Leakage or Identification: Behavior-irrelevant User Identification Leveraging Leakage Current on Laptops

DIAN DING, Shanghai Jiao Tong University, China
LANQING YANG, Shanghai Jiao Tong University, China
YI-CHAO CHEN, Shanghai Jiao Tong University, China
GUANGTAO XUE*, Shanghai Jiao Tong University, China

The convenience of laptops brings with it the risk of information leakage, and conventional security systems based on the password or the explicit biometric do little to alleviate this problem. Biometric identification based on anatomical features provides far stronger security; however, a lack of suitable sensors on laptops limits the applicability of this technology. In this paper, we developed a behavior-irrelevant user identification system applicable to laptops with a metal casing. The proposed scheme, referred to as *LeakPrint*, is based on leakage current, wherein the system uses an earphone to capture current leaking through the body and then transmits the corresponding signal to a server for identification. The user identification is achieved via denoising, dimension reduction, and feature extraction. Compared to other biometric identification methods, the proposed system is less dependent on external hardware and more robust to environmental noise. The experiments in real-world environments demonstrated that *LeakPrint* can verify user identity with high accuracy (93.6%), while providing effective defense against replay attacks (96.5%) and mimicry attacks (90.9%).

CCS Concepts: • **Security and privacy → Authentication**; • **Human-centered computing → Ubiquitous and mobile computing**.

Additional Key Words and Phrases: User Identification, Leakage Current, Laptop

ACM Reference Format:
Dian Ding, Lanqing Yang, Yi-Chao Chen, and Guangtao Xue. 2021. Leakage or Identification: Behavior-irrelevant User Identification Leveraging Leakage Current on Laptops. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 5, 4, Article 152 (December 2021), 23 pages. https://doi.org/10.1145/3494984

1 INTRODUCTION

Laptops are becoming indispensable in people's lives due to the important role in study, work and entertainment; therefore, the information leakage of laptops may cause incalculable damage. Considering the risk of information leakage in a public environment, institutions such as universities and enterprises commonly require staff to access secret documents only in the office premises. Moreover, information security is further ensured by encryption, identification and other methods [30].

*Corresponding author.

Authors' addresses: Dian Ding, Shanghai Jiao Tong University, China, e-mail:dingdian94@sjtu.edu.cn; Lanqing Yang, Shanghai Jiao Tong University, China, e-mail:yanglanqing@sjtu.edu.cn; Yi-Chao Chen, Shanghai Jiao Tong University, China, e-mail:yichao@sjtu.edu.cn; Guangtao Xue, Shanghai Jiao Tong University, China, e-mail:gt_xue@sjtu.edu.cn.

2474-9567/2021/12-ART152 $15.00
https://doi.org/10.1145/3494984

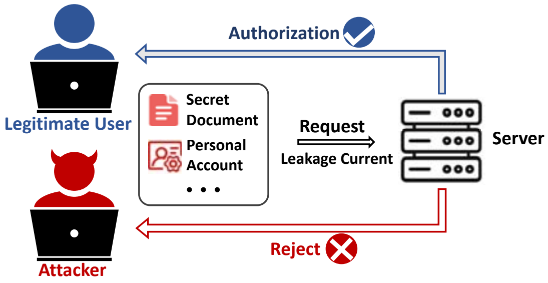


Fig. 1. Illustration of the user identification on laptops.

However, document encryption typically utilizes a specific password [48], and the information can be easily leaked through the keystrokes [19, 20]. Identification methods based on explicit biometrics, such as the fingerprint [7] and the face [29], are vulnerable to replay attacks [2] and mimicry attacks [31]. Therefore, even within a company or school, an attacker may attack these systems to steal the secret documents from laptops in between the departure of legitimate user, and we need to build a reliable user identification system for the information security of laptops.

This has prompted researches into alternative biometric features, such as user behavior [22, 33, 51] and anatomical features [3, 11, 16, 18, 28, 41, 47]. These schemes have proven effective in terms of identification accuracy; however, behavior-based schemes are prone to information leakage and scanning physiological features requires the sensors in mobile phones [15, 16, 18, 22, 47] or other external devices [11, 28, 41, 51]. BreathPrint [3] extracts information from the breath of users through a microphone; however, it is susceptible to external interference. Furthermore, laptops are not equipped with the various sensors found in mobile phones, which hinder the acquisition of rich biometric information.

Leakage current through the metal casing of laptops, such as the MacBook, can be attributed to the safety capacitor in the power adapter. In recent studies [9, 40, 49], researchers have verified the feasibility of using electrical signals for user identification. As shown in Fig. 1, we developed a user identification system predicated on the fact that the capacitance of the human body can be affected by various anatomical characteristics, such as muscle density, bone density, and fat thickness. When a user touches the laptop, leakage current through the body transmits biometric features to a server, which compares the signal against those previously collected from the actual registered user. The fact that most companies and scientific institutions use servers for data storage, and metal casings are favored for their physical strength and heat dissipation performance (e.g., Apple, HP, Huawei and Xiaomi [46]) ensures the widespread applicability of the proposed scheme.

Developing a user identification system based on leakage current imposed a number of daunting challenges. The first challenge involved developing a stable current transmission channel to read the current flowing through the body. Second, the weak current leaking from laptops ($0.3mA$) is highly susceptible to noise. Third, different contact behaviors could potentially affect the propagation of current.

Initial spectral analysis of signals traveling through the body verified the feasibility of a user identification system based on leakage current. In this paper, we used an earphone to create a stable human-machine channel by which to capture the current leaking through the body. Based on the leakage current, we proposed a behavior-irrelevant user identification system *LeakPrint* applied to laptops.

Essentially, when the user touches the laptop wearing an earphone, the laptop casing, the earphone and the user form a current path. The resulting information is forwarded to a server, where it is sampled by a sound card [24]. Biometric characteristics are then extracted based on the aliasing effects imposed by sampling high-frequency signals at a low sampling rate ($48kHz$). Multi-band spectral subtraction [10] is used to denoise the signal, and secondary denoising is applied to frequency components presenting large fluctuations. For the sparsity of biometric characteristics, DC-SIS (Distance Correlation - Sure Independence Screening) [13] is used to reduce the dimensionality of the signal. The samples from multiple users are filtered to build triples for the TCN (Temporal Convolutional Network) [12] with Triplet Loss [29] to enable the extraction of behavior-irrelevant user features. The experiments demonstrated that *LeakPrint* is able to identify users with high accuracy (93.6%), while providing the effective defense against replay attacks (96.5%) and mimicry attacks (90.9%). The contributions of this research are outlined as follows:

- We explored the phenomenon of leakage current in the metal casing of laptops, and verified the feasibility of user identification based on the leakage current.
- We extracted user features from the frequency spectrum of the leakage current, and solved the problems of low signal strength and sparse features;
- We extracted the behavior-irrelevant features from the leakage current based on TCN and Triplet Loss, and built a behavior-irrelevant user identification system on laptops;
- We conducted the experiments in real-world environments and the results demonstrated the feasibility of *LeakPrint* in accurately identifying users and defending against replay and mimicry attacks.

The remainder of this paper is organized as follows: In Sec. 2, we present the related works about user identification. In Sec. 3, we verify the feasibility of leakage current-based user authentication, introduce the threat model and system overview. The preprocessing of the leakage current and identification of user features are detailed in Sec. 4 and Sec. 5. Sec. 6 outlines the experiments used to evaluate the proposed system. In Sec. 7, we discuss the limitations and the future work of *LeakPrint*. Finally, conclusions are presented in Sec. 8.

2 RELATED WORKS

2.1 Conventional User Identification Methods

Classic methods are based on the passwords (e.g., PIN [48] and pattern lock [54]) or the explicit biometrics (e.g., fingerprint [7, 26], face [29], and voice identification [42]) are prone to security breaches. Passwords are easily intercepted through side channels, such as acoustic signals [19] or vibration signals [20], whereas biometric methods are susceptible to performance degradation due to ambient light and noise [17]. Moreover, these methods are vulnerable to replay attacks and mimicry attacks [2, 31, 55].

2.2 Behavior-based User Identification Methods

Behavior-based identification methods identify different users by the specific way they use their computers [33, 51] and mobile phones [22, 51]. Shen [33] used mouse movements for user identification. MagPrint [51] used an external magnetic sensor to read the effect of user operations on the state of the CPU to enable identification based on magnetic signals. TouchWB [22] recognized different users according to the way they swipe the screen.

Shen [33] can be deployed on laptops; however, it requires $8.77s$ to identify the user. MagPrint [51] can also be deployed on laptops with identification in $200ms$; however, it is limited to specific applications.

2.3 Biometrics-based User Identification Methods

In addition to the explicit biometrics like fingerprints and faces, other biometrics have also been used to identify users and are resistant to different attacks, including body size [28, 34, 41], fingers [4, 11, 47], mouth [17, 18], breath [3] and heartbeat[14–16].

BodyPIN [41] and Shi [34] used the effect of body size on WiFi signals to identify users. SkullConduct [28] used bone conduction of sound to differentiate between users wearing smart glasses.

Finger characteristics are reflected in physiological and behavioral characteristics [4, 11, 47]. FingerPass [11] used WiFi signals to extract behavioral features from finger gestures in order to differentiate among users. TouchPass [47] utilized the accelerometer built into mobile phones to read the response of fingers to phone vibrations in order to extract behavior-irrelevant physiological features for user identification. Chen [4] used the ZC sequence to capture the spatial characteristic of a finger when inputting a PIN.

Unlike speech identification, LipPass [17] and VocalLock [18] extracted the behavioral characteristics of the lips and the vocal tract during the formation of speech. LipPass [17] distinguished users based on Doppler profiles of the lips when speaking a particular phrase. VocalLock [18] utilized FMCW to sense the dynamic features in the vocal tract in order to extract passphrase-irrelevant features for user identification.

BreathPrint [3] used a microphone to capture the acoustic signal of breath for user identification on mobile phones and computers. Cardiac Scan [14] used radar to sense the heart motion signals in order to extract motion-invariant identity descriptors from geometric and non-volatile features. The flow of blood through the finger changes the light reflectance characteristics of skin. CardioCam [15] and Seeing Red [16] utilized the camera in mobile phones to read heart motion signals in order to extract user specific heart features.

According to the system hardware, the above methods can be divided into those based on external devices and those based on internal sensors.

Most of the methods based on external devices use WiFi [11, 34, 41] and radar signals [14] to obtain user information, and therefore have specific requirements pertaining to hardware setup. For example, during identification, the user must be close to the access point [11, 41] or radar [14]. Thus, these methods are ill-suited to scenarios covering a large area, such as large offices, conference halls.

