Bit Whisperer: Enabling Ad-hoc, Short-range, Walk-Up-and-Share Data Transmissions via Surface-restricted Acoustics

Youngwook Do*
Georgia Institute of Technology
School of Interactive Computing
Atlanta, GA, USA
youngwookdo@gatech.edu

Siddhant Singh*
Georgia Institute of Technology
School of Computer Science
Atlanta, GA, USA
siddhantsingh@gatech.edu

Zhouyu Li
Georgia Institute of Technology
School of Electrical and Computer Engineering
Atlanta, GA, USA
lizhouyu@gatech.edu

Steven R. Craig
Georgia Institute of Technology
George W. Woodruff School of Mechanical Engineering
Atlanta, GA, USA
scraig32@gatech.edu

Phoebe J. Welch
Georgia Institute of Technology
George W. Woodruff School of Mechanical Engineering
Atlanta, GA, USA
pwelch8@gatech.edu

Chengzhi Shi
Georgia Institute of Technology
George W. Woodruff School of Mechanical Engineering
Atlanta, GA, USA
chengzhi.shi@gatech.edu

Thad Starner
Georgia Institute of Technology
School of Interactive Computing
Atlanta, GA, USA
thad@gatech.edu

Gregory D. Abowd
Georgia Institute of Technology
School of Interactive Computing
Atlanta, GA, USA
Northeastern University
College of Engineering
Boston, MA, USA
g.abowd@northeastern.edu

Sauvik Das
Georgia Institute of Technology
School of Interactive Computing
Atlanta, GA, USA
sauvik@gatech.edu

ABSTRACT

Bluetooth requires device pairing to ensure security in data transmission, encumbering a number of ad-hoc, transactional interactions that require both ease-of-use and "good enough" security: e.g., sharing contact information or secure links to people nearby. We introduce Bit Whisperer, an ad-hoc short-range wireless communication system that enables "walk up and share" data transmissions with "good enough" security. Bit Whisperer transmits data to proximate devices co-located on a solid surface through high frequency, inaudible acoustic signals. The physical surface has two benefits: it enhances acoustic signal transmission by reflecting sound waves as they propagate; and, it makes the domain of communication visible, helping users identify exactly with whom they are sharing data without prior pairing. Through a series of technical evaluations, we demonstrate that Bit Whisperer is robust for common use-cases and secure against likely threats. We also implement three example applications to demonstrate the utility of Whisperer: 1-to-1 local contact sharing, 1-to-N private link sharing to open a secure group chat, and 1-to-N local device authentication.

*Both authors contributed equally to this research.

UIST '21, October 10–14, 2021, Virtual Event, USA

ACM ISBN 978-1-4503-8635-7/21/10…$15.00
https://doi.org/10.1145/3472749.3477980

CCS CONCEPTS

• **Security and privacy** → **Usability in security and privacy**; • **Human-centered computing** → *Sound-based input / output*.

KEYWORDS

ad-hoc connections, acoustic data transmission, usable security and privacy

ACM Reference Format:
Youngwook Do, Siddhant Singh, Zhouyu Li, Steven R. Craig, Phoebe J. Welch, Chengzhi Shi, Thad Starner, Gregory D. Abowd, and Sauvik Das. 2021. Bit Whisperer: Enabling Ad-hoc, Short-range, Walk-Up-and-Share Data Transmissions via Surface-restricted Acoustics. In *The 34th Annual ACM Symposium on User Interface Software and Technology (UIST '21), October 10–14, 2021, Virtual Event, USA.* ACM, New York, NY, USA, 13 pages. https://doi.org/10.1145/3472749.3477980

1 INTRODUCTION

When Alice wants to share a secret with nearby friends in the physical world, she makes sure no one else is around, leans in, and whispers. But how might Alice share a *digital* secret with nearby friends?

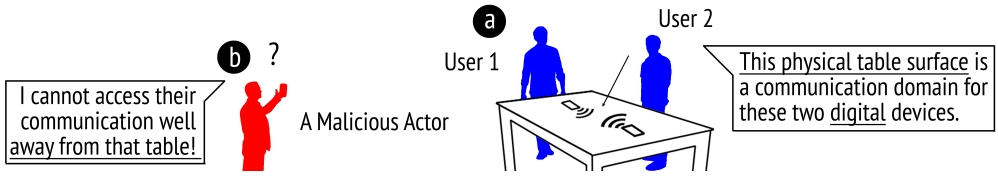

Figure 1: Bit Whisperer is an ad-hoc short-range wireless digital communication that uses a flat and rigid physical surface as a communication domain. This domain allows (a) only devices that are placed on the physical media surface to communicate with each other and (b) does not allow devices that are not placed on the surface to communicate.

Existing solutions for secure, short-range wireless communication require device pairing (e.g., Bluetooth) or specialized hardware (e.g., NFC), which can be inconvenient for a number of everyday sharing tasks that require both ease-of-use and "good enough" security: e.g., sharing contact information with fellow conference attendees, secure link sharing in a coffee-shop meeting, and authenticating into shared devices and resources. In addition, owing to the invisibility and abstractness of wireless data transfer protocols like Bluetooth, prior work suggests that end-users have trouble knowing with whom they are communicating, which, in turn, causes usable security challenges in their use [14, 16, 17, 22]. To illustrate these challenges, consider a scenario where Alice wants to share a link to a private pitch deck with Bob, Carol and David, who she met at a professional conference. One option is for everyone to share contact information and for Alice to send an email — but the process of obtaining this contact information can be cumbersome. Another option is to use short-range, wireless data sharing. To do so, Alice needs to check if her device is paired with others' one-by-one before sharing her secure link. Moreover, even after device pairing, there is no easy way for Alice to discern, with confidence, who among other nearby conference attendees might potentially eavesdrop on the sharing of her link to Bob, Carol and David [3, 11]. Indeed, there may be multiple Davids in attendance who have a device with the name "David's phone"; or, perhaps an Eve who opportunistically changes her device name to "David's phone."

We introduce Bit Whisperer, a new form of ad-hoc, short-range, wireless communication that enables "digital whispering" — wireless data transfer that is physically constrained to nearby devices co-located on a solid surface (e.g., tables) via low-amplitude, high-frequency acoustic signals.

The key insight of Bit Whisperer is that if we can enable "walk-up-and-share" (e.g., simple and ad-hoc) interactions and limit the scope of wireless digital communication to a visible, physical medium, we should be able to solve the aforementioned usable security challenges in existing short-range digital communications by: (i) enabling ad-hoc data sharing without device pairing; (ii) improving users' ability to control with whom they are communicating; and, (iii) making it difficult for attackers to eavesdrop on short-range communications without being obvious (Figure 1). We developed Bit Whisperer as an Android application that transmits and receives acoustic signals using only hardware on existing smartphones so that it is deployable out of the box.

Note that Bit Whisperer is not meant to be a *replacement* for Bluetooth or NFC — rather, it is a complementary approach that facilitates "walk-up-and-share" data transmissions between two or more physically proximate devices for lower-stakes sharing scenarios that require "good enough" security [21]: i.e., security commensurate with the level of sensitivity associated with anticipated use-cases.

To evaluate Bit Whisperer, we first conducted a number of empirical stress tests to understand its utility, speed, security, and accuracy in a controlled lab environment. Through these empirical evaluations, we found that Bit Whisperer has low transmission error when the position of a receiver device, relative to a transmitter device, more closely aligns with how legitimate users might position their devices—i.e., on the same table, with relatively low angular and vertical displacement and up to 1000mm of horizontal displacement. In contrast, when the relative position of a receiver device more closely emulates a possible adversary—i.e., off the table, with higher angular and horizontal displacement—Bit Whisperer has significantly higher transmission error. We show how this result, when used in conjunction with Reed-Solomon error correction codes, can be used for practically secure digital whispering between commodity devices closely co-located on the same physical surface.

We implemented three example applications on top of Bit Whisperer to demonstrate its practical utility: (i) a contact sharing application between two users; (ii) a secret group chat link sharing application among a group of two or more users; and, (iii) a federated authentication application where an authenticated device unlocks others on the same surface.

Concretely, in this paper, we offer the following research contributions:

- We designed and implemented Bit Whisperer, an ad-hoc, secure short-distance wireless communication system. It uses low-amplitude, high-frequency acoustic signals to enable digital "whispering" between devices co-located on a solid, flat surface.
- We systematically evaluated the Bit Whisperer communication protocol to assess its accuracy, robustness and security.
- We implemented three exemplar applications to demonstrate practical use-cases for Bit Whisperer.

