2020 IEEE International Conference on Systems, Man, and Cybernetics (SMC)
October 11-14, 2020. Toronto, Canada

Woodpecker: Secret Back-of-Device Tap Rhythms to Authenticate Mobile Users

Satvik Kulshreshtha
Human-Computer Interaction Group
University of California, Merced
Merced, CA, USA
skulshreshtha@ucmerced.edu

Ahmed Sabbir Arif
Human-Computer Interaction Group
University of California, Merced
Merced, CA, USA
asarif@ucmerced.edu

***Abstract*—This paper presents Woodpecker, a playful mobile user authentication method that enables users to authenticate themselves by performing back-of-device tap rhythms. It uses the microphone and accelerometer data of an off-the-shelf smartphone to compare the sequence, frequency, and intensity of tap rhythms to authenticate users. In a study, Woodpecker yielded a moderate accuracy (70%) and a low successful attack rate (17%) in an ideal shoulder surfing threat model with only three sample rhythms. Besides, most participants found the method easy-to-use and more secure than the conventional methods, thus wanted to keep using it on their devices.**

***Index Terms*—Usable security, security, back-of-device, smartphone, user authentication, audio input, gyroscope, accelerometer, shoulder surfing**

I. Introduction

Securing mobile devices is important as they acquire sensitive information over time and often have access to wireless services and organizational networks [1]. In spite of that, many mobile users (28%) do not use a user authentication method to secure their devices since they find it to be an inconvenience [2]. Besides, those that use a user authentication method do not always pick a strong password or update their passwords regularly, which reduces the effectiveness of the methods. In fact, maintaining a sensible balance between the *security* and the *usability* of user authentication methods has long been a challenge since increasing the security of a method usually compromises its usability, discouraging users to use it, while making it more usable tend to compromise its security.

Woodpecker is a novel playful, user-friendly, yet secure user authentication method that enables users to tap secret rhythms on the back of mobile devices to authenticate themselves. It is inspired by the age-old concept of *"secret knock"*, a knock sequence to allows access only to those who know the correct knock. But unlike a secret knock, Woodpecker accounts for not only tap sequence but also tap frequency and intensity, which enables users to tap their favorite tunes as passwords. With this method, users first select a tap rhythm as their password, then repeats it to unlock mobile devices. Its design is motivated by the following considerations. First, its playful nature can encourage mobile users that are reluctant on securing their devices to start using a user authentication method. Since the method enables users to select tap rhythms representing their favorite music or tunes, it can also motivate them to change their passwords more frequently in keeping with their current musical taste, like some users frequently change their ringtones [3]. Second, Woodpecker does not leave any oily residue on the screen since it is used on the back-of-device. Prior studies showed that attackers can easily guess passwords by studying the smudges left on the touchscreen [1], [4]. Back-of-device interaction also hides finger movements behind the device, and soft taps usually do not make any audible noise, making it difficult for attackers to guess the passwords. These make the method more secure than the traditional digit and pattern lock methods. Finally, Woodpecker does not use touch, therefore can be appropriated for devices that do not have a touchscreen or a display, such as to turn on a projector, unlock a door, or turn on the radio in an automobile.

The reminder of the paper is organized as follows. It starts with a review of the literature, focusing on existing rhythm-based user authentication methods and methods for detecting back-of-device interactions. Then, it presents Woodpecker and describes its system architecture, informed by the findings of two pilot studies. It then presents the results of an empirical study evaluating Woodpecker's usability and security. Finally, it summarizes the contributions and limitations of the work, and reflects on potential future extensions.

II. Related Work

Not many have explored the possibility of using tap rhythms as passwords on mobile devices. TapSongs [5] enables user authentication by performing a sequence of *tap-up* and *tap-down* events using a single binary sensor, such as a physical button. RhythmLink [6], Beat-PIN [7], and TapMeIn [8] use a similar principle that authenticate users through a sequence of *touch-up* and *touch-down* events on the touchscreen of mobile or wearable devices. RhyAuth [9] is also similar, but enables users to both tap and slide to produce rhythm passwords. Arif et al. [10] also use tap and stroke to authenticate users, but do not facilitate creating a rhythm. Arif and Mazalek [11] enable user authentication by performing a sequence stroke and pause on the touchscreen. Aydemir and Toslak [12], on the other hand, attached a force-sensitive button on a door to authenticate users based on the stroking pattern and force on the button. However, the most relevant to this work is Thumprint [13], a group authentication method that

978-1-7281-8526-2/20/$31.00 ©2020 IEEE

authenticate group members via shared secret knocks. In an ideal setting, its success rate and successful attack rate were estimated as 85–91% and 13–19%, respectively. None of these works, however, investigate back-of-device tap rhythms or account for both tap sequence, frequency, and intensity.

