CSE 410/565: Computer Security

Instructor: Dr. Ziming Zhao

Announcement

- HW1 is due tomorrow
- HW2 will be released today

Biometric Authentication

- Biometric authentication systems authenticate an individual based her physical characteristic
- Types of biometric used in authentication
  - face
  - palm geometry
  - fingerprint
  - Iris
  - Signature
  - Voice
- Most common uses of biometric authentication is for specific applications rather than computer authentication

Biometric Authentication

- Like other authentication mechanisms, biometric authentication includes an enrollment phase during which a biometric is captured
  - the initial reading is often called a template
  - at authentication time, a new biometric reading is performed and is compared to the stored template
- Unlike other authentication mechanisms, biometric matching is approximate
  - each reading can be influenced by a variety of factors
    - e.g., light conditions, facial expressions, hair style, glasses, etc. for face recognition
  - some types of biometrics can match more accurately than others
    - e.g., iris vs. face or palm

Biometric Authentication

- Biometric matching can be used to perform
    - verification
        - user’s biometric scan is used to match her own template only
    - identification
        - user’s biometric scan is used to match a database of templates
- Identification might not always be possible
- Biometric systems attempt to minimize
        - false reject rate: authentic biometric is rejected
        - false accept rate: imposter biometric is accepted
- Depending on the environment, minimizing one of them might be more important than minimizing both

Biometric Authentication

- New types of biometrics are being explored
  - brain waves, heart beats, etc.
- Many forms of traditional biometrics can be stolen
- Static biometrics can be replayed

Biometric Authentication

- Current research direction: biometric key generation
  - the idea: a biometric can be used to generate a cryptographic key
  - the key can be reproduced using another biometric close enough to the original
    - no need to remember any information such as a password
  - the key can be used for authentication or encryption
  - key generation algorithm produces a helper data that can later aid in recovering the same key from a noisy version of the biometric
  - security requirements are strict
    - the helper data must leak minimal information about the biometric
    - compromise of the key must not lead to recovery of the biometric

Summary

- Entity authentication is an important topic with the main application in access control
- Various techniques exist ranging from time-invariant passwords to provably secure identification schemes
- Despite the weak security password-base authentication provides, it is the most widely used authentication mechanism
  - ease of use, user familiarity, no infrastructure requirements
- Next time
  - access control mechanisms

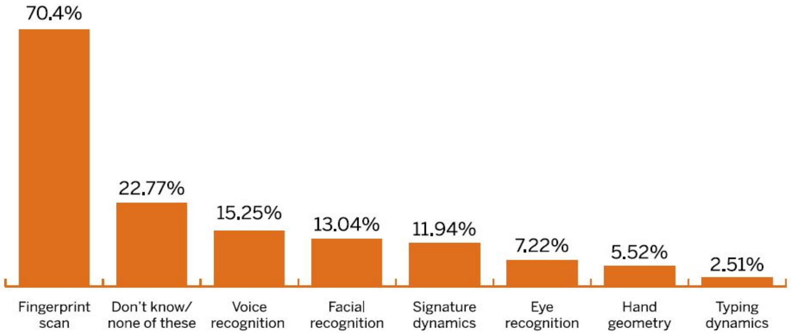
Liveness is Not Enough: Enhancing Fingerprint Authentication with Behavioral Biometrics to Defeat Puppet Attacks

Cong Wu, Kun He, Jing Chen, Ziming Zhao, Ruiying Du

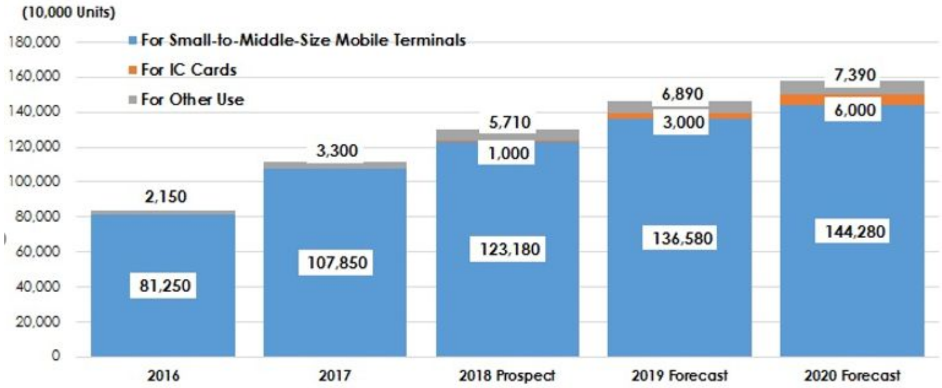
USENIX Security' 20

The Prevailing Fingerprint Authentication

PHOTO: https://www.fingerprints.com/



German, R. L., & Barber, K. S. (2018). Consumer attitudes about biometric authentication. *The University of Texas at Austin.*



Report: Yano Research Institute Ltd.

Attacks on Fingerprint Authentication

ICS › 35 › 35.240 › 35.240.15

ISO/IEC 30107-1:2016

Information technology — Biometric presentation attack detection — Part 1: Framework

Author:
Lindsey O'Donnell

April 8, 2020 / 9:00 am

15:30 minute read

Write a comment

Share this article:

New research used 3D printing technology to bypass fingerprint scanners, and tested it against Apple, Samsung and Microsoft mobile products.

New research has found that it's possible to use 3D printing technology to create "fake fingerprints" that can bypass most fingerprint scanners used by popular devices. But, creating the attack remains costly and time-consuming.

Researchers with Cisco Talos created different threat models that use 3D printing technology, and then tested them on mobile devices (including the iPhone 8 and Samsung S10), laptops (including the Samsung Note 9, Lenovo Yoga and HP Pavilion X360) and smart devices (such as a smart padlock).

ACM NEWS

Attackers Can Bypass Fingerprint Authentication with an ~80% Success Rate

By Ars Technica
April 8, 2020
Comments

VIEW AS: SHARE:

For decades, the use of fingerprints to authenticate users to computers, networks, and restricted areas was mostly limited to large and well-resourced organizations that used specialized and expensive equipment. That all changed in 2013 when Apple introduced TouchID. Within a few years, fingerprint-based validation became available to the masses as computer, phone, and lock manufacturers added sensors that gave users an alternative to passwords when unlocking the devices.

Although hackers managed to defeat TouchID with a fake fingerprint less than 48 hours after the technology was rolled out in the iPhone 5, fingerprint-based authentication over the past few years has become much harder to defeat. Today, fingerprints

Puppet Attack

Police 'visit funeral home to unlock dead man's phone'

23 April 2018

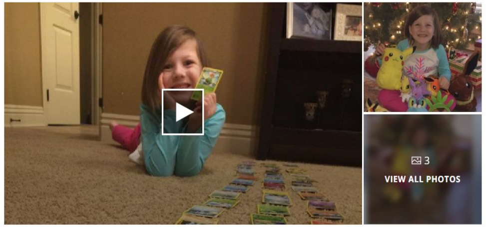
Share

Police in Florida have been criticised for allegedly entering a funeral home in a futile bid to unlock a dead man's smartphone.

6-year-old uses sleeping mom's thumb to go on Amazon shopping spree

by WKRC | Wednesday, December 28th 2016

AA



6-year-old uses sleeping mom's thumb to go on Amazon shopping spree (Provided by/used with permission: Bethany Johnson Howell)

I got drunk last night and got robbed because I was using Touch ID :-(

IaDouche | December 2014 | edited December 2014

hi guys,

not looking to blame anyone but thought i'd share my tale of sorrow here...

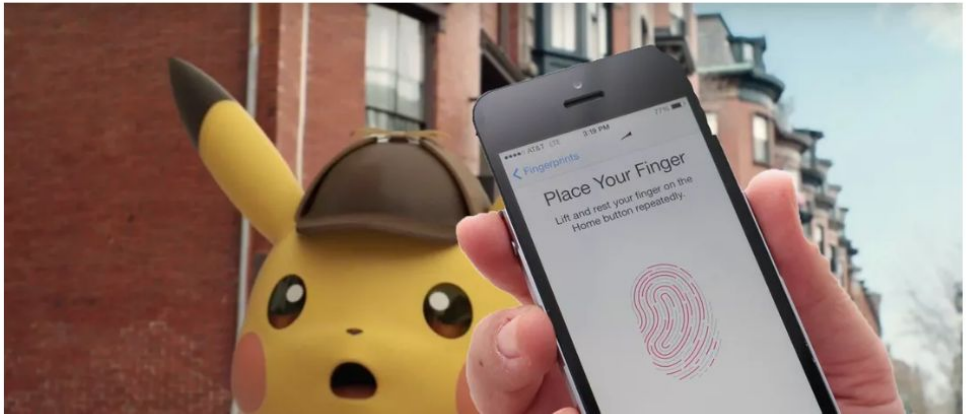
long story short, i was at a party last night and i passed out after some heavy drinking. i woke up this morning and walked to an atm machine wanting to get some cash out for a cab. to my amazement, the transaction was declined. so i whipped out my shiny new iphone 6, fired up 1password, placed my thumb for the touchid, and logged in to my online banking website.