2 BACKGROUND AND RELATED WORK

2.1 Usable Security Challenges of Wireless Communication Protocols

Existing short-range wireless communication technologies pose both usability and security challenges for end-users. Indeed, Chong et al. found that if a user needs to go through complex and troublesome steps to establish communication between devices, they might lose interest and give up [3]. Moreover, owing to the invisibility and

abstraction of a wireless data "connection" between paired devices, users have trouble noticing when their data transfer is interrupted by, interfered with, or intercepted by a third party [ibid]. Consider, for example, that while QR codes allow for quick, unpaired communication between many devices, the domain of communication is unclear: indeed, prior work suggests that QR codes can be covertly scanned from several meters away with a commodity smartphone device's camera [1].

We hypothesize that by implementing pairless wireless communication for which the domain of communication is clearly visible — e.g., constrained to devices co-located on a table surface — we can address both the usability and security challenges outlined above.

2.2 Data transmission Using Sound or Vibration Propagation via Physical Contact

A variety of data transmission techniques that utilize direct physical contact for acoustic and vibration signals to propagate have been proposed in various fields including Human-Computer Interaction. Researchers have studied physical-vibration-based data communication that utilizes direct contact between communication devices [10, 12, 19, 20, 29], and that utilizes direct contact between devices along with a physical media channel [7]. In addition, prior work has also explored the use of acoustic signal propagation for transmitting data through human body, though this approach requires specialized hardware [31, 32].

Our work focuses on acoustic signal propagation on a physical medium between commodity smartphone devices that requires no specialized hardware. Specifically, our approach leverages the property that a receiver device receives acoustic signals differently depending on whether or not it is in direct contact with the same physical medium as the transmitting device, which negates the need for direct contact between the communication devices themselves.

2.3 Acoustic-or-Vibration-based Usable Security System

Acoustic and vibration signal forms have been explored, in prior work, to create usable and secure authentication, communication, and counter surveillance systems. For example, researchers have proposed novel approaches that utilize acoustic signals to demonstrate two-factor authentication systems by measuring proximity between two devices [5] and by matching ambient sound received from two devices [9]. Das et al. introduce a novel method of local authentication via shared secret knocks on a user's smart device [4]. Beat-PIN applies a similar rhythm analysis technique to implement an authentication system [6]. SilentKey proposes an authentication system that reads mouth motions by analyzing the reflected ultrasonic signals generated by a commodity smartphone [24]. Dhwani demonstrates secure acoustic-based communication by leveraging microphone jamming techniques to thwart eavesdropping attacks [15]. And, Li et al. introduce an acoustic-based data encoding method by using computationally structured physical acoustic filters [13]

Building on this prior work, we implement and evaluate a novel acoustics-based communication protocol designed to enable secure, walk-up-and-share communications between proximate devices co-located on the same physical surface.

3 THREAT MODEL

Concretely, our threat model is an adversary who uses a commodity microphone and is at least 1000mm away from the transmitter. The adversary will also have access to the source code used for transmission, encoding and decoding. The goal of this adversary is to breach the confidentiality of data in transit between other parties, by either invisibly "sniffing" the transmitted acoustic signals or by pretending to be the intended audience for transmission through technical means (i.e., not via social engineering).

In justifying this threat model, it is worth considering the anticipated use-cases for Bit Whisperer. We envision Bit Whisperer being used for the ad-hoc transmission of small chunks of low-sensitivity private data — data that users would prefer to keep out of the public domain, but that would not constitute significant harm if sniffed or altered by sophisticated adversaries. Examples of such data might include encrypted contact information, one-time authentication keys, invitation links, and URLs to internal work memos. Note that users can choose for themselves what is and is not worth the risk based on their context—leaking one's contact information might be more precarious in some contexts than others. In general, we expect users to use Bit Whisperer in semi-public social settings (e.g., coffee shops, conferences, office buildings). Generally, then, we assume an adversary whose level of sophistication is commensurate with the "value" of the pay-off of the data they are attempting to compromise. We impose the 1000mm (just over 3 feet) minimum distance requirement because if an adversary is any closer, they will be physically obvious.

4 PRINCIPLE OF OPERATION

In short, we use high-frequency, low amplitude sounds to "whisper" data between unpaired commodity devices across a flat, solid surface. In the subsections to follow, we will discuss and justify our key design considerations.

4.1 Tethering Digital Whispers to Solid Surfaces with Commodity Devices

Repurposing everyday surfaces (e.g., tables, walls) as media for data transmission can offer two additional benefits. First, tables, walls, and other flat, solid surfaces are often present in the sort of social environments where we envision such short-range wireless communications to be useful: e.g., at coffee shops, restaurants, conferences, and office spaces. Second, by tethering a digital whisper to the proximity of a physical table, the boundaries of communication can be seen: devices on the table are privy to whispers; devices off the table are not.

Additionally, we used only commodity hardware and software for implementation to ensure that Bit Whisperer can work "out of the box" with existing Android smartphones.

4.2 Surface-restricted Acoustics

We found evidence that two physical properties of sound may be applied to design Bit Whisperer [2, 26]: (i) sound attenuates over long distances, meaning that devices that are closer are more likely to hear whispers; (ii) sound is reflected from rigid physical surfaces. Accordingly, we hypothesized that a digital whisper transmitted

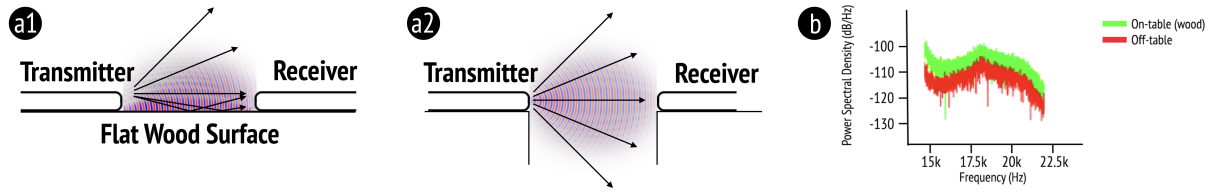

Figure 2: Bit Whisperer leverages the sound reflection. (a1) the receiver that are co-located on the flat wood surface with the transmitter can receive twice as much acoustic pressure as (a2) the receiver that are not. (b) We plot the power spectral density of the received signals of on-table and off-table setups with Google Pixel 4 for the receiver and Samsung Galaxy S8 for the transmitter.

on a solid table would be more clear and audible for devices that are physically on the same table than for devices that are not.

In order to verify this hypothesis, we ran a simulation on the COMSOL Multiphysics software simulation tool [8] evaluating how sound propagation differs above a wood table (material density of $532kg/m^3$) versus open air ($1.225kg/m^3$). We simulated two situations with a fixed distance between receiver and transmitter (1000mm): (i) a transmitter device and a receiver device that are co-located on a flat wood surface (on-table setup); (ii) a transmitter and a receiver device that are placed on separate, air-gapped surfaces (off-table setup). In both situations, we had the transmitter generate 18k-20kHz (100Hz interval) acoustic signals and we measured the acoustic pressure—acoustic signal in time domain (Pa)—that the receiver received. As shown in Figure 2 (a), we found that the on-table receiver received twice as much acoustic pressure as the air-gapped receiver — partially due to the fact that sound is reflected back when it travels above the wood surface instead of being dispersed into the air. [1]

We next empirically verified the simulated tests. We used a transmitter device (Galaxy S8) to play white noise for 10 seconds and a receiver device (Google Pixel 4) to record the noise. We placed the devices 1000mm apart from each device in two different conditions: (i) each device is placed on different, air-gapped tables at the same height (See Figure 3(a)); (ii) both devices are co-located on the same wood surface table (See Figure 3(b)). As the power spectral density (Pa^2/Hz) of two conditions shows in Figure 2 (b), we found that the on-table receiver receives a signal around 7-9dB/Hz higher than the off-table receiver over the 18kHz - 22kHz range. [2]

In short, controlling for distance, surface-restricted acoustics are more robust than acoustics propagated in the open air. This difference is the key design principle that allows BitWhisperer to work: as we will show, using this difference along with Reed-Solomon error correction and encryption, we can design a communication protocol that requires no device pairing, but works robustly *for* proximate devices co-located on a flat, solid surface and securely *against* air-gapped adversaries.

5 IMPLEMENTATION

First, we tested all the 100Hz-wide frequency channels in the 18kHz - 20kHz range to examine which frequency channels would be usable — i.e., robust for acoustic data transmission over flat surfaces. Then, we ran characterization tests across a range of parameters (e.g., horizontal displacement, angular displacement, vertical displacement between transmitter and receiver devices, three different receiver device models, three types of table surface material, levels of environmental noise) to understand how variations in each parameter might affect acoustic data transmission. Through these tests, we learned there are three characteristics that play important roles in surface-restricted acoustic data transmission: (i) distance between a transmitter and a receiver; (ii) angular displacement between the transmitter's speaker and a receiver's microphone; and (iii) whether or not the transmitter and the receiver are co-located on the same rigid surface. Finally, we applied the Reed-Solomon Error Correction [18] algorithm with an empirically established error threshold to encode acoustic data transmissions so that legitimate receivers can receive lossless communication while inhibiting adversarial receivers from receiving meaningful data. This final step allowed us to leverage the signal strength differences between likely legitimate receivers (i.e., on-table, within 1000mm and with low angular displacement) and adversarial receivers (i.e., off-table, farther away, and with higher angular displacement) to construct a robust and secure form of short-range, wireless data transmission with no need for prior device pairing: i.e., "walk up and share without a care."