There has been some research in the detection of back-of-device taps, touches, grips, and gestures. Most of these works either require additional hardware [14]–[20] or provide binary output signal [21], [22]. In addition to these, Lopes et al. [23] augmented touch with acoustic sensing to facilitate expressive gestures, such as tap, knock, slap, and punch, on an interactive tabletop. Sun et al. [24], in contrast, used the built-in speakers and microphones of a smartphone to detect back-of-device taps and gestures. Hudson et al. [25] proposed using accelerometer data to detect expressive gestures on mobile phones. Seipp and Devlin [26] detected finger-specific gestures using built-in microphone and gyroscope of a smartphone. Zhang et al. [27] used the built-in accelerometer, gyroscope, and microphone of a smartphone to detect one-handed, two-handed, and on-table taps. A few have also proposed back-of-device authentication methods. De Luca et al. [28] designed a method where user authenticates themselves by performing a row of simple shapes on the back of the device. Leiva and Català [29] simplified this method by considering tap contacts as the main primitives.

III. Pilot Study 1

We conducted a pilot study to investigate if microphone, accelerometer, and gyroscope data are sufficiently reliable to detect and compare back-of-device tap sequence, frequency, and intensity. The study collected microphone data from four conditions: (I) quiet room (40 *dBA*), (II) crowded room (60–70 *dBA*), (III) quiet outdoors (70–90 *dBA*), and (IV) noisy outdoors (90–110 *dBA*); and accelerometer and gyroscope data from two conditions: (I) in a seated position and (II) while walking.

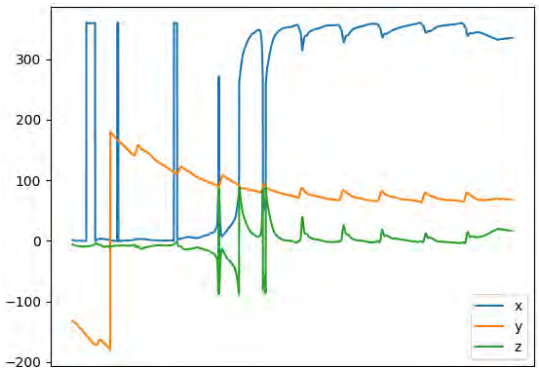

Fig. 1. Erratic gyroscope data in a seated position. All three axis readings are jagged and often cross with each other. The x and y axis of the graph represent time (*ms*) and angular velocity (*deg/s*), respectively.

We used a Motorola G^5 Plus smartphone (15.02×7.4×0.77 *cm*, 155 *g*) running on Android OS 7.0 at 1080×1920 *pixels*. A custom Web app was developed using HTML5 and JavaScript to record accelerometer, gyroscope, and microphone data. It

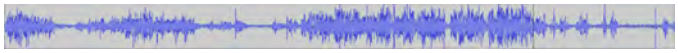

Fig. 2. Noisy microphone data with loud ambient noise. The x and y axis of the graph represent time (*ms*) and amplitude, respectively.

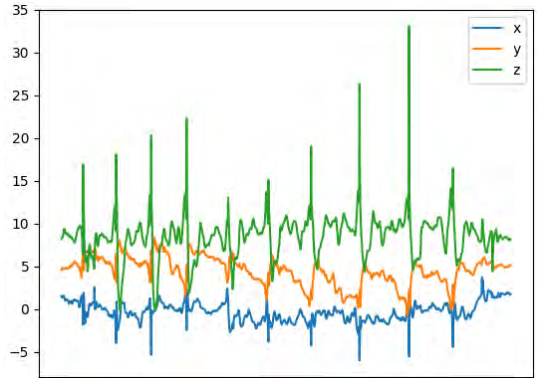

Fig. 3. Accelerometer data while waling. Sudden hand movements caused sharp peaks or drops in all axes, concealing the taps. The x and y axis of the graph represent time (*ms*) and acceleration (m/s^2), respectively.

was accessed using the Mozilla Firefox (v61.0) browser for Android OS. During the pilot study, five participants (aged 22–29 years, all male) were instructed to hold the device in upright position and tap on the back of the device 10 times in approximately 1.0 second interval. Each participant performed this pattern 10 times per condition, resulting in 5×6×10 = 300 patterns in total. The app did not guide participants on when to tap since we wanted to find out whether they can maintain a constant tempo. Analysis of the data revealed that (I) gyroscope data is not reliable in any condition (Fig. 1), (II) microphone data is not reliable in noisy environments (Fig. 2), (III) accelerometer data is not always reliable in mobile settings (Fig. 3), and (IV) tap intensity and tempo varies both within and between participants. In summary, the pilot revealed that gyroscope data is too noisy to detect and compare tap patterns. Microphone and accelerometer data are mostly reliable but fails in some settings even when noise reduction methods are applied. Hence, we decided to exclude gyroscope and use both microphone and accelerometer data to support a wider range of settings. We also found out that it is difficult for users to maintain a steady frequency and intensity. We further explored this in a second pilot study.