Child uses sleeping mom's fingerprints to buy Pokemon gifts

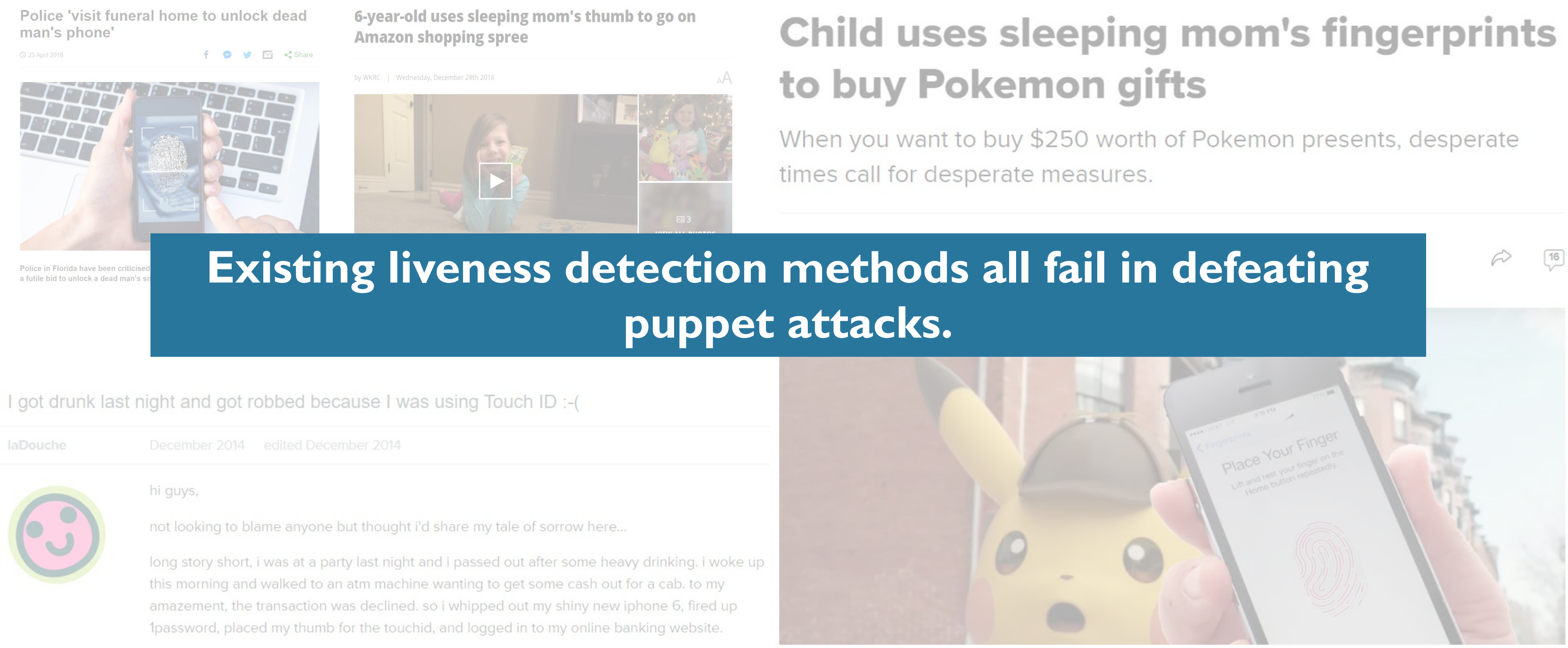
When you want to buy $250 worth of Pokemon presents, desperate times call for desperate measures.

Alfred Ng | Dec. 27, 2016 6:25 a.m. PT

16



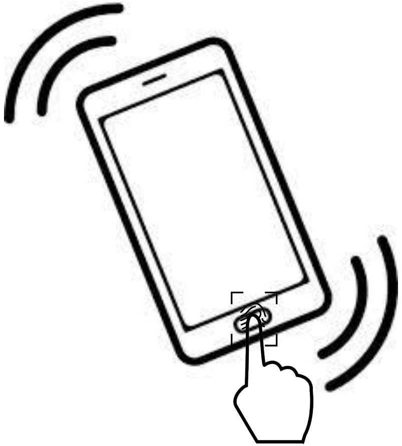
Puppet Attack



Existing liveness detection methods all fail in defeating puppet attacks.

Our Approach

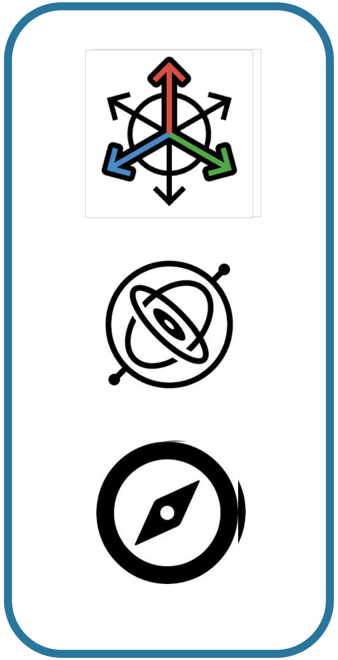
Fingerprint



Fingertip-touch behavior

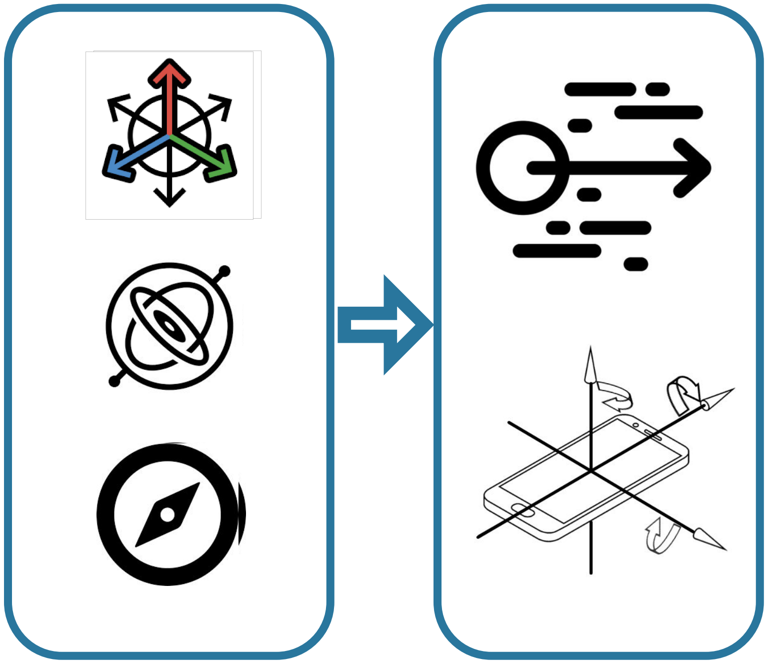
Complement fingerprint authentication with fingertip-touch behavioral characteristics

