Body-Guided Communications: A Low-power, Highly-Confined Primitive to Track and Secure Every Touch

Viet Nguyen[1], Mohamed Ibrahim[1], Hoang Truong[2], Phuc Nguyen[2], Marco Gruteser[1], Richard Howard[1], Tam Vu[2]
[1]WINLAB, Rutgers University, [2]University of Colorado, Boulder

ABSTRACT

The growing number of devices we interact with require a convenient yet secure solution for user identification, authorization and authentication. Current approaches are cumbersome, susceptible to eavesdropping and relay attacks, or energy inefficient. In this paper, we propose a *body-guided communication mechanism* to secure every touch when users interact with a variety of devices and objects. The method is implemented in a hardware token worn on user's body, for example in the form of a wristband, which interacts with a receiver embedded inside the touched device through a body-guided channel established when the user touches the device. Experiments show low-power (μJ/bit) operation while achieving superior resilience to attacks, with the received signal at the intended receiver through the body channel being at least 20dB higher than that of an adversary in cm range.

CCS CONCEPTS

• **Security and privacy** → *Security in hardware*; • **Human-centered computing** → *Interaction design*;

KEYWORDS

Human Computer Interaction (HCI); Body-Guided Communications; Per-Touch Authentication

ACM Reference Format:
Viet Nguyen, Mohamed Ibrahim, Hoang Truong, Phuc Nguyen, Marco Gruteser, Richard Howard, Tam Vu. 2018. Body-Guided Communications: A Low-power, Highly-Confined Primitive to Track and Secure Every Touch. In *Proc. of The 24th Annual International Conference on Mobile Computing and Networking (MobiCom'18), October 29-November 2, 2018, New Delhi, India.* ACM, NY, NY. 16 pages. https://doi.org/10.1145/3241539.3241550

MobiCom '18, October 29-November 2, 2018, New Delhi, India

ACM ISBN 978-1-4503-5903-0/18/10…$15.00
https://doi.org/10.1145/3241539.3241550

1 INTRODUCTION

As users interact with an increasing number of devices, our interaction times with each device become shorter and the overhead of conventional user identification, authorization, and authentication solutions places an increasing burden on users. Ensuring authorization or accountability is particularly challenging in environments where devices are operated by groups of people. Consider an intensive care unit with multiple patient monitoring and life-support devices, that may be operated while several people including nurses, doctors and patient visitors are present. In some cases, the interaction with a device will only be a single touch before moving on to another device or task. How can we support accountability and auditing by tracking which users looked up information or changed a setting at any given time? If desired, how can we ensure that only authorized users operate these devices? Similarly, challenges arise in numerous other scenarios, from industrial or manufacturing settings to the home environment.

Current approaches broadly fall into the categories of passwords, biometrics, and tokens with short-range radio or near-field communications (NFC). Passwords are cumbersome to use for one-touch interactions and require a user interface for entry that is not present on all devices (consider Amazon's Dash button [1]). Biometrics can be convenient if directly integrated into the interaction (e.g., afi ngerprint sensor in the button) but require a sophisticated sensor that adds cost, particularly if every button on a device should have this functionality. Radio tokens, as in keyless entry systems for cars, are more convenient to use but their signals can be easily intercepted, requiring cryptographic protocols. These operations consume significant energy and the implementations of these protocols are surprisingly oftenfl awed [2, 3]. They are also difficult to secure against man-in-the-middle attacks [4].

Near-field communications can reduce but not eliminate the probability of adversarial interception. Achieving a higher level of security usually requires near-touch between the token and the receiver, such as holding a watch or phone against a payment terminal or a signet ring against a tablet screen [5]. This is an extra step that a user needs to perform, which adds inconvenience. None of these techniques can, therefore, provide a convenient and low-complexity solution to securing quick touch interactions on small devices.

This paper explores *body-guided communications* as a primitive for tracking and securing every touch. This allows a wearable touch token to exchange credentials with a receiver through a low-power communication channel that is established at the time the user touches the device. While our technique builds on prior research on touch and body communication [6–10], it differs in that it seeks to create a highly-confined, low-power communication channel between the user's token and devices that is suitable for touches. More specifically, it aims to maintain data rates suitable for touch authentication while improving security by *confining the signal to a few centimeters around the hand and lower arm carrying the transmitter token*. Therefore, we refer to this technique as body-guided communications rather than body communications.

The body-guided communications technique is motivated by an intuition that wearable devices such as a wristband or a ring are particularly suited as security tokens since there is less chance that a user will misplace them and that such devices are in close contact with the body. We also interact with many smart devices through touch, meaning that the human body creates a temporary connection between the device and the user's wearable. This intuition leads to the following fundamental questions. First, can the human body provide a robust transmission medium for body-guided communications in a variety of typical device touch scenarios? Second, can such body-guided communication achieve security properties more akin to those of a wire but with the convenience of wireless communications? Further, can it allow low-power communication at data rates fast enough to execute security protocols during the time of a quick touch?

In this paper, we introduce a body-guided communications model, touch token design, and a prototype for body-guided touch communications. Body-guided communications require closing the circuit through a capacitive return path which is dependent on exact token positions, posture, and environmental factors. To examine the feasibility under different conditions, we prototype two form factors, a wristband and a ring, and study the robustness of touch communication in several touch scenarios such as a button-device, and a handheld smartphone.

While strong cryptographic security protocols can also be implemented with such a device, the current prototype concentrates on exploring the body-guided communication primitive and demonstrates feasibility with a basic passcode protocol, where the wristband stores and transmits a code to identify and authenticate a user. When the user touches an object equipped with a touch receiver, such as on tablets or medical devices, this identification will be transmitted through body-guided communications to the touch receiver and authenticates the user. The current prototype's data rate is about 1kbps, sufficient to transmit a secret key of length 128-bit on most touches longer than 200ms. Higher data rates are also possible.

We show through experiments with this prototype that by including the human body in the communication channel, the humanfi nger effectively "extends" the transmitting electrode to be very close to the receiver, therefore allowing very low power at the transmitter side. This improves communication energy-efficiency but also protects against eavesdropping and man-in-the-middle attacks on this channel. In particular, we also show that in other directions in which free air has very high impedance, an electrode needs to be within centimeters of the transmitter to eavesdrop on the transmitted signal.

In summary, the salient contributions of the paper are:

- Proposing, analyzing and modeling body-guided communications.
- Designing a body-guided low-power authentication token for device interaction through touches.
- Designing an alternative transmitter, that allows reception of signals with unmodified capacitive touchscreen hardware.
- Implementing a prototype and experimentally studying its performance in authenticating every single touch.
- Conducting experiments with these prototypes in three different adversarial scenarios to evaluate the eavesdropping resilience of this design.

2 THREAT MODEL AND BACKGROUND

2.1 Threat Model

Token-based security protocols rely on detecting the presence of a security token during authentication by exchanging information between the token and the authenticating device. We consider an adversary that seeks to eavesdrop the transmitted signal, either to capture a secret passcode or as a means to launch man-in-the-middle relay attacks (e.g., [4]) on more secure one-time passcode protocols.

We assume that the adversary can design a custom receiver to accomplish this, and that this receiver can be more capable than the receivers used in the wearable and small IoT devices that the user may touch. For example, in the case of the radio frequency signals, the adversary could use

a high-gain directional antenna and low-noise receiver to capture weak signals. Similarly, for magnetic coupling-based communications, a larger coil with an iron core would be able to increase signal received at the adversary position. Both of the above devices are simple and can be easily hidden from users. In this paper we do not focus on attacks on the wearable or the touched device itself.

2.2 Existing Wireless Technologies

We categorize existing wireless methods for communicating with security tokens based on the following three criteria. We focus here on *physical layer* properties since upper layer cryptographic methods are equally applicable across all these technologies yet do not solve all security issues. For example, man-in-the-middle attacks are usually still possible, thus improving physical security is still desirable.

- *attack window*: considers the range from which the adversary can intercept or inject signals as well as the availability of known techniques to increase this range.
- *low power*: power consumed in the wearable token should be low.
- *touch association*: the ability to associate every touch with the intended signal.

Table 1 presents a summary comparison of the communication methods across these criteria.

Radio-frequency communications. Data is modulated on a high-frequency signal with a wavelength short enough so that it launches a radiated wave from the transmitter antenna. Transmitter antennas frequently use an omnidirectional pattern, where signal power is distributed evenly across all directions. In this case, the signal is not confined to the intended receiver. A nearby eavesdropper could receive equal or even stronger signals, resulting in a high attacking window. Simple reducing transmission power also reduces the signal at the intended receiver. Directional antennas are larger in size and a directional transmission may still reflect off other objects in unwanted directions. Security-oriented beamforming and other physical layer security techniques can reduce this attack window [11], but it is difficult to apply such techniques to wearables and small IoT devices for several reasons. First, information about the channel state is often needed in advanced, which is impractical for mobile wearable devices. Second, for directional transmissions or beamforming, the size of an antenna array with a reasonably narrow beam angle would be at least 10 times the wavelength. Since the antenna is constrained by the wearable form factor (ring: about 1-2cm, wristband: 5-10cm), the frequency of the radio would have to be tens of GHz. Operating the token at this frequency range consumes significantly higher power than at lower frequency (100-200KHz), so it is less suitable for a small battery-powered wearable device. More problematic is that the adversary may be less constrained in size and could take full advantage of high gain antennas and sophisticated receivers.

