Authentication Frequency as an Important Design Factor

Position Paper: SOUPS 2014 WAY Workshop

Mike Just
Interactive and Trustworthy Technologies Research Group
Glasgow Caledonian University
Glasgow, UK
mike.just@gcu.ac.uk

1. INTRODUCTION

With an ever-increasing number of briefer interactions with a larger number of different "things", innovative perspectives on authentication could be helpful. Ideally, authentication solutions are designed to balance requirements of security with those of usability, with the latter including cognitive ability for choosing credentials such as passwords, and memorability of those credentials. Some important variables to consider include the size and complexity of the credential alphabet, the length of the credential, and the number of credentials and accounts.

Another important variable is the authentication *duration*: the time spent authenticating by a user over a period of time. The duration could be computed as the duration for each authentication action, multiplied by the number of actions over a particular time period. If the duration can be reduced, then the user would spend less time on the secondary task of authentication. There are at least a couple of approaches to reducing the overall authentication duration for users: reduce the time required for each authentication action, or reduce the total number of authentications performed. At the WAY workshop, I would like to expand on the latter and discuss the importance of authentication frequency to secure and usable authentication design, including some of my related research activities.

2. AUTHENTICATION FREQUENCY

For our purposes, *authentication frequency* is the number of authentication actions performed by a single user using the same credential over a defined period of time. For example, a user might authenticate with a frequency of 10 times per day, or 70 times per week. If the user uses the same credential at two or more different accounts, the frequency can similarly be computed for a single user across all such accounts. Thus, this definition of authentication frequency is linked to the use of a single credential for a single user.[1] In terms of the authentication action, for the purpose of this short position paper we include both *explicit actions* in which a user explicitly enters or otherwise uses their credential, as well as *implicit actions* in which a user automatically authenticates, such when an authentication cookie is submitted, or when using forms of continuous authentication. The above definition of authentication frequency does not distinguish between the two types of actions, though such distinctions are important, and are discussed below.

It is our position that understanding authentication frequency can be useful for designing authentication solutions, and perhaps for stimulating ideas for novel authentication solutions. Some related considerations for high and low frequency behaviours are discussed below.

- *High frequency behaviour.* If users authenticate frequently, then there are opportunities for alternate solutions as it can become easier to identify consistent patterns in the authentication behaviour using machine learning [2]. For example, for a user that often authenticates from a small number of locations, or at some particular times of day, a second factor might only be used when at new locations [9], perhaps using a combination of cookies and location information [1]. If sufficient data could be collected about related, implicit behaviour then the collection could be done continuously, such as on mobile devices [15] (as we discuss in Section 3).

- *Low frequency behaviour.* If users don't authenticate often, then it is difficult to recognize consistent behaviour patterns, and it might be more difficult for a user to recall their credential when it comes time to use it. In the case of forgotten credentials, it's not just an opportunity but a necessity for alternate account recovery solutions [12]. Solutions such as password managers, are useful in this case though there are tradeoffs with security and usability in their support for roaming users [3].

It might also be interesting to consider potential advantages and disadvantages for *manipulating the frequency*, e.g., perhaps using methods of persuasion.

- *Increasing frequency.* Artificially increasing the frequency of the explicit use of a credential would potentially help to increase credential memorability, though seems more likely to be considered a nuisance by users if there are increased logins at a single account. However, increasing the use of a password across multi-

[1] Other definitions might consider frequency across several credentials for a single user, or across multiple users.

Symposium on Usable Privacy and Security (SOUPS) 2014, July 9–11, 2014, Menlo Park, CA.

ple accounts offers similar benefits, though raises security [4] as well as privacy concerns as evidenced by some single-sign-on solutions [5].

- *Decreasing frequency.* Decreasing the explicit use of a credential already happens today. For example, browser "save password" tools, password managers and mobile apps allow users to save their passwords, sometimes indefinitely (see examples above). When the saved credential becomes unavailable, users might be challenged to recall their credential, leading to a need for account recovery solutions.

3. DATA-DRIVEN AUTHENTICATION

My current research in this areas focuses on reducing the number of explicit authentications, where collected behavioural data is used. Recent research in this area has started with a location context, so that authentication requirements might be relaxed when a user is in a "low risk" location, such as at home [7, 8]. Others are looking more broadly at the context, including factors such as noise [6, 13, 14, 11]. Such context can offer greater location granularity, and also distinguish actions such as movement and the presence of others, such as being in a crowded area. My own research [10] examines such a broad context and is "data-driven" where input from the set of mobile phone sensors is used to profile user behaviour. I can talk further about related studies and experiments at the WAY workshop.