System Overview



Data capture

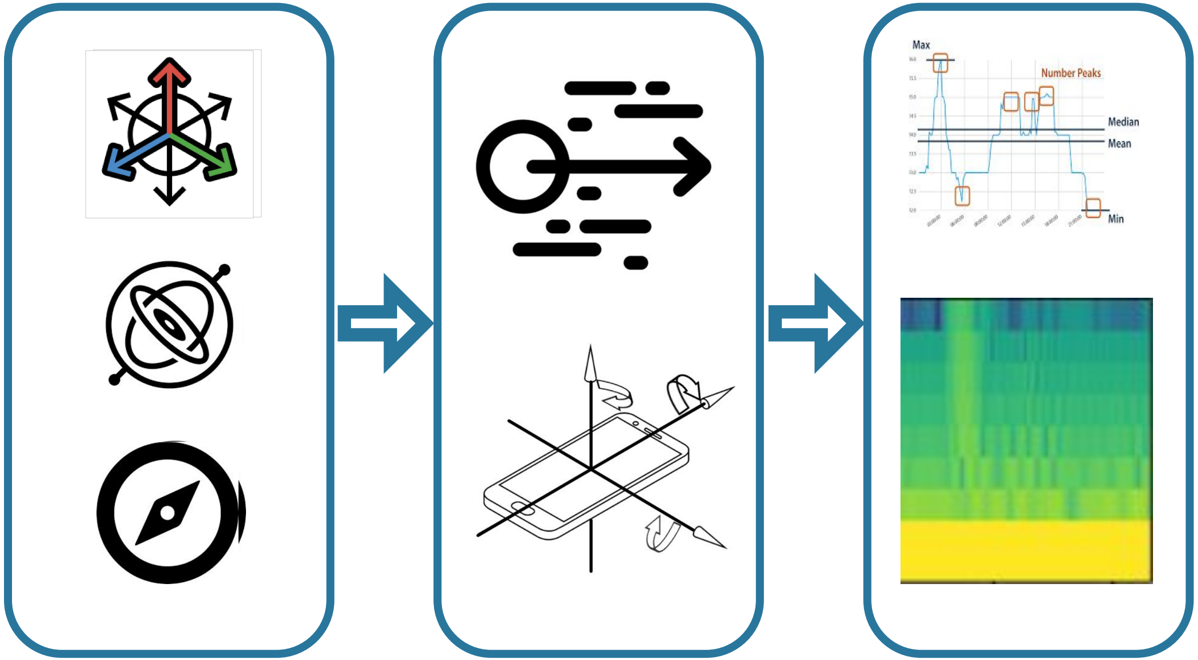
System Overview



Data capture

Behavior characterizing

System Overview

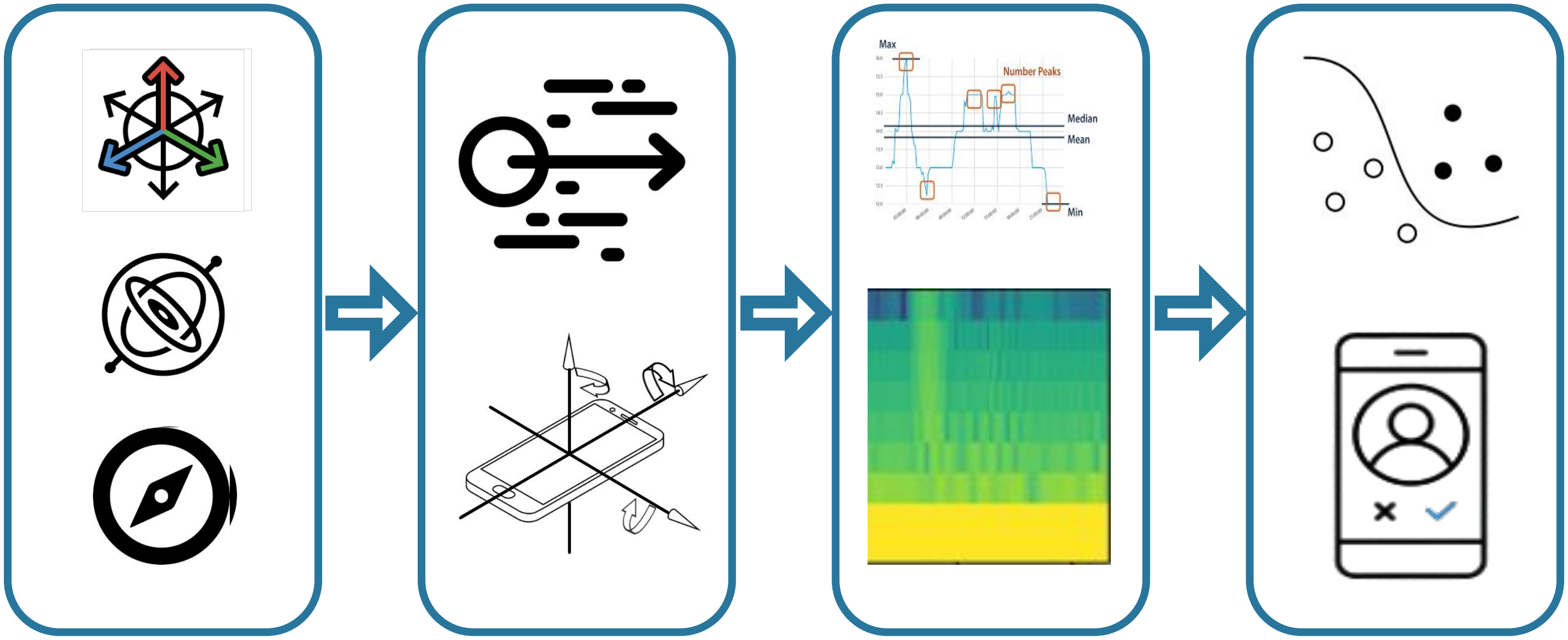


Data capture

Behavior characterizing

Feature extraction

System Overview



Data capture

Behavior characterizing

Feature extraction

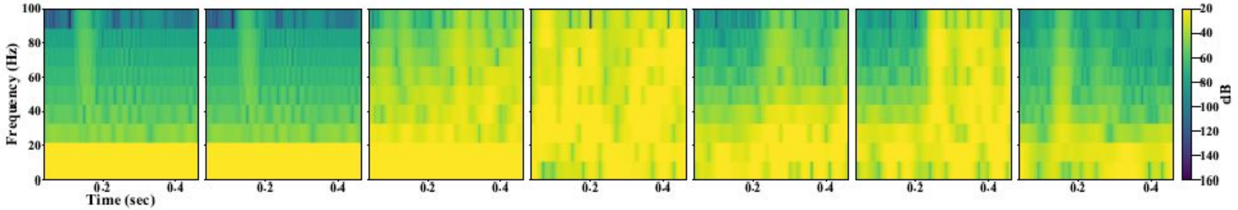
Model training /Authentication

Time- and Frequency- Domain Features (TFF)

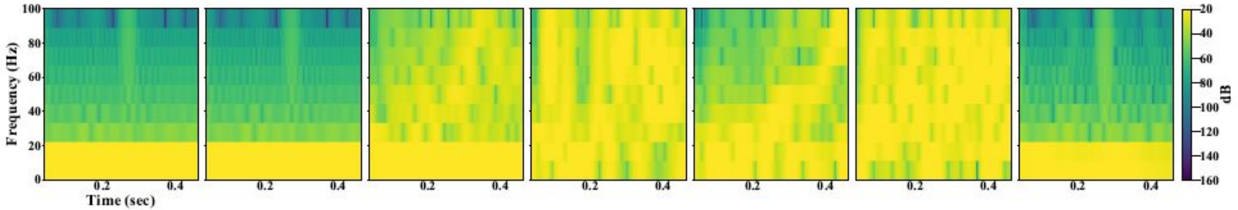
Table 1: Time- and frequency-domain features and their normalized fisher's scores.

Domain	Feature	Description	Normalized Fisher Score of $(\boldsymbol{a}_x, \boldsymbol{a}_y, \boldsymbol{a}_z, \boldsymbol{a}', \boldsymbol{\phi}, \boldsymbol{\theta}, \boldsymbol{\psi})$
Time	Mean	The mean of the time series.	(0.45, 0.01, 0.22, **0.68**, **0.86**, **0.84**, **0.84**)
	Standard deviation	The standard deviation of the time series.	(0.24, 0.56, 0.31, 0.41, 0.58, 0.32, **0.74**)
	Relative standard deviation	The extent of variability in relation to its mean.	(0.34, 0.15, 0.12, 0.56, **0.71**, **0.64**, **0.82**)
	Sum of absolute differences	The sum over the absolute value of consecutive changes in the time series.	(0.32, 0.27, **0.72**, 0.52, 0.53, **0.72**, **0.78**)
	Absolute energy	The absolute energy of the time series.	(**0.63**, **0.98**, **0.85**, 0.57, **0.72**, 0.57, 0.37)
	Autocorrelation	The autocorrelation of the time series.	(0.00, 0.14, 0.15, 0.21, **0.94**, **0.62**, **0.64**)
Frequency	Spectral centroid	The center of mass of the spectrum is located.	(0.34, 0.21, 0.38, 0.12, **0.78**, **0.98**, **0.78**)
	Spectral spread	The average spread of the spectrum in relation to its centroid.	(**0.66**, 0.36, 0.32, **0.78**, 0.46, **0.82**, **0.96**)
	Spectral skewness	The measurement of the asymmetry of the probability distribution of a real-valued random variable about its mean.	(**0.85**, 0.45, 0.58, **0.84**, 0.56, **0.85**, **1.00**)
	Spectral kurtosis	The shape of a probability distribution.	(0.34, 0.17, **0.70**, **0.86**, **0.62**, 0.51, 0.42)
	Power spectral density	Average of distribution of power into frequency components.	(**0.90**, **0.71**, **0.86**, 0.26, **0.85**, **0.68**, **0.82**)
	Spectral entropy	The complexity of the signal in the frequency domain.	(**0.94**, 0.32, **0.82**, 0.21, **0.96**, **0.82**, **0.89**)

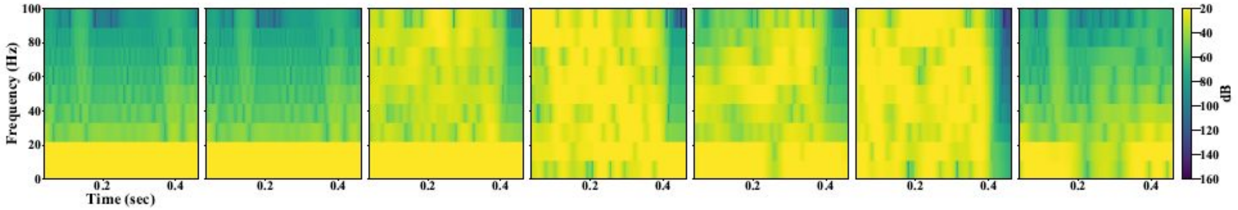
CNN-based Features (CNF)



(a) User A.



(b) User B.



(c) User C.

Figure 3: Characterized fingertip-touch behaviors of three users under STFT. From left to right, spectrograms of $\boldsymbol{a}_x$, $\boldsymbol{a}_y$, $\boldsymbol{a}_z$, $\boldsymbol{a}'$, $\boldsymbol{\theta}$, $\boldsymbol{\phi}$, $\boldsymbol{\psi}$.

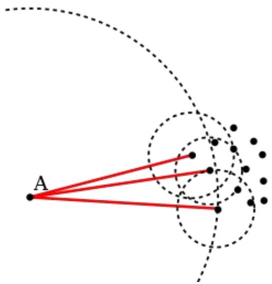
One-class Classifier

$$r_{XY} = \frac{\sum_{i=1}^{n}(X_i - \overline{X})(Y_i - \overline{Y})}{\sqrt{\sum_{i=1}^{n}(X_i - \overline{X})^2}\sqrt{\sum_{i=1}^{n}(Y_i - \overline{Y})^2}}$$

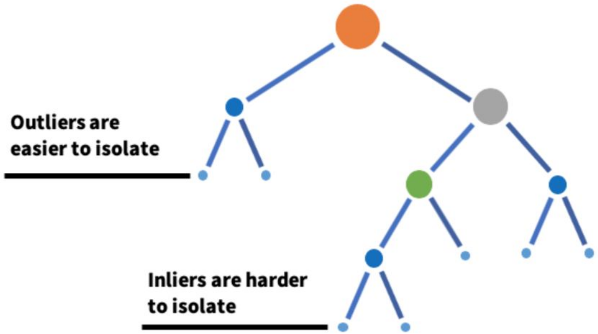
Pearson coefficient-based similarity comparison (PCC)

$$\min_{R,a} R^2 + C\sum_{i=1}^{n}\zeta_i$$
$$s.t. \; ||x_i - a||^2 \leq R^2 + \zeta_i, i = 1, \ldots, n$$
$$\zeta_i \geq 0, i = 1, \ldots, n$$

在此处键入公式。One-class support vector machine (OCSVM)



Local outlier factor (LOF)



Isolation forest (IF)

Data Collection

Table 3: Summary of the compiled datasets

Dataset	Week of Collection	# of Subjects / Attackers	Postures	Device	# of Data Points
1	1 †, 8 and 9 ‡	90	Sitting, standing, lying, walking, running	OnePlus3	63,000
2A	2, 3, 5, 7	24, 24, 22, 21	Sitting	OnePlus3	18,200
2B	10, 11, 12, 13	62, 61, 59, 53			47,000
3	Added Aug. 2019	64	Sitting	Xperia XZ1, Oneplus5, Vivo X21	3,200
4A					3,600
4B	2 †, 10 and 11 ‡	15	Sitting	OnePlus3	3,600
4C					3,600

Datasets

- 90 subjects in the data collection.
- Compiled three datasets in different postures[1], periods[2], and devices[3].
- Compiled one attack dataset[4] by considering three attacks with 15 subjects as adversaries.

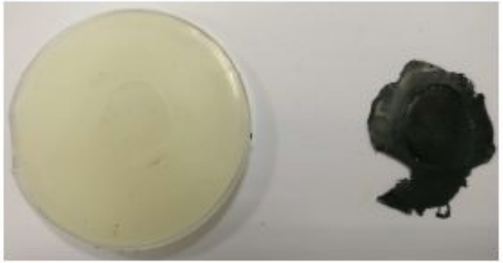
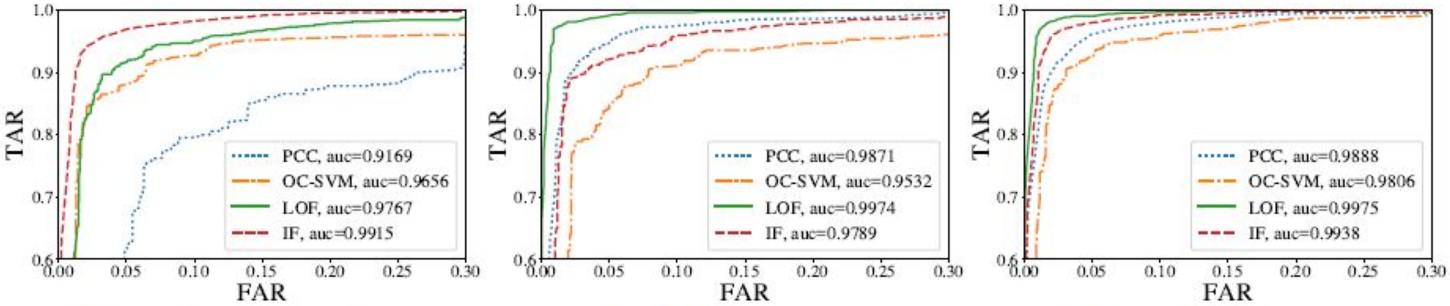