IV. Pilot Study 2

The purpose of this pilot study was to investigate if users can maintain a steady frequency and intensity for self-selected tap patterns and to determine an effective method for comparing the patterns.

A. Apparatus

We used a Motorola G^5 Plus smartphone (15.02×7.4×0.77 *cm*, 155 *g*) running on Android OS 7.0 at 1080×1920 *pixels*. A client-server model was used to record and process accelerometer and microphone data. The client was a custom Web app

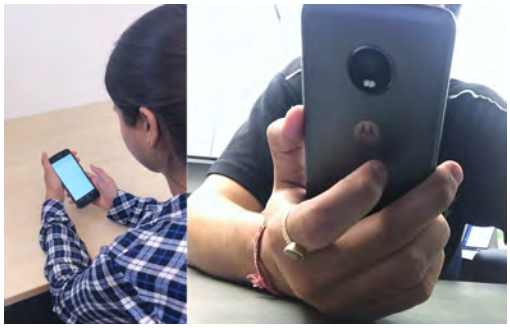

Fig. 4. Two participants performing back-of-device tap rhythms in the second pilot study.

that was developed with HTML5 and JavaScript. It recorded and sent a file in Wave File Audio (*.wav*) format and an integer array of acceleration data (rate of velocity change) to a server running on a 13″ MacBook Pro Retina (2.4GHz, Intel Core i5, 8GB 1600MHz DDR3) running on MacOS Mojave (v10.14.6). The server extracted Mel-Frequency Cepstrum Coefficients (MFCCs) feature from the audio file (*.wav*) using LibROSA[1], processed the microphone and accelerometer data using Web Audio API[2] and SciPy Python Library[3], respectively, then sent the results to the client. We used the Flask Python Library[4] to establish connection between the client and the server. The app was accessed using the Mozilla Firefox browser (v61.0) for Android.

1) Rhythm Comparison: The system compared tap rhythms using the Fast Fourier Transform (FFT) and the Dynamic Time Warping (DTW) algorithms [30]. FFT transforms time domain into frequency domain to analyze time-dependent phenomena. We used it to compare the amplitudes and frequencies of two rhythms. We used DTW to identify the same rhythm with different tempo. DTW is a time series analysis algorithm that measures the similarity between two temporal sequences that may vary in speed.

B. Participants

Fifteen participants voluntarily took part in the pilot study (Fig. 4). Their age ranged from 23 to 34 years (M = 26.2, SD = 3.05). Five of them were female and ten were male. They had on average 6.4 years (SD = 2.2) of experience with touch-based devices. Fourteen of them were right-handed and one was ambidextrous. The ambidextrous person chose to use his right hand to perform the tap patterns.

C. Design and Procedure

The pilot study was conducted in a moderately quiet office room. Upon arrival, we explained the study procedure to all participants and collected their consents. They then completed a short demographics and mobile usage questionnaire. The main study started after that, where participants were asked to hold the device with their preferred hand in any orientation, then tap a rhythm of their choice on the back of the device for 6 times (15×6 = 90 patterns in total). The app automatically recorded and analyzed microphone and accelerometer data.

D. Results and Discussion

All participants chose to hold the device in portrait position with the right hand and perform the taps using the index finger of the same hand. Similar to the first pilot study, participants were having difficulty in maintaining a steady frequency and intensity. We observed a high variability in the patterns. On average there were 6.93 peaks (SD = 4.81) per rhythm; with an average duration of 4.96 seconds (SD = 2.53) per peak. The average maximum and minimum peaks were 6871.90 *dB* (SD = 8131.2) and –7411.14 *dB* (SD = 9265.4), respectively. This indicates a high variability in both rhythm frequency and intensity. FFT and DTW scores also corroborate this. The average FFT and DTW scores were 111.25 (SD = 28.59) and 826.125 (SD = 1732.39), correspondingly. This suggests that comparing tap rhythms using either FFT or DTW alone could yield misleading results since users tend to vary intensity (they often tap harder or softer than the usual) and frequency (they often tap faster or slower than the usual) when performing the same rhythm.

V. System Architecture

Woodpecker requires users to select a tap rhythm as their password by performing it three times on the back of the device. The system then performs FFT and DTW to calculate Mean Square Error (MSE) and Minimum Distance (MD) between the rhythms, respectively. $MSE = 0$ & $MD = 0$ implies that the two compared rhythms are identical, while $MSE > 0$ & $MD = 0$ indicates that they are identical when the tempo is disregarded. The system identifies the maximum MSE and MD values that yield a *match* for all rhythms, then stores those for each user as thresholds. The system also records the total number of peaks, calculated by performing Continuous Wavelet Transform (CWT) on the accelerometer data. Fig. 5 illustrates the architecture of the proposed method.

