Shrinking the Authentication Footprint

K. Renaud and J. Maguire

School of Computing Science, University of Glasgow
e-mail: karen.renaud@glasgow.ac.uk

Abstract

Developers create paths for users to tread. Some users will stay on the beaten track; others will diverge and take risky shortcuts. If user-preferred and developer-created paths diverge too much, it is time for the developer to consider a new path. A case in point is the humble password. They fill an important developer need: a cheap and easy mechanism to control access and enforce accountability. Unfortunately, users find the constant requests for authentication a nuisance. They respond by walking down risky paths that compromise the mechanism but allow them to satisfy goals more quickly. The answer, for some researchers, has been to come up with password alternatives. This focus is misguided, since the alternatives do nothing to reduce the authentication footprint. The reality is that developers overuse authentication. The problem is not the authentication step, but rather its position in the path. Authentication is sometimes used even when there is no real need for it. This creates confusion in the user's mind about the consequences of authentication: sometimes it authorises significant side effects and other times it is difficult to identify its *raison d'etre*. Here we suggest some developer patterns which minimise authentication requests, emphasising necessity rather than gratuitousness. We believe this will help to ease the current situation by moving towards genuine risk mitigation rather than harming authentication by excessive use thereof.

Keywords

Authentication, Patterns, Password

1. Introduction

Researchers have spent a great deal of effort coming up with new authentication mechanisms eg. alternative alphanumeric approaches (Zviran & Haga, 1990), graphical alternatives (Jermyn et al., 1999) and even audible passwords (Gibson et al, 2009). The motivation appears to be to find a more memorable alternative to supplant the password. Having found one, researchers publish details, with evidence of the alternative mechanism's superiority. Yet the password persists.

The widespread use of passwords has accustomed users to access control as a necessary evil. Unfortunately, the very familiarity of the mechanism has also been its undoing. A clear indication of the failure of the password is the prevalence of policies and procedures that use words such as "comply", "sanction" and "disciplinary". Unfortunately these policies, instead of convincing users to walk the developer's intended path, often do more harm than good (Herley, 2009).

As authentication researchers, we have often been obsessed by the mechanism itself, rather than its placement within a workflow, task or path. Developers define such

workflows and lay down paths for navigating them, users merely react. Hence *developers* determine the position, use and frequency of authentication challenges. We need first to understand their perspective, the paths they create, and how these can better be designed to overlap with paths users prefer.

2. Developer Survey

We carried out a survey of software developers to find out what their concerns were with respect to authentication, and alternative approaches, and to assess the level of awareness of alternatives. 89 developers responded to our survey, of whom 71% developed systems for the desktop, 26% developed for mobile environments and the rest developed for both. 33% had had some experience of authentication other than the password although 73% were aware that alternatives to passwords existed.

We asked "*When you need to restrict access, what do you usually use?*". 70% of respondents referred to an identifier/password combination. Two mentioned the use of Lotus auto-authentication, a number simply said "ADS" and three said that they would use device id in conjunction with the identifier and password. One mentioned using a fingerprint and one a token. For this group, the password seemed the most popular authentication choice.

A number of questions were asked about password use, use of alternatives, context of use etc. These questions were designed to elicit open-ended responses. The responses were analysed using a Grounded Theory approach. We wanted themes to emerge rather than using an approach which utilised a-priori themes. First all responses were examined and acceptance-related aspects coded, then codes were grouped into emerging themes.

The first question asked whether respondents thought there were contexts where passwords were unsuitable. A number of themes emerged from their responses in terms of context. (A1) unsuitability for users, either in terms of accessibility or memory; (A2) where the authentication was happening: in public, where people could be observed, and on a single-user device; (A3) what data/application was being protected; (A4) acceptability by users/enterprise.

We asked whether they would consider using a graphical mechanism if it were proven suitable for their user group. Here recurring themes were: (B1) strength of the mechanism; (B2) accessibility and memorial issues; (B3) implementation and deployment concerns; (B4) acceptability.

