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

SMART HOME

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.

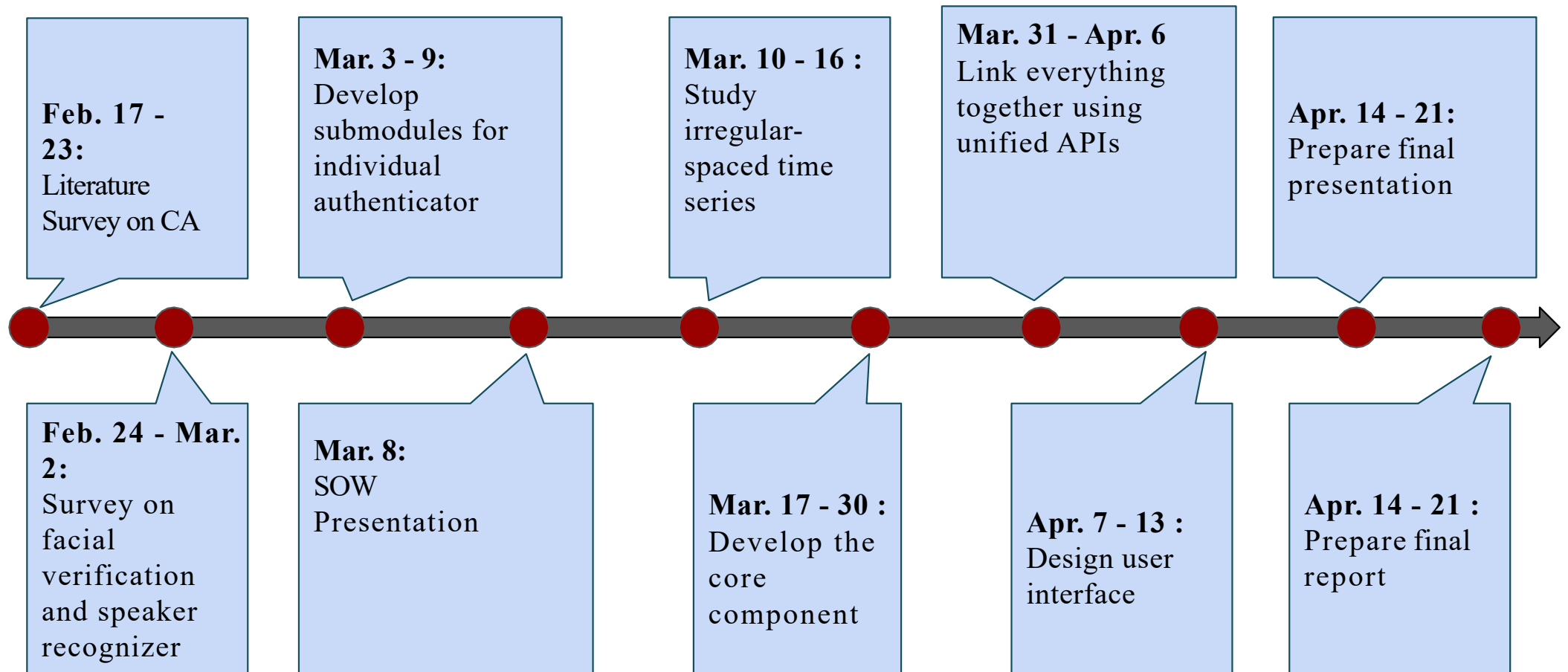3
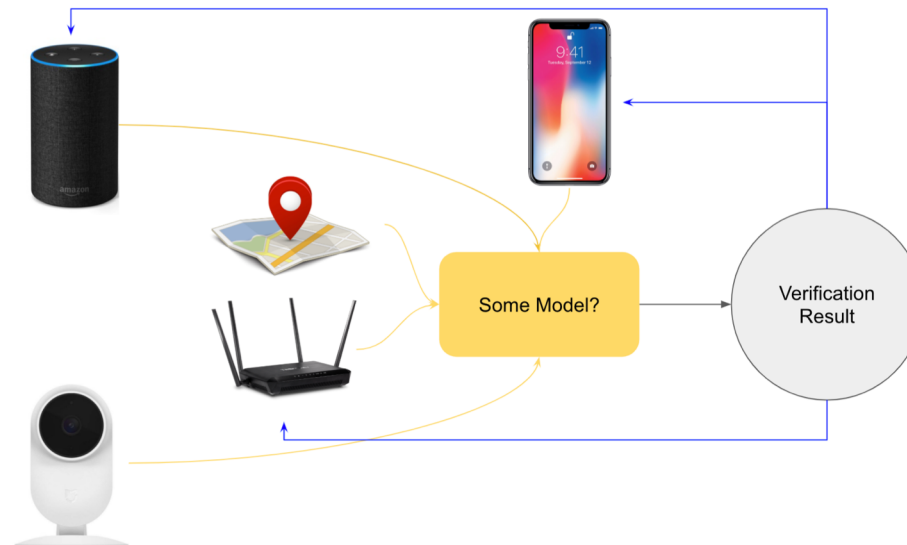
Related Work

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

Mar. 3 - 9: Develop submodules for individual authenticator

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

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

Apr. 14 - 21: Prepare final presentation

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

Mar. 8: SOW Presentation

Mar. 17 - 30 : Develop the core component

Apr. 7 - 13 : Design user interface

Apr. 14 - 21 : Prepare final report

5

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

<u>Team Daemons: Stephanie Lew and Jiyi Zhang</u>

- <u>Primary risk</u>: 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. J. Aviv, K. L. Gibson, E. Mossop, M. Blaze, and J. M. Smith, "Smudge attacks on smartphone touch screens." Woot, vol. 10, pp. 1–7, 2010.

