Universal Authentication: Towards Accessible Authentication for Everyone

Yang Wang
Syracuse University
School of Information Studies
ywang@syr.edu

ABSTRACT

Logging into a system or website with user names and passwords (i.e., authentication) is an essential part of people's everyday computer/Internet activities. However, this mundane operation can be daunting for users with disabilities. In this position paper, I describe my interests in this workshop around the topic of accessible authentication based on my ongoing work on the Inclusive Web project[1].

1. Introduction

Internet has become an integral part of people's daily life. Websites from web email to online shopping, from online banking to social media usually require users to log in to provide personalized services. Authentication ensures that users are who they said they are. Existing authentication schemes such as Personal Identification Numbers (PINs) and textual passwords are widely used. However, these schemes often provide lower security protection or worse usability to people with disabilities (e.g., [D'Arcy & Feng, 2006][Ma et al., 2012][Holman et al., 2008]). For instance, people with motor impairments have difficulty using mouse and keyboard, and thus they may not be able to type special characters which require typing a combination of keys – this decreases the password search space entropy, makes it easier to crack the password (e.g., using brute force attacks), and in turn yields lower security protection [Helkala, 2012].

To make computing truly inclusive, it is critical to develop accessible authentication mechanisms that anyone can use. A representative scenario is that anyone, regardless of what disability they may have, can log into a public terminal with a reasonable amount of effort. The authentication process should be secure and fast to prevent from various attacks such as shoulder surfing (i.e., someone stands close to the user and try to observe what password the user uses to log in the system).

Some existing systems cater their services to users with specific disability. While this is a laudable practice to provide better user experience, the fact that the systems or the service providers know what specific disability a user has can put the user at disadvantages. For instance, the user may experience price discrimination in insurance policies [Coroama & Langheinrich, 2006]. Therefore, there is a genuine need to provide privacy-enhancing personalization for people with disability, i.e., enabling users with disabilities without the system knowing whether a user has a disability and what specific disability she has.

[1] http://inclusiveweb.org/

2. Accessibility of Authentication Mechanisms

Bonneau et al. proposed a comprehensive framework for evaluating and comparing web authentication mechanisms [Bonneau et al. 2012]. One of the criteria in that framework is accessibility. They also used the widely used password scheme as the baseline for comparison. Generally speaking, the longer the passwords, the more secure they are [Kelley et al., 2011]. However, it is practically difficult for people to remember long passwords, thus the security hurts the usability. Various alternative authentication methods have been proposed in the literature including variants of password schemes such as Passphrases [Porter, 1982] and one-time password schemes [Haller, 1995]; tactile authentication methods [Kuber & Sharma, 2010] [Azenkot et al., 2012]; graphical passwords [Biddle, et al., 2012], [Chiasson et al., 2008]; eye-gaze method [De Luca et al., 2007]; audio-based methods such as Passtones [Brown & Doswell, 2010] and Musipass [Gibson et al., 2009]; methods using biometrics data such as FingerID [Alotaibi & Argles, 2011], a system using iris information [Chong et al., 2005], BioID [Frischholz & Dieckmann, 2000], and electrocardiogram (ECG) - based systems [Shen, 2008]. "ECG is suitable for all people including disability population because ECG is vital sign for life" [Shen, 2008]. But, measuring ECG still requires special hardware.

Another promising alternative is hardware token-based authentication such as RSA SecureID [RSA, 2011] and PICO [Stajano, 2011]. For instance, PICO is a dedicated hardware device that contains a user's credential (cryptographic token) that can be used to authenticate a user with a service or application. A user uses her PICO to take a picture of a 2-D visual code (app self-signed certificate of its public key) displayed on the service/app and authenticates her using secure multi-channel protocols (e.g., [McCune et al., 2005][Stajano et al., 2010]). The PICO needs to be securely paired with the service/app before user authentication. To protect against PICO being used by other people, PICO only unlocks itself when it is present with a set of pre-selected and pre-paired devices called Picosiblings. Like the ECG-based systems, PICO also requires special hardware. There are other token-based schemes solely designed for mobile phones such as Phoolproof [Parno et al., 2006], but they often still require the use of passwords.

Overall, four key gaps were discovered in this area: (1) existing accessible authentication techniques are mostly targeted at specific disability, and thus do not support other disabilities or a combination of different disabilities, making them inaccessible for everyone; (2) arguably, the ECG and hardware token-based schemes can work for everyone but they tend to require special hardware; (3) authentication processes enabled by these schemes tend to be slow, which negatively affect user experience; (4) users

with certain disabilities use authentication techniques that fit their needs but that can also reveal their disability conditions to the service providers, which could put users at disadvantages (e.g., price discrimination).

3. Goals of Universal Authentication

To enable practical authentication for everyone, five goals (I call them the "SUPER" principles) need to be satisfied. Examples of measures are also provided.

Secure: the authentication mechanism is secure against the common security attacks. (search space entropy, circumvention difficulty)

Usable: the authentication mechanism is usable for everyone. (transaction time, time delay caused by human error, subjective rating, cognitive load, physical effort)

Privacy-preserving: the authentication mechanism can conceal disability from the host system. (keystroke patterns, data leakage, and transaction time)

Effective: the authentication mechanism is effective in accurately logging users into the system. (identification rate, false acceptance rate, and false rejection rate)

Reachable/Accessible: the authentication mechanism works with public terminals. (system requirements, browser requirements)

4. Acknowledgements

This paper is based upon work developed under a Sub-recipient Agreement that is sponsored by the US Department of Education, Award Number H33A130057. Any opinions, findings, conclusions or recommendations expressed herein are those of the author(s) and do not necessarily reflect the views of the United States Department of Education or Carnegie Mellon University.

