New Directions for User Authentication: Reflex instead of Reflection

Adrian Perrig Dawn Song
UC Berkeley
{perrig,dawnsong}@cs.berkeley.edu

1 Introduction

Password-based user authentication is presently the main mechanism for a user to prove its identity to a computer. The security of a system is limited by the security of the weakest link — but unfortunately, the weakest link is often the human. Designing a more secure password authentication system is an open research challenge.

In this work, we are interested in user authentication systems with the following properties:

- Low setup cost.
- Low false positive rate (secure).
- Low false negative rate (usable).
- Prevent weak passwords.
- Secure even if an adversary is witnessing multiple authentications (shoulder surfing).
- Torture-robust authentication, i.e., the user cannot communicate the authentication information to others, even under duress (sometimes also referred to as rubber-hose crypto).
- No additional equipment required (e.g., no tokens, no smart cards).
- Based on something that humans are naturally good at.

In our research on *hash visualization* [5] and Déjà Vu [1], we present a first step in designing an authentication system with these properties. Déjà Vu is based on a human cognitive strength: the recognition of previously seen images. This is an important improvement over password authentication, which is based on a cognitive weakness: the precise recall of high-entropy strings.

In this work, we focus on two problems: authentication secure against shoulder surfing and torture-robust authentication (so people would not be able to disclose secrets even if under duress). First, we propose an authentication system, Map, that is more secure with respect to shoulder surfers. Second, we present the Focus Tracker systems as an attempt towards torture-robust authentication. The system is based on our observation that a system that only relies on human reflexes, without requiring reflection (or thought), might be a good candidate to provide this property.

1.1 Terminology

In a user authentication system, the authentication server (*authenticator*) authenticates the user, by challenging her with a *user authentication task*.

2 The Map User Authentication System

People often need to authenticate themselves in the presence of others. Bystanders repeatedly watching the authentication process of a user should not be able to authenticate themselves as that user.

We would like to design a user authentication system based on an observation analogous to car driving. In car driving, navigating a car through an area is memorable for the driver, but not the passengers. So in a user authentication system secure against shoulder surfing, a user can authenticate herself, but not the people who are with her.

We propose an example system, the Map system, as a starting point. In this system, a user needs to set up the user authentication information, which could be a real or imaginary world. We call this world the user's Private World. The system could function at various granularities: a coarse-grained world which contains features at the level of roads, pathways, or hallways in a building; or a fine-grained world with various objects, with which the user can interact with.

Let us first consider the simpler case of a coarse-grained world. The user's Private World could consist of a city. The authentication task could be to drive from a random origin to another random destination, both selected by the authenticator. The authentication task is to move from the origin to the destination. A sample authentication task could be to move from the post office to a coffee shop. Note that a bystander can only see the user navigating through the city, and learns little information if our observation is correct.

A finer-grained world might also allow users to enter buildings and interact with objects. In such a world, the authentication task could be to go to the supermarket, pick up a bottle of water, and use it to water Grandmother's flowers. Arbitrary complicated authentication tasks are imaginable, including using a virtual computer terminal to accomplish another authentication task.

3 The Focus Tracker User Authentication System

A user authentication tasks should be based on users' reflexes, without requiring the user to actively think. We call such an approach *reflex instead of reflection*. Because reflexes happen subconsciously, it is hard for people to control them, or even to adopt new patterns to impersonate others.

As an example, we propose to use the eye movement reflex. We could track the eye movement pattern while a user reads text or looks at an image.

Researchers have previously proposed to use inter-keystroke timing patterns [2, 4] and users' voices [3] for authentication. These examples could be considered as biometrics authentication, but are also examples for our approach, reflex instead of reflection.

4 Conclusion and Future Work

Robustness to shoulder surfing is also an important requirement, as people frequently authenticate themselves to a system in the presence of others. The Map system exploits that people have a hard time learning a world if they cannot move around under their own command. By carefully monitoring failed authentication attempts we can detect attempts of others that are trying to become accustomed to a Private World. An interesting conjecture (which might already be well known in the learning community) is that getting feedback on errors is essential in human learning. So if a person is not moving through the world by herself, she does not receive this crucial error feedback.

To strengthen the Map authentication system, the authentication server could constantly change the Private World, similarly to construction in the real world, to which we can quickly adapt. Future research will show how well these systems work in practice.

Torture-robust authentication appears to be a promising direction for the design of user authentication systems, to prevent users from selecting weak passwords, from writing them down, and from telling them to others. The Focus Tracker authentication system is an initial idea for such a system.

References

[1] R. Dhamija and A. Perrig. Déjà vu: A user study, using images for authentication. In *Proceedings of the 9th USENIX Security Symposium*, August 2000.

[2] R. Joyce and G. Gupta. Identity authentication based on keystroke latencies. *Communications of the ACM*, 33(2):168–176, Feb. 1990.

[3] F. Monrose, M. K. Reiter, Q. Li, and S. Wetzel. Cryptographic key generation from voice. In *Proceedings of the IEEE Symposium on Research in Security and Privacy*, pages 202–212, Oakland, CA, May 2001. IEEE Computer Society, Technical Committee on Security and Privacy, IEEE Computer Society Press.

[4] F. Monrose, M. K. Reiter, Q. Li, and S. Wetzel. Password hardening based on keystroke dynamics. *International Journal of Information Security*, 2001. Online First Publication. Published in print form in a future issue.

[5] A. Perrig and D. Song. Hash visualization: A new technique to improve real-world security. In *Proceedings of the 1999 International Workshop on Cryptographic Techniques and E-Commerce (CryTEC '99)*, 1999.