THE UNIVERSITY OF TEXAS AT ARLINGTON

MASTERS THESIS

TaPIN: A Two-Factor User Authentication Scheme for Smartwatches through Secret Finger Tapping

Author:
Akash LOHANI

Supervisor:
Dr. Ming LI

A thesis submitted in fulfillment of the requirements for the degree of Masters of Computer Science

in the

Mobisec
Computer Science and Engineering Department

May 6, 2020

THE UNIVERSITY OF TEXAS AT ARLINGTON

Abstract

Dr. Ming Li
Computer Science and Engineering Department

Masters of Computer Science

TaPIN: A Two-Factor User Authentication Scheme for Smartwatches through Secret Finger Tapping

by Akash LOHANI

Nowadays, smartwatches have become one of the most common wearable gadgets as they are small and portable. As more and more personal information is managed and processed inside smartwatches, it is important to have a secure user authentication scheme in place. There have been many successful authentication schemes for a smartphones such as Password/PIN, bio-metric approach(e.g. fingerprint, face recognition), etc directly used on smartwatches. However, these approaches are not quite suitable for smartwatches due to its constraints in size and limited computation power. To address this issue, we propose TaPIN that allows users to authenticate themselves by playing out the rhythmical tap with their thumb and forefinger. TaPIN is a two-factor user authentication scheme that incorporates not only the user's knowledge-based rhythmical tapping pattern but also the corresponding vibration bio-metric exhibited during finger tapping. To validate the scheme, we built a proof-of-concept prototype, conducted extensive experiments with human subjects, and demonstrated that TaPIN achieves high accuracy and is resistant to various types of attacks. More importantly it is convenient to perform with one hand.

Acknowledgements

I wish to express my deepest gratitude to my supervising professor, Dr. Ming Li, for the consistent support and guidance through my research work. She guided me through the entire process by suggesting me relevant papers, building the experimental setup, testing, verifying the proposal and writing the thesis.

I would also like to appreciate rest of my committee members, Dr. Mohammad Atiqul Islam and Dr. Shirin Nilizadeh, for giving constructive feedback and suggestions throughout my work.

There were a lot of discussions with my PhD fellows from my MobiSec lab, especially Mr. Huadi Zhu and Mr. Wenqiang Jin, who helped me refine my proposal.

Also, a big thanks to everyone who participated in the experiments for the thesis, especially Mr. Asif Faisan Raman, for being a supportive volunteer for the data collection and initial testing so that the process of building the prototype was smooth.

I would like to appreciate Dr. Bill D. Carroll and rest of the faculty chiefs of the department for providing Graduate Assistantship which helped me support my study and focus on the research which I was really into.

Last but not least, my deep and sincere gratitude to my family for their consistent support and love throughout my career. My parents Dr. Tara Nidhi Lohani and Shanta Lohani selflessly pushed me forward and supported me in hard times to get the opportunities and experiences that have made me who I am.

Contents

List of Figures

List of Tables

List of Abbreviations

kNN	**k** **N**earest **N**eighbors
LG	**L**ucky **G**oldstar
PIN	**P**ersonal **I**dentification **N**umber
SNR	**S**ignal to **N**oise **R**atio
FFT	**F**ast **F**ourier **T**ransform
FAR	**F**alse **A**cceptance **R**ate
FRR	**F**alse **R**ejection **R**ate
EER	**E**qual **E**rror **R**ate
API	**A**pplication **P**rogramming **I**nterface

Chapter 1

Introduction

Smartwatches are now one of the most prevalent wearable devices since they are small and portable. Due to its light weight making, it is convenient to perform some tasks that have previously been done on smartphones. These handy features led a huge takeoff on smartwatch applications in health, fitness, and in finance. Many users keep track of their heart rates and body metrics such as weight and height through smartwatches. Recently we also started using it for online accounting, processing electronic payments through apps such as Fitbit [7] and GooglePay [9] and some even use it for stock trading on a daily basis. As more and more people started using various applications and as more personal and sensitive information is aggregated and processed inside the smartwatch, it is important to have a secure user authentication scheme in place. Here the word "authentication" refers to the process or action of proving or showing something to be true, genuine, or valid [16]. In our project, we focused on "user authentication" where we built a system that classifies whether it is a legitimate user or not. Many successful authentication schemes on a smartphone are directly used on smartwatches because of the similarity in its interface. However, the usability between these two devices are different so the system migration of an authentication scheme from a smartphone to a smartwatch is not quite successful.

Password/PIN (e.g. text and graphical patterns), for example, is not appropriate for a smartwatch due to its constraints in size of the touch screen. There are some works being done to enlarge the touch screen to avoid the interaction issue; however, these moves contradicts with the current trend of designing smaller and portable devices to provide better user experience. Password/PIN also comes with a major security issue in Smudge attacks where the oily residue on the surface of the touch screen produces considerable potential for attackers to retrieve the secret [3]. Over-the-shoulder attack occurs when an attacker tries to take a video or directly observe the victim typing on the screen. Even a vigilant person can become a victim because the attacker can sneak the password without being noticed. This is one of the most common and serious consequences of password/PIN because once the password is compromised, we do not have any choice but to change the password to avoid further attacks.

The bio-metric approach (e.g. fingerprint and face recognition) is a widely used authentication scheme for smartphone that provides reliable accuracy. This approach is not quite practical for smartwatches due to its limited computation power. Besides, it requires sophisticated hardware to realize the system which is not ideal for the sake of building commercial products.

To overcome the limitation of the two above, speech recognition is one of the substitutions. However, this approach is susceptible to replay attack where the attacker can use sophisticated acoustic equipment to eavesdrop the secret and play back the signal to bypass the system. Moreover, when using this method the surrounding noises (i.e. cars, birds, people talking) can become one of the intruding factors. There are also some cases where the user feels certain awkwardness to speak on their phone in public.

To break down the issue, we proposed TaPIN, a novel authentication approach which enables user to authenticate their device just by performing a rhythmical tap-gesture using their thumb and forefinger. This is essentially a two factor authentication system which not only authenticates the knowledge-based information but also the vibration bio-metric. Here in TaPIN , knowledge-based information is the rhythm pattern designed by the user

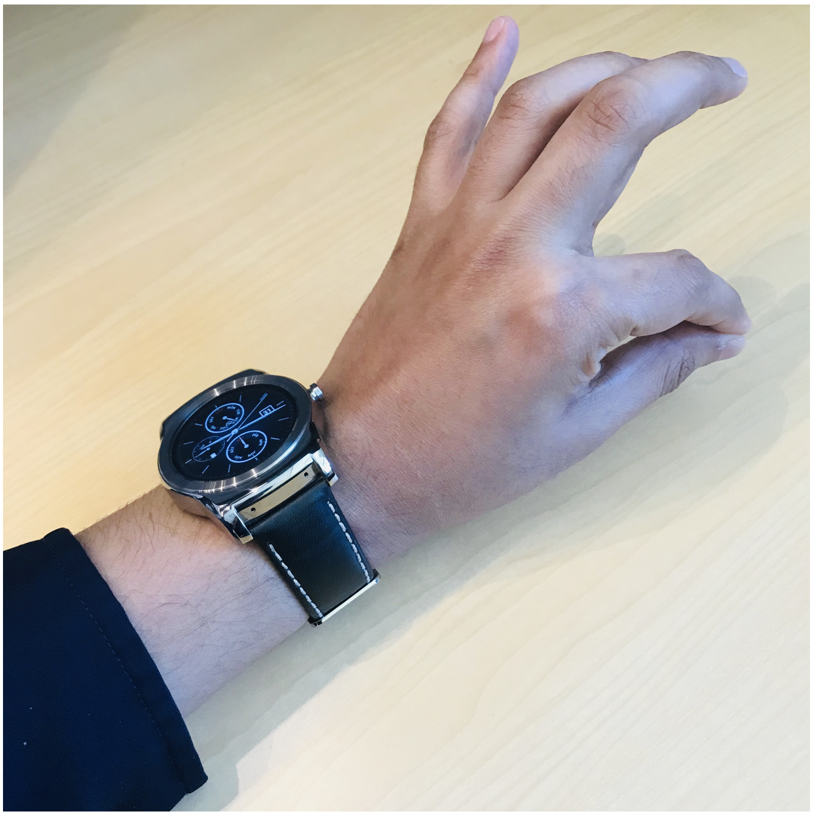


FIGURE 1.1: Demonstration of TaPIN

and the corresponding tapping-induced vibration can be used as a bio-metric information which is different among people due to the variance in the body metrics such as fat, thickness of the skin, and bone structure [10].

TaPIN is a completely one-handed authentication scheme. This novel feature allows users to authenticate their device even while he or she is performing another task with their other hand (i.e. grabbing grocery bags, brushing their teeth, holding dumbbells, etc). Our approach also does not require any interaction with the touch screen which eliminates the concern of smudge attacks mentioned earlier in the password/PIN section.

Our system is also resistant to password theft such as shoulder surfing because of the two factor characteristic. The input signal can hardly be replicated even if the attacker has the knowledge of the secret because the system integrates behavioral and physiological characteristic like fat and bone structures of the user. In other words, even if the attacker tries to unlock the system with identical rhythmical taps, it is able to detect that he or she is an imposter by considering the bio-metric features. This ultimately leads to a low false positive rate.

