Continuous Authentication Using Human-Induced Electric Potential

Srinivasan Murali
srinivasan.murali@mavs.uta.edu
The University of Texas at Arlington
Arlington, Texas, USA

Wenqiang Jin
wqjin@hnu.edu.cn
Hunan University
Changsha, Hunan, China

Vighnesh Sivaraman
vxs8596@mavs.uta.edu
The University of Texas at Arlington
Arlington, Texas, USA

Huadi Zhu
huadi.zhu@mavs.uta.edu
The University of Texas at Arlington
Arlington, Texas, USA

Tianxi Ji
tiji@ttu.edu
Texas Tech University
Lubbock, Texas, USA

Pan Li
pxl288@case.edu
Case Western Reserve University
Cleveland, Ohio, USA

Ming Li
ming.li@uta.edu
The University of Texas at Arlington
Arlington, Texas, USA

ABSTRACT

Most terminal devices authenticate users only once at the time of initial login, leaving the terminal unprotected during an active session when the original user leaves it unattended. To address this issue, continuous authentication has been proposed by automatically locking the terminal after a period of inactivity. However, it does not fully eliminate the risk of unauthorized access before the session expires. Recent research has also investigated the feasibility of using physiological and behavioral patterns as biometrics. This study presents a novel two-factor continuous authentication that explores a new form of signal called *human-induced electric potential* captured by wearables in contact with the user's body. By analyzing this signal, we can determine the time of user-terminal interactions and compare it with information recorded by the terminal's OS. If the original user remains on the same terminal, the two-source readings would match. Additionally, the proposed scheme includes an extra layer of protection by extracting terminal's physical fingerprints from the human-induced electric potential to defend against advanced mimicry attacks. To test the effectiveness of our design, a low-cost wearable prototype is developed. Through extensive experiments, it is found that the proposed scheme has a low error rate of 2.3%, with minimal computational and energy requirements.

CCS CONCEPTS

• **Security and privacy → Authentication**.

KEYWORDS

Continuous authentication; human-induced electric potential; wearables

ACSAC '23, December 04–08, 2023, Austin, TX, USA

ACM ISBN 979-8-4007-0886-2/23/12.
https://doi.org/10.1145/3627106.3627124

ACM Reference Format:
Srinivasan Murali, Wenqiang Jin, Vighnesh Sivaraman, Huadi Zhu, Tianxi Ji, Pan Li, and Ming Li. 2023. Continuous Authentication Using Human-Induced Electric Potential. In *Annual Computer Security Applications Conference (ACSAC '23), December 04–08, 2023, Austin, TX, USA.* ACM, New York, NY, USA, 15 pages. https://doi.org/10.1145/3627106.3627124

1 INTRODUCTION

Terminal devices often contain sensitive information that needs to be protected from unauthorized accesses. To accomplish this, user authentication mechanisms have been developed and implemented. These mechanisms verify a user's identity based on login credentials, such as passwords, facial recognition, and fingerprints, before granting access to the terminal. The verification is executed only at the time of initial login. This can leave the terminal vulnerable to intruders during an active session if the original user leaves the terminal unattended. To address the security flaws of traditional one-time authentication, research has been conducted on *continuous authentication*, also known as *recurring authentication*. It is a verification method that provides identity confirmation on an ongoing basis.

Initial efforts on continuous authentication involve automatically locking the terminal after a period of inactivity. A user needs to re-enter the correct credential to log in again. However, this can be inconvenient for users and does not fully eliminate the risk of unauthorized access before the session expires. Classic approaches use the user's proximity as a decision criterion [9, 10, 15, 16]. If the logged-in user is detected within the terminal's proximity, the terminal is presumably in the user's physical control and remains unlocked. Otherwise, the deauthentication is triggered. The major challenge in this approach is to precisely locate the user at the sub-meter level. Existing solutions mostly use received signal strength (RSS) for distance measurement [9, 10]. Their precision level depends on the employed radio technology. Take Bluetooth Low Energy (BLE) as an example. It only achieves meter-level distance estimation (2-4 m, according to prior study [13]) which is imprecise for proximity-based continuous authentication. While

recent advanced radio technologies, such as ultra-wide band (UWB) and mmWave, have been reported to achieve satisfactory sub-meter level distance estimation [61], they require sophisticated transceiver modules that are not commonly found in commodity devices. Recently, an increasing number of studies utilize physiological signals [11, 12, 27, 28, 38, 40, 42, 64] or behavioral patterns [1, 5, 14, 26, 51, 58] as biometrics for continuous authentication. Appendix 8 provides a comprehensive discussion of them.

Unlike any of the existing approaches, in this work we make use of a new type of signal, *human-induced electric potential*, for continuous authentication. In particular, we find that a certain portion of electric charges are transferred from the screen to the user's body as they touch the screen. This induced electric potential can then be picked up by a wearable in physical contact with the user's body. As shown in our preliminary study (Section 3.2), the signal exhibits a significant correlation with touch events, making it an ideal indicator of user-terminal interactions. Based on this observation, we propose a novel two-factor authentication scheme that adopts a bilateral authentication framework. The user's continued presence is examined by observing her actions from two different sources and cross-checking them. One of them is the realtime measures of the human-induced electric potential, which can be accessed by a self-developed prototype worn by the user. The other is the time-resolved touch events recorded by the target terminal's operating system (OS). Our scheme compares the time sequences of interactions derived from these two sources and checks if they match. If the wearable is worn by the user who provides inputs to the terminal, then the wearable measurement (of the human-induced electric potential) and the terminal's OS readings should be correlated in timing. Conversely, if they no longer correlate, it can be inferred that a different person is now using the terminal.

The above design is called the *basic scheme*. As discussed later, it works well in defending against *innocent adversaries* who accidentally access the target terminal without realizing that another user is already logged in. Nonetheless, it would be defeated by *malicious adversaries* who intentionally mimic the victim user's hand behaviors. To deal with this issue, we develop an *advanced scheme* that further monitors the consistency of the in-use terminal as the second authentication factor, i.e., whether the user switches the terminal during an active session. For this purpose, the advanced scheme recognizes the terminal's identity by analyzing the captured human-induced electric potential by the wearable. It has been validated in prior studies that different hardware exhibits diverse electric characteristics due to manufacturing imperfections [8, 17, 21, 57]. In our case, the pattern of wearable measurements should be consistent if the legitimate user remains on the same terminal. Otherwise, it indicates that the user has made a switch. Therefore, even if an adversary imitates the legitimate user's interaction behavior that produces a time sequence matched with the one generated from the terminal OS, the derived terminal fingerprint would have changed. To sum up, the advanced scheme is a two-factor authentication: It compares the two-source interaction sequences and checks if they match. Additionally, it monitors the in-use terminal's fingerprint consistency by analyzing the wearable measurement. A deauthentication process is triggered if any condition is violated.

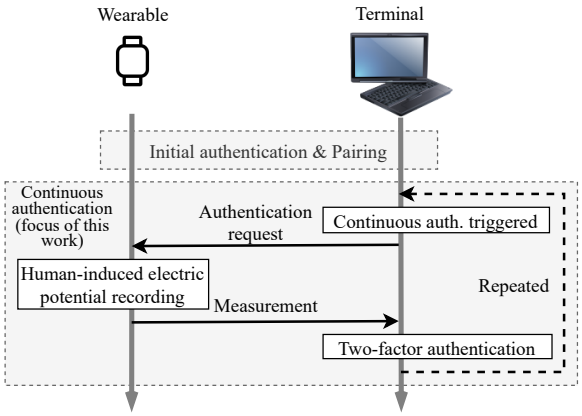

Figure 1: Workflow of the proposed continuous authentication scheme. In this work, we aim to protect target terminals (e.g., all-in-one PCs/laptops, ipad, and tablets) from unauthorized access. The wearable assists with the proposed continuous authentication scheme. The terminal and the wearable are two different parties.

In the technical aspect, our design focuses on (a) detecting critical moments, i.e., screen touch/release, from wearable measurements, and (b) using the same measurement to fingerprint the terminal. To achieve the first objective, we leverage advanced signal processing techniques to develop a series of modules, including envelope extraction, waveform segment, and irrelevant waveform removal. Raw electric measurements are first cleaned and then processed to obtain the timing of touch events. For the second objective, we resort to time-frequency domain analysis. Particularly, we first compute the Gammatone Frequency Cepstral Coefficients (GFCC) from the processed signals as features, then apply the Gaussian Mixtures Model (GMM) for terminal fingerprinting.

Our main contributions are summarized as follows.

- We devise a two-factor continuous authentication scheme that combines examining *what* the user is doing and *which* terminal the user is working on.
- We explore a new type of signal, i.e., human-induced electric potential, to recognize user-terminal interactions. It serves as a reliable source with a high signal-to-noise ratio (SNR) to timestamp touch events. What's more, this signal can be accessed anywhere on the human body, rendering our scheme implementable on a wide range of wearables, an advantage not found in prior wearable-assisted solutions.
- Extensive experiments show that our scheme has a low equal error rate (EER) of 2.3%, which beats state-of-the-art methods. It is also shown robust against various adversaries. Additionally, the presence of illegitimate presence can be detected within 5.1 s. The incurred energy cost at the wearable is as low as 0.02 mAh for the entire authentication procedure.

2 SYSTEM AND ADVERSARIAL MODELS

2.1 System Model

In this study, we consider a shared workspace environment, a prevalent office configuration designed to accommodate multiple professionals, either within the same room or in individual cubicles. This arrangement is widely implemented in various sectors, including businesses, healthcare facilities, and laboratories. We aim to protect the terminals with a touchscreen in such an open work environment from unauthorized access. Take the healthcare workspace as an example. Touchscreen terminals, such as all-in-one PCs/laptops, iPads, and tablets, have become increasingly commonplace in clinics and hospitals [18, 35]. These terminals store sensitive patient information, necessitating robust protection against unauthorized access. Healthcare professionals are typically required to authenticate themselves before using a terminal (e.g., by entering a username and password) and deauthenticate (i.e., log out) upon completion. However, in practice, users often neglect to log out or intentionally avoid doing so to circumvent subsequent log-ins. The failure to log out can have serious consequences: unauthorized individuals may access the terminal to view private information, alter or delete patient data, or steal the logged-in user's credentials to perform actions on their behalf. Even in non-adversarial situations, other authorized users might inadvertently misuse the active user's account if the latter fails to log out. For example, Koppel et al. [23, 24] reported that physicians frequently input data into the incorrect patient's record, assuming that the open record pertained to their current patient, when in reality, another physician had used the terminal to update a different patient's record and neglected to log out. Moreover, clinicians may deliberately leave terminals logged in as a professional courtesy to subsequent users, sparing them the need to log in.

To prevent an intruder from taking control of the target terminal, either unconsciously or intentionally, we adopt a typical continuous authentication framework [12, 27, 29]. The user's identity is continuously verified by the terminal once the user successfully logs in. The terminal keeps unlocked as long as the original user's presence remains; otherwise, the current account is automatically logged off. Our scheme is not an initial authentication, rather it complements any existing initial authentication schemes by providing recurring user authenticity validation and automatic deauthentication.