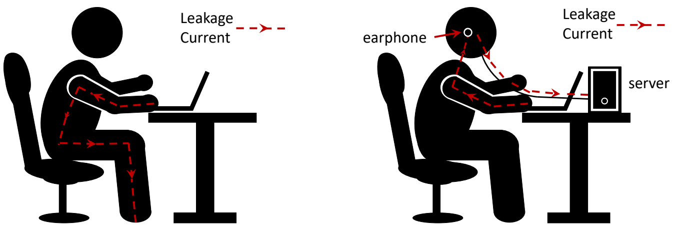
Mobile phones are rich in sensor systems that provide multi-dimensional user characteristics such as built-in accelerometers [47], microphones [3, 4, 17, 18, 28] and cameras [15, 16]. However, identification methods using the microphone [4, 17, 18] or camera [15, 16] depend on the unique structure of the microphone and speaker, or the camera and flash in the mobile phone. As a result, these methods are difficult to implement directly on laptops.

BreathPrint [3] can be applied to laptops via an external microphone; however, the distribution of the breath signal is predominantly below $4kHz$ and the signal is weak, such that user identification accuracy is only 40% under $66dB$ of ambient noise. By contrast, the biometric characteristics of the users in *LeakPrint* are mainly distributed between $7kHz$ and $22kHz$ under the sampling rate of $48kHz$. Thus, even under ambient noise of $65dB$, identification accuracy was 81.3%. Furthermore, the sampling rate can be increased to avoid the low frequency band in which ambient noise is concentrated.

2.4 Body Capacitance

2.4.1 Body Channel Communication. Body Channel Communication refers to the propagation of electrical signals through the human body for the purpose of digital communication [23, 38, 39, 50]. EM-Comm [50] detected the data into the electromagnetic radiation generated by the electronic device, and then stored the signal in the customized wristband via touch. Body-Guided Comm [23] implemented a touch-based security token based on human body communication. TouchCom [38, 39] built an end-to-end wearable BCC system, which can act as a sensor in any part of the human body to enable communication.

2.4.2 Body Capacitance-based User Identification Methods. Recent researches [9, 40, 49] has demonstrated the feasibility of using the capacitance of the body for user identification. Bioamp [9] collected user data using twelve pairs of electrodes on a wristband in conjunction with a touch screen to read user identity information from a contact point. Carpacio [40] used the capacitive coupling produced by a touch screen and the electrodes in a car seat to verify the identity of the user. TouchAuth [49] explored the impact of environmental electric fields on the human body to identify users based on electrical potential.



(a) Leakage current under normal use. (b) Human-machine channel.

Fig. 2. Fundamental principle of leakage current: 2(a) Under normal use, leakage current flows from the laptop through the user's hands into the body and eventually into the ground; 2(b) Earphones can be used to capture the signal for transmission to a server.

As an integral part of capacitance in the human body, micro-currents limit the applicability of these methods. The micro-current involved in the above schemes are derived from touch screens [40] or special bracelets [9, 49], which means that they are not well-suited to laptop-based user identification. *LeakPrint* utilizes the leakage current from the laptop with a metal casing to capture the biometric characteristics of the user via an earphone. Compared with other body capacitance-based methods, the proposed system is highly resistant to attacks (FAR of 9.1%) without reliance on specific devices [9, 49] or specific implementation scenarios [40].

3 BACKGROUND

This section outlines the cause of leakage current in laptops and examines the feasibility of using leakage current to identify the users. We also examine the threat model commonly used to target user identification systems and present the system overview of *LeakPrint*.

3.1 Leakage Current

Leakage current occurs when a laptop with metal casing (e.g., MacBook) is connected to a power source. The current comes from the Y capacitor in the adapter, referred to as the safety capacitor [36]. The Y capacitor is part of the EMI (Electromagnetic interference) filter circuit located between the power line and ground line, which is tasked with eliminating common mode interference and improving electromagnetic compatibility (EMC).

As a common mode capacitor, grounding of the Y capacitor generates leakage current [43], which can be written as:

$$I = 2\pi fCU \tag{1}$$

where f refers to the mains frequency, C indicates the size of the Y capacitor, and U indicates the voltage to the ground. The Y capacitors used in laptop adapters are typically around $5nF$; therefore, a laptop powered by the $220V/50Hz$ mains generates roughly $0.3mA$ of leakage current at the casing.

3.2 User Identification based on Leakage Current

3.2.1 Human-Machine Channel. Researchers [9, 49] have used wristbands equipped with electrodes to collect electrical signals from the human body; however, those methods depend entirely on external hardware. We sought to build a more generalizable signal transmission channel between the laptop and user. As shown in Fig. 2(a), with the user's hands placed on the laptop and the feet on the ground, leakage current flows from the laptop through the human body and eventually into the ground.

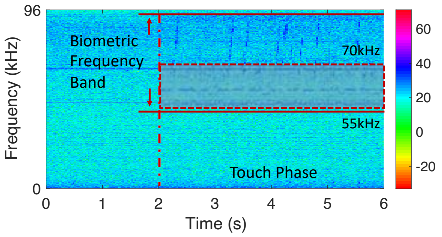


Fig. 3. Spectrum of leakage current showing changes in current captured by an earphone when the user touches the laptop, where the dotted line indicates the time when the use came into contact with the laptop, leading to an increase in signal amplitude in the high frequency band (stable in $55kHz$ and $70kHz$).

The flow of current can induce local heat stress on the body and other hazards [38]; therefore, laptop manufacturers seek to minimize these effects by maintaining the leakage current to roughly $0.3mA$. The human body can be regarded as a conductor with low impedance (a few $k\Omega$) [27], resulting in an average SAR (specific energy absorption rate) of roughly $0.5mW/kg$. ICNIRP guidelines [1] stipulate a limit on leakage current ($20mA$) and average SAR ($80mW/kg$). Furthermore, the impact of leakage current on the human body is lower than that of body channel communication systems [38, 39]. Taken together, it appears that leakage current can be used to derive biometric characteristics without overt risk to the user.

Previous studies have used devices equipped with signal generators, electrodes, and/or ADCs to generate and read electrical signals flowing through the body [9, 40, 49]. We sought to read the leakage current using an earphone (see Fig. 2(b)) to be collected by a sound card [24]. In preliminary experiments, we set the sampling rate of the sound card at $192kHz$ in order to extend the bandwidth. As shown in Fig. 3, the amplitude of the signal received by the earphone increased when the user touched the laptop.

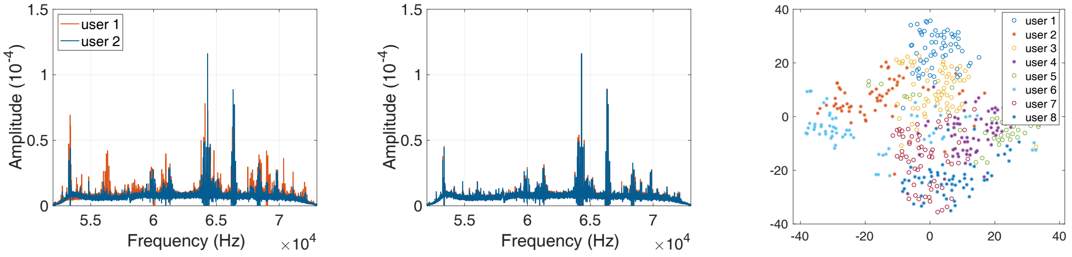
3.2.2 User Identification based on Leakage Current. Leakage current flowing through the body can be affected by the anatomical traits of the individual (e.g., blood vessels, muscle, fat, bone), leading to subtle differences in impedance [21] with corresponding variations in signal attenuation at different frequencies.

Preliminary experiments were conducted to verify the feasibility of the system. A MacBook Pro was used to collect data from two volunteers, both of whom were asked to place a hand in the same fixed position on the right side of the touchpad, while data was collected from a single channel of the earphone.

Most of the biometric characteristics were distributed in the high frequency band (stable in $55kHz$ and $70kHz$), as shown in Fig. 3. Samples (duration = $1s$) were analyzed in terms of frequency distribution after FFT (Fast Fourier Transform). As shown in Fig. 4(a), different users presented obvious differences in distribution and amplitude at some frequencies. As shown in Fig. 4(b), the two samples obtained from the same volunteer were extremely similar in terms of frequency distribution, with only slight differences in magnitude.

We then sought to verify the feasibility of using leakage current for user identification by collecting signals from eight volunteers under the same experimental setup. As shown in Fig. 4(c), we plotted the t-SNE [37] of the biometric characteristics in a two-dimensional space. We found that as the number of volunteers increased, the distinction between biometric characteristics decreased. Clearly, biometric characteristics based on leakage current cannot be used directly for user identification.

The above results can be attributed to the fact that leakage current was weak, and noise hindered the extraction of biometric characteristics. It should also be noted that most of the biometric characteristics were found at a few specific frequencies between $55kHz$ and $70kHz$. Under these conditions, it is essential to minimize the influence of noise, if meaningful biometric characteristics are to be extracted. Moreover, in the preliminary experiment, the



(a) Biometric characteristics of 2 different users.

(b) Biometric characteristics of the same user.

(c) t-SNE of 8 different users.

Fig. 4. Preliminary experiments: 4(a) Biometric characteristics of 2 different users from the frequency spectrum are highly distinguishable in some frequencies; 4(b) Biometric characteristics of the same user have high consistency; 4(c) The distinction between the biometric characteristics of the 8 different users is significantly reduced.

volunteers touched the laptop in the same designated way. For the sake of user experience, this restriction should be eliminated.

3.3 Threat Model

Feature extraction based on the leakage current of laptops is affected by the biometrics (e.g., human capacitance) and behavioral features (e.g., different ways of touch). The leakage current-based user identification is threatened by two types of attacks: replay attack and mimicry attack.

In the replay attack, the attacker steals the identification information of the legitimate user and uses that information for identification. For example, the attacker takes a photo of the legitimate user's fingerprint and performs fingerprint identification [47]. For *LeakPrint*, the attacker can steal user information through electrodes glued to the metal casing and use microphone playback to achieve the replay attack.

In the mimicry attack, the attacker observes the behavior of the legitimate user during identification and mimics that behavior to perform the attack. This type of attack mainly targets identification systems that extract behavioral features, such as gestures or commands [18]. *LeakPrint* is not designed with sophisticated contact methods, and attackers may spy on legitimate users' touch behaviors and imitate them.

3.4 System Overview

As shown in Fig. 5, after the leakage current detection and frequency domain transformation (FFT), the proposed system is implemented in two phases: registration phase and login phase.

In the registration phase, the system is responsible for collecting samples of legitimate users and training the identification system. After the server receives the leakage current, it preprocesses the current signal. First, we use the signal of idle time as a noise sample and denoise the signal using multi-band spectral subtraction. Second, more than 90% of the user features cannot be used for identification; therefore, *LeakPrint* uses DC-SIS to filter out the irrelevant features to reduce the computational burden. Finally, the system uses TCN and Triplet Loss to extract behavior-irrelevant features and produce these features as a dataset for each legitimate user.

