Continuous Transparent Authentication with User-Device Physical Unclonable Functions (UD-PUFs) based on Mobile Device Touchscreen Interactions

Timothy M. Dee
Electrical & Computer Engineering
Iowa State University
Ames, IA, USA
deetimothy33@gmail.com

Ian T. Richardson
Electrical & Computer Engineering
Iowa State University
Ames, IA, USA
ian.t.rich@gmail.com

Akhilesh Tyagi
Electrical & Computer Engineering
Iowa State University
Ames, IA, USA
tyagi@iastate.edu

ABSTRACT

Many applications on mobile phones and tablets utilize information which if compromised would be of major inconvenience to the users of these devices. Mobile devices require security solutions to avoid any damage to the user associated with this loss of private information. There are many existing authentication solutions which provide some degree of protection against malicious parties who could use this information to steal objects from the legitimate user of the mobile device. In this paper we discuss the problems with existing authentication schemes. We then implement a system which seeks to solve problems in these other systems. This system uses an $n-gram$ Markov chain to track properties of a user's interactions with the soft keyboard of a mobile device. This system is used to continuously compare a user's current behavior against the past behavior of that same user. We describe how our system protects against the vulnerabilities existing in current authentication systems and demonstrate the practicality of our implementation.

1. INTRODUCTION

Malicious parties attempt to gain access to data of their victims. Often times these attackers go through the trouble of preforming these attacks because gaining access to the data might be quite lucrative. Take the example of

Many current practices keep mobile devices secure utilizing some nature of lock screen. These protection mechanisms require that the user preform some action when the mobile device state moves from inactive to active. This one-time authentication allows access to a large amount applications, tools, and data on the device. Some of this data could be potentially damaging if compromised by a malicious party.

One issue with this nature of user verification There are many ways an attacker might trick this one-time authentication hence gaining access to resources on the device.

This paper focuses on an idea for creating added security for data stored on mobile devices. Often times there exists a trade off between security and convenience from the user's perspective. This can be seen in solutions such as where The solution presented in this paper provides additional security while requiring no additional actions from the user. This is accomplished by recording touch screen interactions in the background while the user interacts as they normally would with the applications on their mobile device. The most resent interactions are then tested against previous actions to determine if the user's pattern has changed.

We provide a step forward, enhancing the ability of mobile devices to recognize when the device may have been compromised. Compromised here meaning the device is in the physical possession of an illegitimate user. This system provides innovations in the following areas:

- We show that touch screen interactions may be used in order to distinguish a legitimate user of a mobile device apart from illegitimate users. Specifically, section ? shows how a combination of a user's pressure when touching the screen and the location on the screen being touched may be used to develop a model of that user's behavior.
- We establish the behavior of a user on a device is unique to both the device and the user. Section ? establishes that a difference in either device or user may be detected by our implementation.
- There is no convenience cost assessed upon the user. All security improvements are accomplished without requiring any additional actions from the user. The specifications of the implementation used to accomplish this transparency are discussed in Section ?
- The performance of this system is sufficient to make it practical. A performance comparison is presented in Section ? which demonstrates the running time of the system on a Nexus 7 tablet.
- We improve upon the ideas discussed in ? utilizing similar concepts for modeling interactions. We extend beyond this work, modeling soft keyboard interactions

and describing . Section ? provides further discussion of with emphasis on similarities and differences between work described throughout this paper.

In deciding if a user is legitimate, it is useful to define three categories: something the user knows, something the user has, and something the user is. Traditional mobile authentication schemes, such as a lock screen, utilize only something a user knows. Interactions between a user and the touchscreen of a mobile device are rich with information. Current solutions suffer from underutilization of this information; they discard much of the content of these interactions in favor using the location of the interactions exclusively. Our system utilizes pressure, time, and location capturing the currently under-utilized potential of these interactions to expose patterns unique to a user.

