深圳大學
SHENZHEN UNIVERSITY

Taprint: Secure Text Input for Commodity Smart Wearables

Wenqiang Chen, Lin Chen, Yandao Huang, Xinyu Zhang*,
Lu Wang, Rukhsana Ruby, Kaishun Wu
Shenzhen University
*University of California San Diego

Mobicom 2019
Los Cabos

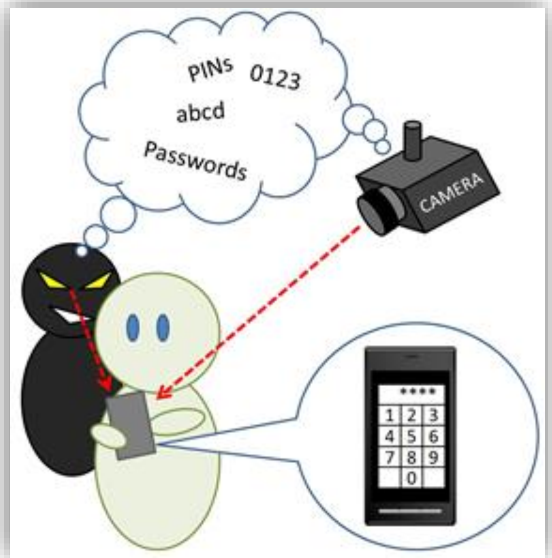
Contents

Background

1. Smart wristbands contain lots of personal data.
2. And the tendency of mobile payment is irreversible.
3. The security & privacy problems become the primary issue that the users concern about !!!

Background

Limitation of Screen Size

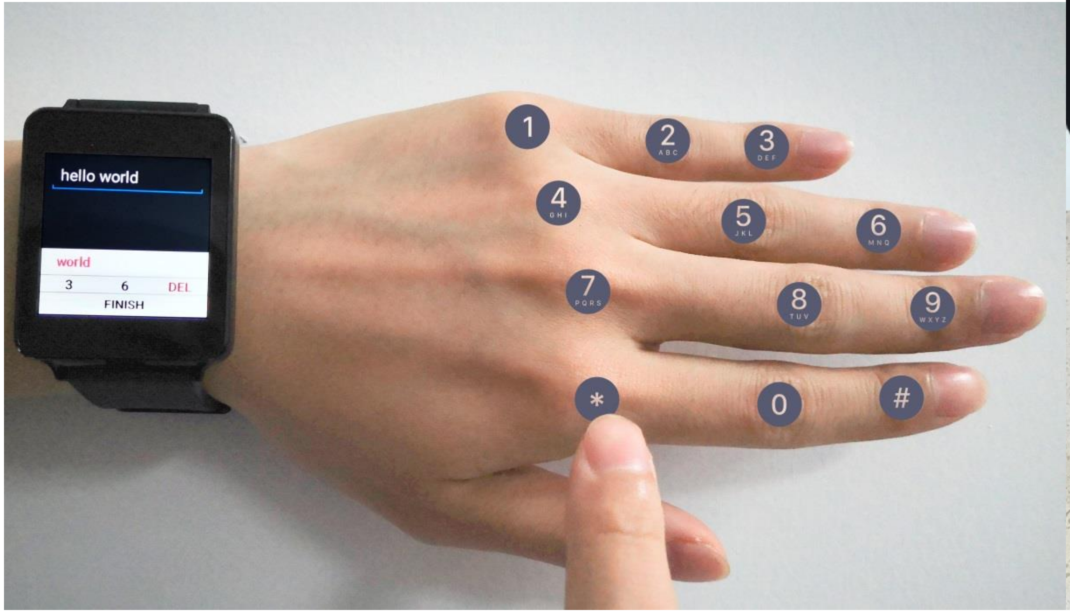


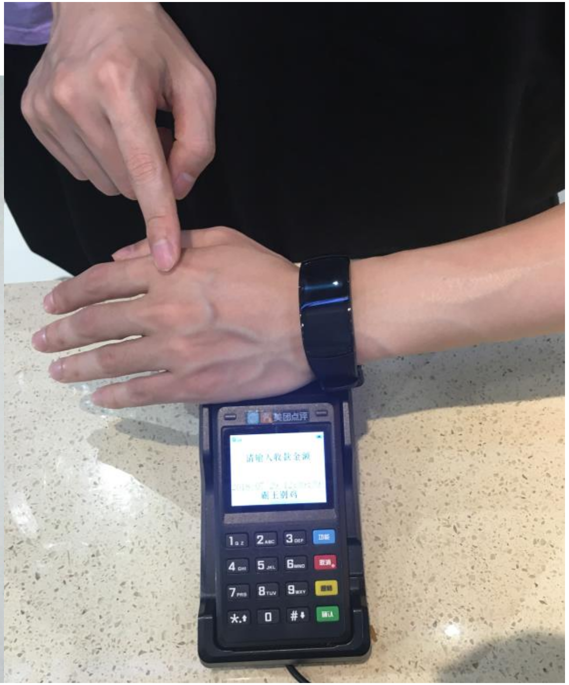
Shoulder Surfing

Smudge Attack

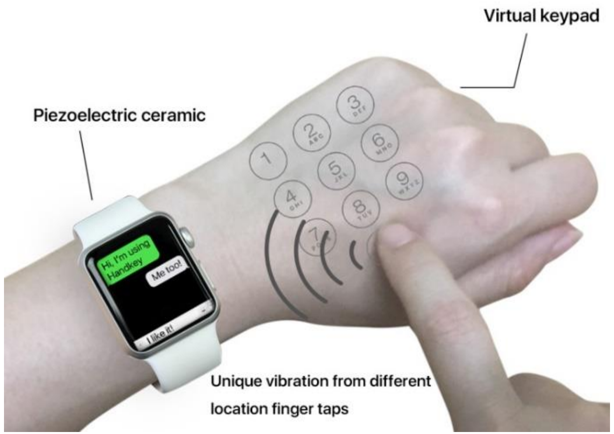
Ourwork——Taprint

- Vibration-based input recognition & authentication
- PIN-code Unlock & Single-touched Unlock
- LG G Watch W100：Accelerometer & Gyroscope
- Modified Linux kernel, 100Hz-->500Hz
- Security：128 paticipants



