One-Step Two-Factor Authentication with Wearable Bio-Sensors

John Chuang
chuang@ischool.berkeley.edu
University of California, Berkeley

ABSTRACT
Two-step verification does not imply two-factor authentication. Conversely, two-factor authentication may not require two-step verification. With ubiquitous bio-sensors, we can strive for one-step two-factor authentication for wearable computing applications.

Author Keywords
wearable authentication, multi-factor authentication, 2FA, bio-sensory computing, passthought

Wearable computing brings new challenges and opportunities for user authentication. On the one hand, wearable devices typically lack a keyboard, and oftentimes even a touchscreen. This presents a fundamental challenge to implementing password or PIN-based authentication. On the other hand, many wearable devices incorporate a range of physiological and kinesthetic sensors. The signals captured by these sensors can conceivably be leveraged for novel authentication techniques that are both more secure and more usable.

For example, fingerprint sensors are already incorporated into smartphones such as the Apple iPhone 5S and the Samsung Galaxy S5 specifically for authentication purposes. Accelerometers capture precise body movements that can be used for gesture-based or gait-based authentication. Motion control sensors offer the promise of authentication based on hand geometry while the hand is in motion. Advances in voice-recognition software allow for voice-based authentication. New consumer-grade bio-sensors that can capture heart, muscle, and even brainwave signals (ECG, EMG, EEG respectively) are now being integrated into devices to be worn on the wrist, arm, and the head. Each of these physiological signals has also been applied to authentication purposes [1, 19, 7].

Going beyond traditional single-factor authentication using biometric signals (e.g., fingerprints, iris patterns), the new standard for consumer wearables authentication should be *one-step two-factor authentication*.

There is some ambiguity in the concepts of two-step verification and two-factor authentication. For example, as of this writing, the Wikipedia entry for "two-factor authentication" redirects to the article for "two-step verification" [20]. The term "two-step verification" highlights the fact that the user has to execute two separate steps in the authentication process. Depending on the type of authenticator presented for each step, a two-step verification may be implementing either a one-factor or a two-factor authentication. To be considered a two-factor authentication, the two presented authenticators must belong to two *distinct* factor types (e.g., a knowledge factor, a possession factor, an inherence factor).

Conventional wisdom and prevailing terminology may lead us to conclude that two-factor authentication methods must also be two-step verification methods. This is congruent with our understanding of the tradeoff between security and usability. Requiring the user to present a second factor adds to the security of the system, but the extra verification step also adds a hassle cost that is deterring more widespread adoption of two-factor authentication. As a concrete illustration of the adoption hurdle faced by two-step two-factor authentication, consider the following – how many smartphone owners will actually choose to unlock their smartphones by entering their passcode on the touchscreen followed by placing their finger on the fingerprint sensor?

Is it possible to design one-step two-factor authentication methods, where two different factors are presented in a single user step?

Keystroke dynamics [15] is a well-established behavioral biometric [21] that fits the one-step two-factor criteria. In this method, when a user types in a password (the knowledge factor), the typing rhythm (the inherence factor) is also employed to authenticate the user. There are numerous commercial products that implement this technique. However, this method does not translate easily to the wearable computing paradigm where typing and password are both being phased out.

Authentication by voice is another well-established authentication method that could fit the one-step two-factor criteria. Specifically, in text-dependent speaker recognition [5, 12, 11], users simultaneously present the inherence factor (their voice) and the knowledge factor (the pre-determined phrase

 This research was supported in part by the National Science Foundation under award CCF-0424422 (TRUST).
WAY'14, July 9, 2014, Menlo Park, California.

to utter). The potential pitfall to this approach as a two-factor method is the difficulty of keeping the knowledge factor secret, when the user has to authenticate within hearing range of others.

Various multi-modal biometric authentication systems have been proposed, where data from multiple biometric traits are fused to boost authentication accuracy. Some of these systems can be considered "one-step multi-modal", since the biometric traits can be collected in a single step. They include: 2D and 3D face captures [6], hand geometry and palmprint [13], face and voice traits [4, 3, 8, 10], and even face, voice, and lip movement [9]. However, they cannot be considered "one-step multi-factor" since the biometric traits all belong to the same inherence factor category.

Two recent results provide affirmative answers to the feasibility of one-step two-factor authentication for wearable computing. Both of them leverage bio-signals captured using consumer-grade bio-sensors. In the first case, the company Bionym is developing a $79 Nymi wristband [1] that offers one-step two-factor authentication. Specifically, the two factors are the possession factor (i.e., the wristband as the physical token) and the inherence factor (i.e., the cardiac rhythm that is unique to the user). Once authenticated, the user will remain authenticated until the wristband is removed.

In the second case, the Passthoughts study at Berkeley [7] demonstrated user authentication at a 99% accuracy level using brainwave signals, where the users performed a single step of thinking their "passthought" while wearing a $99 consumer-grade brainwave sensing headset from Neurosky. Unlike earlier work on EEG-based authentication where all users perform identical mental tasks [14, 16, 17, 18, 2], the passthought approach involves a mental task that may include a user chosen secret, e.g., mentally humming a tune from the user's favorite song, motor imagery of the user's favorite sport, or visual counting of objects of a specific color chosen by the user. Thus, the presented "passthought" contains two distinct factors, the knowledge factor that comes from the chosen secret thought, and the inherence factor that comes from the user's brain. Unlike traditional biometrics, a passthought can be easily replaced on demand, simply by having the user choose a different mental thought. In fact, by integrating a physical token with the headset, or by considering the headset itself as the physical token, this approach can now realize *one-step three-factor authentication*.

