Multi-Modal Continuous Authentication

Team Daemons

Stephanie Lew and Jiyi Zhang

Introduction

Team Daemons: Stephanie Lew and Jiyi Zhang

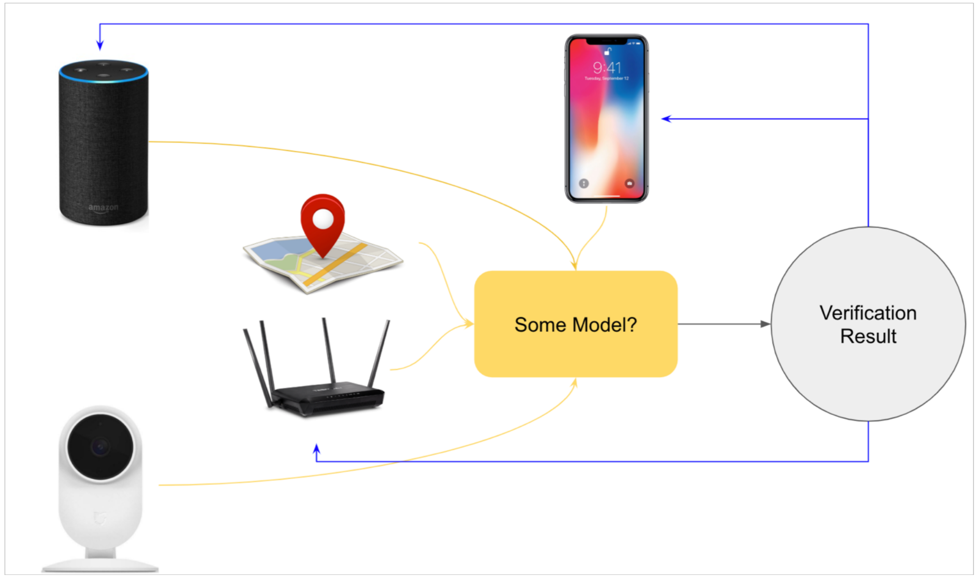
- Multi-Modal Continuous Authentication System fuses information collected from devices of different biometric sensing modalities to provide better security and smoother user experience

- Common authentication information includes:
  - Fingerprint collected from Touch ID
  - Face collected from phone Face ID and CCTV
  - Voice collected from Google Home/Echo
  - GPS location info collected from phone/watch
  - Behavior data from accelerometer/gyroscope

Problem Statement

Team Daemons: Stephanie Lew and Jiyi Zhang

- Our aim is to build a component-based system which combines the sensor capability and computation power of multiple different smart home devices to provide secure, robust, reliable and convenient authentication. In this system:
  - Every smart home device runs a submodule which takes in the device’s sensor input and gives a score describing the likelihood of owner presence.
  - All the submodules connect to the core processing component through an interface.
  - Core component constantly takes in scores from different devices and their respective timestamps to conduct real-time evaluation and produce the authentication decision.



