WatchID: Wearable Device Authentication via Reprogrammable Vibration

Jerry Q. Cheng[1], Zixiao Wang[1], Yan Wang[2], Tianming Zhao[2], Hao Wan[1], and Eric Xie[3]

[1] Department of Computer Science, New York Institute of Technology
[2] Department of Computer & Information Sciences, Temple University
[3] Princeton High School (Princeton, New Jersey)

Abstract. Prevalent wearables (e.g., smartwatches and activity trackers) demand high secure measures to protect users' private information, such as personal contacts, bank accounts, etc. While existing two-factor authentication methods can enhance traditional user authentication, they are not convenient as they require participations from users. Recently, manufacturing imperfections in hardware devices (e.g., accelerometers and WiFi interface) have been utilized for low-effort two-factor authentications. However, these methods rely on fixed device credentials that would require users to replace their devices once the device credentials are stolen. In this work, we develop a novel device authentication system, *WatchID*, that can identify a user's wearable using its vibration-based device credentials. Our system exploits readily available vibration motors and accelerometers in wearables to establish a vibration communication channel to capture wearables' unique vibration characteristics. Compared to existing methods, our vibration-based device credentials are reprogrammable and easy to use. We develop a series of data processing methods to mitigate the impact of noises and body movements. A lightweight convolutional neural network is developed for feature extraction and device authentication. Extensive experimental results using five smartwatches show that WatchID can achieve an average precision and recall of 98% and 94% respectively in various attacking scenarios.

Keywords: Wearables · Device authentication · Vibration signals.

1 Introduction

Due to ever-advancing communication, computing, and sensing technologies, wearables (e.g., smartwatches and activity trackers) have become increasingly ubiquitous for people to use in their daily lives. Many manufacturers produce such gadgets for activity tracking and vital signs monitoring in order to capitalize on the global rise in health and wellbeing awareness. More recently, building on their convenience in usage and popularity among customers, wearables expand their functionalities beyond health and activity monitoring into various applications in other fields, including mobile payment, smart home control, emailing and

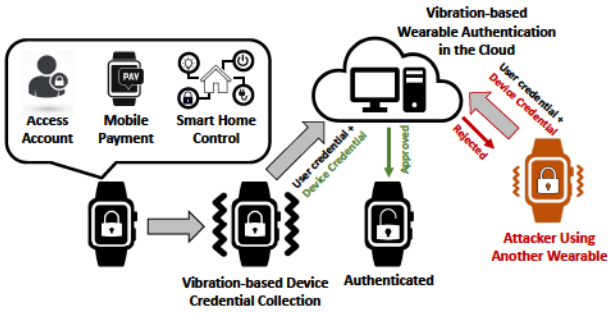


Fig. 1: Illustration of WatchID: the reprogrammable wearable authentication system using vibration-based device credentials.

texting, etc. The growing usage of these applications in wearables provides more opportunities for attackers to compromise users' private information (e.g., email accounts, personal contact lists, etc.) and, more seriously, financial information (e.g., banking and credit card accounts). As a result, it is becoming increasingly vital to secure wearables to protect users' privacy and financial assets.

Existing authentication methods on wearable devices have very limited choices. Most wearables use passwords or PINs [17] to verify users' identities. Recently two-factor authentication has been adopted, using additional user inputs of text codes [2] or taking phone calls [14] for better protections. These methods require additional inputs from users and can only verify the identity of the user based on the knowledge of certain secrete information (i.e., password, PIN, the content of additional messages and calls). These types of information are vulnerable to many attacks, such as shoulder surfing [22] and stolen attacks [36]. Once the user's credentials are compromised, the attacker can easily log into the user's accounts on the attacker's own device. Then the attacker can steal valuable personal information or abuse the user's account (e.g., making payment without users' permission, opening smart-door locks, etc.) inconspicously.

Recently, researchers have discovered that computing devices can be identified based on their unique physical properties. For example, the frequency responses of smartphones' speakers are studied by Zhou *et al.* [41] to generate device identities using inaudible acoustic signals. The imperfections of radio frequncy (RF) transmitter (e.g., the digital-to-analog converter (DAC) errors and the power amplifier (PA) non-linearity) are explored by Polak *et al.* [27] to identify wireless devices. The unique acceleration responses of motion sensors inside mobile devices (e.g., smartphones) are explored in Accelprint [11] to distinguish different mobile devices. These studies have shown that physical properties in hardware can be exploited to create unique device credentials as a second factor to enhance security in users' applications. However, most of the existing device authentication methods are rigid and suffer from stolen attacks because users cannot change their hardware-related device credentials. As a result, users will be forced to use a new device if their device credentials are stolen. In this work, we propose to utilize devices' vibration characteristics, as reprogrammable credentials, to enable practical device authentication in prevalent wearables.

Toward this end, we develop a device authentication system called *WatchID*, illustrated in Figure 1, to identify a wearable device using vibration motions generated by its vibration motor and captured by its accelerometers. The key to this system is that the vibration motor and accelerometers of each individual wearable always have manufacture imperfections. As a result, the vibration signals will exhibit unique device-wise characteristic which we utilize for the purpose of device authentication. Compared to existing methods, WatchID is more flexible as it allows users to generate and reprogram various vibration patterns that are associated with different unique device credentials. Our system is also non-intrusive so users just need to wear their wearables without any active participations. In addition, it is low-cost and practical since it only uses the built-in vibration motors and accelerometers, which are readily available in wearables. In particular, when a user launches an sensitive application on his/her wearable (e.g., accessing a user account, using mobile payment, controlling smart home, etc.), our system uses the wearable's vibration motor to generate a predefined vibration pattern. Meanwhile, the wearable's accelerometers capture the unique vibration signals propagating through the device's body and send them with the user's credentials to a cloud server, where the user has pre-registered the device. Once the wearable's device credential and user credential are verified by the cloud server, the wearable receives the approval to proceed with the protected application.

In designing WatchID, we address several challenges to make it an accurate, fast, and robust device authentication system. First, the vibration characteristics that we use as device credentials should be unique enough to distinguish different wearables for the purpose of device authentication. Second, built-in vibration motors and accelerometers inside wearables are usually of low-quality with unstable vibration signals and low sampling rates. Third, many interfering factors such as wearable postures, body motions, and environmental noises can contaminate the device credentials. To address these challenges, we study the vibration motors and motion sensors in different models of wearables and develop vibration patterns that are suitable for device authentication. In addition, we apply vibration noise filtering methods to mitigate the impacts of motion artifacts and ambient noises to our system. With the denoised device credentials, our system applies a deep neural network designed to performance a robust device authentication process.

