Poster: PIN Number-based Authentication Leveraging Physical Vibration

Jian Liu, Chen Wang, Yingying Chen
Stevens Institute of Technology, Hoboken, NJ 07030, USA
{jliu28, cwang42, yingying.chen}@stevens.edu

ABSTRACT

In this work, we propose the first PIN number based authentication system, which can be deployed on ubiquitous surfaces, leveraging physical vibration signals. The proposed system aims to integrate PIN number, behavioral and physiological characteristics together to provide enhanced security. Different from the existing password-based approaches, the proposed system builds upon a touch sensing technique using vibration signals that can operate on any solid surface. In this poster, we explore the feasibility of using vibration signals for ubiquitous user authentication and develop algorithms that identify fine-grained finger inputs with different password secrets (e.g., PIN sequences). We build a prototype using a vibration transceiver that can be attached to any surface (e.g., a door or a desk) easily. Our experiments in office environments with multiple users demonstrate that we can achieve high authentication accuracy with a low false negative rate.

1. INTRODUCTION

Authentication has become increasingly important and is spreading into every corner of our daily lives. It is not just limited to the locking process of mobile devices, but also plays a critical role in numerous daily activities when accessing corporate facilities, apartment buildings, hotel rooms and smart homes. The general usage of authentication mainly relies on inercom-based, camera-based, card-based, or fingerprint-based systems installed at the security entrance of these places. These approaches require expensive equipment and complex hardware installation. The quest is to seek a general user authentication solution that can be deployed to any surface (such as a door or a table, not just touch screens), involving minimum installation efforts, and integrating human physical characteristics to provide enhanced security.

The traditional authentication solutions are based on passwords including both texts and graphical patterns (e.g., [1]). And the growing popularity of mobile devices makes PIN and pattern lock based authentication available on touch screens, a simplified form of passwords. However, all these approaches suffer from password theft or shoulder surfing. Another direction of authentication involves physiological biometrics (e.g., fingerprints [2]). These mechanisms are less likely to suffer from identity theft. However, they usually stir privacy concerns of the users.

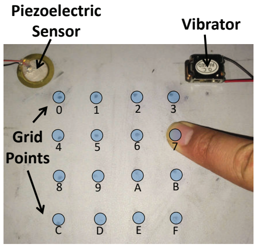


Figure 1: Illustration of the proposed PIN number-based authentication system using physical vibration.

In this poster, we propose a finger-input based authentication system, as illustrated in Figure 1, that has the flexibility to provide users with PIN number secret authentication on any solid surface to gain security access. To enable touching on any surface, we build the authentication system upon a touch sensing technique using physical vibrations. When a vibrator actively excites a surface resulting in the alteration of the shockwave propagation, the presence of the object in contact with the surface can thus be sensed. By relying on vibrating signals, the system is less susceptible to environmental interferences from acoustic or radio-frequency noise.

The proposed system can authenticate legitimate users and reject attacks well because it is based on the following insights. Unique features are embedded in a user's finger pressing at different locations on a solid surface. Such unique features reflect the characteristics (e.g., locations of touching, touching contacting area and force, and finger structure) of the user's finger touching on the medium (e.g., a door panel or a desk surface), making them suitable candidates to differentiate different touching locations of the same user and different users when touching on a same location.

Realizing such an approach involves seeking solutions from a number of challenges. First, unique features need to be extracted from the vibration signals that can not only identify the PIN numbers clearly but also reflect the behavioral and physiological characteristics. Second, the system should ensure fine-grained finger-touching recognition with a high accuracy and a low false negative as a legitimate user should pass the authentication in the minimum number of attempts. Third, an adversary may try to impersonate a legitimate user in any means. The system should have the capability to reject such attempts all the time.

2. SYSTEM DESIGN

2.1 System Overview

As illustrated in Figure 2, after receiving the vibration signal-

MobiCom'16 October 03-07, 2016, New York City, NY, USA

ACM ISBN 978-1-4503-4226-1/16/10.
DOI: http://dx.doi.org/10.1145/2973750.2985261

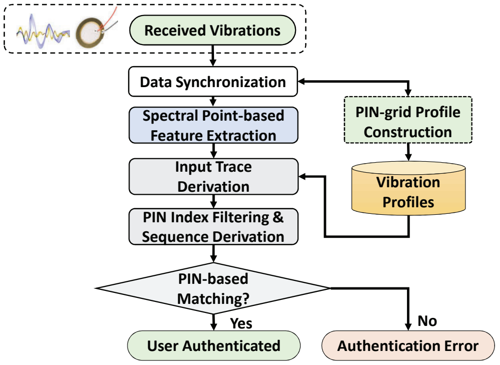


Figure 2: The architecture of our system.

s, the system first performs synchronization on the received vibrations. The system then extracts the unique vibration features, such as frequency magnitude at each spectral point, in the frequency domain from the synchronized vibration signals within a sliding window. The selected vibration features are used by two phases: profiling and authentication. In the profiling phase, the extracted features are captured while users' finger pressing at different locations on the surface and such unique features correspond to the characteristics (e.g., locations of touching, touching contacting area and force) of the users' finger touching on the surface. In this work, a set of grids is drawn on the surface as shown in Figure 1. During the authentication phase, the collected vibration samples are used to extract vibration features. The extracted features first serve as inputs to Input Trace Derivation via a classifier based on Supporting Vector Machine (SVM) trained by the pre-constructed profiles. The derived input trace would then be put into PIN Index Filtering & Sequence Derivation to recover the PIN sequence embedded in the received vibration signals. The recovered PIN number will be compared with the local stored PIN sequence database for the authentication.