As shown in Figure 1, our authentication process is triggered when any interaction involving the screen is detected by the terminal. Upon the reception of an authentication request, the wearable worn by the user records the electric potential signals induced by finger touches and sends them to the terminal for further processing. The authentication decision is made at the terminal using the proposed scheme discussed later. The wearable remains inactive if no request is received.

Clarifications. Our scheme operates with assistance from a user's worn wearable. It is worth mentioning that wearable-assisted (continuous) authentication has been explored by both industry [38] and academia [1, 29, 30]. We also acknowledge that the proposed scheme cannot be directly implemented on COTS wearables due to the requirement of capturing human-induced electric potential from the human skin. Still, the scheme presents a practical continuous authentication solution through a customized wearable. This fashion has been widely embraced in the industry, as demonstrated by products like the Nymi Band [38] and Gatekeeper [15]. For example, Nymi Band is a commercial wearable specifically designed for authentication, which computes an employee's unique biometric signal to unlock their computer in the workplace.

2.2 Adversarial Model

The adversary is in the same space as the victim user and has access to the target terminal. Two types of adversaries are considered: *innocent* and *malicious*. An *innocent adversary* is a user who accidentally accesses the target terminal while it is unlocked, without realizing that another user is already logged in. This is a common occurrence in shared workspaces. On the other hand, a *malicious adversary* deliberately uses an unattended terminal with the intent of impersonating the victim to gain access to sensitive information or exploit the victim's account. It may observe the victim's behavior and actions to perform mimic attacks in order to deceive the terminal into falsely authenticating it as the original logged-in user. The adversary is assumed to have direct visual observation or access to a video aid such as a surveillance camera to observe the victim's interaction with the terminal. It is worth mentioning a special kind of *malicious adversary*, called *opportunistic adversary* [19]. Contrary to replicating every individual activity of the victim (e.g., keyboard events) at the authentication terminal, research indicates that an attacker can achieve success by selectively imitating only a portion of the victim's actions. As a result, certain existing bilateral continuous authentication methods (e.g., [29]) may prove inadequate, given the substantial increase in attack success rates associated with this opportunistic approach.

We make the following assumptions throughout the paper. *First*, each wearable is associated with a specific user and users do not share their wearables. The wearable is worn by the owner. If it is taken off, it will be deactivated. The owner is then required to enter a passcode to activate it again. A similar approach has been adopted by Apple Watch. It can effectively prevent potential misuse of the continuous authentication system when the wearable is stolen by another user. *Second*, the wearable and the terminal are paired prior to the continuous authentication, for example, right after the initial authentication. This can be done using suitable pairing methods as a one-time effort. *Third*, the communication channel between the wearable and the terminal is secure. In this work, the BLE communication protocol is adopted.

3 PRELIMINARIES

3.1 Touchscreen Background

A touchscreen is a typical UI that allows users to interact with a terminal using their fingers. It has been equipped to a variety of devices, such as all-in-one PCs/laptops, smartphones, tablets, cash registers, and information kiosks. While there are various sensing touch technologies, mutual capacitive sensing has been the most prominent owing to its high sensitivity, energy efficiency, and low manufacturing cost [41]. It is reported that capacitive screens account for 65% of touchscreen marketshare in 2021 [6]. We thus focus on this type of touchscreen in this work. A capacitive touchscreen consists of a grid of transmitter (TX) and receiver (RX)

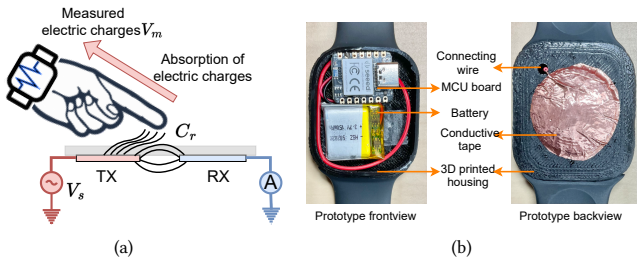

Figure 2: (a) Illustration of how human-induced electric potential is formed and how it is picked up by the wearable. (b) Front- and back-view of the wearable prototype.

electrodes that are mutually coupled. The TX electrodes are driven by an excitation signal with voltage V_s. When a finger touches the screen, some electric charges from the electrode grid are transferred to the human body through a coupling capacitance C_r. This results in the induced electric potential at the human body, which causes a change of the mutual capacitance at the touch point. A touchscreen controller detects this change in the current and reports it as a touch event to the system's OS. The OS then locates the touch point on the screen and timestamps the event. Such information is accessible via designated APIs offered by OS.

Prior research suggests that the human body can be viewed as a conductor with a relatively low impedance [43, 60, 69]. When the finger touches the screen, it absorbs some electric charges from the electric field generated by the driving circuit and forms an electric potential in the human body, known as the *human-induced electric potential*. These charges then traverse through the body. By creating a physical contact (e.g., using an electrode or electric conductor) between the human body and the wearable's analog input (e.g., ADC pin), the device can pick up the charges absorbed by the finger from the touchscreen, as shown in Figure 2(a). The analog input is a common component in commercial off-the-shelf (COTS) wearables that have reading capabilities.

3.2 Feasibility Study

The objective of this part is to investigate the feasibility of utilizing human-induced potential for continuous authentication.

Measurement setup. To measure the human-induced potential, we build a wearable prototype using a Seeed Studio nRF52840 [55] as the microcontroller unit (MCU), as shown in Figure 2(b). A 3D printed housing is created to enclose the MCU and other peripheral components, such as the battery and connecting wires. A conductive tape is attached to the back of the housing case and connected with the board's ADC pin via a connecting wire. The tape establishes physical contact between the human skin and the ADC pin. Then part of the electric charges absorbed from the touchscreen are captured by the prototype. The nRF52840's onboard BLE communication module allows for real-time data exchange between the wearable and the paired terminal. We choose to build our own prototype rather than using COTS wearables, as slight hardware modifications are needed, especially adding a conductive tape and a connecting wire to the ADC pin for interfacing with the human skin. The entire prototype costs less than $30. In the study, a Samsung Galaxy S7+ Android tablet serves as the terminal. The clock

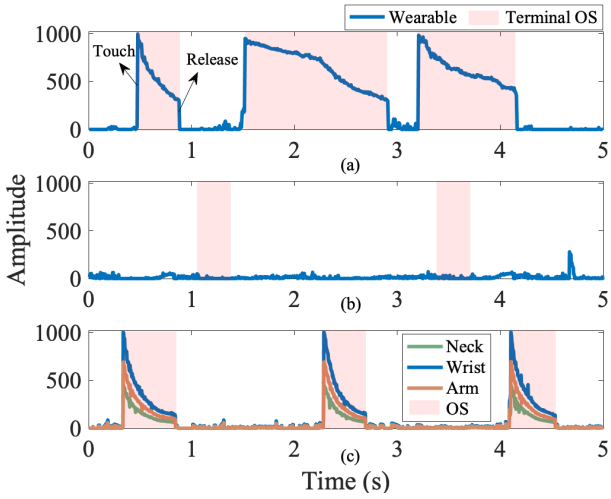

Figure 3: (a) The two-source readings, one from the wearable and the other from the terminal OS, match well in timing when the legitimate user stays on the original logged-in terminal. (b) The readings from both sources become irrelevant when an unauthorized user accesses the target terminal. (c) The readings from both sources match well regardless of where the wearable is placed as long as the legitimate user stays on the original logged-in terminal.

synchronization between the terminal and the wearable is implemented using the classic Flooding Time Synchronization protocol (FTSP) [32].

Relationship between two-source readings. In the first experiment, a user wears the prototype and interacts with the terminal. The interactions can be varied, such as tapping, typing, and swiping. Figure 3(a) shows the readings obtained from the wearable (blue curve) and the terminal OS (red shaded region). Three interactions were performed. In the wearable measurement, the signal peaks occur at the moments the screen is touched, whereas the signal falling edges coincide with finger releases. More importantly, the time sequences of screen onsets and offsets derived from the two sources match well. In a separate experiment, a second user (i.e., an intruder) is asked to interact with the terminal while the legitimate user is away. Figure 3(b) illustrates how the two-source time sequences appear. They are obviously irrelevant to each other. *The result reveals that the time instances of touch events obtained from two sources match well as the legitimate user interacts with the terminal. However, this property vanishes when the terminal is under the control of an intruder.*

Measurements at different parts of a human body. We further ask the user to interact with the terminal while wearing three identical prototypes in different locations: neck, wrist, and arm. As can be seen in Figure 3(c), the variations in the readings across the three locations are highly synchronous: The peak maxima all occur when the user touches the screen, whereas sudden drops exist as the screen is released. Furthermore, they all match well with the touch events recorded at the terminal OS regardless of the wearable's placement, as long as it has direct contact with the user's skin. It is worth noting that the amplitudes of the three measurements differ,

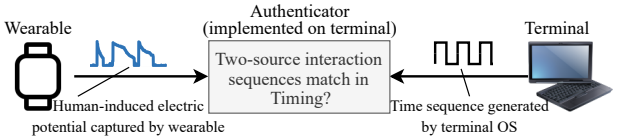

Figure 4: The high-level idea of the basic scheme.

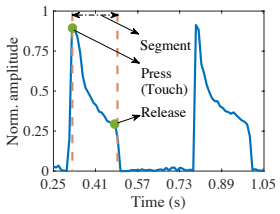

Figure 5: A segment starts from screen touch and ends with release.

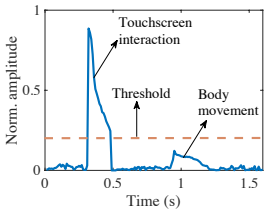

Figure 6: Threshold to remove irrelevant waveforms caused by random movements.

which can be attributed to the corresponding distances between the wearable and the fingertip.

4 BASIC CONTINUOUS AUTHENTICATION SCHEME

Encouraged by the feasibility study, we first present a basic continuous authentication scheme. Its limitation is discussed at the end of this section. To overcome it, an advanced scheme is developed in the next section. The basic scheme serves as a framework and a crucial component of the advanced scheme. To clearly present the entire design, we discuss the basic and advanced schemes separately in an incremental manner.

4.1 Scheme Design

Overview. The basic scheme operates as follows: After the initial login, the terminal continuously verifies the identity of the logged-in user. As the user interacts with the terminal's touchscreen, her wearable captures human-induced electric charges and sends them to the terminal. The terminal then generates a time sequence indicating the moments of touch events, i.e., screen touch and release, based on these readings. Meanwhile, the terminal's OS also generates another time sequence based on the inputs it receives from the touchscreen. The two-source sequences will match in timing, if the current user is still the initial logged-in user, the one with the paired wearable. Otherwise, the terminal is considered to be controlled by an intruder. This is because the sequences are now generated by two distinct sources: The one derived from the wearable measurement still comes from the legitimate user, while the one generated by the terminal OS is now from the intruder's interaction. If a mismatch is detected, the terminal will trigger deauthentication to prevent the intruder from misusing the legitimate user's account.