Through implementing WatchID, we have made several major contributions as follows:

- We extensively investigate the uniqueness of vibration motors and accelerometers in commodity wearables, analyze the vibration characteristics from different vibration patterns which are used for reprogrammable vibration-based device credentials.
- We develop a novel device authentication system with a light-weight deep neural network that can accurately and efficiently identify different wearables based on their vibration-based device credentials.
- We collect a large amount of experimental data using five commercial off-the-shelf (COTS) smartwatches in various scenarios and different days. Our

results show that our device authentication system can achieve over 98% and 94% for precision and recall, respectively.

The rest of paper is organized as follows. Section 2 begins with an extensive review of related work in authentication methods for mobile devices and considers the uniqueness and advantage of our system that can bring into this research field. Section 3 provides attack models to WatchID. Section 4 describes feasibility studies which are used as the basis for our system. Section 5 introduces an overview of the design and process flow of our system. Section 6 explains our vibration noise filtering method and vibration-based device authentication method. Section 7 presents our experimental methodology and results of evaluating this system. Section 8 concludes this work with discussion.

2 Related Work

Traditional user authentication methods for mobile devices usually require user inputs such as usernames, passwords, graphic patterns, which are vulnerable to knowledge-based attacks (e.g., shoulder attacks and smudge attacks). Recently, researchers have proposed to use human biometrics for convenient mobile user authentication. These biometric-based methods can be classified into two types: behavioral-based and physiological-based approaches. The behavioral-based approaches [34, 30, 37] identify users based on users' activity patterns (e.g., keystroke entries, mouse movements, gaits in walking). Recently, Cong *et al.* [33] propose a behavior-based user authentication system using commodity WiFi, which is non-intrusive and low-cost. The physiological-based approaches are non-intrusive and usually exploit fingerprints [29, 7], iris patterns [31, 32], respiratory patterns [25, 26] and cardiac patterns [23, 38, 24, 40] to perform user authentication.

While the above mobile user authentication methods can effectively identify users, users' credentials can still bed be compromised by various attacks (e.g., fingerprint smudge attacks [39] and cardiac pattern attacks [13]). To solve these problems, researchers have exploited and utilized hardware imperfections as device credentials to verify whether certain sensitive operations originate from a legitimate device. According to the source of these credentials, we can classify the existing device credentials into three categories:

1. **Acoustic-based Device Credentials.** Variations in manufacturing processes, although usually small, can often introduce product imperfections off from pre-defined specifications. For example, microphones and speakers of the same brand and model will produce and receive sounds differently. Das *et al.* [9] exploit this observation to distinguish smartphones through playing and recording a pre-recorded audio sample. Daniel *et al.* [15] study statistical characterizations of frequency responses of microphones to identify different devices. Zhou *et al.* [41] exploit inaudible acoustic signals from microphones insides smartphones to generate unique device identity. All these acoustic-based approaches require access to microphones in recording and thus can create privacy concerns.

2. **RF-based Device Credentials.** Researchers also find that RF signals from mobile devices contain identifiable information related to the imperfections of the analog circuits inside these devices. For example, Danev *et al.* [8] compare several device identification systems using modulator circuitry, analog circuitry, and clock skew of WiFi transmitters to identify wireless devices. For the same purpose, Polak *et al.* [27, 28] exploit the digital-to-analog converter (DAC) errors and the power amplifier (PA) non-linearity of RF transmitter components. Brik *et al.* [6] leverage differentiating artifacts of individual wireless frames in the modulation domain caused by the minute imperfections of NICs. Among these RF-based approaches, the quality and speed of RF signal acquisition and processing are easily impacted by environmental factors so that the resulting device credential extraction is complex and difficult.
3. **Motion Sensor-based Device Credentials.** Motion sensors (i.e., accelerometers and gyroscopes) can also be used for fingerprinting as demonstrated in [11, 5, 10]: Bojinov *et al.* [5] exploit the unique linear bias of the accelerometer; Dey *et al.* [11] use vibration motors to stimulate accelerometers in mobile phones; Das *et al.* [10] use audio signals to trigger both accelerometers and gyroscopes in mobile phones with human motions. These research have shown that the motion sensor-based approach is a promising research field with further studies needed for utilizations of predefined vibration patterns, different frequencies and amplitudes. Currently existing studies mostly focus on mobile phones and tablets. And it remains unknown whether they can adapt to wearble devices since the contact surface of human wrists is very different from that of desks or human palms.

In this work, we develop a novel device authentication system for wearables to generate vibration-based device credentials by vibration motors and capture the credentials by accelerometers in wearables. Our work is close to [11] in exploring imperfections with vibration motors and accelerometers, but focusing on wearable devices. Furthermore, our system is reprogrammable in allowing users to change or customize the device credentials. By doing so, users can keep using their wearable devices even after the original device credentials are compromised by attackers.

3 Attack Model

Malicious users may attempt to attack WatchID in order to steal personal information or deny a legitimate user from using services on the device. To study the associated attack models, we assume that the attackers can not access the wearable device directly but may have the following capabilities: 1) the attacker has the capability of stealing the users' credentials, including user names and passwords for the target system; 2) the attacker may also have obtained the device credential that the user registers with the system. Specially, we consider the following attack strategies.

Random Attack/Blind Attacks. We assume that the attacker has obtained a user's credentials, but not the device credential, and the device is not in

his possession. The attacker uses his device to generate some random vibration patterns to match the device credential and bypass WatchID.

Jamming Attacks. The goal of this attack is to make WatchID unable to authenticate legitimate devices. Researchers have found that motion sensors (i.e., accelerometers and gyroscopes) can capture the vibration signals caused by acoustic sounds (e.g., music and human speech) [35]. Based on this, attackers can launch a jamming attack by generating loud acoustic signals (e.g., loud music) with various frequencies near the wearable devices. As a result, vibration-based device credentials may be severely interfered by these loud sounds so that our system is not able to accurately verify the user's device identity.

Credential Stealing Attacks. In the case when attackers have obtained a user's credential as well as the device's credential, the attacker can impersonate the legitimate user using both types of credentials to fool the system. Once the attacker passes the authentication, he can steal the user's personal and financial information or even perform illicit acts. Attackers can launch such attacks by monitoring the communications between the device and the cloud part of WachID at the device registration phase or during normal operations.

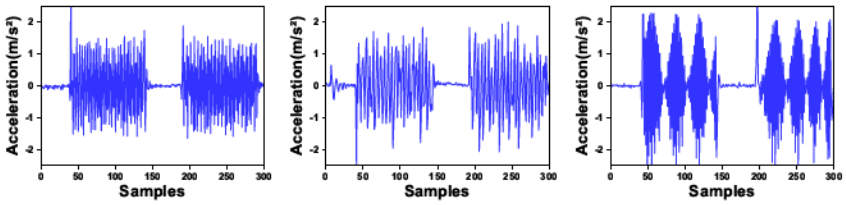
4 Feasibility Study

In this section, we conduct feasibility studies of using the vibration characteristics to construct device credentials for the purpose of distinguishing different wearables.