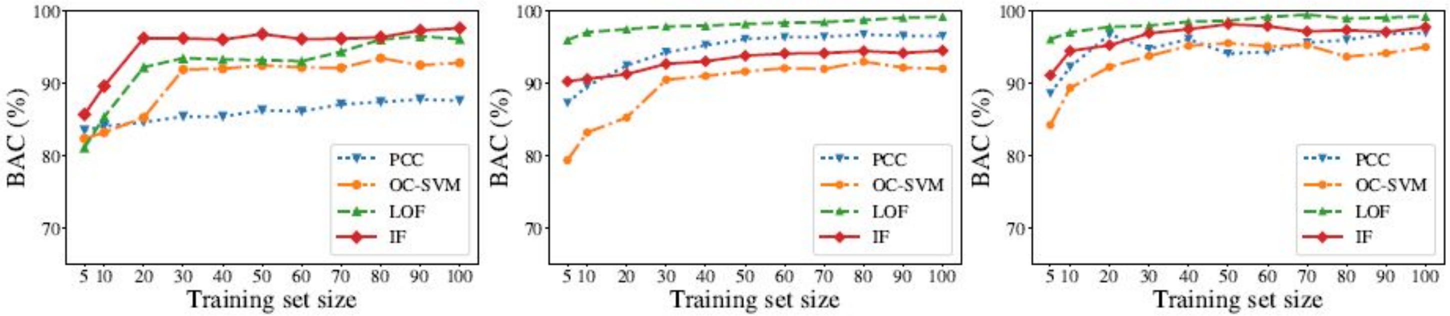
Figure 4: Artificial fingerprint replica. The left is the mold used to capture fingerprint; the right is a fake fingerprint crafted using silicone rubber.

Reliability Evaluation



(a) Time- and frequency-domain features (b) CNN-based features (c) The union of two feature sets

Figure 5: ROC curves of different feature sets under different one-class classifiers.

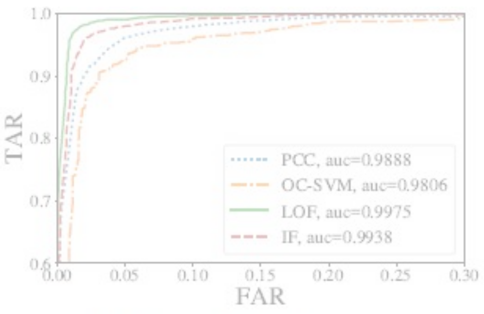


(a) Time- and frequency-domain features (b) CNN-based features (c) The union of two feature sets

Figure 6: BAC under different classifiers and different feature sets at varying training set sizes.

Reliability Evaluation

Feature Set + Classifier	BAC	FAR	FRR	AUC
TFF + PCC	84.41	11.85	19.34	0.9169
TFF + OC-SVM	91.49	5.56	11.45	0.9656
TFF + LOF	93.28	4.32	9.13	0.9767
TFF + IF	96.07	2.51	5.35	0.9915
CNF + PCC	94.65	3.30	7.40	0.9871
CNF + OC-SVM	90.69	6.41	12.21	0.9532
CNF + LOF	97.99	0.86	3.16	0.9974
CNF + IF	93.63	3.72	9.06	0.9789
UnF + PCC	94.76	2.86	7.62	0.9888
UnF + OC-SVM	93.78	4.06	8.37	0.9806
UnF + LOF	98.02	1.52	2.43	0.9975
UnF + IF	96.88	2.03	4.21	0.9938



(c) The union of two feature sets

different one-class classifiers.

Finding: CNF+LOF achieves almost the best performance with the lowest FAR.

Training set size

(a) Time- and frequency-domain features

Training set size

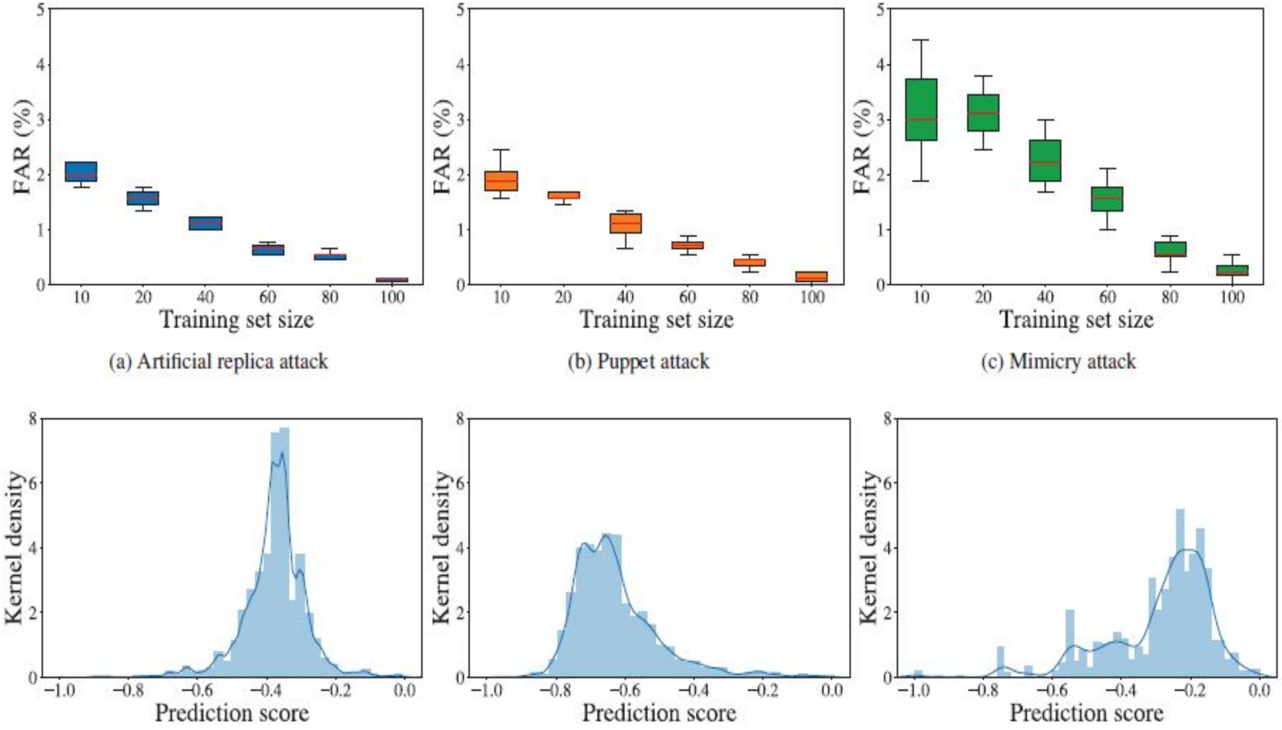
(b) CNN-based features

Training set size

(c) The union of two feature sets

Figure 6: BAC under different classifiers and different feature sets at varying training set sizes.

Evaluation of Presentation Attacks



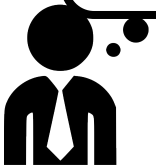
FAR and kernel density of prediction score under attacks

Mean/standard deviation of FAR and prediction score

Attack	FAR	Score
ARA	0.08/0.06	-0.29/0.15
PA	0.12/0.08	-0.62/0.13
MA	0.25/0.14	-0.37/0.10

Limitations

Behavior variability with time elapsing?



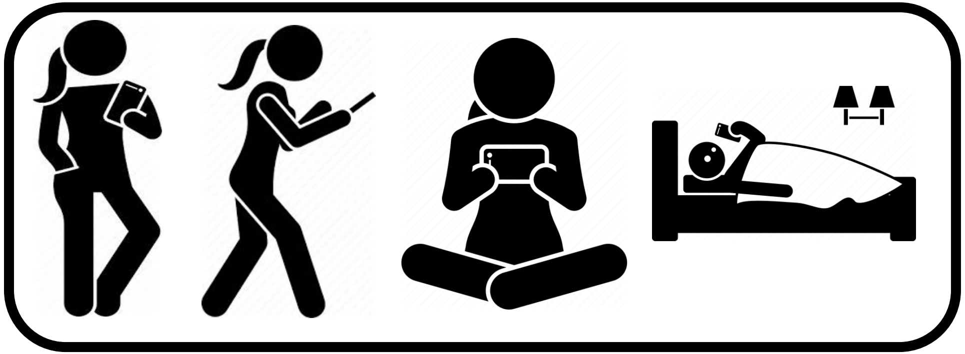
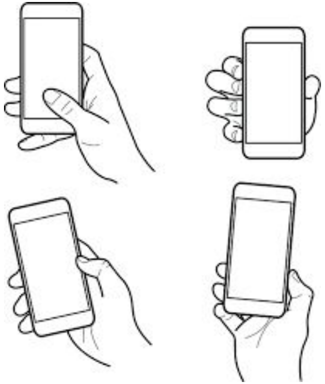
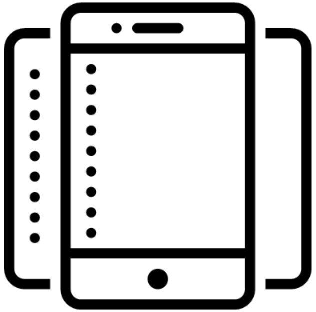


PHOTO: iconfinder.com

PHOTO:
https://parker-marker.com/





EchoHand: High Accuracy and Presentation Attack Resistant Hand Authentication on Commodity Mobile Devices

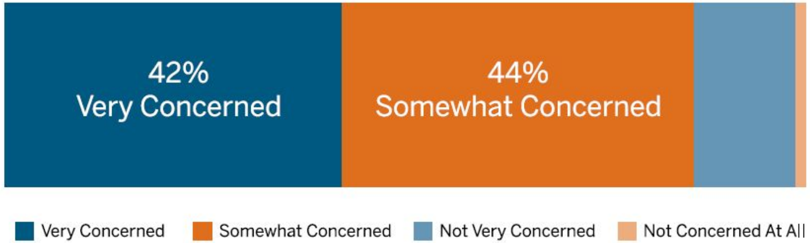
Cong Wu, Jing Chen, Kun He, Ziming Zhao,

Ruiying Du, Chen Zhang

CCS 2022

Promising Hand Authentication

Figure 23. Concerned about Misuse of Personal Information

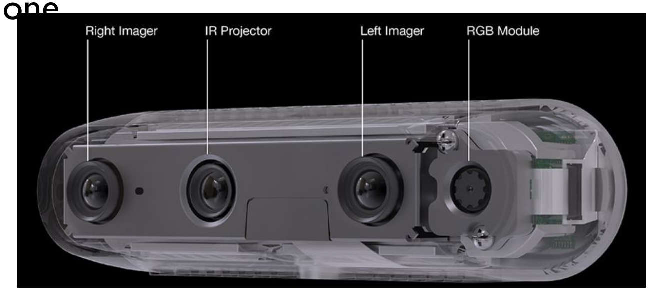


	Very comfortable	Somewhat comfortable	Not very comfortable	Not at all comfortable at all
Eye recognition	34.30%	36.91%	19.56%	9.23%
Fingerprint scan	57.72%	28.36%	9.02%	4.91%
Voice recognition	36.47%	37.68%	17.64%	8.22%
Signature dynamics	38.68%	36.27%	17.94%	7.11%
Typing dynamics	36.07%	35.07%	20.24%	8.62%
Facial recognition	32.83%	36.75%	20.18%	10.24%
Hand geometry	40.42%	36.91%	16.95%	5.72%

[Consumer attitudes about biometric authentication. Technical Report. The University of Texas at Austin Center for Identity. 2018.]