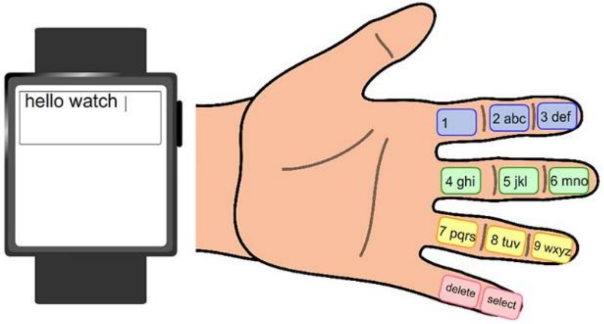


Related Work



ViType[1]

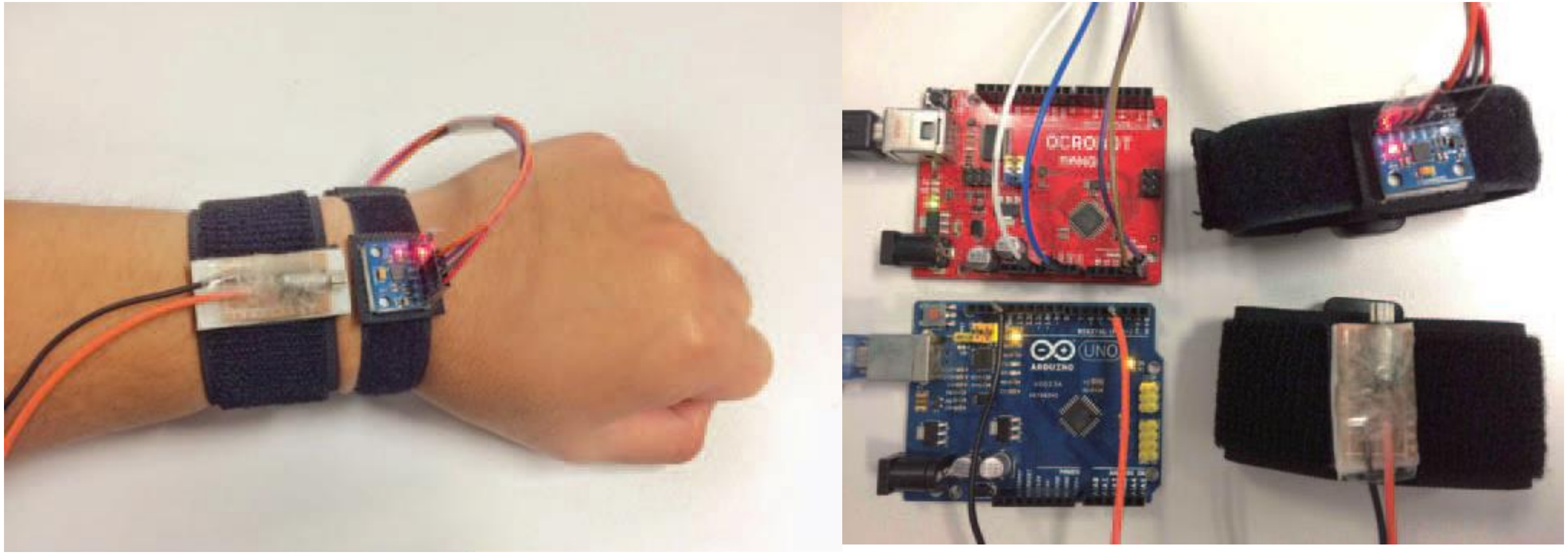
Float [2]



FingerT9 [3]

1. Wenqiang Chen, et.al. ViType: A Cost Efficient On-Body Typing System through Vibration, IEEE SECON, 2018
2. Ke Sun, et.al. Float: One-Handed and Touch-Free Target Selection on Smartwatches, ACM CHI, 2017.
3. Pui Chung Wong, et.al. FingerT9: Leveraging thumb-to-finger interaction for same-side-hand text entry on smartwatches, ACM CHI, 2018.

Related Work



VibID

Yang, L., W. Wang and Q. Zhang. VibID: User Identification through Bio-Vibrometry. IEEE IPSN, 2016