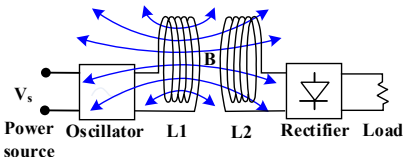


Figure 1: Magnetic coupling.

RF communications can be optimized for energy consumption resulting in about 10 to 100nJ/bit for transmission [12, 13]. Since it is difficult to confine a radio wave to a very short distance, the association of a device with a user touch is not clear when multiple users are around.

Near-field communications: Magnetic Coupling. In this technique, power is transferred between coils of wire through a magneticfi eld. In Fig. 1, an AC signal generates an oscillating magneticfi eld around the transmitter coil L1. the part of the magneticfi eld that passes through the receiving coil L2, generates a corresponding AC current in the receiver. Magnetic coupling is more limited in distance since thefield strength reduces with distance cubed and the fraction of the magneticfl ux passing through the receiver coil depends on orientation alignment.

However, an adversary has several options to increase the received power. The adversary could simply use a larger coil with more turns. Further, without space and cost constraints of a small device, the adversary can add an iron core inside the coil loop, since this material has very high permeability (>10000), thus it concentrates the magneticfi eld towards the adversary [14]. As a result, while more difficult than for radio frequency, any nearby adversary could still achieve higher signal-to-noise ratio than an intended receiver. As an example of attack risks to magnetic coupling-based communications, although NFC has a nominal operating range under 10cm, previous work [15] showed that it is possible to eavesdrop an NFC channel at a distance of 20-90cm, using a loop antenna that couples well with the magneticfi eld. Therefore, the attack window for magnetic coupling is ranked medium.

The power consumption of magnetic coupling tends to be low (transmission energy ≈ nJ/bit [12]), comparable to RF communications. However, since magnetic coupling authenticates all token inside the reception range, it cannot fully associate the touch with the intended signal when two tokens are both in close proximity of the receiver.

Vibration. Recently, vibration-based techniques, such as Ripple II [16] have introduced the ability to associate touch with the intended signal by guiding the acoustic signal through thefi nger bone. Ripple II uses a vibration motor as the transmitter and a microphone as the receiver. It achieves 7kbps from a ring and 2-3kbps from a watch, so it has the

Communication method	Attack window	Power	Touch association
RF	High	Low (≈ nJ/bit)	No
Magnetic Coupling	Medium	Low (≈ nJ/bit)	No
Vibration	Medium	High (≈ 100μJ/bit)	Yes

Table 1: Comparison of existing communication methods.

potential to satisfy the rate needed for authenticating every touch. Moreover, Ripple II is able to mitigate the attacks on vibratory sounds, but still an adversary with high-speed camera and line-of-sight to the device may intercept the vibrating signal.

However, current prototypes have high power consumption due to the vibration motor [17]. Current consumption of a typical vibratory motor [18] is up to 90mA at 2V, so the power consumption is nearly 200mW. At 2kbps bitrate (from a watch), the energy per bit is 100μJ/bit.

Goal. Among the three methods mentioned above, vibration is the only method with touch association ability, but it can only be achieved by at least three orders of magnitude more energy per bit than RF or magnetic coupling. Our goal, therefore, is to provide a low attack window and touch association at low power consumption, ideally comparable energy per bit as RF and magnetic coupling.

2.3 On-Touch and On-Body Communication

Several earlier projects have introduced the concept of communicating upon touch using different forms of body communication. EM-Comm [7] works in reverse direction: information is encoded in electromagnetic emissions of electronic devices and sensed by a receiver in a wristband when the devices are touched. Security was not a focus of this work and given the magnetic component of this signal, the attack range can be expected to be one meter, similar to that of near-field communications. BodyCom from Microchip [19] ostensibly uses the human body to transmit a signal from an on-body mobile unit to an external base unit upon touch. The design relies on capacitive techniques for detecting touch and works well when the user and the touched device can capacitively couple to a large central conductor, such as a door frame or a metal desk, to serve as common ground reference point for both units to close the circuit. The design also includes coils for magnetic coupling, likely to improve data rate particularly when the capacitive coupling is weak. This design also does not confine communications to the human body. Even when only considering the capacitive channel, a significant signal component travels through these external conductors. Moreover, the magnetic component again lends the design similar attack range properties as near-field communication. These techniques, therefore, can provide touch association but do not offer a highly confined attack range.

There are several related works on on-touch communication, which do not focus on confining the signal to a small part of the body. Hessar et al. [6] shows how signals from commodityfi ngerprint sensors and touchpads can be used to transmit information to other devices in contact with the user's body. Due to commodity device constraints, the data rate is limited to 50bps, which does not allow for exchanging longer codes or executing security protocols in the brief subsecond touch scenarios we consider in this paper. Moreover, it demonstrates how the signal can be received anywhere on the human body so that it is available to a broad range of wearable devices. Biometric Touch Sensing [9] also has the same limited bit rate problem: due to the COTS device's update rate, its transmission rate is only 12bps. Our design seeks to satisfy the bit-rate requirement (token is exchanged within one touch) by using a customized receiver that can be easily attached to the current devices. The design also confines the signal more within a small region of the body.

In addition, researchers have explored body communication techniques that can communicate between several devices connected to the human body [8, 20–25]. These also either do not fully confine the signal to a small part of the body or cannot communicate through afi nger touch connection. We will discuss these in more detail in the next section.

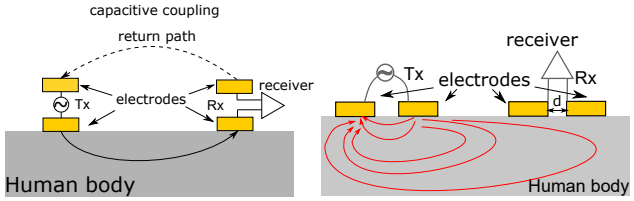
3 BODY GUIDED COMMUNICATIONS

To reduce the attack window and power, we seek to guide signals between the wearable and a touched device through the human body.

3.1 Challenges with employing body communication methods

The goal of transmitting a signal from one body part (at the wearable token position) to another body part (thefingertip) is ostensibly similar to that of intrabody communication (IBC) between two devices coupled to the human body. The challenge with directly employing such body communication methods is that they require direct electrode contact with the human skin for both the transmitting and receiving devices.

Two coupling types are normally used in this communication: capacitive coupling and resistive coupling [24]. In both types, both the transmitter and receiver require two electrodes each. In capacitively coupled IBC (Fig. 2(a)), one of the electrodes on the transmitter and receiver side is attached the human body, while the other isfl oating [26, 27]. In resistive coupled IBC (Fig. 2(b)), both of the electrodes



(a) Capacitive coupling. (b) Resistive coupling.

Figure 2: Different coupling types in IBC.

in the transmitter and receiver are attached to the human body [23].

Callejon et al. [25] observed that in resistive coupling, the signal attenuation increases with the Tx-Rx distance, while in capacitive coupling the path loss is much more dependent on the surrounding environments since the circuit is capacitively formed through thefl oating electrodes. In addition, when interelectrode spacing is longer in resistive coupling (either at the transmitter or at the receiver), the signal attenuation is lower. This is because with close spacing, the current mostlyfl ows along the direct path between them. With larger spacing, there exists more dispersion of the lines of current from the direct path, allowing more current to pass by the remote receiver electrodes.

This creates several challenges when applying the above two coupling types to transfer a signal from a wearable token to thefi ngertip. First, since thefi ngertip size is small, two electrodes touching thefi ngertip could only be spaced by a few mm. This significantly reduces the received power from these two electrodes as we saw above. Second, it is not desirable to require all object touch surfaces to be made of conductive materials (copper, iron, etc.). In most cases, the electrodes could be more easily hidden behind layers of non-conductive materials (plastic, glass, etc.). This means that there is no direct resistive skin contact to the electrode of the touched device and neither the traditional capacitive coupling nor resistive coupling for body communications is possible.

3.2 Double capacitively coupled communications

To overcome these challenges with conventional intra-body communications we design a body-guided communications method that allows for a double capacitively coupled circuit.

Design. The key difference in our design compared to previous on-body communications is the combination of resistive coupling at the transmitter side and double capacitively coupling at the touched receiver. As will be seen below, this design improves received signal at the intended receiver while reducing it at an attacker monitoring the channel on air.