The final question asked what factors would need to be in place for developers to consider switching to another mechanism. Here the themes were: (C1) Cost of the mechanism and the value to the enterprise; (C2) Provable strength; (C3) Evidence of use of the mechanism by others, and empirical evidence of efficacy; (C4) usability and accessibility for users; (C5) ease of implementation and deployment.

We derived the following meta-themes (Figure 1):

Risk: matching the mechanism to the asset being protected
(A2, A3, B1, C2);
Users: ensuring that users will be able to use and accept mechanism
(A1, B2, B4, C4);
Value: cost of implementation and switch and associated value to enterprise
(B3, C1, C5);
Evidence: being able to assess whether other users/enterprises have accepted and used the mechanism
(A4, C3).

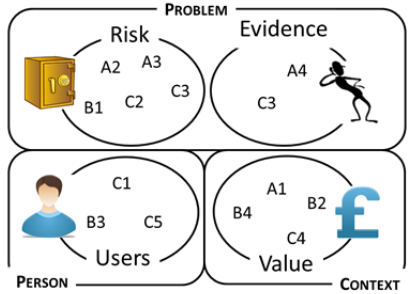

Figure 1: Developers' Perspectives

Bettman (1991) models consumer intentions to adopt online shopping based on three factors: *person, problem* and *context*. Bettman's model was confirmed fifteen years later, after online shopping had become far more common-place, by Moon (2004). What emerged from our analysis was also the *person* (users), the *problem* (choosing a mechanism based on perceived risk and evidence to provide confirmation) and the *context* (value to the organisation). Finally, one comment seems to summarise what many of the respondents were saying:

"Passwords are lame with many downsides... but they are mature, time-tested, and people/organizations are comfortable with them... Any alternatives will need to spend a lot of time gaining mindshare in both the user and enterprise world before it can be adopted... For a fundamental security concept like passwords, "The beast that you know" is definitely better..."

The survey provided responses that highlighted themes of concern related to switching to an alternative form of authentication even though awareness of alternatives was fairly high. It is instructive to consider how the current authentication paths came into being.

3. Paths in the Grass

Siracusa (2006) talks about users making "paths in the grass": paths which allow them to achieve their goals while expending as little extraneous effort as possible. He says:

*"Any viable solution must work within the (often inconvenient) bounds of reality. It must be constructed in such a way that the motivations and actions of the participants—both the good and the bad...*especially *the bad—serve to* ***balance*** *the system as a whole. Suggesting that all would be well, if only certain people would act differently or alter their desires in some way is wishful thinking, not an actual solution."*

This strikes a chord. Wishing that people "*would only behave securely*" has almost been the mantra of security practitioners world-wide for at least the last decade. Siracusa argues that socialism, communism and libertarianism have failed because they attempt to create artificial systems which ignore the nature of participants, or which insist that they change their nature.

Siracusa relates that when the University of California at Irvine campus was first built, they did not lay sidewalks: they planted grass. The next year, they returned and laid the sidewalks where the trails were in the grass. We must find ways to consider *how* users want to authenticate, and design to accommodate their "paths". Trying to coerce them into walking down our paths is futile.

Consider Wikipedia, a collaborative encyclopaedia launched shortly after the millennium. The articles on the website are generated by the man and woman in the street, not by experts. Wikipedia is the 6th most visited website on the planet[1]. The authors are not owners of articles *per se*: instead articles are generated through user collaboration, by crowd-sourcing. Users are not vetted; any individual is able to generate or edit an article. In summary, Wikipedia's developers had *people* (everyone), *problem* (building a knowledge resource), and *context* (accountability is less important than encouraging contributions). They chose a novel approach: no authentication.

Malicious users are always a concern and the obvious solution would have been to require authentication. Yet that would probably have discouraged contributors, and Wikipedia seemingly wanted to be sure that no obstacles impeded the creation of a knowledge resource, so they created a new "path" of unhindered access. It turns out that the developers' path coincided with the path users preferred, as demonstrated by the efforts of millions of contributors. Investigations have found the pages to be of high quality (Giles, 2005) similar to traditional encyclopaedias. Vandalism attacks do occur (Viegas, 2004) but users are unaware of this because tools, such as watchlists (Nasaw, 2012), make contributors aware of changes so that they can be corrected. Wikipedia has essentially outsourced both creation and policing. Their approach perfectly matches the risk problems of their context, and it works. Wikipedia's approach is unusual. Let us consider where traditional password usage originated.