From a technical standpoint, the basic scheme consists of four main components: *denoising*, *waveform segmentation*, *irrelevant waveform removal*, and *two-source interaction sequence comparison*. In the following, we explain each one in detail.

Denoising. The raw readings at the wearable are mixed with electrical noises from two main sources. The first one is the touchscreen itself. Typically, a touchscreen refreshes at a constant frequency, e.g., 60 Hz or 120 Hz [25, 46]. The alternating driving voltage causes constant radiation that can be picked up by the wearable. The second source is EM interference from the power line, which is particularly apparent in indoor environments. In the US, the frequency of such radiation is 60Hz [39]. These noises introduce small-scale variations to the useful readings. To get rid of them, we propose to extract the envelope using the *Hilbert function* [33]. Specifically, a sliding time window is applied over the raw reading. The local maximal value within this window is deemed as the filtered output for the window [34]. Note that other strong EMIs (e.g., WiFi/cellular) operate at a much higher frequency band, e.g., GHz, and would not cause any interference in our case.

Waveform segmentation. The purpose of this step is to segment the signal for each interaction out of a continuous waveform. We first identify critical time instances associated with finger touch/release events. Finger touches correspond to the measured peaks according to the discussion in Section 3.2. We thus apply the classic peak detection algorithm [4] on the envelope signal to identify these events. Once the finger leaves the screen, the decoupling causes a sudden drop in the electric readings as shown in Figure 5. Hence, the finger release event is identified by locating the most negative derivative between two consecutive peaks when the signal amplitude experiences the most significant drop. Upon identifying these critical events, the electric signal of one interaction is the waveform segment between the adjacent finger touch and release as indicated in Figure 5.

Irrelevant waveforms removal. We observe in our experiments that regular hand/body movements can also cause variations in the measurement as shown in Figure 6. This is because EM radiations are ubiquitously present in open space. Typical sources include FM/AM radio stations, power systems, and a wide variety of electronic equipment. Under the hand/body movement, the conductive property of the user's body changes, resulting in changes in the electric measurements at the wearable. These signals can impact the accuracy of touch event detection and should be removed. Our experiment results show that the amplitude of the signal caused by hand/body movements is significantly lower than that caused by touchscreen interactions. This confirms our expectation that the radiation from the touchscreen is stronger than the ambient EM radiation in the open air. To distinguish between the useful signal (from interactions) and the noise caused by hand/body movements, we first perform a statistical analysis of the latter. Specifically, we calculate its average μ and standard deviation σ. Then, we set a threshold $\mu + 2\sigma$, 2 standard deviations above the average profile. If a waveform segment exceeds this threshold, it is considered to be generated by interactions; otherwise, it is treated as noise from irrelevant movements and discarded.

Two-source interaction sequence comparison. In the end, we are able to derive a time sequence from the wearable's electronic measurement during the wearer's interactions. This sequence is represented as $S^w = \{(t^w_{p,1}, t^w_{r,1}), (t^w_{p,2}, t^w_{r,2}), \cdots\}$, where the subscript

w stands for readings from the wearable, t_p^w and t_r^w represent the time instances of screen touch and release, respectively, and the numbers are their indices. The sequence S^w is wirelessly transmitted from the wearable to the terminal. Similarly, another time sequence $S^d = \{(t_{p,1}^d, t_{r,1}^d), (t_{p,2}^d, t_{r,2}^d), \cdots\}$ is obtained at the terminal's OS. By comparing these two sequences of interactions, the terminal verifies whether the user interacting with the terminal is the initially logged-in user. If it is, the two sequences S^w and S^d should match well in the timing; otherwise, they are barely correlated. Once a mismatch between the two-source sequences is detected, the terminal triggers deauthentication, such as logging out the current user and locking the screen.

4.2 Discussions of the Basic Scheme

The basic scheme is effective against the innocent adversary, i.e., users who accidentally access the terminal. The corresponding security analysis is provided in Section 6. However, it is not completely resistant to malicious adversaries in certain situations. For example, in a shared workspace with multiple terminals, a victim user may temporarily switch to another terminal, leaving the original terminal unattended. An adversary can exploit this time window to stealthily access the victim's original terminal. Assume that both the victim and the adversary are working on similar tasks, say, filling out forms. Then it becomes possible for the adversary to mimic the victim's interactions, particularly the timing of screen touch/release. As a result, the adversary can generate an interaction sequence at the terminal's OS that may match the one derived from the victim's wearable electronic measurements. This would cause the basic scheme to wrongly classify the adversary as the original logged-in user. As discussed in the adversarial model, the adversary is assumed to have either direct visual observation or access to a video aid, such as a surveillance camera, to target the victim's hand movements. These types of attacks are possible in a realistic scenario, as a malicious adversary can be motivated and trained to mimic how people interact with terminals. Therefore, the odds of an experienced adversary defeating the basic scheme would be non-negligible.

5 ADVANCED CONTINUOUS AUTHENTICATION SCHEME

Given the limitations of the basic scheme, we propose an advanced scheme that addresses them. In addition to comparing the timing of two-source interaction sequences, the advanced scheme also examines if the in-use terminal has been switched by analyzing the signal patterns of the captured human-induced electric potential. It will be clear soon that the pattern should be consistent if the original logged-in user remains on the same terminal. Otherwise, it implies that the original user has switched to another terminal. Note that the advanced scheme is our final design. Before we delve into the technical details of the advanced scheme, we first present a phenomenon that is essential for our design.

5.1 Terminal Fingerprinting Using Human-Induced Electric Potential

The characteristics of emitted electric charges from touchscreens, such as their amplitude and frequency, vary across terminals. This

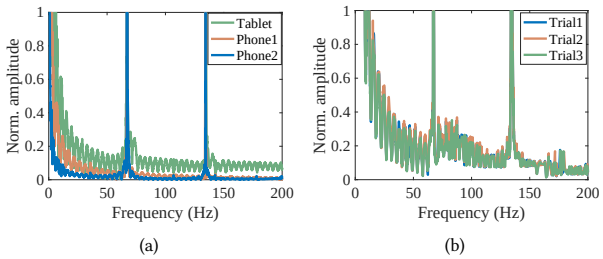

Figure 7: (a) Frequency responses of three terminals are distinguishable. (b) Frequency responses are similar in three trials on the same terminal.

is due to the terminal's unique mechanical and electronic features formed during manufacturing, which is referred to as *manufacturing imperfection* [8, 17, 21, 57]. These imperfections commonly found in various analog circuitry components in electric devices and equipment. The imperfections are terminal-specific and manifest themselves as artifacts of the emitted signals.

As discussed in Section 3, when a user taps on the touchscreen, the finger extracts electric charges from it and some of them are then picked up by the wearable. Hence, the wearable measurement reflects the terminal-specific imperfection. In this work, we propose to leverage these minute imperfections of hardware to fingerprint terminals. Specifically, if a user works on the same terminal, the pattern of wearable's electric measurement should be relatively consistent; if the user switches to another terminal, the pattern would experience some changes before/after the switch. To validate the feasibility of this idea, we perform some preliminary experiments with our wearable prototype. Three terminals are tested, including one Samsung S7+ tablet and two LG V30 smartphones. To eliminate the influence introduced by user behaviors, the subject simply rests the index finger on the screen in all trials. The frequency-domain representation of three measurements with three different terminals are plotted in Figure 7(a). It can be seen that their frequency components are distinguishable. For example, the signal from the tablet exhibits a higher amplitude in the frequency range [0, 200 Hz] than the other two. The difference even exists between the two phones of the same model. Figure 7(b) further shows the measurements in three trials over the same terminal Samsung S7+ tablet. Their patterns are highly similar, which is as expected. This phenomenon motivates us to harness the wearable-captured human-induced electric potential for terminal fingerprinting; the measurement provides evidence of whether a user has changed the terminal or not after initial login.

5.2 Scheme Design

Overview. We enhance the basic scheme by introducing an additional layer of protection. In addition to verifying the correlation of the two-source interaction sequences, it also monitors the pattern consistency in the wearable electric measurement. The user's continued presence is validated only when both conditions are met. Specifically, once the terminal receives measurements from the wearable, it first checks if the timing of interactions obtained from two sources matches. If not, deauthentication is triggered. This is identical to the basic scheme. If the two-source sequences

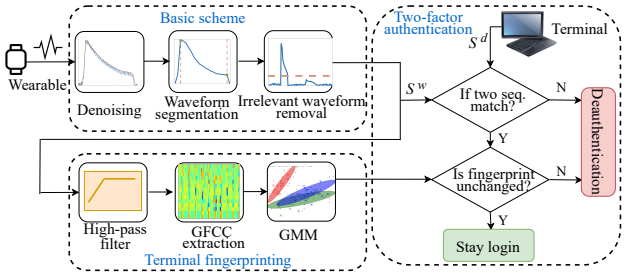

Figure 8: Overview of the advanced continuous authentication scheme.

match, the terminal further examines if the signal pattern, derived from the same wearable measurement, is consistent with the one recorded during initial login. If it is, the user is on the same terminal where she was initially authenticated. It not, the user has switched terminals; the deauthentication is then triggered. In summary, the advanced scheme is two-factor continuous authentication that not only keeps on checking *what* the user is doing but also *which* terminal the user is interacting with.

Next, we focus on the technical design of terminal fingerprinting.

GFCC Feature extraction. To characterize the electric measurement at the wearable, we resort to the signal presentation in the time-frequency (T-F) domain. In particular, the Gammatone Frequency Cepstral Coefficients (GFCCs) are adopted. The GFCC is derived by decomposing the input signal into the T-F domain using a bank of Gammatone filters, followed by a down-sampling operation of the filter-bank responses along the time dimension. GFCCs are one of the most commonly used features in speech and speaker recognition [48, 66, 67]. It is employed here owing to its high resolution at low-frequency bands and its resilience to noise [7]. To extract GFCC from the electric signals, we first divide the processed waveform signals into overlapping frames. Each frame has a duration of 250 ms. The overlap fraction f takes the value from $[0, 1)$, 0 being no overlap. GFCC is calculated for each frame. Due to the hardware restriction, a lightweight MCU board with BLE connection module cannot perform too-high sampling as otherwise realtime communication via BLE tend to be unreliable. In our implementation, we adopt a sampling rate of 400 Hz. According to the *Nyquist theory*, we are able to obtain frequency-domain features below 200 Hz. To facilitate low-frequency feature extraction, a *filterbank* is created by dividing the 0-200 Hz frequency into multiple non-overlapping bands called filters. A filterbank is an array of bandpass filters that separate the input signal into multiple components, each one carrying a single frequency sub-band of the original signal. The filterbank centre frequencies are distributed across frequency in proportion to their bandwidth, known as the Equivalent Rectangular Bandwidth (ERB) scale [37]. ERB scale provides an approximation as how bandwidths of filters should be divided. We then calculate the log-energy for each filter. The final GFCC coefficients are obtained by applying a Discrete Cosine Transformation (DCT) on the output of each filter, to magnify the subtle changes in the lower frequency bands. We extract 10 GFCC as features using a 10-Gammatone filterbank. We also use GFCC *delta* and GFCC *delta-delta* as features, which capture the rate of change between two consecutive GFCC and GFCC delta coefficients respectively. In total, we adopt 30 features. Take an interaction of 1-second duration as an example. Let $f = 0.5$. Then there are a total of 8 frames, each with a duration of 250 ms. Since 30 GFCC features are derived from each frame, then 240 features are derived for this interaction.

