EasyUnlock: A Behavioral Biometric Authentication System

Patrick Nichols Colorado School of Mines Department of Computer Science

Introduction

Smartphones have become ubiquitous in modern life, which means smartphone security is becoming more and more important. To keep their smartphones secure, many people rely on PIN's, passwords or patterns. While effective, all of these methods come with serious drawbacks. The user can forget the number or word that unlocks their phone, and malicious actors can learn the passcode by simply watching the phone get unlocked. To combate these downfalls we developed EasyUnlock.

Objectives

Create a lightweight app to unlock a phone based on the way the user picks the phone up. The app should be:

1. Lightweight (in memory and power consumption)
2. Resiliant to traditional attacks
3. Easy to use
4. Reliable

System Architecture

To decide if the person picking up the phone is our user, we compare the incoming pickup signal to signals we know are from our user. If the distance is above a certain threshold, we reject the pickup attempt.

To compare two signals we used a dynamic time warping (DTW) algorithm. A DTW algorithm is a method of comparing two signals that may have been distorted in time. To compare two signals we use the following pseudocode:

```
int DTWDistance(s: array [2..n], t: array [1..m]) {
    DTW := array [0..n, 0..m]

    for i := 1 to n
        DTW[i, 0] := infinity
    for i := 1 to m
        DTW[0, i] := infinity

    DTW[0, 0] := 0
    for i := 1 to n
        for j := 1 to m
            cost := d(s[i], t[j])
            DTW[i, j] := cost + minimum(DTW[i-1, j ], // insertion
                DTW[i , j-1], // deletion
                DTW[i-1, j-1]) // match

     return DTW[n, m]
}
```

Results

To the right are the similarity metrics we obtained from our ten initial volunteers. Many of them successfully matched with themselves, and the one's that didn't were not far off. The other thing of note is how different the metrics are across users. User 1's best match was 40.11, while User 6's was 4.73. Users 1 and 2 had significantly longer pickup signals than the others which explains their high matching metrics.

User	Self Match	Best Match
1	44.11	40.11
2	31.91	31.91
3	18.03	14.60
4	8.6	8.6
5	7.57	7.57
6	4.73	4.73
7	12.16	12.16
8	5.21	5.21
9	5.09	5.09
10	5.76	5.76

Pickup Signals

To collect pickup signals we used both the accelerometer and the gyroscope of the smartphone. Though other sensors like the magnetometer and thermometer are available, we decided not to incorperate them, as the readings they give are not likely to correlate with the person picking up the phone.

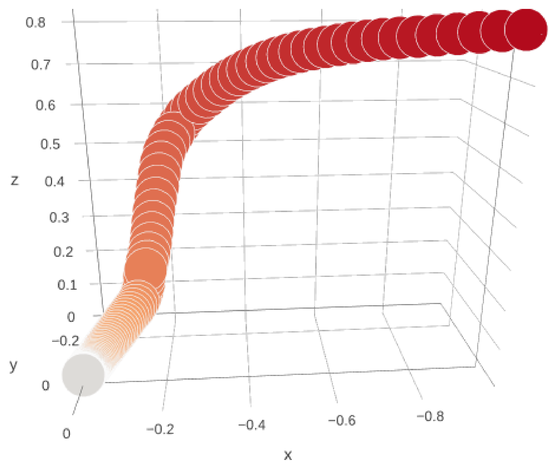

Figure 1: Simple visualization of a pickup signal

Conclusion

Our initial results indicate that a behavioral biometric authentication system is viable. Though we lack rigorous data, the initial matching metrics show 80% of users match with themselves. These results are promising enough to warrent further investigation.

The radical diffrences in matching values seen in our results section is not very concerning. Longer signals naturally produce a higher matching score, but the DTW algorithm penilizes signals that are significantly different in length. This prevents an attacker from using very short signals to try and cheat a lower matching score.

A system such as this prevents the user from losing the thing they authenticate themselves with. This has obvious advantages over the traditional password/PIN method, but our accuracy is still not as high as traditional methods.

We set out to build a lightweight authentication app, but various setbacks mean we haven't gotten as far into the project as we would have liked. Despite that, the promising start has us excited to continue developing.

References

Wei-Han Lee, Xiaochen Liu, Yilin Shen, Hongxia Jin, and Ruby B. Lee. 2017. Secure Pick Up: Implicit Authentication When You Start Using the Smartphone. In *Proceedings of SACMATâĂŹ17, Indianapolis, IN, USA, June 21-23,* 2017, 12 pages.
https://doi.org/http://dx.doi.org/10.1145/3078861.3078870

Future Research

In the future we hope to extend the ideas we are exploring to passivly detect smartphone theft. By constantly monitering the way the user picks up and holds the phone, one could develop a continuous authentication system for a smartphone. Additionally, we hope to continue refining the project to a point where a better understanding of a pick-up by pick-up accuracy can be obtained. With these results, a commercially viable version of our app could potentially be deployed.