Last but not least, our solution is less expensive and has the potential of being commercially available. It can easily be deployed in commercial smartwatches because it uses ordinary embedded accelerator sensor and does not require installation of any expensive equipment.

Chapter 2

Related Works

2.1 User authentication on Smartwatch

A number of traditional authentication schemes on the smartphone have been tested in smartwatches but due to the limitation in screen size, battery life and processing speed, they are not well adapted for smartwatches. Password/PIN [21] and gridlock [1] approach is one of the popular scheme that are widely used in different device system. However, these approaches are not quite popular for the users in smartwatches due to its constraints in the touch screen. It is quite frustrating for the user with bigger fingers where they find it almost impossible to interact with the device. There are some devices which doesn't even have a touch screen which means these approach doesn't work at all. These schemes are also vulnerable to several security attacks. Smudge attacks [3] is one of the common attack that the attacker tries to recover the secret through oily residues on the touch screen. The attacker can compare the location of the smudges and widely used standards for keyboards(i.e. QWERTY) or grids to compromise the pass-code. Shoulder surfing attacks [24] is also one of the serious attacks where the attacker tries to eavesdrop the secret by taking a video of the victim typing on the screen or directly observe them unlock the device over the shoulder. The attack is quite serious because the victim needs to change their password once it is compromised.

Bio-metric based approach such as fingerprint [25], facial recognition [13] and iris scans are the most widely used authentication scheme for smart devices nowadays. These scheme has a higher accuracy than other methods which users find it secure and convenient. The significant issue of these approach is that it requires sophisticated hardware and intensive computation which is not viable for commercially available smartwatches. Besides, the scheme typically raises questions regarding the privacy of the user, forcing the deployment of additional hardware that do not generally appear in inexpensive smartwatches.

In-air gait gesture recognition [2] which only uses the embedded accelerometer are also studied to cope with the hardware limitation of smartwatches, but these approach is quite intrusive to the surrounding environment leading to low usability.

Voice recognition is one of the substitution for the approaches stated above but it is prone to noise and the secret can be effectively replicated with sophisticated software. Attacker can also consider recording and playback the voice of legitimate users onto the system. The user may also find a slight awkwardness to the public while speaking onto the device.

2.2 Rhythm-Based Authentication

There are also some works which allows user to authenticate their device by a rhythm. Wobrock et al. [30] has developed a singlekey authentication method called "TapSongs", allowing user authentication on one "binary" sensor(i.e. button), leveraging the user-designed rhythmical pattern corresponding to tap-down and up event. Thumbprint [6] is a group authentication system introduced by Das et al. which authenticates a number of users with the secret knock rhythm, where the knocks are different from each users. Hutchins et al. [11] developed a rhythmic authentication scheme for wearable device with a touch sensor which records user taps as the hidden pass-code. This system was novel because it allowed user to have a huge input space leading to higher security but this approach which totally relies on rhythmical information is easily be compromised by shoulder-surfing attack.

2.3 Vibration-based Authentication

Some existing efforts have been done to cope with constraints in size of the touch screen. Vibration based authentication is one of the field which is based on the fact that the vibration induced by the user motion varies corresponding to body bio-metrics. Harrison et al. [10] developed Skinput which expands the text input medium to physical body and allows user to type by tapping their forearm. However, this system required several sensors attached onto their body which is quite intrusive to users. Zhang et al. [32] advanced Skinput by just using the embedded accelerometer to realize the text input system. Chen et al. [14] developed Viband which distinguishes hand movements like flicks, clicks, taps and also has the capability of identifying motor-actuated items just by grabbing the item.

On the other hand, Lin et al. [31] developed VibID which enabled the authentication by leveraging the response produced by a motor actuated vibrator. However the feature that it requires continuous physical vibration onto the body is quite obtrusive to the user and also noisy for the surroundings. Jian et al. [18] introduced Vibwrite which is also another example of active authentication scheme that leveraged the difference in the vibration response through physical surface such as door or table to identify users.

Chapter 3

Design goals

3.1 Design Goals

TaPIN is developed based on the following design goals to cope with the existing challenges.

3.1.1 Security

Security is freedom from, or resilience against, potential harm or other unwanted coercive change caused by others [26]. Security is kept on top priority as an authentication scheme where the system should be resilient against widely known attacks on smartwatch to avoid attackers to authenticate victim's device even when physically accessible. We analyzed the following threats which may challenge our proposed authentication scheme.

- **Zero-effort Attack**: The attacker attempts to bypass the authentication by performing random pinch pattern which will generate similar beat and vibration response as the registered one.

- **Over-the-shoulder Attack**: The attacker not only has the knowledge of the credential (i.e. beat length, rhythm pattern) sequence but also try to mimic the behavior of the legitimate user by shoulder surfing.

We aim to build a system which is resilient against the attacks stated above through two factor authentication scheme.

3.1.2 Usability

Usability can be described as the capacity of a system to provide a condition for its users to perform the tasks safely, effectively, and efficiently while enjoying the experience [29]. TaPIN aims higher usability through developing a one-handed authentication system which does not require any interaction on the touch screen. This eliminates a frustration interacting with small screen and allows users to perform other tasks (i.e. grabbing grocery bags, brushing teeth, carrying dumbbells) while using the system. We also further analyzed the usability as means of efficiency such as time consumption and login attempts during the usage of our system.

Chapter 4

Characterization of TaPIN and Background Theory

4.1 Definition of TaPIN

TaPIN is a system that allows users to unlock their devices by playing out the rhythmical tap with their thumb and forefinger as shown in Figure 4.1. This motion is also called a "pinch" which is a common activity we as a human beings perform in daily lives to grab or squeeze some objects. The motion always comes with a "Contact" and "Separation" between fingers and produces a certain vibration through our body. We observed that this vibration can be captured by the embedded accelerometer as shown in Figure 4.2.

TaPIN consists of unique features based upon the sequence of the pinch motion. It is a two-factor authentication scheme that incorporates not only the user′s knowledge-based rhythmical tapping pattern but also the corresponding vibration bio-metrics exhibited during finger tapping. Imagine that you have an instrument and you play a rhythmical beat with that. The beat is confidential and original so that no one but only you knows how to play the rhythm. Besides, since every people carries different instruments, the noise that this beat produces differs from person to person. Here in TaPIN, the instrument is your body and you play your own rhythm through pinching