When a user performs a tap rhythm, the system counts the total number of peaks in the rhythm, then compares it (*Pattern 4*) with the sample rhythms (*Patterns 1–3*) to calculate MSE and MD values. The user is authenticated when the number of peaks matches and the MSE and MD values are above the thresholds calculated for the users using the three samples recorded during the password selection process. We used this approach based on the findings of the pilot studies—to reduce incorrect authentications (false positives), as well as to cope with small fluctuations in the intensity and tempo.

VI. User Study: Evaluation

We conducted an empirical study to evaluate Woodpecker in terms of reliability, usability, and security. A shoulder surfing threat model was used to test the security of the method.

[1]https://librosa.github.io/librosa
[2]https://developer.mozilla.org/en-US/docs/Web/API/Web_Audio_API
[3]https://docs.scipy.org/doc/scipy/reference
[4]https://palletsprojects.com/p/flask

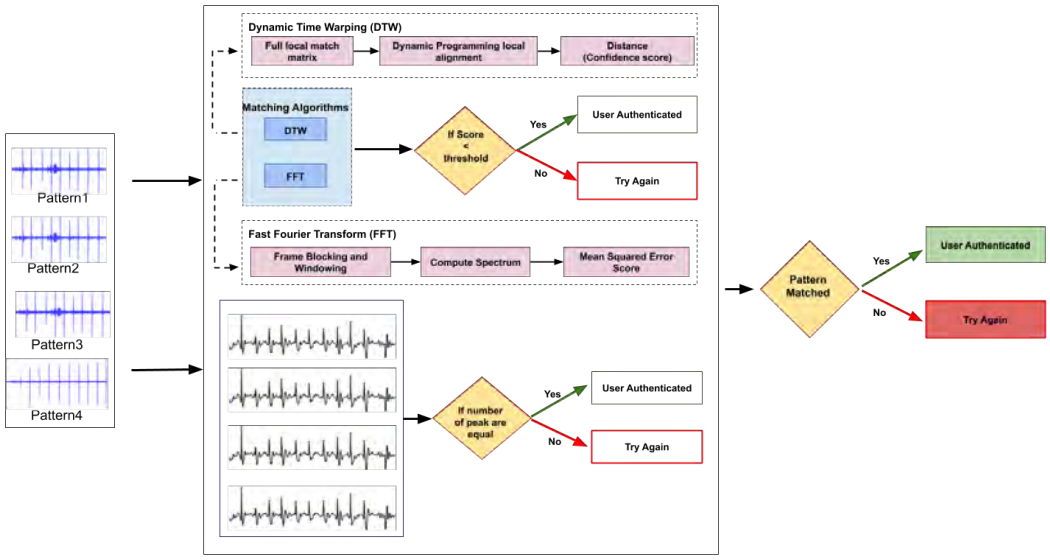

Fig. 5. Architecture of the proposed user authentication method.

A. Apparatus

The study used the same device and the custom app as the second pilot study. But unlike the pilot, the app displayed a message on the screen (visual feedback) indicating whether an authentication attempt was successful or not.

B. Participants

Twelve participants voluntarily took part in the final study. Their age ranged from 21 to 35 years (M = 26.16, SD = 3.05). Three of them were female and nine were male. Thy all were frequent smartphone users. They had on average 7.5 years (SD = 1.78) of experience with smartphones. Eleven of them were right-handed and one of them was ambidextrous. The ambidextrous participant chose to use the right hand to perform the tasks.

Fig. 6. Volunteers participating in the study. Seated participants are unlocking the device with tap rhythms and standing participants are executing shoulder surfing attacks.

C. Design and Procedure

The study was conducted in a quiet room. Upon arrival, we demonstrated Woodpecker and explained the study procedure to all participants. In order to discourage tap rhythms that are audible to bystanders, we informed the participants that they do not have to tap hard on the back of the device since the system can pick up on even softer taps. We then collected their consents and asked them to complete a short demographics and mobile usage questionnaire. We randomly paired participants for one of them to play the role of a *"user"* and another the role of an *"attacker"*. The user was instructed to pick a tap rhythm as her password. For this, she performed a tap rhythm of her choice three times on the back of the device. The custom app automatically recorded microphone and accelerometer data and calculated the thresholds for the user. We then asked her to unlock the device five times by performing her password rhythm. The app recorded all successful and unsuccessful attempts. Users were not required to re-enter the password on unsuccessful attempts. The attacker, on the other hand, was instructed to observe the authentication process by standing in close proximity to the user (Fig. 6). We enabled the attacker to change position for an unobstructed view of the password entry process in an attempt to create an ideal shoulder surfing threat model. We then instructed her to crack the pattern in five attempts. Like the authentication process, the app recorded all successful and unsuccessful attacks. Each participant went through this process for three times, then switched roles—participants that played the role of a user became attackers and vice versa. Hence, the within-subjects design was:

User	**Attacker**
12 participants ×	12 participants ×
3 tap rhythms ×	3 tap rhythms ×
5 attempts =	5 attacks =
180 attempts, in total	180 attacks, in total

Upon completion of the study, participants were asked to take part in a semi-structured interview that inquired about their tap rhythm selection strategy and opinion about various aspects of the authentication method.

