then damaging because it changes the control

mode, and consequently how the task is interpreted and addressed by the individual over time. People do not actively default to ignoring security on every occasion, but instead are defaulting to an established approach which satisfies completion of the primary goal. Security fatigue also puts individuals at risk of making mistakes, not least if they feel drained and exhausted by security, but by forcing a deliberate, error-prone approach, sometimes without the facilities available to find a suitable – secure – solution. If the task is designed badly, new stimuli forces *effortful, error-prone, conscious* evaluation of the task. If practitioners do not want there to be errors, it is necessary to design a security task properly according to how it leverages the individual's memory (learned responses) and capacity to interpret in-situ stimuli; context-of-use is then important as it can determine the capacity to reach a successful outcome.

7. CONCLUSION

We revisit a small set of user-centred studies of security mechanisms, identifying routines and consequences of fatigue for the individual. Strategies that are adopted to manage security fatigue are also identified. Contributors and consequences of security fatigue are then framed in terms of cognitive control modes, using a framework initially developed by James Reason to explore task safety and human performance.

We find that security fatigue can have implications for both the management of security, and for the cognitive approach an individual may adopt when faced with a particular security task – fatigue can change the way individuals apply conscious and unconscious effort to reach their goals. Security fatigue may also change how memory and skills are called upon, if the task is not simple; conversely, if a task proves difficult, without a repertoire of available solutions in mind, a person will resort to effortful adaptive thinking to find a solution.

If practitioners seek to provide workable security, it is necessary to minimise error-prone and tiring conscious effort, but to balance this with a need to anticipate the structure of security tasks – automation of security is laudable but not always appropriate. Routine tasks can be completed with reduced cognitive effort, but are disrupted if situational cues arise which are not anticipated as being part of the task, creating a sense of security fatigue for the individual. Researchers examining security fatigue may wish to consider the points at which security tasks involve the individual, and where a task should make appropriate use of their capabilities. This then informs where support should be provided, either in preparing the individual with relevant skills or in the development of novel, simplified processes. The key to reducing security fatigue is to ensure that individuals feel prepared, supported, and unburdened; providers of user-facing security solutions need to prepare the individual for security tasks in such a way that technology, process and skill are all parts of a complete – arguably inseparable – package.

8. REFERENCES

[1] Beautement, A., Sasse, M. A., and Wonham, M. The compliance budget: managing security behaviour in organisations. In *Proceedings of the 2008 Workshop on New Security Paradigms* (2009), ACM, pp. 47–58.

[2] Cranor, L. F. A framework for reasoning about the human in the loop. *UPSEC 8* (2008), 1–15.

[3] Herley, C. So long, and no thanks for the externalities: the rational rejection of security advice by users. In *Proceedings of the 2009 Workshop on New Security Paradigms* (2009), ACM, pp. 133–144.

[4] Kirlappos, I., Parkin, S., and Sasse, M. A. Learning from "shadow security": Why understanding non-compliance provides the basis for effective security. In *NDSS Workshop on Usable Security (USEC)* (2014).

[5] Kirlappos, I., Parkin, S., and Sasse, M. A. Learning from "shadow security": Why understanding non-compliance provides the basis for effective security.

[6] Krol, K., Parkin, S., and Sasse, M. A. Better the Devil You Know: A User Study of Two CAPTCHAs and a Possible Replacement Technology. In *NDSS Workshop on Usable Security (USEC)* (2016).

[7] Krol, K., Philippou, E., De Cristofaro, E., and Sasse, M. A. "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).

[8] Pfleeger, S. L., Sasse, M. A., and Furnham, A. From weakest link to security hero: Transforming staff security behavior. *Journal of Homeland Security and Emergency Management 11*, 4 (2014), 489–510.

[9] Reason, J. T. *The human contribution: unsafe acts, accidents and heroic recoveries*. Ashgate Publishing, Ltd., 2008.

[10] Renaud, K. Blaming noncompliance is too convenient: What really causes information breaches? *Security & Privacy, IEEE 10*, 3 (2012), 57–63.

[11] Sasse, M. A., Brostoff, S., and Weirich, D. Transforming the 'weakest link'—a human/computer interaction approach to usable and effective security. *BT technology journal 19*, 3 (2001), 122–131.

[12] Sasse, M. A., Steves, M., Krol, K., and Chisnell, D. The great authentication fatigue – and how to overcome it. In *International Conference on Cross-Cultural Design, HCI International* (2014), vol. LNCS 8528, pp. 228–239.

[13] Steves, M., Chisnell, D., Sasse, M. A., Krol, K., Theofanos, M., and Wald, H. Report: Authentication Diary Study. National Institute of Standards and Technology (NISTIR) 7983, 2014.

[14] Wash, R., Rader, E. J., Vaniea, K., and Rizor, M. Out of the loop: How automated software updates cause unintended security consequences. In *SOUPS* (2014), pp. 89–104.