In the login phase, the system identifies the user by leakage current. First, *LeakPrint* detects the touch behavior by signal amplitude and preprocesses the signal, including denoising and dimensionality reduction. Then the behavior-irrelevant features are extracted by TCN. Finally, the system compares the user features with those of legitimate users in the dataset to determine the identity of the current user.

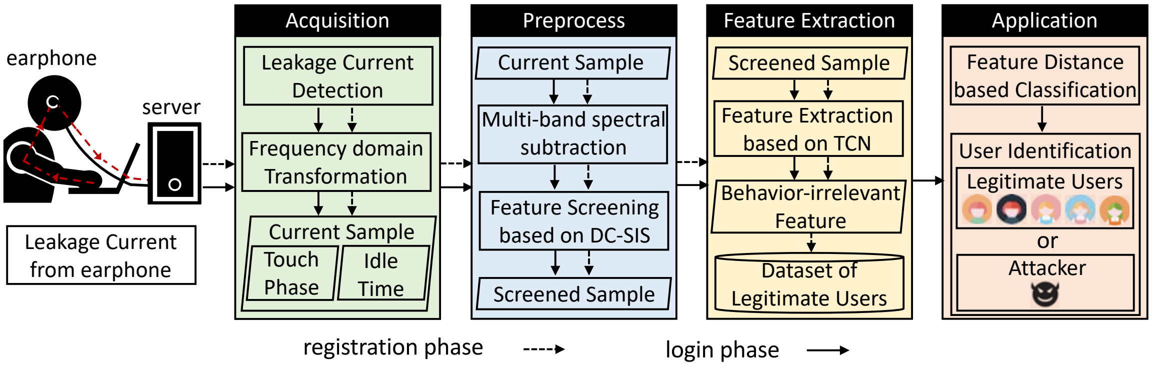

earphone
server
Leakage Current from earphone
Acquisition
Leakage Current Detection
Frequency domain Transformation
Current Sample
Touch Phase
Idle Time
Preprocess
Current Sample
Multi-band spectral subtraction
Feature Screening based on DC-SIS
Screened Sample
Feature Extraction
Screened Sample
Feature Extraction based on TCN
Behavior-irrelevant Feature
Dataset of Legitimate Users
Application
Feature Distance based Classification
User Identification
Legitimate Users
or
Attacker
registration phase
login phase

Fig. 5. System architecture of *LeakPrint*.

4 PREPROCESS OF LEAKAGE CURRENT

4.1 Detection of Leakage Current

Identifying the user via leakage current requires that the system is able to detect the time when the user touches the device. As shown in the Fig. 3, touching the laptop generates a slight increase in the amplitude of the electrical signal in the high frequency range (above $55kHz$). We seek to sample the leakage current based on the aliasing effect, thus reducing the limitation of the sampling rate. The aliasing effect can be written as:

$$f_a = min|f_o - Nf_s| \tag{2}$$

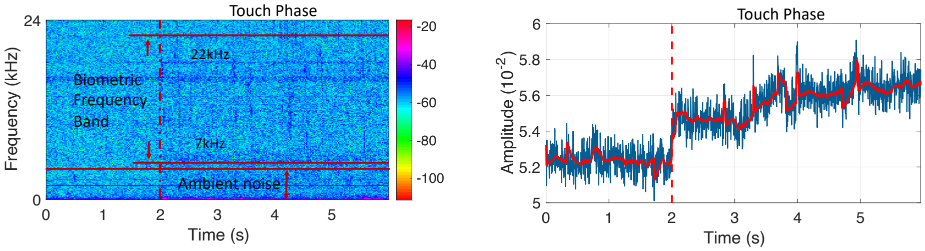
where N is an integer, f_a, f_o, and f_s respectively indicate the aliasing frequency, the signal frequency, and the sampling rate. As shown in Fig. 6(a), when using a sampling rate of $48kHz$, biometric characteristics in the target frequency band ($55kHz$ to $70kHz$) produce corresponding aliasing signals in a lower frequency band ($7kHz$ to $22kHz$). Besides, high-frequency noise (above $70kHz$) also produces a corresponding aliasing signal.

The most straightforward approach to perceiving the user touching the laptop involves setting a signal strength threshold. We set 1024 sampling points as a buffer to calculate the signal amplitude for the entire frequency band. As shown in Fig. 6(a), the sparse biometric characteristics are easily overwhelmed by noise, such that the change in signal amplitude induced by touching the laptop is close to zero.

A band pass filter with high-order cutoff is well suited to the main frequency distribution of the electric signal. To eliminate the effects of human voices (below $1kHz$) and other low-frequency noise, we employed a band-pass filter ($7kHz$ to $22kHz$) to improve the SNR of the signal. Note that threshold-based detection methods are susceptible to outliers; therefore, we employed a mean window to dilute these effects. Considering that a long mean window would reduce the change in signal amplitude generated by touching the laptop casing, we set a mean window length of 10. The mean window can be described as follows:

$$S_{mean}(i) = \sum_{j=i}^{i+N} S(j) \tag{3}$$

where $S(i)$ represents the signal filtered by the bandpass filter, $S_{mean}(i)$ represents the signal filtered by the mean window, and N indicates the window size.



(a) Spectrum of the leakage current.

(b) Amplitude of the leakage current.

Fig. 6. Leakage current detection, where the dotted line indicates the time of contact: 6(a) Spectrum of the leakage current obtained at the sampling rate of $48kHz$, where the aliasing frequency includes user characteristics and high-frequency noise. 6(b) The signal amplitude in the lower frequency band ($7kHz$ to $22kHz$) processed using a mean window (blue) and momentum (red).

Since the change in signal amplitude caused by touch is lower than the amplitude oscillation, we used momentum to weaken the influence of signal oscillation on detection. The process of momentum attenuation can be written as follows:

$$S_{momentum}(i+1) = S_{momentum}(i) + \alpha(S_{mean}(i+1) - S_{momentum}(i)) \tag{4}$$

where $S_{momentum}(i)$ represents the signal after momentum attenuation. We set the momentum decay coefficient α at 0.5 when the amplitude change was greater than 0.002; otherwise, it was set to 0.05. As shown in Fig. 6(b), the effects of touching the laptop can be detected by setting a threshold for the signal amplitude.

4.2 Denoising of Leakage Current

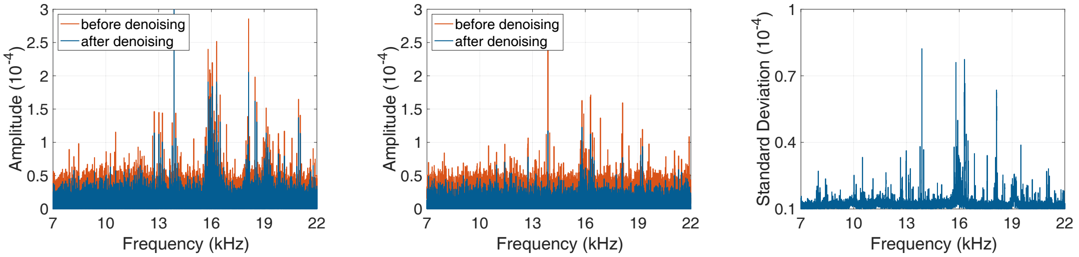
The combination of a mean window and momentum proved effective in detection of leakage current. While signal patterns related to biometric indicators are easily drowned out by noise. We divided the noise into two categories: ambient noise (e.g., voices) and signal aliasing caused by high-frequency noise in electrical signals (e.g., other electrical appliances [32]). The ambient noise remained after using the bandpass filter to preprocess the signal, and the high-frequency noise can be regarded as additive noise with non-uniform distribution in the frequency band. Multi-band spectral subtraction [10] divides the frequency spectrum into several small frequency bands, from which spectral noise was subtracted respectively. Subtraction of the ith frequency band can be written as follows:

$$\|Y_i(k)\|^2 = \|S_i(k)\|^2 - \beta_i \|N_i(k)\|^2 \tag{5}$$

where $b_i < k < e_i$ represents the frequency range of the band, S_i and N_i respectively represent filtered user signal samples and noise signal samples, respectively. We acquired $1s$ samples of both the leakage current and noise, and generated the spectral signals using FFT. β_i is related to the SNR (signal-to-noise ratio) of the signal in a given frequency band:

$$\beta_i = c_1 \cdot log_{10}\left(\frac{\sum_{k=b_i}^{e_i} \|S_i(k)\|^2}{\sum_{k=b_i}^{e_i} \|N_i(k)\|^2}\right) + c_2 \tag{6}$$

A lower SNR means that the proportion of noise signals in the frequency band is larger, such that the coefficient must be increased to reduce the influence of noise. While a higher SNR requires a smaller coefficient to preserve



(a) Spectral subtraction of leakage current. (b) Spectral subtraction of noise signal. (c) Standard deviation of noise fluctuations.

Fig. 7. Multi-band spectral subtraction: 7(a) Leakage current before (red) and after (blue) spectral subtraction; 7(b) Noise signal before (red) and after (blue) spectral subtraction, showing obvious residual noise at specific frequencies; 7(c) Wide fluctuations in noise at specific frequencies.

the biometric characteristics. Therefore, we set $c1$ to -1.5, and set $c2$ to 1 to ensure that denoising would have a noticeable effect.

As shown in Fig. 7(a) and Fig. 7(b), the effect of multi-band spectral subtraction was evaluated using a sample of leakage current and noise. Spectral subtraction acts on the entire frequency band; therefore, to preserve the biometric characteristics as much as possible, we set a smaller spectral subtraction coefficient. Nonetheless, even after spectral subtraction, the signal was still affected by the high-amplitude noise at specific frequencies.

To consider this residual high-amplitude noise in analysis would require secondary denoising. Note that the characteristics of noise differ at different frequencies. Thus, we analyzed noise samples obtained at each frequency to derive a statistic model of changes in amplitude. As shown in Fig. 7(c), the amplitude of noise at some frequencies fluctuated considerably over time (i.e., abnormal noise), which made it very difficult to remove via spectral subtraction.