4. CONCLUSIONS

Investigations into the study of authentication frequency seem to highlight some interesting tradeoffs for security and usability, e.g., is it better for a user to (explicitly) login frequently, or to login once and save their password so that further authentications are implicit or seamless? In one extreme, when the credential is not often used, but is still required for periodic use, authentication to an account may often default to using the recovery mechanism. This is similar to when there is a low frequency of authentication (explicit or implicit) to an account.

My own research into data-driven solutions that recognize different contexts is intended to investigate such tradeoffs further. There are interesting variations for such solutions and I (and others) are investigating the appropriate attack models and impacts on usability.

Acknowledgments

The research leading to these results has received funding from the People Programme (Marie Curie Actions) of the European Union's Seventh Framework Programme (FP7/2007-2013) under REA grant agreement no PIIF-GA-2011-301536. The data-driven authentication research is joint with Hilmi Güneş Kayacık, Nicholas Micallef, Lynne Baillie and David Aspinall.

5. REFERENCES

[1] M. Alsaleh, M. Mannan, and P. Van Oorschot. Revisiting defenses against large-scale online password guessing attacks. *Dependable and Secure Computing, IEEE Transactions on*, 9(1):128–141, 2012.

[2] J. Bonneau. Authentication is machine learning, Dec. 2014.

[3] J. Bonneau, C. Herley, P. C. Van Oorschot, and F. Stajano. The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In *Security and Privacy (SP), 2012 IEEE Symposium on*, pages 553–567. IEEE, 2012.

[4] A. Das, J. Bonneau, M. Caesar, N. Borisov, and X. Wang. The tangled web of password reuse. In *Proceedings of NDSS*, 2014.

[5] S. Egelman. My profile is my password, verify me!: the privacy/convenience tradeoff of facebook connect. In W. E. Mackay, S. A. Brewster, and S. Bødker, editors, *CHI*, pages 2369–2378. ACM, 2013.

[6] I. T. Fischer, C. Kuo, L. Huang, and M. Frank. Short paper: Smartphones: Not smart enough? In *Proceedings of the Second ACM Workshop on Security and Privacy in Smartphones and Mobile Devices*, SPSM '12, pages 27–32, New York, NY, USA, 2012. ACM.

[7] A. Gupta, M. Miettinen, N. Asokan, and M. Nagy. Intuitive security policy configuration in mobile devices using context profiling. In *Proceedings of the 2012 ASE/IEEE International Conference on Social Computing*, pages 471–480. IEEE CS, 2012.

[8] E. Hayashi, S. Das, S. Amini, J. I. Hong, and I. Oakley. Casa: context-aware scalable authentication. In L. Bauer, K. Beznosov, and L. F. Cranor, editors, *SOUPS*, page 3. ACM, 2013.

[9] E. Hayashi and J. Hong. A diary study of password usage in daily life. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 2627–2630. ACM, 2011.

[10] H. G. Kayacık, M. Just, L. Baillie, D. Aspinall, and N. Micallef. Stability and effectiveness of user profiles in sensor-based authentication. In *IEEE CS Workshop on Mobile Security Technology (MoST)*, 2014.

[11] N. Micallef, M. Just, L. Baillie, and G. Kayacik. Non-intrusive and transparent authentication on smart phones. In *Trust and Trustworthy Computing*, pages 271–272. Springer, 2013.

[12] R. W. Reeder and S. E. Schechter. When the password doesn't work: Secondary authentication for websites. *IEEE Security & Privacy*, 9(2):43–49, 2011.

[13] O. Riva, C. Qin, K. Strauss, and D. Lymberopoulos. Progressive authentication: Deciding when to authenticate on mobile phones. In *Proceedings of the 21st USENIX Conference on Security Symposium*, Security'12, pages 15–15, Berkeley, CA, USA, 2012. USENIX Association.

[14] J. Seifert, A. De Luca, B. Conradi, and H. Hussmann. Treasurephone: Context-sensitive user data protection on mobile phones. In *Proceedings of the 8th International Conference on Pervasive Computing*, Pervasive'10, pages 130–137, Berlin, Heidelberg, 2010. Springer-Verlag.

[15] E. Shi, Y. Niu, M. Jakobsson, and R. Chow. Implicit authentication through learning user behavior. In M. Burmester, G. Tsudik, S. S. Magliveras, and I. Ilic, editors, *ISC*, volume 6531 of *Lecture Notes in Computer Science*, pages 99–113. Springer, 2010.