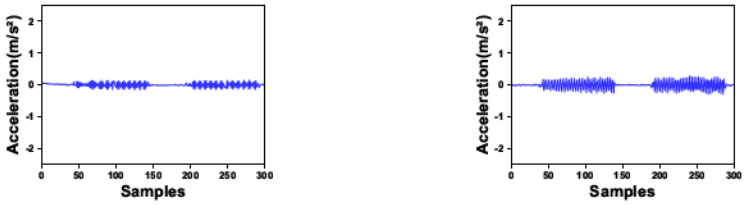
4.1 Device Credential Based on Vibrations

The Background of Vibration Motors. Mobile devices and wearables usually have built-in vibration motors that can be programmed to vibrate in various patterns. Such vibrations are mostly used in mobile applications as an alternative notification mechanism for alarm clocks, incoming calls, text messages, etc. Based on their operating principles, vibration motors in mobile devices and wearables can be categorized into two types: eccentric rotating mass (ERM) vibration motors and linear resonant actuator (LRA) vibration motors. The vibrations of ERM motors are generated by the rotations of a non-symmetric mass, while the vibrations of LRA motors are generated by linear movements of a magnet mass interacting with a voice coil. Vibration motors of the both types in mobile devices and wearable are of miniature size with varying degrees in vibration strengths, stabilities, and frequency ranges due to the differences in their working principles and manufacturers.

Vibration-based Device Credentials. In this work, we consider that a wearable's vibration motor, its device body, and accelerometers are working together as a one-way communication system. The vibration motor (a transmitter) generates a vibration wave that propagate through the device body (a channel) and are received by the accelerometers (receivers). During the propagation, the vibration wave experiences attenuation in its energy level along the transmitting path as well as multipath interference when the wave hits two different media boundaries. Consequently, the received vibration signals (i.e., accelerometer



(a) Watch 1 (b) Watch 2 (c) Watch 3



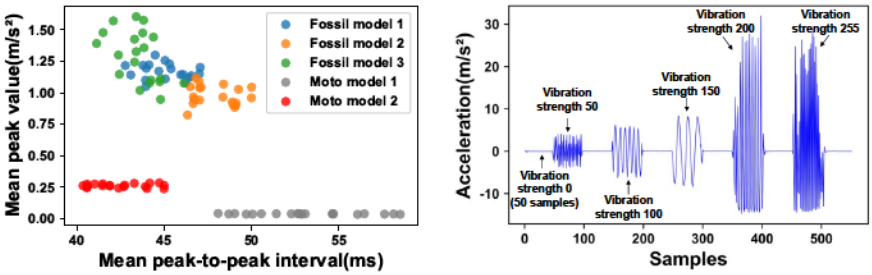
(d) Watch 4 (e) Watch 5

Fig. 2: Z-axis accelerometer readings of 5 smartwatches when the watches have two repetitions of a vibration pattern (i.e., idle for 1 second and vibrating for 2 seconds with the vibration strength of 50). Watch 1 to Watch 3 are Fossil Gen 5, Watch 4 and Watch 5 are Moto 360 Gen 3.

readings) contain unique vibration characteristics as a result of manufacturing imperfections of the vibration motor and accelerometers, attenuations and the multipath interference from the device body. We contemplate that such vibration characteristics are unique for each wearable and can be utilized to identify wearables.

To demonstrate a proof of concept for utilizing such vibration characteristics for device authentication, we develop an app to generate vibrations and collect vibration data on five commodity smartwatches (Three Fossil Gen 5 watches and two Moto 360 Gen 3 watches). Specifically we use Google Wear OS (version 2.27) [16] on these smartwatches to change the vibration strength of the built-in vibration motors within a range of 0 to 255 and vibration durations. We place each watch on a wooden table with its face up and program the app to keep the watch still for 1 second and vibrating for 2 second with the vibration strength set to 50. Meanwhile, the app uses the watch's accelerometers to capture the vibration signals using their maximum sampling rate of 50Hz. We repeat the same vibration pattern for comparison. Figure 2 shows two repetitions of the vibration waves (captured accelerations) along the vertical direction of the five smartwatches. We can observe that the acceleration patterns of all the watches are obviously different from each other in terms of their amplitudes and variations with some resemblance among watches of a same brand.

We repeat the same experiment 50 times for each watch and examine some summary quantities (e.g., mean, standard deviation, maximum, minimum of vibration amplitudes, frequency of the vibration signals, etc) of the captured vibrations signals to quantitatively understand the distinguishable vibration pat-



(a) (b)

Fig. 3: Unique vibration characteristics of wearables: (a) a scatter plot of mean peak values and inter-peak duration of 50 vibration signals from five watches; (b) a sequence of z-axis accelerations captured when a smartwatch vibrates with five different vibration strengths, each segment contains 1 second of data.

terns on wearables. Among these quantities, we pick the mean of peak values and inter-peak duration and make a two-dimensional scatter plot in Figure 3 (a), from which we observe that the data points of the same watch are clustered together. We also find that the clusters of different watches are separable, especially for the watches of different brands (i.e., Fossil versus Moto). Moreover, we can see that the peak values of all Fossil watches are higher but more varied than the Moto watches. In contrast, the inter-peak duration of the Moto watches is more varied than that for all Fossil watches. These observations suggest that each wearable has its own unique vibration characteristics that can be utilized for device authentication.

4.2 Reprogrammable Vibration Patterns

Since existing device authentication methods use hardware manufacturing imperfections to generate rigid and unchangeable device credentials, users are forced to change their hardware to continue using their protected service in case when these device credentials are stolen by attackers. This is neither convenient nor economical. In contrast, WatchID uses the vibration characteristics as device credentials for authentication so that the credentials are configurable in terms of vibration amplitudes and durations. As a result, the corresponding vibration-based device credentials are not only unique, but also programmable (setting to patterns predefined by the manufacture or customized by users), thus making device authentication more convenient and flexible.

To illustrate the programmable vibration-based device credentials, we set the Fossil Gen 5 Watch 1 to vibrate at vibration strengths of 50, 100, 150, 200, and 255 for 1 second, respectively. Figure 3 (b) shows the z-axis accelerometer reading for this experiment. We can observe that the vibration characteristics of the same watch are significantly different when the vibration strength is set to different levels, even when the duration is the same. In addition, we combine vibration strengths and durations as our proposed device credentials for more accurate authentication.

5 System Overview

In this section, we first present several challenges in building a wearable device authentication system. Then we describe the system design of WatchID, which addresses those challenges.