With continued innovations in bio-sensing technologies and their incorporation into wearable computing devices, we can anticipate many new opportunities for one-step two-factor authentication using bio-signals. For example, 3D motion controllers (e.g., Leap Motion) can be designed to recognize both hand geometry (inherence) and hand gesture (knowledge) with a single wave by the user. Gesture control armbands (e.g., Myo) can capture muscular electrical signals (i.e., electromyogram) that may encode both the inherence and knowledge factors of an arm movement.

For one-step two-factor authentication systems to be ready for broad adoption, they must perform well under varying operating conditions, including stress, fatigue, and possibly even duress. At the same time, they must also be robust against impersonation attacks. Third, they must continue to work over extended periods of time. This requires an understanding the temporal stability of signals and developing strategies for continuous or on-demand re-calibration. If well executed, one-step two-factor authentication systems can offer vast improvements to the security *and* usability of user authentication at the same time.

REFERENCES

1. Bionym Nymi. `http://www.bionym.com/`.
2. Corey Ashby, Amit Bhatia, Francesco Tenore, and Jacob Vogelstein. Low-cost electroencephalogram (eeg) based authentication. In *Proceedings of 5th International IEEE EMBS Conference on Neural Engineering*, April 2011.
3. Elizabeth Saers Bigün, Josef Bigün, Benoît Duc, and Stefan Fischer. Expert conciliation for multi modal person authentication systems by bayesian statistics. In *Audio-and Video-based Biometric Person Authentication*, pages 291–300. Springer, 1997.
4. Roberto Brunelli and Daniele Falavigna. Person identification using multiple cues. *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, 17(10):955–966, 1995.
5. Michael J Carey, Eluned S Parris, and J Bridle. A speaker verification system using alpha-nets. In *Acoustics, Speech, and Signal Processing, 1991. ICASSP-91., 1991 International Conference on*, pages 397–400. IEEE, 1991.
6. Kyong Chang, Kevin Bowyer, and Patrick Flynn. Face recognition using 2d and 3d facial data. In *ACM Workshop on Multimodal User Authentication*, pages 25–32, 2003.
7. John Chuang, Hamilton Nguyen, Charles Wang, and Benjamin Johnson. I think, therefore i am: Usability and security of authentication using brainwaves. In *Proceedings of 2013 Workshop on Usable Security*, 2013.
8. Benoît Duc, Gilbert Maître, Stefan Fischer, and Josef Bigün. Person authentication by fusing face and speech information. In *Audio-and Video-based Biometric Person Authentication*, pages 311–318. Springer, 1997.
9. Robert W Frischholz and Ulrich Dieckmann. Biold: a multimodal biometric identification system. *Computer*, 33(2):64–68, 2000.
10. T Hazen, Eugene Weinstein, Ryan Kabir, Alex Park, and Bernd Heisele. Multi-modal face and speaker identification on a handheld device. *Proc. Wkshp. Multimodal User Authentication*, pages 120–132, 2003.
11. Matthieu Hébert. Text-dependent speaker recognition. *Springer Handbook of Speech Processing*, pages 743–762, 2008.

12. Alan Higgins, L Bahler, and J Porter. Speaker verification using randomized phrase prompting. *Digital Signal Processing*, 1(2):89–106, 1991.

13. Ajay Kumar, David CM Wong, Helen C Shen, and Anil K Jain. Personal verification using palmprint and hand geometry biometric. In *Audio-and Video-Based Biometric Person Authentication*, pages 668–678. Springer, 2003.

14. Sebastien Marcel and Jose del R. Millan. Person authentication using brainwaves (eeg) and maximum a posteriori model adaptation. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 29(4), April 2007.

15. Fabian Monrose and Aviel Rubin. Authentication via keystroke dynamics. In *Proceedings of the 4th ACM conference on Computer and communications security*, pages 48–56. ACM, 1997.

16. Ramaswamy Palaniappan. Electroencephalogram signals from imagined activities: A novel biometric identifier for a small population. In *IDEAL 2006, LNCS 4224*, pages 604–611, 2006.

17. Ramaswamy Palaniappan. Two-stage biometric authentication method using thought activity brain waves. *International Journal of Neural Systems*, 18(1):59–66, 2008.

18. M. Poulos, M. Rangoussi, N. Alexandris, and A. Evangelou. Person identification from the eeg using nonlinear signal classification. *Methods of Information in Medicine*, 2002.

19. M. Suresh, P.G. Krishnamohan, and S.H. Mallikarjun. Electromyography analysis for person identification. *International Journal of Biometrics and Bioinformatics*, 5(3), 2011.

20. Wikipedia. Two-factor authentication — Wikipedia, the free encyclopedia, 2014. [Online; accessed 22-May-2014].

21. Roman V Yampolskiy and Venu Govindaraju. Behavioural biometrics: a survey and classification. *International Journal of Biometrics*, 1(1):81–113, 2008.