User-Device Physical Unclonable Functions (UD-PUFs) based on Mobile Device Touchscreen Pressure

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

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

ABSTRACT

Described in this document is a physical unclonable function (PUF) utilizing the variability derived from the pressure with which users interact with their mobile device touchscreens. We illustrate how a sequence of these pressure values from descrete touchscreen interactions may be used to uniquely characterize a user-device pair. This characterization method may find many applications in protecting access to a mobile device from a malicious party. As a result, the effectiveness of this scheme is described in terms of how one user may be differentiated from another.

1. INTRODUCTION

Mobile devices are ubiquitus in the modern world. These devices are becoming progressively more important for many applications with security sensative data. Securing mobile devices poses unique challenges and opportunities compared to traditional data security where it is difficult for an attacker to access the physical device on which the data is stored or from which the sensitive data may be accessed. The reality that an attacker may be able to gain access to a physical device makes securing any data stored on or accessed by a mobile device significantly more challenging. Traditional physical unclonable functions (PUFs) which can be used to uniquely to a given hardware device are no longer sufficient to guarentee the authenticity of a user. This modivates an extension of the traditional PUF known as a user-device physical unclonable function(UD-PUF). This UD-PUF entangles the physical characteristics of the user in combination with the device to enable a more secure authentication scheme.

2. TOUCHSCREEN PRESSURE

current at sides of phone.[1]

3. MODELING A USER-DEVICE PAIR

Interactions between useres and devices are complex. To interpret these actions in a meaningful way, in order to preform an authentication for example, it is necessary to simplify these interations. The chosen model must provide sufficient entropy such that a model generated with a given user-device pair is not consistantly reproducable by another user or on a different device. The modeling method must also be easily reproducable by the origional user on the origional device. A model having the neccessary characteristics required for this application is a Marcov Chain. Marcov Chains are useful in predicting systems who's behavior can be modeled in descrete states. The transitions between states can be identified to happen with some probability. Historically the Marcov Chain has found applications in Upon identification of an appropriate model the next step is to discover an optimal way in which it may be applied to the current problem. The goal is

4. TOUCH PRESSURE MODELING

The goal in modeling a system with a marcov model is to classify the system in terms of its transitions between states. If such a model is to be used to purposes of uniquely identifying a given system, than the states of the model must be chosen in a way which exposes the uniqueness of the system. The states of our marcov model are defined by the range in which

5. DIFFERENTIATING USER-DEVICE PAIRS

6. RESULTS

7. CONCLUSIONS

8. FUTURE WORK

9. REFERENCES

[1] J. Zhu, P. Wu, X. Wang, and J. Zhang. Sensec: Mobile security through passive sensing. In *Computing, Networking and Communications (ICNC), 2013 International Conference on*, pages 1128–1133. IEEE, 2013.

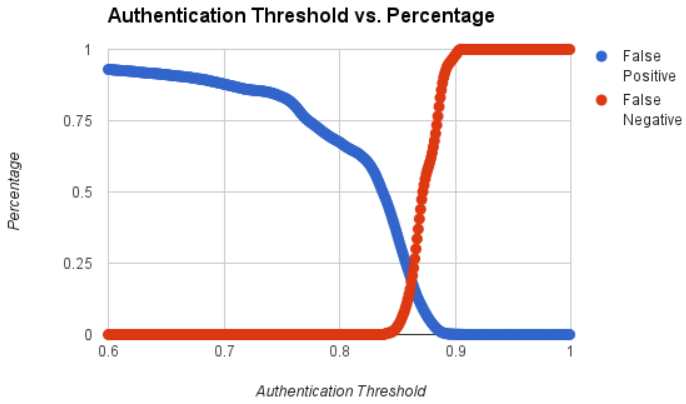

Figure 1: Statistical Concentration/Correction for a User other than Profiled User