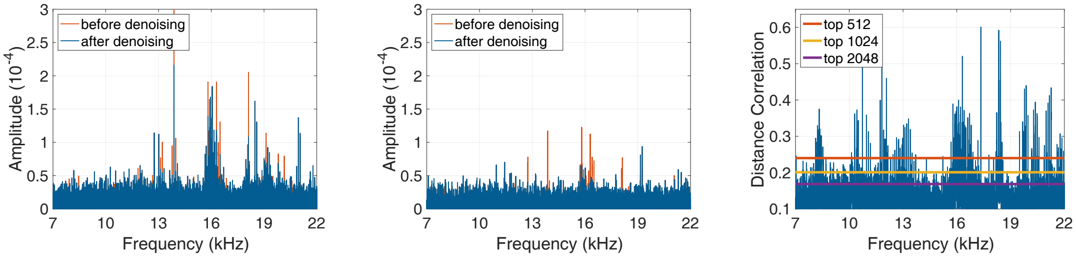
In the current study, we employed adaptive denoising [45] to deal with abnormal noise. Adaptive noise reduction adjusts the denoising strategy according to the characteristics of the sample. In this paper, secondary denoising began with the filtering out of potential abnormal noise based on the variance in each frequency noise sample. Note however that due to the sensitivity of the biometric characteristics, it is essential to confirm the frequencies of the abnormal noise. We designated frequencies with fluctuations greater than twice the average value as abnormal noise, and collected noise samples in real time for updating. We then addressed the frequency corresponding to abnormal noise associated with leakage current. Only samples that exhibited amplitude greater than the standard deviation of the noise frequency underwent secondary denoising:

$$\|\hat{Y}_i(f)\|^2 = \|Y_i(f)\|^2 - \sqrt{2} \cdot std(f) \tag{7}$$

where f represents potential abnormal noise, $std(f)$ indicates the standard deviation of noise, indicating the range of fluctuation in the noise at those frequencies. Fig. 8(a) and Fig. 8(b) respectively present the leakage current and noise signal after secondary denoising. Most of the noise in the $7kHz$ to $22kHz$ frequency band was effectively suppressed without altering the leakage current at frequencies corresponding to the biometric characteristics.

4.3 Feature Screening of Leakage Current

Feature sparseness of leakage current is another important issue in user identification. As shown in Fig. 8(a), the bandwidth of leakage current spans $15kHz$, and only a small portion reflects biometric characteristics. A



(a) Secondary denoising of leakage current. (b) Secondary denoising of noise signal. (c) Distance Correlation of leakage current.

Fig. 8. Secondary denoising of leakage current: 8(a) Leakage current before (red) and after (blue) secondary denoising; 8(b) Noise signal before (red) and after (blue) secondary denoising, showing suppression of frequency corresponding to abnormal noise; 8(c) Distance correlation between different frequencies and user labels, indicating that most frequencies cannot be used for user identification.

large number of redundant features would increase the computational burden and reduce accuracy in user identification. Signal redundancy can be reduced by decreasing the dimensionality of data. The most common approach is Principal Component Analysis (PCA); however, this method imposes requirements pertaining to the number of samples. The wide bandwidth of leakage current would require the collection of an enormous volume of user data, which would no doubt have a negative effect on the user experience.

As an alternative to PCA, DC-SIS (Distance Correlation - Sure Independence Screening) [13] analyzes univariate, which lessens the restriction on the number of samples. Sure screening ensures that all important variables have attributes with a probability of 1 after screening. DC [35] describes the dependence between two random variables and solves the dependence of traditional SIS [6] on the normal distribution of features. The distance covariance between two random vectors $\mathbf{u}$ and $\mathbf{v}$ with finite first moments to the nonnegative number $dcov(\mathbf{u}, \mathbf{v})$ is given by the following:

$$dcov^2(\mathbf{u}, \mathbf{v}) = \int_{R^{d_u+d_v}} \|\phi_{\mathbf{u},\mathbf{v}}(\mathbf{t}, \mathbf{s}) - \phi_{\mathbf{u}}(\mathbf{t})\phi_{\mathbf{v}}(\mathbf{s})\|^2 \omega(\mathbf{t}, \mathbf{s}) d\mathbf{t} d\mathbf{s} \tag{8}$$

where $\phi_{\mathbf{u}}(\mathbf{t})$ and $\phi_{\mathbf{v}}(\mathbf{s})$ represent the respective characteristic functions of $\mathbf{u}$ and $\mathbf{v}$, and $\phi_{\mathbf{u},\mathbf{v}}(\mathbf{t}, \mathbf{s})$ represents the joint characteristic function of $\mathbf{u}$ and $\mathbf{v}$. d_u and d_v are the dimensions of $\mathbf{u}$ and $\mathbf{v}$, and

$$\omega(\mathbf{t}, \mathbf{s}) = \{c_{d_u} c_{d_v} \|\mathbf{t}\|_{d_u}^{1+d_u} \|\mathbf{s}\|_{d_v}^{1+d_v}\}^{-1} \tag{9}$$

where $c_d = \pi^{(1+d)/2}\Gamma\{(1+d)/2\}$, and the DC between $\mathbf{u}$ and $\mathbf{v}$ with finite first moments is defined as follows:

$$dcorr(\mathbf{u}, \mathbf{v}) = \frac{dcov(\mathbf{u}, \mathbf{v})}{\sqrt{dcov(\mathbf{u}, \mathbf{u}) dcov(\mathbf{v}, \mathbf{v})}} \tag{10}$$

Let $\mathbf{x_k} = (x_{k1}, ..., x_{kn})^T$ be the feature vector of the kth dimension from the $n \times m$ sample $\mathbf{X}$, $\mathbf{y} = (Y_1, ..., Y_n)^T$ be the label vector, and $\omega = (\omega_1, ..., \omega_m)^T$ be a m-vector of correlation between the features and the label:

$$\omega_k = dcorr(\mathbf{x_k}, \mathbf{y}) \tag{11}$$

Using the correlation vector, key features can be filtered from ultra-high dimensional features. For a given $\eta \in (0, 1)$, we sort the m components of the vector ω according to the size of the component, and define the model as follows:

$$M_\eta = \{1 \le i \le p : \omega_i \text{ is among the first } [\eta m] \text{ largest of all}\} \tag{12}$$

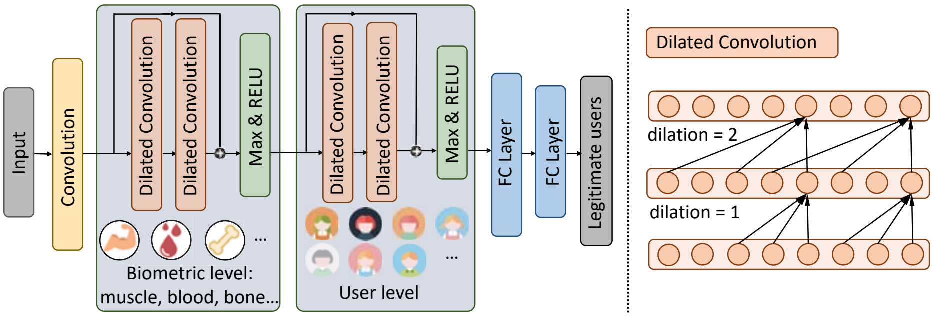


Fig. 9. Architecture of User Identification Network.

where $[\eta m]$ represents the integer part of ηm. Correlation learning is used to rank features in terms of importance according to the marginal correlation between the features and the label, while screening out the features that are not strongly marginal correlated with the label. As shown in Fig. 8(c), for the leakage current spanning a bandwidth of $15kHz$, we screened out the 512, 1024 and 2048 features that were most relevant to the users. Based on these results, we estimate that more than 93% of the features are irrelevant to biometric characteristics and should therefore not be used for user identification.

5 BEHAVIOR-IRRELEVANT USER IDENTIFICATION

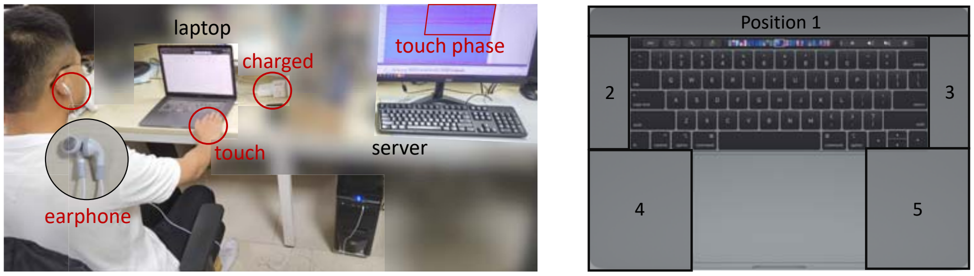
5.1 User Identification Model

CNN (Convolutional neural network) has proven highly effective in the extraction of spectral features [47, 51, 56]. In *LeakPrint*, we built the user identification model based on TCN (Temporal Convolutional Network) [12] and ResNet [8], as shown in Fig. 9. The proposed CNN comprises three components: the convolutional layer, the TCN module and the fully connected layers. Each TCN module comprises three layers, including two dilated convolutional layers, and a max pooling layer (with RELU activation function). The convolutional layer performs the initial extraction of the input features to improve the correlation between the subsets corresponding to the different features of the dilated convolutional layer. In the TCN module, the dilated convolutional layer [52] has a larger perception field with the same amount of computation by inserting space in the convolutional layer. The residual structure incorporates features of various depths and solves the gradient disappearance problem during the training process. The max pooling layer reduces the dimensionality of the features [25]. User identification is achieved using two fully-connected layers based on the user-level features.

Specifically, the first convolutional layer uses 32 convolutional kernels of 3 × 1-dimension to generate a correlated subset for adjacent features of the dilated convolutional layer. The two dilated convolutional layers in the TCN module both use 64 convolutional kernels of 3 × 1-dimension to extract features, with dilation rates of 2 and 4. After the max pooling layer and RELU activation function, two TCN modules respectively extract features at biometric-level and user-level. The numbers of neurons in the two fully connected layers are 512 and 64, respectively.

5.2 Behavior-irrelevant Feature Extraction

In the preliminary experiments, the laptops were touched by users in a strictly controlled manner. As the metal casing of the laptop has a very low resistance, and therefore has very little effect on the propagation of leakage current. Recent biometric-based studies confirmed the impact of user behavior on biometric features [18, 47]. Nonetheless, touching the laptop using fingers, the palm, or the wrist would no doubt alter the contact area



(a) Experimental setup of *LeakPrint*.

(b) Different positions of the laptop.

Fig. 10. Experimental setup: 10(a) Experimental setup of *LeakPrint*. The unknown user touches the laptop with one hand, the server detects the leakage current via the earphone. We use the third party software Audacity to present the leakage current; 10(b) Five regions of the laptop casing.

between the user and laptop, with a corresponding effect on the propagation of leakage current. Therefore, we need to extract common biometric features from the different touch behaviors.