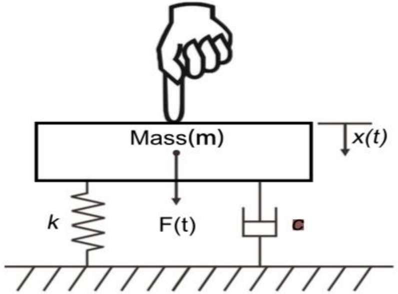
Preliminary——Vibration Model

$$F(t) = ma(t) + kx(t) + cv(t)$$

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

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

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



$$y(t) = x(t)e^{-\alpha d} \qquad Y(w) = X(w)e^{-\alpha d}$$

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

F(t): the external force

v(t): the speed

c: the damping coefficient

k: the spring constant

m: the mass

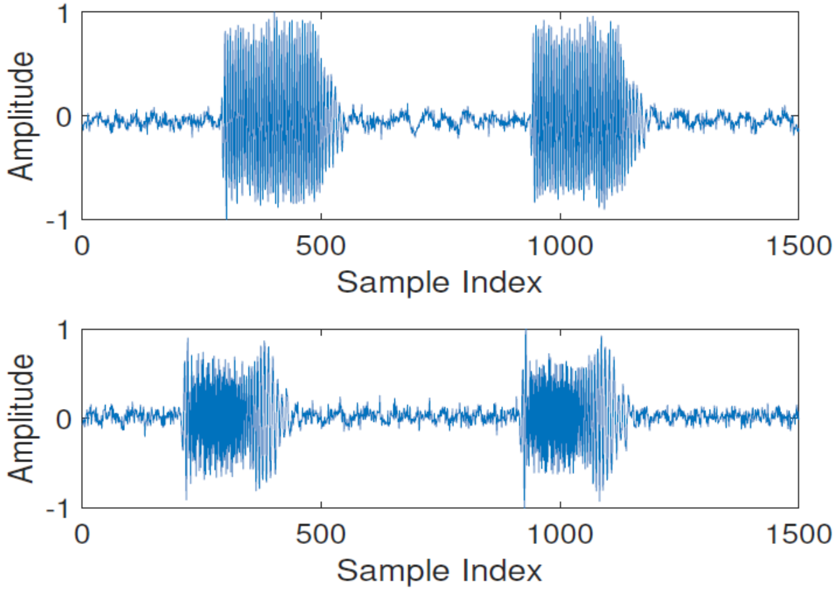
m , c and k vary from person to person[1]

↓

Unique vibration profile

[1] W. E. Siri. "*The gross composition of the body.*" Adv Biol Med Phys, 1956, vol. 4, no. 239-279, pp. 513.

Preliminary——Exp1 （Does the m, c, k really vary from different people?）



(a)

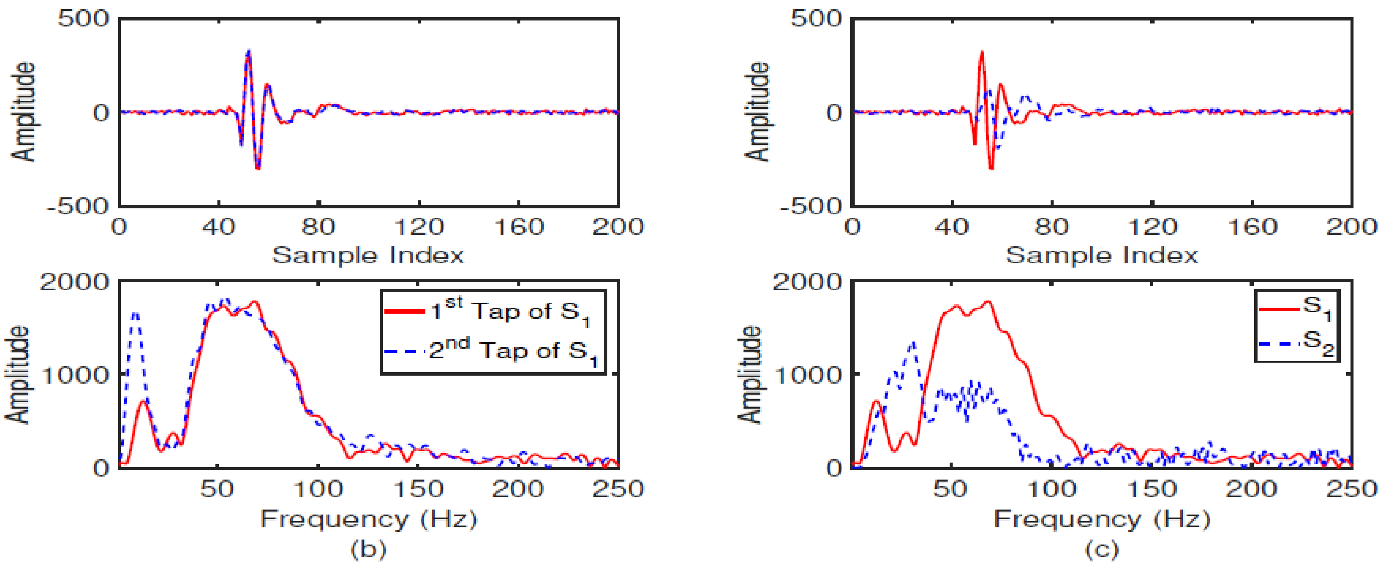
$$Y(w) = \frac{(1-e^{-jw\Delta t})e^{-\alpha d}}{-\frac{jm}{F(0)}w^3 - \frac{c}{F(0)}w^2 + \frac{jk}{F(0)}w}$$

To control the variables of F(0) and △t, we first utilize a motor to vibrate twice on the hand back of two subjects respectively to investigate the profile .