[1] Alexa. Wikipedia Traffic Information. January 2013.http://www.alexa.com/siteinfo/wikipedia.org?range=5y&size=large&y=t

3.1. Antecedents

For many of us, the paths we tread are historical, informed by tradition and a sense that "I have always done it that way". In the academic literature this is referred to as path dependency, the view that technological change in a society depends on its own past. (Shalizi, 2001; David, (1985, 2000)).

The digital password was designed for professionals and originally surfaced in a system designed to empower professionals in 1962 (Corbato, 1962). The password approach was used to enforce access control.

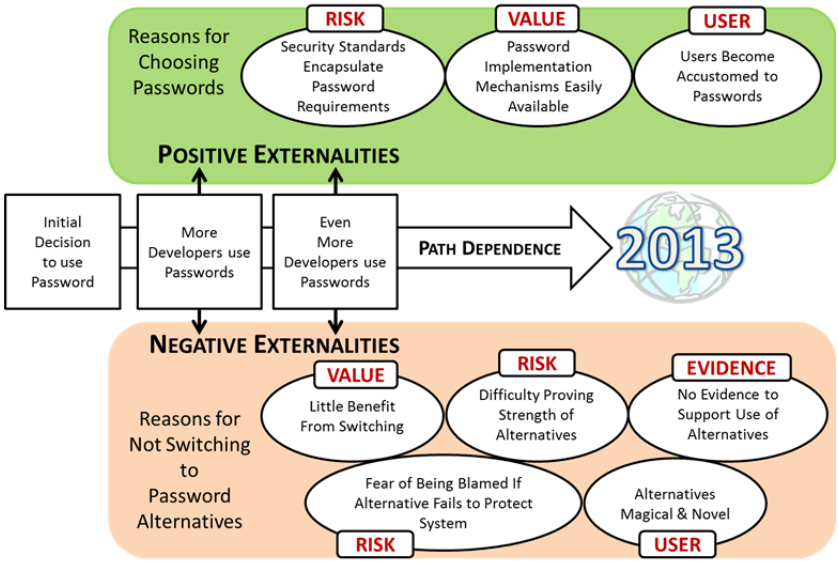

Figure 2: Progress and Path Dependence of Passwords

The current situation, in terms of authentication, is a perfect example of path dependency (Figure 2). This path exhibits extreme dependency on the initial condition (Page, 2006). The initial choice for authentication was the password. This led to operating systems incorporating a password mechanism, and making this available for use by developers. It is a well-understood paradigm, and password rules and requirements are encoded in various security standards. Most importantly, users are comfortable with the *concept* of passwords. They have grown up with stories about Ali Baba and the 40 thieves. The use of passwords throughout history in a military context has familiarised the general populace with the concept, and it is not difficult for them to understand. These are termed positive externalities by Page (2006). There are some negative externalities as well. Our society tends to identify a scapegoat when things go wrong, and this is an unenviable position to be in. "Accountability" is the flavour of the day, and many act defensively and conservatively to ensure that they will not become the focus of rancour.

Choosing a password to protect a system is an approved and widely-used mechanism. There was a saying in the 1970s and 1980s that "*no one is fired for*

buying IBM". Today no one can get fired for using a password. Even if one were to find a developer willing to use an alternative, how would he or she convince the other stakeholders? There is little convincing evidence of the strength of alternatives: most research effort has gone into demonstrating their superior memorability and usability. So, whereas there is significant personal risk in switching and a powerful self-protecting motive to use passwords, it is unsurprising that the password still pervades.