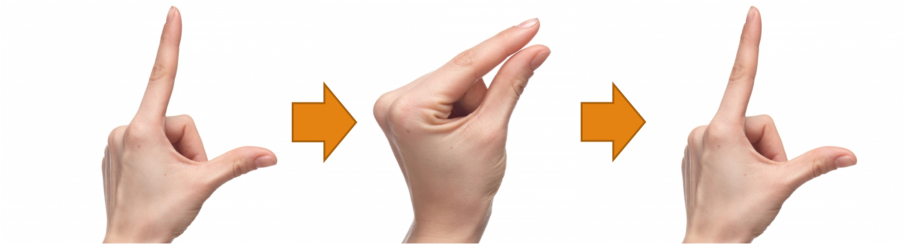


FIGURE 4.1: How to unlock TaPIN

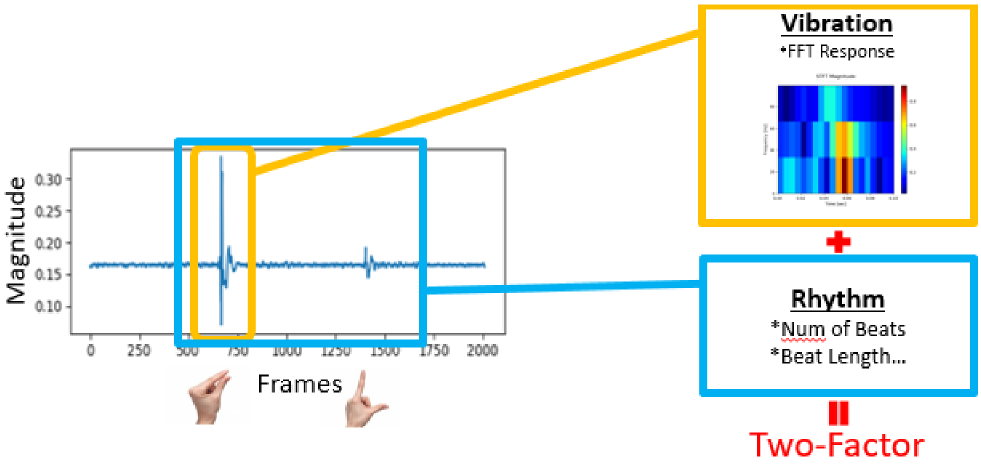
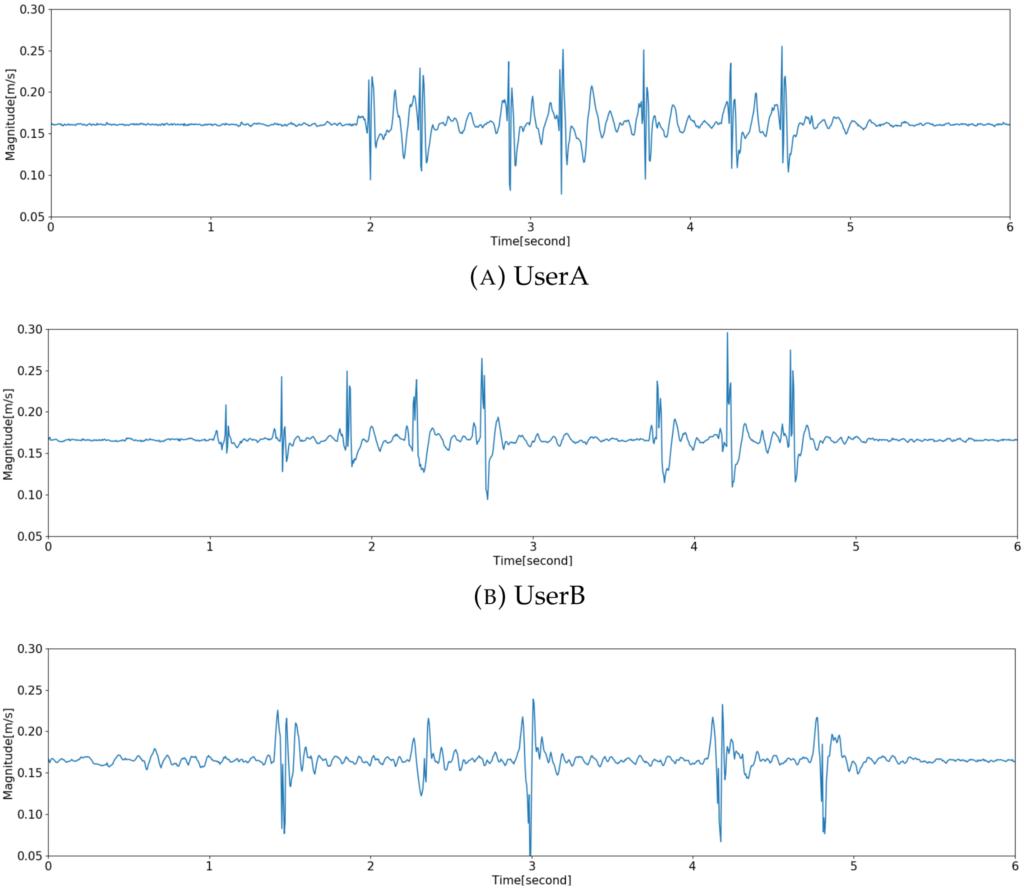


FIGURE 4.2: Realization of two factor scheme in TaPIN

your fingers. Since these two features (e.g rhythm and body structure) are different among users, we are able to achieve a two factor user authentication scheme for smartwatches. Figure 4.3 demonstrates some of the examples of TaPIN enrolled by different users. Note that we can observe a different beat pattern from each signal and each user has a different shape of vibration during finger tapping. For example, User A has 7 beats in total and each finger taps are distributed (2-2-1-2) in time domain. On the other hand, User B has different rhythm pattern compared to User A with 8 beats distributed as (5-3) in time domain. We can also observe that User C has higher attenuation making each vibration signal sharper than other two users. These difference in the signal can effectively be used as a factor for authentication since there are number of designs for rhythm pattern and body bio-metric cannot be easily replicated to make the same shape of the vibration produced by legitimate user.



(A) UserA

(B) UserB

(C) UserC

FIGURE 4.3: TaPIN signal from different users

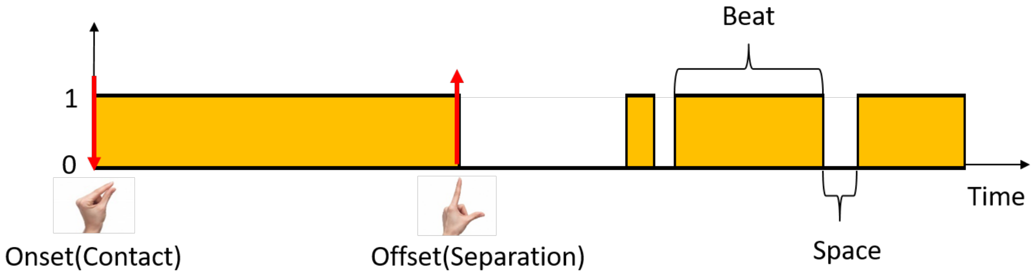


FIGURE 4.4: Rhythm Design

4.2 Rhythm pattern

TaPIN is rhythm based authentication scheme. Morse code is a one of the famous rhythm based code system which codes letters and numbers into uniform sequences of "dots" and "dashes". This system has a potential of being used as a secret but it is quite complicated and not user friendly for the normal users. TaPIN utilizes the rhythm generated by user's pinching motion. When we pinch our fingers, we will experience contact and separation between our thumb and forefinger. Here in our problem set, we defined the contact between two fingers as "Onset", whereas the separation as "Offset". The interval between "Onset" and "Offset" is called a "Beat" and the interval between "Offset" and "Onset" is called a "Space". Therefore, the rhythm design for our problem set looks like as shown in Figure 4.4. By combining the "Beat" and "Space", a lot of combination of rhythm can be designed by users.

4.3 Body Vibration

As mentioned earlier, pinching motion consists of "Contact" and "Separation" between thumb and forefinger. These two motion produces specific vibration signal which propagates through our body. Typically, the mathematical model of the complex vibration systems such as human body is difficult to analyze. To keep it simple, we built a single degree-of-freedom model to
]

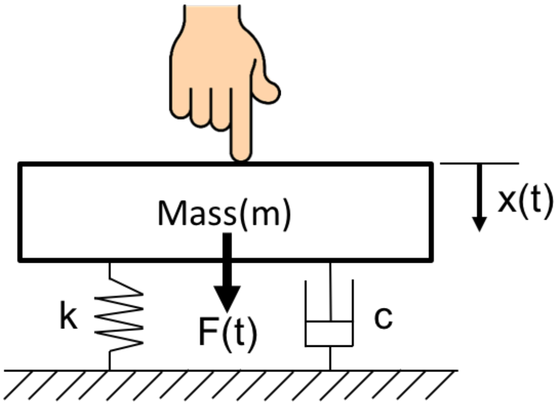


FIGURE 4.5: The vibration model of a tap

demonstrate the basic structure as shown in Figure 4.5. This model is called spring mass damper system [28] where, mass is represented by m, spring constant is k, and a damping coefficient is c. These constants represents body bio-metric such as body mass, thickness of the skin, bone and fat structure.

When an external force is applied through the body, vertical displacement take into place. From the equilibrium of forces, we can derive the following equation.

$$F(t) = ma(t) + kx(t) + v(t) \tag{4.1}$$

where $F(t)$ is the external force, v(t) is the velocity, $x(t)$ is the vertical displacement. By substituting acceleration and velocity with x(t), we can further get,

$$F(t) = m\frac{d^2x(t)}{dt^2} + kx(t) + c\frac{dx(t)}{dt} \tag{4.2}$$

Since pinching the fingers produces forced vibration with initial constant force $F(0)$, by applying Fourier Transform to the both side of 4.2, we can derive

$$\frac{F(0)}{jw}(1 - e^{-jw\Delta t}) = -w^2 mX(w) + kX(w) + jwcX(w) \tag{4.3}$$

after solving for $X(w)$,

$$X(w) = \frac{1 - e^{-jw\Delta t}}{-\frac{jm}{F(0)}w^3 - \frac{c}{F(0)}w^2 + \frac{jk}{F(0)}w} \tag{4.4}$$

where w is the frequency, and $X(w)$ is the power spectrum of the vertical vibration. The vertical vibration will be exposed to certain attenuation along the horizontal axis until it reaches the accelerometer as described 4.5.

$$y(t) = x(t)e^{-\alpha d} \tag{4.5}$$

Here $x(t)$ is the vertical displacement where the external force was applied (i.e. finger tips), whereas $y(t)$ is the vertical displacement that the vibration has propagated to, d is propagation distance, and α is an attenuation coefficient. Again after applying the Fourier transform to both sides of 4.5, we get

$$Y(w) = X(w)e^{-\alpha d} \tag{4.6}$$

Note that α is dependant upon propagating medium. α is large which means the attenuation is large when the wave is propagating through soft tissue such as fat, whereas α is small which means the attenuation is small when through hard structure such as bone. After putting 4.4 to 4.6, we obtain,

$$Y(w) = \frac{(1 - e^{-jw\delta t})e^{-\alpha d}}{-\frac{jm}{F(0)}w^3 - \frac{c}{F(0)}w^2 + \frac{jk}{F(0)}w} \tag{4.7}$$

Note that we assume initial constant force $F(0)$ and the duration Δt is stable due to users' pinching habit, while α, d, m, c, k is different among people which produces the discrepancies in vibration response among people. Therefore, frequency analysis such as FFT will effectively give us an insight of the user identity.

