OneTouch: Effortless 2FA Scheme to Secure Fingerprint Authentication with Wearable OTP Token

Yihui Yan [†‡]
School of Information Science and Technology
ShanghaiTech University

Zhice Yang [*]
School of Information Science and Technology
ShanghaiTech University

Abstract

The security of fingerprint authentication is increasingly at risk from various attacks. Two-factor authentication (2FA) is a widely adopted approach to mitigate unauthorized access caused by compromised credentials. However, existing 2FA methods are not well-suited for direct use with fingerprint authentication devices, as they often require distinct and additional user interactions that disrupt established user habits, or they depend on specialized I/O interfaces that are not available on these devices. In this paper, we propose a novel 2FA scheme termed OneTouch, which maintains the simplicity of conventional fingerprint authentication - merely touching the scanner with a finger - while integrating a secondary challenge-response OTP (One-Time Password) authentication scheme using a wearable OTP token. This is accomplished by transforming the fingerprint scanner from a device designed for imaging fingerprints to an I/O device capable of capturing temporal voltage variations of the contact object. Consequently, OneTouch is capable of establishing touch-based communication channels between the scanner and the wearable token for OTP protocol exchange. By directly wiring the OTP token to the authentication device through human body, OneTouch minimizes the risk of interception by adversaries, thereby reducing the attack surface. We provide an extensive discussion of the security risks and evaluate the effectiveness of the touch-based channel for OTP credential exchange.

1 Introduction

Fingerprints have long been used for authentication due to their inherent uniqueness and permanence. However, recent technological advances have introduced new security challenges for fingerprint authentication systems. For instance, the fingerprint acquisition modules used in mobile devices, with their small form factors, limit the completeness of fingerprint collection, resulting in weak fingerprint templates and allowing a synthetic fingerprint sample to bypass multiple users' authentication systems [43]. Furthermore, advanced 3D printing technology has made it easier than ever to fabricate high-fidelity fingerprint replicas from weak or leaked fingerprint data [17]. Forged fingerprint artifacts could then be exploited to spoof the authentication system and gain access to a user's digital and physical assets, including sensitive information such as accounts and passwords stored on mobile devices (*e.g.*, laptops) and private spaces secured by fingerprint-locked doors, posing significant security risks.

For password-based authentication, two-factor authentication (2FA) is commonly used to mitigate the risk of unauthorized access caused by weak or leaked passwords [19]. For instance, after entering a username and password, the 2FA process is complemented by the entry of an OTP (One-Time Password) received via SMS (Short Message Service). This additional step allows the authentication system to confirm that the person being authenticated also possesses the authorized phone number, serving as the secondary factor. Such a scheme is extensively utilized across a variety of web and mobile applications.

2FA can also be used to secure fingerprint authentication systems. However, if the 2FA method introduces additional interaction overhead, *e.g.*, manually entering an OTP, it could undermine the convenience of fingerprint authentication. Therefore, one widely discussed solution is to use accessory devices, such as wearables, to automatically complete 2FA via wireless channels, *e.g.*, Bluetooth [16],while authenticating fingerprint. However, vulnerabilities associated with wireless channels are frequently reported [52], and this approach is not compatible with authentication devices that lack wireless interfaces. For example, among the 50 best-selling fingerprint door locks on Amazon, 20 (40%) do not have Bluetooth support, and 7 (14%) do not have any wireless capabilities.

To this end, we propose OneTouch, an effortless 2FA scheme to secure fingerprint authentication using a wearable OTP token. As shown in Figure 1, OneTouch is built upon existing fingerprint authentication devices. It not only identifies the fingerprint but also seamlessly verifies the wearable

[†]Also with Shanghai Institute of Microsystem and Information Technology, Chinese Academy of Science.
[‡]Also with University of Chinese Academy of Sciences.
[*]Corresponding Author: Zhice Yang.

token. OneTouch has two key features. First, throughout the entire authentication process, the user simply needs to press their finger onto the scanner once, with no further interactions required, preserving the user experience consistent with original fingerprint authentication. Second, OneTouch only requires the authentication device's built-in capacitive fingerprint scanner[1], without the need for additional I/O (Input/Output) interfaces. This means OneTouch can be integrated into existing fingerprint devices via a firmware update.

The grand challenge in realizing OneTouch lies in establishing a non-intrusive communication channel between the fingerprint scanner and the wearable token for exchanging OTP credentials. Our key innovation is recognizing that, in addition to imaging fingerprints, a fingerprint scanner can function as a general I/O device capable of generating and capturing temporal voltage variations on the contact object.

This approach stems from our understanding of the working mechanisms of fingerprint scanners. First, during operation, fingerprint scanners apply a drive voltage to the sensor surface, a mechanism that prior work has shown can transmit signals from the fingerprint scanner to the contact finger, which can then be detected by a wearable device [23]. We refer to this as a *touch-based scanner-to-wearable* channel. Second, in this paper, we further identify another important feature of capacitive fingerprint scanners: they record voltage variations on the contact surface line-by-line to generate the fingerprint image. We realize that this feature can be leveraged for high-speed temporal signal acquisition, such as sensing voltage changes applied by a wearable device to the body. We refer to this capability as the *touch-based wearable-to-scanner* channel.

These two touch-based channels form the foundation for OneTouch to establish bidirectional communication between the fingerprint scanner and the wearable token. By utilizing them, it enables seamless and secure OTP authentication. The main contributions of this paper include:

- We systematically study and explain the imaging mechanism of capacitive fingerprint sensors, revealing that they record capacitive voltage in a line-by-line scanning manner into image pixels.
- We present a novel method for using fingerprint sensors to capture temporal voltage signal, opening up new opportunities for using fingerprint scanners as an input interface for temporal signal acquisition.
- We design and implement OneTouch, a system that leverages the user's body as a medium to establish a bidirectional touch-based messaging mechanism between existing fingerprint scanners and compatible wearable devices, serving as a seamless 2FA method to secure fingerprint authentication.
- We conduct an evaluation and security analysis of the full authentication process of OneTouch in a test group of 30 participants. The experiments demonstrate the feasibility of touch-based channels under different settings, as well as the OneTouch's usability, *e.g.*, efficiency, effectiveness and user satisfaction.

[1]The 50 best-selling fingerprint door locks on Amazon all adopt capacitive fingerprint scanner.

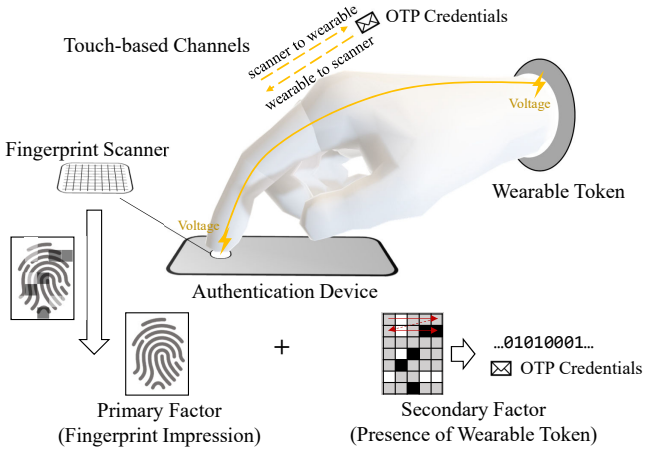


Figure 1: **Overview of OneTouch.** The user wears a wearable token and places their finger on the fingerprint scanner to initiate the authentication process. OneTouch enhances the standard fingerprint authentication system by not only verifying the user's fingerprint but also automatically confirming the presence of the token via the touch-based channels.

2 Overview of OneTouch

2.1 Design Goals

Given the increasing threats to fingerprint authentication, rather than focusing solely on improving the fingerprint system itself, *e.g.*, developing new anti-spoofing fingerprint scanners [42], incorporating additional authentication factors is a reasonable and viable option [11, 15]. The advantage of 2FA lies in its proven effectiveness and ease of deployment. In the case of fingerprint authentication, the introduced secondary factor should meet the following criteria.

- **Seamless Interaction Flow**. Fingerprint authentication is commonly used in high-frequency scenarios, such as unlocking phones and door locks. Any extra steps, such as entering a PIN, can disrupt the smoothness of the authentication process. Therefore, a 2FA solution should prioritize preserving the ease of use that fingerprint authentication originally offers.
- **Minimal Hardware Requirements**. Fingerprint-enabled devices are already widely deployed. Introducing additional hardware would increase costs and reduce adoption willingness. We envision that a viable 2FA solution should be smoothly deployable without requiring hardware changes or device replacements.
- **Enhanced Security Features**. The additional factor itself should provide extra security features that fingerprint authentication alone cannot offer, such as resistance to replay attacks. It should have a reduced attack surface, rather than

introducing new security risks. For example, methods relying on wireless channels that are vulnerable to eavesdropping or injection [7, 8, 52] should be avoided.

2.2 Threat Model

This work focuses on computing devices that use fingerprint identification/verification as an authentication method, referred to as the *authentication device*. The adversary aims to gain access to the device user's (victim's) assets by bypassing the device's authentication mechanisms.

Given the awareness of potential threats to fingerprint authentication, we assume that the user is willing to adopt additional measures or accessories, *e.g.*, a wearable token, to enhance the security of the authentication device. We also assume that the manufacturer of the authentication device has an incentive to continually improve and enhance the security of their product, for example through new releases or firmware upgrades.

We assume the adversary is not a network attacker. They have physical access to the authentication device, but cannot disassemble it [13], as this typically requires time and specific conditions. Additionally, we assume the adversary may possess sophisticated capabilities to spoof fingerprint authentication. They can fabricate physical fingerprint artifacts [2] based on legitimate fingerprint impressions obtained through various means, *e.g.*, social media exposure [1], leaked databases [3], social engineering [4], *etc.* We assume the adversary possesses advanced capabilities to eavesdrop on and generate arbitrary wireless signals in the surrounding area. However, to maintain stealth, the adversary avoids direct physical contact with the user, *e.g.*, touching the user's skin.