On the *touched device*, none of the electrodes have to be in direct skin contact, but one is placed as close as possible to

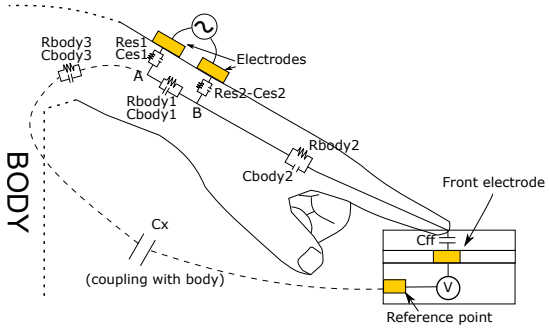


Figure 3: Body-guided communication method: Channel modeling.

the expected touch-point of the device (usually behind non-conductive material that the device is made of), while the other electrode is simplyfl oating and even less constrained in position. On the *wearable side*, we exploit direct skin contact since this can usually be accomplished for wearables. Both electrodes are placed in direct contact with the user's skin, and their electrode spacing is maximized given the size constraint of the wearable token (wristband or ring).

In other words, the link between the wearable and the user's body is through resistive coupling, while both links between the user's body and the touched device are through capacitive coupling. Note that this differs from conventional capacitively coupled body communications on both sides. The intuition here is that by attaching the wearables second electrode closer to the main body, the large human arm effectively forms a larger capacitor with thefl oating electrode of the touched device. This creates a stronger signal and compensates for the reduction in signal due to the double capacitive coupling on the touched device while keeping the signal largely confined in the arm.

Our approach differs from Microchip's BodyCom [19] and other capacitive body communication techniques in that the return path directly couples to the body. Thus, it does not require common external ground planes for the two units to couple. This allows the system to work well in more environments and reduces the attack window. Our design also differs from work by Hessar et al. [6]: it allows both electrodes on the touched device to be capacitively coupled, while their work assumes a metal surface with direct resistive skin contact at the receiver side. Capacitive coupling is easier to incorporate into many objects made out of non-conductive materials.

Model. To understand this better, consider the circuit model for body guided communications in Fig. 3. The two electrodes in the wearable are powered by an AC signal generator and placed in direct contact with the user's skin. Inside the human body, there are conductive tissues, which are separated from the electrodes by a layer of skin's epidermis. We model the epidermis layer between each electrode and the

conductive tissues as a parallel pair of resistor and capacitor ($[R_{es1}, C_{es1}]$ and $[R_{es2}, C_{es2}]$). We separately model the impedance between these 2 points in the conductive tissues under the two electrodes ($[R_{body1}, C_{body1}]$) because the resistance in the tissue is far lower than the skin's. The majority of the current willfl ow through this skin-tissue-skin path. A second much weaker current path, but one significant for our design,fl ows through thefi ngertip and through the touched device. This path can be modeled as the tissue impedance between point B and thefi nger ($[R_{body2}$,$C_{body2}]$) and the double capacitive coupling to the human body. Since the surface of the touched object can be non-conductive, thefingertip and the front electrode forms a capacitor C_{ff}. Finally, the reference point forms a capacitance C_x through the air with the large human body, which is connected through a last impedance with the other wearables electrode A, effectively closing the circuit loop. The voltage at the front electrode is measured by a receiver with respect to the reference point (internal ground) of the device. Note that this ground point can also be a metal surface inside the device.

Note that due to the large distance, C_x is much smaller (pFs) than C_{ff} as well as the tissue or skin impedances (nFs). Therefore, it is the limiting factor on the circuit allowing the signal tofl ow through the touched device. Since electrode A is also attached to the body, the comparatively large human body can capacitively couple to the device, increasing the capacitance C_x to about 100pF according to the Human Body Model [28].

Consider now the change occurring when thefi nger stops touching the device. The increasing distance between the fingertip and the front electrode reduces C_{ff}. Since the size of thefi ngertip and the front electrode are small compared to the size of the human body, C_{ff} becomes smaller than C_x even at very small distances. Then C_{ff} is the limiting factor and the resulting high impedance lets only a negligible currentfl ow through the device. Since the presence of a detectable signal is so closely linked to actual touch, this shows how thefi nger guides the signal and promises to achieve our goal of touch association and small attack windows.

All other paths through the air have higher impedance than the above path through the body, leading to much weaker signal received at any point on air. For a given double capacitively coupled touch device, we experimented with different setups of the two electrodes at the wearable side: both with direct skin contacts (resistive coupling), one with direct skin contact and one separates from the skin by a thin mylar layer (capacitive coupling), and both capacitive coupling. More details of the form factor of the wristband are in Section 4.1. Fig. 4 shows the average signal-to-noise ratio at the intended receiver and at a position on air that is 1cm and 5cm away from the token. When the touch device has double capacitively coupled electrodes, the configuration

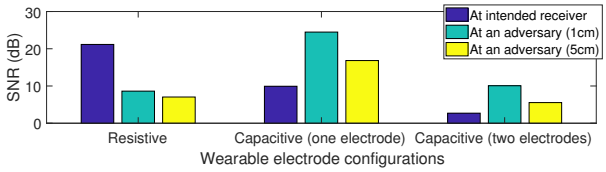


Figure 4: SNR at the intended receiver vs. at an adversary on air for different wearable electrode configurations.

with both resistively coupled electrodes on the wearable side gives us the highest signal advantage at the intended receiver over an adversary monitoring the channel on air. This is the rationale for our design choice.

4 TOUCH AUTHENTICATION TOKEN DESIGN

Let us now consider how to use this body guided communication primitive to design a per-touch authentication token. Our system consists of a transmitter embedded in a wearable token, which is worn on the user's body and sends the user code through thefi nger to thefi ngertip. When the user touches an object with an embedded receiver, the receiver can detect the signal and decode the authentication credentials for each touch event. The design sets aside more sophisticated protocols such as time-based one time passwords [29], and focuses on demonstrating the feasibility of improving the token communication with body-guided communications through a passcode exchange from the wearable to the touched device. It assumes that the wearable is activated just before such an exchange.

4.1 Wearable Design

Electrode placement and size of the token are key design factors since the body guided communication signal is dependent on body resistance as well as environmental capacitance. The goal is to enable a wide range of possible touch scenarios.

Touch Interaction Scenarios. To guide the design, we chose the following samples of device interaction scenarios: (1) a wall-mounted device touched by a standing user. This represents a switch, smart thermostat, or display for example; (2) a device on a table touched by a sitting user, representing a tablet or touch screen; (3) a user holding a touch device, while touching it with the same hand; and (4) a user holding a touch device, while touching it with the other hand. In most cases, the actual touch will occur with the indexfinger of the dominant hand, except for case 3, when touches are performed with the thumb.

Form Factors. Based on the modeling of body guided communications in Section 3, we seek to increase signal quality by 1) placing a token close to the intended receiver and 2) maximizing the electrode spacing.

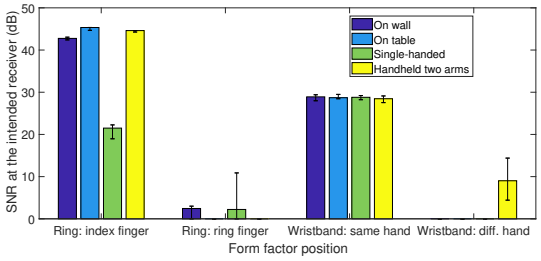


Figure 6: SNR received at the receiver for different form factor positions and different touch scenarios.

Rings or watch- and wristbands stand out as wearables thatfi t the distance criterion. Let us, therefore, consider the following electrode designs that maximize electrode spacing within the size constraints of these form factors (Fig. 5):

Ring: the ring has the shape of a cylinder with height H = 2cm. There are 2 thin strips of copper on the inner side of the ring (in contact with thefi nger); they are placed on two sides of the ring and wrapped around thefi nger. Each electrode strip has height d = 0.3cm, and they are separated by 1.4cm.

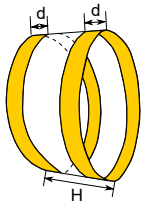


Figure 5: Wearable design.

Wristband: the wristband has the same shape and electrode placement as the ring, but with H = 2.4cm, d = 0.6cm, and larger electrode spacing of 1.2cm.

Generality of Wristband Design. In order to choose a suitable form factor, in terms of usability and ability to deliver the signal to the intended receiver, let us study the effect of form factor position for the different touch scenarios on the SNR at the intended receiver. For the ring, we then explore two positions: on the indexfi nger, which is also used to touch the receiving device and on the ringfi nger. For the wristband, we test on both wrists of the hand that is used to touch and on the wrist of the other arm.

Fig. 6 shows the signal quality received at the device in terms of signal-to-noise ratio for all combinations of these interaction scenarios and wearable positions. The transmitter is a microcontroller producing a square wave signal at 150KHz, and the receiver has a small electrode pad covered by a thin non-conductive mylar tape. The received signal at 150KHz is measured by a USB oscilloscope that is disconnected from earth ground. We give more details in Section 5. As evident, the signal quality varies significantly across these use cases. The indexfi nger ring and wristband form factor provide the most consistent signal quality across all scenarios when the device is located on the same hand, whose indexfi nger touches the device. Since wristbands are more commonly worn than index-finger rings, particularly given thefi tness tracker trend, we focus on the wristband design.