Observation

Twice vibrations on subject 1 generate the same profile with respect to time domain

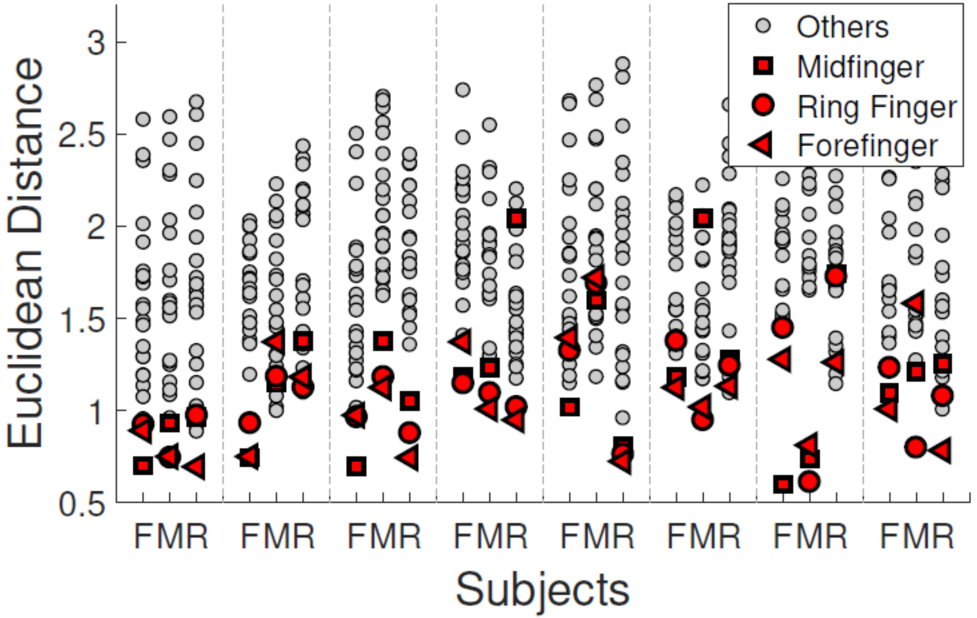
Preliminary——Exp1（Does the m, c, k really vary from different people?）



Observation

Vibrations on subject 1 and subject 2 generate different profile with respect to time domain and frequency domain.

Preliminary——Exp2（Does the distinction comes from the hand back or the finger?）



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

Observations

- The Euclidean distance of most legal samples is smaller than that of illegal samples.
- The Euclidean distance of different finger is about the same.
- Some of the legal samples mix with illegal ones, which might be caused by the variation of tapping force.

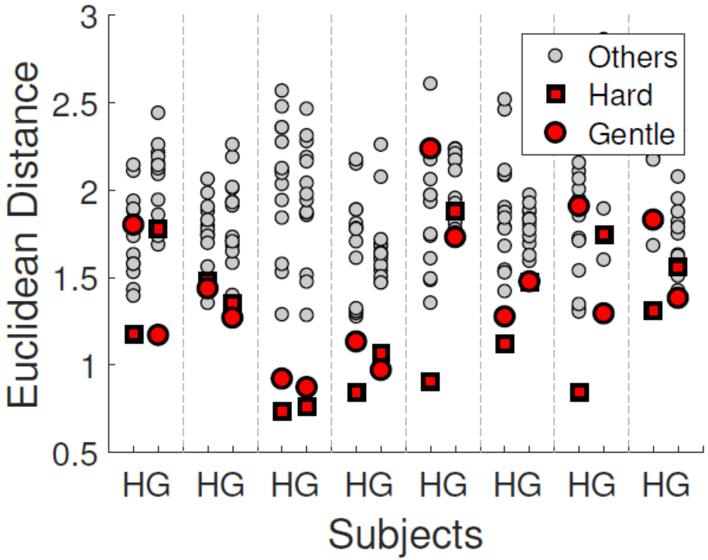
Preliminary——Conclusion of Exp1 & Exp2

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

1. The features of m, c, k dose vary from different people.
2. Distinct signals is generated mainly by hand back with features of m, c, k rather than finger.

Preliminary——Exp3 （Does the initial force F(t) impacts the vibration? ）

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



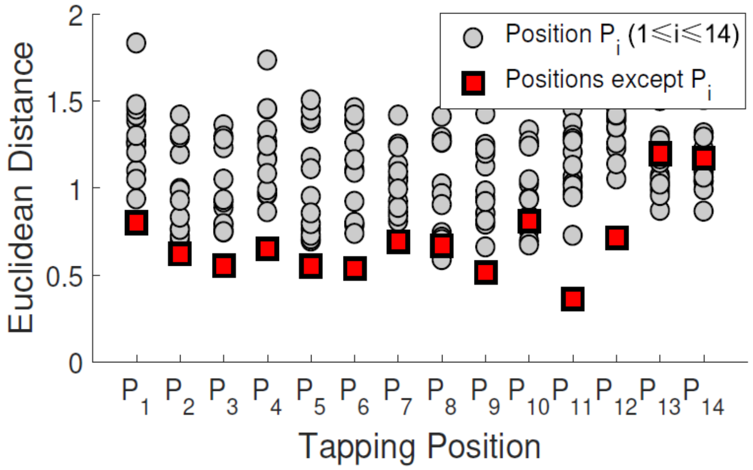
The tapping force is an interference factor that needs to be resolved

Challenge

How to distinguish legal users from illegal ones under the variance of tapping force?

Preliminary——Exp4 （What about the situation when the tapping positions change?）

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



Observation

The Euclidean distance is different when the distance from finger tapped position to sensor varies.