Hence the password has prevailed, not as the outcome of scientific experiments which found it to be optimal, but rather as a consequence of compromises, *ad hoc* decisions and hardware affordances. Many of the problems which have emerged over the last years are a direct consequence of their extensive use and deployment. Corbato stated that although passwords had seemed theoretically sound, in practice flaws became apparent (Corbato, 1990). Corbato's comments have been echoed numerous times by a number of researchers in the authentication area, not to speak of security practitioners and end users.

Passwords, in 2013, are more aligned to the aims and perspectives of the security lobby than human requirements. The developer path has deviated from the paths users would like to tread. The result appears to be an impasse.

Boas (2007) argues that changes to entrenched technologies will only occur if they are replaced wholesale, by a disruptive technology. He suggests that the Sholes QWERTY keyboard, for example, might be replaced by voice recognition, but not by another keyboard, even if the new keyboard is superior. Password practice has worn deep furrows into the landscape. Authentication researchers have been striving towards finding the disruptive technology which will effect this replacement. It is time to step back and reconsider our assumptions and approach.

The reality is that the password will probably be around, in the same format, a decade from now (Herley *et al*., 2009). Herley *et al.* argue that researchers have failed to realise that the password *is* actually the best authentication solution in many contexts. The password is powerful, accessible and versatile (O'Gorman, 2003). Passwords, in their first incarnation, performed exactly as planned. Many of the problems we have today are a direct consequence of indiscriminate and excessive usage thereof. Consequently, rather than attempting to replace the password, a near-term solution may be to accept it but to find a better way of mediating its use, of tackling the gratuitousness of password usage.

3.2. Usage Paths

The password, as a general concept, has a historical path dependency. There are also usage paths in how passwords have been applied by developers. Authentication is essentially used as a gateway, to mediate all access, both risky and innocuous. Once authenticated, the verified individual is free to perform any action at will. This can be depicted as shown in Figure 3. This pattern dictates that users authenticate in order to use the device or application. Having done so, they can carry out any of the mediated actions on the device or within the application.

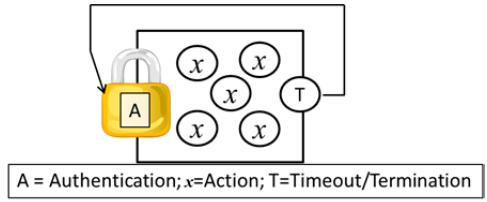

Figure 3: Gateway Authentication Pattern

This password positioning pattern is historical, and harks back to the era of shared desktop computers. These are far less common than they used to be. Nowadays most employees have dedicated desktop or mobile computers: essentially their own devices. Moreover, if the computer is located within an unshared secured office space then the device is secured by other means: requiring device-oriented authentication becomes gratuitous and wasteful. Moreover, such binary access does not deliver the kind of nuanced access within applications that could be delivered. It is generally recognised that activities have associated and diverse risk levels. Some are easily reversed, and others have side effects which cannot be remediated. To apply one authentication mechanism, which we know to have flaws, to permit activities of wide-ranging risk categories seems rather *passé*.

Developers have failed to accommodate the emergent changing *user context.* The following section presents patterns that position authentication to accommodate the emergent user context of the 21st century.

4. Developer Usage Patterns

Here we present authentication usage patterns that would serve to reduce the deployment of authentication to sufficiency rather than extravagance. It is worth considering how many times an individual is required actively to unlock their device during any given day. They may infrequently perform actions with serious or risky side-effects. Nevertheless, whether or not they want to use their device to check the time or to stop music playing, they are presented with an authentication hurdle. This traditional approach can be referred to as "exhaustive access control". Consider that we could categorise actions, rather coarsely, as follows:

1. *No Risk*: No side effects, including actions such as playing music, carrying out a web search, or consulting the system calendar.

2. *Some or Major Risk*: Access sensitive information, or initiate significant side effects such as, for example, making a purchase on an ecommerce site, or accessing email.

Hence we can introduce a new pattern which positions authentication differently. Our proposal for a more prudent access control pattern would be that a user can carry out any no-risk activity without authenticating but if they want to carry out a risky activity, they have to authenticate first (after which all risky activities are permitted).

