Jonathan Chen and Noam Zilberstein
November 2, 2014 23:51
CIS 700: Cryptography
Due: Monday, November 3

Authentication Using Keystroke Dynamics

1 Problem

We wish to develop a protocol to authenticate users without the use of a password. Passwords have many inherent problems. Several well known companies such as Dropbox and Apple have recently been targets of large scale security breaches in which passwords were compromised. Because of this risk, users are urged to use different passwords for each account. It is very difficult to come up with and remember enough secure passwords considering how many online accounts most people have today.

Many common websites such as Facebook and Dropbox are already encouraging the use two-factor authentication to subvert these issues. These forms of authentication usually involve confirming the possession of a piece of hardware. Instead, we would like to analyze another authentication factor that does not require possession of additional hardware. This authentication scheme is based on keystroke dynamics; the user is authenticated based on the timing of his/her keystrokes when typing a particular phrase (such as their name). When typing, each individual has their own typing pattern consisting of lag/dwell time (how long a key is pressed) and rhythms (typing certain clusters of letters faster). This typing pattern translates into a typing signature which can be measured and used as a form of biometric data.

2 Approach/Projected Timeline

Our approach is to record and analyze the keystroke dynamics of users typing their name or username. We can then make a distribution of this data and form conclusions about a person's individual typing patterns. This information can be used to authenticate a user's identity without requiring a password.

We plan to implement this by querying the user for a sufficient sample of the biometric data related to their typing patterns. We then use this information to construct a unique identity for the user by combining the plaintext (their username) with the typing biometric and hashing that result with a known hashing algorithm. Our application will then verify this hash and authenticate the user.

- By mid-November: familiarize with literature and current research on TBPA.
- By end of November: implementation of algorithm
- By December: debugging and formalizing final paper

3 Results

3.1 Expected Results

By the end of the semester, we expect to have a working implementation of our authentication algorithm using keystroke dynamics. Users should be able to log in without a password, and our program can verify with significant confidence the users' signature.

3.2 Backup Results

Working implementation of our authentication algorithm, with a larger tolerance for variance, making it more susceptible to forgery, but verifies the authenticity of the user when the corresponding user is logging in.

3.3 Stretch Results

Ideally, we hope to have an implementation that is immune to forgery. Optimally, we would like the biometric data to be unique to each person and the typing signature to be unforgeable. We would like to have a fault tolerance that allows the real user some variance but invulnerable to impersonators.

References

[1] Francesco Bergadano, Daniele Gunetti, and Claudia Picardi. User authentication through keystroke dynamics. *ACM Trans. Inf. Syst. Secur.*, 5(4):367–397, November 2002.

[2] S. Bleha, C. Slivinsky, and B. Hussien. Computer-access security systems using keystroke dynamics. *IEEE Trans. Pattern Anal. Mach. Intell.*, 12(12):1217–1222, December 1990.

[3] Soumik Mondal, Patrick Bours, and S. Z. Syed Idrus. Complexity measurement of a password for keystroke dynamics: Preliminary study. In *Proceedings of the 6th International Conference on Security of Information and Networks*, SIN '13, pages 301–305, New York, NY, USA, 2013. ACM.

[4] Fabian Monrose and Aviel D. Rubin. Authentication via keystroke dynamics. In *ACM Conference on Computer and Communications Security'97*, pages 48–56, 1997.

[5] Deian Stefan and Danfeng Yao. Keystroke-dynamics authentication against synthetic forgeries. In *CollaborateCom*, pages 1–8. IEEE, 2010.