CS6282: Statement of Work
8 Mar 2019

Multimodal Continuous Authentication

Stephanie Lew, Zhang Jiyi
Department of Computer Science, National University of Singapore
Email: stephanie_lew@u.nus.edu, jiyizhang@u.nus.edu

Keywords: Continuous Authentication, Biometrics, Multimodal biometrics, IoT, smarthomes

Executive Summary

It is well known that single sign-in solutions involving passwords and tokens are not very secure. Behavioral biometrics promises to be stronger authenticators as user behaviors can be learned from biometric features collected from embedded sensors in mobile devices. However, these methods still does not solve the single point-of-entry problem and is vulnerable to attacks. On the other hand, continuous authentication ensures that users' identity are verified continuously and strengthens the ability of a system to lock out imposters, even when the recognition ability of a single sample is not high. The use of multi-modal biometrics such as fusing face, voice, teeth modalities, or touchscreen gestures and textual information has proven to be more effective overall authenticators as compared to a single biometric authenticator alone. Our work tries to solve the problem of seamlessly authenticating users across multiple devices in a smart home setting by continuous authentication. We realise that the existing methods may not work in a complex setting like a smart home, where not all mobile devices are equipped with the same sensing modality. Furthermore, processing time costs increase as with the increase in the number of biometric modalities considered for continuous authentication. Thus, we propose a multi-modal continuous authentication system that is capable of fusing time-stamped information (e.g. face, voice and location) collected from devices of different common biometric sensing modalities, that is not limited by device hardware configurations. We envision that our research can open up new works for evaluating which combination of sensing modalities can be most effective for smart home use.

Introduction

Mobile devices are becoming an inherent part of our daily lives. Several applications in smartphones for example, provide us with the means to communicate, plan work and organize our lives. The smartphones collect and compile a growing amount of private information, to which access needs to be controlled to protect the privacy of the users.

To prevent unauthorized access to private data in smartphones, smartphone manufacturers employ traditional access control mechanisms using passcode, lock pattern and fingerprint. Previous work [1, 2, 3] has shown that these single sign-in methods are limited in terms of the security, usability and cost. In response, researchers propose continuous and passive authentication as an enhancement to existing schemes [4, 5]. A continuous and passive authentication system continually senses a user's interactions with the device and authenticates the user in

runtime based on behavioral data, such as touchscreen gestures, walking gait, face and voice modalities [6, 7]. These behavioral characteristics promise to be stronger authenticators than passwords alone. Also, continuous authentication promises to verify a user's identity continuously, strengthening the ability of the system of locking out impostors even when the recognition ability on an individual sample is not high.

Such information can be collected from different sources of context, like a device, a network, online resources or the environment, which can then be factored into an authentication decision, either as separate authentication factors or as an authentication adaptation, augmenting the decision to grant a user access to a given resource. While considering a high number of attributes for authentication would increase security and reliability, processing time cost would also increase. Ashibani et. al [8] suggests that any proposed solution should contain contextual attributes that do not require direct user interaction and the verification functions should work in the background without any response delay.

In this project, we will focus on continuously authenticating users who own multiple smart home devices, using a multi-modal biometric approach.

Problem Statement

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. This core component constantly takes in scores from different devices and their respective timestamps to conduct real-time evaluation and produce the authentication decision. The evaluation should be done in such a way that the score itself is independent of the sampling rate and type of sensor activated at the moment of authentication. A higher sampling frequency increases the confidence of the decision while a lower sampling frequency does the opposite. Adaptive sampling is applied to maintain the confidence level above a minimum threshold while avoiding hogging the computation resources for prolonged time period.

Many smart home devices like security cameras and voice assistants can be controlled through end-user devices like smartphones and tablets. Notably, current passcode-based and cryptographic-based authentication methods for such devices are neither convenient nor secure. Though biometric authentication methods such as fingerprint verification and facial verification have become more popular recently, they are often used as a simple replacement of the password authentication, which is deemed unsafe. Hence, the issue of single point of failure still remains unresolved. When a mobile device using such kind of authentication is in possession of an adversarial, the attacker will have enough time and resource to achieve partial or total break eventually, and may result in serious consequences.

Related Work

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, object-based and behavioural-

based.

One type of knowledge-based authentication is Single sign-on, which relies on the user to provide one login credential to access many other applications [9, 10]. This increases convenience and reduce the burden of the user having to remember many passwords. They assume that the user's identity is legitimate throughout the access session, which is not necessarily the case (an imposter may try to use the applications after the initial login).