5.1 Challenges

In order to build an effective, robust, and flexible wearable device authentication system using the vibrations generated and collected by wearable devices' vibration motors and accelerometers respectively, we need to address the following challenges for requiring:

- **Effective Credential Using Vibration Motors and Accelerometers in COTS Wearables**. Due to size and battery limitations, COTS wearables are usually equipped with vibration motors of lower quality and accelrometers with sample rates no more than 50Hz. As a result, it is difficult to obtain fine-grained measurements of the vibration signals from wearables in order to extract effective credentials for the devices.
- **Robust Vibration Signals for Practical Use**. In practice, a user might be moving or swinging his/her arms while the surrounding environment can be noisy and vibrant. Therefore the vibration signals captured by accelerometers from the user's watch are often mixed with noises. This will make it challenging to extract device credentials from the vibration signals for robust device identification.
- **Reprogrammable Device Credential**. Device credentials along with regular user login information are subject to various attacks from malicious users. When a particular set of device credential is compromised, the authentication system will disable the device and make it unusable for its protected services. In order to re-secure the device, the device authentication system should be able to provide a reprogrammable functionality for a new device credential thus to obsolete the stolen one.

5.2 System Design

To address the aforementioned challenges, we design WatchID as a reprogrammable device authentication system leveraging low-cost vibration motors and accelerometers in commodity wearables. The basic idea of the system is to identify wearables devices based on the unique vibration characteristics induced by the manufacture imperfection of wearables' vibration motors and accelerometers. When a wearable equipped with WatchID tries to perform a critical operation (e.g., mobile payment or online purchasing), it triggers WatchID to verify the authenticity of the operation by sending the user's user credentials and device credentials to a remote server. Figure 4 illustrates the overview of the our system design. WatchID first performs *Programmable Vibration Signal Generation* to generate a vibration signal that has been pre-registered with the remote server using the

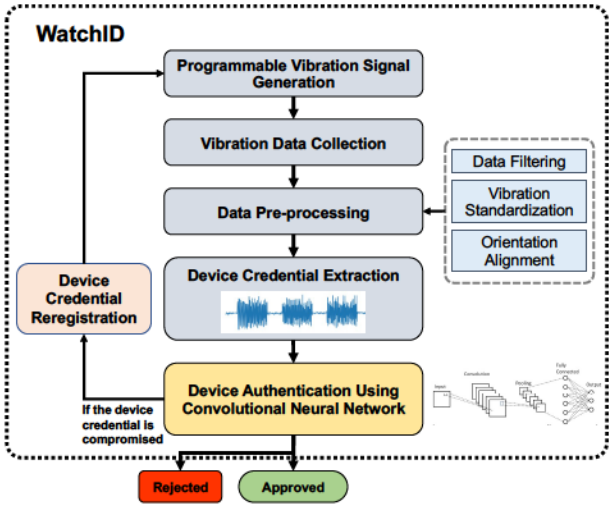


Fig. 4: Overview of the WatchID system.

wearable's built-in vibration motor. Meanwhile, the system performs *Vibration Data Collection* to capture the vibration signals propagating from the vibration motor by the wearable's accelerometers. Then, the *Data Pre-processing* module performs on the vibration signals: removing high-frequency noises, standardizing sensing data, and aligning the signals' orientations to ensure the robustness of the system with different activities and poses in practice. Next, WatchID extracts the vibration-based device credential by examining the energy of the vibration signals in *Device Credential Extraction*. The device credentials will be transmitted to the remote server and perform *Device Authentication Using Convolutional Neural Network* to verify the identity of the wearable using an advanced deep neural network. In particular, we develop a lightweight convolutional neural network (CNN) to abstract a high-dimensional representation of the device credential and determine whether the representation is highly close to the device credential pre-registered with the server. If the answer is positive, WatchID verifies the identity of the user's device and approves the critical operation. Otherwise, WatchID will issue an rejection.

One significant advantage of WatchID is that WatchID allows the user to use the same device but change the vibration-based device credentials by reprogramming the vibration motor to induce new, unique vibration characteristics as device credentials. Compared to traditional device authentication methods that use unchangeable device credentials, WatchID is more practical and convenient if the device credentials are compromised. When WatchID rejects a device authentication, it sends the user's wearable device a warning message about the attempted unauthorized operation. The user then has the option to use a different vibration-based device credential by initiating *Device Credential Re-registration*. Here the user just needs to generate vibration signals of a new pattern on the wearable, preprocess the collected accelerometer data, extract the vibration-based device credentials, and send them to the server for registra-

tion through a secure channel. The user can define his/her own vibration pattern in terms of vibration strengths and duration or use factory-predefined patterns. After the registration, the user will be able to use the new device credential to perform the device authentication.

6 Watch Identification Using Vibration

6.1 Reprogrammable Vibration Signal Generation and Vibration Data Collection

The major advantage of WatchID is that the vibration-based device credentials are reprogrammable on the same device. Specifically, a vibration signal can be mainly determined by four independent parameters: *vibration strength*, *vibration duration*, *sleep duration* (i.e., idle time between two vibrations), and *vibration frequency*. Using different combinations of these four parameters, we can generate a large group of vibration patterns used for distinctive vibration-based device credentials.

In this work, we use Google WearOS (i.e., v2.27)[16] to configure the vibration strengths and vibration durations of the built-in vibration motors in commodity wearable via the *VibrationEffect* method. Here the vibration strength is an integer value between 0 to 255, and the vibration duration and sleep duration can be any length of time in seconds. We discover that the vibration strength values do not reflect the amplitude of the generated vibration signals. Moreover, the same vibration strength will produce different readings from different wearable's accelerometers (see, e.g., Figure 2). This device-wise input-output relationship further validate our usages of vibration characteristics in wearables for the purpose of device authentication.

While there are many possible vibration patterns that can be generated as the vibration-based device credentials, not all of them are suitable for device authentication. The rule of thumb is that the vibration signals should be short in time (i.e., about 1s in our work) so that the device authentication process will have almost no impact to the user experience in using the device for normal applications. In addition, when reprogramming a vibration signal to replace the existing vibration-based device credential, it is important to choose a vibration signal that are much different from the previous one for better security. In this work, we use five vibration signals with different levels of the vibration strength as shown in Figure 3 (b). We note users can also create their own vibration patterns.

6.2 Data Pre-processing

The accelerometers capture vibration signals carrying the unique vibrations characteristics of wearables as well as accelerations caused by human body movements and gravity. To ensure the system can extract the vibration-based device credentials accurately, we adopt the following methods to pre-process the vibration signals captured by the wearable's accelerometers.