System Overview

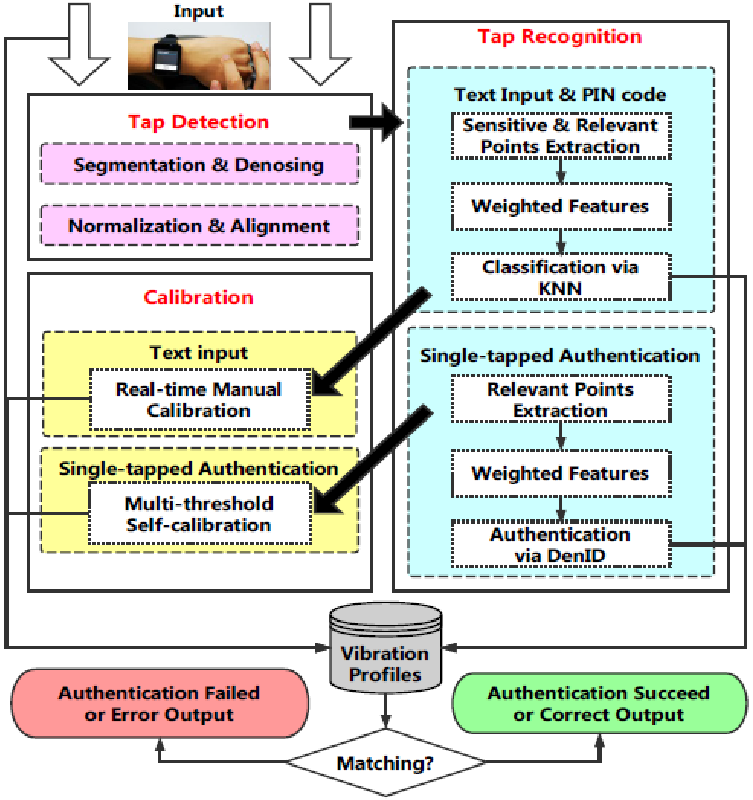


Figure 5: The workflow of Taprint.

Threat Model

Zero-effort Attack.
The attacker attempts to find a potential tapping location that can generate similar vibration signals to bypass the authentication, by tapping randomly without knowing either the PIN code or the location of the single-tap lock.

Credential-aware Attack.
The attacker obtains the legitimate user's credentials, including the PIN code and the location of the single-tap lock. However, attacker does not know the behaviors of the legitimate user such as tapping force, tapping angle, gesture, contact duration.

Observer Attack.
The attacker possesses the prior knowledge of legitimate user's PIN code and the location of singletap lock, and tries to imitate the behavior of the legitimate user based on stealthy observations via shoulder surfing or camera recording.

Intimate Attack.
The attacker, who may have an intimate relationship with the legitimate user, acquires knowledge of the legitimate user's PIN code and the location of the single-tap lock. The attacker attempts to pass the authentication by tapping on the legitimate user's hand when she is unaware of it (e.g., during sleeping).

Detection

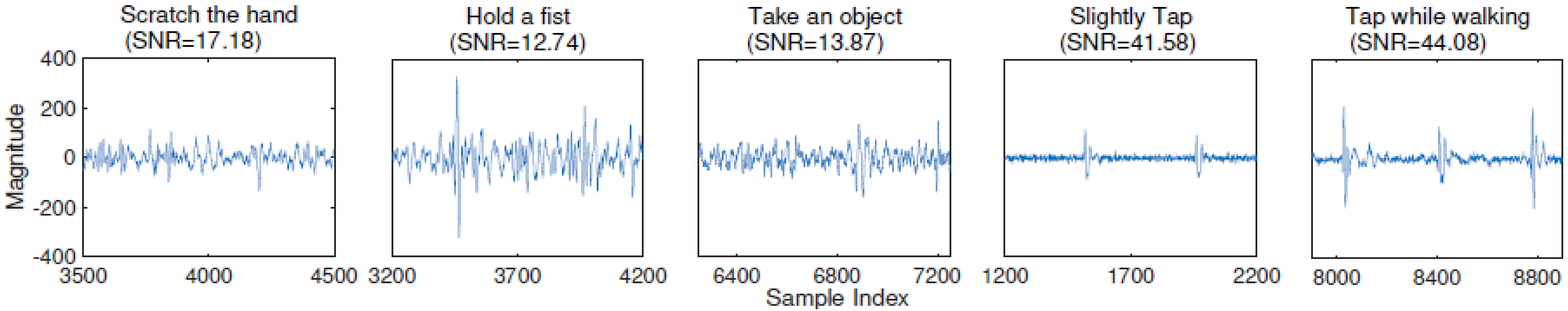


Figure 6: Comparison of SNR resultant from five different actions with a 20 Hz highpass filter.

