CS6282: Statement of Work

Spring 2019 Teammates: Stephanie Lew, Zhang Jiyi

Prof. Jun Han Date: 08/03/19

Keywords: Continuous Authentication, Multi-modal biometrics

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 [] has shown that these 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 []. 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 []. These characteristics promise to be stronger than passwords alone.

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. []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 propose a multi-modal biometric approach toward authenticating users continuously and transparently in smart home environments.

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. These authentication approaches commonly fall into three categories: knowledge-based, object-based and physiological.

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 [**?**] . 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 [], 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.

Some researchers realized the importance of continuity and context in security implementations [1, 2, 3, 4, 5]. They proposed the idea of behavioral-based authentication. Nonetheless, the 'side channel' nature of behavioral based method made 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.

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

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

References

[1] 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

[2] 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

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

[4] 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

[5] 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.