VII. Results

A complete study session took about 40 minutes to complete, including demonstrations and optional breaks.

A. Orientation, Position, and Posture

We enabled participants to hold the device and perform the tap rhythms in their preferred orientation, position, and posture. Yet, all participants chose to hold the device in portrait position with the right hand, and performed the taps using the index finger of the same hand. One participant (8%) also used the middle finger to perform some taps. Some of the participants occasionally held the device with two hands for added support (Fig. 6, left). Most participants (92%, N = 11) performed the taps at the center of the device, while one (8%, N = 1) performed at the top-right corner.

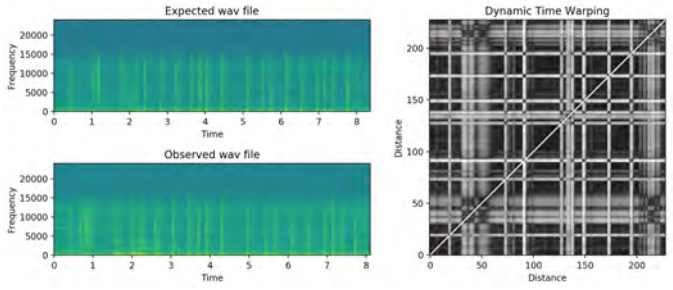

Fig. 7. Comparison of two rhythms performed by the same user. Both (left) Mean Square Error (MSE) and (right) Dynamic Time Warping (DTW) indicating a match.

B. Tap Rhythms

On average, tap rhythm passwords were composed of 4.1 taps (SD = 1.4). The average maximum and minimum intensity of peaks were 10532.96 *dB* (SD = 3913.64) and –9749.26 *dB* (SD = 3666.73), respectively. The average duration of peaks was 2.70 seconds (SD = 0.62).

TABLE I
Successful authentication and attack attempts per participant (N) with true positive and false positive rates. Note that each participant made 15 authentication and 15 attack attempts.

N	Authentication	TPR	FPR	Attack
1	12	0.80	0.20	1
2	12	0.80	0.20	1
3	12	0.80	0.20	0
4	13	0.86	0.13	3
5	9	0.60	0.40	3
6	7	0.46	0.53	2
7	9	0.60	0.40	6
8	9	0.60	0.40	1
9	10	0.66	0.33	2
10	11	0.73	0.26	7
11	9	0.60	0.40	2
12	12	0.86	0.20	2

C. Reliability and Security

Table I presents the total number of successful (Fig. 7) and failed authentication attempts per participant. Fig. 8 illustrates a Receiver Operating Curve (ROC) that plots the true positive rate (TPR) against the false positive rate (FPR). Woodpecker yielded a moderate accuracy rate of 70%. On average 11 out of 15 valid attempts (SD = 1.75) were successful in authenticating the users. However, Woodpecker yielded a relatively low attack rate of 17%. On average only 2.5 out of 15 attacks (SD = 1.9) were successful in cracking the passwords.

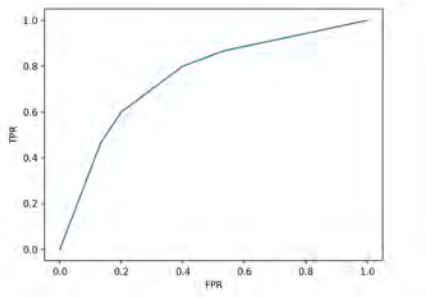

Fig. 8. Receiver Operating Curve (ROC) for Woodpecker at the examined threshold settings.

VIII. User Feedback

Upon completion of the user study, participants took part in a semi-structured interview that asked them about their tap rhythm selection strategy and opinion about various aspects of Woodpecker.

A. Password Selection

When asked about the strategy employed to select their passwords, most participants (58%, N = 7) responded that they picked their favorite songs or tunes. The remaining participants picked rhythms that are easy to remember (25%, N = 3) and/or easy to perform (17%, N = 2). Most participants (92%, N = 11) found tap rhythms easy to recall during the study, while one (8%) found it difficult.

B. Mental and Physical Stress

Most participants responded that performing back-of-device rhythms did not cause any cognitive (92%, N = 11) or physical stress (83%, N = 10). However, some participants reported slight cognitive (8%, N = 1) and physical stress (17%, N = 2) for extensive use. Note that we encouraged all participants to take breaks between the blocks, but not all obliged.

C. Willingness to Use

Most participants (67%, N = 8) wanted to use Woodpecker on their mobile devices, while one was undecided (8%) about it. One participant (male, 24 years) responded, *''Yes [I will use Woodpecker], because it is secure"*. Likewise, another (male, 27 years) responded, *''Yes [I will use Woodpecker as it is] convenient [and leaves] no smudges on the touchscreen"*. The remaining three participants (25%) were on board with the idea but did not want to use the current version due to

its relatively high false negative rate. One of them (male, 28 years) responded, *"I won't use the current version as it's not robust enough"*.