2.3 Idea of OneTouch

We propose a 2FA solution, OneTouch, that seamlessly integrates with existing fingerprint authentication systems to meet the requirements outlined above. The working flow of OneTouch is illustrated in Figure 1. Compared to standard fingerprint authentication, the interaction remains largely the same: the user simply places their finger on the device's fingerprint scanner for authentication. However, OneTouch introduces two key differences on the device side. First, the user must wear a wearable token that supports OneTouch. Second, the authentication device's software or firmware must also be compatible with OneTouch. These new components enable the authentication device to collect and verify two factors during the user's touch: 1) the user's inherent fingerprint, and 2) the presence of the specific wearable token. The former factor has already been supported by standard fingerprint scanners, while the latter relies on a touch-based communication channel established between the wearable token and the scanner.

On-Body Communication. The touch-based channel utilized by OneTouch is a form of on-body communication leveraging capacitive sensing technology [20,23], where the human body acts as a conductor. When a device in contact with the body (*e.g.*, via an electrode) alters its voltage, another device in contact with the same body can detect the voltage change. This enables communication between devices in direct contact with the human body, *e.g.*, wearables and implants [28].

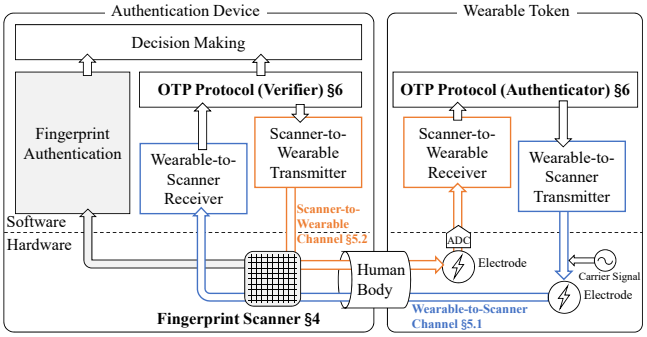


Figure 2: **System Architecture.**

Fingerprint Scanner as an On-body Communication Interface. To facilitate the transmission and reception of on-body signals, electrodes and other components can be added to the wearable token. However, fingerprint scanners, by design, do not typically support this functionality. Capacitive fingerprint scanners (Figure 3) consist of an array of sensors that are highly sensitive to voltage changes on the contact surface. These sensors measure changes line-by-line, making them capable of detecting subtle variations in voltage. As a result, when the wearable token induces a voltage change on the user's body, the fingerprint scanner records not only the spatial distribution of the fingerprint ridges but also the voltage changes occurring at specific moments. This mechanism can be leveraged for establishing communication from the wearable token to the scanner.

2.4 System Overview

OneTouch leverages the existing hardware capabilities of capacitive fingerprint scanners to implement the touch-based communication channel. When the user touches the scanner, the authentication device performs fingerprint verification while simultaneously verifying the possession of the wearable token. This approach enables a seamless and efficient authentication process. The system diagram of OneTouch is shown in Figure 2. In Section 3, we will provide a detailed explanation of the fingerprint scanner's working mechanisms. In Section 4.1 and Section 4.2, we will discuss the design of the downlink and uplink touch-based communication channels. Finally, in Section 5, we will describe the challenge-response OTP protocol between the scanner and the wearable token.

3 Capacitive Fingerprint Scanner

As shown in Figure 3(a), a typical capacitive fingerprint scanner consists of two main components: the sensor and the control circuit (controller). The sensor is composed of an array of small capacitive sensing elements. The controller manages

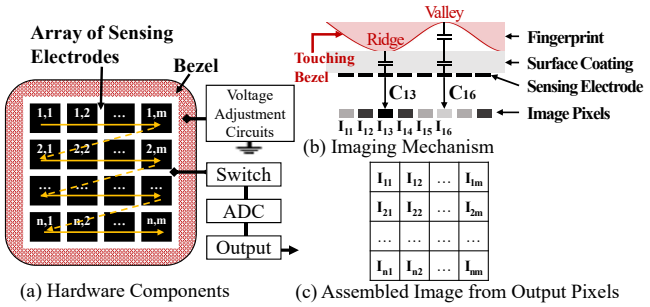


Figure 3: **Capacitive Fingerprint Scanner.**

the operation of sensing elements, performs analog-to-digital conversion (ADC) of the output signals, buffers the data, and transmits it to the next-stage processing unit. In this section, we will first explain the imaging mechanism of the scanner in Section 3.1, followed by an investigation into how on-body voltage influences the imaging results in Section 3.2.

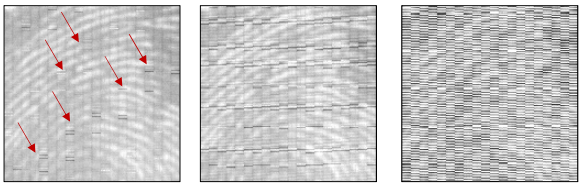
3.1 Imaging Mechanism

The surface of the sensing array forms the sensing area of the fingerprint scanner. Each sensing element in the array is a capacitor, consisting of an electrode and a default capacitance value. As shown in Figure 3(b), when a user places their finger on the surface, the skin's ridges and valleys affect the capacitance of the elements to varying degrees. For instance, the ridges, being closer to the sensor electrode, increase the capacitance of the corresponding sensing elements. As a result, the capacitance values of the elements can be used to reflect the texture of the contacting skin.

The array consists of thousands of sensing elements, and measuring and recording the capacitance of all elements simultaneously would significantly increase circuit complexity and cost. As a result, industrial practice typically involves scanning the elements sequentially [6]. The controller uses a switching circuit to select elements row by row, while an ADC digitizes the capacitance values one by one. Although the elements scanned earlier capture capacitance data before those scanned later, the total scan time for the entire array is typically on the order of dozens of milliseconds. During this brief period, the finger typically remains still, allowing the capacitance values captured at different times to be assembled into a 2D image that reflects the spatial distribution of the ridges and valleys. The pixel intensity in this image corresponds to the capacitance values of the sensing elements at the corresponding positions in the sensing array (Figure 3(c)).

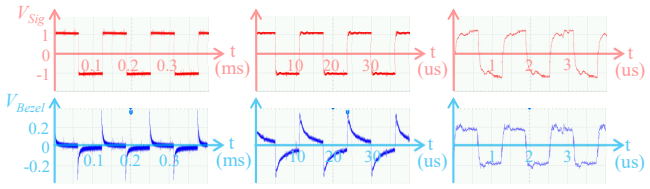
3.2 Imaging with On-body Voltage Signals

Capacitance measurement is a key aspect of the above imaging process. However, capacitance, which represents the ability to store electrical charge, is a physical property that cannot be easily measured directly. Given the relationship between capacitance and voltage, most measurement techniques make use of voltage. For example, the scanner can apply a known *drive voltage* to the electrodes, and as the capacitance changes,



(a) 8 kHz (b) 80 kHz (c) 800 kHz

Figure 4: **Impact of On-body Voltage V_{Sig} on Fingerprint Images.** V_{Sig} is a square wave and set to different frequencies.



(a) 8 kHz (b) 80 kHz (c) 800 kHz

Figure 5: **Impact of On-body Voltage V_{Sig} on V_{Bezel}.**

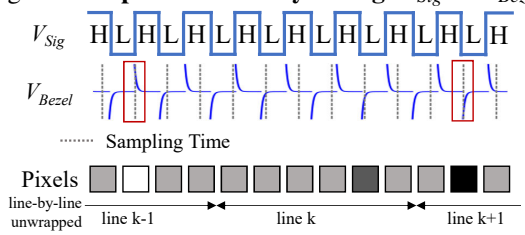


Figure 6: **Explanation of Imaging Results with Low-Frequency V_{Sig}.** Pixel values are determined by both V_{Bezel} and the scanner's sampling time.

the voltage across the electrodes will also vary. By measuring this voltage change, the scanner can indirectly infer the variation in capacitance. This raises an intriguing question: if the contacting object itself carries a biased voltage, will it affect the scanner's output? This issue is closely related to our goal of on-body communication, so we conducted a series of empirical studies to explore this effect.

We applied an on-body voltage V_{Sig} to the wrist of a participant using a signal generator and collected the output images from various fingerprint scanners. We observed that:

1. A constant voltage signal has minimal to no effect on the output image.
2. A varying voltage signal causes interference in certain regions of the output image, and the extent of this interference depends on the frequency of V_{Sig}.

The first observation can be explained by the scanner's discharge mechanism. As shown in Figure 3(a), the border surrounding the sensor array is referred to as the bezel. When the user touches the sensor, they also make contact with the bezel. One design purpose of the bezel is to protect the sensor from electrostatic discharge. For example, when the human body is carrying static charge, the bezel channels the discharge current to the voltage adjustment circuit, which consumes the discharge energy. Therefore, when a fixed voltage is applied to the finger, its effect will be neutralized by this module, so it does not affect the imaging results.

The second observation is more intriguing. We used a square wave as the V_{Sig} signal and Figure 4 shows the imaging results from one of the tested scanners (FPC1020AM by Fingerprint Cards AB). The results reveal that the impact of V_{Sig} does not exhibit the expected continuity and alternation trend of a square wave. Instead, the degree of interference is proportional to the frequency of V_{Sig}.

To better understand this phenomenon, we measured the voltage V_{Bezel} at the bezel, which reflects the scanner's discharge response. Figure 5 shows the synchronized waveform of V_{Sig} and V_{Bezel}. The curve of V_{Bezel} shows the discharge of the scanner follows a typical exponential decay. When the frequency of V_{Sig} is high enough (*e.g.*, 800 kHz), the discharge speed can no longer keep up. At this point, the voltage measured by the electrodes will be biased by the voltage from the finger, and the output image will be primarily driven by V_{Sig}.

Further, Figure 4(a)(b) show that at lower frequencies of V_{Sig}, the image may still occasionally contain interference caused by V_{Sig}. As shown in Figure 6, this happens because, at the moment of sampling, the scanner may encounter situations where V_{Sig} has not fully discharged. Moreover, since the scanner's sampling pace does not synchronize with the period of V_{Sig}, the interference appears with a certain periodicity.

4 Touch-Based Channels

Based on the previous section, this section first introduces a touch-based channel that allows the scanner to receive information through on-body signals, without the need for any hardware updates or modifications (Section 4.1). Next, building on existing work, we enable the scanner to transmit signals to the body, which is essential for supporting protocols that require bidirectional communication (Section 4.2). Then, when the user touches the scanner with a compatible wearable token, a valid data connection is established between the devices.