Chapter 5

System Design

5.1 System Overview

Figure 5.1 shows an overview of the TaPIN system. The basic workflow can be summarized as following: When a user awaken the screen, opens an app, or triggers some function that requires the user authentication, the system continuously monitors the accelerometer readings and when the user enters his/her own beat pattern by performing several pinch which produces certain vibration to the readings, it performs segmentation and obtains the signal which includes consecutive TaPIN secret. Once it obtains the TaPIN signal, it performs decomposition where it extract knowledge based rhythm information and biometric based vibration information. A classifier is trained by pre-enrolled feature vectors and when a new test sample comes it decides whether the feature input is legitimate user or not to give the authentication result to the user.

5.2 Capturing

We use accelerometer as a major sensing hardware to capture the tapping-induced vibration. We used LG W150 Urbane [17] for our whole project where the accelerometer model is MPU6515 from Inven Sense [12] which is an embedded accelerometer sensor in a lot of smart devices. MPU 6515 is

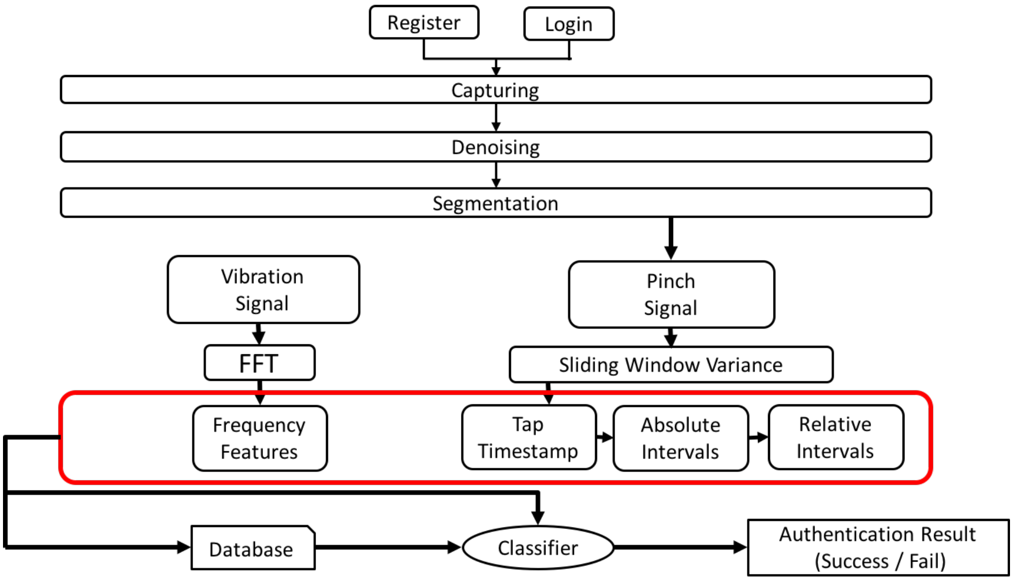


FIGURE 5.1: System Design

capable of capturing the data in each of 3 axis (x, y, z) with the sampling rate over 1000Hz but in most of the smartwatches, sampling rate is suppressed by the kernel with the maximum frequency of 200Hz. That was not an exception with LG W150 Urbane and we decided to stick with this suppressed sampling rate to validate our idea for commercial smartwatches.

5.3 Denoising

We need to denoise our data in order to remove the signal which is irrelavant to our scope. We observe users' unintentional motion in the reading which usually falls below 5Hz. We also observe gravity acceleration as DC component (0 Hz) in each axis of the readings. We need to remove this because this will lead to certain classification error at the end. This is because the power spectrum we obtain from frequency analysis integrates the gravity component which is dependant upon the angle rotation of the smartwatch. Butter-worth high pass filter with a cut off frequency of 20 Hz can successfully filter out the unnecessary readings stated above.

5.4 Segmentation

We perform segmentation to get the signal which has consecutive TaPIN secret. This process is to narrow down the signal from continuous accelerometer readings. According to previous works [4], Signal to Noise Ratio is used to segment a tapping-induced vibration. SNR can be expressed by mean divided by standard deviation of specific time interval as in equation 5.1 [27].

$$SNR = \frac{\mu}{\sigma} \tag{5.1}$$

SNR of finger taps even with slight taps are lower than that with other actions. Therefore, the signal is segmented when SNR exceeds certain threshold. In our proposal, we decided to calculate the SNR with the sliding window size of 2 seconds. This means that SNR will show lower value if there is tapping induced-vibration within 2 seconds. We observed that the offset which is the separation of the fingers have larger SNR than onset event with the value ranging around 50. Therefore, we decided to set the threshold as 75, and segment the data using the landmark as shown in the Figure 5.2. Note that the end point was set to the 0.5 seconds after the landmark to avoid collision with the vibration signal.

5.5 Decomposition

We extract "Knowledge based information" and "Biometric Based Information" from segmented signal. Here, Knowledge based information includes beat information such as timestamps of onset and offset event, Intervals, and relative intervals. Biometric based information consists of the statistical features of the vibration response in time and frequency domain.

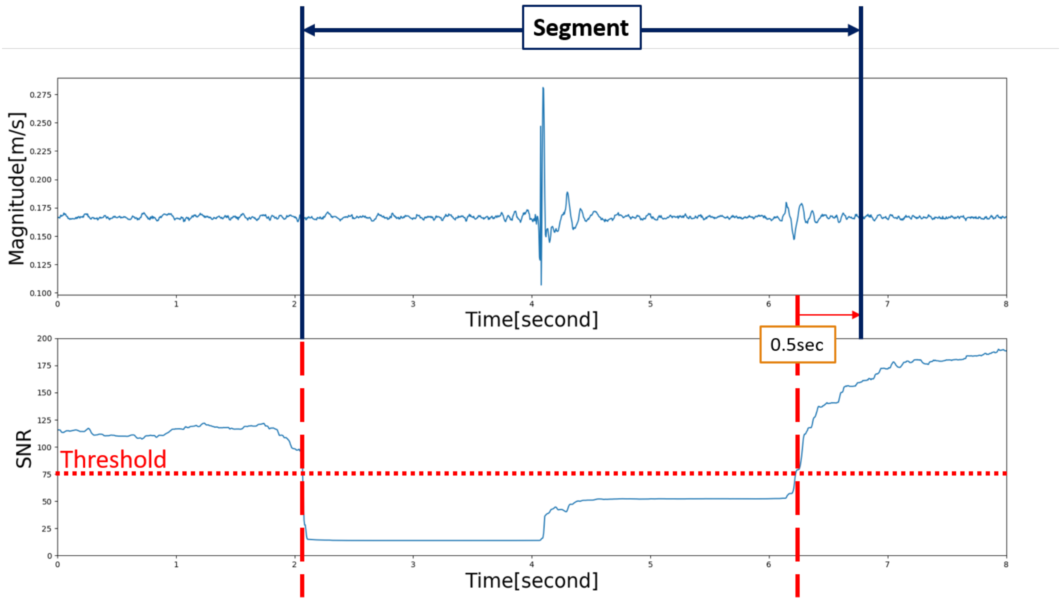


FIGURE 5.2: Overview of segmentation

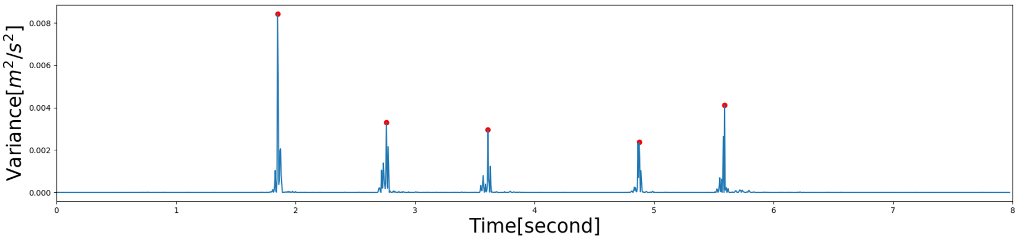


FIGURE 5.3: Variance (window size=0.01sec) and Onset detection

5.5.1 Knowledge based feature

Timestamps

We used variance based approach to get the beat information. Figure 5.3 shows the variance with the sliding window size of 0.01 second. We mark the time which exceeds the threshold as "Onset", where we set the threshold as $Threshold = \mu + \sigma$.