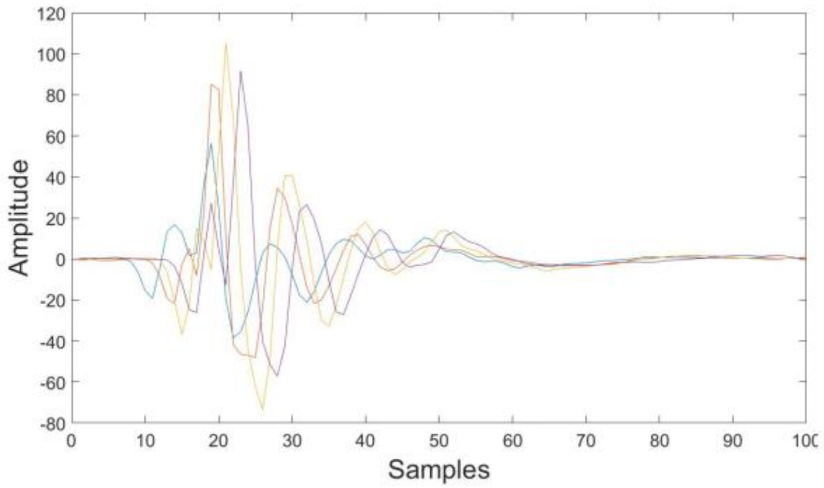
Energy-based detection start point

$$E(t) = \sum_{i=t}^{t+L} s^2(i)$$

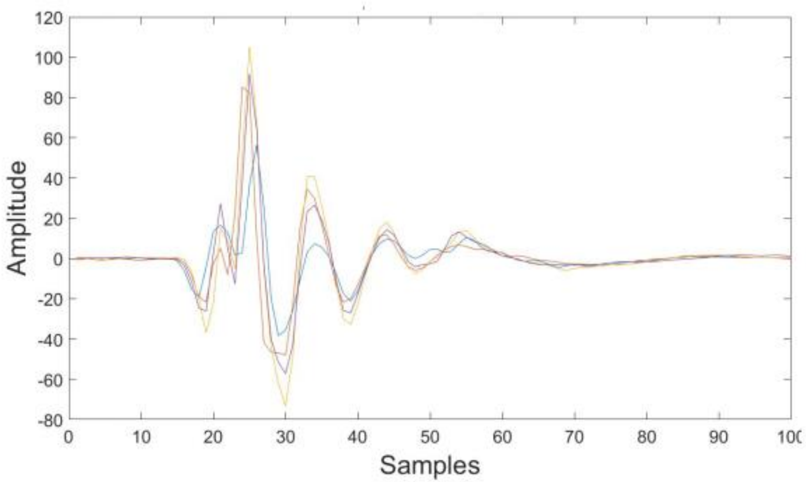
L: the length of the sliding time window

s(i): the amplitude of the received vibration signals

Detection



Before GCC aligning



After GCC aligning

Feature extraction

Pin-code Unlock

- Fisher score

$$F_r = \frac{\sum_{i=1}^{c} n_i (u_i - u)^2}{\sum_{i=1}^{c} n_i \delta_i^2}$$

r : the i-th dimension of feature
n_i : the number of samples of i-th class
u_i : the mean value of i-th class
δ_i^2 : the variance of i-th class
u : the mean value of all class

Single-touched Unlock

- Designed Weight

$$w = \frac{\max(E(X_i)) - E(X_i)}{\sum(\max(E(X_i)) - E(X_i))}$$

E(·) : variance

Feature extraction

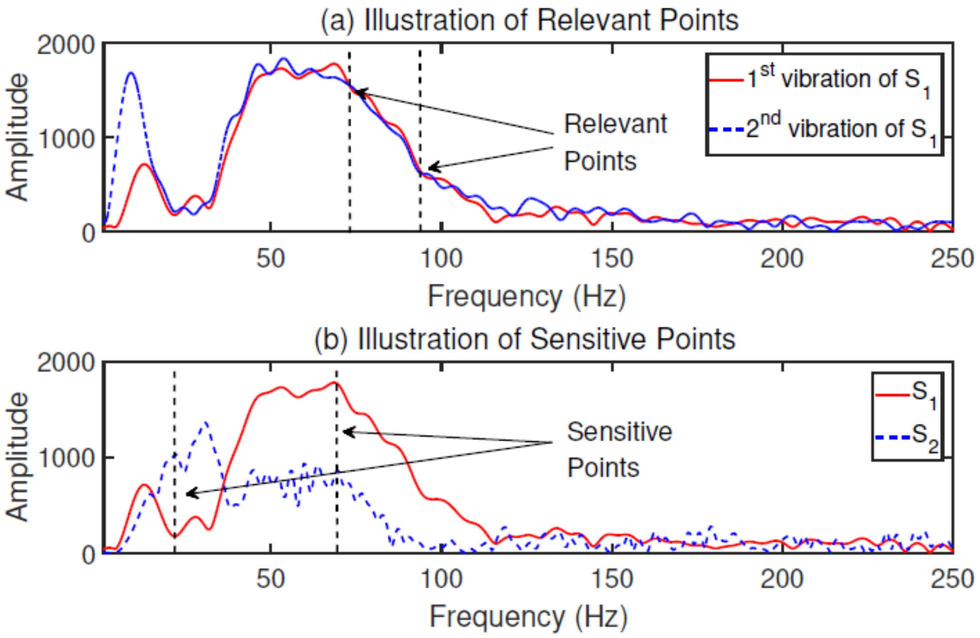


Figure 7: Illustration of relevant and sensitive points. The dotted black line shows the example points.

Single-touched Unlock

- Designed Weight

$$w = \frac{\max(E(X_i)) - E(X_i)}{\sum(\max(E(X_i)) - E(X_i))}$$

E(·) : variance

Calibration

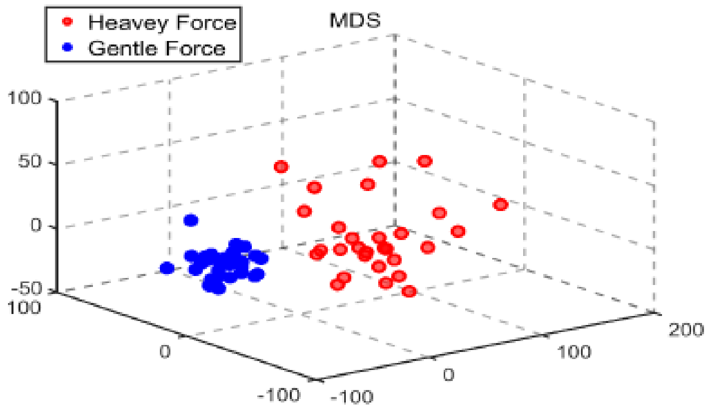


Figure 8: Illustration of sample distribution of different tap strength using the MDS technique.

