Demo: Garda - Robust Gesture-Based Authentication for Mobile Systems

Can Liu
Rutgers University
Piscataway, NJ 08854, USA
can.liu@rutgers.edu

Gradeigh D. Clark
Rutgers University
Piscataway, NJ 08854, USA
gradeigh.clark@rutgers.edu

Janne Lindqvist
Rutgers University
Piscataway, NJ 08854, USA
janne.lindqvist@rutgers.edu

UbiComp/ISWC'17 Adjunct, September 11–15, 2017, Maui, HI, USA
ACM 978-1-4503-5190-4/17/09.
https://doi.org/10.1145/3123024.3123171

Abstract
This is a demo for a full paper in CHI'17 proceedings http://dx.doi.org/10.1145/3025453.3025879 [6]. We designed and implemented a secure, robust and usable multi-expert recognizer, Garda, for gesture passwords. This demo demonstrates two real scenarios of using Garda as a gesture recognizer in mobile devices: under normal use and under a shoulder-surfing attack. As a supplement to the demo, we describe technical details of Garda in this report. Our demo shows the usability of our Garda gesture authentication method on mobile devices in daily life.

Author Keywords
Security; Gesture; Authentication; Mobile device.

ACM Classification Keywords
H.5.2. [Information Interfaces and Presentation (e.g. HCI)]: Input devices and strategies; I.5.2. [Pattern Recognition]: Classifier design and evaluation

Introduction
Gesture passwords have been proposed as an authentication method for mobile devices [1, 2, 7, 8, 9]. Figure 1 shows an example of a gesture, which is defined as a set of sequences of X, Y coordinates drawn on the surface of a touchscreen device [2, 5, 8, 9].

Figure 1: An example of a free-form gesture.

Gesture-based authentication systems require algorithms to interpret gestures due to users' inability to exactly replicate their gestures every time. Those algorithms are called gesture recognizers. Proposed gesture authentication work often focuses on designing new systems with different recognizers [4], such as using Support Vector Machines instead of Dynamic Time Warping. However, single-method recognition can miss useful information when recognizing gestures, hampering recognition performance.

We created a Multi-Expert (ME) recognizer, Garda [6], by combining Gaussian Mixture Model (GMM) and Protractor [3]. In the full paper, we implemented and evaluated 13 popular recognition methods for gestures. We found that our new system, Garda, achieved the lowest error rate (0.015) in authentication performance, reached the lowest error rate (0.040) under imitation attacks, and resisted all brute-force attacks [6].

This is a demo for a full paper available in CHI'17 proceedings http://dx.doi.org/10.1145/3025453.3025879 [6]. In this demo, we will show the usability of Garda running in two real scenarios. In scenario one, we will show how to use Garda as a gesture password system on a mobile device. In scenario two, we will show that Garda is robust at differentiating gestures from real users and attackers.

Scenarios

We described the two real scenarios for using gestures as passwords: normal use and under shoulder-surfing attacks.

Scenario One: Normal Use

A person would create a gesture password account under Garda similar to how he or she would create a text password account under a standard system. First, the user needs to create a new account by registering a username and a gesture password. Similar to text passwords, the user needs to enter the gesture password twice to ensure the user is able to replicate the password. The user can also input more than two gesture passwords samples since more gesture samples improve Garda's performance.

Figure 2: An attacker is trying to steal the user's password by standing behind him.

After this registration step, the user can normally log in to the system by entering the username and performing the gesture password.

Scenario Two: Under Shoulder-Surfing Attacks

Figure 2 shows an attacker trying to steal a user's password while the user is entering it into the system. When the attacker gets access to the device, he can attempt to log in to the system by imitating the user's gesture. However, our demo will show that Garda is robust at distinguishing between the real gesture and the imitation gesture. The reason is that Garda combines Gaussian Mixture Model (GMM) and the inverse of cosine distance (Protractor). It recognizes gestures with the gesture shape feature (by GMM) and adjacent point feature (by Protractor),

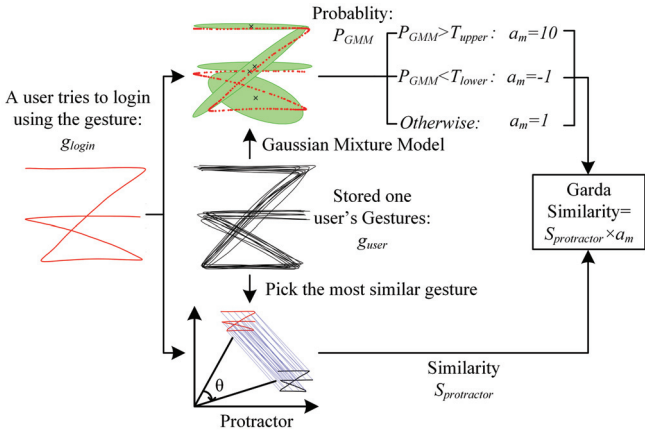

Figure 3: Garda gesture authentication system.

respectively. Therefore, it is difficult for attackers to crack the Garda system just by imitating how the user performs the gesture password.