4.1 Wearable-to-Scanner Channel

According to Section 3.2, since the scanner can capture high-frequency on-body voltage signals, as shown in Figure 2, we use electrodes in the wearable token to apply modulated voltage signals to the body, transmitting information to the scanner (modulation). The scanner then extracts this information from the captured images (demodulation).

4.1.1 Modulation and Demodulation

As shown in Figure 7(a), we use on-off modulation to convey bits. The wearable token applies a high-frequency V_{Sig} onto the body to represent bit "1" and mutes V_{Sig} to 0 V to represent bit "0". This is a simple yet effective method. When a high-frequency V_{Sig} is applied, noticeable interference appears in the fingerprint image. To simplify the wearable token's design, we use a clock signal as the carrier, allowing modulation to be achieved by simply switching this signal on and off to generate the desired V_{Sig}.

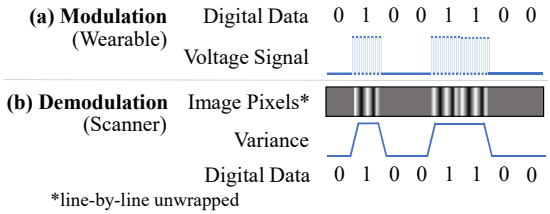


Figure 7: **Modulation of Wearable-to-Scanner Channel.**

The high-frequency carrier wave generates a high-frequency footprint in the fingerprint image. As a result, we use pixel variance to distinguish between bit "0" and bit "1". Specifically, the scanner unwraps the captured image pixels line by line in their imaging sequence, then calculates the intensity variance using a sliding window. While the fingerprint's ridges and valleys also affect the image pixels, they produce variance levels much lower than those caused by the modulated voltage signals. For instance, when an 800 kHz square wave with amplitudes ranging from -1 V to 1 V is applied to the FPC1020AM scanner, the resulting variance value is four times greater than that of a fingerprint image without interference. Additionally, due to variations in discharge circuits, the optimal carrier frequency may vary slightly across scanners. However, a common non-optimal value is typically sufficient for most scenarios.

4.1.2 Synchronization

The time at which the scanner begins capturing the image may not necessarily align with the time the wearable token starts emitting voltage signals. As a result, the data signal can appear at any position within the fingerprint image. To ensure the correct order of bits, we package the data into packets, each consisting of a preamble and a payload. The preamble is a predefined signal pattern, *e.g.*, "1000000001", that can be used to locate its position within the image prior to demodulation.

Once the start of the data packet is identified, it is possible that the image may not contain a complete packet. Although we limit the maximum size of the data packet to fit within a single image frame, this can still occur if the packet appears too close to the end of the image frame. In such cases, due to the time gap between successive scanning operations, the portion of the data signal not captured by this image frame will not be fully recorded in the next, resulting in data loss, as shown in Figure 8(a).

To resolve this issue, we have the wearable token repeatedly send the data packet in a loop. A typical case is illustrated in Figure 8(b). Although part of the signal following the preamble is missing, the signal is cyclic, allowing the missing parts to be recovered by referencing the part prior to the preamble.

4.2 Scanner-to-Wearable Channel

Existing research has shown that fingerprint scanners can actively send on-body signals to the contacted human body [23].

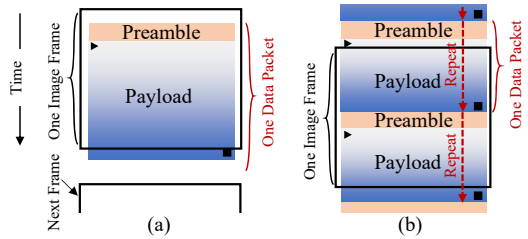


Figure 8: **Unsynchronized Data Packet and Image Frame.** (a) Data packet can appear at any position within the image. The part not captured in one image frame will also be missed in the next. (b) Looped data packets ensure a complete packet is contained within a single image frame.

Building on this, OneTouch enables bidirectional communication between two devices, which provides enhanced interactivity and security.

The feasibility of the scanner-to-wearable channel lies in the *driver voltage* mechanism of the scanner. As introduced in Section 3.2, the scanner measures capacitance by applying a drive voltage to the electrode. In practice, the scanner can further enhance the measurement by actively applying a drive voltage to the body [27]. Specifically, in addition to discharging the on-body voltage, the bezel in contact with the finger also can apply a driver voltage to the body when the scanner samples each sensing electrode. As shown in Figure 9, during fingerprint imaging, a high-frequency on-body signal is detected[2].

To transmit data using the drive voltage, the scanner employs an on-off modulation scheme, similar to the wearable-to-scanner channel. The presence or absence of the high-frequency drive voltage signal represents bit "1" and bit "0", as shown in Figure 9. To capture the drive voltage, the wearable token connects an electrode to an analog-to-digital converter (ADC), as illustrated in Figure 2.

A key improvement over the previous study [23] (25 bps) is the substantial increase in the data rate of the scanner-to-wearable channel (several kbps). The presence of the drive voltage depends on whether the scanner is actively imaging. For data transmission, the scanner switches between imaging and idle states, with the switching frequency determining the transmission rate. Unlike prior work, we directly utilize the low-level command interface of the scanner's controller to eliminate unnecessary processing delays. For example, we send the `CAPTURE_IMAGE` command to the FPC1020AM controller to initiate scanning, and the `ACTIVATE_IDLE_MODE` command to cancel the operation, achieving submillisecond-level switching intervals.

4.3 Reliable Data Delivery

Errors are inevitable in both directions, so we use error correction and acknowledgment (ACK) mechanisms to ensure reliable message delivery.

[2]The on-body signal generated by the wearable token will be superimposed with the drive voltage generated by the scanner. For clarity, Figure 9 records V_{Bezel} when the token is muted.

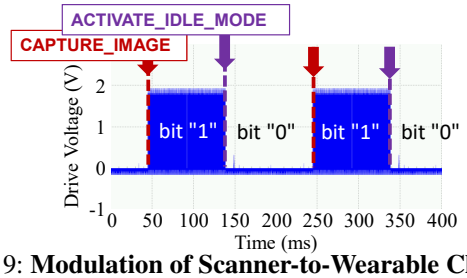


Figure 9: **Modulation of Scanner-to-Wearable Channel.**

The payload of the data packets consists of three fields: the data, the cyclic redundancy check (CRC), and the error correction code (ECC). The CRC is used to verify the integrity of the received data, while the ECC helps correct erroneous bits. Specifically, we apply Reed-Solomon (RS) ECC codes to both channels.

Despite these measures, it is still possible for the number of erroneous bits to exceed the ECC's correction capability, resulting in failure. To address this, we introduce an ACK-based retransmission mechanism. Figures 10 (1, 2) and (3, 4) illustrate the general message transmission flow between the scanner and the wearable. After receiving a data message, the receiver immediately sends an ACK to confirm receipt. The sender, after transmitting a message, waits for the ACK. If no ACK is received within a specified time, the message is retransmitted. Unlike typical protocols, the wearable token repeats the same packet multiple times (by default, 5 attempts)—whether it is data or an ACK. This design is specifically tailored to accommodate the scanner's unique receiving mechanism (Section 4.1.2).

5 OneTouch OTP Authentication

OneTouch utilizes touch-based channels to implement a 2FA scheme, verifying user identity through a combination of fingerprint and challenge-response OTP authentication.

5.1 Setup Stage

Before using OneTouch for 2FA, the wearable token must first be associated with the user's identity information in the authentication device. This step is required for every token-scanner pair. For generality, we describe the process of binding the token right after fingerprint enrollment in Figure 11.

The user first enrolls their fingerprint through standard procedures in step ❶. Afterward, the user places their finger on the scanner to complete steps ❷ to ❺. In step ❷, the scanner advertises its `Scanner ID` and its data reception preferences (*e.g.*, carrier wave frequency, frame length) to the token. The token then transmits its `Token ID` and Diffie-Hellman (DH) public key to the scanner in step ❸. After step ❹, both the scanner and the token can derive a `Shared Key`. In step ❺, the token confirms the reception of the scanner's public key. Following this, the scanner records the [`Fingerprint Template`, `Token ID`, `Shared Key`] as the user's identity information,

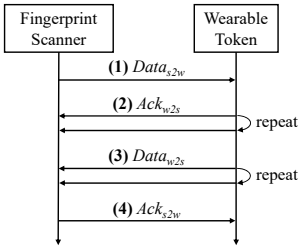


Figure 10: **Reliable Data Delivery Protocol.**

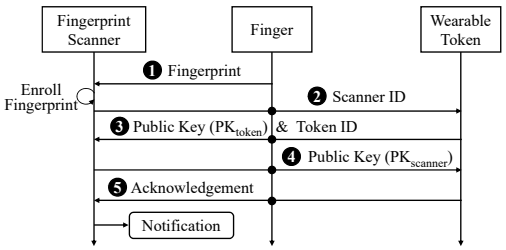


Figure 11: **OTP Setup Protocol.**

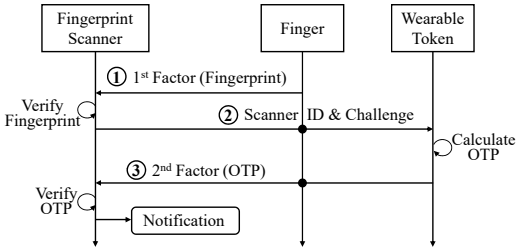


Figure 12: **OTP Authentication Protocol.**

while the token stores [`Scanner ID`, `Shared Key`] for future authentication. Both the scanner and the token set a validity period for the identity records to contain the risks associated with key or device compromise. Finally, the scanner notifies the user that the setup has been completed.

5.2 Authentication Stage

The authentication stage follows a canonical challenge-response protocol, similar to CRAM [5]. As outlined in Figure 12, the process begins with the scanner conducting a biometric fingerprint verification in step ①. Upon successful identification, and confirmation that the fingerprint is associated with a valid `Shared Key`, the scanner transmits its `Scanner ID` along with a challenge in step ②. The challenge is a non-repetitive random value. After receiving the challenge, the token generates a response by calculating the secure hash of the received challenge using the `Shared Key` associated with the `Scanner ID`. In step ③, the token truncates the hash result and uses the last 3 bytes as the OTP[3] , which is then sent back to the scanner. Upon receiving the OTP, the scanner verifies the challenge using the same hash method. Since a user may have registered multiple tokens, the scanner iterates over all valid tokens' associated `Shared Key`s to compute the hash. If any of the hashes match OTP, this indicates successful validation, and the user is notified.