User interactions introduce an additional dimension of uncertainty to the electric signal due to the behavior diversity. To eliminate its impact, we propose to apply a high-pass filter with a cutoff frequency of 15 Hz to the signal before calculating its GFCC. According to a prior study [3], human finger-tapping speed is upper-bounded by 61 taps for 10 seconds. We select 15 Hz as a conservative value to accommodate users with all kinds of typing styles and speeds. This step ensures that the GFCC features are user-independent and thus more accurate for terminal fingerprinting.

Terminal fingerprinting using GMM. The next step in the pipeline is to decide if the obtained GFCC features are from the original terminal where the user was initially authenticated. We adopt the *Gaussian Mixtures Model* (GMM) as a classifier. We pick GMM over the Support Vector Machine model (SVM) because the inputs in our case have variant sizes. Although Dynamic Time Warping (DTW) is also capable of clustering time series that vary in length, GMM has shown to outperform DTW in recognition and classification tasks [22, 44]. GMM is a probabilistic model, which assumes that all the data points from the same class are generated from a mixture of a finite number of Gaussian distributions. Each Gaussian distribution has its own mean and covariance and is called a *component* in the GMM model.

Consider a set of GFCC features $\boldsymbol{x}$ obtained by one or multiple interactions. Our terminal identity recognition task can be formulated as a hypothesis test between

- λ_{hyp}: feature set $\boldsymbol{x}$ is from the original terminal;
- $\lambda_{\overline{hyp}}$: feature set $\boldsymbol{x}$ is not from the original terminal.

The verification test to decide between these two hypotheses is a log-likelihood ratio test given by

$$\Gamma(\boldsymbol{x}) = \log \frac{p(\boldsymbol{x}|\lambda_{hyp})}{p(\boldsymbol{x}|\lambda_{\overline{hyp}})} \begin{cases} \geq \theta, & \text{Accept hypothesis } \lambda_{hyp} \\ < \theta, & \text{Reject hypothesis } \lambda_{hyp} \end{cases} \quad (1)$$

where $p(\boldsymbol{x}|\lambda)$ is the probability density function (pdf) and θ is the decision threshold. For a feature vector $\boldsymbol{x}$, the mixture density used for the likelihood function can be written as $p(\boldsymbol{x}|\lambda) = \sum_{i=1}^{K} w_i p_i(\boldsymbol{x})$, where $p_i(\boldsymbol{x})$ is the individual Gaussian density function $\mathcal{N}(\boldsymbol{\mu}_i, \boldsymbol{\sigma}_i)$, and w_i is the mixture weight with $\sum_{i=1}^{K} w_i = 1$. $\boldsymbol{\mu}_i$ and $\boldsymbol{\sigma}_i$ are the mean vector and covariance matrix, respectively. Once the parameters $\{w_i, \boldsymbol{\mu}_i, \boldsymbol{\sigma}_i\}$ of $p(\boldsymbol{x}|\lambda)$ are fixed, the classification decision can be made for an given $\boldsymbol{x}$ using (1).

The parameters of $p(\boldsymbol{x}|\lambda_{hyp})$ and $p(\boldsymbol{x}|\lambda_{\overline{hyp}})$ are estimated using the collected GFCC feature vectors from the original terminal (i.e., the terminal itself) and reference terminals (i.e., other terminals), separately. The estimation is performed using the iterative expectation-maximization (EM) algorithm [36] and is done offline. During the authentication, the incoming electric signal is divided into 250 ms frames. Time-series GFCC features are extracted $\boldsymbol{X} = \{\boldsymbol{x}_1, \boldsymbol{x}_2, \cdots \boldsymbol{x}_T\}$. Then the log-likelihood of a model λ for $\boldsymbol{X}$ is

calculated as

$$\log p(\boldsymbol{X}|\lambda) = \sum_{t=1}^{T} \frac{1}{T} \log p(\boldsymbol{x}_t|\lambda).$$

The log-likelihood value is divided by T to normalize out duration effects from inputs with variant sizes.

5.3 Parameter Considerations

The authentication performance is mainly fine-tuned by three parameters: *synchronization tolerance* (Δt), *window size* (w), and *match threshold* (ρ). While FTSP is employed to align the clocks at the wearable and the terminal, clock synchronization is not perfect in practice. Timing mismatches are occasionally observed through the tests, mostly within 200 ms. To alleviate false alarms caused thereby, we adopt a common practice to introduce a parameter *synchronization tolerance* Δt [49, 60, 62]. The two time sequences are deemed matched as long as the pair-wise element comparison holds within Δt. The *window size* w is the number of interactions the authenticator considers to reach a decision. For each window the authenticator applies the pair-wise element comparison to compute a matching score indicating how well the two sequences match in that window. If the score is higher than the *match threshold* ρ, they match; otherwise, they do not. We set ρ as the fraction of interactions in a window that should match for the authenticator to decide the user's legitimacy. We are going to examine the impact of these parameters in Appendix A.

6 SECURITY ANALYSIS

In this section, we perform analytic evaluation regarding the security performance with reference to the adversarial model.

Innocent adversary. An innocent adversary is a user who uses an unattended terminal inadvertently without realizing that another user (i.e., legitimate user) is already logged in. We consider the following three cases based on the legitimate user's behaviors. *In the first case*, the legitimate user is performing random activities, e.g., walking to a different cubic or grabbing snacks nearby. As shown in Figure 6, while variations are observed in the received signal at the wearable, its amplitude is much lower than when the legitimate user interacts with the terminal. The component of *irrelevant waveform removal* of our scheme eliminates these signals. The filtered signals would not produce any time sequence. Consequently, the two-source timing comparison fails. *In the second case*, the legitimate user is touching a conductive surface, e.g., using smartphones or working on another terminal. The time sequence of user's interactions (with the conductive surface) can still be obtained at the wearable, but it is unlikely to correlate with that produced by the adversary at the terminal. As a result, the two-source timing comparison would fail too. *In the third case*, the legitimate user walks out of the terminal's vicinity, causing the wearable to lose its connection with the terminal. Since no measurement is received from the wearable, the time sequence comparison fails. In all these cases, the deauthentication will be triggered, logging out the current account and locking the screen immediately.

From the discussion above, it can be inferred that the detection of the innocent adversary is based on the comparison of two-source interaction sequences in timing. As both the basic and advanced schemes have this module, they are effective in detecting and preventing the actions of an innocent adversary.

Malicious adversary. We further analyze how the advanced scheme can defend against malicious adversaries, including opportunistic adversaries. A malicious adversary can observe the actions of the victim user and imitate her hand movements made while interacting with another terminal, e.g., the victim's smartphone or any other device with a touchscreen in a shared workspace. To pass the timing matching, the adversary performs screen touches/releases at the correct moments mimicking the victim's actions. As discussed earlier, the chance of success is non-negligible for an experienced attacker who has been trained to mimic how people interact with terminals. Fortunately, our advanced scheme introduces an additional defensive layer by taking into consideration the terminal fingerprint, a unique identifier for each terminal. As the terminal changes, the pattern of wearable signals changes accordingly, as elaborated in Section 5.1. Although the adversary may produce a matched time sequence, fabricating the electronic characteristics of the terminal would pose a considerable challenge. This holds true for opportunistic adversaries as well. Consequently, the advanced scheme remains capable of detecting the presence of such adversaries.

7 EVALUATION

The evaluation of the proposed scheme is conducted using the prototype as described in Section 3.2. Five terminals are used, including Google Pixel 6 Pro, Samsung Galaxy S10, Galaxy S8, Pixel 5a, and the Samsung Galaxy S7+ tablet. The evaluation consists of two phases. The goal of phase-I study is to determine the optimal system parameters that deliver the best overall performance. (Details are given in Appendix A.) Once they are identified, the phase-II study is carried out to evaluate the real-world performance of our scheme. To facilitate evaluation, we adopt several commonly used metrics: false acceptance rate (FAR), false rejection rate (FRR), equal error rate (EER). A wide range of impact factors are thoroughly examined. A comprehensive comparison is made with state-of-the-art solutions.

The participants are recruited through various methods, such as emails, social media postings, and verbal communications. Efforts have been made to recruit a diverse population based on age, gender, and race. A total of 25 participants, including 15 males and 10 females, are recruited. Before each experiment, participants are also asked to fill out the informed consent document. It provides a detailed description of the study's procedure, compensation, possible risks, and rights. Participants are free to take a break or quit at any time without penalty. The entire study is IRB-approved. Upon completion of the two phases, each participant is asked to take a short survey to assess the perceived usability of our scheme. The survey result is presented in Appendix D. Besides, participants are asked to wear the prototype with a reasonably snug fit to maintain the necessary skin contact for accessing human-induced potential readings.

7.1 Performance Against Adversaries

In this part, we evaluate the performance against adversaries, including both the innocent adversary and the malicious adversary.

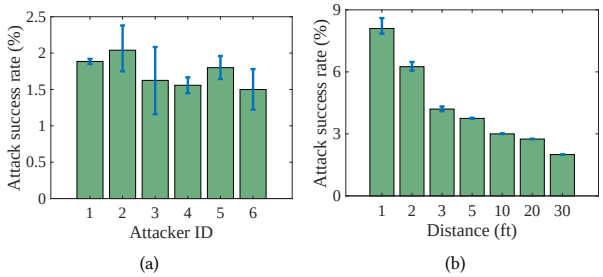

Figure 9: Attack success rate of (a) innocent adversary and (b) malicious adversary.

Robustness against the innocent adversary. An innocent adversary is a user who happens to use an unattended terminal inadvertently. Six pairs of subjects participate in the experiment. In each pair, the two take turns to play as the innocent adversary, with the other as the legitimate user. The attackers simply interact with the target terminal with no intention of mimicking the legitimate user. The legitimate user can freely a) perform random activities, b) interact with a second terminal, or c) walk around. It resembles the three scenarios discussed in Section 6. For each pair, the experiment is repeated 80 times. Figure 9(a) depicts the success rate across six pairs. It is consistently low, ranging between 1.5% to 2%. Hence, the odds are rare for an innocent adversary to act synchronously with the legitimate user without any side information.

Robustness against the malicious adversary. The same set of subjects participate in the experiment. The adversary has a direct line of sight observation of the victim subject. The former is asked to mimic the latter's typing interactions on the original terminal, when the latter interacts with a second terminal. Figure 9(b) depicts the attack success rate by varying the observation distance from 1 to 30 feet. The maximum success rate 8.5% exists when the distance is at 1 ft. Compared with the innocent adversary, the malicious one passes the authentication at a higher chance, which meets our expectation. Still, its advantage is marginal thanks to the proposed terminal fingerprinting component. We also observe that the adversary's performance gain vanishes quickly as the observation distance increases. In particular, its success rate is almost similar to that of the innocent adversary when the distance becomes 20 ft or larger.