D. Security

When enquired about their experience as shoulder surfers, most participants (92%, N = 11) responded that it was very difficult. One participant (male, 25 years) responded, *"It was difficult because finger movements were not visible, and the back side of the phone was not visible. The taps were also not audible [...]"*. Another participant (female, 31 years) commented, *"[Initially, it] felt easy but it was difficult. The patterns [entered by the others] were unrecognizable"*. Many pointed out that they were able to crack some passwords since they were provided with an ideal shoulder surfing setting, and felt that it will be much more difficult in real-world. One participant (female, 27 years) stated, *"It will be [difficult in real-world scenarios] as there will be other sounds and the back of the device will not be visible, [making] the patterns indistinguishable"*. Likewise, another participant (male, 35 years) responded, *"It will be very difficult to crack the passwords in open environment"*.

IX. Discussion

The proposed method yielded a 70% accuracy rate and a 17% successful attack rate. The successful attack rate is impressive considering that attackers were provided with an ideal threat model, where they were provided with a quiet room, and unobstructed and repeated views of the authentication process. Almost all studies evaluating novel user authentication methods allow only one view of the authentication process in their threat models [28]. The accuracy rate of the method is not as impressive, which could be due to the *"Hawthorne Effect"* [31] that suggests that users tend to modify their behavior in response to their awareness of being observed. The fact that attackers were studying them while entering the passwords may have affected their input, resulting in some failed attempts (relevantly, Woodpecker yielded a much higher accuracy rate in pilot studies). Thumprint [13], a similar method, yielded a 85-91% accuracy rate and 13-19% successful attack rate. This method, however, was designed to authenticate group members (all members of a group shared the same password), hence likely tolerated a higher variances in the data. Besides, Thumprint used 10 samples, when we used only 3. We believe that the accuracy of the proposed method can be improved by fine-tuning the mechanism used for determining the thresholds for matching tap rhythms. Improvement on this is a direction for future work.

A. Limitations

We identified several limitations of the proposed method.

1) Diverse Settings and Attachments: Although the method yielded a comparable performance in all explored settings, its performance is likely to reduce in extremely noisy environments, when commuting [32], and in different orientations, positions, and postures. In extremely loud environments (e.g., at a rock concert), the noise in the microphone data could conceal tap rhythms. Likewise, there could be severe changes in the velocity and the peaks when the user's hand is shaking or moving (e.g., when taking a bumpy ride). However, we argue that these could be addressed by collecting more sample and using more sophisticated smoothing and matching algorithms. This is a scope for future research. Besides, users tend to use different types of covers, cases, and attachments for grip [33], [34] on mobile devices. While theoretically the method should work on devices with attachments, we did not test this in our studies.

2) Guessable Tunes, Hard Taps, and Nails: Using popular tunes as passwords could reduce the security of the method as some attackers may be able to successfully guess a password. However, using a popular tune is much more secure than using a common personal identification number (PIN) like "1234", because the second pilot showed that different users tend to tap the same rhythm differently, thus are not identical. Further, some users may tap hard, making the rhythm audible to bystanders, compromising the security. We observed this in the pilot studies, thus informed the participants that they do not have to tap hard for the system to recognize the patterns. Tapping with nails or knuckles poses similar risks.

X. Conclusion

This paper presented Woodpecker, a playful mobile user authentication method that enables users to select back-of-device tap rhythms as their passwords. It uses the built-in microphone and accelerometer of an off-the-shelf smartphone to detect and distinguish between different tap rhythms. We conducted a user study to evaluate the reliability, usability, and security of the method, where it yielded a 70% accuracy rate, and a 17% successful attack rate in an ideal shoulder surfing scenario. Besides, most participants found the method easy-to-use, more secure than the traditional digit and pattern lock methods; and wanted to keep using it on their mobile devices.

The contribution of this work is twofold. First, it demonstrated that secret back-of-device tap rhythms can be used to authenticate mobile users, potentially increasing the usability and security. Second, based on the findings of a study, this work discussed design considerations and the challenges that remains in the area, which may inspire researchers to design and develop more effective and secure user authentication methods.

XI. Future Work

In the future, we will address the limitations listed above. We will apply machine learning approaches to learn users' tap behaviors in various settings. We believe, this will increase the reliability of the method. In addition, we will explore the possibility of using the method on wearables and devises that do not have a display and for other types of authentications, such as to pair devices.

REFERENCES

[1] A. S. Arif, A. Mazalek, and W. Stuerzlinger, "The Use of Pseudo Pressure in Authenticating Smartphone Users," in *Proceedings of the 11th International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services*. Brussels, Belgium: ICST, 2014, pp. 151–160.