LeakPrint uses Triplet Loss [29, 53] to blunt the influence of these factors on the leakage current. Triplet Loss is meant to maximize the distance between two samples with different labels, and minimize the distance between two samples with the same label within the feature space during the encoding process. Specifically, Triplet Loss constructs triplets based on the training set. The triplets can be written as follows:

$$(I^a, I^p, I^n) \tag{13}$$

where I^a and I^p are from the same user, and I^n is from another user. The distance of the samples in the feature space can be written as:

$$\|f(I^a) - f(I^p)\|_2^2 + margin < \|f(I^a) - f(I^n)\|_2^2 \tag{14}$$

where $f(I)$ represents the process of feature extraction and the corresponding loss function can be written as:

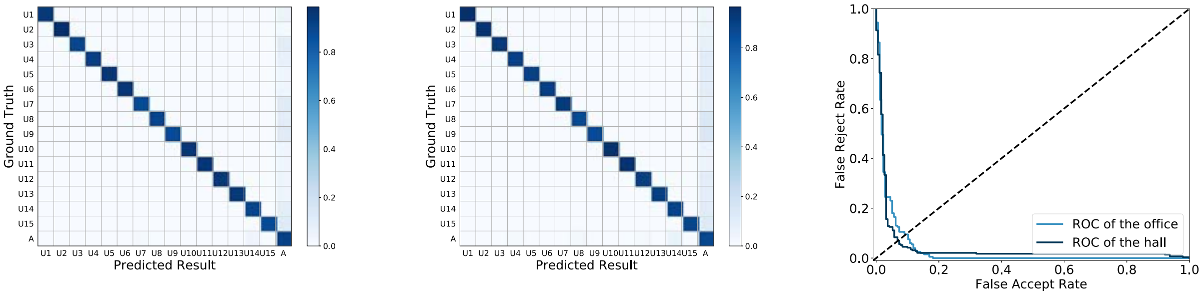
$$L = max(\|f(I^a) - f(I^p)\|_2^2 - \|f(I^a) - f(I^n)\|_2^2 + margin, 0) \tag{15}$$

5.3 Attacker Detection

Identifying and defending against attackers is crucial to the feasibility of user identification systems. *LeakPrint* compares user-level features of leakage current in the login phase versus the legitimate users to perform user identification and attack detection. We set n users as legitimate users, and collect N samples for each user. The feature distance between an unknown user $f_{unknown}$ and the legitimate user f_i is defined as follows:

$$D_i = \frac{1}{N} \sum_{k=1}^{N} \|f_{unknown} - f_{ik}\|_2^2 \tag{16}$$

The distances between the unknown user and all the legitimate users is $[D_1, ..., D_n]$. If the minimum distance between the unknown user and all the legitimate users is larger than the given threshold δ, then the unknown user is determined as an attacker; otherwise, the unknown user is identified as the legitimate user presenting the minimum distance.



(a) Confusion matrix in an office.

(b) Confusion matrix in the conference hall.

(c) ROC in two environments.

Fig. 11. Micro Benchmarks of *LeakPrint* in two real-world environments.

6 EVALUATION

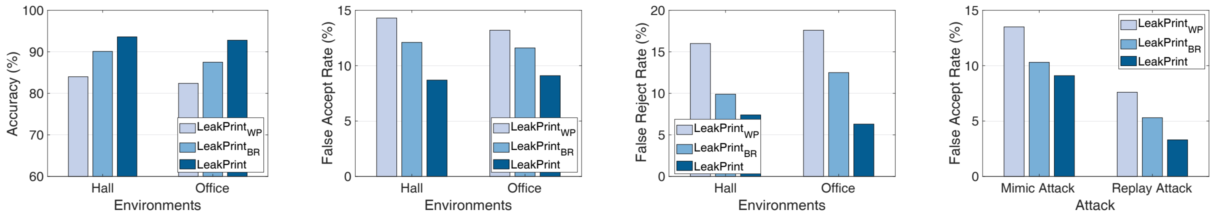
6.1 Experimental Setup

In the experiment, *LeakPrint* was implemented on a MacBook Pro, and a desktop computer was used as the server, as shown in Fig.10(a). We chose the earphone with metal dust mesh (Meizu) to collect the leakage current. The MacBook was always on charge and placed on the desk. The user wore the earphone normally and touched the MacBook, and the earphone was connected to the server. We also sought to assess the influence of other electrical appliances in the circuit [32] by conducting experiments in two real-world environments: an office (multiple electrical interference) and a conference hall (few electrical interference).

We hired 40 participants to validate *LeakPrint*, containing 27 males and 13 females with ages ranging from 19 to 47 (average age of 29.6 and SD of 8.53). 30 participants (10 females) played the role of legitimate users and 10 participants played the role of attackers. We divided the participants who played the role of legitimate users into a training group and a test group (15 people each). In the benchmark experiments, first, we let the participants in the training group perform the registration phase and pre-train the encoder with these samples. Second, we let the participants in the test group perform the registration and login phases to evaluate the system's identification accuracy of legitimate users. Finally, we let the attackers perform the login phase to verify the system's defense capability against attacks. In the experiments with different environments and different parameters, we evaluated the identification accuracy of the system by the legitimate users in the test group and the resistance of the system to the attacks by the attackers in the same way. The specific operations of the registration phase and the login phase are as follows.

Registration phase. The legitimate users were asked to touch five regions of the laptop (Fig. 10(b)) with each hand (fingers, palms, and wrists) for $1min$, for a total of 15 different ways of touch. The samples were $1s$ in duration and 240 samples were obtained under each hand/region configuration (both hands, dual channels of the earphone). Then, the system filtered the feature frequencies of the legitimate users with DC-SIS. Finally, the system used TCN to extract the behavior-irrelevant features and produced a dataset for each legitimate user.

Login phase. The participants were asked to touch the laptop with all 15 configurations for $15s$ in two environments. Then, the system performed feature extraction and extraction on the user samples in the same way. Finally, the feature of the participants were compared with the dataset of legitimate users for identification.



(a) Accuracy in two environments. (b) FAR in two environments. (c) FRR in two environments. (d) FAR of *LeakPrint* for attacks.

Fig. 12. Comparison of different *LeakPrint* versions.

System parameters. The sampling rate was set at $48kHz$, and FFT was used to generate the spectral characteristics of the users. In the registration and login phases, the same parameters were used to process the leakage current: the sample time ($1s$), the feature length (1024), the size of training set for each volunteer (240) and the threshold of the attacker detection (0.8). These parameters are discussed in detail in Section. 6.4.

The performance of *LeakPrint* was assessed using the following metrics:

Identification Accuracy: The probability that user A is correctly identified in all relevant samples.

Confusion Matrix: Each row of the matrix represents the predicted result, and each column represents the actual label. The ith row and jth column of the matrix indicate the proportion of the ith user identified as the jth user.

False Accept Rate (FAR): The probability of identifying an attacker as a legitimate user.

False Reject Rate (FRR): The probability of identifying a legitimate user as an attacker.

Equal Error Rate (EER): The common value when FAR and FRR are equal.

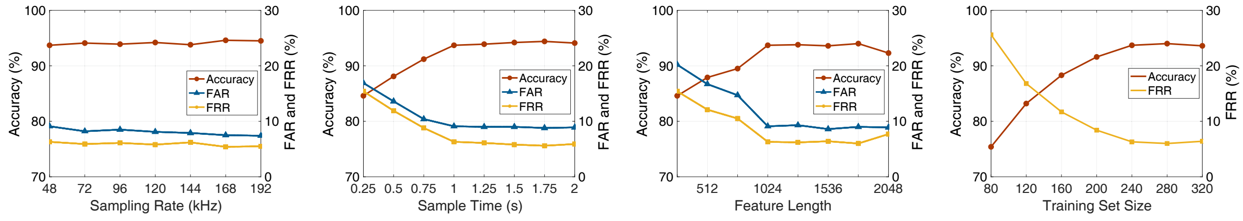
6.2 Micro Benchmarks

We first evaluated the identification performance of *LeakPrint* in two environments (Fig. 11(a) and Fig. 11(b)). The 15 legitimate users were denoted as $(U_1, U_2, ..., U_{15})$, and the attackers were denoted as A. The average accuracy of *LeakPrint* in identifying legitimate users was 92.8% and 93.6% respectively in the two environments. The FAR of attacks was 9.1% and 8.7%, the FRR was 7.2% and 6.4%, and the EER was around 8.6% and 7.1% in the two environments. As shown in Fig. 11(c), we plotted the ROC (Receiver Operator Characteristic) curves consisting of FAR and FRR for the two environments. These results demonstrate that *LeakPrint* can accurately identify the identity of legitimate users and detect attackers, even under the effects of other influence of other electrical appliances.

We then examined the effects of touching the laptop in various areas using various parts of the hand. As shown in Table. 1, *LeakPrint* achieved high detection accuracy regardless of the way the laptop was touched.

Table 1. Identification accuracy of different touches in different positions.

	Position 1	**Position 2**	**Position 3**	**Position 4**	**Position 5**
Finger	92.5%	94.2%	93.8%	95.1%	95.6%
Palm	91.7%	94.3%	94.1%	92.8%	93.1%
Wrist	92.1%	93.6%	92.5%	94.6%	95.5%



(a) Influence of sampling rate. (b) Influence of sample time. (c) Influence of feature length. (d) Influence of training set size.

Fig. 13. Evaluation of the *LeakPrint* system.

To verify the need to preprocess the current signal and extract of behavior-irrelevant features, we built two incomplete systems for comparison: $LeakPrint_{WP}$ (Signal without Preprocessing) and $LeakPrint_{BR}$ (Behavior-Relevant Features). As shown in Fig. 12(a), Fig. 12(b) and Fig. 12(c), we compare the identification accuracy and FAR of three versions. *LeakPrint* significantly outperformed the other two versions, thereby demonstrating that signal preprocessing and behavior-irrelevant feature extraction are both indispensable.

6.3 Performance on Attacker Resistance

The performance of *LeakPrint* was also evaluated under different attacks, the attacker can attack the system in two ways. During the login process of a legitimate user, the attacker glues electrodes to the metal enclosure to record the current signal, since current signals in parallel circuits can interact with each other [32]. The microphone is then used to play that signal to perform the replay attack. And in the mimicry attack, the attacker tries his best to mimic the touch behavior of the legitimate user.

In this experiment, the 15 legitimate users were asked to perform the user identification. We then replayed the leakage current signal using a speaker as the replay attack, and had 10 attackers mimic the behavior of legitimate users by touching the laptop for 30 times ($1s$ each).

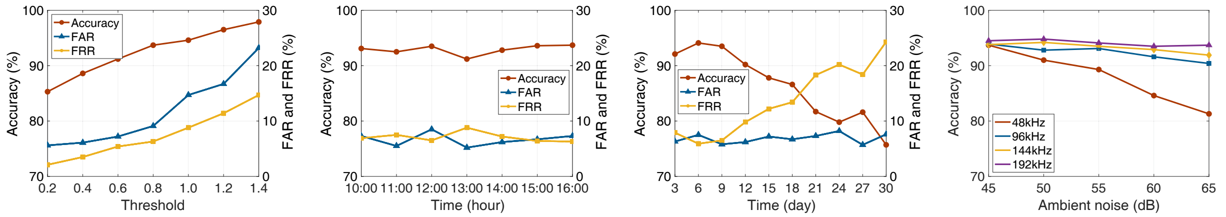
As shown in Fig. 12(d), the FAR of *LeakPrint* did not exceed 9.1%, regardless of the threat model. Replay attacks using speakers were severely disturbed by environmental noise, and mimicry attacks could not match the biometric characteristics. Besides, the threshold for attacker detection can also be adjusted according to the application scenario. However, there are certain special circumstances that can cause *LeakPrint* to fail, such as the possibility that an attacker could replay the stolen data in an extremely quiet environment, or that the attacker's biometric characteristics happen to match a legitimate user.

