Vi Any Means: Proposal

Authors redacted

Biometrics have been employed as a secure authentication method for decades. However, conventional biometric security presents some inherent vulnerabilities. For starters, unique physical characteristics such as a fingerprint or an iris can be rendered useless if compromised just once, and even someone's voice can be replicated and manipulated with current deepfake technology [1]. Research within the last three years has identified significant vulnerabilities in fingerprint- and iris-based biometric systems [2, 3]. Replay attacks, for instance, leverage pre-recorded templates created from prior successful authentications to impersonate users and deceive systems [4]. Instead, we propose a more secure and seamless alternative, which relies on an individual's unique skin dampening property as a means for authenticating, via the vibration functionality of a smartwatch.

By combining a user-created vibration pattern (the passcode) with dampening level analysis (DLA), we are embedding biometry in two-factor authentication to effectively achieve an impermanent third factor. Since there is no (currently-known) way to replicate an individual's skin dampening properties, the smartwatch has to be worn by the legitimate user in order to authenticate successfully. Thus, any replay attack on this system would require physical control of both the device and the individual. What's more, the low permanence of this hybrid approach serves to mitigate any potential breach of either the passcode or DLA data, since a user can simply generate a new vibration pattern. While our prototype will be focused exclusively on the implementation of a viable replacement for current two-factor authentication systems, we expect the underlying technology will ultimately present many more use cases. Vibration dampening analysis could usher in an era of pseudo-biometric authentication for less sensitive scenarios, like pairing with IoT devices in public spaces.

Other works have looked into harnessing vibration as a way to understand pressure inputs on smart devices. Based on existing studies, we hypothesize that skin dampening differs from person to person, so a stranger wearing someone's smartwatch would not be able to authenticate as the original user with our system [5]. These differences are attributed to each person having a unique bone structure and a prior paper used this idea for bone conduction [6]. Additionally, Laput et al. developed a smartwatch device that boosted the existing accelerometer to 4 kHz, giving them the ability to recognize different hand motions and gestures with bio-acoustic signals [7]. The researchers were able to identify differences between flicks, taps, and scratches. They also implemented features that allowed for data packet transmittal and individual identification using their developed "vitro-tags." In another study, a watch that would send a short vibration was deemed the preferred method over SMS and Token for 2FA. User concerns around the security of the watch became a secondary point since it was found by participants to be the most usable. This important part demonstrated that if a device is secure but too difficult to use, its

security benefits are rendered meaningless as users look for alternative solutions [8]. These articles have allowed us to get a definitive sense of the myriad possibilities from using vibration and skin dampening properties as a viable method for our authentication model.