[2] M. Anderson, "Many Smartphone Owners Don't Take Steps to Secure Device," Pew Research Center, Washington, DC, USA, Mar. 2017. [Online]. Available: https://www.pewresearch.org/fact-tank/2017/03/15/many-smartphone-owners-dont-take-steps-to-secure-their-devices/

[3] D. M. Ewalt, "What Does Your Ringtone Say About You?" Forbes, Jersey City, NJ, USA, Jun. 2005. [Online]. Available: https://www.forbes.com/2005/06/01/cx_de_0601ringtone.html

[4] A. J. Aviv, K. Gibson, E. Mossop, M. Blaze, and J. M. Smith, "Smudge Attacks on Smartphone Touch Screens," in *Proceedings of the 4th USENIX Conference on Offensive Technologies*. Berkeley, CA, USA: USENIX Association, 2010, pp. 1–7.

[5] J. O. Wobbrock, "TapSongs: Tapping Rhythm-Based Passwords on a Single Binary Sensor," in *Proceedings of the 22nd Annual ACM Symposium on User Interface Software and Technology*. New York, NY, USA: ACM, 2009, pp. 93–96.

[6] F. X. Lin, D. Ashbrook, and S. White, "Rhythmlink: Securely Pairing I/O-Constrained Devices by Tapping," in *Proceedings of the 24th Annual ACM Symposium on User Interface Software and Technology*. New York, NY, USA: ACM, 2011, pp. 263–272.

[7] B. Hutchins, A. Reddy, W. Jin, M. Zhou, M. Li, and L. Yang, "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*, ser. ASIACCS '18. New York, NY, USA: ACM, 2018, pp. 101–115, event-place: Incheon, Republic of Korea.

[8] T. Nguyen and N. Memon, "Tap-Based User Authentication for Smartwatches," *Computers & Security*, vol. 78, pp. 174–186, Sep. 2018.

[9] Y. Chen, J. Sun, R. Zhang, and Y. Zhang, "Your Song Your Way: Rhythm-Based Two-Factor Authentication for Multi-Touch Mobile Devices," in *2015 IEEE Conference on Computer Communications (INFOCOM)*, Apr. 2015, pp. 2686–2694, iSSN: 0743-166X.

[10] A. S. Arif, M. Pahud, K. Hinckley, and W. Buxton, "A Tap and Gesture Hybrid Method for Authenticating Smartphone Users," in *Proceedings of the 15th international conference on Human-computer interaction with mobile devices and services*, ser. MobileHCI '13. Munich, Germany: Association for Computing Machinery, Aug. 2013, pp. 486–491.

[11] A. S. Arif and A. Mazalek, "Slide-to-Unlock Revisited: Two New User Authentication Techniques for Touchscreen-Based Smartphones," in *Proceedings of the 11th International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services*, ser. MOBIQUITOUS '14. Brussels, Belgium: ICST, 2014, pp. 389–390.

[12] E. Aydemir and F. Toslak, "Unlock a Device with Pressure and Rhythm Based Password," *Balkan Journal of Electrical and Computer Engineering*, vol. 7, no. 2, pp. 137–142, Apr. 2019.

[13] S. Das, G. Laput, C. Harrison, and J. I. Hong, "Thumprint: Socially-Inclusive Local Group Authentication Through Shared Secret Knocks," in *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, ser. CHI '17. New York, NY, USA: ACM, 2017, pp. 3764–3774.

[14] L. Besançon, M. Ammi, and T. Isenberg, "Pressure-Based Gain Factor Control for Mobile 3D Interaction Using Locally-Coupled Devices," in *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, ser. CHI '17. New York, NY, USA: ACM, 2017, pp. 1831–1842.

[15] D. Wigdor, C. Forlines, P. Baudisch, J. Barnwell, and C. Shen, "Lucid Touch: A See-Through Mobile Device," in *Proceedings of the 20th Annual ACM Symposium on User Interface Software and Technology*, ser. UIST '07. New York, NY, USA: ACM, 2007, pp. 269–278.

[16] M. F. Mohd Noor, A. Ramsay, S. Hughes, S. Rogers, J. Williamson, and R. Murray-Smith, "28 Frames Later: Predicting Screen Touches from Back-of-Device Grip Changes," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ser. CHI '14. New York, NY, USA: ACM, 2014, pp. 2005–2008.

[17] P. Baudisch and G. Chu, "Back-of-Device Interaction Allows Creating Very Small Touch Devices," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ser. CHI '09. New York, NY, USA: ACM, 2009, pp. 1923–1932.

[18] D. Holman, A. Hollatz, A. Banerjee, and R. Vertegaal, "Unifone: Designing for Auxiliary Finger Input in One-Handed Mobile Interactions," in *Proceedings of the 7th International Conference on Tangible, Embedded and Embodied Interaction*, ser. TEI '13. New York, NY, USA: ACM, 2013, pp. 177–184.