Related Work

Team Daemons: Stephanie Lew and Jiyi Zhang

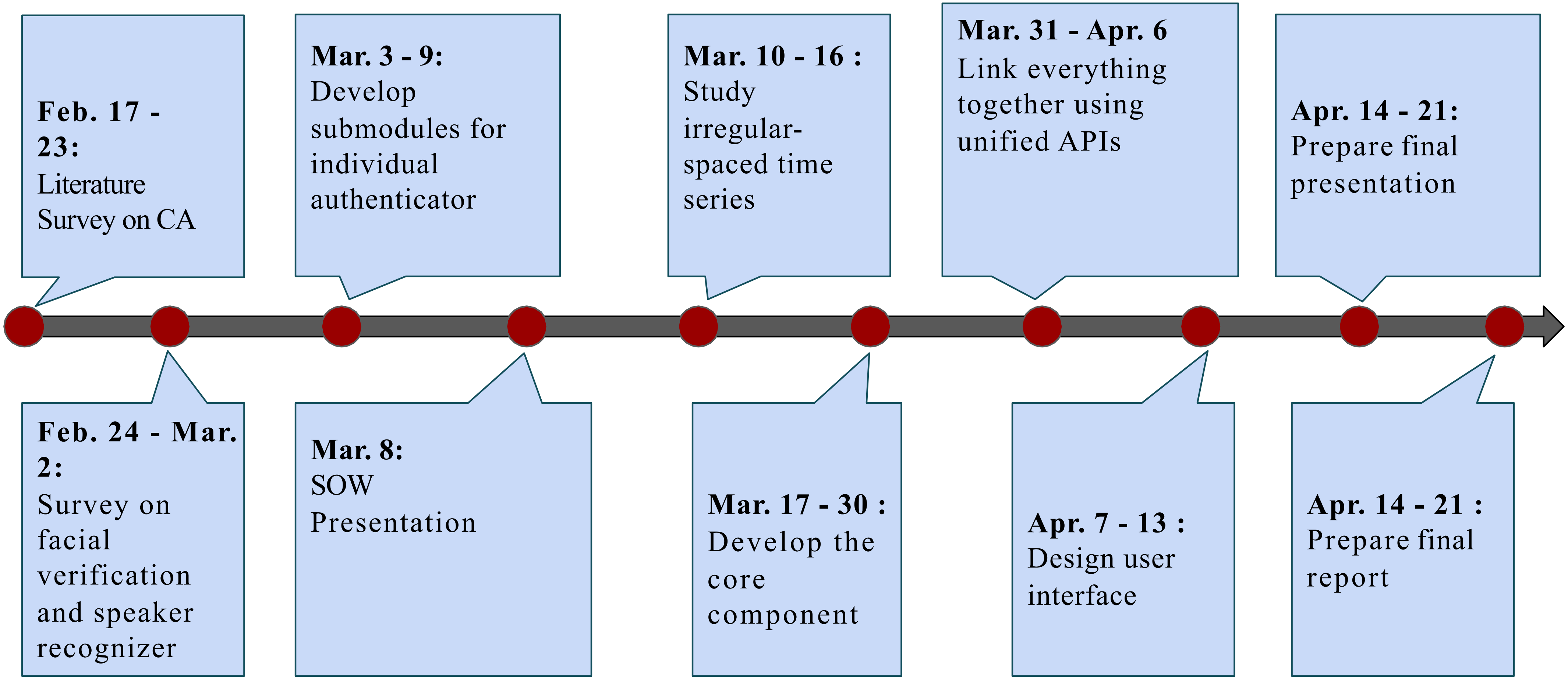
- A number of researches have upheld the need for more innovative authentication methods that aim to balance the trade-off between security and convenience. Current authentication approaches commonly fall into three categories:
    - Knowledge-based (E.g. Single sign-on)
    - Object-based (E.g. Token-based authentication in a form of hardware or software tokens)
    - Behavioral-based (E.g. behavioral biometric techniques based on SMS texting activities and messages)

- We will concentrate on combining multiple biometric modalities across devices using a general continuous authentication method.

- We envision that the new fusion system will be sensor-independent and is able to verify users in a variety of smart home configurations.

Project Timeline

Team Daemons: Stephanie Lew and Jiyi Zhang



Feb. 17 - 23: Literature Survey on CA

Feb. 24 - Mar. 2: Survey on facial verification and speaker recognizer

Mar. 3 - 9: Develop submodules for individual authenticator

Mar. 8: SOW Presentation

Mar. 10 - 16 : Study irregular-spaced time series

Mar. 17 - 30 : Develop the core component

Mar. 31 - Apr. 6 Link everything together using unified APIs

Apr. 7 - 13 : Design user interface

Apr. 14 - 21: Prepare final presentation

Apr. 14 - 21 : Prepare final report

Team Member Responsibilities

Team Daemons: Stephanie Lew and Jiyi Zhang

- All members will work on all tasks, lead of each task defined as follows:
  - Literature Survey: *Stephanie*
  - Designing biometric fusion system: *Jiyi*
  - Analysing results: *Stephanie*
  - Investigating for vulnerabilities: *Jiyi*
  - Testing possible defense: *Stephanie*