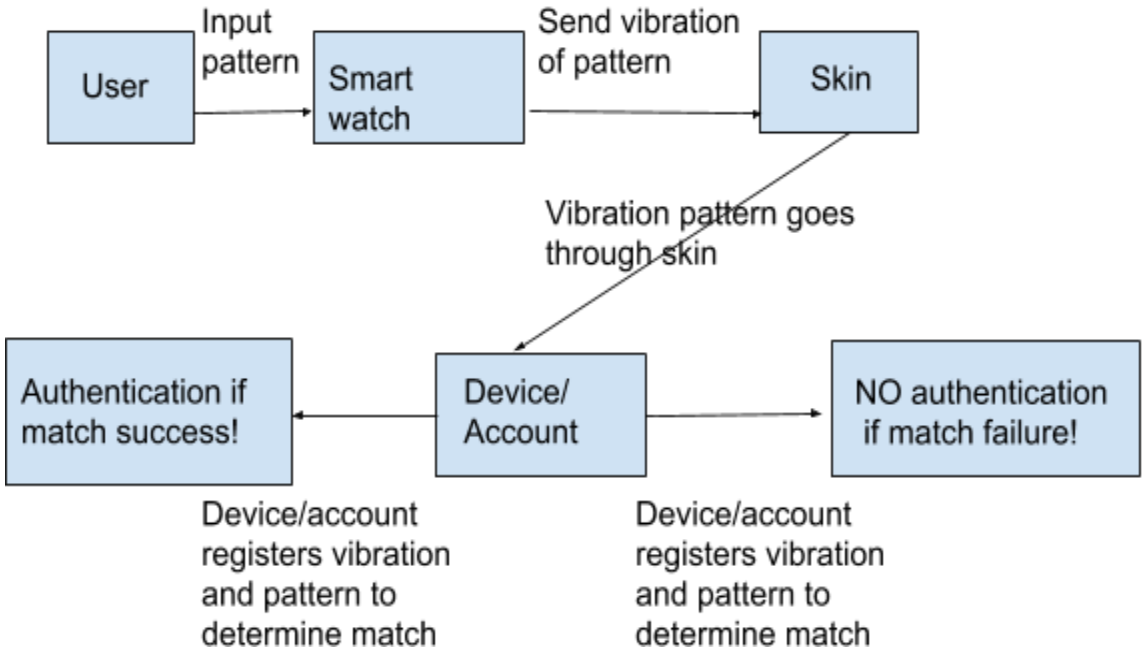

Figure 1. Schematic of Vi Any Means: Input and Output features

From a technical standpoint, we plan to use an Android smartwatch or an Apple Watch as the source of vibration for our first prototype. An MPU-6050 sensor [9] will act as the receiver to whichever target device will be authenticated with the smartwatch. This sensor can detect vibrations at a sampling rate of 1 kHz, which is accurate enough to not only sense the vibration code provided by the smartwatch, but also the dampening level caused by an individual's skin characteristic.

Figure 2 illustrates how the 'Vi Any Means' system is intended to be used. First, a user wears a smartwatch and activates their secret vibration code. Second, the user touches the target device with which she wants to authenticate. The target device embedded with the vibration sensor then analyzes whether the secret code it has received is correct, as well as the user's vibration dampening level. If the user is properly identified, the target device can be authenticated.