There is always one separation between two contacts, therefore, almost similar to detecting "Onset" event, we mark the time as "Offset" which gives the maximum variance between two "Onset" vibration. Figure 5.4 shows the overview of offset detection. Note that, based on the previous paper [4][5], we knew that the vibration duration is within 0.1 second so that here the

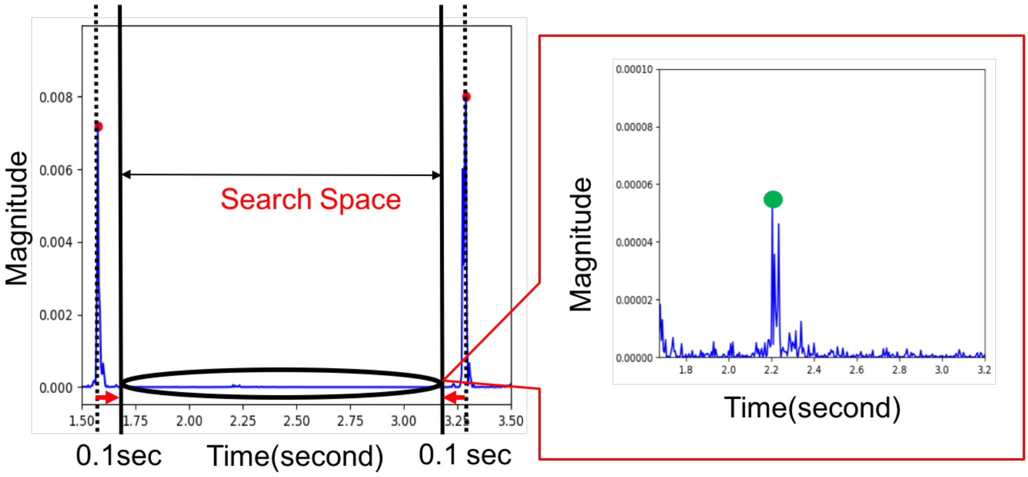


FIGURE 5.4: Offset detection

search space is between two "Onset" vibration which can be described as $[Onset[i] + 0.1sec, Onset[i+1] - 0.1sec]$.

We obtain two vectors; $\alpha = \{\alpha_2, \alpha_3, \alpha_4, ..., \alpha_n, \}$ and $\beta = \{\beta_1, \beta_2, \beta_3, ..., \beta_n, \}$, where α_i and β_i are the i_{th} onset and offset timestamps, respectively, and n is the TaPIN length. Note that each time stamp is the time from the first onset timestamp, therefore, α_1 is always 0 which we remove from our feature set.

Absolute intervals

In order to express the temporal correlation between two adjacent beats we also derive "Absolute Interval" by subtracting two adjacent "Onsets". We obtain $\gamma = \{\gamma_1, \gamma_2, \gamma_3, ..., \gamma_{n-1}, \}$, where $\gamma_i = \alpha_{i+1} - \alpha_i$.

Relative intervals

The user may tap slowly or faster than the registered inputs depending on his mood or environment. "Relative Interval" is used to cope with this temporal variance of the users' beat by dividing the "Interval" with entire signal duration. We obtain $\nu = \{\nu_1, \nu_2, \nu_3, ..., \nu_{n-1}, \}$, where $\nu_i = \frac{\gamma_{i+1}}{\beta n}$.

So to sum up if we perform n number of taps for TaPIN, the signal decomposes n-1 onsets, n offsets, n-1 relative intervals which results in 4n-3 features for Knowledge based information.

5.5.2 Bio-metric based feature

Bio-metric based information includes the statistical metrics of each "Onset" vibration in time and frequency domains. This feature helps defend against knowledge-aware attacks such as phishing attacks.

We first segment each vibration signal based on "Onset" timestamp by setting the end point as 0.1 second from the start point which is the duration of the typical tapping induced vibration [4][5].

Fourier Analysis is performed to each of the onset vibration to obtain frequency bio-metric. According to the previous paper [4][14], 30Hz-120Hz well distinguishes user because the frequency response are relevant among same user and sensitive among different user in the range. Therefore, we set the window size as 0.03 second, abandon first bin(0Hz-33Hz) and use second and third bin (34Hz-100Hz).

Then we derive multiple statistical features(Mean, Standard deviation, Max, Minimum, Root Mean Square, Kurotsis, Skewness, Inter Quartile Range, Entropy) that have been widely adopted representing signals [15][19][14] in Time and Frequency domain as shown in the Figure 5.5. However, some of these statistical features may not well distinguish user from the metrics. We perform feature selection using Fisher Scoring which is widely adopted supervised feature selection method based on following equation.

$$F_r = \frac{\Sigma_{i=1}^{l} n_i(\mu_i - \mu)}{\Sigma_{i=1}^{l} n_i \delta^2} \tag{5.2}$$

Fisher score computes the ratio between inter-class variance and the in-class variance of certain feature. The larger ratio means that the feature is distant

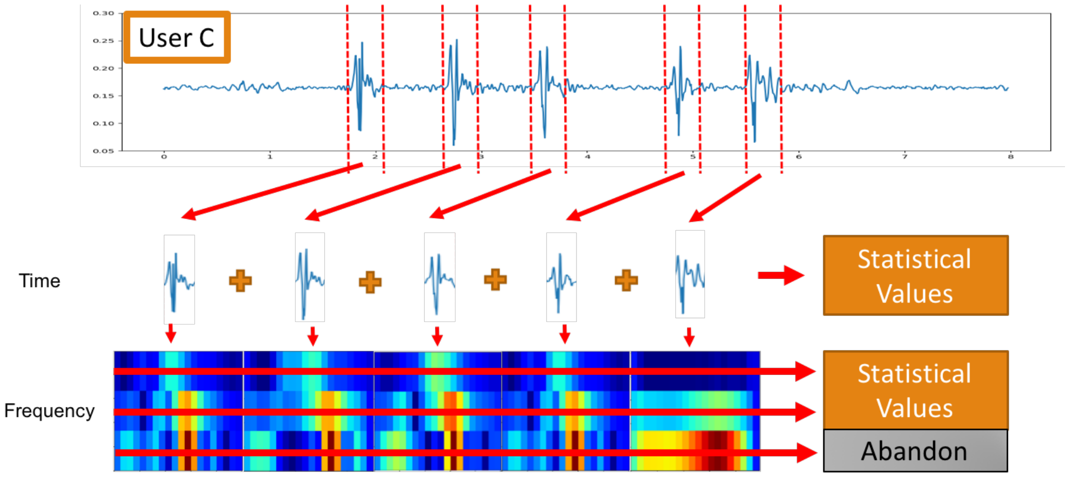


FIGURE 5.5: Biometric based feature extraction

among other classes and close within the same class, thus suggesting that this feature well represents the data. For the sake of simulation, we recruited 15 volunteer and collected 50 data samples from each of the the volunteers, each time performing a consistent 7-beat TaPIN. From the dataset, after multiple preprocessing including denoising, segmentation, feature extraction, we selected top 20 features as described in the Table 5.1 for bio-metric information.

5.6 Classification

We perform classification to compare the input with pre-enrolled data points to decide whether the input is the legitimate user or the imposter. We used a model inspired by one class kNN classifier which is categorized as an unsupervised learning method. kNN assumes that new samples from the same user will be similar to the samples in the training data. This similarity is represented by the Euclidean distance. In the training phase, a threshold is determined by computing an average of distances between each two training

Feature	Domain	axis	bins	Fisher Score rank
Mean	Time	x	-	16
Mean	Time	y	-	1
Mean	Time	z	-	12
Standard Deviation	Time	z	-	8
Maximum	Time	z	-	15
Skewness	Time	y	-	17
Entropy	Time	x	-	13
Entropy	Time	y	-	18
Mean	Frequency	x	2	11
Mean	Frequency	x	3	2
Mean	Frequency	z	2	6
Standard deviation	Frequency	x	2	3
Standard deviation	Frequency	y	2	10
Standard deviation	Frequency	y	3	20
Standard deviation	Frequency	z	3	7
RMS	Frequency	x	2	14
Kurtosis	Frequency	y	3	19
Skewness	Frequency	x	3	5
Skewness	Frequency	y	3	9
Entropy	Frequency	x	2	4

TABLE 5.1: Top 20 feature based of Fisher score

samples as expressed in equation 5.3.

$$Thres = \alpha \frac{\Sigma_{i=1}^{N-1} \Sigma_{j=i+1}^{N} dij}{C_N^2} \tag{5.3}$$

On the other hand, in the testing phase, a classification score is assigned based on the average distances calculated between the test sample and the nearest training samples as shown in equation 5.4.

$$Score = \frac{\Sigma_{i=1}^{k} dij}{k} \tag{5.4}$$

If the score is below the threshold, this test sample is considered as a legitimate input. If not, then it will fail the authentication.

Note here that the value of alpha and k decided the trade-off between "Usability" and "Security". Larger alpha and smaller k leads to larger threshold and smaller score which leads to higher acceptance rate for user inputs. This contributes to the “Usability” of the legitimate user. On the other hand, smaller alpha and larger k leads to smaller threshold and larger score which lead to higher rejection rate. This contributes to the “Security” against attacks. Therefore, we need to find alpha and k which gives the best balance between “Usability” and “Security”. We evaluated our classifier using following four metrics.

- **False Rejection Rate (FRR)**: The rate that the legitimate user is denied by the system. It is calculated as the ratio of the number of incorrect classification result of legitimate user input to the total number of attempts by legitimate user.

- **False Acceptance Rate (FAR)**: The rate that the imposter is classified as the legitimate user. It is calculated as the ratio of the number of accepted classification result of imposter input to the total number of attempts by imposter.