5.1 Acoustic Signal Frequency Range Selection

In selecting an acoustic frequency range for data transmission, we were primarily interested in three properties: deployability, robustness, and unobtrusiveness. For deployability, we drew inspiration from Han et al.'s prior work which found that acoustic signals between 18kHz and 20kHz are minimally affected by environmental noise, and can be generated by commodity devices [5, 33]. For robustness, as we found from our preliminary white noise tests, flat surfaces can increase acoustic signal strength above the 18kHz range. For unobtrusiveness, frequencies above 18kHz are generally inaudible or minimally perceptible [25] by humans. Thus, the 18k–20kHz range satisfied all three properties.

5.2 Data Communication via Frequency-shift keying (FSK)

Data communication channel. With an acoustic range selected, our next step was to implement a communication protocol through which a pair of devices can communicate. We drew inspiration from prior work, adopting the basic system structure employed in Proximity-Proof [5]. Similar to Proximity-Proof, we evaluated 20 frequency channels from 18kHz to 19.9kHz with 100 Hz intervals between adjacent frequency channels. The 100Hz interval was

[1] We provide the simulation results in our supplementary materials.
[2] We ran the white noise tests with the different volume levels of white noise. We provide their frequency response results in our supplementary materials.

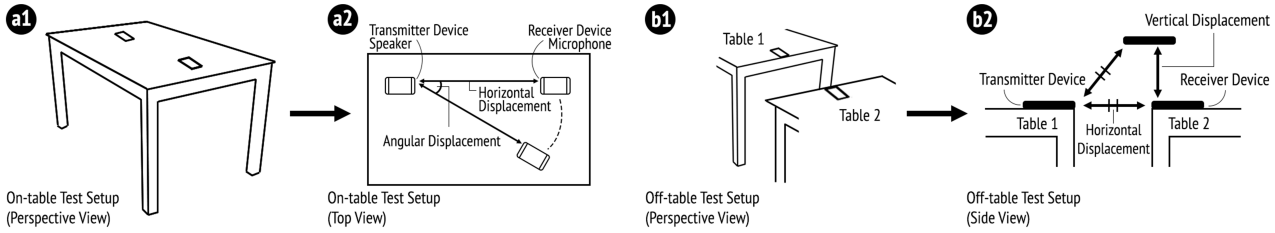

Figure 3: Experiment apparatus for on-table and off-table tests: (a1) a transmitter and a receiver device are placed on the same physical table surface; (a2) We measured the power spectral density of the signal received by a receiver with two parameters: horizontal displacement between two devices and angular displacement between a Tx device and a Rx device; (b1) a Tx device and a Rx device are placed on different physical table surfaces on the edge; (b2) We examined the power spectral density of the signal received by a receiver with three parameters : horizontal displacement, angular displacement, and vertical displacement between two devices.

determined empirically from preliminary tests: it was the interval at which cross-talk between adjacent channels was minimal. Then, we chose the eight channels that would be best suited for Bit Whisperer, which will be discussed in the following section. We call these 8 frequency channels the "data transmission channels".

Inspired by prior work [30, 31], we also employed frequency-shift keying to transfer binary data: i.e., we assigned another shifted frequency to each frequency channel. The shifted frequency is 50Hz higher than each frequency channel. If the shifted frequency's amplitude is over or below the amplitude of its corresponding original frequency, the system decodes the information as binary bit 1 or 0, respectively.

Clock signal channel. The clock signal channel is a dedicated frequency channel to indicate the beginning and the end of transmission for each data packet. We chose the frequency of the clock signal channel to be 17.5kHz. This frequency ensures a sufficiently large gap between the clock channel and data transmission channels so that the clock signals do not interfere with data transmission signals. The FSK was also used for the clock signal channel.

Flag signal channel. The flag signal indicates the start and end of transmission by utilizing on-off keying. If the amplitude of the flag channel is over or below a certain threshold value, the system decodes the information as binary bit 1 or 0, respectively. We dynamically determine the threshold value through a calibration step. In the calibration step, the receiver will record the ambient sound for 5 transmission cycles (around 0.4 seconds) right after being opened and taking the average of the recorded amplitudes for the flag signal. The threshold for the flag signal is the sum of the average ambient amplitude and a manually set parameter. We picked 17kHz as the frequency for the flag signal.

Once a receiver starts to receive signals from the transmitter, it runs a Fast Fourier Transformation (FFT) to analyze the amplitude of each frequency carrier component of the signal.

5.3 Robust, Secure communication with Forward Error Correction and Encryption

Any lossy communication channel must account for transmission error, and must do so in a manner that allows legitimate receivers to accurately recover lossy messages while preventing adversarial receivers from doing the same. We accomplish this with a combination of Forward Error Correction (FEC) and encryption.

FEC encompasses a suite of techniques in which "error correcting codes" are appended to transmitted messages that allow receiving devices to reconstruct missing or erroneous bits of a transmitted message. These error correcting codes are usually "parity symbols" (or bits), a specific set of bits calculated on the basis of the rest of the message that are transmitted alongside the message. They work such that in combination with a certain number of un-corrupted bits they can serve as sufficient error correcting information to reconstruct the rest of the erroneous data on the Rx side of a noisy communication medium. FEC is widely used in communication protocols such as the Universal Datagram Protocol (UDP) and in video broadcast transmissions where re-transmission of the data and receipt acknowledgment is not possible or create large overheads [28]. In particular, we implemented the Reed-Solomon FEC scheme to develop practically secure communication with Bit Whisperer [18, 23]. One key benefit of the Reed-Solomon algorithm is that there is a tunable error "cliff" below which a message is recoverable, and above which it is not. We set this "cliff" empirically based on our tests (as described in the next section).

An astute reader may note that it is not necessary for an adversary device to detect and correct all errors: even if the intercepted message is 70% accurate (e.g, Jxxn Dxe instead of John Doe), that may be good enough for many adversarial purposes. We address this by first transmitting a 128-bit AES encryption key [27] and encrypting future correspondences with that key. This way, if the adversary receives even one erroneous bit of the ciphertext (the encrypted raw data), they will not be able to recover any of the plaintext (the decrypted raw data). For stronger security, users may use a larger AES key (at the expense of speed).

5.4 Receiver and Transmitter Setup

We developed two separate Android apps for receiver and transmitter devices. We installed these apps on four Android smartphone devices (S8, S10, Pixel 4, and V35): S8 as the transmitter, and the others as receivers. We only used one transmitter because we expect data transmission to be broadly the same, which could be possible by tuning amplitudes for each sound frequency even if devices have variable speakers. We set the transmitter's volume to 40 percent of the device's maximum volume, a value that we empirically determined was best for data transmission. We set the audio sampling rate as 48000Hz and used a buffer size of 4096. We

configured the transmitter to transmit, and the receiver to receive, a block of data every 150ms (the fastest rate that we empirically found shows the robust communication quality). The transmitter system converts the data into arrays of 20 bits. After the conversion, the system assigns the bits to 20 data transmission channels. For each bitstream transmission, the transmitter acoustically transmits the bitstream for 150ms. Then, once the receiver receives the signals, it analyzes frequency response via FFT and checks which bit is received by each channel. Then, it reconstructs an array of subsequent collections of 20 bits accordingly.

6 SYSTEM EVALUATION

Ultimately, we show that Bit Whisperer can be used to transmit wireless messages to unpaired devices that are within 500mm of one another and co-located on the same flat, solid surface with an accuracy between 80%-98% (depending on the receiver device). For devices within 1000mm, we observed an accuracy between 75%-89%. Conversely, we show that the success rate for the air-gapped adversaries we tested was between 8% and 10%. Moreover, the adversary we tested represented a "best-case" upper bound: exactly 1000mm away, at the exact height of the transmitter, and only 60 degrees displaced from the transmitter's microphone. In practice, it would be hard for any adversary to be able to replicate these conditions without being obvious. In the text to follow, we describe a progression of tests we followed to achieve these results.

In evaluating Bit Whisperer, we focused on answering two high-level questions: (i) How robust and accurate is data transmission under Bit Whisperer for legitimate use cases? (ii) How secure is Bit Whisperer against nearby eavesdroppers?