We also validate that this form factor achieves our goal of touch association, that is that the received signal is only present when the token-wearing user touches the device. This can be characterized by the SNR difference at the receiver between an actual touch and close centimeter-level proximity. We conduct experiments to investigate this SNR difference for three cases: off-hand table, one-hand, and two-hand operations. We noted that the exact SNR depends on various factors: on the wearable token, the electrode size, the distance between them; on the receiving pad, the electrode size, the distance between the front surface and the electrode, etc. In this specific experiment, the user wears a wristband with dimensions described above, covered by a thin mylar tape layer of 0.1mm. The receiving pad is a small electrode of size 1cm^2, also covered by a thin mylar tape layer of 0.1mm.

Fig. 7 demonstrates the SNR difference between touch and no-touch for three cases: off-hand, one-hand and two-hand operations. The SNR increases with transmitting voltage, but SNR difference between touch and no touch remains relativelyfi xed in each case. These SNR differences are 13dB, 5dB, and 23dB for off-hand, one-hand and two-hand operations, respectively. As will be shown later, the small SNR difference for the one-hand case would decrease the touch recognition accuracy.

4.2 Receiver Design

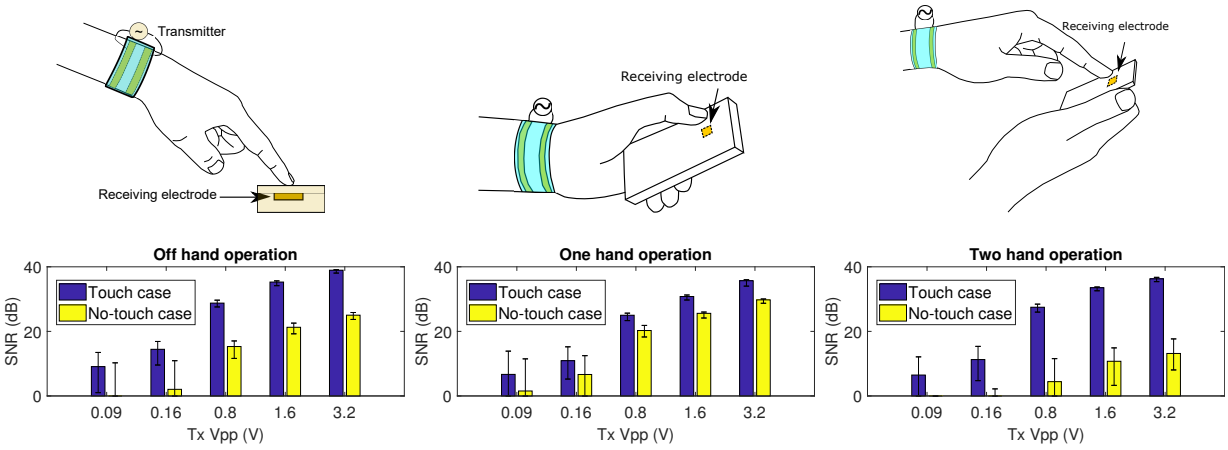
Since a goal of this work was to provide morefl exibility for electrode placement in devices, there are different ways of putting a receiving electrodes into an object that needs authentication/identification. We choose the following example designs:

- **button design:** For small IoT devices like Amazon dash buttons, we embedded an electrode behind its front-facing plastic/glass case. The electrode size is 1cm^2 (about thefi ngertip size), and the front-facing case is under 1mm thick.
- **phone case design:** For phones and tablets, we can put electrodes in plastic cases used to cover the back of the devices, so that the electrodes have direct contact with the device body. Since the device can be as thick as 1cm, we increase the size of the electrode to be nearly the same size as the device dimension. For example, for a Nexus 5 phone, the electrode size is 13×6cm^2.

In these designs, we do not use an explicit second electrode in the device. The receiver connects to the electrode above and measures the voltage with respect to its internal ground.

4.3 Transceiver Design

Operating frequency. We look for the optimal carrier frequency for operating the transmitter. Fig. 8 shows the SNR received at the receiver for different frequencies when the transmitter sends a 3.3Vpp square wave. Note that the analysis is limited to 450KHz because of the limitation of the



(a) Off-hand operation. (b) One-hand operation. (c) Two-hand operation.

Figure 7: SNR difference between touch and no touch for different touch interaction scenarios.

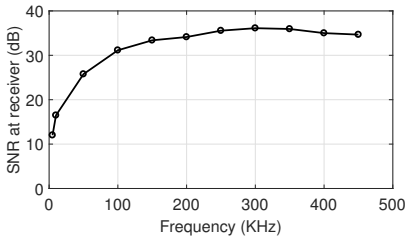


Figure 8: SNR received at the receiver for different frequencies.

microcontroller used for the wearable token. We can see that SNR is worse at frequencies less than 100 KHz, but starting from 100KHz, the SNR doesn't change much with frequencies: the difference is within 5dB. As the result, we should choose frequency above 100KHz to ensure good received signal level at the receiver. On the other hand, the frequency in use should be kept as low as possible since: (i) high frequency means smaller wavelength, but we want the wavelength to be several orders of magnitude larger than the electrode size to minimize any RF radiated signal that an adversary can capture, and (ii) low frequency allows lower power consumption. In all of our evaluations, we choose 150KHz as the operating frequency of the wearable token.

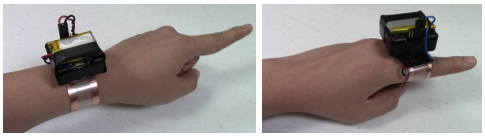
Modulation. The frequency above can be used as the carrier wave for modulating bits in the user's identification code. We choose On-off keying (OOK) modulation method, which represents the bits as the presence or absence of the carrier wave. Given high SNR at the intended receiver when the user touches the device, it is possible to use Amplitude-shift Keying (ASK) to achieve a higher bit rate. However, we will later show that the simple OOK modulation satisfies the necessary bit rate and code length needed for common per-touch authentication applications.

Authentication process and protocols. For per-touch authentication, the receiver needs to associate each touch with a user ID code. This includes two steps: *touch recognition*, which triggers the authentication process, and *bit decoding*, which demodulates the received signal to get the user's ID code. Touch recognition can be implemented through other components of the device or with the detection mechanism in the signal receiver itself. For packet detection and bit decoding, methods include power-based detection, correlation detection based on known bit sequence (such as Barker sequence [30]). When activated, the transmitter can repeatedly transmit the authentication credentials with a preamble to mark the beginning of a transmission of the code. In this paper, we focus on the touch recognition ability of the standalone receiver and a simple power-based bit detection; we leave the design of the full authentication process and protocols for future work.

Power. From measurements, we observed that during touch, received signal voltage at the intended receiver is about two order of magnitudes smaller than the original transmitted voltage. For example, when the transmitter is powered by a 3V coin cell battery, the received voltage is about 25mV. We can design a custom receiver to amplify this signal to detect the code being sent; we give details about one such implementation in Section 5. For off the shelf phones or tablets, since they are not designed to sense this small signal, we seek a method to generate high voltage at the transmitter to deliver big enough signal to the devices to trigger their touch events.

5 SYSTEM IMPLEMENTATION

On the transmitter side, we implement both a low-power token with a custom receiver and a token that allows using off-the-shelf touchscreen hardware as a receiver.



(a) Wristband form-factor. (b) Ring form-factor.

Figure 9: Transmitter prototype.

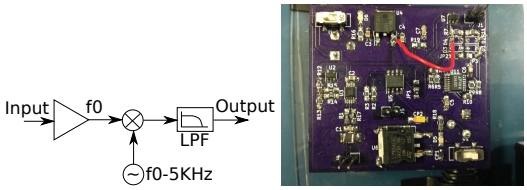
5.1 Low power token

Transmitter. We use a Teensy 3.2 board [31], powered by a 3.7V LiPo battery, to generate a square wave of the frequency of 150KHz. This board has a Digital-to-Analog Converter for output voltage control, allowing experimentation with different transmission power levels. The microcontroller output is connected to two electrodes in direct contact with the user's skin. We demonstrate our technique for two form factors of the token: a wristband (Fig. 9(a)) and a ring (Fig. 9(b)). The microcontroller and battery are inside a small plastic case sitting on top of the electrodes. Note that the electronics of the prototype can be easily miniaturized. The transmitter circuit has much lower complexity than common radio chips and size is primarily determined by electrodes and the battery. It could be integrated into smartwatches as an add-on feature.

Receiver. The receiver downconverts the signal to allow a microcontroller to implement sampling and processing. The design and our fabricated board are shown in Fig. 10. The input signal from the sensing electrodes isfi rst amplified with an instrumentation amplifier (INA332 [32]), then fed into an analog multiplier (AD835 [33]) with a reference signal set to $f_0 - 5KHz$, where f_0 is the frequency of the signal generated by the transmitter. The local oscillator is controlled by an Analog Discovery 2 instrumentation device [34]. The output signal from the analog multiplier consists of a 5KHz frequency component together with higher frequency components. By applying a low passfi lter (LT1563 [35]) with a cutoff frequency above 5KHz on this output, we can extract the low-frequency component, whose amplitude is proportional to the received signal at frequency f_0.