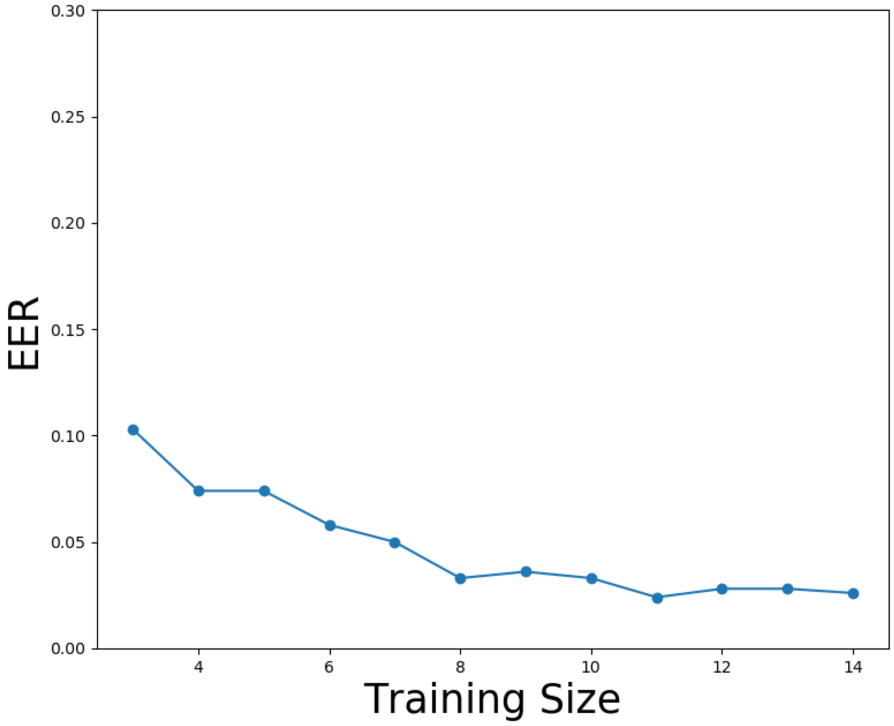


FIGURE 5.6: EER under different training sample size

- **Equal Error Rate (EER)**: The rate when the FAR and FRR provides same value based on parameter decision.

The same dataset described in "Decomposition" section was used to decide the parameter for the classification model.

Training size

Training sample size plays an important role to system accuracy. We will get better performance result if we have larger training size. Based on the result shown in Figure 5.6, we obtain the stable EER once after the size of 10, thus we adopt 10 as configured training sample size for our prototype.

Parameter Decision

We further analyzed the system using training size of 10 to find the alpha and k which gives the best balance between “Usability” and “Security.” The Table

5.2 displays the "False Acceptance Rate" which is the rate that an attacker is detected as the legitimate user. So when alpha is 1.82 and when k is 2, there is a 5.3% chance that an attacker enrolls into the system. On the other hand, the Table 5.3 displays "False Rejection Rate" which is the rate that the legitimate user is denied by the system. So when alpha is 1.82 and k=2 there is 4.0% chance that the legitimate user will experience an issue enrolling into the system.

FAR		α							
		1.75	1.76	1.77	1.78	1.79	1.80	1.81	1.82
k	1	4.7	4.8	4.9	5.1	5.3	5.4	5.6	5.8
	2	4.0	4.1	4.3	4.5	4.7	4.8	5.1	5.3
	3	3.0	3.2	3.4	3.6	3.8	3.9	4.1	4.2
	4	3.0	3.2	3.4	3.5	3.7	3.9	4.1	4.2
	5	2.9	3.0	3.2	3.4	3.6	3.8	4.0	4.3
	6	3.1	3.4	3.6	3.7	3.9	4.2	4.3	4.5
	7	3.1	3.3	3.5	3.6	3.8	3.9	4.2	4.4
	8	2.6	2.8	2.9	3.1	3.2	3.3	3.6	3.9
	9	2.7	2.9	3.1	3.2	3.3	3.6	3.8	4.0
	10	2.8	3.0	3.1	3.2	3.4	3.6	3.9	4.1

TABLE 5.2: FAR at different parameter values

FRR		α							
		1.75	1.76	1.77	1.78	1.79	1.80	1.81	1.82
k	1	5.5	5.0	5.0	4.5	4.3	4.3	4.0	4.0
	2	5.0	4.8	4.7	4.3	4.3	4.3	4.2	4.0
	3	4.0	3.8	3.7	3.3	3.2	2.8	2.7	2.5
	4	3.2	3.2	3.2	3.2	3.0	3.0	2.7	2.3
	5	3.3	3.0	2.7	2.5	2.3	2.3	2.2	2.2
	6	3.0	2.8	2.7	2.5	2.5	2.3	2.3	2.3
	7	3.2	3.2	3.2	3.2	3.2	3.0	2.8	2.5
	8	3.7	3.3	3.3	3.3	3.3	3.2	3.2	2.8
	9	3.7	3.7	3.7	3.5	3.3	3.0	3.8	2.5
	10	3.7	3.70	3.5	3.3	3.2	3.2	2.7	2.3

TABLE 5.3: FRR at different parameter values

So as explained earlier, the left table refers to "Security" and the right table refers to "Usability". We need to find alpha and k which gives the best balance between these 2 goals. From this tables we chose alpha as 1.79 and k as 9 so that it gives 3.3% rate for both goals.

So to sum up, we used 10 training inputs and set alpha as 1.79 and k as 9 to build the prototype.

Chapter 6

Implementation and Experimental setup

6.1 Implementation

To validate our idea, we built a proof-of-concept prototype on LG W150 Urbane smartwatch with a 1.3″ Full Circle P-OLED touchscreen, 1.2GHz Quad-Core processer, a RAM with 512MB, 410mAh of battery and Android Wear 2.1.3. LG W150 Urbane incorporates Inven Sense MPU6515 as a embedded accelerometer which is widely used in commercial smartwatches such as Moto 360 [22], Samsung Gear 2 [23] and Gear Fit [8]. The prototype captures the data through existing Android Wear API so that it is also deployable to other Android smartwatches. Note here that for the sake of efficient data collection and faster computation, we streamed the data to the server where the signal is further processed and analyzed to provide a real-time registration and authentication scheme.

6.2 Experimental Setup

We recruited 16 volunteers to perform extensive experiments on prototype as means of "Usability" and "Security". The Table 6.1 shows some of statistical information our volunteers. Our volunteers was 18-29 years old, with

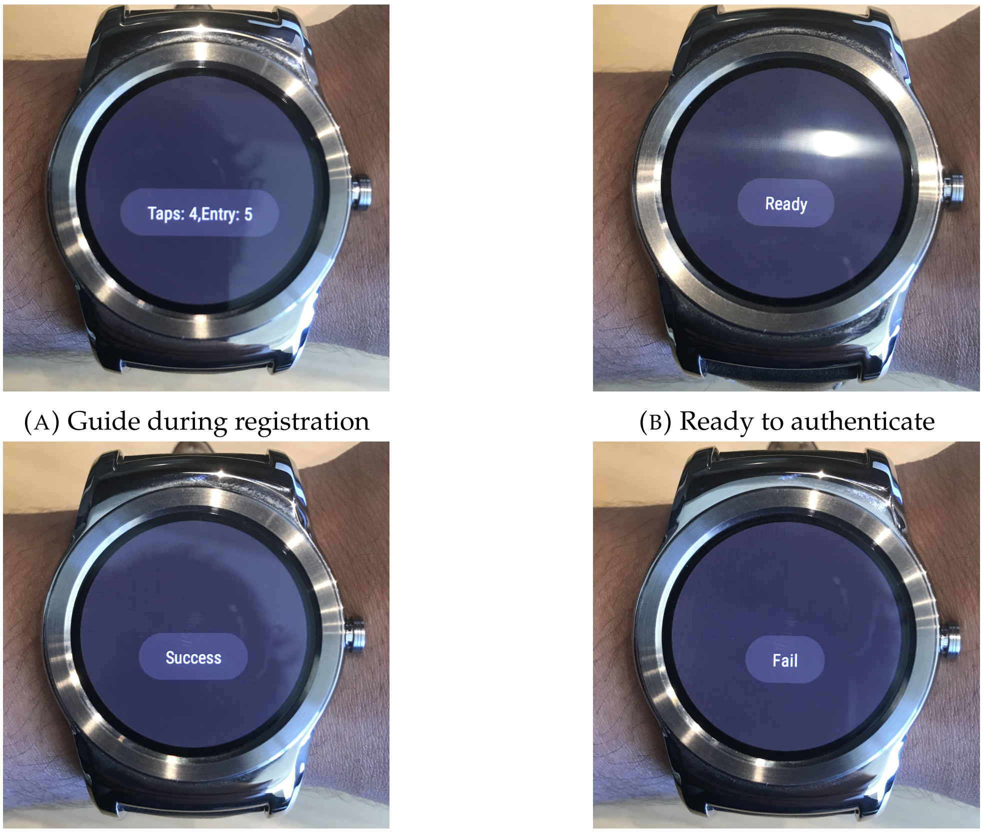
Gender	No.	Age	No.	BMI	No.	Experience	No.
Female	2	18-23	7	15.00-19.99	2	None	13
Male	14	24-29	9	20.00-24.99	10	Smartwatch	2
				25.00-40.00	3	Authentication	1
				N/A	1		

TABLE 6.1: Distribution of volunteer information

the BMI ranging from 15-40. Besides, around 80% of our volunteers used a smartwatch for the first time. We asked the volunteers to do the registration, authentication, and widely known security attacks. For the registration, user is asked to enroll their self-designed TaPIN 10 times without any constraints in beat pattern. During the process, our prototype guides the user by displaying the popups showing the number of taps and total number of entries up to now as shown in Figure 6.1a. Once the entry reaches to 10, it notifies users that it is ready to be used as shown in Figure 6.1b.