Data Filtering. When collecting the vibration signals for device authentication on a wearable, the accelerometers also capture noises (e.g., ambient sound and thermal noise) and interferences (e.g., human body movements and background music). WatchID filters the accelerometer data using a band-pass filter with the passband centered at the vibration frequency of the generated vibration signals to mitigate these noises and interferences. Specifically, we first use the fast Fourier transform to discover that the range of all our wearables' vibration frequencies is between 11.3Hz and 24.8Hz. In addition, the frequency of most human activities is below 10Hz [4]. Therefore we develop a Butterworth band-pass using the cutting-off frequencies of 10Hz and 24.8Hz to filter the vibration noises and interferences outside of this range.

Vibration Standardization. The vibration signals collected by a wearable's accelerometer are accelerations of three dimensions along x, y, and z axis. The range of values differ greatly among the three axes, even more among different device models. To ensure the comparability of data, the system applies the Z-score standardization method [21] to the accelerometer readings from each axis as follows:

$$a' = \frac{a - \mu}{\delta},$$

where a is a vibration acceleration value along a certain axis, μ and δ are the mean and standard deviation of the accelerations along the same axis respectively. After the standardization, the accelerometer data (a') is centered at 0 and scaled to have the standard deviation of 1. Thus, the data from different devices and dimensions are made to be comparable.

Orientation Alignment. Usually the orientation of a wearable keeps changing because its owner's wrist does not stay still for the most of the time. As a result, the directions of the three axes of the built-in accelerometers are varying accordingly. To ensure that our system can obtain the same device credentials regardless of the wearable's orientation, we need to subtract the gravitational acceleration ($9.8m/s^2$) from the accelerometer readings projected in each of the three directions. In particular, we adopt a low-pass filter [3] for this purpose:

$$a''_i = (1 - \beta)(a_i - g_i), \qquad i = \{x, y, z\},$$
$$\beta = \frac{dT}{t + dT},$$

where g_i and a_i are the projection of the gravitational acceleration and raw acceleration captured by the accelerometer along the i-th axis respectively, β is a filter factor determined by filter's time constant t and event delivery rate dT. Here, a''_i will be used by the system as the aligned acceleration. In this work, we empirically choose β to be 0.2.

6.3 Device Credential Extraction

After pre-processing the accelerometer data, WatchID needs to extract the vibration-based device credential and send them to the remote server for device authentication. To ensure the robustness and accuracy of WatchID, we need to precisely

determine the starting and ending points of the vibration signals used as the device credential. In particular, WatchID derives the short-time energy of the pre-processed accelerometer readings based on a sliding window:

$$E(t) = \sum_{n=t}^{t+w} a^2(n),$$

where $a(n)$ is the accelerometer reading at the time n and w is the size of the sliding window. The system examines $E(t)$ and determines the starting and ending points of the device credential depending on whether $E(t)$ is above or below the threshold, respectively. We empirically determine the threshold based on our study with three volunteers and five watches. We find that even if the volunteers' arms shake slightly, the short-time energy after Z-score standardization does not exceed the value of 0.4 for the Fossil watches and 0.01 for the Moto watches. Therefore, we set the threshold to 0.4 and 0.01 for the two types of watches respectively. In practice, this process can be done fairly easily and quickly. In addition, due to sampling variations in accelerometers, the number of samples of the same vibration duration may be slightly different. To solve this problem, we employ the cubic spline interpolation [12] to ensure the extracted device credentials have the same number of samples every time. Specifically, we interpolate each device credential to 200 samples, which can well preserve the details of a device credential captured by the maximum sampling rate (i.e., 50Hz) of wearbles' accelerometers within 4 seconds.

6.4 Device Authentication Using Convolutional Neural Network

While the vibration-based device credentials are observed to be unique for different wearables, modeling based analyses can quantitatively answer the question whether the set of device credentials of a particular device is a legitimate one. Toward this end, we propose to train a 1-dimensional convolutional neural network (1D CNN) on the fine-grained representations of device credentials and perform the device authentication on the remote server. With this approach, there is no need for the feature extraction process, which is required for traditional machine learning methods. Instead we can directly utilize the device credentials after pre-processing without loss of any information.

1D CNN has been used for signal processing and acceleration data analysis [20, 18, 1]. In this work, we design a 1D CNN with 4 convolutional layers, 2 max pooling layers, 1 flatten layer, 1 dropout layer and 1 fully connected layer. The parameters of our 1D CNN are specified in Figure 5. In the first two convolutional layers, we define 64 kernels with a kernel size of 2. Max pooling layer is introduced to reduce the complexity of the output of previous layer. In the third and fourth convolutional layers, 256 kernels with a kernel size of 2 are designed to learn more advanced features. A dropout layer is added to avoid overfitting and improve the generalization of the CNN model. In the fully connected layer, a softmax activation function is used to reduce the features to a vector of 2. We use the binary cross entropy as the loss function. An Adam optimizer [19] with a

Fig. 5: Architecture of the 1D CNN used in WatchID.

learning rate of 0.001 is used to optimize the neural network. The output of the softmax activation function contains the probabilities of two labels (i.e., 1 for legitimate device and 0 otherwise). Upon receiving a device credential, WatchID transforms the device credential into a 4×200 vector and feeds the vector into the 1D CNN to determine whether the received device credential matches the pre-registered device credential of the legitimate wearable.

7 Evaluation

7.1 Experimental Hardware and Scenarios

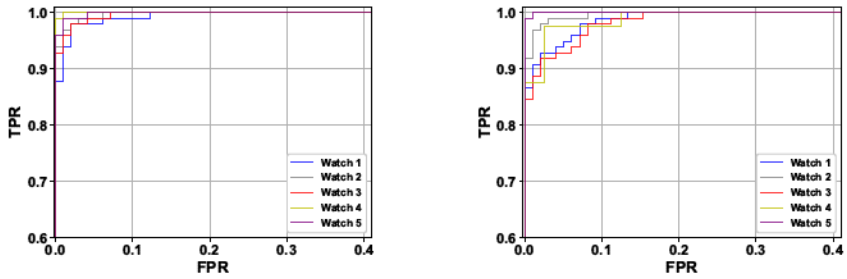
We use three Fossil Gen 5 and two Moto 360 Gen 3 smartwatches to evaluate the performance of WatchID. An app is developed to collect the vibration-based device credentials on these smartwatches using Google Wear OS (version 2.27) [16]. The collected device credentials are downloaded to a desktop to perform the model training and device authentication.

We evaluate the system under two scenarios: *on desk* and *on wrist* for practical usage situations. In the first scenario, we collect the vibration-based device credentials of each smartwatch when it is fixed on the desk, while in the second, we carry the operation when the watch is worn on a human wrist .