Garda

Figure 3 depicted the multi-expert recognizer, Garda. Unlike other recognizers, which are based on single recognition method, Garda combines the individual advantages of the Protractor and GMM methods. Protractor recognizes the gesture's temporal features while GMM recognizes the temporal-independent distributions of a gesture's sample points.

To use the Garda authentication system, the user needs to register an account with a set of genuine gestures g_{user} to the system. With the user's genuine gestures, Garda will train a GMM for this user.

To log in to the system, a user draws a gesture g_{login}. The gesture g_{login} will be compared to the stored GMM in the system, outputting the probability that the gesture g_{login} fits the stored GMM, P_{GMM}. We set two thresholds T_{upper} and T_{lower} for P_{GMM}. If P_{GMM} is either higher than T_{upper} or lower than T_{lower}, Garda is confident about either accepting or refusing the gesture. Otherwise, Garda cannot make a reliable decision. The output of GMM is a modification parameter a_m. On the other hand, Protractor will measure the similarities between the gesture g_{login} and all of stored gestures g_{user} and select the most similar one as $S_{protractor}$. The Garda similarity is calculated by combining the results of GMM (a_m) and Protractor ($S_{protractor}$).

Summary

We designed and implemented a robust multi-expert gesture authentication method: Garda. We showed how to use Garda as a gesture password recognizer on mobile devices with two real scenarios: normal use and under shoulder-surfing attacks. The results of our full paper showed that, with rigorous evaluations on the authentication accuracy and resistance to two types of attacks, Garda outperformed the other 12 gesture recognizers across different datasets [6]. All our results showed that Garda is a strong alternative authentication method for mobile devices. More information and related work can be found at http://securegestures.org.

Acknowledgment

This material is based upon work supported by the National Science Foundation under Grant Number 1228777. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation. Gradeigh D. Clark was supported by the Department of Defense (DoD) through the National Defense Science & Engineering Graduate Fellowship (NDSEG).

REFERENCES

1. Gradeigh D. Clark and Janne Lindqvist. 2015. Engineering Gesture-Based Authentication Systems. *IEEE Pervasive Computing* 14, 1 (2015), 18–25. DOI: http://dx.doi.org/doi.ieeecomputersociety.org/10.1109/MPRV.2015.6

2. Gradeigh D. Clark, Janne Lindqvist, and Antti Oulasvirta. 2017. Composition Policies for Gesture Passwords: User Choice, Security, Usability and Memorability. In *2017 IEEE Conference on Communications and Network Security (CNS)*. IEEE.

3. Yang Li. 2010. Protractor: A Fast and Accurate Gesture Recognizer. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '10)*. ACM, New York, NY, USA, 2169–2172. DOI: http://dx.doi.org/10.1145/1753326.1753654

4. Janne Lindqvist. 2017. Could a Doodle Replace Your Password? *Scientific American via The Conversation US* (May 7, 2017). https://www.scientificamerican.com/article/could-a-doodle-replace-your-password/

5. Can Liu, Gradeigh D. Clark, and Janne Lindqvist. 2017a. Guessing Attacks on User-Generated Gesture Passwords. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 1, 1, Article 3 (March 2017), 24 pages. DOI:http://dx.doi.org/10.1145/3053331

6. Can Liu, Gradeigh D. Clark, and Janne Lindqvist. 2017b. Where Usability and Security Go Hand-in-Hand: Robust Gesture-Based Authentication for Mobile Systems. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (CHI '17)*. ACM, New York, NY, USA, 374–386. DOI: http://dx.doi.org/10.1145/3025453.3025879

7. Alexander De Luca and Janne Lindqvist. 2015. Is Secure and Usable Smartphone Authentication Asking Too Much? *Computer* 48, 5 (May 2015), 64–68. DOI: http://dx.doi.org/10.1109/MC.2015.134

8. Michael Sherman, Gradeigh Clark, Yulong Yang, Shridatt Sugrim, Arttu Modig, Janne Lindqvist, Antti Oulasvirta, and Teemu Roos. 2014. User-generated Free-form Gestures for Authentication: Security and Memorability. In *Proceedings of the 12th Annual International Conference on Mobile Systems, Applications, and Services (MobiSys '14)*. ACM, New York, NY, USA, 176–189. DOI: http://dx.doi.org/10.1145/2594368.2594375

9. Yulong Yang, Gradeigh D. Clark, Janne Lindqvist, and Antti Oulasvirta. 2016. Free-Form Gesture Authentication in the Wild. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (CHI '16)*. ACM, New York, NY, USA, 3722–3735. DOI: http://dx.doi.org/10.1145/2858036.2858270