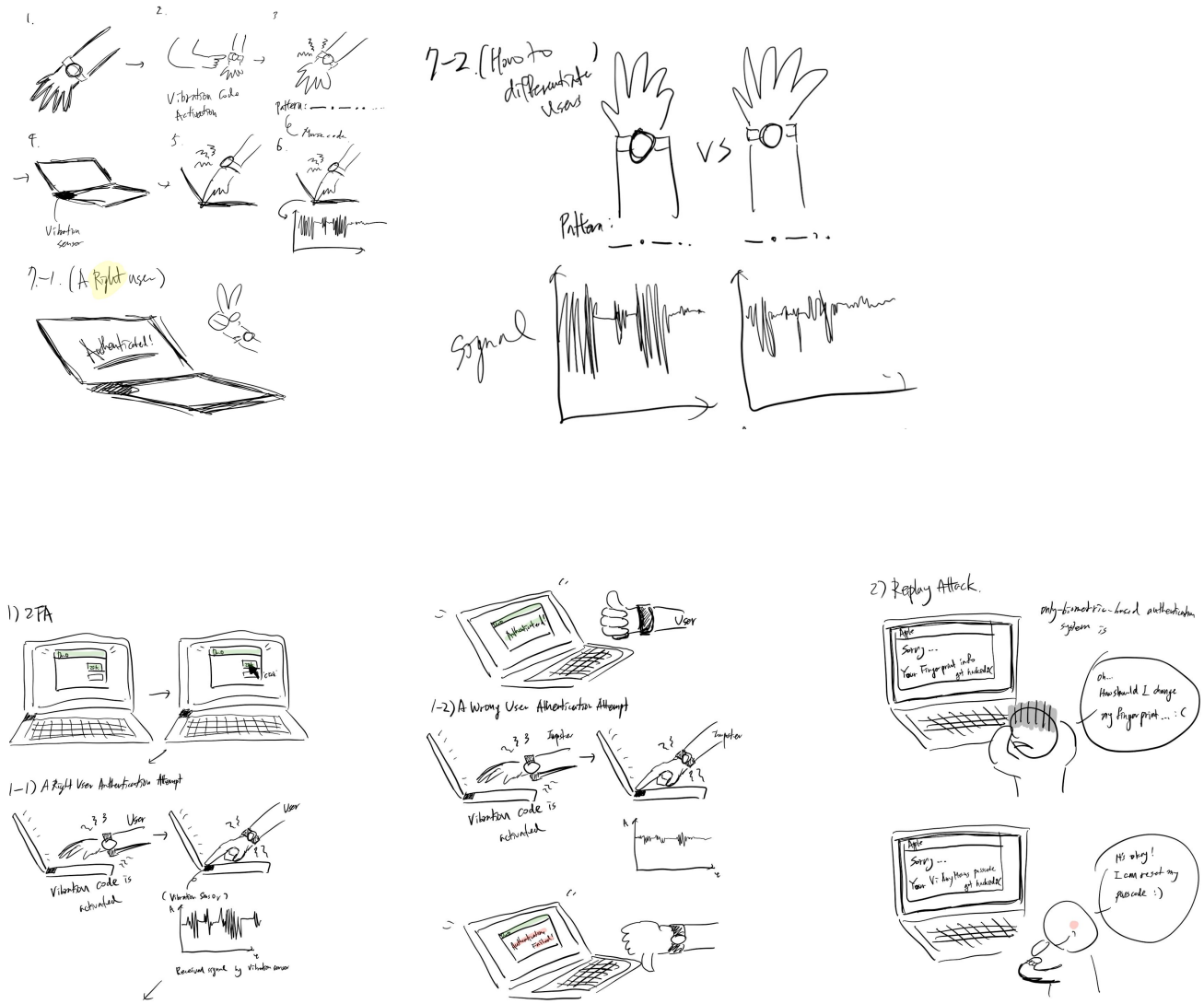

Figure 2. Steps of how to use the 'Vi Any Means' system

Figure 3 graphs a user's journey when signing up for Amazon's 2FA. The journey map indicates the pain points that a user may hit throughout their experience. Here we can see that there are several points where there is room for improvement in easing usability.

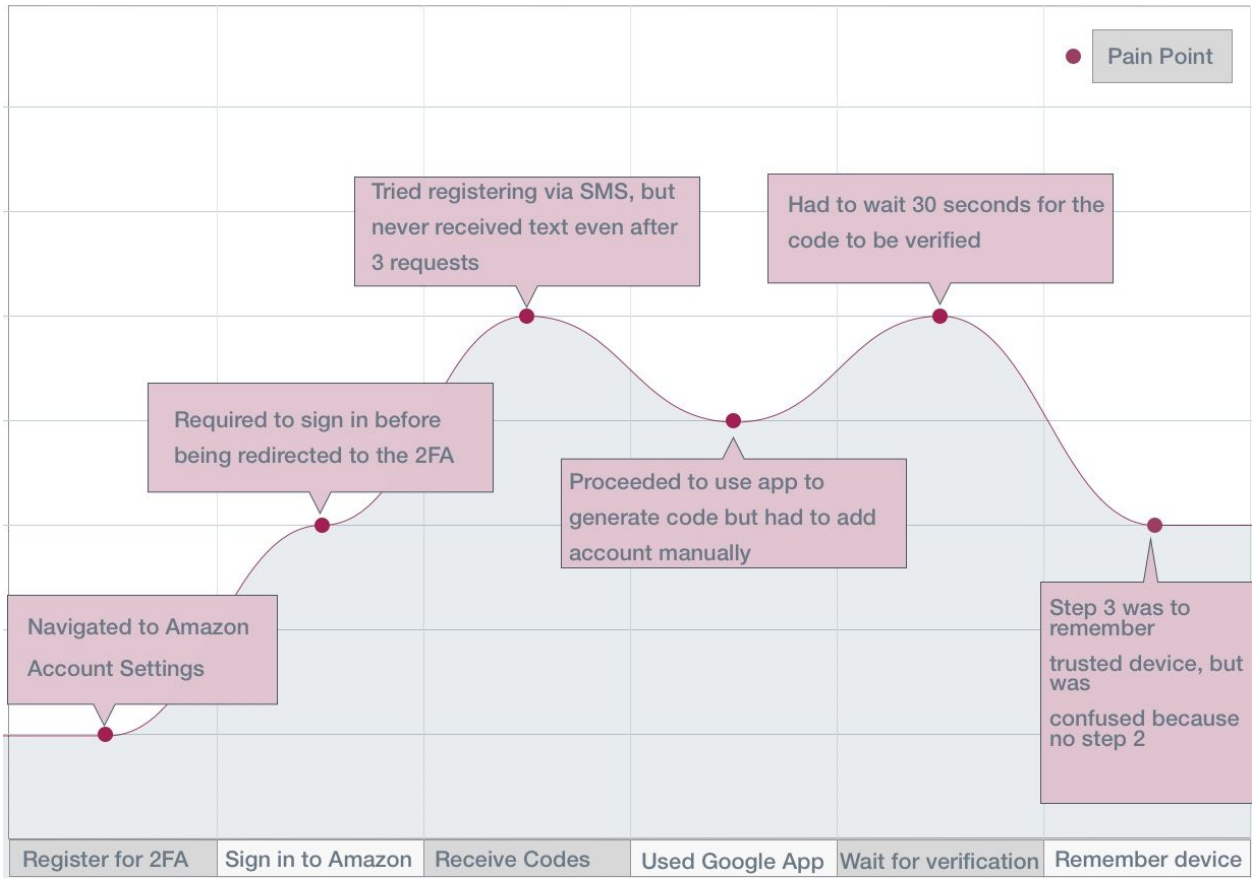

Figure 3. User journey map for signing up for 2FA on Amazon

SInce our study is a proof of concept, we will focus on answering the following questions:

R1) How effective are skin dampening vibrations as a method of authenticating individuals?
R2) Is Vi Any Means easier to use than common 2FA authentication methods like that for Amazon or Google?
R3) Is VI Any Means more usable than current 2FA methods?