7.2 Data Collection

In the *on desk* scenario, we focus on studying the efficacy of the vibration-based device credentials. For each smartwatch, we collect 120 device credentials. In the *on wrist* scenario, we collect device credentials with different settings on the smartwatches to evaluate the efficacy and robustness of the system. In particular, we conduct experiments with 5 different vibration patterns, and 3 jamming attacks under different sound noises. In total, we have two participants collecting around 600 device credentials in the *on desk* scenario and 1680 device credentials in the *on wrist* scenario across over 4 weeks.

Unless stated otherwise, we use the vibration strength of 50 with 1 second vibration duration and 1 second sleep duration to generate vibrations. We use the maximum sampling rate of the smartwatches' accelerometers (i.e., 50Hz) to collect data. We randomly select 30 device credentials from a legitimate device and 30 device credentials from the other four watches (as attackers) to construct a training dataset. The rest of the data (i.e., 90 device credentials from the legitimate user and 90 device credentials from the attacker) is used for testing. We repeat the training and testing five times and use the average results to evaluate our system's performance.



(a) Watch on desk (b) Watch on wrist

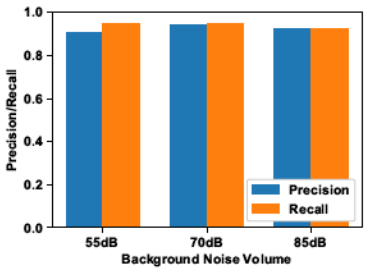
Fig. 6: Overall performance of WatchID with different smartwatches in different scenarios.

7.3 Evaluation metrics

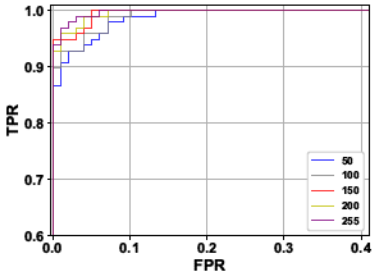
Precision. Precision is the ratio between the number of device credentials correctly predicted as from the legitimate user (i.e., true positive) to the overall number of the device credentials predicted as from the legitimate user (i.e., true positive + false positive). We want to have a high precision to avoid mistakenly identifying the attacker's device credentials as an legitimate one.
Recall. Recall is the ratio between the number of device credentials correctly predicted as the legitimate (i.e., true positive) to the overall number of legitimate device credentials (i.e., true positive + false negative). A low recall means a sizable amount of legitimate user's device credentials are mistakenly identified as the illegitimate ones. This is not desirable for user experience.
Rejection Rate. We define the rejection rate as the ratio between the number of the attacker's device credentials successfully identified as the illegitimate ones (i.e., true negative) to all the stolen device credentials (i.e., true negative + false positive). We want to achieve a high rejection rate since none of the attacker's device credentials should pass the device authentication.
ROC Curve. ROC curve plots true positive rate (TPR) against false positive rate (FPR). The TPR denotes the rate of the legitimate user's device credentials passing the system, while FPR denotes the rate of the attackers' device credentials passing the system. Through varying prediction thresholds, we can get a series of TPR and FPR and draw ROC curves to evaluate the system performance. The closer to the point $(0, 1)$ the ROC curve, the better the performance. Thus, we choose the TPR and FPR at the point closest to $(0, 1)$ on the ROC curve as our system's optimal performance.

7.4 Overall Performance

We first evaluate the performance of our system with the watch on human wrist or on the desk. For the *on desk* scenario, a watch is horizontally laying on the surface of a desk with its face up and its belt taped the desk by sticky tapes. This is quite an ideal case with few impacting factors to disturb the data collection process. For the *on wrist* case, the watch is worn on a person's wrist with his



(a) Under jamming attacks.



(b) Watch 1 under five different vibration strengths.

Fig. 7: Performance under jamming attacks and different vibration strengths.

forearm horizontally laying on the desk and the watch facing up. Specifically, 5 smartwatches are used to collect the vibration data. We alternatively select one watch as a legitimate device and the other four watches as attackers. Figure 6 (a) shows the ROC curve of the *on desk* scenario, and we can observe that our system can achieve an average optimal TPR of 98% and FPR of 2% among 5 smartwatches. For the *on wrist* situation, our system can still achieve an average optimal TPR of 95% and FPR of 5% as shown in Figure 6 (b). From these two figures, we find that human wrist slightly impacts the performance in our authentication system. Moreover, the two Moto watches (i.e., Watch 4 and 5) have slightly better performance than the three Fossil watches (i.e., Watch 1, 2, and 3). This observation is in line with our observations from Figure 3 where the two Moto watches have more distinguishable features from the Fossil watches. Overall, those results demonstrate that our system have good authentication performances no matter whether a watch is put on a desk or worn on human wrists. Therefore vibration signals from wearables can indeed serve as a reliable and consistent device credential.

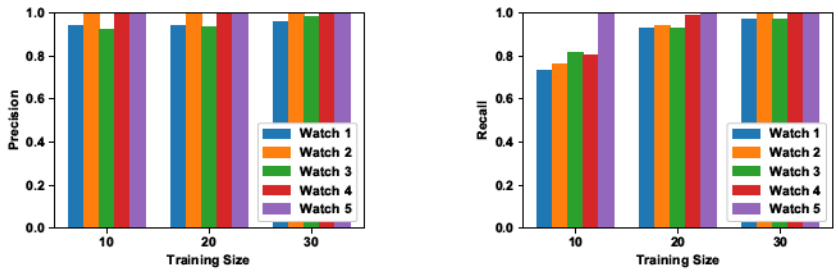
7.5 Effectiveness Under Different Attacks

Against Random Attacks. We first explore the robustness of our system against random attacks. Specifically, we alternatively select two watches out of the five with one as a legitimate watch and the other as an illegitimate watch. Then, we train our system using the device credentials from those two selected watches and use the other three unselected watches to mimick random attacks. Our experimental results show that the three random attackers are always classified as the illegitimate watches by our system with a 100% rejection rate. Therefore our system is robust against random attacks.

Against Jamming Attacks. We next test our system under jamming attacks by playing different volumes (i.e., 55dB, 70dB, 85dB) of background sound noises. These volumes are selected to correspond to various real-life environmental noises. For instance, the average decibel level of human speech is near 55dB.

Table 1: Performance under jamming attacks.

Noise(dB)	Precision(%)	Recall(%)
55	90.57	95.31
70	94.68	95.31
85	92.51	92.8



(a) (b)

Fig. 8: Performance under different training sizes.

Living room music, radio or TV-audio, and sound of vacuum cleaner are close to 70dB. Power mowers, motorcycles, diesel trucks can produce noises about 85dB. As shown in Figure 7 (a) and Table 1, our system can achieve an average precision and recall around 92% and 94% under the jamming attacks at various typical audio volumes. This result indicates that our system can still perform well under realistic jamming attacks.