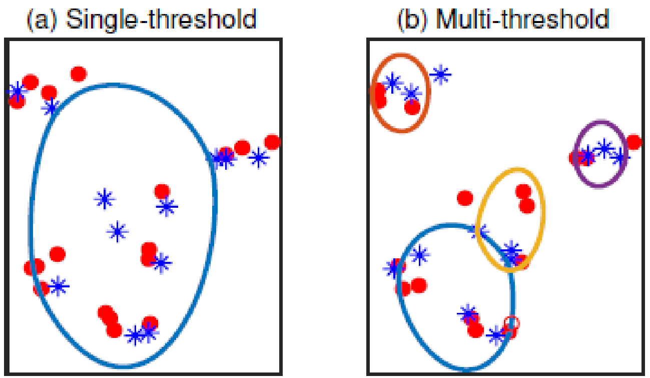


Figure 9: Sample result of the multi-threshold calibration mechanism.

$$P_i = \arg\min_{P_i \in \complement_u R} D_{iR}$$

$$D_{iR} = \min d_{ij}$$

R: visited set

P_i: next sample

D_{iR} : the distance between P_i and R.

Evaluation Setup

- Recruited 128 participants (43 of them are female)
- Age range between [19, 26].
- body mass indexes (BMIs) are ranging from 17.16 (lean) to 29.28 (obese)
- 113 × 4 × 30 + 30 × 12 × 30=24360 samples in total

Evaluation Metric

PIN-code Authentication

Verification Success Rate（VSR）： the success rate of inputting a complete PIN sequence by a legitimate user

Attack Failure Rate（AFR）： the success rate of inputting a complete PIN sequence by a legitimate user

Single-tap Authentication

FAR： the ratio between the number of falsely accepted attacker samples and the total number of attacker test samples

FRR： the ratio between the number of falsely rejected legitimate samples and the total number of legitimate test samples

EER： equal-error rate, where the FAR is equal to the FRR

Evaluation——Accuracy——Baseline

	K1	K2	K3	K4	K5	K6	K7	K8	K9	K10	K11	K12
K1	0.91	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
K2	0.00	0.97	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
K3	0.00	0.00	0.94	0.00	0.00	0.01	0.00	0.01	0.01	0.00	0.00	0.01
K4	0.00	0.00	0.00	0.97	0.00	0.00	0.00	0.00	0.01	0.00	0.00	0.00
K5	0.00	0.00	0.00	0.00	0.97	0.00	0.00	0.00	0.00	0.00	0.00	0.00
K6	0.00	0.00	0.03	0.00	0.00	0.97	0.00	0.00	0.00	0.00	0.00	0.00
K7	0.00	0.00	0.00	0.00	0.00	0.00	0.95	0.00	0.00	0.00	0.00	0.00
K8	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.91	0.02	0.00	0.01	0.00
K9	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.01	0.96	0.00	0.01	0.01
K10	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.99	0.00	0.00
K11	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.98	0.00
K12	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.01	0.00	0.03	0.95

(a)

	K1	K2	K3	K4	K5	K6	K7	K8	K9	K10	K11	K12
K1'	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
K2'	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
K3'	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
K4'	0.00	0.00	0.00	0.10	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
K5'	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.01	0.00	0.00	0.00
K6'	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.01
K7'	0.00	0.00	0.00	0.27	0.00	0.00	0.00	0.00	0.20	0.00	0.01	0.01
K8'	0.00	0.00	0.00	0.01	0.00	0.00	0.00	0.00	0.17	0.00	0.00	0.01
K9'	0.00	0.00	0.00	0.04	0.03	0.00	0.00	0.00	0.14	0.00	0.01	0.00
K10'	0.00	0.00	0.00	0.05	0.00	0.00	0.00	0.01	0.42	0.00	0.01	0.00
K11'	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.05	0.00	0.00	0.05
K12'	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.21	0.00	0.00	0.05

(b)

Figure 10: Confusion matrix of 12 keys, where (a) both the training and test samples are from the legitimate users (b) the training samples are from the legitimate users while the test samples are from the attackers.

Taprint obtains an average accuracy of **95.64%** for twelve keys

Evaluation——Accuracy——Verification

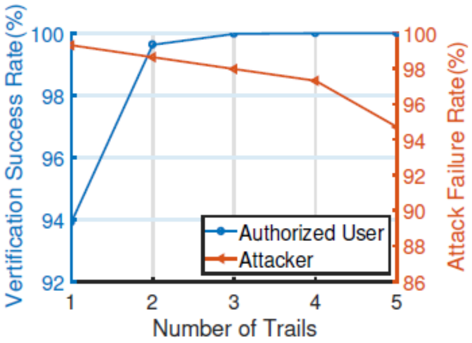


Figure 11: The VSR and AFR with multiple trials.

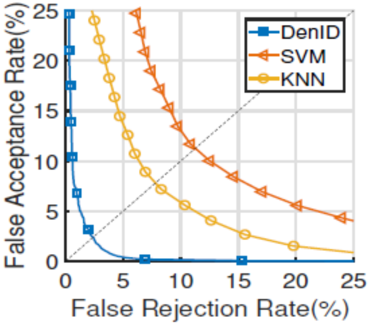


Figure 12: Sample ROC curves of single-tap authentication.