Hand authentication is promising

Amazon one



RealSense depth camera

Relying no dedicated hardware

Existing Hand Authentications

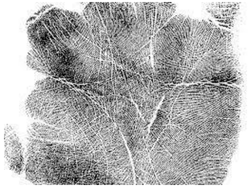
Palm vein, blood flowing pattern of hand

- ❖ Relying on infrared camera.

[PHOTO:thestar]

Palm print, i.e., skin texture of palm region

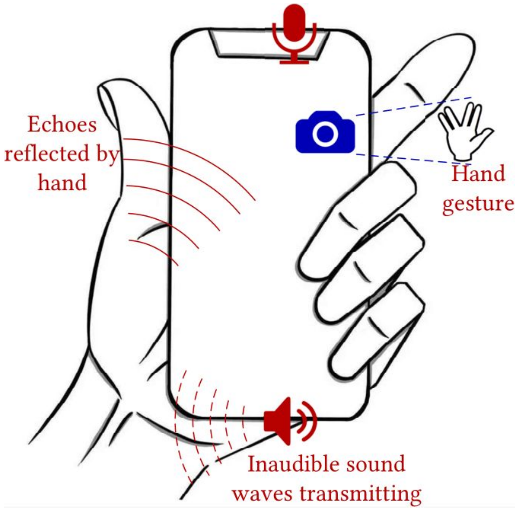
- ❖ Vulnerable to presentation attack.

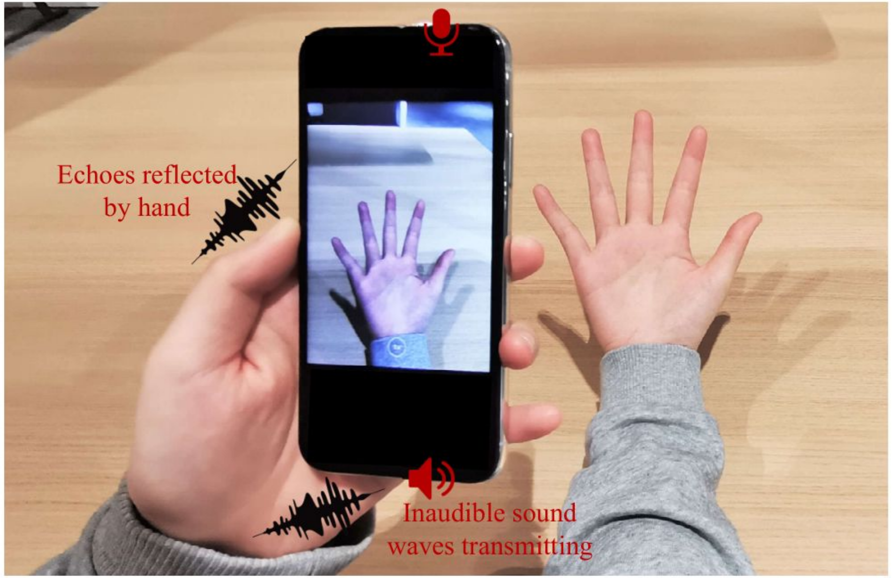


Hand geometry features, e.g., finger length, width, hand shape, size

- ❖ 3D hand geometry authentication rely on dedicated hardware, e.g., depth camera ;
- ❖ 2D hand geometry authentication suffer from presentation attack.

Motivation





Key idea: complement camera-based hand geometry recognition of one hand with active acoustic sensing of the other holding hand.

Acoustic Sensing

Multi-path propagation of acoustic signal

- ❖ Path 1: traveling through the device
- ❖ Path 2: traveling through the air, **reflecting the by the hand holding device**, and direct transmission
- ❖ Path 3: traveling through the air, and reflecting by other surrounding objects

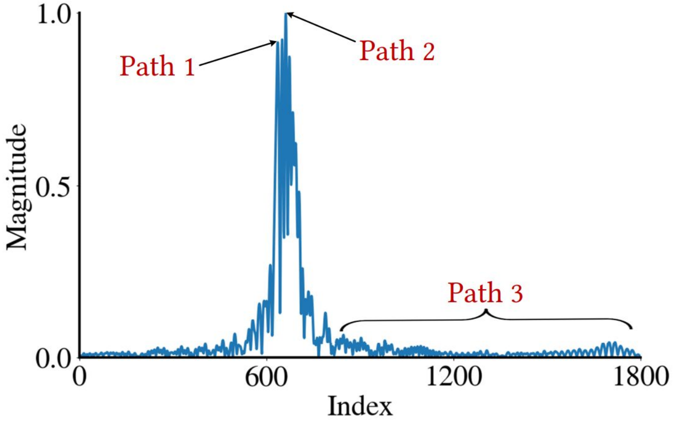


Table 1: Propagation speed, distance, delay, and energy level of different propagation paths

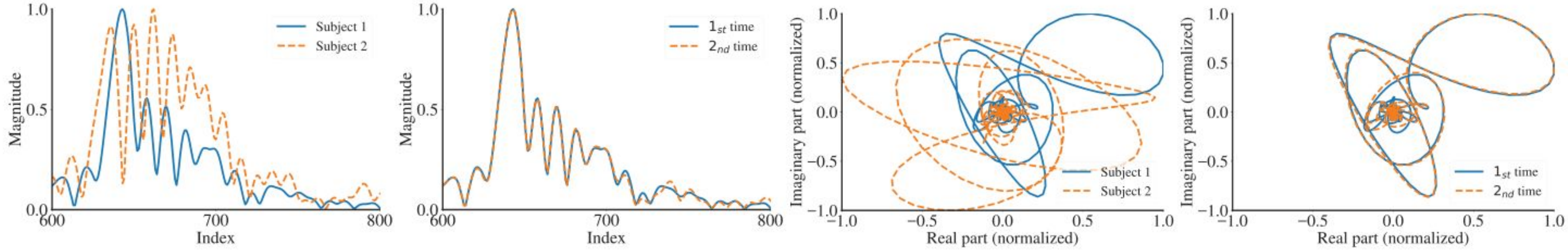
Path	Speed (m/s)	Distance (cm) †	Delay (ms) / Points	Energy
1	>3,000	15.2	0.05/-19	Medium
2	~343	[15.2, 15.2×2]	[0.44/0, 0.89/22]	High
3	~343	[15.2×2, ∞]	[0.87/22, ∞]	Low

†: As an example, we use the distance of Pixel 3A in which the microphone and bottom speaker are 15.2cm apart.

Acoustic Sensing

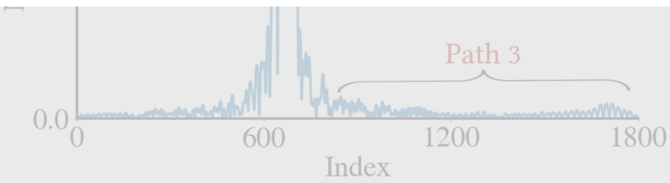
Multi-path propagation of acoustic signal

- Path 1: traveling through the device
- Path 2: traveling through the air, **reflecting the by the hand holding**



(a) Two subjects (b) The same user (c) Two subjects (d) The same user

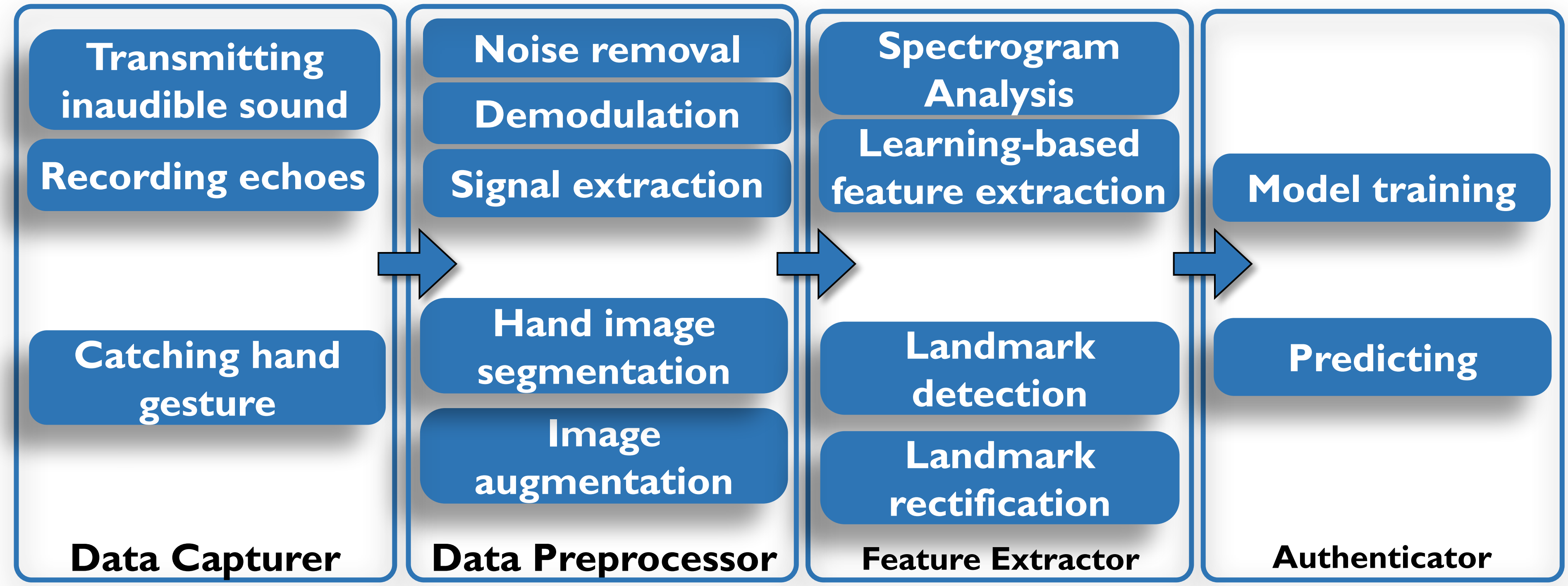
Figure 4: IR estimations using cross-correlation of the received signal and the transmitted signal for two subjects: the magnitude of IR from two subjects (a); the magnitude of IR from the same subject at two times with 48kHz sampling rate (b); trace of the real/imaginary parts from two subjects (c); trace of the real/imaginary parts from the same subject at two times (d)



2	~343	[15.2, 15.2×2]	[0.44/0, 0.89/22]	High
3	~343	[15.2×2, ∞]	[0.87/22, ∞]	Low

†: As an example, we use the distance of Pixel 3A in which the microphone and bottom speaker are 15.2cm apart.