6 Security Analysis

Since the security properties of fingerprint authentication are well-established, the primary focus of this section is the security of the touch-based channels and the OTP protocol.

6.1 Security of Touch-based Channels

The touch-based channel used by OneTouch is a unique messaging method that utilizes voltage signals conducted through the human body to transmit information. Unlike manual OTP input methods, OneTouch is immune to human-input-induced attacks such as shoulder-surfing [50], keystroke inference [53], smudge [9], and thermal attacks [34]. In terms of physical properties, the touch-based channel falls between wireless and wired connections, sharing similarities with Near Field Communication (NFC), which is induction-based and widely used in payment systems. They share similar security properties and potential attack surfaces:

- **In-Contact Injection**: The signal-receiving hardware of both the scanner and wearable can only detect voltage or capacitance changes at close proximity. This feature makes it difficult for an adversary to inject malicious inputs or alter message data through common wireless signals. Instead, the adversary must directly contact the sensing parts of the devices to perform the attack.
- **Wireless Eavesdropping**: When high-frequency voltage signals are applied to the human body, the body radiates corresponding electromagnetic (EM) signals, a phenomenon known as the human antenna effect [37]. An adversary can capture these EM signals from a distance (typically less than 10 meters) to extract the transmitted data.

6.1.1 In-Contact Relay Attack

In NFC-based authentication systems, relay attacks pose a threat, and OneTouch faces similar risks. In the OneTouch threat model, the adversary can make close contact with the authentication devices (*e.g.*, touching the scanner to spoof fingerprint authentication). If the adversary also has the opportunity to make contact with the wearable token, a relay attack could be launched.

Specifically, a sophisticated adversary could relay messages from the user's wearable token to the scanner, bypassing the need for direct contact between the token and the scanner. A possible scenario is shown in Figure 13, where the adversary first spoofs the fingerprint authentication (step ❶), prompting the scanner to transmit a challenge. The adversary then forwards (and amplifies) the data signals using relays (step ❷). Relay B can be strategically attached to a conductive object commonly touched by the user in daily life, such as a metal handrail on a subway. This tricks the wearable token into responding with a valid OTP. The adversary then captures the OTP and relays it back to the scanner, successfully passing the OTP authentication (step ❸).

Executing such a relay attack requires advanced skills and a certain degree of luck, as the adversary must simultaneously make contact with both the scanner and the wearable token. Furthermore, this attack can be mitigated by introducing a

[3] A single image frame has a capacity of around 30 bytes. We use a 3-byte OTP to ensure reliable transmission and offer flexibility in interaction. For instance, if on-body transmission fails, the token can display (if available) the OTP for manual input.

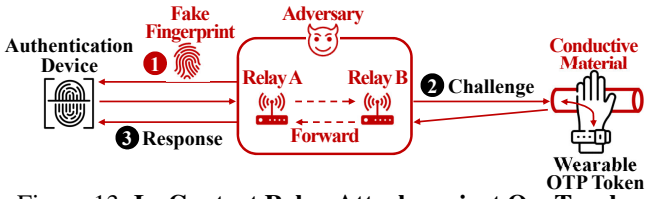


Figure 13: **In-Contact Relay Attack against OneTouch.**

distance/time bounding protocol [41], which limits the physical separation between the scanner and the token, ensuring they are within the length of a palm.

6.2 Security of OTP Protocol

The touch-based channels offer various options for the token authentication protocol. Different options may lead to trade-offs between security and usability to varying degrees. The security of OneTouch authentication is ensured by its underlying challenge-response protocol.

For example, we consider some common attacks. According to OneTouch's threat model, while the adversary can eavesdrop on the message exchange, they cannot infer the shared secret because the information is hashed, ensuring the confidentiality of the secret. Although the adversary can inject arbitrary messages into the authentication device by interacting with the scanner, they cannot directly forge a valid response to pass authentication because they do not have the correct shared key required for the OTP calculation. Furthermore, the adversary cannot replay previously successful challenge-response messages, as each challenge contains a unique random value. At the same time, OneTouch also inherits some limitations from the protocols it employs, which we discuss below.

6.2.1 Man-in-the-Middle Attack

Since the OTP setup stage uses only Diffie-Hellman for key exchange, the scanner and token cannot be certain that they are communicating with the intended device (rather than an adversary) when generating the shared secret. This creates an opportunity for a patient and sophisticated adversary to launch a man-in-the-middle (MITM) attack, for example, using a setup similar to the relay attack (Section 6.1.1). To mitigate this risk, certificates could be introduced for the authentication devices to prove their identities. However, this would increase interaction time, and managing device certificates would present additional challenges.

6.2.2 Brute Force Attack

OneTouch intentionally limits the response length to 3 bytes. This makes brute force attacks feasible—simply, the adversary could use the same response for all challenges. In practical implementations, this attack can be mitigated by introducing delays between each failed attempt, making repeated guesses impractical. Additionally, increasing the length of the OTP can exponentially expand the search space for brute force attacks, which, if manual input is not a design objective (footnote 3), is an effective method to thwart such attacks.

6.3 Lost and Compromised Devices

If the scanner's information is compromised, an adversary could forge a fingerprint and use the same `Shared Key` in their own token to spoof that specific scanner. However, they are not able to spoof other scanners, as different scanner-token pairs have different shared secrets based on the DH exchange.

If the token's information is compromised, or if the adversary obtains the token, they could forge a fingerprint and use the token to spoof all registered scanners. This is a common limitation of token-based 2FA. OneTouch contains this risk by setting an expiration period for the identity information.

Additionally, previous research has indicated that RF transmitters can be distinguished by the unique hardware characteristics embedded in their transmitted RF signals, such as carrier frequency offset and phase noise due to oscillator imperfections [40, 54]. Similarly, when a signal is relayed to the token through two relay devices and a conductive object across different spaces, the sensed on-body voltage series would encapsulate information about the unusual propagation channel. This physical information could probably be utilized to authenticate the scanner before the response is transmitted.

7 Implementation

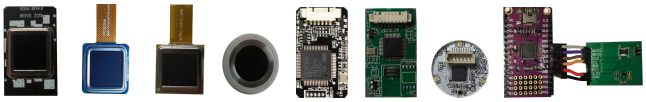
The implementation of OneTouch consists of the authentication device and the wearable token (Figure 2).

Authentication Device. We implement five different authentication devices (D1 – D5), as detailed in Table 1 and Figure 14. Commercial scanners typically output fingerprint images directly via the Serial Peripheral Interface (SPI), enabling direct connection to, for example, an SoC chip. For peripheral scanners, a host board with a microprocessor is commonly used to receive data from the SPI and provide other accessible I/O interfaces, such as serial port and USB. Some also offer basic fingerprint verification functionality. Table 1 lists the host boards for these devices, with some scanners being compatible with specific host boards.

A scanner and host board together form a basic authentication device. However, host boards of commercial products (H1 - H3) do not offer development interfaces. As a workaround, we route the scanner's data from the host board to a PC, where the PC handles the implementation of the OTP protocol and the modulation and demodulation of the touch-based channels. A limitation of this setup is the slow transfer speed of image data from the host board to the PC (via the serial port), resulting in large delays. Table 1 shows the time required to sample all sensing electrodes (Imaging Latency) and the total latency to the PC (Total Latency). To better assess usability (Section 8.3), we develop a customized authentication device (D5) to reduce the latency. Its setup involves connecting the scanner's SPI to our host board (H4, based on STM32

Table 1: **Authentication Devices**

Authentication Device ID	Scanner Model	Host ID	Image Size (px)	Imaging Latency (ms)	Total Latency (ms)
D1	FPC1020AP	H1	160*160	176	600
D2	FPC1020AM	H2	160*160	47	330
D3	FPC1021AM	H2	160*160	47	330
D4	Unknown	H3	160*160	34	400
D5	FPC1020AM	H4	160*160	150	157



(a) Fingerprint Scanners (b) Host Boards

Figure 14: **Fingerprint Scanners and Host Boards of the Authentication Devices.**

microcomputer) through a custom-designed printed circuit board (PCB). The host board is programmed to mimic the behavior of commercial products, but it is configured with a high-baud-rate serial port to upload image data to the PC.

Wearable Token. We use a laptop to build the token prototype. On this platform, we implement the OTP protocol, as well as the modulation and demodulation of touch-based channels using Python. The laptop is connected to two electrodes placed beneath a soft wristband, with the electrodes in contact with the skin. The laptop collects voltage signals from one electrode via a USB signal acquisition module (ADC). The other electrode is connected to a signal generator through a custom-designed switch circuit. The signal generator produces a carrier signal, and the switch circuit is controlled by the laptop via a serial port to achieve on-off modulation.

8 Evaluation

In this section, we evaluate the effectiveness of touch-based channels (Section 8.1 and Section 8.2) and the overall usability of OneTouch system (Section 8.3). We use the prototype devices introduced in Section 7 for testing. The evaluation involves a total of 30 participants. All of them take part in the user study, while 6 of them participate in the performance evaluation of the touch-based channels. Detailed participant information will be provided in Section 8.3.

8.1 Wearable-to-Scanner Channel Evaluation

As discussed in Section 3.2, the imaging mechanism of the capacitive fingerprint scanner makes it sensitive to on-body voltage signals (V_{Sig}) in a way that differs from typical signal acquisition scenarios. In Section 4.1.1, we propose using the presence of interfered pixels to represent bits. Therefore, in this subsection, we first examine the relationship between pixel variance—our key metric for interfered pixels—and the voltage signal to characterize the basic properties of this channel. Then, we evaluate the performance of on-off modulation based on pixel variance by measuring the error rates in actual data transmission.