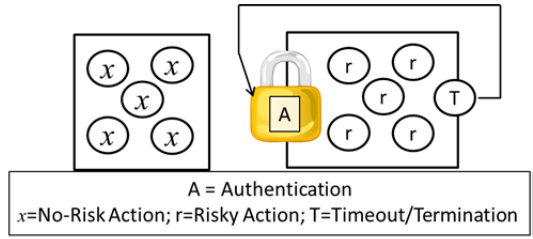

Figure 4: Risk Categorisation Authentication Pattern

The advantage of this pattern is that authentication is used only when necessary. In so doing it fosters a clear connection in the user's mind between authentication and significant consequences. This pattern makes it possible to match the strength of the authentication to the significance/riskiness of the authorised action and to use a bespoke authenticator for different applications. Why would developers use this pattern? It depends on their analysis of the risk. If they are able to separate activities within their application into those that create no harmful side effects, and those that do, then this pattern would be especially beneficial in increasing usage. This pattern is already applied by canny e-commerce sites, such as Amazon. They only authenticate for purchases or to access personal information. All other actions proceed unhindered. Email, which does not support such categorisation, requires a traditional authentication gateway approach.

We can take this a step further. Consider that we could split category 2 (risky) above into two sub-categories: (2a): Has side effects which are easily reversed; and (2b): Has side effects which are difficult or costly to reverse. Email and purchases of goods that need to be delivered physically are an example of 2b. An example of the former is digital media purchases. Digital goods, for the most part, are tightly controlled using digital rights management (DRM) and their use is heavily restricted. Individual purchases are generally tied to a specific account and set of devices.

For 2a, we could put the focus on compensating transactions rather than prevention. The techniques used by Wikipedia to preserve articles, coupled with DRM, could be used to remove the need for an authentication step and still mitigate risk. The user's device acts as a token removing the need for explicit authentication. Users discovering unauthorised purchases could report this and DRM used to remotely deactivate disputed digital goods. Watchlists could be deployed, as in Wikipedia, to improve the ability of the digital content providers to uncover fraudulent behaviours. Hence we have a third pattern. Users can carry out a no-risk or a compensatable activity without authenticating, but once they wish to carry out an action with significant side-effects they have to authenticate. (Figure 5)

This pattern is more fine-grained than the previous one and clearly only applies in particular contexts. However, we need to be creative in finding ways to reduce unnecessary authentication, and this is a relatively simple way of achieving it. Why would developers want to use this pattern? Because humans always act to minimise effort (Zipf, 1949), so removing hurdles encourages action and will probably lead to increased sales and application usage.

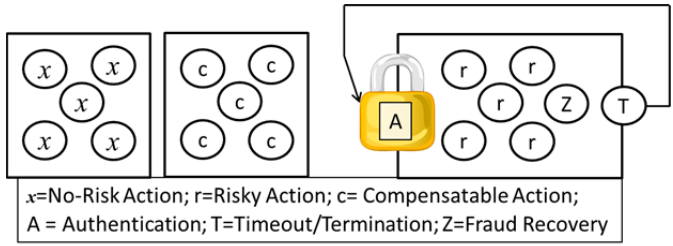

Figure 5: Minimal Authentication Pattern

What about lost or stolen devices? Device authentication, as implemented on most devices, offers little resistance to a determined thief. Using our pattern ensures that only no-risk and compensatable actions could be performed. The owner would then deactivate the device with companies he/she usually purchases electronic goods from and the thief will be unable to use the device to defraud the original owner.

5. Conclusion

The problems of passwords are not necessary insurmountable or bad enough to warrant instant replacement. In the near-time we can make changes in patterns to get more life out the password. Here we have provided two alternative usage patterns which will ease overuse while still accommodating the needs of risk mitigation. Our patterns fit better into a 21st century context of single-owner and single-user devices, accommodating human path preferences.

6. References

Bettman, J.R., Johnson, E.J. and Payne, J.W. (1990), "A componential analysis of cognitive effort in choice", *Organizational Behavior and Human Decision Processes*, Vol. 41,pp93–110.