Detection efficiency. It is desirable to detect the presence of an adversary on the terminal quickly, so we can prevent any accidental or intentional misuse of the logged-in user's account. We call it *detection efficiency*. Figure 10(a) plots the cumulative distribution function (CDF) of time needed for adversary detection, as a result of 476 trials. The time ranges between 2.8 s and 5.1 s, with 90% of illegitimate presence spotted within 4.3 s. The detection efficiency is practically satisfactory. This metric is partially determined by the window size (w), i.e., the number of interactions needed to make a decision. The window size is set to 4 per the discussion of Appendix A.

The time to perform the 4 interactions varies in accordance with the interaction types and the context. As a controlled study, we further measure how long a legitimate user remains authenticated under the proposed scheme. Participants are asked to freely interact with the terminal as they would normally. The total length of each trial is 5 min, which covers the duration for most common

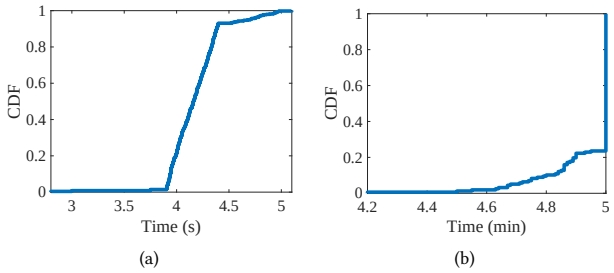

Figure 10: Detection efficiency. (a) CDF of how soon an adversary's presence is detected. (b) CDF of how long a legitimate user remains authenticated.

Table 1: Performance comparison with ZEBRA [29].

	Our scheme				ZEBRA			
Window size	2	3	4	5	5	7	9	11
FAR (%)	1.5	2.8	4.3	4.7	27.5	25	22.5	21
FRR (%)	11.2	7.5	4.5	3.9	6	4.5	3	2.8

interactions, such as typing a message or composing an email. We find in Figure 10(b) that around 5% of participants are wrongly deauthenticated within 4.6 min. The percentage increases slightly as time proceeds. The majority (78%) of the participants remain logged in even for the total duration of 5 min, with the 90% percentile at 4.85 min. Combining the results above, we infer that the detection can be performed efficiently without sacrificing usability.

7.2 Comparison with Prior Works

We further compare the performance with prior works. For a fair comparison, we directly cite the results from these works. Table 1 compares with ZEBRA [29] in terms of FAR and FRR with respect to window size. In ZEBRA, a user wears a bracelet equipped with IMU sensors to track the user's hand movement. ZEBRA utilizes IMU readings to infer the time sequence of interactions. As shown, our scheme beats ZEBRA by a large margin given the same window size. For example, ours produces FAR=4.7% and FRR=3.9% while ZEBRA produces FAR=27.5% and FRR=6% when the window size is 5. Note that a larger window size corresponds to a longer authentication time. There is a trade-off between the authentication time and the accuracy. Ideally, the authentication accuracy comparison should be made given the same window size between the two schemes. ZEBRA adopts a minimum window size of 5, as its accuracy becomes unsatisfactory with a smaller window. In contrast, ours performs reasonably well even when the size is as small as 2. The superiority of our scheme is due to the fact that human-induced electric potential can timestamp touch events more precisely than IMU readings.

Table 2 compares the detection efficiency, i.e., the time duration to detect an adversary. Ours is the fastest; its 90 percentile is 4.3 s. Regarding ZEBRA, as IMU readings tend to be noisier, it takes a longer duration to reach a decision. Its 90 percentile is around 8 s. For [12], it exploits eye movements as biometrics for user identification. Its 90 percentile is around 40 s. Prior work [63] also leverages eye movement to monitor user's continued presence.

Table 2: Performance comparison on detection efficiency.

Schemes	Eberz et al. [12]	Our scheme	*ZEBRA* [29]	Zhang et al. [63]	Segundo et al. [40]
Time (s)	≈40	4.3	≈8	≈125	1

Differently, eye movement is driven by implicit visual stimuli. The whole process takes around 125 s. The approach [40] employs facial recognition for identity recognition. It is the fastest among the four for taking only 1 s to detect the adversary. Note that not all terminals are equipped with a camera. Besides, keeping cameras on all the time, especially in a shared workspace, would cause severe privacy concerns.

7.3 Evaluation Under Various Scenarios

Impact of different touch gestures. Users interact with the terminal via various touch gestures. It is essential to ensure that authentication is robust to touch diversity. Figure 11(a) shows the result. Three common touch gestures are evaluated: tap, swipe, and pinch. We find that tap has the best performance with an average FAR and FRR of 1.9% and 2.5% respectively. FRR for pinch is a little bit higher. It is probably due to the complexity of the gesture involving two fingers, as opposed to single-finger gestures. Besides, FAR remains stable for all gestures. It implies that touch gestures do not affect the security performance of our scheme.

Impact of wearable positions. In this set of experiments, we evaluate the impact of device placements on the body surface. Several locations are examined, including the head, wrist, arm, and finger. Figure 11(b) shows that FRR and FAR are relatively stable for all locations. This is because the received electric charges at different locations of the body experience similar varying tendencies, as the user touches/releases the screen. The result agrees with our feasibility study in Section 3.2. This is a desirable property as the wearable is not restricted to specific locations on the human body. In comparison, many prior works [1, 29, 30, 65] require the wearable to be wrist-worn to access meaningful readings. Their deployment is thus largely confined.

Impact of body movements. We observe in the preliminary study that hand/body movements would cause variations in the wearable's measurement. Luckily, those variations are associated with weaker amplitudes than those caused by touch events. Motivated by this phenomenon, in the design we develop a module that removes irrelevant waveforms caused by body movements, as mentioned in Section 4. In the experiments, we consider four typical movements, including sitting, grabbing a book, drinking from a mug, and making a turn. The corresponding FAR/FRR is depicted in Figure 11(c). We find that the best performance is achieved at the sitting status with the averaged FAR=1.5% and FRR=3.2%, while moving actions slightly bring up the error rate. Still, the authentication accuracy is practically acceptable. It validates the efficacy of the proposed module. Some prior works [29, 30] make use of IMU readings to characterize hand movements. They cannot tell which readings are associated with intended interactions and which are caused by random hand/body movement. The polluted readings easily degrade the authentication accuracy especially when the user is not completely static.

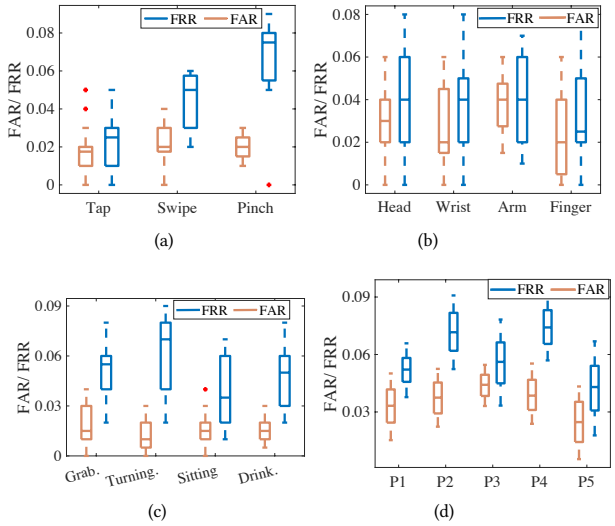

Figure 11: Impact of (a) touch gestures (b) wearable positions (c) body movements, and (d) device heterogeneity.

Impact of different devices. To evaluate the impact of different devices, the proposed scheme is implemented on a variety of terminals, including Google Pixel 6 Pro (P1), Samsung Galaxy S10 (P2), Galaxy S8 (P3), Pixel 5a (P4), and the Samsung Galaxy S7+ tablet (P5). Note that the wearable prototype is the same for all experiments. According to Figure 11(d), the performance remains stable across devices. It indicates that the proposed scheme is terminal-agnostic and can be widely deployed.

Impact of skin conditions. Users may interact with the terminal while their finger skin is exposed to varying degrees of moisture, such as after hand-washing or due to perspiration. To assess the impact of these conditions, we conduct experiments involving different skin states (dry, moderately wet, and soaked). In order to replicate real-world scenarios, water is sprayed onto the hands of the user to achieve the desired levels of wetness. Table 3 presents the results of the experiment. As the finger becomes wetter, we observe a decline in authentication accuracy. Nevertheless, the overall performance remains practically acceptable even when the finger is moderately wet, with FAR and FRR measuring 3.84% and 8.33%, respectively. This can be attributed to the fact that a wet finger distributes the electrical charge over a larger area, rather than focusing it at the point of contact. Consequently, the capacitive touchscreen may struggle to detect the exact location of the touch or might fail to register the touch altogether. It is worth noting that manufacturers typically advise against using terminals with touchscreens while hands are wet, as the terminal may have difficulty recognizing touch inputs from a wet hand.

Due to the limited space, we present the ablation study, evaluation of system performances, and the user study in Appendix B, C, and D, respectively. Particularly, in the ablation study, the performance is compared between the basic scheme and the advanced scheme to understand the contribution of the terminal fingerprinting component. We examine computation time and energy

Table 3: Performance comparison on different skin conditions.

Skin condition	Dry	Moderately wet	Soaked
FAR (%)	3	3.84	7.82
FRR (%)	3.5	8.33	21.6

consumption of the proposed scheme in the evaluation of system performances. The user study analyzes participant's subjective opinions on our proposed scheme.

8 RELATED WORK

We focus on discussing prior works on continuous authentication. In general, they can be classified into the following three categories.

Physiological biometrics based mechanisms. Physiological biometrics have been widely investigated for continuous authentication [11, 12, 27, 28, 38, 40, 42, 64]. For example, Cardiac Scan [27] leverages geometric and non-volitional features of cardiac motion for identity recognition. There are also works using photoplethysmography (PPG) signals [64] and eye movement [11, 12] to verify user's continued presence. However, all these schemes require dedicated sensors (e.g., PPG, Doppler radar sensors, or eye trackers), which are not readily available in most commodity devices. Some schemes utilize electrocardiogram (ECG) [28, 38]. Despite the availability of ECG signals on some COTS devices, their applicability for user authentication has been subject to scrutiny. An individual's ECG patterns may exhibit considerable variations depending on her physical activity, such as when she is seated in contrast to walking. Rasmussen et al. used human body bio-impedance for continuous authentication [42]. A metal keyboard sends small electric current through the user's body; the user's identity is verified by examining his body's resistance to the current. It is well-known that the body bio-impedance can be altered by a variety of factors, such as instant body movement, skin moisture level, and even the wearing clothes [47]. Hence, its performance stability is not guaranteed. Segundo et al. employed facial recognition for continuous authentication using cameras [40]. First of all, keeping cameras on all the time, especially in a shared workspace, would cause severe privacy concerns. Besides, it depletes the battery-powered terminal's battery quickly. Our scheme does not have these limitations.