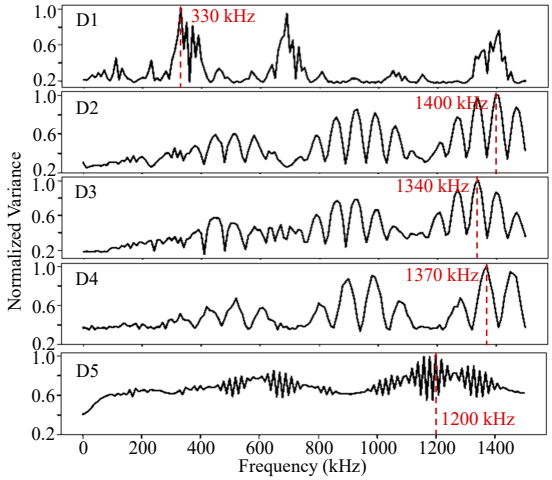


Figure 15: **Impact of Carrier Frequency.**

8.1.1 Basic Channel Properties

Our method involves applying a continuous carrier signal to the participant's body using the wearable token. The scanner then captures the image, and we compute the variance of the unwrapped pixels. The intensity of this variance reflects the strength of the "effective signal" capable of carrying information. A larger variance, compared to the baseline (with the carrier muted), indicates a stronger effective signal, implying a better signal-to-noise ratio and fewer transmission errors.

The pixel variance is calculated as the variance of pixel values across the entire image. We measure pixel variance for different carrier signal attributes—frequency, intensity, and waveform. When modifying one attribute, the others are kept constant. For each finger and scanner combination, we scan fingerprint images with varying values of one attribute, which we refer to as a *test*. The participant conducts three tests on each scanner using three different fingers. To minimize interference from background noise, such as fingerprint patterns, the finger position is held constant during each test. During data processing, the pixel variance for each image is normalized based on the maximum variance observed within its respective test. The average pixel variance from the three tests of different fingers, is displayed in the following figures.

Carrier Frequency. In this test, the carrier wave is a square wave with a 2 V amplitude. Its frequency is varied from 0 Hz to 1.5 MHz in steps of 10 kHz. As illustrated in Figure 15, devices D1–D4 exhibit the highest peaks at frequencies of 330 kHz, 1400 kHz, 1340 kHz, 1370 kHz, and 1200 kHz, respectively. We use these values as the optimal carrier frequencies for these scanners and apply them in subsequent experiments.

Since Device D4 uses a different sensor compared to the others, its distinct frequency response is expected. However, there are also significant differences between the reference responses of D2 and D5, as well as between D1 and D2. While D2 and D5 use the same scanner, D1 and D2 actually use the same fingerprint sensor, with the only difference being the

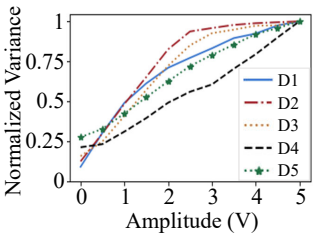


Figure 16: **Impact of Carrier Amplitude.**

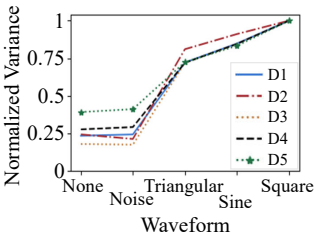


Figure 17: **Impact of Carrier Waveform.**

packaging. This suggests that the host board has a dominant impact on the frequency attribute of the channel.

The observed behavior can be attributed to how the scanner delivers image data. In Section 3, we explain how the scanner's controller manages the sampling of the sensing electrodes. In practice, two factors cause the scanner's imaging sampling to operate in a dependent mode, rather than independently: 1. The scanner lacks an independent crystal oscillator and relies on the clock provided by the host board via the SPI interface to function. 2. The host board controls the pacing of data reception by continuously writing dummy SPI signals. Since the scanner does not maintain a deep pixel buffer, its sampling is likely driven by the pace of the host's read signal.

Carrier Amplitude. In this test, the carrier wave is a square wave. Its amplitude is varied from 0 V to 5 V in steps of 0.5 V. The frequency is set to its optimal value. The results shown in Figure 16 illustrate a positive correlation between pixel variance and the amplitude. For scanners D2 and D3, the variance reaches a plateau when the amplitude exceeds 3 V. Further increasing the amplitude continues to raise the variance for other scanners.

It is important to note that a high amplitude may negatively impact the user experience. When tested with a 5 V amplitude, participants occasionally reported a tingling sensation in their fingers, particularly when their skin was damp from perspiration. Therefore, the amplitude should be set to a level that provides sufficient communication performance while avoiding any tingling sensation. Based on our experience, an amplitude of 2 V is generally sufficient for most situations.

Carrier Waveform. In previous tests, we used square waves by default because their sharp rising and falling edges are more difficult for the scanner's discharge mechanism to suppress. In this part, we will assess the pixel variance using different waveforms such as sine wave, triangular wave, square wave, and white noise, each with an amplitude ranging from 0V to 2V. The frequencies of the waveforms, except for white noise, are set to the optimal frequency for each scanner.

In Figure 17, all the devices exhibit a similar trend, with the square wave resulting in the highest variance. Due to the steeper slope compared to the triangular wave, the sine wave also shows a higher variance. Furthermore, the white noise seems to have minimal impact on the captured image, indicating that the scanner's discharging mechanism can effectively eliminate the white noise.

Preamble	Data	CRC	ECC
10 bits	24 bits	8 bits	8n bits

Figure 18: **Packet Structure.**

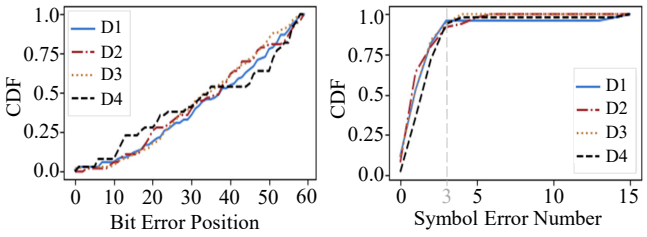


Figure 19: **Error CDF of Wearable-to-Scanner Channel.**

8.1.2 Data Transmission Performance

This subsection aims to verify the feasibility and reliability of using the wearable-to-scanner channel for message transmission. To achieve this, the token employs the on-off modulation scheme proposed in Section 4.1.1, with the carrier wave parameters configured as described in the previous subsection. The structure of the data packet is shown in the Figure 18, where the data field has a length of 24 bits. This choice is made to validate the most frequently transmitted message in our design: the 3-byte OPT.

Each packet uses CRC-8 for error detection and Reed-Solomon (RS) coding for error correction. The RS coding is based on the Galois field $GF(2^4)$, meaning each RS symbol consists of 4 bits, and the maximum encoding length is 15 symbols, corresponding to 60 bits. Within these 60 bits, the length of the ECC field is variable. The more ECC bits included, the greater the error correction capability, but the higher the protocol's overhead. Specifically, to correct n erroneous RS symbols, $8n$ ECC bits are required, as illustrated in the packet structure.

Bit Error Rate. We first measure the error statistics on the channel with one participant by transmitting 50 packet, each containing 60 random bits, excluding the preamble. In Figure 19, we depict the CDFs for both bit error positions and RS symbol error counts. Figure 19(a) shows a uniform distribution of bit errors, suggesting that errors are spread evenly across the bit positions. In Figure 19(b), we observe that in most cases, the number of error symbols remains below three. This indicates that setting $n = 3$ for the ECC bits is sufficient to handle the majority of errors.

Packet Error Rate with Error Correction. We transmit packets with n=1, 2, and 3, and measure the Packet Error Rate (PER) with the same participant. For each n, 50 frames were transmitted to each authentication device. We list the PER in Table 2. It shows that scanners D2 and D4 exhibit the lowest PER at n=3, whereas scanners D1 and D3 demonstrate the lowest PER at n=2. We use the value of n with the lowest PER as default configuration in the following experiments.

Table 2: **Packet Error Rate with Different ECC Length n.**

n	D1	D2	D3	D4
1	20%	14%	10%	16%
2	**6%**	8%	**0%**	8%
3	10%	**4%**	4%	**6%**

Table 3: **Packet Error Rate of Different Participants.**

Scanner		D1	D2	D3	D4
n		2	3	2	3
Participant	P0	6%	4%	0%	6%
	P1	4%	0%	6%	6%
	P2	8%	2%	4%	2%
	P3	10%	4%	4%	8%
	P4	6%	4%	2%	0%
	P5	4%	2%	6%	6%
Avg PER		6.3%	2.7%	3.7%	4.7%

Different Body Medium. Since on-body signals are conducted through the participant's body, and the way each participant interacts with the scanner can vary, these factors may potentially affect data transmission performance. In this experiment, we repeat the previous test with 6 participants, instructing them to ensure their fingers maintain proper contact with the scanner throughout the test. The results, summarized in Table 3, show that the PER values remain relatively consistent across all participants. This suggests that the physical characteristics of the human body are not strongly correlated with wearable-to-scanner communication performance. In Section 8.3.3, we will discuss how, in less controlled real-world scenarios, participant behaviors—such as incorrect finger placement—serve as the primary source of human-induced errors.

8.2 Scanner-to-Wearable Channel Evaluation

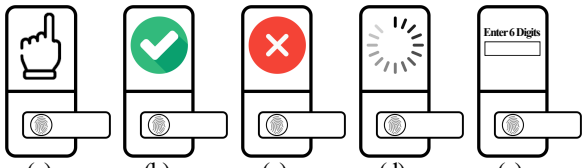
The properties of the scanner-to-wearable channel have been thoroughly evaluated in [23]. Building on their work, we further enhance the achievable data rate. We validate our design using device D5, which actively terminates the scanner's imaging process to reduce the time required for each bit. With the token's ADC operating at a 48 kHz sampling rate to capture the on-body voltage, the bit duration is reduced to 150 μs, resulting in a raw data rate of approximately 6.7 kbps, which is fully sufficient for transmitting OneTouch messages. By increasing ADC's sampling rate, the bit duration can be further reduced. As commercial host boards do not provide an interface to terminate the imaging process, the need to wait for the completion of the entire frame's sampling. As a result, their achievable data rate is limited to just a few bps.

8.3 User Study

This subsection evaluates the usability of OneTouch by analyzing user interactions and their feedback.

8.3.1 Methodology

Our study strictly follows ethical guidelines (see Section I).



(a) (b) (c) (d) (e)

Figure 20: **GUI of Virtual Lock.** (a) Detecting Finger. (b) Authentication Succeeded. (c) Authentication Failed. (d) Transmitting Challenge-Response. (e) Entering 6-Digit OTP.