2.2 Vibration Source & Synchronization

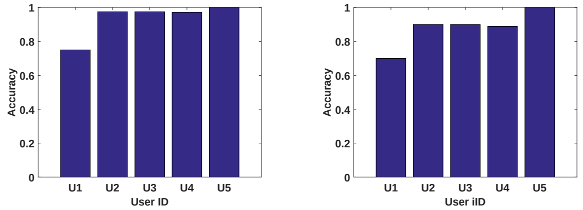
In this work, we generate repeated chirp vibration signals to linearly sweep frequency from $16kHz$ to $22kHz$, which contain a broad range of frequencies and are inaudible to most people ears. To synchronize the vibration transmitting, we add a pseudo-noise sequence preamble ($0.1s$) at the beginning of the repeated sweep signals, then synchronize the received vibrations using cross-correlation between the PN sequence of the received vibration signal and the known generated PN sequence.

2.3 Vibration Feature Extraction

We analyze the received vibration signals in the frequency domain. We find that the amplitude of some designated frequency components in the signals, called *spectral points*, are most sensitive to the minute changes caused by finger touching or swiping. We design a strategy to find peaks of the frequency response in the frequency interested range(i.e., $16k - 22kHz$) to identify the frequency of each spectral point. The frequency response at these spectral points are then extracted as the spectral point-based feature to differentiate the user's finger pressing locations.

2.4 PIN Number based Authentication

Deriving Input Traces. The system takes the received vibration signals as input, and determines the locations of the finger presses in terms of the grid point indices. In particular, we apply FFT to a sliding window of the vibration signals and extract the vibration feature in frequency domain for every window. Then we estimate the location of the finger press in terms of the grid point index for each sliding window by using a machine learning based grid point classifier based on SVM.



(a) Identification accuracy of each number in the PIN

(b) Identification accuracy of each complete PIN sequence

Figure 3: Performance of PIN-number based authentication in verifying legitimate users.

PIN Index Filtering. Due to the fact that the grid point segments that have consecutive same grid point indices corresponds to the firm finger presses on a grid point, the Grid Point Index Filter takes three steps to keep these segments: i) calculating the difference between every two consecutive grid point indices in the trace; ii) utilizing the End-to-End Search algorithm to find the starting and ending points of the segments of consecutive zeros, which is called *finger-press segments*, indicating the time periods of firm finger presses; iii) mapping the starting and ending times of the segments back to the grid point index trace, and remove the grid point indices that are out of the segments.

PIN Sequence Derivation. We further confirm each finger-press segment based on their time length and derive the PIN sequence. We empirically determine the minimum pressing duration to be $300ms$, and remove the segments that last for a shorter time because these estimations may not represent the true finger presses. Finally, given the length of the user's PIN sequence, the system finds the corresponding number of longest finger-press segments in the trace and derives the PIN sequence by mapping the virtual keys to the grid point indices contained in these finger-press segments.

3. PRELIMINARY EVALUATION

We evaluate the performance of user authentication using PIN on a 4×4 square-shaped grid. The grid is drawn on a solid surface in a typical office environment (i.e., a wooden table) as shown in Figure 1. Each user is asked to sequentially press the 16 grid points 10 seconds to create his/her profiles for the grid points. To evaluate the system, the users are further asked to respectively press 4-digit PIN sequences.

Figure 3 shows the identification accuracy of each number and each complete PIN sequence of 5 legitimate users. Specifically, Figure 3(a) shows that the legitimate users can obtain over 95% average identification accuracy of recognizing each number in the PIN. We also find that the legitimate users have up to 90% average accuracy to pass verification using their individual PINs as shown in Figure 3(b). Our system thus is effective in verifying all the legitimate users.

4. ACKNOWLEDGEMENT

This work was partially supported by the National Science Foundation Grants CNS1409767, CNS1514436 and SES1450091.

5. REFERENCES

[1] Adam T Timmons and Osman D Altan. Grid unlock, February 2 2010. US Patent App. 12/698,321.

[2] Arathi Arakala, Jason Jeffers, and Kathy J Horadam. Fuzzy extractors for minutiae-based fingerprint authentication. In *Advances in Biometrics*, pages 760–769. Springer, 2007.