To answer these questions, we conducted a series of robustness and threat evaluations in a controlled lab environment. Specifically, we conducted 4-stage evaluations where we expected to find high disparity in transmission accuracy between legitimate receivers (on table) and adversarial receivers (off table). First, we evaluated bit error rate (BER)—the number of bits accurately transferred from transmitter to receiver—to find the eight data-transmission frequency channels that show the highest disparity between on and off table setups. We present BER values for each of the twenty data-transmission frequency channels we assessed. Second, we evaluated character error rate (CER), the number of 8-bit ASCII characters accurately transferred from transmitter to receiver. To assess CER, we used the eight frequency channels that offered the highest BER disparity between legitimate and adversarial receivers. We view CER as a more functional unit of measure, as even low BERs can accumulate into significant cumulative losses over larger data transmissions. Third, in a more functional test that more closely emulates real-world use, we tested the relative rate of success for transmitting a 128-bit AES encryption key, encoded with Reed-Solomon error correction, for both adversarial and legitimate receivers

In a controlled lab environment, we tested the accuracy of data transmission between a transmitter and receiver device across six parameters: (1) one transmitter model and three receiver models (legitimate users and adversaries may have different receiver models), (2) on table (legitimate users)—wood, plastic, and glass surfaces—vs. off table (adversaries); (3) horizontal displacement (legitimate users should be close, adversaries should be farther); (4) angular displacement (legitimate users should be more head-on, adversaries off-center); (5) vertical displacement (legitimate users should be on the same vertical plane, adversaries may be lower or higher); and (6) noise levels (See Figure 3).

We ran our tests in a controlled, quiet space (Ambient noise sound level: 42.3-43.2dB). We conducted our tests on three flat, rigid table surface types– wood, plastic, glass. We removed all items on the table surface except for the testing devices.

6.1 Bit Error Rate Test

We first measured bit error rate (BER) — the average number of bits, per 100, incorrectly transmitted from transmitter (Tx) to receiver (Rx) — to determine which frequency channels were most effective for transmitting acoustic signals to proximate, on-table devices (legitimate users) but not to distant, off-table devices (adversaries).

Our goal in testing BER was to select the most promising frequency channels with which to later conduct a more thorough character error rate test — i.e., the average number of 8-bit characters, per 100, incorrectly transmitted from Tx to Rx. Accordingly, for our BER evaluation, we focused on the effects of horizontal displacement and whether or not a Rx device was on or off the table. High angular and vertical displacement, while important factors to evaluate, should represent less favorable conditions for adversaries as legitimate users are more likely to have low-to-no angular and vertical displacement. Accordingly, we left the evaluation of those dimensions to our character error rate tests.

Test Setup. We ran three test sessions. For each session, we varied the relative position of the Rx device to the Tx device along a dimension — on-table (Plastic) vs off-table— with the fixed horizontal displacement (1000mm). For this test, we used a Galaxy S8 as the Tx device and S10, Pixel 4, and V35 as the Rx devices. Thus, in total, we ran $3 * 2 * 3 = 18$ distinct BER tests. For each one of these tests, the Tx device sent 1000 bits for each channel. All data was transmitted at the 40 percent volume level that we empirically determined was ideal for data transmission from our prior preliminary volume tests.

As noted in our threat model, we considered horizontal displacements under 1000mm to be "safe" distances that adversaries would have trouble broaching without being obvious. In contrast, we consider any device more than 1000mm away to be adversarial.

Results. We show results for each frequency channel in Table 1 over three Rx devices. We averaged the BER for each channel across the Rx devices to take into account frequency channels that are suited for various receiver devices. Then, based on the averaged BER, we selected the eight frequency channels that showed the highest disparity between on-table (legitimate) and off-table (adversarial) receivers to proceed with to our CER test—18kHz, 18.1kHz, 18.3kHz, 18.4kHz, 18.5kHz, 18.8kHz, 19.2kHz, and 19.7kHz.

6.2 Character Error Rate Test

For the character error rate (CER) tests, we transmitted 8-bit symbols from 00000001_2 to 01011111_2 corresponding to the 95 non-control ASCII-characters from the space character to the tilde character. The 8-bits were transmitted simultaneously through each of the eight channels — one per bit — that demonstrated the largest BER difference between on-table and off-table tests (see Table 1)

LG V35	Frequency (kHz)	18	18.1	18.2	18.3	18.4	18.5	18.6	18.7	18.8	18.9	19	19.1	19.2	19.3	19.4	19.5	19.6	19.7	19.8	19.9
BER (%)	Off table	1.67	1.00	0.57	1.70	2.07	1.70	1.20	1.27	1.90	0.57	0.67	1.27	1.67	0.57	0.87	0.27	0.37	0.73	0.57	0.40
	Plastic	0.30	0.43	0.80	0.23	0.40	0.30	0.63	0.30	0.20	0.27	0.23	0.23	0.33	0.43	0.27	0.53	0.37	0.30	0.17	0.73
BER Difference (Off table - Plastic)		1.37	0.57	-0.23	1.47	1.67	1.4	0.57	0.97	1.7	0.3	0.43	1.03	1.33	0.13	0.6	-0.27	0	0.43	0.4	-0.33
S10	Frequency (kHz)	18	18.1	18.2	18.3	18.4	18.5	18.6	18.7	18.8	18.9	19	19.1	19.2	19.3	19.4	19.5	19.6	19.7	19.8	19.9
BER (%)	Off table	0.10	0.50	0.00	0.30	0.20	0.60	0.00	0.20	0.00	0.20	0.40	0.10	0.40	0.70	0.00	0.10	0.10	0.77	0.77	0.20
	Plastic	0.13	0.10	0.23	0.03	0.20	0.07	0.10	0.03	0.37	0.03	0.13	0.77	0.37	0.10	0.37	0.17	0.07	0.17	1.10	0.33
BER Difference (Off table - Plastic)		-0.03	0.4	-0.23	0.27	0	0.53	-0.1	0.17	-0.37	0.17	0.27	-0.67	0.03	0.6	-0.37	-0.07	0.03	0.6	-0.33	-0.13
Pixel 4	Frequency (kHz)	18	18.1	18.2	18.3	18.4	18.5	18.6	18.7	18.8	18.9	19	19.1	19.2	19.3	19.4	19.5	19.6	19.7	19.8	19.9
BER (%)	Off table	1.30	0.80	0.03	0.90	0.93	0.63	0.07	0.17	0.77	0.30	0.73	0.80	0.70	0.53	0.47	0.67	0.37	1.53	0.93	0.63
	Plastic	0.53	0.13	0.20	0.20	0.10	0.07	0.23	0.33	0.27	0.43	0.13	0.07	0.23	0.43	0.13	0.23	0.13	0.37	0.30	0.40
BER Difference (Off table - Plastic)		0.77	0.67	-0.17	0.70	0.83	0.57	-0.17	-0.17	0.50	-0.13	0.60	0.73	0.47	0.10	0.33	0.43	0.23	1.17	0.63	0.23
Average of BER Differences		0.70	0.54	-0.21	0.81	0.83	0.83	0.10	0.32	0.61	0.11	0.43	0.37	0.61	0.28	0.19	0.03	0.09	0.73	0.23	-0.08

Table 1: We measured BER by running three rounds of sending 1000 bits for each channel at 1000mm distance. This table shows BER result with two parameters (on-table (plastic) vs. off-table, and three receivers—V35, S10, Pixel 4). We chose 8 frequency channels based on the highest disparity of BER between on and off table setups.

We defined CER as the number of incorrectly received characters between a Tx and Rx device per 100 — i.e., even a single incorrectly transmitted bit was coded as a character error.

We evaluated CER as a function of three positional parameters describing the relative position of a receiving device to a Tx device: horizontal displacement (500mm, 1000mm), angular displacement (0°, 30°, 60°and 90°) and vertical displacement (50mm, 100mm). For each of the horizontal and angular displacement tests, we tested both on-table vs. off-table variants. For the on-table setup, we tested with three different types of table surfaces—wood, plastic, and glass. We ran three rounds of data collection. For each round, we transmitted the aforementioned 95 ASCII characters from Tx to Rx device. For our evaluations, the Tx device transmitted each 8-bit symbol for 150ms, through 8 distinct channels, with 150ms clock signals in-between each transmission. This afforded a bit rate of 26.7bits/s (8bits/0.3s) for the CER evaluation. Transmission speed can be scaled up by using more channels and by reducing the transmission interval, but we focused first on evaluating robustness and security against likely threats. We describe the testing setup and results for each of these parameters in more detail in the following subsections.