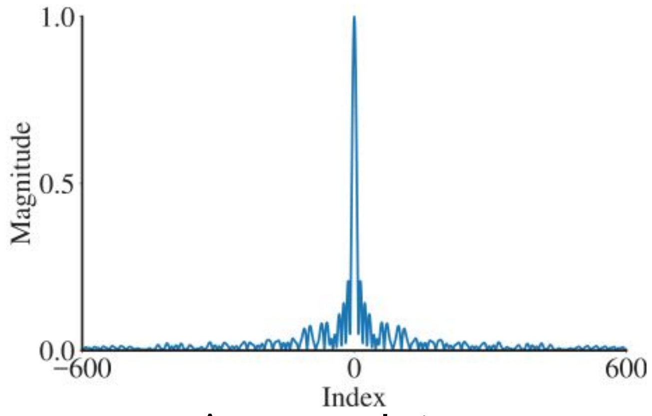
System Overview



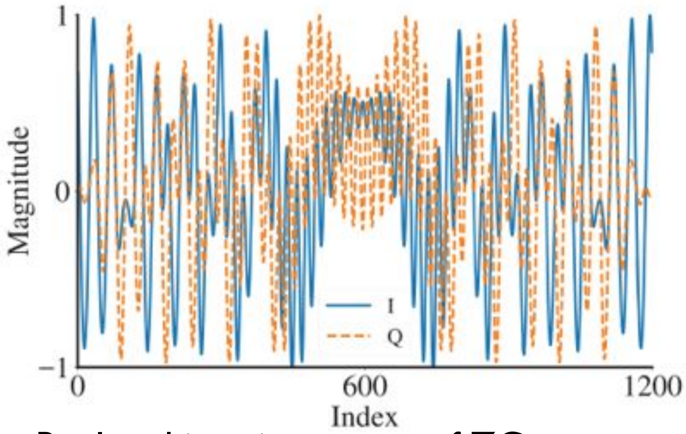
Data Capturer

Acoustic signal transmitting and receiving

- ❖ Select ZC sequence as the base signal.
- ❖ Modulate the signal to a inaudible high-frequency band.
- ❖ Use bottom speaker to play, and top microphone to record echoes.



Auto-correlation



Real and imaginary part of ZC sequence

Data Preprocessor

Acoustic data preprocessing

- ❖ Noise removal and signal demodulation to reconstruct the baseband signal.
- ❖ Extracting the **target signal shaped by the holding hand(Path 2)** based on the **relative energy and delay of different paths.**

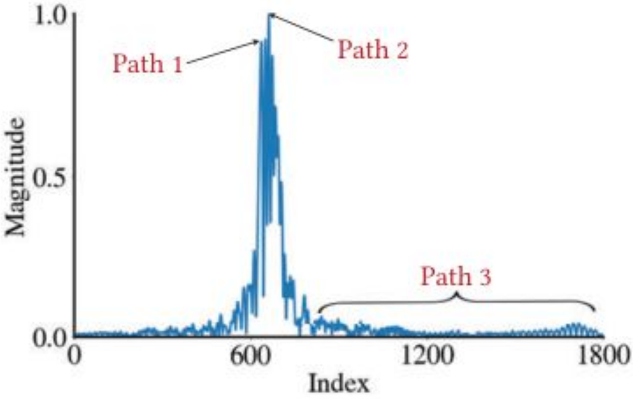


Table 1: Propagation speed, distance, delay, and energy level of different propagation paths

Path	Speed (m/s)	Distance (cm) †	Delay (ms) / Points	Energy
1	>3,000	15.2	0.05/-19	Medium
2	~343	[15.2, 15.2×2]	[0.44/0, 0.89/22]	High
3	~343	[15.2×2, ∞]	[0.87/22, ∞]	Low

†: As an example, we use the distance of Pixel 3A in which the microphone and bottom speaker are 15.2cm apart.

Feature Extractor

Acoustic features

- ❖ Analyze time-frequency spectrogram of magnitude and phase using **continuous wavelet transform**.
- ❖ Learn representative acoustic features using a pretrained network.

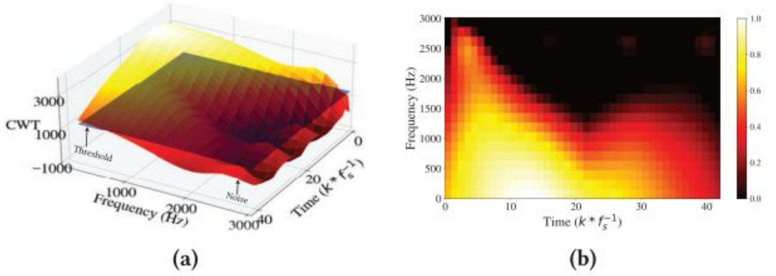
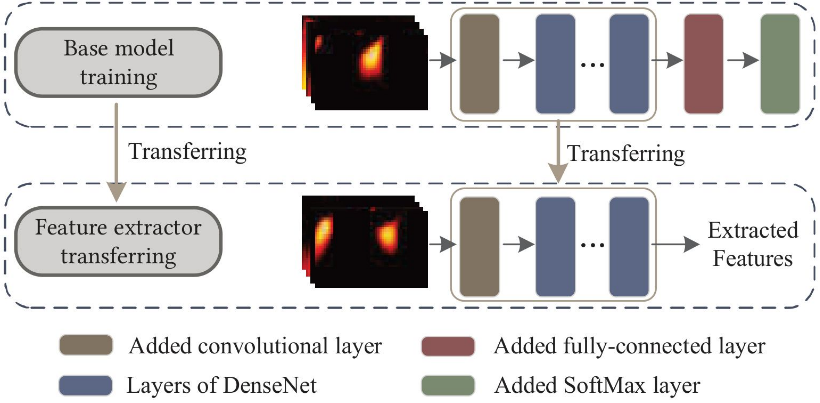


Figure 5: An example CWT result of the magnitude: the raw CWT result (a); the CWT result after applying threshold (b)

Time-frequency spectrogram

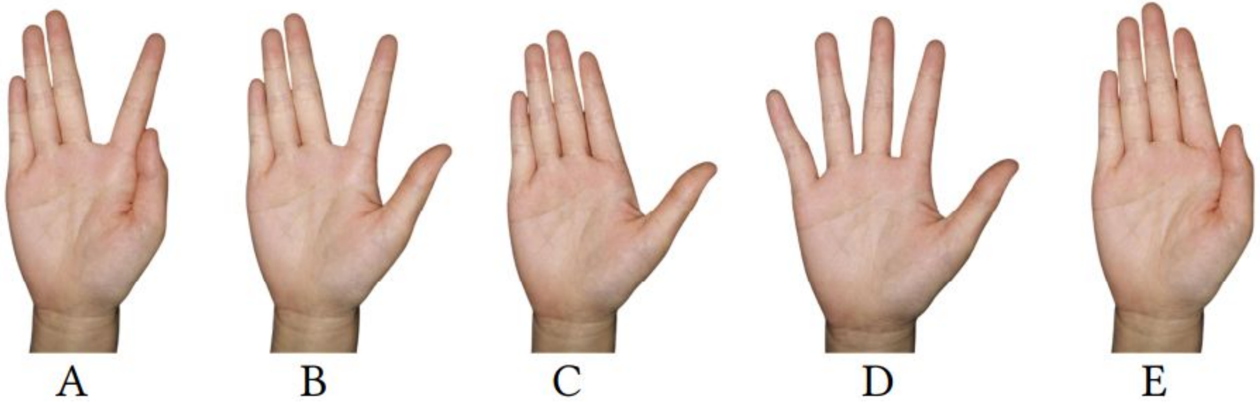


Build the feature extractor

Data Capturer - Hand Gesture

Hand gesture catching

- ❖ The fingers and palm should be approximately in the same plane.
- ❖ The fingers should be straight and not overlap with each other.



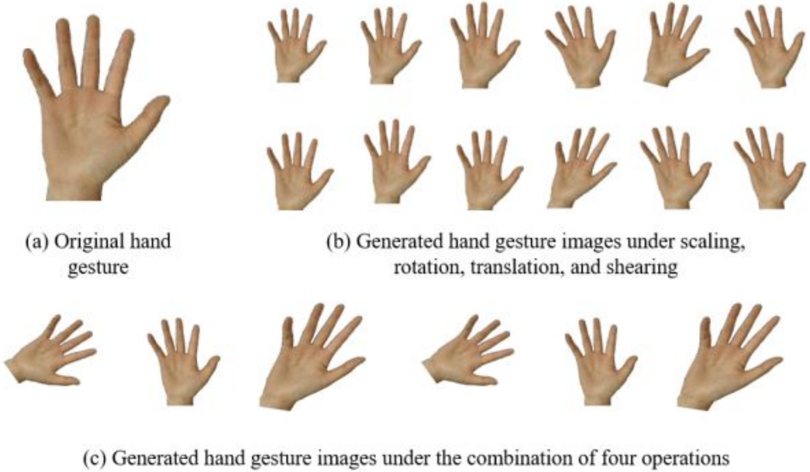
Five example hand gestures in our experiments.

Data Preprocessor - Hand Gesture

Hand gesture image preprocessing

- ❖ Hand segmentation and contour detection, DeepLabv3 model.
- ❖ Hand image augmentation, scaling, rotation, translation, and shearing.

Hand segmentation, and contour detection



Hand image augmentation

Feature Extractor - Hand Gesture

Hand geometry features

- ❖ Hand landmark detection and rectification
- ❖ Hand geometry features representation, e.g., finger length, length, distance palm size.