6.4 Influence of System Parameters

The performance of *LeakPrint* was also evaluated under various system parameters, including sampling rate, sample time, feature length, training set size and threshold for attacker detection.

6.4.1 Influence of Sampling Rate.

To reduce limitations on hardware, we perceived the leakage current with the sampling rate of $48kHz$; however, differences in the sampling rates could lead to differences in the aliasing signal at different frequencies. Furthermore, the noise distribution in various frequency bands could also conceivably affect user identification. In this experiment, we evaluated *LeakPrint* in terms of identification accuracy, FAR and FRR at various sampling rates ranging from $48kHz$ to $192kHz$. As shown in Fig. 13(a), when the sampling rate was increased from $48kHz$ to $192kHz$, identification accuracy increases from 93.6% to 94.5% and FAR dropped from 9.1% to 7.4%. The results indicate that an increase in sample rate has a positive impact on the identification



(a) Influence of threshold.
(b) Influence of evaluation time.
(c) Influence of evaluation time.
(d) Influence of ambient noise.

Fig. 14. Evaluation of the *LeakPrint* system.

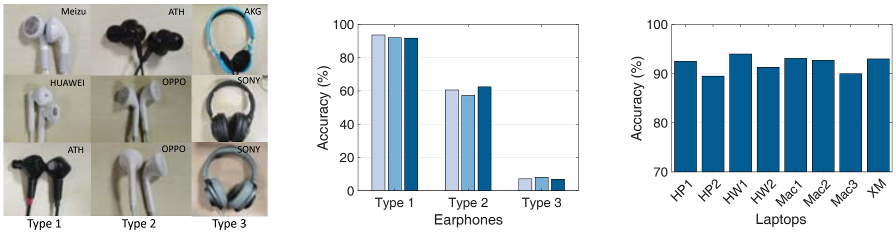
results. Typically, most servers can achieve the minimum sample rate required (48kHz). Therefore, *LeakPrint* can be deployed at low cost in most universities, companies, etc.

6.4.2 Influence of Sample Time. At a given sampling frequency, the resolution of user features in the spectrum was inversely proportional to the sample time. In this experiment, we evaluated the *LeakPrint* in terms of identification accuracy, FAR and FRR under various sample times ranging from 0.25s to 2s. As shown in Fig. 13(b), when the sample time was increased from 0.25s to 2s, identification accuracy increased from 84.6% to 94.1% and FAR dropped from 16.9% to 8.9%. When the sample time was increased from 1s to 2s, the system did not improve significantly. Considering the impact of identification speed on the user experience, we set the sample time at 1s. Nevertheless, as the number of users is further increased, we can improve the fine-grained level of physiological features by increasing the sample time to optimize the identification performance of the system.

6.4.3 Influence of Feature Length. To reduce the impact of high-dimensional samples on identification accuracy, we used the DC-SIS algorithms to extract key features from the spectrum. Thus, we evaluated *LeakPrint* in terms of identification accuracy, FAR and FRR under feature lengths ranging from 256 to 2048. As shown in Fig. 13(c), increasing the feature length from 256 to 1024 greatly improved the performance of the system. As shown in Fig. 8(c), when the feature length was increased beyond 1024, most of the improvement would have little or no effect. We therefore set the feature length at 1024. However, the feature length is closely related to the features of legitimate users. The features of the users in different groups, and the differences in the features between users will respond to the different feature frequencies and feature lengths of the leakage current. Therefore, we have to set different feature frequencies and feature lengths for different user groups with DC-SIS.

6.4.4 Influence of Training Set Size. The training set size determines the amount of time required to collect samples of legitimate users. A larger training set would no doubt improve generalization performance; however, it would also increase the initial workload and perhaps inconvenience the user. We evaluated the accuracy of the system with training sets of various sizes. As shown in Fig. 13(d), increasing the size of the training set from 80 to 320 increased identification accuracy from 75.4% to 93.6%, accuracy plateaued when the size reached roughly 240. In this experiment, we did not examine FAR, due to the fact that a small training set would lead to over-fitting, such that the FAR of the attack would have little practical reference value.

6.4.5 Influence of Threshold for Attacker Detection. Our determination of whether an unknown user is legitimate is based on the distance between user-level features; therefore, the threshold for attacker detection is crucial to the security of the system. As shown in Fig. 14(a), identification accuracy and FAR are both positively correlated with this threshold. For laptops with few security risks, we recommend setting a higher threshold to obtain



(a) Different types of earphones. (b) Influence of different earphones. (c) Influence of different laptops.

Fig. 15. Evaluation of the *LeakPrint* system.

higher identification accuracy (above 98%). For laptops with a high probability of being attacked, we recommend setting a lower threshold to make the system more resistant to attacks (below 6%).

6.4.6 Influence of Evaluation Time Points. To verify the relationship between the physiological features and evaluation time, we evaluated *LeakPrint* at different time points. As shown in Fig.14(b), first, we evaluated the system at multiple time points during the day. We performed the registration phase at 9:00 a.m. and the login phase every hour thereafter (including special cases such as before and after meals). On the other hand, we set the timeline of the experiment to one month. We performed the registration phase on the first day and the login phase every three days thereafter (Fig.14(c)).

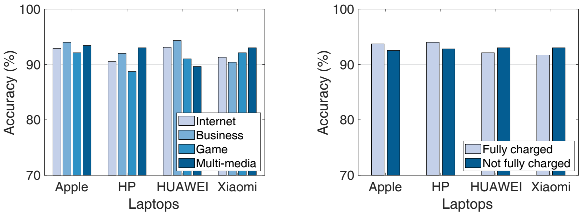
It can be seen that the identification accuracy can be maintained above 91.2% and the FAR is below 8.5% at different time points of the same day. The result implies that the physiological features of the human body are stable in the short-term. Moreover, as the time interval increases, the identification accuracy decreases from 92.1% to 75.7% and the FAR remains below 8.2%. This confirms that the physiological features change slowly over time. Although we did not encounter this situation in the experiments, we cannot rule out that the attacker's features may gradually approximate the samples in the legitimate user dataset over time. Therefore, we recommend updating the user dataset in real time to maintain the accuracy of identification and resistance to attacks.

6.4.7 Influence of Ambient Noise. We evaluated identification performance under ambient noise of $45dB$ (normal office) and $65dB$ (noisy conference room). As shown in Fig. 14(d), the system was more sensitive to ambient noise at a sampling rate of $48kHz$, as indicated by a decrease in identification accuracy from 93.6% to 81.3%. Increasing the sampling rate significantly increased the robustness of the system by reducing the effect of ambient noise in lower frequency bands. Overall, higher sampling rates provided greater stability in noisy environments.

6.5 Influence of Devices

We evaluated the performance of *LeakPrint* using a variety of laptops and earphones under various working conditions.

6.5.1 Influence of Different Earphones. As an important part of signal collection, we evaluated and discussed various aspects of the earphones, including the type of earphones, earphone aging and other issues. First, we can regard earphones as electrodes in contact with the human body, and different types of earphones can seriously affect the reception of leakage current. As shown in Fig. 15(a), we have chosen three different types of earphones for comparison (type 1: earphones with metal dust mesh, type 2: earphones with plastic dust mesh, and type 3: earphones with headband). For each type, we chose three different earphones. When using different types of earphones to receive signals, the accuracy will be significantly reduced by the weakening of signal strength (Fig. 15(b)). Therefore, we recommend using earphones with metal dust mesh. Besides, earphones of the same type



(a) Influence of applications. (b) Influence of the laptop battery.

Fig. 16. Evaluation of the *LeakPrint* system.

have similar conductive properties, and replacing the same model (or type) of earphones during the identification process will not affect the accuracy of the system. While different brands achieve different music playback by adjusting the frequency response of the earphones (e.g. Harman and ToneTeam Curve [44]), this is mainly focused on the human ear hearing range (below $20kHz$). Therefore, it does not affect the reception of the leakage current by the server (above $55kHz$).

Second, we can regard the aging of the earphones as a slight rusting of the electrodes, while the human body can be regarded as a conductor with the impedance of a few $k\Omega$ [27]. Therefore, the aging of the earphones will not have a serious impact on the leakage current. Finally, the choice of the sound channels of the earphones also affects the reception of the leakage current. We separated the current signal received by the dual channels into two samples, so that we can also perform effective identification in the case of a single channel damage.

6.5.2 Influence of Different Laptops. In this experiment, we evaluated *LeakPrint* on different laptops, including three Apple laptops, two HP laptops, two Huawei laptops and one Xiaomi laptop. As shown in Fig. 15(c), the system maintains the high identification accuracy, which demonstrates that the system can be deployed on the majority of laptops with metal casing. Furthermore, given the excellent strength and heat dissipation performance of the metal casing, companies such as Apple, Xiaomi and Huawei are focusing on laptops with metal casings [46]. Therefore, we believe LeakPrint has high promotion prospects.

6.5.3 Influence of Different Working Conditions. As shown in Fig. 16(a), we evaluated *LeakPrint* when running a variety of applications on the laptop: Internet (Chrome), Business (Microsoft Word), Game (MineCraft) and Multi-media (PotPlayer). The overall accuracy exceeded 88.7%, indicating identification performance was unaffected by applications running in the background.

On the other hand, the charging current of an adapter differs according to the state of the laptop battery (i.e., fully charged or not fully charged). We therefore evaluated *LeakPrint* with the battery in various charging states. As shown in Fig. 16(b), the state of the battery did not affect identification accuracy, due to the fact that leakage current is related only to voltage, the frequency of the mains, and the size of the safety capacitor.

7 DISCUSSION

In this paper, we developed a high-precision user identification system based on leakage current. In this section, we discuss the limitations of *LeakPrint* as a research prototype and provide an outlook on future work.

Security Aspects. Compared to other methods implemented on the laptop, *LeakPrint* is more resistant to attacks. Fingerprint identification can be easily attacked by fingerprint theft [2]; face identification can be attacked by wearing a special mask [31]; and password entry can cause bypass information leakage [19, 20, 48]. For *LeakPrint*, it is difficult for an attacker to steal leakage current from the bypass or to mimic the capacitive characteristics of a legitimate user's body. *LeakPrint* is also superior to other methods applied with laptops, BreathPrint [3] performed the user identification based on the breathing sound and the lower signal band (below $4KHz$) reduces the robustness of the method in real world environments.