Behavioral biometrics based mechanisms. They can be classified into gait-based methods [52, 59], keystroke-based methods [1, 58], touch gesture-based methods [5, 14, 26, 51], and the combination of multi-modal behavioral biometrics [45, 50, 54]. Gait-based methods identify individuals by the manner of walking using the target device's IMU readings. They work only when users are moving so that motion sensors can produce meaningful measures for authentication. Keystroke-based methods exploit the phenomenon that users exhibit distinctive keystroke dynamics, such as typing frequency, hold time, finger pressure, pressed area size, etc., when interacting with an end device. The touch gesture-based methods share a similar idea. Nonetheless, both keystroke and touch gesture-based methods have been criticized for being incapable of handling users' behavior dynamics. For example, the behavioral patterns for web browsing and playing games are totally different.

Other approaches. The timeout solution is widely adopted in numerous commodity devices, where a terminal is automatically locked if left idle for a specified duration. However, this approach fails to mitigate risks entirely before the timeout occurs. Prior research has explored utilizing the relative distance between the terminal and the logged-in user for authentication purposes, with the target terminal remaining unlocked when the user is detected within close proximity [9, 10, 16]. The primary challenge in this approach lies in accurately measuring proximity at a sub-meter level. Conventional methods rely on received signal strength (RSS) to estimate distance; however, commonly used radio technologies in terminal devices, such as Wi-Fi [31, 68] and Bluetooth Low Energy (BLE) [13], only provide meter-level distance estimation. Furthermore, radio frequency signals are dynamic and highly variant due to mutual interference and multi-path effects. As a result, approximation-based solutions have faced criticism for their unreliability and high authentication error rates [29, 53]. It is worth noting the Auto Unlock feature offered by Apple [2]. It enables users to unlock their Mac computers when they are in close proximity while wearing their Apple Watch. However, it does not solve the key problem–when to execute the deauthentication.

A more comprehensive comparison with prior works is given by Table 5 in Appendix E.

9 CONCLUSION

In this work, we investigate the feasibility of leveraging a new form of signal, human-induced electric potential, for continuous authentication. We find this signal superior in timestamping touch events by exhibiting sharp rises and falls in its waveforms as the user interacts with the terminal. This property renders the two-source timing comparison, a crucial component of our design, highly precise. Additionally, the unique patterns embedded in the signal allow for fingerprinting the in-use terminal. We exploit this phenomenon to resist malicious adversaries who intend to mimic victim user's touch behavior to gain authentication. Furthermore, as the human-induced electric potential is observable throughout the human body, the wearable can be placed anywhere as long as it has physical contact with the skin. Through an extensive evaluation involving 25 participants, we observe an average EER of 2.3% with our scheme. In conclusion, we believe our design is a competitive candidate for practical adoption.

ACKNOWLEDGEMENTS

We sincerely thank the anonymous reviewers for their insightful comments and valuable suggestions. The work of M. Li is supported by National Science Foundation (NSF) CNS-1943509. The work of P. Li is supported in part by NSF EEC-2133630 and CNS-2125460. The work of W. Jin is supported by National Natural Science Foundation of China (NSFC) Grant 62202150.

REFERENCES

[1] Abbas Acar, Hidayet Aksu, A Selcuk Uluagac, and Kemal Akkaya. 2018. WACA: Wearable-assisted continuous authentication. In *IEEE Secur. Priv. Workshops*. 264–269.

[2] Apple. 2023. Unlock your mac with apple watch. https://support.apple.com/guide/watch/unlock-your-mac-with-apple-watch-apd4200675b8/watchos. (2023).

[3] Çağatay Barut, Erhan Kiziltan, Ethem Gelir, and Fürüzan Köktürk. 2013. Advanced analysis of finger-tapping performance: a preliminary study. *Balk. Med. J.* 2013, 2 (2013), 167–171.

[4] Eli Billauer. 2023. Peak detection. http://www.billauer.co.il/peakdet.html. (2023).

[5] Cheng Bo, Lan Zhang, Xiang-Yang Li, Qiuyuan Huang, and Yu Wang. 2013. Silentsense: silent user identification via touch and movement behavioral biometrics. In *Proc. Annu. Int. Conf. Mobile Comput. Netw. (MobiCom)*. 187–190.

[6] Fortune business insights. 2023. Touch Screen Display Market Share & Growth | Forecast. https://www.fortunebusinessinsights.com/touch-screen-display-market-105362/. (2023).

[7] Jagmohan Chauhan, Yining Hu, Suranga Seneviratne, Archan Misra, Aruna Seneviratne, and Youngki Lee. 2017. BreathPrint: Breathing acoustics-based user authentication. In *Proc. Annu. Int. Conf. Mobile Syst. Appl. Serv. (MobiSys)*. 278–291.

[8] Yushi Cheng, Xiaoyu Ji, Juchuan Zhang, Wenyuan Xu, and Yi-Chao Chen. 2019. Demicpu: Device fingerprinting with magnetic signals radiated by cpu. In *Proc. ACM SIGSAC Conf. Comput. Commun. Secur. (CCS)*. 1149–1170.

[9] Mark D Corner and Brian D Noble. 2002. Zero-interaction authentication. In *Proc. Annu. Int. Conf. Mobile Comput. Netw. (MobiCom)*. 1–11.

[10] Mark D Corner and Brian D Noble. 2003. Protecting applications with transient authentication. In *Proc. Annu. Int. Conf. Mobile Syst. Appl. Serv. (MobiSys)*. 57–70.

[11] Simon Eberz, Giulio Lovisotto, Kasper B Rasmussen, Vincent Lenders, and Ivan Martinovic. 2019. 28 blinks later: Tackling practical challenges of eye movement biometrics. In *Proc. ACM SIGSAC Conf. Comput. Commun. Secur. (CCS)*. 1187–1199.

[12] Simon Eberz, K Rasmussen, Vincent Lenders, and Ivan Martinovic. 2015. Preventing lunchtime attacks: Fighting insider threats with eye movement biometrics. In *Netw. Distrib. Syst. Secur. Symp. (NDSS)*.

[13] Bernhard Etzlinger, Barbara Nußbaummüller, Philipp Peterseil, and Karin Anna Hummel. 2021. Distance estimation for ble-based contact tracing–a measurement study. In *Wirel. Days (WD)*. 1–5.

[14] Mario Frank, Ralf Biedert, Eugene Ma, Ivan Martinovic, and Dawn Song. 2012. Touchalytics: On the applicability of touchscreen input as a behavioral biometric for continuous authentication. *IEEE Trans. Inf. Forensics Secur.* 8, 1 (2012), 136–148.

[15] Gatekeeper. 2023. MFA hardware token|Proximity-based wireless security key. https://gkaccess.com/products/2fa-token-halberd/. (2023).

[16] Github. 2023. Blue Proximity. https://github.com/tiktaalik-dev/blueproximity. (2023).

[17] Dianqi Han, Yimin Chen, Tao Li, Rui Zhang, Yaochao Zhang, and Terri Hedgpeth. 2018. Proximity-proof: Secure and usable mobile two-factor authentication. In *Proc. Annu. Int. Conf. Mobile Comput. Netw. (MobiCom)*. 401–415.

[18] Micromax Health. 2023. All-In-One Medical PC – Mate Series. https://micromaxhealth.com/products-2/all-in-one-medical-pc/. (2023).

[19] Otto Huhta, Prakash Shrestha, Swapnil Udar, Mika Juuti, Nitesh Saxena, and N Asokan. 2016. Pitfalls in designing zero-effort deauthentication: Opportunistic human observation attacks. In *Netw. Distrib. Syst. Secur. Symp. (NDSS)*.

[20] Texas Instruments. 2023. INA 219. https://www.ti.com/product/INA219. (2023).

[21] Kyungho Joo, Wonsuk Choi, and Dong Hoon Lee. 2020. Hold the door! Fingerprinting your car key to prevent keyless entry car theft. In *Netw. Distrib. Syst. Secur. Symp. (NDSS)*.

[22] Tomi Kinnunen and Haizhou Li. 2010. An overview of text-independent speaker recognition: From features to supervectors. *Speech Commun.* 52, 1 (2010), 12–40.

[23] Ross Koppel, Joshua P Metlay, Abigail Cohen, Brian Abaluck, A Russell Localio, Stephen E Kimmel, and Brian L Strom. 2005. Role of computerized physician order entry systems in facilitating medication errors. *Jama* 293, 10 (2005), 1197–1203.

[24] Ross Koppel, Sean Smith, Jim Blythe, and Vijay Kothari. 2015. Workarounds to computer access in healthcare organizations: you want my password or a dead patient? In *Driv. Qual. Inform. Fulfill. Promis.* 215–220.

[25] Lenovo. 2023. Lenovo yoga tab 13 tablet. https://www.lenovo.com/us/en/p/tablets/android-tablets/lenovo-tab-series/yoga-tab-13/wmd00000469?org. (2023).

[26] Lingjun Li, Xinxin Zhao, and Guoliang Xue. 2013. Unobservable re-authentication for smartphones.. In *Netw. Distrib. Syst. Secur. Symp. (NDSS)*, Vol. 56.

[27] 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 *Proc. Annu. Int. Conf. Mobile Comput. Netw. (MobiCom)*. 315–328.

[28] Wael Louis, Majid Komeili, and Dimitrios Hatzinakos. 2016. Continuous authentication using one-dimensional multi-resolution local binary patterns (1DMRLBP) in ECG biometrics. *IEEE Trans. Inf. Forensics Secur.* 11, 12 (2016), 2818–2832.

[29] Shrirang Mare, Andrés Molina Markham, Cory Cornelius, Ronald Peterson, and David Kotz. 2014. ZEBRA: Zero-effort bilateral recurring authentication. In *IEEE Symp. Secur. Privacy*. 705–720.

[30] Shrirang Mare, Reza Rawassizadeh, Ronald Peterson, and David Kotz. 2019. Continuous smartphone authentication using wristbands. In *Proc. Workshop Usable Secur.*

[31] Alex T Mariakakis, Souvik Sen, Jeongkeun Lee, and Kyu-Han Kim. 2014. Sail: Single access point-based indoor localization. In *Proc. Annu. Int. Conf. Mobile Syst. Appl. Serv. (MobiSys)*. 315–328.

[32] Miklós Maróti, Branislav Kusy, Gyula Simon, and Akos Lédeczi. 2004. The flooding time synchronization protocol. In *Proc. Int. Conf. Embed. Netw. Sens. Syst. (SenSys)*. 39–49.

[33] MathWorks. 2023. Discrete time analytic signal using hilbert transform. https://www.mathworks.com/help/signal/ref/hilbert.html. (2023).

[34] MathWorks. 2023. Envelope extraction. https://www.mathworks.com/help/signal/ug/envelope-extraction-using-the-analytic-signal.html. (2023).

[35] HIMSS Media. 2023. The Usage of Tablets in the Healthcare Industry. https://www.healthcareitnews.com/blog/usage-tablets-healthcare-industry. (2023).