Once the user completes the registration, they try to unlock the device with their legitimate TaPIN. When the user is classified as a legitimate user, the word "Success" shows up on the screen, whereas if the user is classified as imposter the word "Fail" shows up on the screen as shown in Figure 6.1c and Figure 6.1d.

We also asked the user to attack the system enrolled by another user. In our proposal, we consider two types of widely known attacks; Zero-effort attack and Over-the-shoulder attack. In Zero-effort attack, the attacker doesn't have any knowledge about the secret so that they try to randomly generate the pin to bypass the system. On the other hand, in Over-the-shoulder attack, user gets the knowledge by observing the victim performing the pinch motion. This is considered a one of the serious attacks that has a potential to mimic not only the rhythm pattern but also initial force which is incorporated to vibration response.



(A) Guide during registration

(B) Ready to authenticate

(C) Success

(D) Fail

FIGURE 6.1: User interface in TaPIN

Chapter 7

Performance Evaluation

7.1 Security

The goal of the attacker is to impersonate a legitimate user by generating similar signal with pre-registered data. This means that attacker has a physical access to the device and tries to mimic the rhythm pattern or the behavior such as initial tapping force, the location of the pinch, angle of the legitimate users arm etc. In our experimental setup, we considered two types of widely known security attacks; Zero-effort Attack and Over-the-shoulder Attack. We asked the volunteers to strictly obey not to share the secret to another volunteers so that we consider each attack to be an authentic one in real scenario.

7.1.1 Zero-effort Attacks

Zero-effort attack is one of the most common attack we observe in different authentication scheme and also not the exception for our model. The attacker isn't required to do some data collection and analysis for the secret, so that this attacking scheme is possible for any imposter who has the physical access to the device. During the experiment, attacker is not provided with the secret from the victim so that we can simulate the scenario that the attacker blindly tries to guess the TaPIN. We asked each volunteers to attack 3 times independently to several model and Table 7.1 shows there was 208 trials distributed in each beat length. By using our registered user model, we achieved a success rate of 0.0 to all the beat length. Here, as a feature of rhythm based approach, the longer the beat length is, the more difficult it is to crack the system. The result of the success rate with 0.0 for the beat length of 3 suggests that the system is highly resistant and robust against zero-effort attack.

Beat Length	Success	Total Attacks	FAR
3	0	36	0.00
4	0	18	0.00
5	0	36	0.00
6	0	42	0.00
7	0	54	0.00
8	0	18	0.00

TABLE 7.1: Success rate under Zero-effort Attack

7.1.2 Over-the-shoulder Attacks

Over-the-shoulder attack is also one of the common attacking scheme to the authentication system. The attacker tries to take a video or physically observe the victim performing the authentication. This is considered as the most serious attack for existing Password/PIN and graphical pattern authentication scheme.

This can also be a major threat to TaPIN, since the user is focused on unlocking the system which allows an attacker to carefully observe the secret without noticed by a victim. Besides, TaPIN produces certain motion to the public so that the attacker can visually check the secret so that leads to a huge potential of replicating the same rhythm pattern with same behavior such as initial force, angle rotation of the arm, location of the tap etc. However, theoretically TaPIN incorporates several bio-metric based information which is different among people so that the system is resistant to these attacks. To evaluate the attacking scheme, we asked the victim to show the attacker how

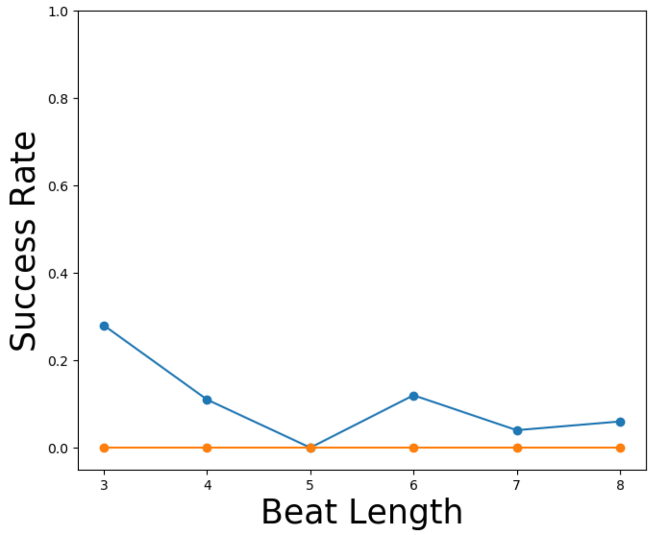
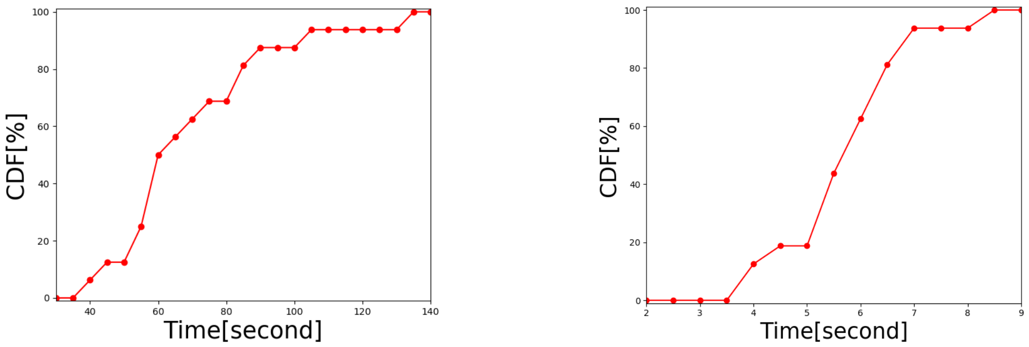


FIGURE 7.1: Success rate under Zero-effort Attack and Over-the-shoulder Attack

to perform the taps by showing them with their own hands. The victim also provided the attacker with some knowledge of the music or rhythm which they utilized to design the secret. We asked each of the volunteers to attack the model enrolled by another user 3 times independently. The Table 7.2 shows there was 208 trials distributed in each beat length. By using our registered user model, we achieved a success rate below 0.3. We also observed from Figure 7.1 that success rate can be decreased down to 0.06 if we have the beat length over 7.

Beat Length	Success	Total Attacks	FAR
3	10	36	0.28
4	2	18	0.11
5	0	36	0.00
6	5	42	0.12
7	2	54	0.04
8	1	18	0.06

TABLE 7.2: Success rate under Over-the-shoulder Attack



(A) Enrollment Time

(B) Login Time

7.2 Usability

Usability is also one of the important factor we need to consider if we are configuring for practical implementation. We evaluated the usability of TaPIN as aspects in Time consumption and Login attempts.

7.2.1 Time Consumption

We measured the time consumption of enrollment and authentication. Specifically, time consumption of enrollment is the time it required users to register TaPIN for 10 times and build the model. On the other hand, time consumption of authentication is the time it required users to perform TaPIN and get the result back from the server.

Enrollment Time

Figure 7.2a plots the cumulative density function of the time consumption during enrollment. The enrollment time of TaPIN ranges from 36.3 to 134.0 seconds, with the average value as 68.2 seconds, its median value as 58.7 seconds, and its 90th percentile as 93.8 seconds.

Authentication Time

Figure 7.2b plots the cumulative density function of the time consumption during authentication. The authentication time of TaPIN ranges from 3.59 to 8.27 seconds, with the average value as 5.63 seconds, its median value as 5.61 seconds, and its 90th percentile as 6.72 seconds.

7.2.2 Login Attempts

The number of login attempts until success is also one of the scale we need to consider for usability. Google applications allow user to try 5 times at most but it is desired that we can shrink this limitation as much as possible. In our experiment, all the 16 valid user was able to successfully unlock their system by a single trial.

7.3 User Perception

We conducted a user study after experiment to analyze how they feel about the "Usability" and "Security" of TaPIN compared to other existing methods(Password, PIN, Pattern). We used Likert Scale where 10 refers to "Best" and 1 refers to "Worst".