6.2.1 Horizontal Displacement. **Test Setup.** First, we examined how the horizontal displacement between a Tx and a Rx device affected CER under "ideal" conditions — i.e., with the devices placed on the same table, with no angular displacement, and no vertical displacement. We plot the results in Figure 4.

Results. The result shows that the farther away the Rx, the higher the CER. Notably, the effect of horizontal displacement is more apparent for off-table Rx than on-table Rx. As shown in Figure 4, at 1000mm, the average CER for an on-table receiver (<2.5%) was generally lower than an off-table receiver (>4.0%). As we will discuss in more detail, it is possible to correct for a configurable threshold of data error using Reed-Solomon (RS) error correction. These results suggest that by setting the threshold to approximately 2.5%, legitimate (on-table) users will be able to reconstruct the transmitted data, while off-table adversaries will be unable to do so. Moreover, adversaries are unlikely to be under 1000mm away from a Tx device — if they were, they would be trivially detectable by the user transmitting the data.

6.2.2 Angular Displacement. **Test Setup.** For the angular displacement test, we tested two horizontal displacement setups—500mm and 1000mm—and vertical displacement at 0mm, while varying the angle between the Tx device's speaker and the Rx device's microphone along four values (0°, 30°, 60°and 90°). We also tested these parameters for both on-table—wood, plastic, and glass surfaces—and off-table Rx. We plot the results in Figure 5.

Results. As shown in Figure 5, from 0°to 90°, CER values are lower in on-table test than in off-table test in general. While for both 500mm and 1000mm horizontal displacement, the average CER of 0°and 30°angular displacement on-table setups is below 2.5%, the average CER for the on-table setup with 1000mm horizontal displacement at 60°and 90°angular displacement is above 2.5%. In addition, with 1000mm horizontal displacement, generally, the average CER of the off-table setup at 60°and 90°(V35, Pixel4 > 6.0%) is higher than the average CER of the off-table setup at 0°and 30°(V35, Pixel4 > 4.0%). This result suggests that it should be possible to fan out multiple "legitimate" on-table Rx in front of a Tx while making it more difficult for an off-table adversary to successfully carry out an eavesdropping attack without being in front of the Tx.

6.2.3 Vertical Displacement. **Test Setup.** Finally, we tested the impact on CER of vertically displacing the Tx and Rx devices by 50mm and 100mm. We fixed the horizontal and angular displacements at 1000mm and 0°, respectively. This represents a potential case where an attacker finds a table of approximately similar height and is otherwise allowed to freely position their device in favorable conditions (e.g., with no angular displacement). We plot the results in Figure 6.

Results. We found that while there is little trend between the vertical displacement and CER, the average CER values (>4.0%) at all levels of vertical displacement are lower than CER of the on-table Rx (<2.5%). In short, vertically displaced Rx devices that are at least 1000mm away are unlikely to be able to reconstruct messages

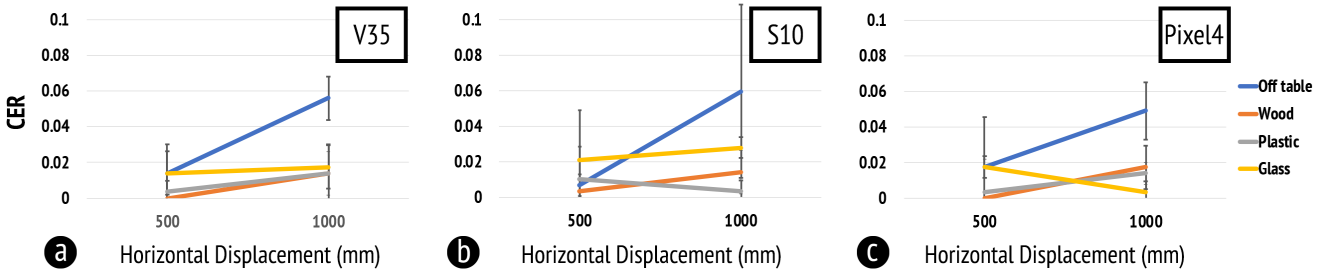

Figure 4: We measured CER with 95 non-control ASCII-characters with different horizontal displacement (500mm, 1000mm) across all the receivers: (a) V35; (b) S10; and (c) Pixel4.

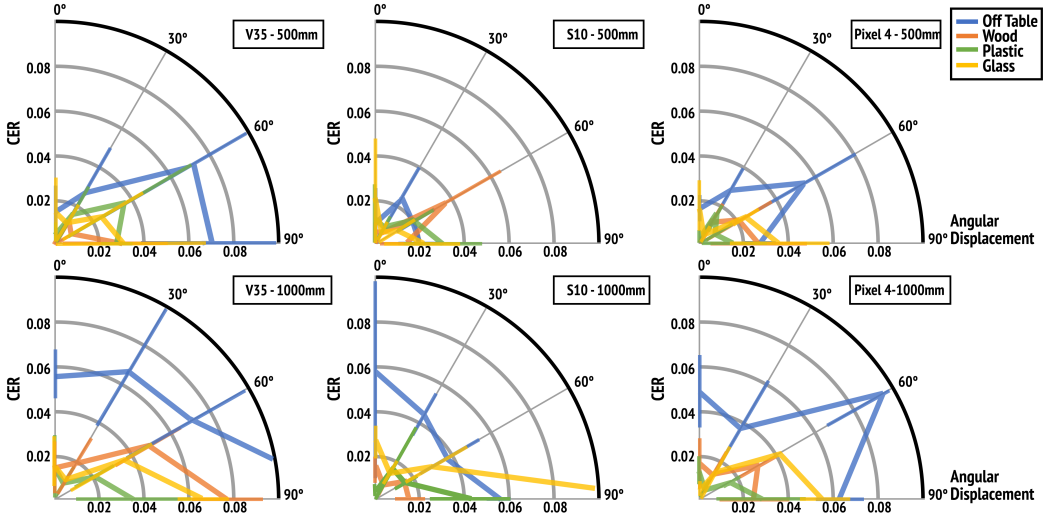

Figure 5: We measured CER with 95 non-control ASCII-characters with various angular displacement between a Tx and a Rx (0°, 30°, 60°, 90°) in two conditions: on table and off table.

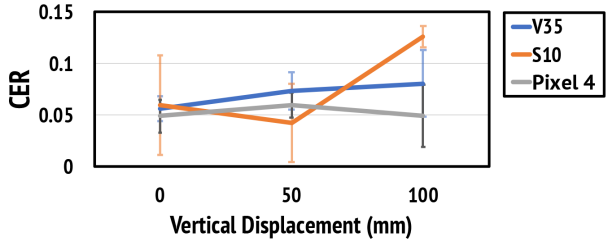

Figure 6: We measured CER with 95 non-control ASCII-characters with various vertical displacements between a Tx and a Rx (50mm, 100mm) in the off-table setup.

transmitted through Bit Whisperer, even at relatively low levels of vertical displacement and head-on.

6.2.4 Noise Tests. To evaluate if Bit Whisperer can be used in environments with ambient noise, we next evaluated the signal-to-noise ratio (SNR) and CER of acoustically transmitted data in noisy environments. Due to the ongoing COVID-19 pandemic, we were unable to conduct tests in uncontrolled environments (e.g., coffee shops, lobbies to public buildings). Instead, we used a white noise generator in a controlled environment to conduct our noise tests.

Test Setup. We placed the Tx (S8) and the Rx (S10) 1000mm apart on the same wood table. We placed another device (S8) 2.5 meters away from the Rx and played white noise at three different volume levels: 20, 40, and 60 percent of its maximum volume level. For each volume level, we ran two rounds of tests. In the first round, we recorded the sound from the Rx without any data transmission. In the second round, we recorded the sound from the Rx with transmitted data, and evaluated the CER. We derived SNR by comparing the recorded sounds from the first and second rounds.

Results. We found that CER is not significantly affected by white noise played at 20% volume, but started getting impacted by white noise played at 40 percent of the maximum volume of the device playing the white noise. Specifically, with the white noise at the 20 percent of the maximum volume, CER is 0.011 (std=0.011) while CER is 0.035 (std=0.012) with the white noise at the 40 percent of the maximum volume. Assuming a maximum allowable CER of 0.025, in terms of signal-to-noise ratio for each frequency channel, Bit Whisperer's CER is usable as long as SNR values, for each channel, are higher than: 18kHz—12.9dB/Hz, 18.1kHz—35.8dB/Hz, 18.3kHz—13.4dB/Hz, 18.4kHz—17.5dB/Hz, 18.5kHz—26.9dB/Hz, 18.8kHz—13.9dB/Hz, 19.2kHz—11.1dB/Hz.