We use these properties to construct a model of how the user interacts with a mobile device. This model takes as input a sequence of touches preformed by the user. From this sequence probabilities are developed which represent the likelihood of a given touch screen interaction based on the properties of a number of previous interactions. A type Markov model which uses n previous states in computing next state probabilities is used for the purpose of developing these probabilities. This model is explained more throughly in Section 3.

2. THE PROBLEM

3. THE SOLUTION

The main idea of this paper is that user touch screen interactions may be used in order to distinguish a legitimate user of a mobile device apart from illegitimate users. We implement a continuous authentication system based on user interactions with the soft keyboard of a mobile device. This system uses properties of the interactions including pressure and location.

A large part of a user's interactions with a mobile device involve the input of data with a soft keyboard. These soft keyboard applications require that the user put their finger on the screen at a consistent location to indicate a given letter should be taken as input. This input is rich with information including pressure, key code, and timestamp. As the keys on the soft keyboard are always in the same place on the screen, we take the key code value to represent the location in our model. Through interactions with multiple applications over time, the user produces a sequence of these inputs. This sequence is used to construct a model of user behavior.

The goal in creating the model is to be able to distinguish the behavior of one user from another user on the same device and from the same user on a different device. That is, the pairing of user and device will create a model unique to that pair. If either the user or device is changed, the model will be sufficiently different that it is detectable. The input sequence will be used to characterize the user-device pair. This uniqueness is possible because the pressure metric is a product of unique properties in the silicon of the device and the finger of the human user. The silicon's unique properties are a product of the fabrication process while the uniqueness of the human user is derived from the way in which they touch the screen.

Let's say we want to model the behavior of an individual in terms of where they choose to spend their time. Say further that the goal in creating this model is to predict their $t+1^{st}$ location based on their current location. The outcome of using a Markov model to describe a system is a vector $\hat{P}$ of probabilities for each possible state. For the individual in our behavior model, $\hat{P}_i$ corresponds to the probability that the i_{th} location will be the location of the person at time $t+1$ if the current time is t. Such a probability outcome for our individual might be that if at time t the person is in the living room, then at time $t+1$ there might be a 70% probability they are still in the living room, a 20% probability they are in the kitchen, and a 10% probability they are in the bathroom. Such a model might be useful in understanding the behavior patterns of one person, or comparing behavior patterns among persons.

If a Markov model can describe the trans

Our n-Markov model uses tokens which are a tuple of location and pressure generated through user touch screen interactions. There are a very large number of possible location, pressure combinations. Since it is unlikely that the user will be very precise in location or pressure, having such a large number of tokens creates a situation where each sequence of touch interactions will be different for the same user on the same device; this is not desirable. In fact, if the entire space were used the variations in location and pressure, even when generated by a single user, would result in a very large number of tokens each having low probabilities of succeeding any n token sequence.

We require some way of splicing this space

Let us return to the situation where a Markov model was used to predict the $t+1^{st}$ location of an individual. Now suppose that these probabilities have been developed for two people who's behavior patterns we would like to compare. Our goal is to quantify the difference between the location patterns of these individuals.

4. THE DETAILS

5. RELATED WORK

6. CONCLUDING REMARKS

The findings we have presented suggest that touch screen interactions may be used in order to distinguish a legitimate user of a mobile device apart from illegitimate users. Many current solutions utilize one-time authentication schemes These solutions do not provide sufficient protection in a mobile environment. This work represents a step toward a holistic approach toward mobile security, catering to threats existing in this environment.

This work presents as part of a positive trend in mobile security. Technologies part of this trend incorporate elements of the mobile environment, providing enhanced security by incorporating properties of the human user as part of the authentication. This approach is superior to exclusive use of things the user knows, because knowledge may be easily imitated while human biometrics can not.

[1]

7. REFERENCES

[1] Rosenfeld, K., Gavas, E., and Karri, R. Sensor physical unclonable functions. In *Hardware-Oriented Security and Trust (HOST), 2010 IEEE International Symposium on* (2010), IEEE, pp. 112–117.