[2] E. Chin, A. P. Felt, V. Sekar, and D. Wagner, "Measuring user confidence in smartphone se- curity and privacy," in Proceedings of the eighth symposium on usable privacy and security. ACM, 2012, p. 1.

[3] A. De Luca, A. Hang, F. Brudy, C. Lindner, and H. Hussmann, "Touch me once and i know it's you!: implicit authentication based on touch screen patterns," in proceedings of the SIGCHI Conference on Human Factors in Computing Systems. ACM, 2012, pp. 987–996.

[4] M. Frank, R. Biedert, E. Ma, I. Martinovic, and D. Song, "Touchalytics: On the applica- bility of touchscreen input as a behavioral biometric for continuous authentication," IEEE transactions on information forensics and security, vol. 8, no. 1, pp. 136–148, 2013.

[5] V. M. Patel, R. Chellappa, D. Chandra, and B. Barbello, "Continuous user authentication on mobile devices: Recent progress and remaining challenges," IEEE Signal Processing Magazine, vol. 33, no. 4, pp. 49–61, 2016.

[6] W. Meng, D. S. Wong, S. Furnell, and J. Zhou, "Surveying the development of biometric user authentication on mobile phones," IEEE Communications Surveys & Tutorials, vol. 17, no. 3, pp. 1268–1293, 2015.

[7] I. C. Stylios, O. Thanou, I. Androulidakis, and E. Zaitseva, "A review of continuous au- thentication using behavioral biometrics," in Proceedings of the SouthEast European Design Automation, Computer Engineering, Computer Networks and Social Media Conference. ACM, 2016, pp. 72–79.

[8] Y. Ashibani, D. Kauling, and Q. H. Mahmoud, "Design and implementation of a contextual-based continuous authentication framework for smart homes," Applied System Innovation, vol. 2, no. 1, p. 4, 2019.

[9] A. Al Abdulwahid, N. Clarke, I. Stengel, S. Furnell, and C. Reich, "Continuous and trans- parent multimodal authentication: reviewing the state of the art," Cluster Computing, vol. 19, no. 1, pp. 455–474, 2016.

[10] V. Radha and D. H. Reddy, "A survey on single sign-on techniques," Procedia Technology, vol. 4, pp. 134–139, 2012.

[11] F. Aloul, S. Zahidi, and W. El-Hajj, "Two factor authentication using mobile phones," in 2009 IEEE/ACS International Conference on Computer Systems and Applications. IEEE, 2009, pp. 641–644.

Bibliography

Team Daemons: Stephanie Lew and Jiyi Zhang

[12] I. Nakanishi, "Unconscious biometrics for continuous user verification," in Proceedings of the 8th International Conference on Signal Processing Systems, ser. ICSPS 2016. New York, NY, USA: ACM, 2016, pp. 20–25. [Online]. Available: http://doi.acm.org/10.1145/3015166.3015180

[13] K. Sitara and B. Mehtre, "Digital video tampering detection," Digit. Investig., vol. 18, no. C, pp. 8–22, Sep. 2016. [Online]. Available: https://doi.org/10.1016/j.diin.2016.06.003

6

[14] M. Carrillo, Cassandra, "Continuous biometric authentication for authorized aircraft personnel : a proposed design," 2003. [Online]. Available: https://calhoun.nps.edu/ handle/10945/1011

[15] R. Janakiraman, S. Kumar, S. Zhang, and T. Sim, "Using continuous face verification to improve desktop security," in Proceedings of the Seventh IEEE Workshops on Application of Computer Vision (WACV/MOTION'05) - Volume 1 - Volume 01, ser. WACV-MOTION '05. Washington, DC, USA: IEEE Computer Society, 2005, pp. 501–507. [Online]. Available: http://dx.doi.org/10.1109/ACVMOT.2005.120

[16] G. Chetty and M. Wagner, "Multi-level liveness verification for face-voice biometric au- thentication," in Proceedings of 2006 Biometrics Symposium, L. Williams, Ed. United States: IEEE, Institute of Electrical and Electronics Engineers, 2006, pp. 1–6.

[17] D.-J. Kim, K.-W. Chung, and K.-S. Hong, "Person authentication using face, teeth and voice modalities for mobile device security," IEEE Transactions on Consumer Electronics, vol. 56, no. 4, pp. 2678–2685, 2010.

[18] H. Saevanee, N. L. Clarke, and S. M. Furnell, "Multi-modal behavioural biometric au- thentication for mobile devices," in IFIP International Information Security Conference. Springer, 2012, pp. 465–474.

[19] E. Shi, Y. Niu, M. Jakobsson, and R. Chow, "Implicit authentication through learning user behavior," in International Conference on Information Security. Springer, 2010, pp. 99–113.

[20] X. Wang, T. Yu, O. Mengshoel, and P. Tague, "Towards continuous and passive authentica- tion across mobile devices: an empirical study," in Proceedings of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks. ACM, 2017, pp. 35–45.