Nonetheless, it is conceivable that changes in some anatomical features (e.g., muscle and bone density) could change sufficiently over time to render stored samples of the legitimate users obsolete. Thus, we believe that *LeakPrint* could collect data samples on an on-going basis and update the datasets to reflect gradual changes in biometric.

In this paper, we build the system and conduct experiments with the premise that the device is secure. It is possible for an attacker to change the acquisition device of the system (e.g., a earphone with storage function) and steal the raw data to attack the system. We will do further research for device security in future work.

Different Occasions and Devices. The leakage current used in *LeakPrint* comes from a safety capacitor in the adapter, so the leakage current can be generated in different scenarios configured with a power source. However, in the mobile scenarios, signal collecting devices are more difficult to configure than power source (e.g. the server in the system). We will focus on the development of convenient collecting devices in our future work.

Moreover, the leakage current may also be present in some household appliances, such as the metal casing or the metal button of some smart appliances. Since the operating current of household appliances is higher than that of laptops, we have to pay more attention to physical safety. We will investigate household appliances with the leakage current and explore the possibility of extending the system to these devices in our future work.

Future Work. We will optimize *LeakPrint* both in terms of hardware and algorithm. While the earphone offer advantages such as easy availability and low cost, it limits the application of the system in mobile scenarios. As an alternative to the earphone and server, we attempt to use mobile devices such as smart watches to capture the leakage current or detect the effects of the leakage current on the human body. The electrodes on the special bracelet are able to read the leakage current flowing through the body [38, 39, 49]. Besides, based on the ability of the current to stimulate muscles and cause involuntary movement [5], such slight movements may affect the blood vessels and thus alter the acquisition of ECG (electrocardiogram) by smart watches [15, 16]. Currently, we are unable to acquire the corresponding sensor data directly from smart watches. We attempt to verify our conjecture in future work using a bracelet configured with light sensors and electrodes.

On the other hand, we try to capture the dynamic features of human capacitance over time using temporal models such as LSTM [51], thus to improve the robustness of the system to fluctuations in capacitance features. Moreover, *LeakPrint* relies on anatomical features, which can be regarded as a static feature. In the future, we will explore the integration of gestures or actions with data related to leakage current, with the aim of developing an identification system based on static biometric as well as dynamic behavioral features.

8 CONCLUSION

This paper presents a user identification system for laptops with a metal casing. The proposed *LeakPrint* system uses an earphone to detect leakage current flowing through the body, and then transmits the signal to a server for identification. Based on the aliasing effect, the leakage current captured at the sampling rate of $48kHz$ are used in conjunction with denoising, dimension reduction, and feature extraction to enable behavior-irrelevant user identification. The experiments demonstrated the feasibility of LeakPrint in identifying users with a high degree of accuracy (93.6%), with excellent resistance to attack (FAR of 9.1%). Considering the ubiquity of servers in companies and research institutes, the system could be deployed in a variety of scenarios at low cost.

ACKNOWLEDGMENTS

We thank the anonymous reviewers for their valuable and professional comments that helped us to improve and refine this work. This work is supported by NSFC (61936015, U1736207, 62072306), Startup Fund for Youngman Research at SJTU, and Program of Shanghai Academic Research Leader (20XD1402100).

REFERENCES

[1] A Ahlbom, U Bergqvist, JH Bernhardt, JP Cesarini, M Grandolfo, M Hietanen, AF Mckinlay, MH Repacholi, David H Sliney, J AJ Stolwijk, et al. 1998. Guidelines for limiting exposure to time-varying electric, magnetic, and electromagnetic fields (up to 300 GHz). *Health physics* 74, 4 (1998), 494–521.

[2] P. Bontrager, A. Roy, J. Togelius, N. Memon, and A. Ross. 2018. DeepMasterPrints: Generating MasterPrints for Dictionary Attacks via Latent Variable Evolution*. In *2018 IEEE 9th International Conference on Biometrics Theory, Applications and Systems (BTAS)*. 1–9. https://doi.org/10.1109/BTAS.2018.8698539

[3] Jagmohan Chauhan, Yining Hu, Suranga Seneviratne, Archan Misra, Aruna Seneviratne, and Youngki Lee. 2017. BreathPrint: Breathing Acoustics-Based User Authentication. In *Proceedings of the 15th Annual International Conference on Mobile Systems, Applications, and Services* (Niagara Falls, New York, USA) *(MobiSys '17)*. Association for Computing Machinery, New York, NY, USA, 278–291. https://doi.org/10.1145/3081333.3081355

[4] Huijie Chen, Fan Li, Wan Du, Song Yang, Matthew Conn, and Yu Wang. 2020. Listen to Your Fingers: User Authentication Based on Geometry Biometrics of Touch Gesture. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 4, 3, Article 75 (Sept. 2020), 23 pages. https://doi.org/10.1145/3411809

[5] Yuxin Chen, Zhuolin Yang, Ruben Abbou, Pedro Lopes, Ben Y. Zhao, and Haitao Zheng. 2021. *User Authentication via Electrical Muscle Stimulation*. Association for Computing Machinery, New York, NY, USA. https://doi.org/10.1145/3411764.3445441

[6] Jianqing Fan and Jinchi Lv. 2008. Sure independence screening for ultrahigh dimensional feature space. *Journal of the Royal Statistical Society: Series B (Statistical Methodology)* 70, 5 (2008), 849–911. https://doi.org/10.1111/j.1467-9868.2008.00674.x arXiv:https://rss.onlinelibrary.wiley.com/doi/pdf/10.1111/j.1467-9868.2008.00674.x

[7] Diego Gragnaniello, Giovanni Poggi, Carlo Sansone, and Luisa Verdoliva. 2015. Local Contrast Phase Descriptor for Fingerprint Liveness Detection. *Pattern Recogn.* 48, 4 (April 2015), 1050–1058. https://doi.org/10.1016/j.patcog.2014.05.021

[8] Kaiming He, Xiangyu Zhang, Shaoqing Ren, and Jian Sun. 2016. Deep Residual Learning for Image Recognition. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*.

[9] Christian Holz and Marius Knaust. 2015. Biometric Touch Sensing: Seamlessly Augmenting Each Touch with Continuous Authentication. In *Proceedings of the 28th Annual ACM Symposium on User Interface Software amp; Technology* (Charlotte, NC, USA) *(UIST '15)*. Association for Computing Machinery, New York, NY, USA, 303–312. https://doi.org/10.1145/2807442.2807458

[10] S. Kamath and P. Loizou. 2002. A multi-band spectral subtraction method for enhancing speech corrupted by colored noise. In *2002 IEEE International Conference on Acoustics, Speech, and Signal Processing*, Vol. 4. IV–4164–IV–4164. https://doi.org/10.1109/ICASSP.2002.5745591

[11] Hao Kong, Li Lu, Jiadi Yu, Yingying Chen, Linghe Kong, and Minglu Li. 2019. FingerPass: Finger Gesture-Based Continuous User Authentication for Smart Homes Using Commodity WiFi. In *Proceedings of the Twentieth ACM International Symposium on Mobile Ad Hoc Networking and Computing* (Catania, Italy) *(Mobihoc '19)*. Association for Computing Machinery, New York, NY, USA, 201–210. https://doi.org/10.1145/3323679.3326518

[12] Colin Lea, Michael D. Flynn, Rene Vidal, Austin Reiter, and Gregory D. Hager. 2017. Temporal Convolutional Networks for Action Segmentation and Detection. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*.

[13] Runze Li, Wei Zhong, and Liping Zhu. 2012. Feature Screening via Distance Correlation Learning. *J. Amer. Statist. Assoc.* 107, 499 (2012), 1129–1139. https://doi.org/10.1080/01621459.2012.695654 arXiv:https://doi.org/10.1080/01621459.2012.695654 PMID: 25249709.

[14] Feng Lin, Chen Song, Yan Zhuang, Wenyao Xu, Changzhi Li, and Kui Ren. 2017. Cardiac Scan: A Non-Contact and Continuous Heart-Based User Authentication System. In *Proceedings of the 23rd Annual International Conference on Mobile Computing and Networking* (Snowbird, Utah, USA) *(MobiCom '17)*. Association for Computing Machinery, New York, NY, USA, 315–328. https://doi.org/10.1145/3117811.3117839

[15] Jian Liu, Cong Shi, Yingying Chen, Hongbo Liu, and Marco Gruteser. 2019. CardioCam: Leveraging Camera on Mobile Devices to Verify Users While Their Heart is Pumping. In *Proceedings of the 17th Annual International Conference on Mobile Systems, Applications, and Services* (Seoul, Republic of Korea) *(MobiSys '19)*. Association for Computing Machinery, New York, NY, USA, 249–261. https://doi.org/10.1145/3307334.3326093

[16] G. Lovisotto, H. Turner, S. Eberz, and I. Martinovic. 2020. Seeing Red: PPG Biometrics Using Smartphone Cameras. In *2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*. IEEE Computer Society, Los Alamitos, CA, USA, 3565–3574. https://doi.org/10.1109/CVPRW50498.2020.00417

[17] L. Lu, J. Yu, Y. Chen, H. Liu, Y. Zhu, Y. Liu, and M. Li. 2018. LipPass: Lip Reading-based User Authentication on Smartphones Leveraging Acoustic Signals. In *IEEE INFOCOM 2018 - IEEE Conference on Computer Communications*. 1466–1474. https://doi.org/10.1109/INFOCOM.

2018.8486283

[18] Li Lu, Jiadi Yu, Yingying Chen, and Yan Wang. 2020. VocalLock: Sensing Vocal Tract for Passphrase-Independent User Authentication Leveraging Acoustic Signals on Smartphones. 4, 2, Article 51 (June 2020), 24 pages. https://doi.org/10.1145/3397320

[19] L. Lu, J. Yu, Y. Chen, Y. Zhu, X. Xu, G. Xue, and M. Li. 2019. KeyListener: Inferring Keystrokes on QWERTY Keyboard of Touch Screen through Acoustic Signals. In *IEEE INFOCOM 2019 - IEEE Conference on Computer Communications*. 775–783. https://doi.org/10.1109/INFOCOM.2019.8737591

[20] Philip Marquardt, Arunabh Verma, Henry Carter, and Patrick Traynor. 2011. (Sp)IPhone: Decoding Vibrations from Nearby Keyboards Using Mobile Phone Accelerometers. In *Proceedings of the 18th ACM Conference on Computer and Communications Security* (Chicago, Illinois, USA) *(CCS '11)*. Association for Computing Machinery, New York, NY, USA, 551–562. https://doi.org/10.1145/2046707.2046771

[21] Ivan Martinovic, Kasper B. Rasmussen, Marc Roeschlin, and Gene Tsudik. 2017. Pulse-Response: Exploring Human Body Impedance for Biometric Recognition. *Acm Transaction on Information System Security* 20, 2 (2017), 6.1–6.31.