To contextualize these values, we recorded ambient environmental noise at a local coffee shop and compared the resultant power spectral density to that of the 40% volume white noise we used in our noise tests. We found that the coffeeshop noise was 1-13 dB/Hz lower than the 40% volume white noise over the frequency channels we use in Bit Whisperer, suggesting that Bit Whisperer would function robustly in that coffeeshop (and, likely, most other day-to-day environments as well). [3]

6.3 Functional Data Transmission Test

We found that the CER is lower for configurations in which the relative positioning of the Rx device(s) more closely aligns with where a legitimate user would be as opposed to an adversary: i.e., on the same table, and with relatively low horizontal and angular displacement. Specifically, as shown in Figure 5, we found the CER to be no higher than 2.5% for legitimate use-cases (e.g., on-table, up to 1000mm or horizontal displacement and 0–30°of angular displacement) and no lower than 3.5% for adversarial use-cases (off-table, over 1000mm of horizontal displacement and 60–90°of angular displacement). To develop a reliable, secure communication protocol using Bit Whisperer, we should be able to tolerate up to 2–3.5% CER while making the protocol unusable at CER higher than 3.5%. Accordingly, we set our tunable error "cliff" for Reed-Solomon Forward Error Correction to be 3.5%. Given this tunable error "cliff", our next and final test was to assess — in practice — the robustness and security of actual data transmitted with Bit Whisperer.

Test Setup. The goal of this final test is to assess the hypothesis that Bit Whisperer can be used for robust, secure and pairless short-range wireless communication. We test this hypothesis by transmitting a 128-bit AES encryption key, and testing the success rate of data transmission for legitimate and adversarial Rx. If legitimate Rx can reliably receive or reconstruct the AES key, but adversarial Rx cannot, then all other correspondences between the Tx and legitimate Rx can be considered robust and secure.

As shown in Figure 7, we tested both an on-table (for legitimate Rx) and off-table (for adversarial Rx) set-up. For the on-table setup, we randomly assigned a legitimate Rx to be in one of 16 positions within 1000mm and between 0 and 60 degrees of angular displacement The results of the on-table setup, thus, can be considered the average / expected data transmission success rate for Rx anywhere in the "legitimate" zone. For the off-table setup, we fixed the Rx to the position that we found Bit Whisperer would work best for adversaries from our CER tests. Thus, the results of the off-table setup represents the "best" chance that an adversary might have to intercept data transmitted with Bit Whisperer. Note that this adversary is likely impractical in practice — it represents someone who is exactly a meter away, with a Rx device within line-of-sight of the Tx, and with the Tx device right at the end of the table on which it is placed. Still, it serves as a useful upper-bound for adversarial success.

We ran 100 rounds of data transmission for each setup. For the on-table test, we randomly assigned the Rx to one of the sixteen positions in the "legitimate" zone. For each test, we transmitted a 128-bit AES encryption key encoded in Base64 (6-bit data blocks with two padded 0 bits for 7th and 8th bit channels). The parity symbols derived from the RS scheme are also added to the original data stream. We used an allowable error threshold of 2% for the Reed-Solomon algorithm, which we set empirically based on our CER test results — i.e., two symbols could be corrected corrected among the 128-symbol key. Then, we evaluated data transmission success rate for each Rx device (V35, S10, Pixel4).

Results. As shown in Table 2, for the on-table setup, we observed a successful data transmission rate of 0.89, 0.86, and 0.75 across all 16 positions for the Pixel4, S10 and V35, respectively. For positions at or under 500mm in distance, we observed a successful data transmission rate of 0.98, 0.91, and 0.80 for those same devices. In contrast, for the best-case adversarial off-table setup, we observed a successful attack success rate of 0.08, 0.10, and 0.09, again for those same devices.

To contextualize these results, it is worth reiterating that Bit Whisperer is not meant to replace Bluetooth anymore than whispering in the physical world is meant to replace closed-room meetings. However, just as whispering has its uses — for sharing ad-hoc secrets with nearby people — the upshot of our results is that Bit Whisperer facilitates the ad-hoc, pairless, wireless sharing of data like contact information, or secure links to shared documents and chatrooms, or one-time-use authentication token between two or more physically proximate devices at a level of robustness and security that is "good enough" [21].

7 APPLICATIONS

Since Bit Whisperer uses only commodity hardware and software, it is deployable out-of-the-box: it can be used by existing devices that are programmable and that have a microphone and a speaker. We implemented three Android applications exemplifying the practical utility of Bit Whisperer.

7.1 1-to-1 data transfer: Contact Information Sharing

When two people first meet, they may want to exchange contact information. However, they may not want to establish a persistent Bluetooth connection between their respective devices, and systems like AirDrop may be saturated by other conference attendees. To facilitate this interaction, we built a contact sharing Android application that uses Bit Whisperer. To share contact information, two people must place their devices on a table with the microphone of the receiver facing the speaker of the transmitter. Then, the two devices can alternate between transmitting and receiving their owners' respective contact information (Figure 8(a)). Moreover, the two people who exchanged contact information can be assured that they are exchanging information with each other and only each other; no one else nearby should be able to eavesdrop on the exchange nor impersonate one of the two transactors without being physically obvious.

7.2 1-to-N Data Transfer: Decentralized End-to-End Encrypted Chat

Bit Whisperer can also be used to transmit information from one device to many others as long as they are on the same physical platform and facing each other. This property could prove useful for a range of sharing scenarios in which the individual participants do

[3] Detailed CER results from the noise test are shared in the supplementary materials.

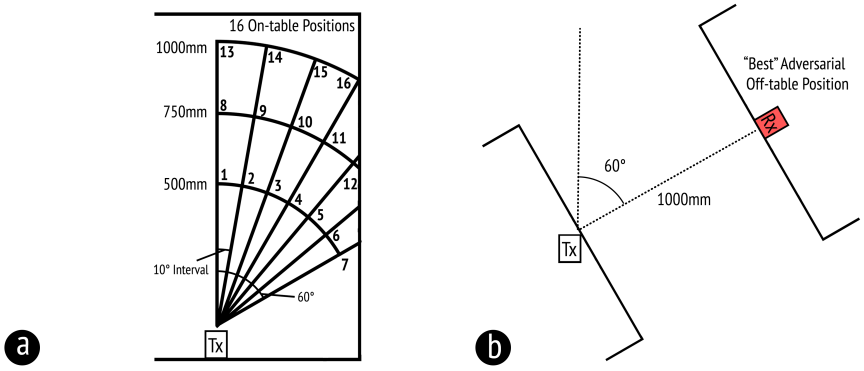

Figure 7: We could amplify the significant cumulative losses into a situation that the on-table setup can achieve lossless communication while adversarial Rx in the off table setups could not receive any meaningful data by adopting the FEC scheme to encrypted messages. We evaluated data transmission success rate for on-table and off-table setups. (a) For the on-table setup, we made the grid with 16 positions selected which replicates an arbitrary Rx placement. (b) For the off-table setup, we only tested with the "best" adversary off-table setup which the adversary could have the best chance to sniff the data, assuming that the device on the other off-table areas is less likely to able to access the data transmission than the "best" adversary position determined based on the lowest CER.

	Device	V35	S10	Pixel4	Device	V35	S10	Pixel4
Successful Data Transmission Rate	16 Position Ontable	0.75	0.86	0.89	Within 500mm	0.80	0.91	0.98
	"Best" Adversarial Offtable	0.09	0.10	0.08				

Table 2: This table shows data transmission success rate for three different setups across all the Rx devices (V35, S10, and Pixel4): (1) 16 on-table positions; (2) "best" adversary off-table position. The FEC scheme allows Bit Whisperer to achieve higher data transmission rate for on-table setups than off-table setups across all the Rx devices. Among positions at 500mm for the on-table setup, we observed 0.98, 0.91, and 0.80 successful data transmission rate for Pixel4, S10, and V35 respectively.

not want to first share their personal contact information with the group — e.g., sharing a secure link, or sharing public keys with one another to establish an end-to-end encrypted (e2ee) group chat. For example, a group of co-located individuals might want to initialize an encrypted group chat while they are physically near to continue their conversation when they split apart (Figure 8 (b)).

We built an application that allows a group of devices, placed on a table in a circular configuration with microphones and speakers facing the center of the circle, to share encrypted key information with one another in order to initiate an end-to-end encrypted group chat. We use Bit Whisperer to share public keys from one device to many others in order to start a private group chat. This facilitates secure and decentralized group chat communications, precluding the need to use a trusted third party service for key distribution or share contact information apriori.