- The VSR reaches **94%** with a single trial, rises to around **99.5%** with two trials
- The EER is **2.4%** for single-tap authentication with 113 subjects

Evaluation——Accuracy——Effectiveness of Techniques

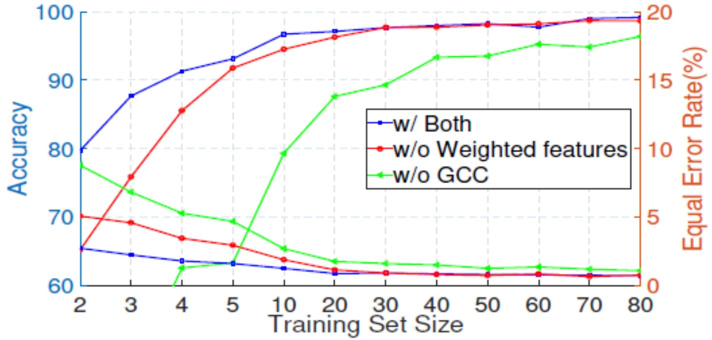
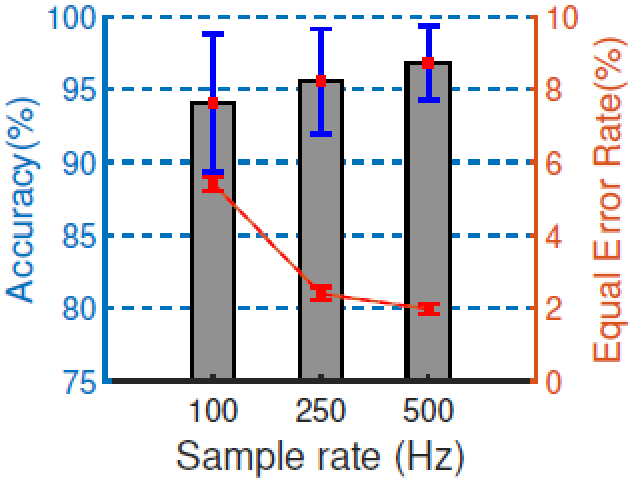


Figure 13: Impact of initial training set size.



Weighted features, GCC, Modfication of Kernel

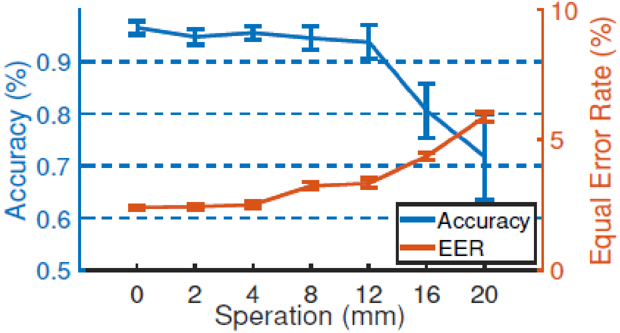
Evaluation——Security

Table 1: EER(%) and AFR(%) of four threat models with 20-sample training

Type of Attack	EER	AFR (1 trial)	AFR (5 trials)
Zero-effort Attack	0.80	99.92	99.60
Credential-aware Attack	2.40	99.65	98.27
Observer Attack	1.12	99.72	98.60
Intimate Attack	1.74	99.32	96.65

Evaluation——Robustness

- Strength of Tap
- Resilience to Dispalcement
- Arm Rotation
- User State
  - Mobility
  - Hand-wash
- Different Environment(noisy office, subway, airplane)
- Temporal Stability



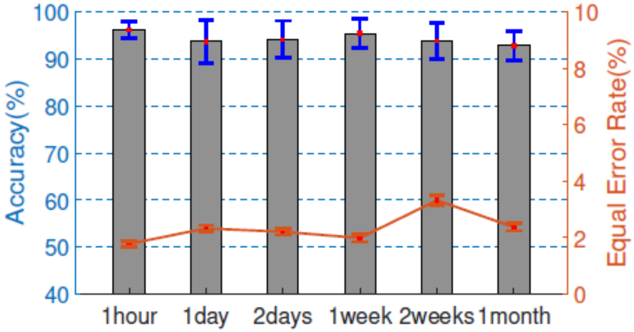


Table 2: Accuracy(%) and EER(%) of different user state & environment with 20-sample training.

Item&	Acc.	EER
Mobility	92.1	4.51
After Hand-wash	97.72	1.65
Quite office (44 dB)	96.43	2.40
Noisy office (85 dB)	97.44	1.76
Subway (65 dB)	96.65	2.47
Airplane (77 dB)	94.73	3.35

User Study

Authentication

Table 3: The average ranking of different authentication method.

Item	1)	2)	3)	4)	Ranking
PIN code	3.8	3	4	3.8	3.65
Password	5	5	5	5	5
Pattern	2.8	3.2	2.8	2.6	2.85
PIN code(Taprint)	2.4	2.8	2.2	2.2	2.4
Single-tap(Taprint)	1	1	1	1.4	1.1

1) the speed of login
2) the easiness to memorize
3) the convenience to perform
4) the difficulty to cause the error

Input

Table 4: The input accuracy, speed and user experience of Taprint and Huawei Watch2

Item	Accuracy	Speed(s)	Score
Taprint	95%	170	4.5
Huawei Watch 2	83%	218	2.2
Tightness	**Comfort**	**Traning accept**	
2.8	4.8	positive	

ticipants response an average tightness degree of 2.8 (1 = loose, 5 = tight) and an average comfort degree of 4.8 (1 = uncomfortable, 5 = comfortable).

Conclusions

- We are the first to propose a novel secure text input system for smart wristbands solely relying on the motion sensors on the commodity smartwatch, without requiring any extra dedicated hardware
- **We have built an on-body tapping induced vibration model and verify its feasibility for secure input. We have proposed a set of novel vibration detection/classification mechanisms to ensure the robustness and temporal stability.**
- We have implemented Taprint as an efficient application running on COTS Android smartwatch and validated its performance through comprehensive examinations under some realistic attack scenarios

Thank You