Boas, T. C. (2007), "Conceptualizing Continuity and Change: The Composite-Standard Model of Path Dependence", *Journal of Theoretical Politics,* Vol. 19, No. 1, pp33-54.

Corbato, F.J. (1990), "On building systems that will fail" In ACM Turing Award Lectures. ACM.

Corbato, F.J., Merwin-Daggett, M. and Daley, R.C. (1962), "An Experimental Time-sharing System", In: *Proceedings of the Spring Joint Computer Conference*, San Francisco, California. May 1-3. pp335-344. ACM.

Norman, D. A. and Fisher, D. (1982), "Why Alphabetic Keyboards Are Not Easy to Use: Keyboard Layout Doesn't Much Matter" *Human Factors: The Journal of the Human Factors and Ergonomics Society,* Vol. 24, No. 5, pp509-519.

David, P. A. (1985), "Clio and the Economics of QWERTY", *American Economic Review,* Vol. 75, No. 2, pp332–37.

David, P. (2000), "Path dependence, its critics and the quest for 'historical economics'", In P. Garrouste and S. Ioannides (eds), Evolution and Path Dependence in Economic Ideas: Past and Present, Edward Elgar Publishing, Cheltenham, England.

Flechais, I., Sasse, M. A. and Hailes, S. (2003), "Bringing security home: a process for developing secure and usable systems" In *Proceedings of the 2003 workshop on New security paradigms*, Ascona, Switzerland, 18-21 August, pp49–57, ACM.

Gibson, M., Renaud, K. and Conrad, M. (2009), "Authenticating me softly with "my" song" *Proceedings of the 2009 workshop on New security paradigms*. The Queen's College University of Oxford, UK, September 8-11, pp85-100

Giles, J. (2005), "Internet encyclopaedias go head to head", *Nature,* Vol. 438, pp900-901

Herley, C. van Oorschot, P. and Patrick, A. (2009), "Passwords: If we're so smart, why are we still using them?" *Financial Cryptography and Data Security*, Accra Beach: Barbados, February, pp230–237.

Herley, C. (2009), "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 workshop*, The Queen's College University of Oxford, UK, September 8-11, pp133–144.

Herley, C. and Van Oorschot, P. (2012), "A research agenda acknowledging the persistence of passwords" *IEEE Security & Privacy*, Vol. 10, No. 1, pp28–36.

Jermyn, I. Mayer, A. Monrose, F., Reiter, M. and Rubin, A. (1999), "The Design and Analysis of Graphical Passwords", In *Proceedings of the 8th USENIX Security Symposium*, Washington DC, 23-26 August, pp1–14.

Moon, B-J. (2004), "Consumer adoption of the internet asan information search and product purchase channel: some research hypotheses", *Int. J. Internet Marketing and Advertising*, Vol. 1, No. 1, pp104–118.

Nasaw, D. (2012), Meet the `bots' that edit Wikipedia. *BBC News Magazine*. http://www.bbc.co.uk/news/magazine-18892510

O'Gorman, L. (2003), "Comparing passwords, tokens, and biometrics for user authentication" In: *Proceedings of the IEEE*, Vol. 91, No. 12, pp2021–2040.

Page, S. E. (2006), "Path Dependence", *Quarterly Journal of Political Science*, Vol. 1, pp87-115.

Shalizi, C. (2001), "QWERTY, Lock-in, and Path Dependence", unpublished website (http://cscs.umich.edu/~crshalizi/notebooks/qwerty.html), with extensive references

Siracusa, J. (2006), "Paths in the grass. We have created, for the first time in all history, a garden of pure ideology" http://arstechnica.com/staff/2006/02/2918/

Wurster, G. and van Oorschot, P. (2008), "The developer is the enemy" In *Proceedings of the 2008 workshop on New security paradigms*, Lake Tahoe, CA, September 22-25, pp89–97.

Zipf, G. K. (1949) *Human behavior and the principle of least effort*. Oxford, England: Addison-Wesley Press.

Zviran, M. and Haga, W. (1990), "Cognitive Passwords: The Key to Easy Access Control", *Computers & Security*, Vol. 9, No. 8, pp723–736.