7.3 1-to-N Data Transfer: Local Device Authentication

Bit Whisperer can also facilitate interaction between many devices owned by the same person, e.g., to serve as an authentication hub for all other devices in a workstation. At present, Bluetooth is sometimes used to simplify authentication by allowing one authenticated device to authenticate into another (e.g., Apple Watches can unlock MacBooks). Bit Whisperer can scale this interaction up: instead of requiring a series of individual device pairings, a transmitter device can broadcast an authentication request to all other devices on the same table. Doing so has little security risk: as the communication is physically constrained to the desk, there is little chance for an eavesdropper to sniff this request or for an impersonator to intercept the request unless these attackers physically place malicious devices on the user's work desk. We implemented a local authentication hub application for Android that unlocks a tablet device from a commodity Android smartphone.

Consider the case of Carl who operates a workstation with a tablet device, a desktop computer, and several other devices. Carl, coming back from lunch, places his phone on his desk. The phone, using Bit Whisperer, communicates with all of the other devices on the desk in order to automatically unlock the devices as Carl settles in (Figure 8 (c)).

8 DISCUSSION

We implemented and systemically evaluated Bit Whisperer, a system that enables digital whispering between nearby devices co-located on a flat, solid surface via low-amplitude, high-frequency acoustic signals. Bit Whisperer, as implemented, offers three concrete benefits for ad-hoc, short-range wireless digital communications.

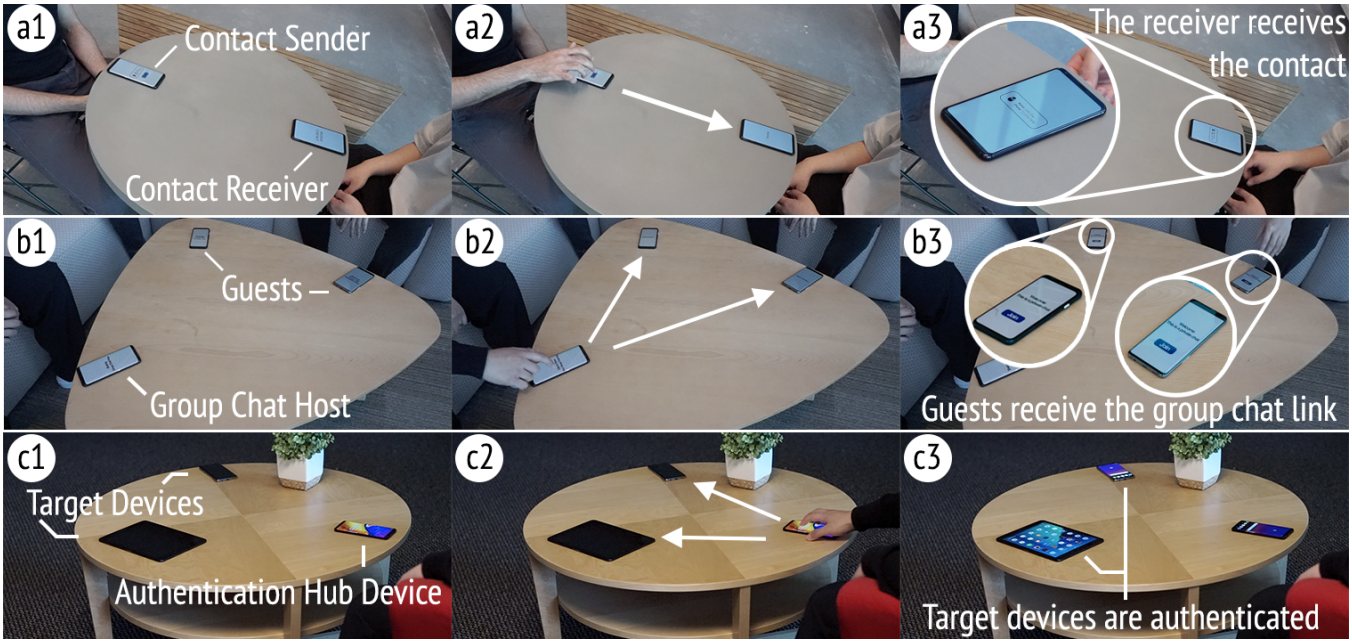

Figure 8: We present three applications of Bit Whisperer: (a) Contact Sharing Application; (a1) when two individuals want to share their contacts, they place their smartphones on the same table; (a2) A user presses the 'Share Your Contact' button to send their contact information; (a3) Then, the other receives the contact information; (b) Encrypted Group Chat Link Sharing: (b1) if a group of members want to share their private group chat link, a host and group members place their smart devices on the same table; (b2) Then, the host sends the link by tapping the 'Share a Private Chat Room' button; (b3) Once the link is sent, the 'Join' button shows up for the other members to join the chat.; (c) Automated Local Device Authentication: (c1) a user places an authenticated smart device on a table where other personal smart devices are placed; (c2) Once a user presses the 'Authenticate' button, the authenticated device sends a password signal to other devices; (c3) When the password sent by the authenticated device is matched with the stored password in other devices, the authenticated device can authenticate other devices.

1. Security through Proximity and Line of Sound. Bit Whisperer limits the area within which an adversary could potentially eavesdrop to within 1000mm (just over 3 feet) and in a shallow arc (±30°) around the direction in which sound is transmitted. Thus, it is difficult for an adversary with commodity hardware to eavesdrop invisibly — any adversary who wants to reliably intercept data transmitted by Bit Whisperer will need to be clearly present in the immediate vicinity of or be physically situated on the table where the communication occurs.

2. Immediate deployability. As implemented, Bit Whisperer uses only commodity hardware and software — in other words, it can be used by modern smartphones out-of-the-box. Note, however, that while our tests suggest that Bit Whisperer can work with a variety of phones and on a variety of table surfaces, some calibration will be necessary for each device model given hardware variability on Android phones.

3. Physical Metaphors for Granular Audience Selection. In emulating verbal whispering, Bit Whisperer can improve users' understanding of and control over the domain of their digital communications. Taking this idea further, users can take advantage of other physical world properties to exert even more granular control over the domain of their communications. One simple example is placing physical barriers to block or selectively direct ongoing communications. One might, for example, unpair two devices or interrupt data transmission by placing one's hand in between the devices or restrict communication to only a subset of nearby devices by obfuscating line of sound between the transmitter and incorrect receivers with a solid object like a book (see Figure 9).

8.1 Limitations & Future Work

Improving Bit Whisperer. We observed a 75–98% success rate for on-table communication (based on device and distance), and a 8–10% success rate for the"best" off-table adversary. As we noted in our results, this level of robustness and security should be "good enough" [21] for most use-cases given the physical security assumed in Bit Whisperer's use. Still, there is room for improvement. One possibility is to increase the number of channels of data transmission — in selecting the eight channels we used for data transmission, we observed that the accumulated probability of error across the eight channels resulted in stronger on-off table difference in successful data transmission. Using more than eight data transmission channels may further widen the gulf between on and off table success rates.

Testing the user experience of Bit Whisperer. In future work, it would be helpful to run field evaluations with a range of participants, who own varied devices and who can test the protocol in

Figure 9: Hand action and everyday objects on a physical surface can play various roles for the Bit Whisperer communication: (a) a hand can block to stop communication between two devices and open up to restart the communication; (b) Access control can be managed by blocking the line of sound with a hand to share data selectively; (c) everyday object like a book can be an obtrusive shield to protect the communication between Device A and B from a sniffing attempt of Device C.

varied environments and use-contexts. Doing so will also allow us to answer user experience questions regarding how people might use Bit Whisperer in practice, such as: In what contexts and for what sorts of data do people find Bit Whisperer to be useful? How easy is it for users to notice off-table adversaries?

Protection against stronger threats. While Bit Whisperer provides "good enough" security against eavesdropping adversaries using devices with commodity hardware, we did not test its resilience to eavesdropping against adversaries with specialized audio equipment. Bit Whisperer might also be susceptible to availability attacks (e.g., denial of service attacks) where adversaries who want to block ongoing transmissions saturate the environment with loud signals at the frequencies used to send data. We consider these adversaries out-of-scope, however, as we did not design Bit Whisperer to be used to send high-value confidential data. In future work, it would be pertinent to consider pre-emptive defensive tactics (e.g., by switching to different frequency bands or by informing users of the obstruction).

9 CONCLUSION

We designed, implemented, and evaluated Bit Whisperer, a secure, ad-hoc short-range wireless communication system and protocol that transmits data acoustically above solid surfaces. Bit Whisperer enables secure "walk-up-and-share" interactions for short-range digital communications and limits the scope of wireless digital communication to a visible, physical medium such as a table. Through a series of formative evaluations, we found that the fidelity of acoustic data transmissions is significantly higher for nearby devices co-located on the same table than for off-table and far away devices. We then demonstrated how these differences in transmission fidelity between legitimate and adversarial receivers can serve as the foundation to build a reliable and secure communication protocol by applying forward error correction and encryption. We implemented three different applications to demonstrate practical use-cases of Bit Whisperer. Finally, our implementation of Bit Whisperer requires only commodity hardware, making it deployable on a large number of commodity devices out-of-the-box.