[36] Todd K Moon. 1996. The expectation-maximization algorithm. *IEEE Signal Process. Mag.* 13, 6 (1996), 47–60.

[37] Brian CJ Moore and Brian R Glasberg. 1983. Suggested formulae for calculating auditory-filter bandwidths and excitation patterns. *J. Acoust. Soc. Am.* 74, 3 (1983), 750–753.

[38] Nymi. 2023. Wearable identity for the future-ready workplace. https://www.nymi.com/nymi-band. (2023).

[39] U.S. Department of Energy. 2023. United States electricity industry primer. https://www.energy.gov/sites/prod/files/2015/12/f28/united-states-electricity-industry-primer.pdf. (2023).

[40] Mauricio Pamplona Segundo, Sudeep Sarkar, Dmitry Goldgof, Luciano Silva, and Olga Bellon. 2013. Continuous 3D face authentication using RGB-D cameras. In *Proc. IEEE Conf. Comput. Vis. Pattern Recognit. Workshops*. 64–69.

[41] Mickaël Pruvost, Wilbert J Smit, Cécile Monteux, Philippe Poulin, and Annie Colin. 2019. Polymeric foams for flexible and highly sensitive low-pressure capacitive sensors. *npj Flex. Electron.* 3, 1 (2019), 1–6.

[42] Kasper Bonne Rasmussen, Marc Roeschlin, Ivan Martinovic, and Gene Tsudik. 2014. Authentication using pulse- response biometrics.. In *Netw. Distrib. Syst. Secur. Symp. (NDSS)*.

[43] J Patrick Reilly. 2012. *Applied bioelectricity: from electrical stimulation to electropathology.*

[44] Douglas A Reynolds. 2002. An overview of automatic speaker recognition technology. In *Proc. IEEE Int. Conf. Acoust. Speech Signal Process. (ICASSP)*, Vol. 4. IV–4072.

[45] Hataichanok Saevanee, Nathan Clarke, Steven Furnell, and Valerio Biscione. 2015. Continuous user authentication using multi-modal biometrics. *Comput. Secur.* 53 (2015), 234–246.

[46] Samsung. 2023. Samsung galaxy tab S7 / S7+. https://www.samsung.com/us/tablets/tab-s7/. (2023).

[47] Munehiko Sato, Rohan S Puri, Alex Olwal, Deepak Chandra, Ivan Poupyrev, and Ramesh Raskar. 2015. Zensei: Augmenting objects with effortless user recognition capabilities through bioimpedance sensing. In *Adjunct Proc. Annu. ACM Symp. User Interface Softw. Technol. (UIST)*.

[48] Ralf Schluter, Ilja Bezrukov, Hermann Wagner, and Hermann Ney. 2007. Gammatone features and feature combination for large vocabulary speech recognition. In *Proc. IEEE Int. Conf. Acoust. Speech Signal Process. (ICASSP)*. IV–649.

[49] Mohit Sethi, Markku Antikainen, and Tuomas Aura. 2014. Commitment-based device pairing with synchronized drawing. In *Proc. IEEE Int. Conf. Pervasive Comput. Commun. (PerCom)*. 181–189.

[50] Chao Shen, Yuanxun Li, Yufei Chen, Xiaohong Guan, and Roy A Maxion. 2017. Performance analysis of multi-motion sensor behavior for active smartphone authentication. *IEEE Trans. Inf. Forensics Secur.* 13, 1 (2017), 48–62.

[51] Chao Shen, Yong Zhang, Xiaohong Guan, and Roy A Maxion. 2015. Performance analysis of touch-interaction behavior for active smartphone authentication. *IEEE Trans. Inf. Forensics Secur.* 11, 3 (2015), 498–513.

[52] Yiran Shen, Chengwen Luo, Weitao Xu, and Wen Hu. 2015. Poster: An online approach for gait recognition on smart glasses. In *Proc. ACM Conf. Embed. Netw. Sens. Syst. (SenSys)*. 389–390.

[53] Sara Sinclair. 2014. *Access control in and for the real world.* Dartmouth College.

[54] Zdeňka Sitová, Jaroslav Šeděnka, Qing Yang, Ge Peng, Gang Zhou, Paolo Gasti, and Kiran S Balagani. 2015. HMOG: New behavioral biometric features for continuous authentication of smartphone users. *IEEE Trans. Inf. Forensics Secur.* 11, 5 (2015), 877–892.

[55] Seeed Studio. 2023. Seeed studio XIAO nRF52840. https://www.seeedstudio.com/Seeed-XIAO-BLE-nRF52840-p-5201.html. (2023).

[56] Tom's-guide. 2023. iPhone X Face ID Slower Than Touch ID. https://www.tomsguide.com/us/iphone-x-face-id-speed-up,news-26060.html. (2023).

[57] Ge Wang, Haofan Cai, Chen Qian, Jinsong Han, Xin Li, Han Ding, and Jizhong Zhao. 2018. Towards replay-resilient RFID authentication. In *Proc. Annu. Int. Conf. Mobile Comput. Netw. (MobiCom)*. 385–399.

[58] Jiyun Wu and Zhide Chen. 2015. An implicit identity authentication system considering changes of gesture based on keystroke behaviors. *Int. J. Distrib. Sens. Netw.* 11, 6 (2015), 470274.

[59] Weitao Xu, Guohao Lan, Qi Lin, Sara Khalifa, Mahbub Hassan, Neil Bergmann, and Wen Hu. 2017. KEH-Gait: Towards a mobile healthcare user authentication system by kinetic energy harvesting. In *Netw. Distrib. Syst. Secur. Symp. (NDSS)*.
[60] 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 *Proc. Annu. Int. Conf. Mobile Comput. Netw. (MobiCom)*.
[61] Fusang Zhang, Jie Xiong, Zhaoxin Chang, Junqi Ma, and Daqing Zhang. 2022. Mobi2Sense: empowering wireless sensing with mobility. In *Proc. Annu. Int. Conf. Mobile Comput. Netw. (MobiCom)*. 268–281.
[62] Tengxiang Zhang, Xin Yi, Ruolin Wang, Yuntao Wang, Chun Yu, Yiqin Lu, and Yuanchun Shi. 2018. Tap-to-pair: associating wireless devices with synchronous tapping. *Proc. ACM Interact. Mobile Wearable Ubiquitous Technol.* 2, 4 (2018), 1–21.
[63] Yongtuo Zhang, Wen Hu, Weitao Xu, Chun Tung Chou, and Jiankun Hu. 2018. Continuous authentication using eye movement response of implicit visual stimuli. *Proc. ACM Interact. Mobile Wearable Ubiquitous Technol.* 1, 4 (2018), 1–22.
[64] Tianming Zhao, Yan Wang, Jian Liu, and Yingying Chen. 2018. Your heart won't lie: PPG-based continuous authentication on wrist-worn wearable devices. In *Proc. Annu. Int. Conf. Mobile Comput. Netw. (MobiCom)*. 783–785.
[65] Tianming Zhao, Yan Wang, Jian Liu, Yingying Chen, Jerry Cheng, and Jiadi Yu. 2020. TrueHeart: Continuous authentication on wrist-worn wearables using PPG-based biometrics. In *IEEE Conf. Comput. Commun. (INFOCOM)*. 30–39.
[66] Xiaojia Zhao, Yang Shao, and DeLiang Wang. 2012. CASA-based robust speaker identification. *IEEE Trans. Audio Speech Lang. Process.* 20, 5 (2012), 1608–1616.
[67] Xiaojia Zhao and DeLiang Wang. 2013. Analyzing noise robustness of MFCC and GFCC features in speaker identification. In *IEEE international conference on acoustics, speech and signal processing (ICASSP)*. 7204–7208.
[68] Xiaoqiang Zhu, Tie Qiu, Wenyu Qu, Xiaobo Zhou, Mohammed Atiquzzaman, and Dapeng Oliver Wu. 2023. BLS-Location: A Wireless Fingerprint Localization Algorithm Based on Broad Learning. *IEEE Trans. Mobile Comput.* 22, 1 (2023), 115–128.
[69] Thomas G Zimmerman, Joshua R Smith, Joseph A Paradiso, David Allport, and Neil Gershenfeld. 1995. Applying electric field sensing to human-computer interfaces. In *Proc. SIGCHI Conf. Hum. Factors Comput. Syst. (CHI)*. 280–287.

APPENDIX

A SYSTEM PARAMETER SELECTION

In the phase-I study, we aim to select the proper parameters for the proposed scheme. They include synchronization tolerance (Δt), window size (w), match threshold (ρ), and overlap fraction (f). In the experiment, participants are asked to interact with the terminal arbitrarily. Each participant performs 5 sets of interactions, with 20 trials in each set. We thus collect a total of 100 samples from each participant. The system parameters are selected by striking a balance between security (FAR) and usability (FRR). In particular, FAR is the probability by which an adversary passes the authentication, while FRR is the chance that a legitimate user is wrongly classified as an imposter. To calculate FAR in the phase-I study, we simply treat samples from participants other than the target user as attacker's trials to pass the authentication.

Synchronization tolerance. As discussed in Section 5.3, we introduce a synchronization tolerance (Δt) to alleviate the false alarm caused by imperfect clock synchronization. The two interactive sequences are deemed matched if the pair-wise element comparison holds within Δt. Figure 12(a) shows FAR/FRR with respect to Δt. By increasing Δt, FAR grows whereas FRR drops. This is because a larger Δt corresponds to a more loose decision rule. It thus leads to more wrong acceptances. On the other hand, the chance that a legitimate user is wrongly classified is reduced. EER exists when Δt is around 165 ms.

Window size. It refers to the number of interactions the authenticator compares to reach a decision. A larger window size (w) allows more interactions to be considered. As shown, FRR drops as w increases. However, it is in the trade of system security, as FAR climbs accordingly. From the perspective of usability, a small window size is preferred; it implies the decision can be made with

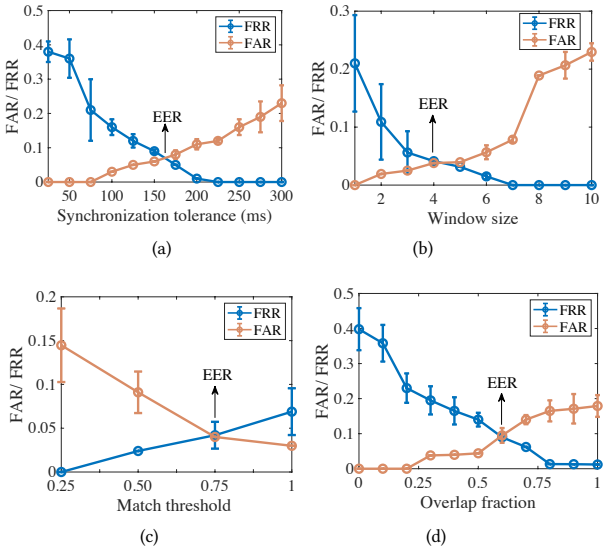

Figure 12: Scheme parameter selection. (a) Synchronization tolerance (Δt) (b) window size (w) (c) match threshold (ρ) (d) overlap fraction (f).

fewer interactions. Besides, a big window size equivalently allows the system to remain unlocked for a longer time, which renders the system more vulnerable to other attacks. In our design, EER (3.8%) exists when $w = 4$ as shown in Figure 12(b). The result is quite promising because only 4 finger-screen interactions are needed to spot an adversary with satisfactory accuracy. As shown later, prior works typically need far more interactions to make a concrete decision.