To do this, we have setup the experiment to be conducted in three parts. The first part of our study is to answer R1 and determine if Vi Any Means is a feasible method of authentication. We will construct the hardware and conduct incremental experiments with the researchers to validate whether the skin dampening vibrations is able to differentiate between users correctly and effectively as well as authenticate correctly and effectively.

The second part of our study involves designing a wearable system interface as well as a compatible phone interface for users. We will follow the design heuristics set forth by Nielsen [10]. A cognitive walkthrough will be used to evaluate the usability of the system from the perspective of a novice user. We, the researchers, will complete the tasks of registering and authenticating using the system, making sure our system answers these questions:

- What is the user's task?
- Will the user know what the correct action is?
- Will the user be able to tell what action will achieve their task?
- Will the user receive any feedback regarding if the task was successful or not?

After developing a hi fidelity prototype, we will attempt to answer R2 and R3 by conducting a usability test. We will assess the system by evaluating it against Amazon or Google 2FA authentication. Participants will be given two timed tasks to complete: 1) registering and 2) authenticating. We will recruit 2 to 4 participants from within class or outside of class to pilot our study. Participants must be 18 years or older and will be recruited using a convenience sampling method. No compensation or benefits will be provided to the users except for the general knowledge that they are helping us in our research.

We will use a within-subjects design where participants are exposed to all experiment scenarios. To answer R2, we will compare timed results for the timed tasks to determine which method of authentications was easier. We will ask users to sign up for a 2FA that they are not already enrolled in, like Google or Amazon and time them to determine how long it takes for this task to be completed. Second, they will be given scenarios and asked to authenticate via 2FA, which will also be timed. Participants will then be given the same set of timed tasks but using the Vi Any Means system. To answer R3, upon completion of the tasks, we will ask the participants SUS questions to determine usability and ask them to explain their reasoning [11]. Finally, we will ask for an assessment about which system users would prefer to use. Total study time will take approximately one hour to complete per user.

References

[1] M. Faundez-Zanuy, "On the vulnerability of biometric security systems," in IEEE Aerospace and Electronic Systems Magazine, vol. 19, no. 6, pp. 3-8, June 2004.
[2] S. Hosseini, "Fingerprint vulnerability: A survey," *2018 4th International Conference on Web Research (ICWR)*, Tehran, 2018, pp. 70-77.
[3] Gupta, Richa & Sehgal, Priti. (2016). A survey of attacks on iris biometric systems. International Journal of Biometrics. 8. 145.
[4] Shankar, S., Udupi, V. R., & Gavas, R. D. (2016). Biometric verification, security concerns and related issues-a comprehensive study. Int. J. Inf. Technol. Comput. Sci.(IJITCS), 8(4), 42-51.
[5] Sungjae Hwang, Andrea Bianchi, and Kwang-yun Wohn. 2013. VibPress: estimating pressure input using vibration absorption on mobile devices. In Proceedings of the 15th international conference on Human-computer interaction with mobile devices and services (MobileHCI '13). ACM, New York, NY, USA, 31-34.
[6] T. Deyle, S. Palinko, E. S. Poole and T. Starner, "Hambone: A Bio-Acoustic Gesture Interface," 2007 11th IEEE International Symposium on Wearable Computers, Boston, MA, 2007, pp. 3-10.
[7] 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 (UIST '16). ACM, New York, NY, USA, 321-333.
[8] Chen, A., & Goh, W. (2015, June). Two Factor Authentication Made Easy. Retrieved from https://www.researchgate.net/publication/280027625_Two_Factor_Authentication_Made_Easy
[9] MPU-6050 Accelerometer Gyro. (n.d.). Retrieved from https://playground.arduino.cc/Main/MPU-6050#easy
[10] Nielsen, J. (2013, July 11). 10 Usability Heuristics for User Interface Design. Retrieved from https://www.designprinciplesftw.com/collections/10-usability-heuristics-for-user-interface-design
[11] System Usability Scale (SUS). (2013, September 06). Retrieved from https://www.usability.gov/how-to-and-tools/methods/system-usability-scale.html