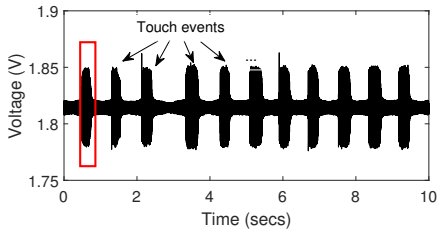
The signal after the low passfi lter is read by an MSP432 microcontroller [36] at 20KHz sampling rate. To ensure real-time performance with no sample loss during processing, we implemented a dual-buffered memory, with 2KB for each buffer, to store ADC samples. A ping-pong DMA is implemented so that ADC samples accumulate in one buffer while the processor works on the other buffer.

As an illustration, Fig. 11 shows the signal received from the receiver board. The user wears the wristband with the transmitter board on the wrist and touches the receiving electrode (for simplicity, the electrode is touched directly here, while the remainder of the evaluation focuses on electrodes that are behind non-conductive material) multiple times with the same hand. The transmitter continuously modulates a

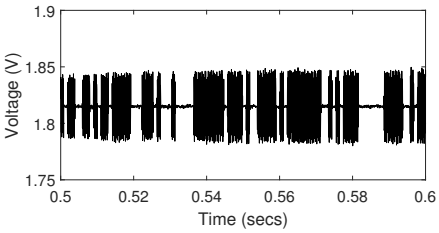


(a) Receiver design. (b) Fabricated receiver.

Figure 10: Touch receiver.



(a) Signal received from the receiver board.



(b) Signal received from the receiver board (zoomed in from red area in Fig. 11(a)).

Figure 11: Signal received from the receiver board.

random 128-bit identification code on this signal by using On-Off Keying: bit 0 turns off the output and bit 1 turns on the 150kHz signal. As shown in Fig. 11(a), the amplitude of the 5kHz signal significantly increases during the time the user touches the receiving electrode and is very weak even when thefi nger is only about a cm away from the receiver. This helps the receiver recognize touch events and trigger the bit decoding process. Fig. 11(b) is the zoomed-in version of one example touch event. At this scale, we can observe the ID code sent from the user token with OOK modulation.

Note that our custom receiver can be easily integrated with smartphones. For the current COTS mobile devices, the receiver can be added in the form of a case with electrodes in contact with the back of the devices and a small receiver circuit inside. The receiver circuit can send the code received to the mobile device through Bluetooth or USB, and the mobile device can integrate this information with its own touch position identification. For the next generation of mobile devices, the receiver can be made in the form of an ID detection chip alongside the current touch detection circuit and reuse the electrodes in the touch screen as its input.

Our receiver design differs from COTS receivers in the touch sensing mechanism and data rate. COTS touchscreen recognizes touches via the change in capacitance on a matrix of sensing electrodes [37, 38]. It only detects the *presence* and *position* offi ngers; its scanning andfi ltering mechanisms limit the reception of high-speed signals transmitted from the token to thefi ngertip. In contrast, our receiver is designed to sense the current running through the receiver electrodes when afi nger touches the device surface, as described in Sec. 3.2. It is optimized to detect signal at the frequency generated at the token transmitter, thus allows much higher data rate, which is needed for per-touch authentication.

5.2 Token for COTS touchscreens

In order to elaborate the pervasive of our method to secure every touch with body-guided communication, we show the operation scenario using our custom transmitter along with a COTS touchscreen such as smartphone screen as the receiver. In particular, we generate a modulated signal that will go through the human body and observe the phenomenon at the contact point of user'sfi ngertip and touchscreen. Whenever the modulated signal is transmitted from the signal generator, the touchscreen is affected and *artificial* touch events are generated correspondingly. We confirm that the artificial touches can also be created on COTS devices using the following method, but at a lower rate of communication.

Transmitter. We used Analog Discovery 2 [34] to generate a 10V peak to peak sweeping sinewave signal (200kHz sweep to 500kHz in 1ms) using OOK modulation. The Analog Discovery waveform output is connected to the user's indexfi nger through a wire and ring-like form electrode. The ground pin of the Analog Discovery output isfl oated.

Receiver. The receiver is a Samsung Galaxy S5 running Android 6.0.1. The app is written on the phone to capture the artificial touch events and decode the transmitted bit sequence using OOK demodulation. Through experiments, we found that the system obtains up to 92.5% of accuracy at 10 bps rate. Details evaluation results are presented in Section 6.

We conducted experiments tofi nd out the best waveforms and frequencies that could create reliable communication between our customized transmitter (Analog Discovery) and COTS receiver (Samsung Galaxy S5). We tested the frequencies from 100kHz to 1MHz with sine, square, triangle waveforms. The sine and square waves sometimes can generate expected artificial touches, but we found that sweeping frequency technique obtained better results and is more reliable.

6 PERFORMANCE EVALUATION

6.1 Difficulty of Eavesdropping

Since the received signal at the adversary is dependent on factors such as the transmission power used, we measure the difficulty of eavesdropping as the signal advantage of the receiver, which is independent of transmission power. We define signal advantage as the difference between the SNR at the intended receiver and that at the adversarial receiver. The signal advantage characterizes how easily the token can be designed: a large positive signal advantage allows us to choose an appropriate transmission power to ensure necessary signal level at the intended receiver while reducing the receive signal at the adversary to an undecodable level. A signal advantage equal to or below zero means that this is not possible.

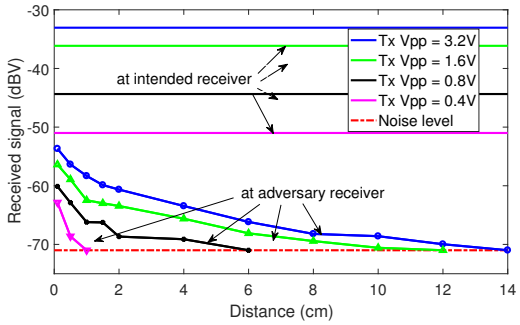


Figure 12: Received signal at different distances from the wearable token (wristband form factor).

We focus this evaluation on extremely challenging scenarios, where existing wireless technologies cannot achieve positive signal advantages.

Protection against remote monitoring over the air. To evaluate how secure the body-guided communication channel against an adversary monitoring over the air with a wearable-size receiver, for each transmission power, we measure the received signal at a 3×3 cm^2 electrode over a range of small distances d to the token. We focus on the most challenging case, with very small distances in the mm to cm range. Fig. 12 shows the received signal level at the intended receiver and at the adversary, for different distances and different transmission powers. The received signal at the adversary's receiving electrode degrades quickly as distance increases. Even at an extremely close distance of 1mm, the signal received at the adversary's electrode is 20dB worse than at the intended receiver. This means that at our highest transmit power setting the signal was below the noisefl oor for the adversary at a distance of 15cm. A signal from a well-designed transmitter would be well below the noisefl oor at mm-range. For comparison, related work [6] reports a signal advantage of 16dB at a distance of 6cm compared to 30dB in our design and requires resistive contacts at both the transmitter and receiver to achieve this.

Note that one cannot expect any signal advantage of the intended receiver with radio or magnetic coupling when the adversary is at such close proximity. As discussed in Section 2

the attacker could further take advantage of high gain antennas (for RF) or a larger coil with an iron core (for magnetic coupling), to achieve a strong negative signal advantage, meaning that the adversary has the advantage. These techniques do not apply to body-guided communications.

Low SNR leads to high bit error rate (BER) in the decoding process. Table 2 shows the BER using the same receiver for several distances when the transmission voltage is 3.2Vpp. Although BER is 0% when the receiver touches the token, a small gap between the receiver and token increases the BER the BER significantly; at 10cm, the BER is 44.7%, disabling the attacker's ability to eavesdrop the code. This demonstrates how the body-guided communication token design reduces the attack windows.

d (cm)	0	2	4	6	8	10
P(Rx) (dBV)	-53.68	-60.65	-63.45	-66.17	-68.21	-68.60
BER (%)	0	12.78	15.7	28.19	22.7	44.7

Table 2: BER vs. distances (received power at each distance is also recorded).

Protection against direct and indirect contact. Besides over the air remote eavesdropping, as can happen in RF security risks, we also consider other example scenarios where an adversary can get in direct or indirect contact with a user to attempt to eavesdrop on his body-guided communications. Fig. 13 illustrates these scenarios. To measure the SNR at the adversarial receiver, we use an Analog Discovery 2 100Msps USB oscilloscope [34] connected with an ungrounded laptop. The noise level is about -71dBV.