Match threshold. Match threshold (ρ) refers to the fraction of interactions in a window that should match for the authenticator to make a decision. We observe in Figure 12(c) that FAR is pretty high for a small ρ and it drops significantly as ρ increases to 1; FRR is generally low across all ρ's. The best overall performance exists when $\rho = 75\%$.

Overlap fraction. In the GFCC feature extraction, we first divide the processed waveform signals into overlapping frames. The overlap fraction (f) determines the overlapping relationship between adjacent frames. It ranges from [0,1), with 0 being no overlap. Figure 12(d) shows the impact of f on the authentication accuracy. We find that f also plays an important role for striking a balance between security and utility. According to the result, $f = 0.6$ is a proper value in our case.

B ABLATION STUDY

In the ablation study, the performance is compared between the basic scheme and the advanced scheme to understand the contribution of the terminal fingerprinting component. Recall that the advanced scheme differs from the basic scheme by introducing the terminal fingerprinting component.

We conduct this study with consideration of both innocent and malicious adversaries. The malicious adversary tries to mimic the victim's interactions with a direct line of sight observation. We show the attack's success rate by varying the distance from 1 to 30 ft. It is observed from Table 4 that the success rate drops in both schemes.

Table 4: Impact of terminal fingerprinting (TF) on attack success rates.

	Malicious adversary							Innocent adversary
Distance (ft)	1	2	3	5	10	20	30	n/a
Without TF (%)	33	30	27	25	16.5	12	10	3
With TF (%)	8.5	6.2	4.2	3.7	3	2.7	2.6	2.4

The advanced scheme (with terminal fingerprinting) outperforms the basic scheme (with terminal fingerprinting) by a considerable margin in all cases. For instance, their success rates are 33% and 8.5%, respectively, under a distance of 1 ft. Regarding the innocent adversary, its success rate is 3% and 2.4% for the advanced and basic schemes, respectively. The above result validates the effectiveness of terminal fingerprinting.

C SYSTEM PERFORMANCE

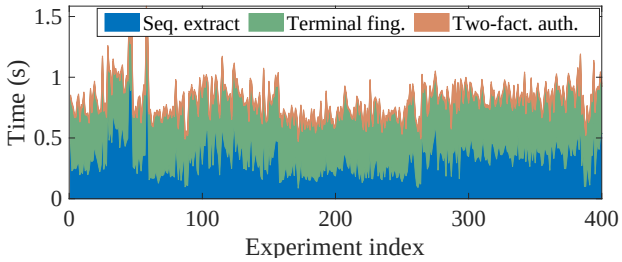

Figure 13: Stacked computation time.

Computation time. Figure 13 shows the stacked time duration for the three main components of our scheme, namely, interaction sequence extraction, terminal fingerprinting, and two-factor authentication. Among them, terminal fingerprinting takes the longest time, with an average of 0.47 s, owing to the GFCC feature extraction and the GMM module. For interaction sequence extraction and two-factor authentication, their average time is 0.33 s and 0.02 s, respectively. We observe that all trials are accomplished within 1.6 s, with the 90 percentile at 1.0 s. As a reference, the execution time for FaceID and TouchID on iOS is 1.48s and 0.91s, respectively [56]. Hence, our scheme is practical for real-world implementation.

Energy consumption. We focus on the energy consumption of the wearable due to its battery constraint. The measurement is done using a programmable power monitor INA 219 sensor [20]. As shown in Figure 14(a), the leads of INA 219 are connected across the power supply line between the wearable and the battery. An Arduino MCU board is connected to INA 219 for reading collection and analysis. The power consumption is recorded for every experiment instance.

To facilitate the measurement, we first set up the wearable in standby mode and get its energy consumption baseline. The energy consumption of our scheme is derived by subtracting the baseline from the instant measurements. Figure 14(b) depicts the CDF of energy consumption at the wearable. We find that its 90 percentile is around 0.0098 mAh, with a maximum value of 0.02 mAh. This is negligible compared to a typical wearable's battery capacity. For instance, Apple Series 7 watch has a battery capacity of 309 mAh.

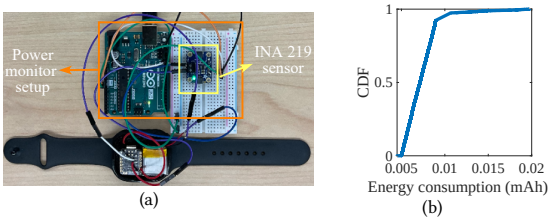

Figure 14: (a) Measurement setup. (b) CDF of energy consumption at the wearable.

In our design, the operations executed at the wearable are limited, including human-induced electric potential measurement and its transmission (to the terminal). Most operations are performed at the terminal. Besides, the wearable will not be activated unless it receives from the terminal an authentication request that is triggered by touch events. These strategies contribute to energy efficiency at the wearable.

D USER STUDY

The goal of the user study is to evaluate participants' perception toward our proposed authentication scheme.

Design. All participants are asked to provide their perception of our scheme after all the experiment sessions by responding to 10 questions on a 5-point Likert scale (with 1 = strongly disagree, 3 = neutral, and 5 = strongly agree). These questions cover multiple aspects of security and usability. The following is a list of questions.

- Q1 I would like to adopt the proposed continuous authentication scheme for daily usage.
- Q2 The proposed scheme requires no effort from me.
- Q3 The system is easy to use.
- Q4 The system performance is consistent.
- Q5 I would not be less worried about temporarily leaving my working terminal unattended with the proposed scheme implemented.
- Q6 The proposed scheme is more secure compared to the current session timeout approach.
- Q7 The operation is easy to learn.
- Q8 The scheme would not disrupt my regular activities on the terminal.
- Q9 The scheme is more convenient than the session timeout approach.
- Q10 The system is reasonably fast and unobtrusive.

To make a fair comparison with the session timeout approach, participants are asked to interact with it on a lab computer where the approach is implemented. They are also provided with the requisite understanding of the underlying mechanisms involved in the session timeout approach.

Results. Figure 15 illustrates the participant's responses on a 5-point Likert scale. 80% of the participants express their willingness to use this system into their daily life (Q1). Only 16% report that the proposed scheme requires some effort to perform (Q2). 88% agree that the system is easy to use (Q3). 84% of participants find the system performance reasonably consistent (Q4) and 80% indicate that they would feel less stressed about leaving their working terminals unattended when augmented with our scheme (Q5).

Table 5: Comparison among different continuous authentication schemes, which are categorized into: physiological biometric authentication (light gray), behavioral biometric authentication (gray), and other approaches (dark gray). ●: method fulfills criterion. ◐: method quasi-fulfills criterion. ○: method does not fulfill criterion. –: not enough information/not applicable.

Scheme	Additional device free	COTS device compatible	Robust to user movement	Restriction-free on device placement	Fast authentication	Cost efficient	Against zero-knowledge attack	Against mimic attack	Signal type cs
Cardiac Scan [27]	○	○	◐	○	●	○	●	●	Cardiac motion (Doppl. Radar Sens.)
Eberz et.al [12]	○	◐	○	○	–	◐	●	◐	Gaze (Eye)
1DMRLBP [28]	○	●	○	○	–	○	●	●	ECG
TrueHeart [65]	○	○	◐	○	–	◐	●	●	PPG
Segundo et.al [40]	●	●	○	●	–	●	●	◐	Face (camera)
Rasmussen et.al [42]	○	○	○	○	–	○	●	●	Electric pulse response
Touchalytics [14]	●	●	◐	●	–	●	●	◐	Touch behavior
WACA [1]	○	●	○	○	–	●	●	◐	Keystroke(IMU)
KEH [59]	○	○	●	◐	–	◐	●	◐	Gait (IMU)
HMOG [54]	●	●	◐	●	○	●	●	◐	Hand movement (IMU)
Shen et.al [50]	●	●	◐	●	–	●	●	◐	Touch behavior (IMU)
Li et.al [26]	●	●	◐	●	–	●	●	◐	Touch behavior
Timeout	●	●	●	●	◐	●	○	○	–
ZEBRA [29]	○	●	○	○	○	●	●	◐	IMU
CSAW [30]	○	●	○	○	●	●	●	◐	Motion sensor (Wrist Motion)
Transient Auth. [10]	○	●	–	●	○	–	●	○	Proximity (Radio)
This work	○	◐	●	●	●	●	●	●	Human-induced electric potential

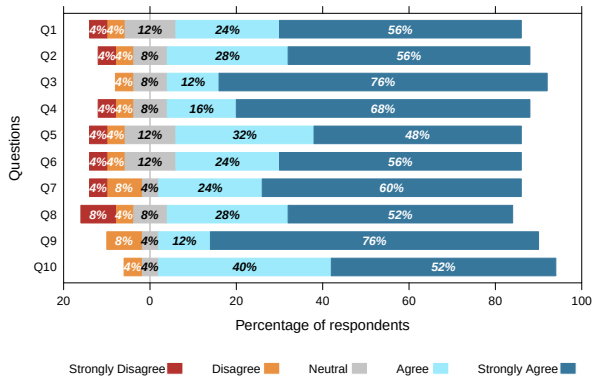

Figure 15: Survey results.

56% of the respondents strongly believe that our scheme would be more secure than the current continuous authentication methods (Q6). If implemented in real-world devices, only 16% indicate that the scheme would be difficult to learn or get used to (Q7). When asked if our scheme would disrupt daily activities, only 8% strongly feel that there may be some disruption (Q8). 76% of participants find our design more convenient than current methods (Q9). This number increases to 92% when asked if the system is fast enough and unobtrusive (Q10).

In summary, the results indicate that most users hold a positive view of our scheme. They are willing to adopt it in their daily lives due to the security and convenience offered, in comparison with the state-of-the-art solution.

E COMPARISON WITH PRIOR WORKS

Additional device free: Whether an additional device, other than the target terminal itself, is necessary for the scheme to work.

COTS device compatible: Whether the scheme is readily applicable to COTS devices.

Robust to user movement: To ensure better usability, the scheme should be robust even when there are some random user movements irrelevant to the scheme.

Restriction-free on device placement: For the scheme that involves an additional device, it may impose restrictions regarding the device placement (on the human body).

Fast authentication: A measure of how fast the scheme works, i.e., the time it takes for the authenticator to make a decision about whether a target user is legit or not. Training time is not included.

Cost-efficient: The implementation overhead of the scheme, particularly the hardware, should be affordable.

Against zero-knowledge attack: Resilience against adversaries who have zero knowledge about the authentication system or the victim user's secret credentials or biometrics.

Against mimic attack: Resilience against adversaries who mimic the legit user's actions to bypass the authentication.

Signal type: It specifies the signal modality utilized by the scheme.