An object-based approach can be taken to overcome the drawbacks of knowledge-based approach like passwords. For example, Token-based authentication in a form of hardware or software tokens are used for logging in to the service. A software token such as the Google Authenticator [11], installed as a software on a device, issues a new password that changes with every access time. This method removes the burden of remembering or choosing passwords. Yet, user are still required to provide the generate passwords for continuous authentication.

Some researchers realized the importance of continuity and context in security implementations [12, 13, 14, 15, 16]. They proposed the idea of behavioral-based authentication, where users can be identified through biometric features, such as fingerprint or facial recognition. Biometric features can be considered as robust for authentication, and require little response time. Moreover, the 'side channel' nature of the behavioral-based method makes it inadequate to act as a strong authenticator alone. Therefore, it becomes crucial to implement a mechanism which combines weak authenticators together to provide strong authentication.

Several studies have been conducted to study the feasibility of multimodal behavior biometric authentication system. Kim et. al [17] proposed an enhanced multimodal personal authentication system for mobile device security, that fuses information from face teeth and voice modalities to improve performance. They demonstrated that the error rates for the integration of three modalities were lower that the error rates regarding a single modality. Saevanee et al. [18] combined three behavioral biometric techniques based on SMS texting activities and messages, as a multi-modal biometric authentication method for mobile devices. They showed that behavior profiling, keystroke dynamics and linguistic profiling can be used to discriminate users and showed that the two fusion methods can improve the classification performance. Shi et al. [19] hypothesized that most users are habitual in nature and are prone to performing similar tasks at a certain time of the day. They collected a wide range of behavioral information such as location, communication, and usage of applications, to form a user profile. Their method identifies positive events and boosts the authentication score when a "good" or habitual event is observed. While these fusion methods show promise of a strong authenticator, it is observed the quality and type of biometric data used is still sensor-dependent.

Also, we realise that not all smart home devices (e.g. router, voice assistant, security camera) are equipped with the same biometric modality. Wang et. al [20] studied the problem of translating behavioral models for user authentication across multiple dissimilar mobile devices based on app-independent modalities like user clicks and swipes. In contrast, we do not attempt to bootstrap trust on newer device. 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 Plan

1. We will start from making submodules for a specific set of sensors first. These submodules will be the 'weak authenticators' which get combined to provide 'strong' authentication in the later stages. In particular, we will make face verification module, speaker recognition module and GPS location module. This approach will give a good coverage for sensors on most mobile and IoT devices, as cameras, microphones and GPS are the most common sensors available.

2. Each 'weak authenticator' will provide a score and a timestamp of this score whenever a 'authentication' command is issued to it. We will design unified APIs for submodules so each module can just 'plug-and-play'. Addition of new modules in the future will be easy too.

3. When we have the three submodules we need for prototyping, we will design the core component. The core component will be the brain of the whole system. It will issue authentication command to each submodule when necessary, and it will give an authentication decision based on the scores it collected.

4. The design of the core component will also start from simple approach such as sliding window method so that we can make things work first. We can then move on to use machine learning methods such as LSTM. Eventually, we hope to come up with our own solution for the irregular-spaced time series problem which is crucial in this context of continuous authentication.

5. Finally, we would like to think about how users can interact with this system. If we have time, we can come up with a flow from recording biometric data to setting policy and eventually activating the authentication system.

Project Timeline

Week	Task
Feb. 17 - 23	Literature Survey on Continuous Authentication
Feb. 24 - Mar. 2	Literature Survey on state-of-art facial verification and speaker recognizer
Mar. 3 - 9	Develop submodules for individual authenticator
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 report

Team Responsibilities

Each member will take part equally in all tasks, but one member is assigned to each task to ensure that requirements of the deliverables are met and submitted by the course deadlines.

Project Tasks

1. Literature Survey: Stephanie
2. Designing data fusion system: Jiyi
3. Analysing results: Stephanie
4. Investigating for vulnerabilities: Jiyi
5. Testing possible defense: Stephanie

Course Deliverables

1. Presentation: Stephanie
2. Demo: Jiyi
3. Poster: Stephanie
4. Written Report: Jiyi

Potential Risks

1. The difficult part of our project is the design of the core component which combines scores from different authenticators meaningfully. It will be hard to give a rigorous mathematical formulation. 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.
2. 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.

Backup Plan

As we plan our project well and 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 (E.g. cross-device authentication to single-device authentication, fusion multiple biometric modalities to fusion of two major modalities). In fact, using speech recognition to achieve continuous authentication would be a novel solution to solve the authentication problem for voice assistant type of smart home devices.

References

[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 security 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 applicability 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 authentication 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 transparent 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.

[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

[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 authentication," 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 authentication 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 authentication 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.