Study Design. The goal of the experiment is to understand user behavior and feedback when using the authentication device. To achieve this, we develop an application layer for the authentication device to emulate a fingerprint-based lock. This virtual lock has a simple GUI, as shown in Figure 20, and provides feedback on authentication success or failure through a screen and a speaker. In addition to OneTouch, we use a keypad-based OTP system as a baseline for comparison. For both systems, we assume that fingerprint authentication always succeeds, focusing on the OTP authentication factor.

Captured Data. In this study, we collected the following data: (1) Logs from the authentication systems, including events and timestamps, where we can record authentication duration and failed authentication attempts for efficiency and effectiveness evaluation. (2) Participants' demographic information and questionnaire feedback with the System Usability Scale (SUS) [12] for satisfaction assessment. (3) Images captured by the scanner for further analysis.

Apparatus. To use the OneTouch system, participants are required to wear the OneTouch wearable token (Section 7). Once the finger is detected, the device initiates the challenge-response process (steps ② and ③ in Figure 12) five times over the touch-based channels. Participants are instructed to keep their finger pressed throughout the authentication process. If none of the five challenges receive a correct response, the lock GUI displays a failure icon and plays an alert sound. The participant must then press their finger again to attempt unlocking. Upon successful authentication, the lock signals success with a green light and a success prompt sound.

To use the baseline system, a separate GUI is employed to emulate the OTP token display, which shows a random 6-digit OTP after the participant presses their finger on the scanner. The participant then enters the OTP using a keypad. If the entered OTP is incorrect, the OTP remains unchanged, and the participant must re-enter it until authentication is successful. Feedback on whether the unlocking was successful is provided in the same manner as in OneTouch.

During the participants' use of both authentication devices, we logged the timestamps of finger detection (T_d), authentication failure (T_f) and success (T_s) from both authentication devices, and timestamps of challenge reception (T_c) from the OneTouch token additionally. The images captured during failed OneTouch authentication attempts are also recorded for error case analysis.

Study Procedure. After reading and signing a consent

Table 4: **Demographics.**

Gender		Age			Education Level			
M	F	18-25	26-35	35+	Dr	Ms	Ba	Others
15	15	17	5	8	3	13	9	5

form which outlining the study's background and the ethical considerations, *e.g.*, their rights and the data protection policy. Then, each participant completes four tasks in sequence:

(1) Fill out an entry survey to collect demographic information, including gender, age and educational level.

(2) Perform 10 unlocking attempts using baseline system.

(3) Perform 50 unlocking attempts using OneTouch.

(4) Complete an exit survey to evaluate their satisfaction with the two systems using SUS.

Participant Recruitment. Participants were randomly recruited around our campus, including students and passersby, and must be at least 18 years old. No other special requirements apply. Participants were provided with a detailed informed consent form outlining the study's background and purpose. They were clearly informed of their right to withdraw from the study at any time and for any reason without penalty. Each participant spent approximately half an hour completing the experiments in user study and received a $10 gift card. The participants who additionally took part in the performance evaluation of the touch-based channels received an additional $10 gift card.

Limitations. We conducted a study involving 30 participants. Although we obtained many samples regarding time cost and authentication errors, only 30 samples were collected for the satisfaction survey, with only 8 samples from middle-aged and elderly participants. This limits our quantitative analysis of satisfaction. While this study provided preliminary satisfaction analysis, a broader study would yield more solid conclusions.

Results. In the following, we will analyze the collected data to understand the efficiency, effectiveness and user satisfaction of OneTouch.

8.3.2 Efficiency of Using OneTouch

Based on the logged timestamps, we first profile the time costs of each unlocking attempt for both authentication systems. An *unlocking attempt* is defined as the process from the initial detection of the finger to the successful authentication. For instance, if the participant re-presses their finger after a failure, we will get the following timestamps: $\{T_d,\ T_{c_1},\ T_{f_1},...,\ T_{c_5},\ T_{f_5},\ T'_d,\ T'_{c_1},\ T_s\}$. The unlocking attempt includes events and operations from T_d to T_s, and its time cost can be calculated as $T_s - T_d$.

We analyze the log data from all 30 participants. The mean time cost of unlocking attempts for the baseline system is 4.31 s (std=1.86 s), while for OneTouch, it is 1.02 s (std=1.26 s), which is less than a quarter of the former. We also find that the time cost of the baseline system is primarily spent on viewing and entering the OTP digits, whereas the time cost of OneTouch is mainly spent on transmitting and demodulating OTP messages (with each challenge-response handshake taking 550 ms).

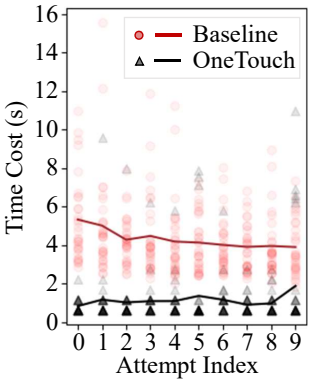
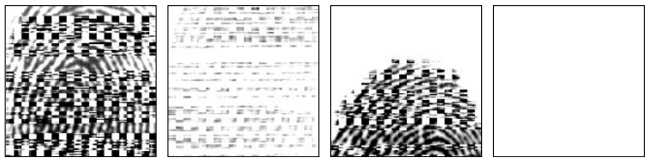


Figure 21: **Time Cost of Unlocking Attempts.** Values are shown as scatter points, with the average as a line.

Num of Challenge -Response	Unlocking Attempts %
1	77.3%
2	16.1%
3	1.9%
4	1.2%
5	0.9%
Re-press	2.6%
Total	100%

Figure 22: **Statistics of Unlocking Attempts with OneTouch.**



(a) (b) (c) (d)

Figure 23: **Human-Induced Errors on the Wearable-to-Scanner Channel.** (a) Good Sample. (b) Light Pressure. (c) Incomplete Touching. (d) Early Lifting.

Figure 21 plots the time costs of the first 10 unlocking attempts from all 30 participants using semi-transparent scatter circles and triangles. The overall color trend shows that using the keypad generally takes more time than using OneTouch. When the average time cost for all 30 participants is represented by a line, we observe that as participants use the keypad to enter OTPs, the time cost decreases with the increasing number of attempts. By comparing the time costs of the first five and subsequent five attempts, we find proficiency (familiarity with the keypad layout) is a significant effect on the baseline's time cost ($T = 3.19,\ p < 0.01$). In contrast, the time cost of OneTouch shows no significant difference, as it involves only a single action—pressing the finger—which is independent of user proficiency.

8.3.3 Human-Induced Errors

As shown in Figure 22, 22.4% of unlocking attempts do not succeed during the first challenge-response handshake when using OneTouch. By analyzing the collected images of these error cases, we found that the majority were caused by the randomness of the channel. However, approximately 20% of the cases were clearly attributed to improper fingerprint input behaviors, including:

Too Light Pressure Applied. As pixel values increase with the distance between the skin and the sensing plates,

a lighter pressure results in a whiter image, as depicted in Figure 23(b). In this case an excessive distance causes the outliers to appear white, thereby reducing the signal strength. Conversely, when pressure is increased, the image becomes darker, and the region of outliers becomes more pronounced, as illustrated in Figures 23(a).

Incomplete Touching. When no skin is in contact with the sensing plate (*i.e.*, at an infinite distance), the detected pixel remains consistently white (the upper part of Figure 23(c)). This implies that data is partially lost when the finger does not completely cover the sensing surface. If the uncovered area is minimal, the number of erroneous bits is sufficiently low for error correction mechanisms to be effective. However, the overall packet error rate is still elevated due to the presence of the uncovered areas.

Finger Leaving the Scanner. Sometimes, the participants incorrectly lifting the finger when the icon shown on the virtual lock changes to the transmitting state (Figure 20(d)). This operational mistake disconnects the touch-based channels, therefore, the scanner captures an empty image as shown in Figure 23(d).

Comparing to the experiment evaluated the impact of different body medium with 6 participants, this study involves a more diverse range of participants' physical characteristics. By comparing the error counts of young (18-35) and older (35-60) participants, we find age is a significant effect on the number of errors occurred with each participant ($\chi^2(1) = 35.4, p < 0.01$). Because the elder participants are more likely to cause improper presses. After filtering the above human-induced errors, we observe the similar error rate across 30 participants, which is consistent to the conclusion obtained in Section 8.1.2, *i.e.*, human body's physical characteristics have little effect on the channel.

8.3.4 Effectiveness of OneTouch

Errors caused by channel randomness are unavoidable and can only be mitigated by using more effective transmission scheme. Additionally, these random errors are unlikely to occur consecutively, which is why 93.4% of authentication attempts are successful within two challenge-response handshakes. As a result, participants do not need to take any special actions. However, errors caused by suboptimal input methods, such as improper pressure or incomplete impressions, are much harder to correct by simply repeating the transmissions. After five failed challenge-response attempts, an "Authentication Failed" notification is triggered in the GUI, prompting the participant to re-press their finger. In all of the logged attempts we collected during testing, participants were able to successfully authenticate by pressing their finger again.

8.3.5 User Satisfaction

In the Exit Survey, we collected user feedback on OneTouch using the System Usability Scale (SUS) [12]. SUS is commonly used to gather subjective assessments of satisfaction and is frequently used for comparison between different systems. An SUS score, ranging from 0 to 100, is calculated based on the participants' answers to the survey questions. A higher score means a higher satisfaction with the system.

Table 5: **User Feedback in SUS Scores.**

Age Group		18 - 25	26 - 35	36 - 45	46 - 60
SUS Score	Baseline (S_b)	75.29	81.5	76.25	65.63
	OneTouch (S_o)	80.59	84.5	85	81.25
S_b - S_k		5.3	3.0	8.75	15.62

For comparison, we also gathered user feedback on the baseline system. In the collected survey responses, we excluded the results from two participants who gave the same answer to all questions. The average SUS score for the baseline system is 75.09 (grade C [10]), while the average SUS score for OneTouch is 81.7 (grade B). This suggests that OneTouch brings better user satisfaction.

Compared to the baseline system, OneTouch, as a relatively new authentication method, received slightly lower ratings for *learnability*. However, in terms of *ease of use*, OneTouch was rated significantly higher than the baseline system. Additionally, as shown in Table 5, we observe that OneTouch is more user-friendly for middle-aged and elderly individuals than keypad. This is because older participants are less proficient with keypad input. To better understand the significance of the observed differences, Cohen's d was calculated as a measure of effect size. The comparison of SUS score difference (*i.e.*, $S_b - S_k$) between young (18-35) and older (36-60) yields a Cohen's d value of 0.64, indicating a medium effect size.