[22] Weizhi Meng, Yu Wang, Duncan S. Wong, Sheng Wen, and Yang Xiang. 2018. TouchWB : Touch behavioral user authentication based on web browsing on smartphones. *Journal of Network and Computer Applications* 117 (2018), 1–9. https://doi.org/10.1016/j.jnca.2018.05.010

[23] Viet Nguyen, Mohamed Ibrahim, Hoang Truong, Phuc Nguyen, Marco Gruteser, Richard Howard, and Tam Vu. 2018. Body-Guided Communications: A Low-Power, Highly-Confined Primitive to Track and Secure Every Touch. In *Proceedings of the 24th Annual International Conference on Mobile Computing and Networking* (New Delhi, India) *(MobiCom '18)*. Association for Computing Machinery, New York, NY, USA, 353–368. https://doi.org/10.1145/3241539.3241550

[24] Jay Prakash, Zhijian Yang, Yu-Lin Wei, Haitham Hassanieh, and Romit Roy Choudhury. 2020. EarSense: Earphones as a Teeth Activity Sensor *(MobiCom '20)*. Association for Computing Machinery, New York, NY, USA, Article 40, 13 pages. https://doi.org/10.1145/3372224.3419197

[25] Charles R. Qi, Hao Su, Kaichun Mo, and Leonidas J. Guibas. 2017. PointNet: Deep Learning on Point Sets for 3D Classification and Segmentation. arXiv:1612.00593 [cs.CV]

[26] Aditya Singh Rathore, Weijin Zhu, Afee Daiyan, Chenhan Xu, Kun Wang, Feng Lin, Kui Ren, and Wenyao Xu. 2020. SonicPrint: A Generally Adoptable and Secure Fingerprint Biometrics in Smart Devices. In *Proceedings of the 18th International Conference on Mobile Systems, Applications, and Services* (Toronto, Ontario, Canada) *(MobiSys '20)*. Association for Computing Machinery, New York, NY, USA, 121–134. https://doi.org/10.1145/3386901.3388939

[27] J Patrick Reilly. 2012. *Applied bioelectricity: from electrical stimulation to electropathology*. Springer Science & Business Media.

[28] Stefan Schneegaß, Youssef Oualil, and Andreas Bulling. 2016. SkullConduct: Biometric User Identification on Eyewear Computers Using Bone Conduction Through the Skull. 1379–1384. https://doi.org/10.1145/2858036.2858152

[29] Florian Schroff, Dmitry Kalenichenko, and James Philbin. 2015. FaceNet: A Unified Embedding for Face Recognition and Clustering. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*.

[30] Syed W. Shah and Salil S. Kanhere. 2019. Recent Trends in User Authentication – A Survey. *IEEE Access* 7 (2019), 112505–112519. https://doi.org/10.1109/ACCESS.2019.2932400

[31] Shawn Shan, Emily Wenger, Jiayun Zhang, Huiying Li, Haitao Zheng, and Ben Y. Zhao. 2020. Fawkes: Protecting Privacy against Unauthorized Deep Learning Models. In *29th USENIX Security Symposium (USENIX Security 20)*. USENIX Association, 1589–1604. https://www.usenix.org/conference/usenixsecurity20/presentation/shan

[32] Zhihui Shao, Mohammad Islam, and Shaolei Ren. 2020. Your Noise, My Signal: Exploiting Switching Noise for Stealthy Data Exfiltration from Desktop Computers? *ACM SIGMETRICS Performance Evaluation Review* 48 (07 2020), 79–80. https://doi.org/10.1145/3410048.3410094

[33] C. Shen, Y. Chen, X. Guan, and R. A. Maxion. 2020. Pattern-Growth Based Mining Mouse-Interaction Behavior for an Active User Authentication System. *IEEE Transactions on Dependable and Secure Computing* 17, 2 (2020), 335–349. https://doi.org/10.1109/TDSC.2017.2771295

[34] Cong Shi, Jian Liu, Hongbo Liu, and Yingying Chen. 2017. Smart User Authentication through Actuation of Daily Activities Leveraging WiFi-Enabled IoT. In *Proceedings of the 18th ACM International Symposium on Mobile Ad Hoc Networking and Computing* (Chennai, India) *(Mobihoc '17)*. Association for Computing Machinery, New York, NY, USA, Article 5, 10 pages. https://doi.org/10.1145/3084041.3084061

[35] Gábor J. Székely, Maria L. Rizzo, and Nail K. Bakirov. 2007. Measuring and testing dependence by correlation of distances. *Ann. Statist.* 35, 6 (12 2007), 2769–2794. https://doi.org/10.1214/009053607000000505

[36] Ting Guo, D. Y. Chen, and F. C. Lee. 1995. Diagnosis of power supply conducted EMI using a noise separator. In *Proceedings of 1995 IEEE Applied Power Electronics Conference and Exposition - APEC'95*, Vol. 1. 259–266 vol.1. https://doi.org/10.1109/APEC.1995.469028

[37] Laurens van der Maaten and Geoffrey Hinton. 2008. Visualizing Data using t-SNE. *Journal of Machine Learning Research* 9, 86 (2008), 2579–2605. http://jmlr.org/papers/v9/vandermaaten08a.html

[38] Virag Varga, Gergely Vakulya, Alanson Sample, and Thomas R. Gross. 2018. Enabling Interactive Infrastructure with Body Channel Communication. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 1, 4, Article 169 (Jan. 2018), 29 pages. https://doi.org/10.1145/3161180

[39] Virag Varga, Marc Wyss, Gergely Vakulya, Alanson Sample, and Thomas R. Gross. 2018. Designing Groundless Body Channel Communication Systems: Performance and Implications. In *Proceedings of the 31st Annual ACM Symposium on User Interface Software*

and Technology (Berlin, Germany) *(UIST '18)*. Association for Computing Machinery, New York, NY, USA, 683–695. https://doi.org/10.1145/3242587.3242622

[40] Edward Jay Wang, Jake Garrison, Eric Whitmire, Mayank Goel, and Shwetak Patel. 2017. Carpacio: Repurposing Capacitive Sensors to Distinguish Driver and Passenger Touches on In-Vehicle Screens *(UIST '17)*. Association for Computing Machinery, New York, NY, USA, 49–55. https://doi.org/10.1145/3126594.3126623

[41] Fei Wang, Zhenjiang Li, and Jinsong Han. 2019. Continuous User Authentication by Contactless Wireless Sensing. *IEEE Internet of Things Journal* 6, 5 (2019), 8323–8331. https://doi.org/10.1109/JIOT.2019.2916777

[42] Wechat. 2015. Voiceprint: The New Wechat Password. https://blog.wechat.com/2015/05/21/voiceprint-the-new-wechat-password/

[43] S. Westerlund and L. Ekstam. 1994. Capacitor theory. *IEEE Transactions on Dielectrics and Electrical Insulation* 1, 5 (1994), 826–839. https://doi.org/10.1109/94.326654

[44] Wikipedia. 2021. Wikipedia, Equal-loudness contour. https://en.wikipedia.org/wiki/Equal-loudness_contour

[45] Xiao-Ping Zhang and M. D. Desai. 1998. Adaptive denoising based on SURE risk. *IEEE Signal Processing Letters* 5, 10 (1998), 265–267. https://doi.org/10.1109/97.720560

[46] Xiaomi. 2021. https://www.mi.com/index.html

[47] Xiangyu Xu, Jiadi Yu, Yingying chen, Qin Hua, Yanmin Zhu, Yi-Chao Chen, and Minglu Li. 2020. TouchPass: Towards Behavior-Irrelevant on-Touch User Authentication on Smartphones Leveraging Vibrations. In *Proceedings of the 26th Annual International Conference on Mobile Computing and Networking* (London, United Kingdom) *(MobiCom '20)*. Association for Computing Machinery, New York, NY, USA, Article 24, 13 pages. https://doi.org/10.1145/3372224.3380901

[48] J. Yan, A. Blackwell, R. Anderson, and A. Grant. 2004. Password memorability and security: empirical results. *IEEE Security Privacy* 2, 5 (2004), 25–31. https://doi.org/10.1109/MSP.2004.81

[49] Zhenyu Yan, Qun Song, Rui Tan, Yang Li, and Adams Wai Kin Kong. 2019. Towards Touch-to-Access Device Authentication Using Induced Body Electric Potentials. In *The 25th Annual International Conference on Mobile Computing and Networking* (Los Cabos, Mexico) *(MobiCom '19)*. Association for Computing Machinery, New York, NY, USA, Article 23, 16 pages. https://doi.org/10.1145/3300061.3300118

[50] Chouchang Jack Yang and Alanson P. Sample. 2017. EM-Comm: Touch-Based Communication via Modulated Electromagnetic Emissions. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 1, 3, Article 118 (Sept. 2017), 24 pages. https://doi.org/10.1145/3130984

[51] L. Yang, Y. C. Chen, H. Pan, D. Ding, G. Xue, L. Kong, J. Yu, and M. Li. 2020. MagPrint: Deep Learning Based User Fingerprinting Using Electromagnetic Signals. In *IEEE INFOCOM 2020 - IEEE Conference on Computer Communications*. 696–705. https://doi.org/10.1109/INFOCOM41043.2020.9155534

[52] Fisher Yu and Vladlen Koltun. 2016. Multi-Scale Context Aggregation by Dilated Convolutions. arXiv:1511.07122 [cs.CV]

[53] Xiao Zeng, Kai Cao, and Mi Zhang. 2017. MobileDeepPill: A small-footprint mobile deep learning system for recognizing unconstrained pill images. In *Proceedings of the 15th Annual International Conference on Mobile Systems, Applications, and Services*. ACM, 56–67.

[54] Emanuel Zezschwitz, Paul Dunphy, and Alexander De Luca. 2013. Patterns in the wild: a field study of the usability of pattern and pin-based authentication on mobile devices. 261–270. https://doi.org/10.1145/2493190.2493231

[55] Linghan Zhang, Sheng Tan, and Jie Yang. 2017. Hearing Your Voice is Not Enough: An Articulatory Gesture Based Liveness Detection for Voice Authentication. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security* (Dallas, Texas, USA) *(CCS '17)*. Association for Computing Machinery, New York, NY, USA, 57–71. https://doi.org/10.1145/3133956.3133962

[56] Yongzhao Zhang, Wei-Hsiang Huang, Chih-Yun Yang, Wen-Ping Wang, Yi-Chao Chen, Chuang-Wen You, Da-Yuan Huang, Guangtao Xue, and Jiadi Yu. 2020. Endophasia: Utilizing Acoustic-Based Imaging for Issuing Contact-Free Silent Speech Commands. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 4, 1, Article 37 (March 2020), 26 pages.