10 ACKNOWLEDGMENTS

This research was generously supported, in part, by the National Science Foundation through grant SaTC-2029519 and CMMI-2037565. We thank members of GT Ubicomp lab and GT SPUD lab for their feedback to help improve our work. We are also grateful to the Georgia Tech Research Network Operations Center for lending devices for our evaluations. Lastly, we would like to thank the reviewers for their valuable reviews.

REFERENCES

[1] Pavel ANDREEV, Bohos Aprahamian, and Marin Marinov. 2019. QR code's maximum scanning distance investigation. In *2019 16th Conference on Electrical Machines, Drives and Power Systems (ELMA)*. IEEE, 1–4.
[2] Richard E. Berg. 2019. Sound absorption. https://www.britannica.com/science/sound-physics/Sound-absorption
[3] Ming Ki Chong and Hans Gellersen. 2012. Usability Classification for Spontaneous Device Association. *Personal Ubiquitous Comput.* 16, 1 (Jan. 2012), 77–89. https://doi.org/10.1007/s00779-011-0421-1
[4] Sauvik Das, Gierad Laput, Chris Harrison, and Jason I Hong. 2017. Thumprint: Socially-inclusive local group authentication through shared secret knocks. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. 3764–3774.
[5] Dianqi Han, Yimin Chen, Tao Li, Rui Zhang, Yaochao Zhang, and Terri Hedgpeth. 2018. Proximity-Proof: Secure and Usable Mobile Two-Factor Authentication. In *Proceedings of the 24th Annual International Conference on Mobile Computing and Networking*. ACM, 401–415.
[6] Ben Hutchins, Anudeep Reddy, Wenqiang Jin, Michael Zhou, Ming Li, and Lei Yang. 2018. Beat-PIN: A User Authentication Mechanism for Wearable Devices Through Secret Beats. In *Proceedings of the 2018 on Asia Conference on Computer and Communications Security* (Incheon, Republic of Korea) *(ASIACCS '18)*. ACM, New York, NY, USA, 101–115. https://doi.org/10.1145/3196494.3196543
[7] Inhwan Hwang, Jungchan Cho, and Songhwai Oh. 2012. Privacy-aware communication for smartphones using vibration. In *2012 IEEE International Conference on Embedded and Real-Time Computing Systems and Applications*. IEEE, 447–452.
[8] COMSOL Inc. 2019. COMSOL Multiphysics 5.4. https://www.comsol.com/
[9] Nikolaos Karapanos, Claudio Marforio, Claudio Soriente, and Srdjan Capkun. 2015. Sound-proof: usable two-factor authentication based on ambient sound. In *24th {USENIX} Security Symposium ({USENIX} Security 15)*. 483–498.
[10] Younghyun Kim, Woo Suk Lee, Vijay Raghunathan, Niraj K Jha, and Anand Raghunathan. 2015. Vibration-based secure side channel for medical devices. In *2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC)*. IEEE, 1–6.
[11] Marc Langheinrich. 2001. Privacy by design—principles of privacy-aware ubiquitous systems. In *International conference on Ubiquitous Computing*. Springer, 273–291.
[12] Gierad Laput, Robert Xiao, and Chris Harrison. 2016. Viband: High-fidelity bio-acoustic sensing using commodity smartwatch accelerometers. In *Proceedings of the 29th Annual Symposium on User Interface Software and Technology*. ACM, 321–333.
[13] Dingzeyu Li, David IW Levin, Wojciech Matusik, and Changxi Zheng. 2016. Acoustic voxels: Computational optimization of modular acoustic filters. *ACM Transactions on Graphics (TOG)* 35, 4 (2016), 1–12.
[14] Angela M Lonzetta, Peter Cope, Joseph Campbell, Bassam J Mohd, and Thaier Hayajneh. 2018. Security vulnerabilities in Bluetooth technology as used in IoT. *Journal of Sensor and Actuator Networks* 7, 3 (2018), 28.
[15] Rajalakshmi Nandakumar, Krishna Kant Chintalapudi, Venkat Padmanabhan, and Ramarathnam Venkatesan. 2013. Dhwani: secure peer-to-peer acoustic NFC. *ACM SIGCOMM Computer Communication Review* 43, 4 (2013), 63–74.
[16] S. Pallavi and V. A. Narayanan. 2019. An Overview of Practical Attacks on BLE Based IOT Devices and Their Security. In *2019 5th International Conference on Advanced Computing Communication Systems (ICACCS)*. 694–698. https://doi.org/10.1109/ICACCS.2019.8728448
[17] J. Potts and S. Sukittanon. 2012. Exploiting Bluetooth on Android mobile devices for home security application. In *2012 Proceedings of IEEE Southeastcon*. 1–4. https://doi.org/10.1109/SECon.2012.6197001

[18] Irving S Reed and Gustave Solomon. 1960. Polynomial codes over certain finite fields. *Journal of the society for industrial and applied mathematics* 8, 2 (1960), 300–304.

[19] Nirupam Roy and Romit Roy Choudhury. 2016. Ripple {II}: Faster Communication through Physical Vibration. In *13th {USENIX} Symposium on Networked Systems Design and Implementation ({NSDI} 16)*. 671–684.

[20] Nirupam Roy, Mahanth Gowda, and Romit Roy Choudhury. 2015. Ripple: Communicating through physical vibration. In *12th {USENIX} Symposium on Networked Systems Design and Implementation ({NSDI} 15)*. 265–278.

[21] Ravi Sandhu. 2003. Good-enough security. *IEEE Internet Computing* 7, 1 (2003), 66–68.

[22] Karen Scarfone and John Padgette. 2008. Guide to bluetooth security. *NIST Special Publication* 800, 2008 (2008), 121.

[23] Dominik Schürmann and Stephan Sigg. 2011. Secure communication based on ambient audio. *IEEE Transactions on mobile computing* 12, 2 (2011), 358–370.

[24] Jiayao Tan, Xiaoliang Wang, Cam-Tu Nguyen, and Yu Shi. 2018. SilentKey: A New Authentication Framework Through Ultrasonic-based Lip Reading. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 2, 1, Article 36 (March 2018), 18 pages. https://doi.org/10.1145/3191768

[25] Wikipedia. 2019. Audio frequency — Wikipedia, The Free Encyclopedia. http://en.wikipedia.org/w/index.php?title=Audio%20frequency&oldid=923460999. [Online; accessed 15-November-2019].

[26] Wikipedia. 2019. Speed of sound — Wikipedia, The Free Encyclopedia. http://en.wikipedia.org/w/index.php?title=Speed%20of%20sound&oldid=924904463. [Online; accessed 12-November-2019].

[27] Wikipedia. 2021. Advanced Encryption Standard — Wikipedia, The Free Encyclopedia. http://en.wikipedia.org/w/index.php?title=Advanced%20Encryption%20Standard&oldid=1008726613. [Online; accessed 27-March-2021].

[28] Zhenyu Wu, Ali Bilgin, and Michael W Marcellin. 2002. Unequal error protection for transmission of JPEG2000 codestreams over noisy channels. In *Proceedings. International Conference on Image Processing*, Vol. 1. IEEE, I–I.

[29] Robert Xiao, Sven Mayer, and Chris Harrison. 2020. VibroComm: Using Commodity Gyroscopes for Vibroacoustic Data Reception. In *22nd International Conference on Human-Computer Interaction with Mobile Devices and Services*. 1–9.

[30] Bingsheng Zhang, Qin Zhan, Si Chen, Muyuan Li, Kui Ren, Cong Wang, and Di Ma. 2014. PriWhisper: Enabling Keyless Secure Acoustic Communication for Smartphones. *IEEE internet of things journal* 1, 1 (2014), 33–45.

[31] Cheng Zhang, Sinan Hersek, Yiming Pu, Danrui Sun, Qiuyue Xue, Thad E Starner, Gregory D Abowd, and Omer T Inan. 2017. Bioacoustics-based human-body-mediated communication. *Computer* 50, 2 (2017), 36–46.

[32] Lin Zhong, Dania El-Daye, Brett Kaufman, Nick Tobaoda, Tamer Mohamed, and Michael Liebschner. 2007. OsteoConduct: Wireless body-area communication based on bone conduction. In *Proceedings of the ICST 2nd international conference on Body area networks*. 1–8.

[33] Zhe Zhou, Wenrui Diao, Xiangyu Liu, and Kehuan Zhang. 2014. Acoustic Fingerprinting Revisited: Generate Stable Device ID Stealthily with Inaudible Sound. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security* (Scottsdale, Arizona, USA) *(CCS '14)*. ACM, New York, NY, USA, 429–440. https://doi.org/10.1145/2660267.2660300