Against Credential Stealing Attacks. Here we assume an attacker has gained access to a legitimate user's device credential and our system has informed the user to reset his/her device credential. Specifically, we select one watch as the legitimate device and reset its credential by using a new vibration strength (i.e., 100) from the original strength (i.e., 50 by default). The other four watches are treated as illegitimate ones with their original device credentials.

After the legitimate user's device credential is reset, we retrain a new 1D CNN model after the same data collection and preprocessing steps. To simulate the credential stealing attacks, the attacker will still try to use the previous legitimate user's device credential to bypass the system. Our experimental result show that this type of requests are denied by our system using the newly trained 1D CNN model with a 100% rejection rate. This demonstrates that reprogrammable WatchID can successfully defend against credential stealing attacks.

7.6 Robustness Under Different Vibration Patterns

Device credential reconfiguration plays an important role in the our system. Hence, we study the robustness of our system under different vibration patterns to generate the device credentials. We know that different vibration strengths of

Table 2: Performance under different training sizes (P: Precision(%); R: Recall(%)).

Training Size	Watch 1		Watch 2		Watch 3		Watch 4		Watch 5	
	P	R	P	R	P	R	P	R	P	R
10	93.54	72.91	100	75.42	91.82	81.25	100	79.94	100	100
20	93.42	92.17	100	93.88	92.85	92.34	100	98.51	100	100
30	95.54	96.8	100	99.2	97.54	96.85	100	100	100	100

a smartwatch can generate different device credentials as shown in Figure 3(b). In this study, we test 5 different device credentials of a legitimate user's watch (i.e., Watch 1) by setting 5 different vibration strengths (i.e., 50, 100, 150, 200, 255). And the device credentials of the other four watches (i.e., illegitimate ones) are generated using the same vibration strength (i.e., 50). Figure 7 (b) shows the ROC curves of our system under different vibration patterns. We find that our system has a similar optimal performance (i.e., about 95% in TPR and 5% in FPR) under different vibration patterns. Therefore our system has achieved good authentication results under different levels vibration strengths or associated vibration patterns.

It is also worth noting that a larger vibration strength (e.g., 255) can generate a slightly better performance. However, since a lower vibration strength generates more stable patterns as demonstrated in Section 4, we adopt the value of 50 as the default vibration strength in WatchID.

7.7 Impact of Training Size

Amount of data required by an authentication system is an importance parameter in order to ensure and maintain a high level of performance. To study the impact of different data sizes to our system, we generate 10, 20, 30 sets of device credentials for each of the five watches. For a specific size (i.e., 10), we pick one watch (i.e., Watch 1) as a legitimate device and use all the 10 sets of its credentials with the label of 1 as a part of the training data, and pick another 10 sets randomly from the other four watches with the labels of 0 as the other part of the training data. Then WatchID performs the device authentication process for this set of data. Our experimental results are presented in Figure 8 and Table 2.

We observe that our system can achieve an average precision of 97% using only 10 device credentials for a legitimate device (20 in total). As the size of the training data grows, the system performance improves accordingly. More specifically, the average precision and recall reach 98% and 99% respectively when 20 or more device credentials for a legitimate device are used. These results indicate our system can achieve good performance with only a limited number of device credentials. As a result, our system is fast and efficient in training of authentication models with a high level of performance.

8 Conclusion

In this paper, we devise WatchID, a vibration-based device authentication system for wearables. The system can provide an extra layer of security to the traditional user authentication methods without requiring a user's participation. WatchID utilizes the manufacturing imperfections of a wearable's vibration motor, device body, and accelerometers to create unique vibration characteristics, using them as device credentials to determine the wearable's identity. Our system is more practical and convenient than existing methods as the vibration-based device credentials are reprogrammable by changing the vibration patterns on wearables. We extensively study the vibration characteristics of different wearables and develop data pre-processing methods to ensure the system's robustness. We also develop a lightweight CNN model to capture the unique vibration characteristics and predict the wearable's identity under various practical scenarios. Over 2500 vibration-based device credentials are collected in the experiments with five commodity smartwatches across 4 weeks. We demonstrate that our system can achieve an average precision and recall of 98% and 94% under various scenarios of vibration patterns and training sizes. We also show that our system can achieve a 100% rejection rate under different types of attacks.

Acknowledgment - Need to change

This work was partially supported by the NSF Grants CCF1909963, CCF2000480, CCF2028858, CCF2028873, CNS1954959, CNS2120276, and CNS2120350.

References

1. Abdoli, S., Cardinal, P., Koerich, A.L.: End-to-end environmental sound classification using a 1d convolutional neural network. Expert Systems with Applications **136**, 252–263 (2019)
2. Aloul, F., Zahidi, S., El-Hajj, W.: Two factor authentication using mobile phones. In: 2009 IEEE/ACS International Conference on Computer Systems and Applications. pp. 641–644. IEEE (2009)
3. AndroidDeveloper: Work with raw data, use the accelerometer, `https://developer.android.com/guide/topics/sensors/sensors_motion#sensors-motion-accel`
4. Antonsson, E.K., Mann, R.W.: The frequency content of gait. Journal of biomechanics **18**(1), 39–47 (1985)
5. Bojinov, H., Michalevsky, Y., Nakibly, G., Boneh, D.: Mobile device identification via sensor fingerprinting. arXiv preprint arXiv:1408.1416 (2014)
6. Brik, V., Banerjee, S., Gruteser, M., Oh, S.: Wireless device identification with radiometric signatures. In: Proceedings of the 14th ACM international conference on Mobile computing and networking. pp. 116–127 (2008)
7. Clancy, T.C., Kiyavash, N., Lin, D.J.: Secure smartcardbased fingerprint authentication. In: Proceedings of the 2003 ACM SIGMM workshop on Biometrics methods and applications. pp. 45–52 (2003)