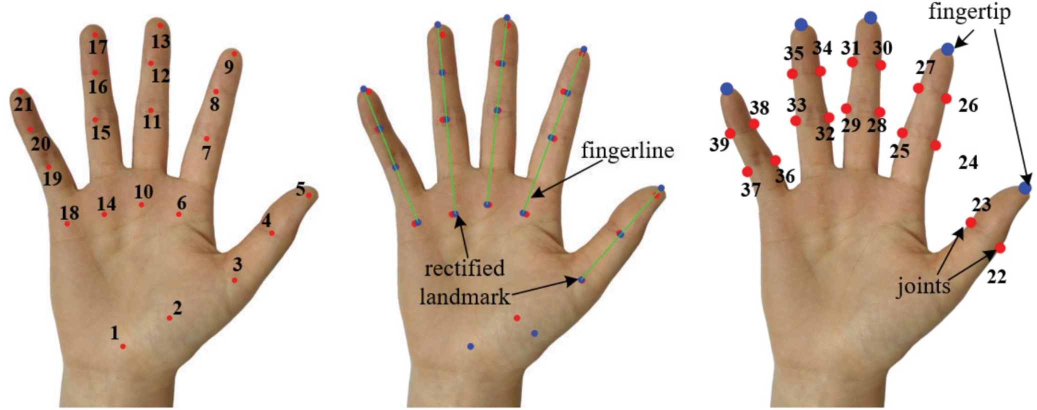
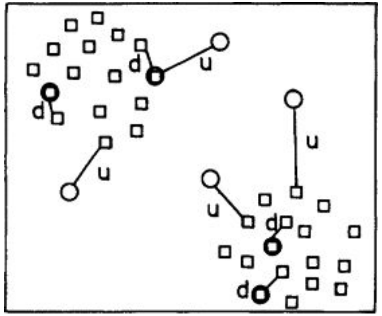


Table 4: List of extracted hand geometry features

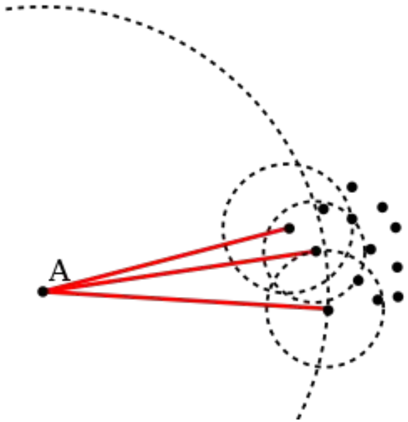
Feature	Description	# Of features
Finger length	Length of each finger, including 3-5, 6-9, 10-13, 14-7, and 18-21	5
Finger width	Distance between pairs of finger joints, including 22-23, 24-25, 26-27, 28-29, 30-31, 32-33, 34-35, 36-37, 38-39	9
Palm size	Area and length of polygons consisting with lines 1-3-6-10-14-18. Distance of 1-3, 1-6, 1-10, 1-14, 1-18	7
Finger distance	Distance between 2 adjacent fingers, including 2-6, 3-7, 4-8, 5-9, 6-10, 7-11, 8-12, 9-13, 10-14, 11-15, 12-16, etc.	16

Authenticator

Only legitimate user's data is available in enrollment: one-class classifier.



Centroid classifier (CC)



Local outlier factor (LOF)

$$\min_{R,a} R^2 + C\sum_{i=1}^{n}\zeta_i$$

$$s.t.\ ||x_i - a||^2 \leq R^2 + \zeta_i, i = 1, \ldots, n$$

$$\zeta_i \geq 0, i = 1, \ldots, n$$

One-class support vector machine (OCSVM)

Evaluation Setup

Implementation

- ❖ Sampling rate, 48kHz.
- ❖ Signal length, 25ms.
- ❖ Frequency band, 17.46-22.54kHz (inaudible band).

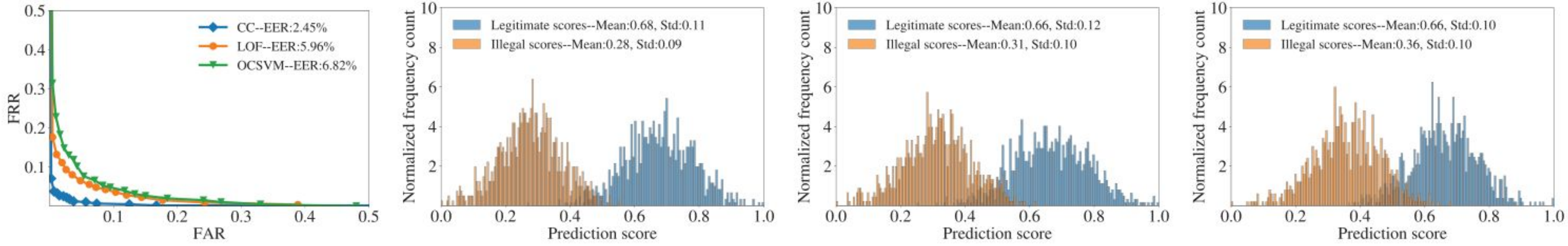
Dataset

- ❖ **30 subjects** in the data collection.
- ❖ Compiled datasets under **different settings and real environments, e.g., low light, audible noise, different devices, periods, and hardware settings.**
- ❖ Compiled the attack dataset by **considering three attacks** with 6 subjects as adversaries.

Metrics

- ❖ False acceptance rate, false rejection rate
- ❖ Equal error rate (EER)
- ❖ Receiver operating characteristics (ROC) curve
- ❖ Area under the ROC curve (AUC)

Reliability Evaluation



(a) ROC curves (b) FCS under CC (c) FCS under LOF (d) FCS under OCSVM

Figure 15: ROC curves (a) and normalized FCS (b, c, d) when using acoustic features to complement hand geometry features

EER under CC, LOF, and OCSVM: 2.45%, 5.96%, and 6.82%

Table 5: The average EERs of gesture A, B, C, D, E (Figure 8)

	Classifier	A	B	C	D	E
W. IA	CC	7.38%	6.90%	7.52%	6.48%	7.70%
	LOF	11.15%	10.88%	11.80%	10.13%	12.15%
	OCSVM	9.31%	8.83%	8.96%	8.85%	9.37%
W/o. IA	CC	6.36%	6.16%	6.38%	6.06%	6.39%
	LOF	6.89%	5.70%	6.05%	5.91%	7.24%
	OCSVM	7.49%	6.97%	8.17%	7.10%	8.78%

Impact Factors Study

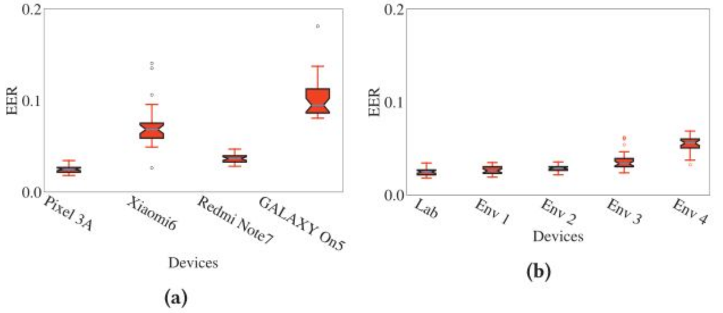


Figure 17: EERs under different devices (a), and environments (b)

EER on Pixel 3A, Xiaomi 6, Redmi Note7, GALAXY On5: 2.45%, 7.24%, 3.69%, and 10.33%.

EER under lab and four real environments: 2.45%, 4.95%, 4.79%, 5.55%, and 6.53%

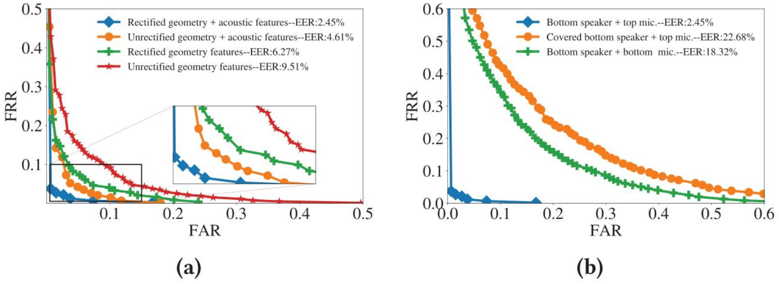
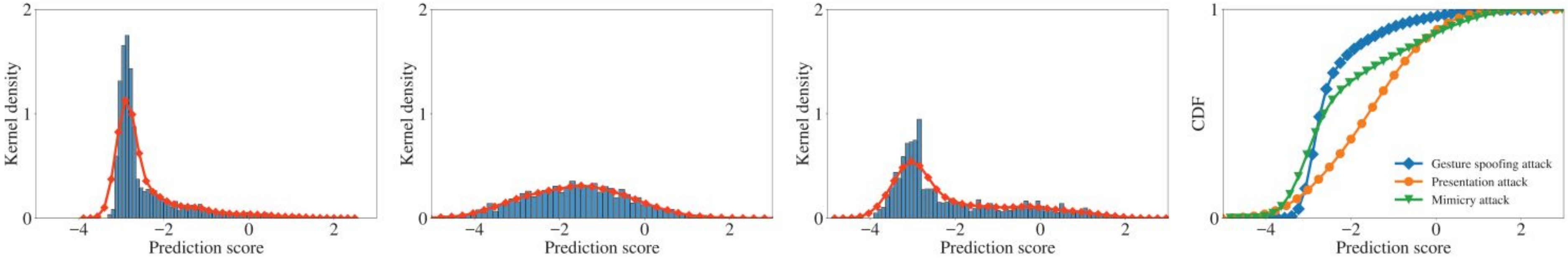


Figure 18: ROC curves under landmark rectification (a), and different hardware settings (b)

Covered bottom speaker and top microphone, EER: 22.68%.
Bottom speaker and bottom microphone, EER:18.32%.