5. References

1. Alotaibi, S.J. and Argles, D. FingerID: A new security model based on fingerprint recognition for personal learning environments (PLEs). *2011 IEEE Global Engineering Education Conference (EDUCON)*, (2011), 142–151.
2. Azenkot, S., Rector, K., Ladner, R., and Wobbrock, J. PassChords: secure multi-touch authentication for blind people. *Proceedings of the 14th international ACM SIGACCESS conference on Computers and accessibility*, ACM (2012), 159–166.
3. Biddle, R., Chiasson, S., and Van Oorschot, P.C. Graphical passwords: Learning from the first twelve years. *ACM Comput. Surv. 44*, 4 (2012), 19:1–19:41.
4. Bonneau, J., Herley, C., van Oorschot, P.C., and Stajano, F. The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes. *2012 IEEE Symposium on Security and Privacy (SP)*, (2012), 553–567.
5. Brown, M. and Doswell, F.R. Using passtones instead of passwords. *Proceedings of the 48th Annual Southeast Regional Conference*, ACM (2010), 82:1–82:5.
6. Chong, S.C., Teoh, A.B.J., and Ngo, D.C.L. Iris Authentication Using Privatized Advanced Correlation Filter. In D. Zhang and A.K. Jain, eds., *Advances in Biometrics*. Springer Berlin Heidelberg, 2005, 382–388.
7. Coroama, V. and Langheinrich, M. Personalized Vehicle Insurance Rates - A Case for Client-Side Personalization in Ubiquitous Computing. Workshop on Privacy-Enhanced Personalization. *CHI 2006 22*, (2006), 56–59.
8. Frischholz, R.W. and Dieckmann, U. BiolD: a multimodal biometric identification system. *Computer 33*, 2 (2000), 64–68.
9. Gibson, M., Renaud, K., Conrad, M., and Maple, C. Musipass: authenticating me softly with "my" song. *Workshop on New security paradigms workshop*, ACM (2009), 85–100.
10. Haller, N. The S/KEY One-Time Password System. 1995. http://tools.ietf.org/html/rfc1760.
11. Helkala, K. Disabilities and Authentication Methods: Usability and Security. *International Conference on Availability, Reliability and Security (ARES)*, (2012), 327–334.
12. Holman, J., Lazar, J., and Feng, J. Investigating the Security-related Challenges of Blind Users on the Web. In P.L. BSc, J.C.M., , CEng MIEE and P.R.M. Ceng, eds., *Designing Inclusive Futures*. Springer London, 2008, 129–138.
13. John D'Arcy and Jinjuan Feng. Investigating Security-Related Behaviors Among Computer Users With Motor Impairments. (2006).
14. Kelley, P., Komanduri, S., Mazurek, M.L., et al. *Guess Again (and again and again): Measuring Password Strength by Simulating Password-Cracking Algorithms*. 2011.
15. Kuber, R. and Sharma, S. Toward tactile authentication for blind users. *Proceedings of the 12th international ACM SIGACCESS conference on Computers and accessibility*, ACM (2010), 289–290.
16. De Luca, A., Weiss, R., and Drewes, H. Evaluation of eye-gaze interaction methods for security enhanced PIN-entry. *Proceedings of the 19th Australasian conference on Computer-Human Interaction: Entertaining User Interfaces*, ACM (2007), 199–202.
17. Ma, Y., Feng, J.H., Kumin, L., Lazar, J., and Sreeramareddy, L. Investigating authentication methods used by individuals with down syndrome. *Proceedings of the 14th international ACM SIGACCESS conference on Computers and accessibility*, ACM (2012), 241–242.
18. McCune, J.M., Perrig, A., and Reiter, M.K. Seeing-Is-Believing: Using Camera Phones for Human-Verifiable Authentication. *IEEE Symposium on Security and Privacy*, IEEE Computer Society (2005), 110–124.
19. Parno, B., Kuo, C., and Perrig, A. Phoolproof phishing prevention. *Proceedings of the 10th international conference on Financial Cryptography and Data Security*, Springer-Verlag (2006), 1–19.
20. Porter, S.N. A password extension for improved human factors. *Computers & Security 1*, 1 (1982), 54–56.
21. RSA. *RSA SecurID Two-factor Authentication*. 2011.
22. Shen, T.-W. Applied ECG biometric technology for disability population personalization. *International Convention on Rehabilitation Engineering & Assistive Technology*, Singapore Therapeutic, Assistive & Rehabilitative Technologies (START) Centre (2008), 103–107.
23. Sonia Chiasson, Alain Forget, and Robert Biddle. Accessibility and Graphical Passwords. (2008).
24. Stajano, F., Wong, F.-L., and Christianson, B. Multichannel protocols to prevent relay attacks. *Proceedings of the 14th international conference on Financial Cryptography and Data Security*, Springer-Verlag (2010), 4–19.
25. Stajano, F. Pico: no more passwords! *Proceedings of the 19th international conference on Security Protocols*, Springer-Verlag (2011), 49–81.