8. Danev, B., Zanetti, D., Capkun, S.: On physical-layer identification of wireless devices. ACM Computing Surveys (CSUR) **45**(1), 1–29 (2012)
9. Das, A., Borisov, N., Caesar, M.: Do you hear what i hear? fingerprinting smart devices through embedded acoustic components. In: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security. pp. 441–452 (2014)
10. Das, A., Borisov, N., Caesar, M.: Tracking mobile web users through motion sensors: Attacks and defenses. In: NDSS (2016)
11. Dey, S., Roy, N., Xu, W., Choudhury, R.R., Nelakuditi, S.: Accelprint: Imperfections of accelerometers make smartphones trackable. In: NDSS (2014)
12. Dukkipati, R.V.: Numerical methods (2010)
13. Eberz, S., Paoletti, N., Roeschlin, M., Kwiatkowska, M., Martinovic, I., Patané, A.: Broken hearted: How to attack ecg biometrics (2017)
14. Fujii, H., Shigematsu, N., Kurokawa, H., Nakagawa, T.: Telelogin: a two-factor two-path authentication technique using caller id. NTT Technical review **6**(8), 1–6 (2008)
15. Garcia-Romero, D., Espy-Wilson, C.Y.: Automatic acquisition device identification from speech recordings. In: 2010 IEEE International Conference on Acoustics, Speech and Signal Processing. pp. 1806–1809. IEEE (2010)
16. Google: Wear OS, `https://wearos.google.com/`
17. Jøsang, A., Sanderud, G.: Security in mobile communications: Challenges and opportunities. In: Proceedings of the Australasian information security workshop conference on ACSW frontiers 2003-Volume 21. pp. 43–48. Citeseer (2003)
18. Kim, J.W., Jang, J.S., Yang, M.S., Kang, J.H., Kim, K.W., Cho, Y.J., Lee, J.W.: A study on fault classification of machining center using acceleration data based on 1d cnn algorithm. Journal of the Korean Society of Manufacturing Process Engineers **18**(9), 29–35 (2019)
19. Kingma, D.P., Ba, J.: Adam: A method for stochastic optimization. arXiv preprint arXiv:1412.6980 (2014)
20. Kiranyaz, S., Avci, O., Abdeljaber, O., Ince, T., Gabbouj, M., Inman, D.J.: 1d convolutional neural networks and applications: A survey. Mechanical systems and signal processing **151**, 107398 (2021)
21. Kreyszig, E.: Advanced engineering mathematics 10th edition (2009)
22. Lashkari, A.H., Farmand, S., Zakaria, D., Bin, O., Saleh, D., et al.: Shoulder surfing attack in graphical password authentication. arXiv preprint arXiv:0912.0951 (2009)
23. Li, H., Xu, C., Rathore, A.S., Li, Z., Zhang, H., Song, C., Wang, K., Su, L., Lin, F., Ren, K., et al.: Vocalprint: A mmwave-based unmediated vocal sensing system for secure authentication. IEEE Transactions on Mobile Computing (2021)
24. Lin, F., Song, C., Zhuang, Y., Xu, W., Li, C., Ren, K.: Cardiac scan: A non-contact and continuous heart-based user authentication system. In: Proceedings of the 23rd Annual International Conference on Mobile Computing and Networking. pp. 315–328 (2017)
25. Liu, J., Chen, Y., Dong, Y., Wang, Y., Zhao, T., Yao, Y.D.: Continuous user verification via respiratory biometrics. In: IEEE INFOCOM 2020-IEEE Conference on Computer Communications. pp. 1–10. IEEE (2020)
26. Liu, J., Wang, Y., Chen, Y., Yang, J., Chen, X., Cheng, J.: Tracking vital signs during sleep leveraging off-the-shelf wifi. In: Proceedings of the 16th ACM International Symposium on Mobile Ad Hoc Networking and Computing. pp. 267–276 (2015)

27. Polak, A.C., Dolatshahi, S., Goeckel, D.L.: Identifying wireless users via transmitter imperfections. IEEE Journal on selected areas in communications **29**(7), 1469–1479 (2011)
28. Polak, A.C., Goeckel, D.L.: Rf fingerprinting of users who actively mask their identities with artificial distortion. In: 2011 Conference Record of the Forty Fifth Asilomar Conference on Signals, Systems and Computers (ASILOMAR). pp. 270–274. IEEE (2011)
29. Ratha, N.K., Bolle, R.M., Pandit, V.D., Vaish, V.: Robust fingerprint authentication using local structural similarity. In: Proceedings Fifth IEEE Workshop on Applications of Computer Vision. pp. 29–34. IEEE (2000)
30. Ren, Y., Chen, Y., Chuah, M.C., Yang, J.: Smartphone based user verification leveraging gait recognition for mobile healthcare systems. In: 2013 IEEE international conference on sensing, communications and networking (SECON). pp. 149–157. IEEE (2013)
31. Revenkar, P., Anjum, A., Gandhare, W.: Secure iris authentication using visual cryptography. arXiv preprint arXiv:1004.1748 (2010)
32. Sanchez-Reillo, R., Sanchez-Avila, C.: Iris recognition with low template size. In: International Conference on Audio-and Video-Based Biometric Person Authentication. pp. 324–329. Springer (2001)
33. Shi, C., Liu, J., Borodinov, N., Leao, B., Chen, Y.: Towards environment-independent behavior-based user authentication using wifi. In: 2020 IEEE 17th International Conference on Mobile Ad Hoc and Sensor Systems (MASS). pp. 666–674. IEEE (2020)
34. Sun, L., Wang, Y., Cao, B., Philip, S.Y., Srisa-An, W., Leow, A.D.: Sequential keystroke behavioral biometrics for mobile user identification via multi-view deep learning. In: Joint European Conference on Machine Learning and Knowledge Discovery in Databases. pp. 228–240. Springer (2017)
35. Trippel, T., Weisse, O., Xu, W., Honeyman, P., Fu, K.: Walnut: Waging doubt on the integrity of mems accelerometers with acoustic injection attacks. In: 2017 IEEE European symposium on security and privacy (EuroS&P). pp. 3–18. IEEE (2017)
36. Wazid, M., Zeadally, S., Das, A.K.: Mobile banking: evolution and threats: malware threats and security solutions. IEEE Consumer Electronics Magazine **8**(2), 56–60 (2019)
37. Zeng, Y., Pande, A., Zhu, J., Mohapatra, P.: Wearia: Wearable device implicit authentication based on activity information. In: 2017 IEEE 18th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM). pp. 1–9. IEEE (2017)
38. Zhang, Q., Zhou, D., Zeng, X.: Heartid: A multiresolution convolutional neural network for ecg-based biometric human identification in smart health applications. Ieee Access **5**, 11805–11816 (2017)
39. Zhang, Y., Xia, P., Luo, J., Ling, Z., Liu, B., Fu, X.: Fingerprint attack against touch-enabled devices. In: Proceedings of the second ACM workshop on Security and privacy in smartphones and mobile devices. pp. 57–68 (2012)
40. Zhao, T., Wang, Y., Liu, J., Chen, Y., Cheng, J., Yu, J.: Trueheart: Continuous authentication on wrist-worn wearables using ppg-based biometrics. In: IEEE INFOCOM 2020-IEEE Conference on Computer Communications. pp. 30–39. IEEE (2020)
41. Zhou, Z., Diao, W., Liu, X., Zhang, K.: Acoustic fingerprinting revisited: Generate stable device id stealthily with inaudible sound. In: Proceedings of the 2014

ACM SIGSAC Conference on Computer and Communications Security. pp. 429–440 (2014)