Scenario 1: Direct touch of user's skin. This scenario represents a crowded or close-collaboration setting where an adversary could achieve direct skin contact without much suspicion while the user authenticates. In this case, the adversary touches the receiver electrode onto the user's skin just below elbow level, as shown in Fig. 13(a). For this scenario, the signal advantage remains between 10-16dB across all transmission powers, as shown in Fig. 14. We also observed that the received signal power decreases significantly as the receiver moves centimeters away on the arm from the transmitter token (Fig. 15). This shows our configuration confines the signal to lower arm carrying the token and virtually no eavesdropping is possible on other body parts.

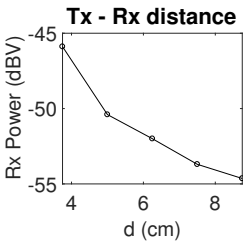


Figure 15: Received signal vs. distance on arm.

Scenario 2: Indirect touch through conductive material. This scenario could occur when two persons are both leaning on the metal door, holding handrails in a metro, or on the stairs. In this scenario, we assume that the attacker places his receiving electrode on the hand that touches the metal surface and thereby directly connects to the token user'sfi nger, as shown in Fig. 13(b). The intended receiver has an SNR advantage of 21dB over the eavesdropper when the eavesdropper's SNR decreases to 0dB, as shown in Fig. 14.

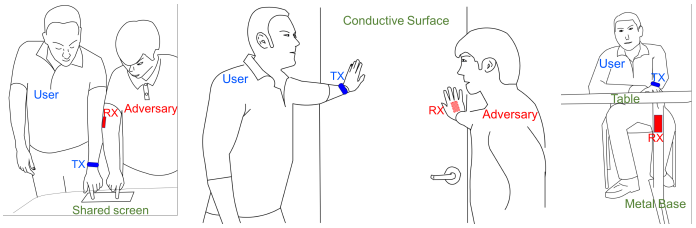
Scenario 3: Indirect touch through non-conductive surface. Here the adversary attaches the receiver to a large metal body hidden behind a non-conductive surface that is touched by the user's hand. An example is the metallic support of a table, as shown in Fig. 13(c). The intended receiver has SNR advantage of 10-17dB over the eavesdropper across all transmission powers, as shown in Fig. 14.

Overall, these results show that even with direct contact to the user's body the adversary receives a significantly weaker signal than the intended receiver and therefore requires more sophisticated receiver hardware to capture the signal.

6.2 Per-touch authentication/identification

To successfully authenticate every touch, it is important to associate each touch event with one user ID. The receiver should be able to process the signal stream following two steps: (i) recognize touch events, and (ii) detect the user's ID code in the signal portion inside the detected touch event's duration. We evaluate two metrics corresponding to these two steps: *touch recognition rate*, the percentage of the touch events that are recognized, and *decoding success rate*, the percentage of the touch events that the receiver can successfully decode a full ID code that was sent from the wearable token. We also evaluate *bit error rate* of the communication channel for different users. For the following experiments, the users are not constrained on how they touch the device: they can tap or swipe in any direction.

Touch recognition rate vs. transmitted power and touch scenarios. The touch recognition ability can be provided by other components of the device: for example, the Amazon dash button knows when the user presses it, thus can notify our receiver to start decoding the signal. Here we also investigate the capability of a standalone receiver, which can extract touch events from the received signal stream. We tested with 1826 touches for three power levels of the transmitter (peak-to-peak voltages are 0.09V, 0.8V, and 3.3V) and three different touch interaction scenarios as described in Fig. 7. A touch event is detected when the amplitude of the received signal crosses an adaptive threshold, which we derive from the statistics of the signal when there is no touch. In our implementation, given S is a window of signal when there is no touch, we choose the threshold to be $T = average(S) + k[max(S) - average(S)]$, and k is empirically chosen to be 1.8. Fig. 16 shows touch recognition rate for all these cases. At higher power (0.8V and 3.3V peak-to-peak), the touch recognition rates for all three cases are above 92%. As analyzed in Section 4, the SNR difference



(a) Adversary touches user's arm. (b) Indirect touch(conductive material). (c) Indirect touch (non-conductive surface).

Figure 13: Touch-based eavesdropping.

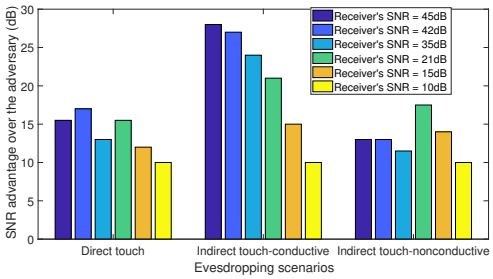


Figure 14: Intended receiver's SNR advantage over the adversary.

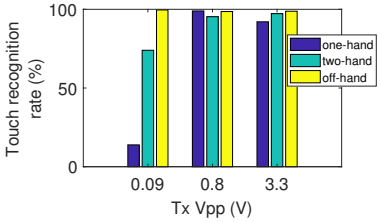


Figure 16: Touch recognition rate vs. transmission power.

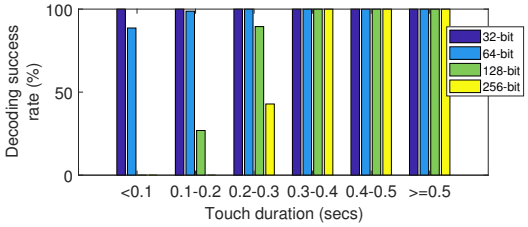


Figure 17: Decoding success rate vs. touch duration and code length.

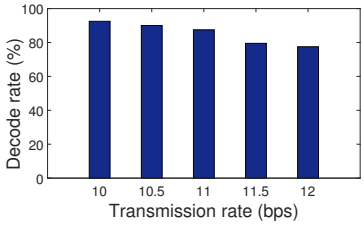


Figure 18: Decode rate vs. transmission rate (COTS receiver).

between touch and no-touch in the one-hand scenario is the lowest, thus at low power (0.09Vpp), the touch recognition rate for this scenario decreases to only 13.81%.

Decoding success rate vs. touch duration and code length. We conducted experiments with two people touching the objects for a total of 2170 touches over 5 days with varying touch durations from 50.7ms to 1.78s. We also experimented with different code lengths: 32, 64, 128, and 256-bit long. The data rate is 1kbps. Fig. 17 shows the decoding success rate versus touch duration. As can be seen, for all code lengths, the decoding success rate increases as the touch duration becomes longer. Also, for the same touch duration, shorter keys have a higher decoding success rate. For the common 128-bit ID, it achieves 89.5% accuracy when the touch duration is between 200ms and 300ms, and 100% accuracy when the touch duration is longer than 300ms.

This result is, of course, dependent on the data rate of 1kbps. The current receiver is limited by the microcontroller sampling rate and not optimized for data rate. According to Shannon theory, the achievable bit rate at 100 kHz is $C = Blog_2(1 + SNR) = 100kHz \times log_2(1 + 100) = 665kbps$.

Bit error rate vs. different users. Since our body-guided communication method relies on human hands as the transmission medium, we examine its performance across different users. Eight graduate students wore the prototype wristband and naturally touched two prototype devices for 5 minutes each: one is an Amazon IoT button [39] with an electrode attached behind its front-facing plastic case, and the other is a Galaxy Nexus 5 phone with an electrode attached on its back. Figure 19 shows the bit error rate across these users. As can be seen, for all users and both devices, the BER remains under 10^{-2}. This suggests that with coding robust body-guided communication can be achieved.

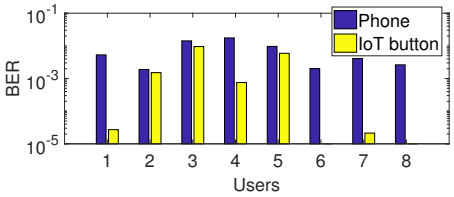


Figure 19: BER vs. different users.

COTS touchscreen as receiver. To confirm the feasibility of enabling this channel of communication with an unmodified touchscreen as the receiver, we implemented a simple receiver software to decode the artificial touch event sequence, generated by the Analog Discovery transmitter through the user's body (Sec. 5.2). By counting the number of software-reported touch events during the transmission period (i.e. the effect of the transmitter to the touchscreen during the period of turning the signal generator on), we achieve a decoding rate of 92.5% at 10bps. When the transmission rate is increased the receiver's performance reduces due to the mismatch between the signal being generated and the response of the screen as shown on Fig. 18. While the data rate is low, it can still improve security as part of two-factor authentication protocols, especially over a sequence

of touches or during longer swipes. For example, when a user types a password or swipes a secret pattern with his/her finger on the screen, the wearable device can simultaneously transfer a proof that the user possesses the hardware authentication token (e.g., the wristband). In addition, we expect that the data rate can also improve significantly by modifying the touch driver of the COTS receiver for increasing its touch sensing frequency.

