Vision Statement

Team: Not Our (Seg)Fault
Project: AuthentiKey

15/10/2017

1 Team Members

Alex Wein (lead)	awein@umail.ucsb.edu
Ashlynn Cardoso (scribe)	ashlynncardoso@umail.ucsb.edu
Clara Frausto	cfrausto@umail.ucsb.edu
Caitlin Scarberry	caitlinscarberry@umail.ucsb.edu
William Bennett	wbennett@umail.ucsb.edu

2 What problem are we solving?

Computer systems are inseparable from modern daily life, making secure authentication more vital than ever. However, despite its many flaws, the most common authentication method remains the password. Users frequently re-use passwords across different platforms, which increases the severity of database breaches; users often set insecurely short passwords to make them easier to remember; and once a password has been acquired by a malicious party, that party can immediately use the password. Additional authentication is clearly required for a secure system.

3 How is it currently solved?

Multiple-factor authentication can mitigate some concerns about password security. Most methods, however, are often inconvenient. Two-factor authentication through a separate device such as a cellphone or Yubikey requires the user to have that device on hand, and a user who misplaces the device will be unable to log in. Biometric two-factor authentication removes the need for separate devices, but often relies on special hardware such as fingerprint scanners that are not present on many user devices.

4 How will we solve it?

The end goal of our project is a robust authentication system using keystroke dynamics. Keystroke dynamics, which analyze how a user types, are a biometric authentication method that avoids the pitfalls of both methods listed above. The vast majority of users interface with their devices through a keyboard, whether that is an on-screen mobile keyboard or the physical keyboard of a personal computer. This eliminates the need for separate devices or specialized hardware.

5 Milestones

1. In-browser keylogger to sample required keystroke dynamics data.
2. Public web interface for demonstrating authentication.
3. 80% accuracy in user identification through typing patterns data.
4. Develop a method to securely store each user's typing data, so that it cannot be used to mimic a user.
5. 90% accuracy in user identification.
6. A public web API that allows third parties to use AuthKey as a form of multiple authentication.

6 Implementation

The core technology is as follows:

- We will use the AWS machine learning service to create and test our machine learning models.
- Our backend will be a python web server, and use the python SDK for AWS ML to interface for us.
- JS/HTML/CSS for web portal
- As of yet undecided DB, security model

The technology/services we plan on using for workflow/team management is:

- Slack for communication. GitHub for code management and version control.
- Travis CI for continuous testing.
- Trello for task assignment/management.