9 Discussion

In this section, we discuss the potential deployment issues of OneTouch and explore the possibility of applying its key design concepts to other applications.

OTP with Single Direction Channel: Some fingerprint scanners might not rely on a drive signal to capture fingerprint images, making it impossible to establish a scanner-to-wearable channel. In such cases, OneTouch can adopt a time-based OTP scheme [36], where both the token and the authentication device maintain a clock. During the setup stage, key exchange and clock synchronization can be performed via a wired connection (*e.g.*, USB). For each authentication attempt, the token generates an OTP based on its clock and the shared key, and sends it to the authentication device through the wearable-to-scanner channel.

User not Willing to Use Wearable: For users who are unwilling to wear additional wearable devices, integrating OneTouch into a smartphone could be a viable solution. In this case, users would only need to hold the smartphone during fingerprint authentication to complete the authentication process. However, this approach introduces a usability penalty. An alternative approach is to not directly exclude users who opt not to use wearables in authentication devices, but instead

offer other secondary factors, such as PIN entry. These devices could also help educate users by periodically reminding them after authentication, demonstrating the practical benefits of using a 2FA wearable, which can provide higher security without compromising usability.

Support for None-Capacitive Fingerprint Scanners: Currently, OneTouch focuses the implementation for capacitive fingerprint sensors. However, optical [22] and ultrasonic [51] fingerprint sensors also hold a market share for mobile devices. We believe the concept of OneTouch can be adapted to these sensors using different mechanisms. For instance, since ultrasonic waves can propagate through the body via bone conduction, it may be possible for the wearable device to use an ultrasonic emitter to interact with ultrasonic fingerprint sensors. Additionally, as light can propagate through body tissues [14], an LED could be employed by the wearable to transmit information to optical fingerprint sensors.

Adoption of OneTouch. As introduced in Section 3, the imaging mechanism used by fingerprint scanners, which rely on minimal ADC for sequential scanning to achieve 2D imaging, is a cost-effective practice. We believe this approach is widely adopted in commercial fingerprint scanners, which is also why we were able to easily implement multiple prototypes in Section 7. However, the adoption of OneTouch depends not only on users' willingness but also on software support from fingerprint scanner manufacturers. This challenge is more commercial than technical. Given the growing awareness of security risks, many users would likely be open to adopting such a method to enhance the security of their authentication devices. Additionally, fingerprint scanner manufacturers have an incentive to support new features, as it increases the value of their products without incurring significant additional costs. Companies most likely to be interested in OneTouch are those offering both authentication devices and wearables, such as Apple and Huawei. To promote the adoption of OneTouch, we will share our design and implementation, which could potentially lead to a technical alliance with companies interested in utilizing fingerprint sensors as an additional security I/O interface.

10 Related Work

10.1 Two Factor Authentication

For research on 2FA methods, one branch of work involves using a personal device as a factor to authenticate identity. To avoid introducing additional user actions, these studies have leveraged wireless communication technologies to transmit identity messages, such as Bluetooth [16], Wi-Fi [46] and sounds [21, 29]. The personal device can also fingerprint the surrounding environment to detect co-presence with the authentication device based on its physical characteristics (*e.g.*, ambient sound [26], location [33], radio frequency [18], temperature and humidity [47]). In addition to the surrounding environment, an alternative method is to fingerprint user's behavioral characteristics during the authentication process. For instance, the authentication device can sense the timing of keystroke dynamics when user entering a password [30] or the friction sounds emitted while interacting with a pattern lock [55]. Additionally, a wearable device can assist the authentication device by detecting the typing gesture through its integrated motion sensors [32, 48].

The aforementioned methods are specifically designed for Web and mobile applications, where can easily meet the requirements for a wide range of I/O interfaces and sensing capabilities. However, certain fingerprint authentication devices, such as fingerprint locks, not only lack wireless interfaces for communication with secondary devices but are also devoid of sensors to detect environmental conditions and the user's behavior. OneTouch is designed for fingerprint authentication based on the existing imaging principle of fingerprint sensors, which reduces the difficulty and cost of deployment.

10.2 Secure Fingerprint Authentication

For defending against spoofing attacks with forged fingerprint, liveness detection techniques have been widely discussed. Existing studies try to distinguish forged fingers from real ones through side information, *e.g.*, perspiration [49], time series of images [38,39], electrical properties [45], haptic response [42]. Some of these approaches require the authentication device to have specialized hardware, while some only need software deployment. However, liveness detection techniques are in a constant race against adaptive adversaries employing more advanced fabrication technologies [31]. In contrast, OneTouch relies on proven secure and effective OTP protocol to defend against spoofing attacks, making it a more reliable solution.

10.3 Capacitance based Authentication

Some existing work also utilizing the sensing capability of capacitive devices to propose authentication schemes. 3D-Auth [35] enables a 2FA scheme with a 3D-printed conductive token. When user interacts with the token, a customized pattern would be sensed by a touch screen. The touch screen is also used to sense the hand contours [44], ears [24] and electric signals emitted by a wristband [25] for user identification. And the work, we referred to establish the scanner-to-token channel [23], uses the electromagnetic signals generated by fingerprint sensors and touchpads to authenticating electronic locks. Inspired by these works, OneTouch also utilizing the capacitance characteristics of capacitive fingerprint sensor to achieve 2FA for fingerprint authentication.

11 Conclusion

In this paper, we propose OneTouch, an unobtrusive two-factor authentication scheme that enhances fingerprint authentication systems with a wearable OTP token. This token connects to the fingerprint scanner through the human body, utilizing on-body communication to enable a secure

challenge-response OTP protocol. OneTouch leverages the imaging mechanism already present in capacitive fingerprint scanners to detect the on-body signal, making it friendly for practical deployment. In terms of security, OneTouch requires direct physical contact, which effectively limits attack vectors relying on message eavesdropping and tampering.

Acknowledgments

We thank anonymous USENIX Security reviewers and Shepherd. Their valuable comments help us improve this paper. This work is supported by ShanghaiTech.

I Ethical Considerations

We have active Institutional Review Board (IRB) approval to collect data from adult participants for our research. All evaluations adhere to IRB regulations.

We collected participants' demographic information and their perceptions to OneTouch through a questionnaire. Besides, when participants used OneTouch images containing fingerprint information were captured and stored for offline processing and analysis. All data is anonymized, encrypted, and stored offline on a hard disk drive. The decryption key is accessible only to the authors.

II Open Science

We will make our code and hardware specifications publicly available[4]. This will include detailed guidelines on how to modulate and demodulate fingerprint images for the purpose of data transmission. Given the sensitive nature of the fingerprint data in our dataset, we have decided to offer a limited set of sample data for functionality and reproducibility assessment. This data will be sourced from the author's non-dominant finger to ensure privacy. Furthermore, to facilitate ease of use and understanding, we will supply thorough documentation and clear instructions alongside our open-sourced materials.

References

[1] Hacker fakes German minister's fingerprints using photos of her hands. https://www.theguardian.com/technology/2014/dec/30/hacker-fakes-german-ministers-fingerprints-using-photos-of-her-hands, 2014.

[2] UP: Man learns 'cloning fingerprints' online, 'hacks' 500 bank accounts. https://timesofindia.indiatimes.com/city/bareilly/man-26-learns-cloning-fingerprints-online-hacks-nearly-500-accounts-with-bank-mitrass-help/articleshow/81158623.cms, 2019.

[3] Over 27.8m records exposed in BioStar 2 data breach. https://www.trendmicro.com/vinfo/us/security/news/online-privacy/over-27-8m-records-exposed-in-biostar-2-data-breach, 2022.

[4] Hackers can unlock a smartphone with fingerprints on glass of water. https://www.hackread.com/hackers-unlock-smartphone-fingerprints-glass-of-water/, 2024.

[5] IMAP/POP authorize extension for simple challenge/response. https://www.rfc-editor.org/rfc/rfc2195.txt, 2025.

[6] Sony CXA3621GE Fingerprint Sensor. https://biometrics.mainguet.org/types/fingerprint/product/Sony/Sony_CXA3621GE_a6803076.pdf, 2025.

[7] Mingrui Ai, Kaiping Xue, Bo Luo, Lutong Chen, Nenghai Yu, Qibin Sun, and Feng Wu. Blacktooth: breaking through the defense of bluetooth in silence. In *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*, pages 55–68, 2022.

[8] Daniele Antonioli. Bluffs: Bluetooth forward and future secrecy attacks and defenses. In *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security*, pages 636–650, 2023.

[9] Adam J Aviv, Katherine Gibson, Evan Mossop, Matt Blaze, and Jonathan M Smith. Smudge attacks on smartphone touch screens. In *4th USENIX workshop on offensive technologies (WOOT 10)*, 2010.

[10] Aaron Bangor, Philip Kortum, and James Miller. Determining what individual sus scores mean: Adding an adjective rating scale. *Journal of usability studies*, 4(3):114–123, 2009.

[11] Christina Braz and Jean-Marc Robert. Security and usability: the case of the user authentication methods. In *Proceedings of the 18th Conference on l'Interaction Homme-Machine*, pages 199–203, 2006.

[12] John Brooke et al. Sus-a quick and dirty usability scale. *Usability evaluation in industry*, 189(194):4–7, 1996.

[13] Yu Chen, Yang Yu, and Lidong Zhai. Infinitygauntlet: Expose smartphone fingerprint authentication to brute-force attack. In *32nd USENIX Security Symposium (USENIX Security 23)*, pages 2027–2041, 2023.

[14] Wai-Fung Cheong, Scott A Prahl, and Ashley J Welch. A review of the optical properties of biological tissues. *IEEE journal of quantum electronics*, 26(12):2166–2185, 1990.

[4] https://doi.org/10.5281/zenodo.14699610

[15] Federal Financial Institutions Examination Council. Authentication in an internet banking environment. *Retrieved June*, 28:2006, 2005.

[16] Alexei Czeskis, Michael Dietz, Tadayoshi Kohno, Dan Wallach, and Dirk Balfanz. Strengthening user authentication through opportunistic cryptographic identity assertions. In *Proceedings of the 2012 ACM conference on Computer and communications security*, pages 404–414, 2012.