Evaluation of Attack Resistance



(a) Gesture spoofing attack (b) Presentation attack (c) Mimicry attack (d) CDF of attack data points' score

Kernel density of prediction score under attacks

Attack type	FAR	Prediction scores
Gesture spoofing attack	0.21%	-2.42/ 0.86
Presentation attack	0.62%	-1.60/ 1.21
Mimicry attack	1.35%	-2.11/ 1.37

Attack success rate: **< 1.5%**

Other Hand Authentications

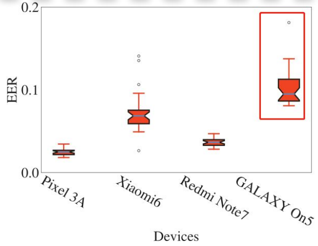
Table 9: Comparison of existing mature commercial hand authentications, the latest related research work

Method	Required hardware	Description of hand features	EER	PAR[1]	Hand motion[2]
		Commercial product			
Amazon One [9]	Unknown customized hardware (Maybe infrared camera, RGB camera)	Palm vein and palmprint patterns	N/A	✓	✗
Hand ID [10]	Infrared illuminator, TOF sensor[3]	Palm vein patterns	N/A	✓	✗
PalmID [6]	Infrared camera	Palm vein patterns	N/A	✓	✗
PalmID [6]	RGB camera	Palmprint patterns	N/A	✗	✗
PalmSecure [12]	Near-infrared imaging camera	Palm vein patterns	N/A	✓	✗
Vein ID [11]	Near-infrared illuminator, common RGB camera	Finger vein patterns	N/A	✓	✗
		Research paper			
[60]	Leap motion controller[4]	3D motion depth features of gesture movement	~ 2%	✓	✓
[27]	Leap motion controller	3D motion characteristics of fingertips and finger joints	< 4%	✓	✓
[50]	Multi-touch screen	Hand geometry and motion characteristics of swiping on a multi-touch touchscreen	5.84%	✓	✓
[33]	Optical scanner	Hand geometry features, including finger width and length	0.59%	✗	✗
[15]	Optical scanner	Hand geometry graph topology	3.05%	✗	✗
[23]	RGB camera, infrared lamp	Palm dorsal veins and hand geometry features	1.87%	✓	✗
[47]	IntelRealSense[5]	Palm vein patterns	< 1%	✓	✗
[13]	RGB camera	Hand images features extracted from different layers of a neural network	~ 5.2%	✗	✗
[65]	Speaker, microphone	Time-domain, frequencey-domain, MFCC[6], and chromagram features of structure-borne echos when holding a device (Without solid hand features)	~ 6%	✓	✗
[26]	Speaker, microphone, accelerometer	Spectrogram of microphone and accelerometer incurred by notification tones when holding a device (Without solid hand features)	~ 5%	✓	✗
EchoHand	RGB camera, speaker, microphone	Learning-based acoustic features of structure-borne and air-borne echos while sensing the hand holding device, hand geometry features including finger length, width, palm size and finger distance	~ 2.45%	✓	✗

[1] Presentation attack resistant. [2] Require users to perform hand motion. [3] A type of depth camera with a range imaging camera system. [4] An infrared-based depth camera used for tracking motions. [5] A high quality LiDAR-based depth cameras. [6] Mel-frequency cepstral coefficients, a kind of typical acoustic features.

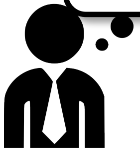
Limitation

Short distance between the microphone and speaker.



Behavior variability over time.

Consistency over a longer time span?



Require users to hold the device.

PHOTO: https://parker-marker.com/

Others: low sampling rate, poor lighting, off-normal shooting angles,

Summary

- EchoHand characterizes the holding hand **using acoustic sensing to complement hand geometry features** from the other hand.
- Comprehensive experiments to evaluate the effectiveness of EchoHand under **different settings and real environments**.
- Evaluation of **attack resistance against three types of attacks**, the overhead.

2012 IEEE Symposium on Security and Privacy

The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes*

Joseph Bonneau
University of Cambridge
Cambridge, UK
jcb82@cl.cam.ac.uk

Cormac Herley
Microsoft Research
Redmond, WA, USA
cormac@microsoft.com

Paul C. van Oorschot
Carleton University
Ottawa, ON, Canada
paulv@scs.carleton.ca

Frank Stajano†
University of Cambridge
Cambridge, UK
frank.stajano@cl.cam.ac.uk

Category	Scheme	Described in section	Reference	*Memorywise-Effortless*	*Scalable-for-Users*	*Nothing-to-Carry*	*Physically-Effortless*	*Easy-to-Learn*	*Efficient-to-Use*	*Infrequent-Errors*	*Easy-Recovery-from-Loss*	*Accessible*	*Negligible-Cost-per-User*	*Server-Compatible*	*Browser-Compatible*	*Mature*	*Non-Proprietary*	*Resilient-to-Physical-Observation*	*Resilient-to-Targeted-Impersonation*	*Resilient-to-Throttled-Guessing*	*Resilient-to-Unthrottled-Guessing*	*Resilient-to-Internal-Observation*	*Resilient-to-Leaks-from-Other-Verifiers*	*Resilient-to-Phishing*	*Resilient-to-Theft*	*No-Trusted-Third-Party*	*Requiring-Explicit-Consent*	*Unlinkable*
				Usability								Deployability						Security										
(Incumbent)	Web passwords	III	[13]			●		●	●	○	●	●	●	●	●	●	●		○						●	●	●	●
Password managers	Firefox	IV-A	[22]	○+	●+	○−	○+	●	●	●+	−	●	●	●	−	●	●	○+	○					●+	●	●	●	●
	LastPass		[42]	○+	●+	○−	○+	●	●	●+	○−	●	○−	●	−	●	−	○+	○	○+	○+		○+	●+	●	−	●	●
Proxy	URRSA	IV-B	[5]	●+		−		●	−	○	−	−	●	○−	●	−	−		○			○+		●+	−	−	●	●
	Impostor		[23]	○+	●+	●		●	−	−	●	●	−	●	○−	−	●	●+	○			○+		●+	●	−	−	●
Federated	OpenID	IV-C	[27]	○+	●+	●	○+	○−	●	●+	●	●	●	−	●	●	●	○+	○	○+	○+		●+		●	−	●	−
	Microsoft Passport		[43]	○+	●+	●	○+	●	●	●+	●	●	−	−	●	●	−	○+	○	○+	○+		●+		●	−	●	−
	Facebook Connect		[44]	○+	●+	●	○+	●	●	●+	●	●	●	−	●	●	−	○+	○	○+	○+		●+		●	−	−	−
	BrowserID		[45]	○+	●+	●	○+	●	●	●+	●	●	●	−	○−	○−	●	○+	○	○+	○+		●+		●	−	●	−
	OTP over email		[46]	○+	●+	●		●	−	●+	●	●	●	−	●	−	●	○+	○	○+	○+		●+	●+	●	−	●	−
Graphical	PCCP	IV-D	[7]			●		●	○−	○	●	−	●	−	●	−	●		●+	○+			●+	●+	●	●	●	●
	PassGo		[47]			●		●	○−	○	●	−	●	−	●	○−	●		●+						●	●	●	●
Cognitive	GrIDsure (original)	IV-E	[30]			●		●	○−	○	●	−	●	−	●	−	−		●+						●	●	●	●
	Weinshall		[48]			●		−	−	−	−	−	●	−	●	−	●	○+	●+				●+	●+	●	●	●	●
	Hopper Blum		[49]			●		−	−	−	−	●	●	−	●	−	●	○+	●+				●+	●+	●	●	●	●
	Word Association		[50]			●		●	●	○	○−	●	●	−	●	−	●		−						●	●	●	●
Paper tokens	OTPW	IV-F	[33]			−		●	−	−	●	−	●	−	●	●	●		●+	●+	●+	●+	●+	●+	●	●	●	●
	S/KEY		[32]	●+		−		●	−	○	●	−	●	−	●	●	●		●+	●+	●+	●+	●+	○+	−	●	●	●
	PIN+TAN		[51]			−		●	−	○	○−	−	○−	−	●	●	●		●+	●+	●+	●+	●+	●+	○−	●	●	●
Visual crypto	PassWindow		[52]	●+		−		−	−	−	−	−	○−	−	●	●	−	○+	●+	●+	●+	●+	●+	●+	−	●	●	●
Hardware tokens	RSA SecurID	IV-G	[34]			−		●	○−	○	−	−	−	−	●	●	−	●+	●+	●+	●+	●+	●+	●+	●	−	●	●
	Yubikey		[53]			−		●	○−	○	−	●	−	−	●	●	−	●+	●+	●+	●+	●+	●+	●+	●	−	●	●
	Ironkey		[54]	○+	●+	−	○+	○−	○−	○	−	●	−	●	●	●	−	●+	○			○+		●+	●	●	●	●
	CAP reader		[55]			−		●	○−	○	−	−	−	−	●	●	−	●+	●+	●+	●+	●+	●+	●+	●	●	●	●
	Pico		[8]	●+	●+	−	●+	−	○−	○	−	−	−	−	−	−	●	●+	●+	●+	●+	●+	●+	●+	○−	●	●	●
Phone-based	Phoolproof	IV-H	[36]			○−		●	○−	○	−	○−	○−	○−	−	−	●	●+	●+	●+	●+	○+	●+	●+	●	●	●	●
	Cronto		[56]			○−		●	○−	○	−	−	○−	−	●	●	−	●+	●+	●+	●+	○+	●+	●+	●	●	●	●
	MP-Auth		[6]			○−		●	○−	−	○−	○−	○−	−	−	−	●		○					●+	●	●	●	●
	OTP over SMS			●+	●+	○−		●	−	○	○−	○−	−	−	●	●	●	●+	●+	●+	●+	○+	●+	●+	○−	−	●	●
	Google 2-Step		[57]			○−		●	○−	○	○−	○−	−	−	●	●	−	○+	○	●+	●+		●+	●+	●	●	●	●
Biometric	Fingerprint	IV-I	[38]	●+	●+	●	○+	●	○−	−	−	○−	−	−	−	○−	−	●+	−	●+					−	●	●	−
	Iris		[39]	●+	●+	●	○+	●	○−	−	−	○−	−	−	−	○−	−	●+	−	●+					−	●	○−	−
	Voice		[40]	●+	●+	●	○+	●	○−	−	−	○−	○−	−	○−	○−	−	●+	−	○+					−	●	●	−
Recovery	Personal knowledge		[58]	○+		●		●	●	○	●	●	●	−	●	●	●		−						●	●	●	●
	Preference-based		[59]	○+		●		●	○−	●+	○−	●	●	−	●	−	−		○					●+	●	●	●	●
	Social re-auth.		[60]			●		●	−	●+	−	●	●	−	●	○−	−	○+	−	●+	●+	○+	○+	●+	●	−	●	○−

● = offers the benefit; ○ = almost offers the benefit; *no circle* = does not offer the benefit.

||| = better than passwords; ≡ = worse than passwords; *no background pattern* = no change.

We group related schemes into categories. For space reasons, in the present paper we describe at most one representative