[19] C. Corsten, B. Daehlmann, S. Voelker, and J. Borchers, "BackXPress: Using Back-of-Device Finger Pressure to Augment Touchscreen Input on Smartphones," in *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, ser. CHI '17. New York, NY, USA: ACM, 2017, pp. 4654–4666.

[20] C. Corsten, C. Cherek, T. Karrer, and J. Borchers, "HaptiCase: Back-of-Device Tactile Landmarks for Eyes-Free Absolute Indirect Touch," in *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, ser. CHI '15. New York, NY, USA: ACM, 2015, pp. 2171–2180.

[21] E. Granell and L. A. Leiva, "Less Is More: Efficient Back-of-Device Tap Input Detection Using Built-in Smartphone Sensors," in *Proceedings of the 2016 ACM International Conference on Interactive Surfaces and Spaces*, ser. ISS '16. New York, NY, USA: ACM, 2016, pp. 5–11.

[22] ——, "βTap: Back-of-Device Tap Input with Built-in Sensors," in *Proceedings of the 19th International Conference on Human-Computer Interaction with Mobile Devices and Services*, ser. MobileHCI '17. New York, NY, USA: ACM, 2017, pp. 52:1–52:6.

[23] P. Lopes, R. Jota, and J. A. Jorge, "Augmenting Touch Interaction Through Acoustic Sensing," in *Proceedings of the ACM International Conference on Interactive Tabletops and Surfaces*, ser. ITS '11. New York, NY, USA: ACM, 2011, pp. 53–56.

[24] K. Sun, T. Zhao, W. Wang, and L. Xie, "VSkin: Sensing Touch Gestures on Surfaces of Mobile Devices Using Acoustic Signals," in *Proceedings of the 24th Annual International Conference on Mobile Computing and Networking*, ser. MobiCom '18. New York, NY, USA: ACM, 2018, pp. 591–605.

[25] S. E. Hudson, C. Harrison, B. L. Harrison, and A. LaMarca, "Whack Gestures: Inexact and Inattentive Interaction with Mobile Devices," in *Proceedings of the Fourth International Conference on Tangible, Embedded, and Embodied Interaction*, ser. TEI '10. New York, NY, USA: ACM, 2010, pp. 109–112.

[26] K. Seipp and K. Devlin, "BackPat: One-Handed Off-Screen Patting Gestures," in *Proceedings of the 16th International Conference on Human-computer Interaction with Mobile Devices & Services*, ser. MobileHCI '14. New York, NY, USA: ACM, 2014, pp. 77–80.

[27] C. Zhang, A. Guo, D. Zhang, C. Southern, R. Arriaga, and G. Abowd, "BeyondTouch: Extending the Input Language with Built-in Sensors on Commodity Smartphones," in *Proceedings of the 20th International Conference on Intelligent User Interfaces*, ser. IUI '15. New York, NY, USA: ACM, 2015, pp. 67–77.

[28] A. De Luca, E. von Zezschwitz, N. D. H. Nguyen, M.-E. Maurer, E. Rubegni, M. P. Scipioni, and M. Langheinrich, "Back-of-Device Authentication on Smartphones," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ser. CHI '13. New York, NY, USA: ACM, 2013, pp. 2389–2398.

[29] L. A. Leiva and A. Català, "BoD Taps: An Improved Back-of-Device Authentication Technique on Smartphones," in *Proceedings of the 16th International Conference on Human-computer Interaction with Mobile Devices & Services*, ser. MobileHCI '14. New York, NY, USA: ACM, 2014, pp. 63–66, event-place: Toronto, ON, Canada.

[30] J. Huo, "Dynamic Time Warping and FFT: A Data Preprocessing Method for Electrical Load Forecasting," *International Journal of Advanced Computer Science and Applications*, vol. 2, no. 9, 2018.

[31] R. Macefield, "Usability Studies and the Hawthorne Effect," *Journal of Usability Studies*, vol. 2, no. 3, pp. 145–154, 2007.

[32] A. S. Arif, "A Survey on Mobile Text Entry Handedness: How Do Users Input Text on Handheld Devices While Nomadic?" in *2012 4th International Conference on Intelligent Human Computer Interaction (IHCI)*, Dec. 2012, pp. 1–6.

[33] M. Shen, G. Rakhmetulla, and A. S. Arif, "Put a Ring on It: Text Entry Performance on a Grip Ring Attached Smartphone," Sep. 2018. [Online]. Available: https://arxiv.org/abs/1809.05352v1

[34] S. Kulshreshtha and A. S. Arif, "Text Entry Performance on an Expandable Socket Attached Smartphone in Stationary and Mobile Settings," in *Advances in Usability and User Experience*, ser. Advances in Intelligent Systems and Computing, T. Ahram and C. Falcão, Eds. Cham: Springer International Publishing, 2020, pp. 207–217.