[17] Joshua J Engelsma, Sunpreet S Arora, Anil K Jain, and Nicholas G Paulter. Universal 3d wearable fingerprint targets: Advancing fingerprint reader evaluations. *IEEE Transactions on Information Forensics and Security*, 13(6):1564–1578, 2018.

[18] Nirnimesh Ghose, Kaustubh Gupta, Loukas Lazos, Ming Li, Ziqi Xu, and Jincheng Li. Zita: Zero-interaction two-factor authentication using contact traces and in-band proximity verification. *IEEE Transactions on Mobile Computing*, 2023.

[19] Maximilian Golla, Grant Ho, Marika Lohmus, Monica Pulluri, and Elissa M Redmiles. Driving 2FA adoption at scale: Optimizing Two-Factor Authentication notification design patterns. In *30th USENIX Security Symposium (USENIX Security 21)*, pages 109–126, 2021.

[20] Tobias Grosse-Puppendahl, Christian Holz, Gabe Cohn, Raphael Wimmer, Oskar Bechtold, Steve Hodges, Matthew S Reynolds, and Joshua R Smith. Finding common ground: A survey of capacitive sensing in human-computer interaction. In *Proceedings of the 2017 CHI conference on human factors in computing systems*, pages 3293–3315, 2017.

[21] Dianqi Han, Yimin Chen, Tao Li, Rui Zhang, Yaochao Zhang, and Terri Hedgpeth. Proximity-proof: Secure and usable mobile two-factor authentication. In *Proceedings of the 24th Annual International Conference on Mobile Computing and Networking*, pages 401–415, 2018.

[22] Manhyeop Han, CHOO Kyoseop, MoonBong Song, and CHO Jiho. Fingerprint sensor integrated type touch screen device, June 26 2018. US Patent 10,007,828.

[23] Mehrdad Hessar, Vikram Iyer, and Shyamnath Gollakota. Enabling on-body transmissions with commodity devices. In *Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing*, pages 1100–1111, 2016.

[24] Christian Holz, Senaka Buthpitiya, and Marius Knaust. Bodyprint: Biometric user identification on mobile devices using the capacitive touchscreen to scan body parts. In *Proceedings of the 33rd annual ACM conference on human factors in computing systems*, pages 3011–3014, 2015.

[25] Christian Holz and Marius Knaust. Biometric touch sensing: Seamlessly augmenting each touch with continuous authentication. In *Proceedings of the 28th Annual ACM Symposium on User Interface Software & Technology*, pages 303–312, 2015.

[26] Nikolaos Karapanos, Claudio Marforio, Claudio Soriente, and Srdjan Capkun. {Sound-Proof}: Usable {Two-Factor} authentication based on ambient sound. In *24th USENIX security symposium (USENIX security 15)*, pages 483–498, 2015.

[27] Alan Kramer. Enhanced fingerprint detection, January 28 2003. US Patent 6,512,381.

[28] Maoyuan Li, Yong Song, Xu Zhang, Yu Chen, and Chenqiong Tang. A review of implant intra-body communication. *Journal of Beijing Institute of Technology*, 31(1):1–29, 2022.

[29] Dan Liu, Qian Wang, Man Zhou, Peipei Jiang, Qi Li, Chao Shen, and Cong Wang. Soundid: Securing mobile two-factor authentication via acoustic signals. *IEEE Transactions on Dependable and Secure Computing*, 20(2):1687–1701, 2022.

[30] Ximing Liu, Yingjiu Li, and Robert H Deng. Typing-proof: Usable, secure and low-cost two-factor authentication based on keystroke timings. In *Proceedings of the 34th Annual Computer Security Applications Conference*, pages 53–65, 2018.

[31] Davide Maltoni, Dario Maio, Anil K Jain, Salil Prabhakar, et al. *Handbook of fingerprint recognition*, volume 2. Springer, 2009.

[32] Shrirang Mare, Reza Rawassizadeh, Ronald Peterson, and David Kotz. Saw: Wristband-based authentication for desktop computers. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, 2(3):1–29, 2018.

[33] Claudio Marforio, Nikolaos Karapanos, Claudio Soriente, Kari Kostiainen, and Srdjan Capkun. Smartphones as practical and secure location verification tokens for payments. In *NDSS*, volume 14, pages 23–26, 2014.

[34] Karola Marky, Shaun Macdonald, Yasmeen Abdrabou, and Mohamed Khamis. In the quest to protect users from {Side-Channel} attacks–a {User-Centred} design space to mitigate thermal attacks on public payment terminals. In *32nd usenix security symposium (usenix security 23)*, pages 5235–5252, 2023.

[35] Karola Marky, Martin Schmitz, Verena Zimmermann, Martin Herbers, Kai Kunze, and Max Mühlhäuser. 3d-auth: Two-factor authentication with personalized 3d-printed items. In *Proceedings of the 2020 chi conference on human factors in computing systems*, pages 1–12, 2020.

[36] David M'Raihi, Salah Machani, Mingliang Pei, and Johan Rydell. RFC 6238: TOTP: Time-based one-time password algorithm, 2011.

[37] Mayukh Nath, Shovan Maity, Shitij Avlani, Scott Weigand, and Shreyas Sen. Inter-body coupling in electro-quasistatic human body communication: Theory and analysis of security and interference properties. *Scientific Reports*, 11(1):4378, 2021.

[38] S.T.V. Parthasaradhi, R. Derakhshani, L.A. Hornak, and S.A.C. Schuckers. Time-series detection of perspiration as a liveness test in fingerprint devices. *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, 35(3):335–343, 2005.

[39] Richard Plesh, Keivan Bahmani, Ganghee Jang, David Yambay, Ken Brownlee, Timothy Swyka, Peter Johnson, Arun Ross, and Stephanie Schuckers. Fingerprint presentation attack detection utilizing time-series, color fingerprint captures. In *2019 International Conference on Biometrics (ICB)*, pages 1–8, 2019.

[40] Adam C. Polak and Dennis L. Goeckel. Wireless device identification based on rf oscillator imperfections. *IEEE Transactions on Information Forensics and Security*, 10(12):2492–2501, 2015.

[41] Kasper Bonne Rasmussen and Srdjan Capkun. Realization of {RF} distance bounding. In *19th USENIX Security Symposium (USENIX Security 10)*, 2010.

[42] Aditya Singh Rathore, Yijie Shen, Chenhan Xu, Jacob Snyderman, Jinsong Han, Fan Zhang, Zhengxiong Li, Feng Lin, Wenyao Xu, and Kui Ren. FakeGuard: Exploring haptic response to mitigate the vulnerability in commercial fingerprint anti-spoofing. In *NDSS*, 2022.

[43] Aditi Roy, Nasir Memon, and Arun Ross. Masterprint: Exploring the vulnerability of partial fingerprint-based authentication systems. *IEEE Transactions on Information Forensics and Security*, 12(9):2013–2025, 2017.

[44] Dominik Schmidt, Ming Ki Chong, and Hans Gellersen. Handsdown: hand-contour-based user identification for interactive surfaces. In *Proceedings of the 6th nordic conference on human-computer interaction: extending boundaries*, pages 432–441, 2010.

[45] Toshishige Shimamura, Hiroki Morimura, Nobuhiro Shimoyama, Tomomi Sakata, Satoshi Shigematsu, Katsuyuki Machida, and Mamoru Nakanishi. A fingerprint sensor with impedance sensing for fraud detection. In *2008 IEEE International Solid-State Circuits Conference - Digest of Technical Papers*, pages 170–604, 2008.

[46] Maliheh Shirvanian, Stanislaw Jarecki, Nitesh Saxena, and Naveen Nathan. Two-factor authentication resilient to server compromise using mix-bandwidth devices. In *NDSS*, 2014.

[47] Babins Shrestha, Nitesh Saxena, Hien Thi Thu Truong, and N Asokan. Drone to the rescue: Relay-resilient authentication using ambient multi-sensing. In *International Conference on Financial Cryptography and Data Security*, pages 349–364. Springer, 2014.

[48] Prakash Shrestha, Nitesh Saxena, Diksha Shukla, and Vir V Phoha. Press @$@$ to login: Strong wearable second factor authentication via short memorywise effortless typing gestures. In *2021 IEEE European Symposium on Security and Privacy (EuroS&P)*, pages 71–87. IEEE, 2021.

[49] Bozhao Tan and S. Schuckers. Liveness detection for fingerprint scanners based on the statistics of wavelet signal processing. In *2006 Conference on Computer Vision and Pattern Recognition Workshop (CVPRW'06)*, pages 26–26, 2006.

[50] Brian Jay Tang and Kang G Shin. Eye-Shield:Real-Time protection of mobile device screen information from shoulder surfing. In *32nd USENIX Security Symposium (USENIX Security 23)*, pages 5449–5466, 2023.

[51] Hao-Yen Tang, Yipeng Lu, Xiaoyue Jiang, Eldwin J Ng, Julius M Tsai, David A Horsley, and Bernhard E Boser. 3-d ultrasonic fingerprint sensor-on-a-chip. *IEEE Journal of Solid-State Circuits*, 51(11):2522–2533, 2016.

[52] Xinyi Xie, Kun Jiang, Rui Dai, Jun Lu, Lihui Wang, Qing Li, and Jun Yu. Access your tesla without your awareness: Compromising keyless entry system of model 3. In *NDSS*, 2023.

[53] Zhuolin Yang, Yuxin Chen, Zain Sarwar, Hadleigh Schwartz, Ben Y Zhao, and Haitao Zheng. Towards a general video-based keystroke inference attack. In *32nd USENIX Security Symposium (USENIX Security 23)*, pages 141–158, 2023.

[54] Junqing Zhang, Roger Woods, Magnus Sandell, Mikko Valkama, Alan Marshall, and Joseph Cavallaro. Radio frequency fingerprint identification for narrowband systems, modelling and classification. *IEEE Transactions on Information Forensics and Security*, 16:3974–3987, 2021.

[55] Man Zhou, Yuting Zhou, Shuao Su, Qian Wang, Qi Li, Shengshan Hu, Chunwu Yu, and Zhengxiong Li. Fingerpattern: Securing pattern lock via fingerprint-dependent friction sound. *IEEE Transactions on Mobile Computing*, 2023.