6.3 Power consumption

The microcontroller in the hardware token only needs to continuously modulate the user code using On-Off Keying, so it can be operated at low power. The results from the prior sections are obtained from ourfi rst prototype where the wristband token was implemented using a Teensy microcontroller development board [31]. The average current drawn in this unoptimized prototype is 37mA at 4V supply voltage, which means the token consumes 148mW on average. Given the simple functionality of the token, we started optimizing for power with a low-power microcontroller to understand to what extent the power consumption of the wearable token can be reduced. In particular, we implemented a second prototype token using an MSP430G2553 microcontroller [40] in its low power mode and measured the power consumption of the token when worn on the user's wrist. This prototype is capable of producing the same output signal as thefirst one, so we do not expect any change in the prior results. Measurement results with this second prototype show that the average current drawn is 1.3mA at the 3V supply voltage, which means the microcontroller only consumes 3.9mW on average. At 1kbps, the energy per bit is 3.9μJ/bit. Even though the microcontroller is not fully optimized yet, the energy per bit is already two orders of magnitudes lower than the estimated power of the only other communication prototype with a smaller attack window (vibration-based communication with 100μJ/bit, see Sec. 2).

For comparison, the measured power consumption of our prototype receiver is 525mW. This consists mostly of heat dissipated at inefficient linear regulators (225mW) and power at the mixer chip (250mW). The power consumption of the receiver can be optimized in an integrated circuit form. Receivers could also be activated by the user's touch to avoid continuous operation but this is out of the scope of this paper.

7 DISCUSSION AND FUTURE WORK

Benefits of body-guided communication over near-field communications. Capacitive coupling is the dual of magnetic coupling: they both occur in near-field region, not in the radiated farfi eld region. However, when the authentication token is worn on user's body, capacitive coupling has an advantage over magnetic coupling: human tissues have a high dielectric constant, so the capacitive coupling approach can alter the electricfi eld to focus on the intended receiver. In contrast, the relative permeability of human tissues is close to that of free-space, so the human body plays no role in guiding the magneticfi eld. Also, received signals when touch and when no-touch occur (even when thefi nger is separated only a few mm from the object) have a large difference, which provides a primitive feature for *touch association*.

Security and Activation. Through-body capacitive coupling reduces the attack window by its "beam-forming" ability to create a better channel from the transmitter to receiver than in any other direction. We are not aware of any method that an adversary could employ to increase receiver gain as easily as for magnetic coupling (more turns), RF (high gain antennas), and vibration (high-speed camera). As with wired communications, the adversary can, of course, capture the signal with high quality when directly in the circuit—that is between thefi nger and the button (e.g., ATM skimming device). Our results also show that the signal can be captured while shaking hands if the signal was inadvertently transmitted during this time. This highlights the needs of one-time password protocols or an activation mechanism (the wearable only transmits when the user touches the intended receiver). The latter would also decrease the token's power consumption.

Currently, our experiments only demonstrate the feasibility of unidirectional communication from the wearable token to the touch receiver. To support sophisticated authentication protocols such as challenge-response, this technique can be complemented with a reverse channel. Note that many protocols can obtain security benefits from our technique even if the reverse channel uses a less secure magnetic or radio-frequency communication medium. For example, the challenge in a challenge-response protocol could be broadcast over Bluetooth or NFC.

Power consumption. The clearly defined channel along thefi nger also helps lower power at the transmitter, while maintaining a sufficient level at the touched device. Power is also reduced through the operating frequency of hundreds KHz instead of the tens of GHz that would be necessary for RF beamforming approaching a similar level.

There is ample room for optimizing power-consumption of the design. Assuming a highly optimized design with negligible processing power, an estimate for the lower bound can be found in the necessary transmission power. Since the transmitted signal feeds two electrodes in contact with the human skin, two factors affect the transmission power. The first factor is power to charge and discharge the body capacitance: assume the energy per bit is the energy to charge up the capacitance between two electrodes. The measured capacitance is about 10nF, leading to energy per bit at an operating voltage of 3V is $Eb = CV^2 = 10^{-8} \times 3^2$ J/bit = 90nJ/bit. The second part is power dissipated from the body resistance between the two electrodes: The measured resistance is about

10MΩ, leading to power ($P_R = V^2/R$) of about 0.9μW. For 1kbps data rate, the energy per bit consumed by body resistance is 0.9nJ/bit. In total, lower bound of energy per bit of our token is 90nJ/bit, which is comparable to that of common wireless technologies (Wi-Fi, BLE, NFC).

8 RELATED WORK

Device authentication techniques. Although password, PIN or pattern are widely used for device authentication, they are inconvenient when entering frequently and susceptible to shoulder surfing attacks [41] and smudge attacks [42]. User identification code can also be encoded as a series of electrical pulses that trigger the capacitive touch sensing when the ring's token directly contacts the mobile's touch surface, e.g., SignetRing [5]. While this ring also allows transmitting a few bits per second when only thefi nger touched the screen, this rate is insufficient to identify users on a brief half-second touch. Further, since a high voltage is needed to spoof the screen, the ring has high power consumption. Nguyen et al. [43] presented a low-power, battery-free device to transmit data from 3D printed object to the touchscreen. However, the supported bit rate is only up to 32bps, which limits its use in per-touch authentication applications. Also, these approaches still require the tokens to have direct contact with touch surfaces, which is inconvenient for normal touches.

Biometric authentication [44] is another authentication technique used in current devices. Fingerprint identification is currently supported using a dedicatedfi ngerprint scanner, which makes the device design more complex and expensive. Face identification, such as Apple's Face ID [45] identifies the user's face by applying neural networks classifier on images captured by the infrared camera along with the conventional camera. Although our approach also uses dedicated receiver hardware, it offers a different design point. As a much larger number of devices become smart the economics shift so that adding hardware to a few wearables in order to simplify the receiver hardware on each device becomes more efficient. Furthermore, our system allows faster recognition, thus supports authentication on the per-touch basis, not only at the session level as withfi ngerprint sensors and face identification. Also, the main drawback of biometric authentication is once the userfi ngerprint/face is captured by an adversary, they are hard to change compared to tokens or passwords. It is also not straightforward to integrate camera-based or face authentication solutions into devices with smaller interfaces or lower specs (such as Amazon buttons), and there is no direct association between people recognized by the camera and actions performed on the touched devices, especially in multi-user operation scenarios.

On-body wireless communication has been proposed for paring wearable devices with smartphones [6]. In this work, they demonstrate transmission bit rate of up to 50bps over the human body using electromagnetic signals, which is insufficient for per-touch authentication.

Per-touch authentication. Different wearable devices were proposed to augment the user's touch with its ID. Bioamp [9] is a wristband augmented with electrodes in contact with user's skin, and powered by a high-frequency signal source. The signal is then modulated onto the user's body through the skin and transmitted to the user'sfi nger. When the person touches the touch screen, the signal affects the capacitive measurement, and allow the device to decode the modulated information. However, the bit rate is low (up to 12bps), limiting its use for per-touch authentication. IR-Ring [46] is a ring-like device that continuously transmits the user's ID code in the form of infrared light pulses to a touch device. This helps the touch device associate all touch events inside the region surrounding the point where the infrared light points to. However, this technique still relies on the touch sensing capability of the device for the association, so it cannot be extended to everyday objects. VibRing [47] is also a ring-like device equipped with a vibration motor, which is used to transmit vibration patterns to a touchscreen when thefi nger wearing the ring is in contact with the touchscreen. Since relying on a mechanical vibrator, the ring can only modulate up to 20Hz frequency, significantly limiting the bit rate of the channel. A vibratory ring is also mentioned as an application of Ripple [16], which claims to be able to achieve 7.41kbps of throughput. However, power consumption was not investigated in the paper.

9 CONCLUSION

In this paper, we propose a body-guided communication method for securing every touch interaction from users with a variety of devices and objects. Through prototype touch-token measurements, we showed that the body-guided channel established during every single touch is more secure against eavesdropping than other wireless communication technologies, that is the signal received at the intended receiver is at least 20dB higher than that received at an adversary's receiver in proximity. It can achieve this at low-power consumption of 3.9μJ/bit in an unoptimized prototype, with potential to reach 90nJ/bit. Our current prototype for per-touch authentication is robust enough to reliably deliver a 128-bit ID code on every touch longer than 300ms. We believe this touch token design will provide secure while convenient authentication mechanism for users when interacting with a growing number of devices.

ACKNOWLEDGEMENTS

We thank the anonymous shepherd and the anonymous reviewers for their insightful comments. This material is based upon work supported by the National Science Foundation under Grant No CNS-1618019 and CNS-1619392.

REFERENCES

[1] Amazon dash button. https://www.amazon.com/ddb/learn-more.

[2] Chad Brubaker, Suman Jana, Baishakhi Ray, Sarfraz Khurshid, and Vitaly Shmatikov. Using frankencerts for automated adversarial testing of certificate validation in ssl/tls implementations. In *Proceedings of the 2014 IEEE Symposium on Security and Privacy*, SP '14, pages 114–129, Washington, DC, USA, 2014. IEEE Computer Society.