While answering this questionnaire, volunteers tries to compare each methods with TaPIN so that the result indicate the preference and improvement over existing methods. Figure 7.3 shows the result of our user study. We can say that TaPIN outperformed as in aspect of Usability compared to other existing methods. We expect this positive outcome for our design goals is because the user was happy about not interacting with small touch screen which exists in other existing methods. While as for the Security aspects, our

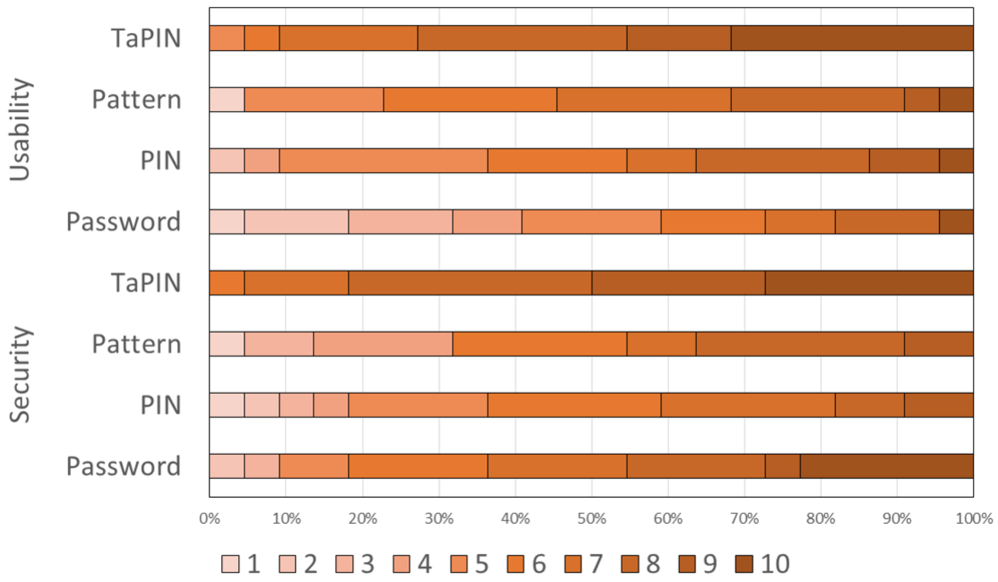


FIGURE 7.3: User perception

volunteers thought it is as resistant as the password based approach. However, this has to be addressed in the future work for further improvement utilizing bio-metric information to avoid credential aware attacks.

Chapter 8

Future Works

8.1 Robustness against user motion

We observed that some of the daily activities such as walking or squatting sometimes gives the SNR below 75 where the system starts processing approach where we set a lower threshold around 20 for the start point and if and only if the start point is detected, we end the signal with the threshold value of 75. This approach help the system ignore most of the daily activities because the SNR of those activity aren't as low as 20. Extensive experiments has to be done to validate the scheme.

8.2 Robustness against user state

As discussed in Chapter4, the frequency response of the vibration integrates certain bio-metric coefficient which is different among people. However, these response also may vary within same user corresponding to the users' wearing state. This includes different initial tapping force, variance in wearing position, or the arm rotation which typically changes the force dispersion. Further evaluation and analysis is required to validate the robustness against these temporal variation.

8.3 Classification Performance

Further data collection has to be done to configure the parameter which builds a reliable authentication scheme. The volunteers has to be distributed in different categories as in age, gender, BMI,and user experience. This ensures that the system has the integrity in the performance while used by a different types of people.

We also can evaluate our performance as in different classification model. One class SVM [20], DenID [4] are one of the model directly applicable to our problem set. We can also think of using two class classification model such as kNN, SVM, Neural Networks, Random Forest etc. However, two class classification model requires huge training samples in the training phase to obtain a better accuracy so that further analysis on computation is required.

8.4 Development of stand alone app

We streamed the captured data to the server for the sake of efficient data collection and faster processing during experiments. We can develop a stand alone app in smartwatch itself so that it doesn't rely on server computation. This development also includes some of the UI improvement by combining some interactive effects which entertains users.

Bibliography

[1] Panagiotis Andriotis, Theo Tryfonas, and George Oikonomou. "Complexity Metrics and User Strength Perceptions of the Pattern-Lock Graphical Authentication Method". In: vol. 8533. June 2014, pp. 115–126. DOI: 10.1007/978-3-319-07620-1_11.

[2] Buriro Attaullah et al. "AirSign: A Gesture-Based Smartwatch User Authentication". In: Oct. 2018, pp. 1–5. DOI: 10.1109/CCST.2018.8585571.

[3] Adam Aviv et al. "Smudge Attacks on Smartphone Touch Screens". In: *Proceedings of the 4th USENIX Conference on Offensive Technologies, WOOT'10* (Dec. 2010).

[4] Wenqiang Chen et al. "Taprint: Secure Text Input for Commodity Smart Wristbands". In: May 2019, pp. 1–16. ISBN: 978-1-4503-6169-9. DOI: 10.1145/3300061.3300124.

[5] Wenqiang Chen et al. "ViType: A Cost Efficient On-Body Typing System through Vibration". In: June 2018, pp. 1–9. DOI: 10.1109/SAHCN.2018.8397098.

[6] Sauvik Das et al. "Thumprint: Socially-Inclusive Local Group Authentication Through Shared Secret Knocks". In: May 2017, pp. 3764–3774. DOI: 10.1145/3025453.3025991.

[7] *Fitbit*. https://www.fitbit.com/us/home. Accessed: 2020-04-30.

[8] *Gear Fit*. https://www.samsung.com/us/support/owners/product/gear-fit. Accessed: 2020-04-30.

[9] *GooglePay*. https://pay.google.com/about/. Accessed: 2020-04-30.

[10] Chris Harrison, Desney Tan, and Dan Morris. "Skinput". In: *Communications of the ACM* 54 (Aug. 2011), p. 111. DOI: 10.1145/1978542.1978564.

[11] Ben Hutchins et al. "Beat-PIN: A User Authentication Mechanism for Wearable Devices Through Secret Beats". In: May 2018, pp. 101–115. DOI: 10.1145/3196494.3196543.

[12] *Invensense-MPU6515*. https://invensense.tdk.com/products/motion-tracking/6-axis/mpu-6500/. Accessed: 2020-04-30.

[13] Umarani Jayaraman et al. "Recent Development in Face Recognition". In: *Neurocomputing* (Apr. 2020). DOI: 10.1016/j.neucom.2019.08.110.

[14] Gierad Laput, Robert Xiao, and Chris Harrison. "ViBand: High-Fidelity Bio-Acoustic Sensing Using Commodity Smartwatch Accelerometers". In: Oct. 2016, pp. 321–333. DOI: 10.1145/2984511.2984582.

[15] Oscar Lara and Miguel Labrador. "A Survey on Human Activity Recognition Using Wearable Sensors". In: *Communications Surveys Tutorials, IEEE* 15 (Jan. 2013), pp. 1192–1209. DOI: 10.1109/SURV.2012.110112.00192.

[16] *LEXICO powered by OXFORD*. https://www.lexico.com/en/definition/authentication. Accessed: 2020-04-30.

[17] *LG W150 Urbane*. https://www.lg.com/us/smart-watches/lg-W150-lg-watch-urbane. Accessed: 2020-04-30.

[18] Jian Liu et al. "VibWrite: Towards Finger-input Authentication on Ubiquitous Surfaces via Physical Vibration". In: Oct. 2017, pp. 73–87. DOI: 10.1145/3133956.3133964.

[19] Dong Ma et al. “SolarGest: Ubiquitous and Battery-free Gesture Recognition using Solar Cells”. In: May 2019, pp. 1–15. ISBN: 978-1-4503-6169-9. DOI: 10.1145/3300061.3300129.

[20] Larry Manevitz and Malik Yousef. “One-class SVMs for document classification”. In: *J. Mach. Learn. Res* 2 (Jan. 2002), pp. 139–154.

[21] William Melicher et al. “Usability and Security of Text Passwords on Mobile Devices”. In: May 2016, pp. 527–539. DOI: 10.1145/2858036.2858384.

[22] *Moto360*. https://www.motorola.com/us/moto360/p. Accessed: 2020-04-30.

[23] *Samsung Gear S2*. https://www.samsung.com/global/galaxy/gear-s2/. Accessed: 2020-04-30.

[24] Florian Schaub, Ruben Deyhle, and Michael Weber. “Password entry usability and shoulder surfing susceptibility on different smartphone platforms”. In: Dec. 2012, p. 1. ISBN: 9781450318150. DOI: 10.1145/2406367.2406384.

[25] Nadzril Sulaiman and Q. Ariffin. “Overview on Fingerprinting Authentication Technology”. In: Mar. 2020, pp. 451–462. ISBN: 978-981-15-2316-8. DOI: 10.1007/978-981-15-2317-5_38.

[26] *Wikipedia-Security*. https://en.wikipedia.org/wiki/Security. Accessed: 2020-05-03.

[27] *Wikipedia-Signal to Noise Ratio*. https://en.wikipedia.org/wiki/Signal-to-noise_ratio. Accessed: 2020-04-30.

[28] *Wikipedia-SpringMassDamperSystem*. https://en.wikipedia.org/wiki/Mass-spring-damper_model. Accessed: 2020-04-30.

[29] *Wikipedia-Usability*. https://en.wikipedia.org/wiki/Usability. Accessed: 2020-05-03.

[30] Jacob Wobbrock. "TapSongs: Tapping rhythm-based passwords on a single binary sensor". In: Jan. 2009, pp. 93–96. DOI: 10.1145/1622176.1622194.

[31] Lin Yang, Wei Wang, and Qian Zhang. "VibID: User Identification through Bio-Vibrometry". In: Apr. 2016, pp. 1–12. DOI: 10.1109/IPSN.2016.7460725.

[32] Cheng Zhang et al. "TapSkin: Recognizing On-Skin Input for Smartwatches". In: Nov. 2016, pp. 13–22. ISBN: 978-1-4503-4248-3. DOI: 10.1145/2992154.2992187.