- Course deliverables
  - Presentation: *Stephanie*
  - Demo: *Jiyi*
  - Poster: *Stephanie*
  - Written Report: *Jiyi*

Project Budget

Team Daemons: Stephanie Lew and Jiyi Zhang

Item	Cost	Comments
Stephanie	Free	The best things in life are free
Jiyi	Free	The best things in life are free
Two Laptops	Free	The best things in life are free
Time	Free	The best things in life are free
Food	Free	The best things in life are free
Oxygen	Free	The best things in life are free

Potential Risks and Backup Plan

Team Daemons: Stephanie Lew and Jiyi Zhang

- Primary risk: the difficult part of our project is the design of the core component which combines scores from different authenticators meaningfully. We need to have a rigorous estimation of error bound based on the confidence threshold, sampling distribution and individual authenticator's precision and recall. Otherwise, our contribution will be less significant.

- We will have good amount of data for us to play around with and build the individual authenticators. However, it will be hard to collect data from actual smart home setting and test the whole system.

- As we divide the deliverables into several stages, we are quite safe. In the case that we are unable to solve the challenging part of the project, we can always fall back to simpler sub-problems

- In fact, using speech recognition to achieve continuous authentication would be a interesting problem as it brings a novel solution for the authentication on voice assistant type of keyboard-less smart home devices.

Bibliography

Team Daemons: Stephanie Lew and Jiyi Zhang

1. A. Dmitrienko, C. Liebchen, C. Rossow, and A.-R. Sadeghi. Security analysis of mobile two-factor authentication schemes. *Intel Technology Journal*, 18(4), 2014.
2. Duo Security. RSA-Proofing Our Duo Push Two-Factor Authentication. https://duo.com/blog/rsa-proofing-our-duo-push-two-factor-authentication. Accessed: 2017-09-21.
3. Duo Security. Two-Factor Authentication (2FA). https://duo.com/product/trusted-users/two-factor-authentication. Accessed: 2017-09-21.
4. Duo Security. What is Modern Two-Factor Authentication (2FA)?. https://duo.com/blog/what-is-modern-two-factor-authentication. Accessed: 2017-09-21.
5. GSuite Updates Blog. Better experience for SMS 2-Step Verification users with Google prompt. https://gsuiteupdates.googleblog.com/2017/07/better-experience-for-sms-2-step-verification.html. Accessed: 2017-10-11.
6. Gemalto. Mobile Push Authentication with Gemalto's SafeNet MobilePASS+. https://www2.gemalto.com/sas/mobilepass-plus-push-authentication.html Accessed 2017-10-10.
7. N. Karapanos, C. Marforio, C. Soriente, and S. Capkun. Sound-proof: Usable two-factor authentication based on ambient sound. In *USENIX Security Symposium*, pages 483–498, 2015.
8. R. K. Konoth, V. van der Veen, and H. Bos. How anywhere computing just killed your phone-based two-factor authentication. In *International Conference on Financial Cryptography and Data Security*, pages 405–421, 2016.
9. B. Shrestha, M. Shirvanian, P. Shrestha, and N. Saxena. The sounds of the phones: Dangers of zero-effort second factor login based on ambient audio. In *ACM SIGSAC Conference on Computer and Communications Security*, pages 908–919, 2016.
10. The Hacker News. Real-World SS7 Attack — Hackers Are Stealing Money From Bank Accounts. http://thehackernews.com/2017/05/ss7-vulnerability-bank-hacking.html. Accessed: 2017-09-21.
11. Twilio. Authy. https://www.twilio.com/docs/api/authy. Accessed: 2017-10-11.
12. XDA Developers. Android O will Improve SMS Authentication for Apps. https://www.xda-developers.com/android-o-will-improve-sms-authentication-for-apps/. Accessed: 2017-09-21.
13. Yubico. YubiKey NEO. https://www.yubico.com/products/yubikey-hardware/yubikey-neo/. Accessed: 2017-10-08.