[3] Roel Verdult, Flavio D. Garcia, and Baris Ege. Dismantling megamos crypto: Wirelessly lockpicking a vehicle immobilizer. In *Supplement to the Proceedings of 22nd USENIX Security Symposium (Supplement to USENIX Security 15)*, pages 703–718, Washington, D.C., 2015. USENIX Association.

[4] Aurélien Francillon, Boris Danev, and Srdjan Capkun. Relay attacks on passive keyless entry and start systems in modern cars. In *Network and Distributed System Security Symposium (NDSS) (to appear)*, 2011.

[5] Tam Vu, Akash Baid, Simon Gao, Marco Gruteser, Richard Howard, Janne Lindqvist, Predrag Spasojevic, and Jeffrey Walling. Distinguishing users with capacitive touch communication. In *Proceedings of the 18th Annual International Conference on Mobile Computing and Networking*, Mobicom '12, pages 197–208, New York, NY, USA, 2012. ACM.

[6] 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*, UbiComp '16, pages 1100–1111, New York, NY, USA, 2016. ACM.

[7] Chouchang Jack Yang and Alanson P. Sample. Em-comm: Touch-based communication via modulated electromagnetic emissions. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.*, 1(3):118:1–118:24, September 2017.

[8] S. j. Song, S. J. Lee, N. Cho, and H. j. Yoo. Low power wearable audio player using human body communications. In *2006 10th IEEE International Symposium on Wearable Computers*, pages 125–126, Oct 2006.

[9] 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*, UIST '15, pages 303–312, New York, NY, USA, 2015. ACM.

[10] Kurt Partridge, Bradley Dahlquist, Alireza Veiseh, Annie Cain, Ann Foreman, Joseph Goldberg, and Gaetano Borriello. Empirical measurements of intrabody communication performance under varied physical configurations. In *Proceedings of the 14th annual ACM symposium on User interface software and technology*, pages 183–190. ACM, 2001.

[11] Y. Zou, J. Zhu, X. Wang, and L. Hanzo. A survey on wireless security: Technical challenges, recent advances, and future trends. *Proceedings of the IEEE*, 104(9):1727–1765, Sept 2016.

[12] Comparing Low-Power Wireless Technologies. https://goo.gl/sYPVzM.

[13] M. Ghamari, H. Arora, R. S. Sherratt, and W. Harwin. Comparison of low-power wireless communication technologies for wearable health-monitoring applications. In *2015 International Conference on Computer, Communications, and Control Technology (I4CT)*, pages 1–6, 2015.

[14] Antenna Circuit Design for RFID Applications. http://ww1.microchip.com/downloads/en/AppNotes/00710c.pdf.

[15] Thomas P. Diakos. Eavesdropping near-field contactless payments: a quantitative analysis. *The Journal of Engineering*, 2013:48–54(6), October 2013.

[16] Nirupam Roy and Romit Roy Choudhury. Ripple II: Faster communication through physical vibration. In *13th USENIX Symposium on Networked Systems Design and Implementation (NSDI 16)*, pages 671–684, Santa Clara, CA, 2016. USENIX Association.

[17] Joshua Adkins, Genevieve Flaspohler, and Prabal Dutta. Ving: Bootstrapping the desktop area network with a vibratory ping. In *Proceedings of the 2Nd International Workshop on Hot Topics in Wireless*, HotWireless '15, pages 21–25, New York, NY, USA, 2015. ACM.

[18] LRA. goo.gl/sBYDLH.

[19] Microchip BodyCom Technology. http://ww1.microchip.com/downloads/en/DeviceDoc/30685a.pdf.

[20] M. D. Pereira, G. A. Alvarez-Botero, and F. Rangel de Sousa. Characterization and modeling of the capacitive hbc channel. *IEEE Transactions on Instrumentation and Measurement*, 64(10):2626–2635, Oct 2015.

[21] J. Bae and H. J. Yoo. The effects of electrode configuration on body channel communication based on analysis of vertical and horizontal electric dipoles. *IEEE Transactions on Microwave Theory and Techniques*, 63(4):1409–1420, April 2015.

[22] M. Seyedi, B. Kibret, D. T. H. Lai, and M. Faulkner. A survey on intrabody communications for body area network applications. *IEEE Transactions on Biomedical Engineering*, 60(8):2067–2079, Aug 2013.

[23] B. Kibret, M. Seyedi, D. T. H. Lai, and M. Faulkner. Investigation of galvanic-coupled intrabody communication using the human body circuit model. *IEEE Journal of Biomedical and Health Informatics*, 18(4):1196–1206, July 2014.

[24] M. Seyedi, B. Kibret, D. T. H. Lai, and M. Faulkner. A survey on intrabody communications for body area network applications. *IEEE Transactions on Biomedical Engineering*, 60(8):2067–2079, Aug 2013.

[25] M. A. Callejon, D. Naranjo-Hernandez, J. Reina-Tosina, and L. M. Roa. A comprehensive study into intrabody communication measurements. *IEEE Transactions on Instrumentation and Measurement*, 62(9):2446–2455, Sept 2013.

[26] Thomas G Zimmerman, Joshua R Smith, Joseph A Paradiso, David Allport, and Neil Gershenfeld. Applying electrici eld sensing to human-computer interfaces. In *Proceedings of the SIGCHI conference on Human factors in computing systems*, pages 280–287. ACM Press/Addison-Wesley Publishing Co., 1995.

[27] T. G. Zimmerman. Personal area networks: Near-field intrabody communication. *IBM Systems Journal*, 35(3.4):609–617, 1996.

[28] Fundamentals of Electrostatic Discharge. https://goo.gl/y5UEwG.

[29] Time-Based One-Time Password Algorithm. https://tools.ietf.org/html/rfc6238.

[30] S. Golomb and R. Scholtz. Generalized barker sequences. *IEEE Transactions on Information Theory*, 11(4):533–537, October 1965.

[31] Teensy 3.2 board. https://goo.gl/Qt5tYt.

[32] INA332. http://www.ti.com/product/INA332.

[33] AD835. http://www.analog.com/en/products/linear-products/analog-multipliers-dividers/ad835.html.

[34] Analog Discovery 2. https://goo.gl/sbfwSw.

[35] LT1563. http://www.linear.com/product/LTC1563.

[36] MSP432 Launchpad. https://goo.gl/vucGRm.

[37] Hoang Truong, Phuc Nguyen, Viet Nguyen, Mohamed Ibrahim, Richard Howard, Marco Gruteser, and Tam Vu. Through-body capacitive touch communication. In *Proceedings of the 9th ACM Workshop on Wireless of the Students, by the Students, and for the Students*, S3 '17, pages 7–9, New York, NY, USA, 2017. ACM.

[38] Hoang Truong, Phuc Nguyen, Anh Nguyen, Nam Bui, and Tam Vu. Capacitive sensing 3d-printed wristband for enriched hand gesture recognition. In *Proceedings of the 2017 Workshop on Wearable Systems and Applications*, WearSys '17, pages 11–15, New York, NY, USA, 2017. ACM.

[39] Amazon IoT button. https://aws.amazon.com/iotbutton/.

[40] MSP430G2553. http://www.ti.com/product/MSP430G2553.

[41] Florian Schaub, Ruben Deyhle, and Michael Weber. Password entry usability and shoulder surfing susceptibility on different smartphone platforms. In *Proceedings of the 11th International Conference on Mobile and Ubiquitous Multimedia*, MUM '12, pages 13:1–13:10, New York, NY,

USA, 2012. ACM.

[42] Adam J. Aviv, Katherine Gibson, Evan Mossop, Matt Blaze, and Jonathan M. Smith. Smudge attacks on smartphone touch screens. In *Proceedings of the 4th USENIX Conference on Offensive Technologies*, WOOT'10, pages 1–7, Berkeley, CA, USA, 2010. USENIX Association.

[43] Phuc Nguyen, Ufuk Muncuk, Ashwin Ashok, Kaushik R. Chowdhury, Marco Gruteser, and Tam Vu. Battery-free identification token for touch sensing devices. In *Proceedings of the 14th ACM Conference on Embedded Network Sensor Systems CD-ROM*, SenSys '16, pages 109–122, New York, NY, USA, 2016. ACM.

[44] Alexander De Luca, Alina Hang, Emanuel von Zezschwitz, and Heinrich Hussmann. I feel like i'm taking selfies all day!: Towards understanding biometric authentication on smartphones. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, CHI '15, pages 1411–1414, New York, NY, USA, 2015. ACM.

[45] Apple face security. https://goo.gl/XvP2Wu.

[46] Volker Roth, Philipp Schmidt, and Benjamin Güldenring. The ir ring: Authenticating users' touches on a multi-touch display. In *Proceedings of the 23Nd Annual ACM Symposium on User Interface Software and Technology*, UIST '10, pages 259–262, New York, NY, USA, 2010. ACM.

[47] Andrea Bianchi and Seungwoo Je. Disambiguating touch with a smartring. In *Proceedings of the 8th Augmented Human International Conference*, AH '17, pages 27:1–27:5, New York, NY, USA, 2017. ACM.