UltraSonic Watch: Seamless Two-Factor Authentication through Ultrasound

Dimitra Zarafeta
HCI Group, University of Patras
Patras, Greece
d.zarafeta@upnet.gr

Christina Katsini
HCI Group, University of Patras
Patras, Greece
katsinic@upnet.gr

George E. Raptis
HCI Group, University of Patras
Patras, Greece
raptisg@upnet.gr

Nikolaos M. Avouris
HCI Group, University of Patras
Patras, Greece
avouris@upatras.gr

ABSTRACT

Two-factor authentication (2FA) provides an extra layer of security as it requires two pieces of evidence to be provided to an authentication mechanism before granting access to a user. However, people do not prefer 2FA; a reason for this is that 2FA requires performing extra actions. In this late-breaking work, we present *UltraSonic Watch* which provides a seamless 2FA through ultrasound. We report a small-scale within-subjects study ($N = 30$) which investigates the performance of *UltraSonic Watch* and the participants' experience (in terms of perception, preference, and willingness to adopt). The results are promising as they revealed that ultrasound can be used to provide an efficient 2FA mechanism, transparent to the users, who are positive in adopting such an approach to increase the security of the authentication process.

CHI'19 Extended Abstracts, May 4–9, 2019, Glasgow, Scotland UK

ACM ISBN 978-1-4503-5971-9/19/05.
https://doi.org/10.1145/3290607.3313093

CCS CONCEPTS

• **Security and privacy** → **Multi-factor authentication**; • **Human-centered computing** → **Human computer interaction (HCI)**; • **Computer systems organization** → *Sensors and actuators*;

KEYWORDS

Two-factor authentication (2FA); Ultrasonic Sensor; Internet of things (IoT); Seamless Authentication.

ACM Reference Format:

Dimitra Zarafeta, Christina Katsini, George E. Raptis, and Nikolaos M. Avouris. 2019. UltraSonic Watch: Seamless Two-Factor Authentication through Ultrasound. In *CHI Conference on Human Factors in Computing Systems Extended Abstracts (CHI'19 Extended Abstracts), May 4–9, 2019, Glasgow, Scotland UK*. ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3290607.3313093

INTRODUCTION

The rise of security breaches, digital crime, and internet fraud compounded by poor user password choices (e.g., creation of easily guessable passwords, reuse of passwords across multiple accounts) have turned the protection of users' information (e.g., authentication credentials) a challenging task for service providers. One way to mitigate the harm of password breaches is to use two-factor authentication (2FA) schemes. In 2FA, the passwords are coupled with another authentication factor. Such factors can be something the user knows (e.g., answers to security questions), something the user has (e.g., one-time token), or something the user is (e.g., biometric characteristics).

However, users still prefer password-only authentication over 2FA; a reason for this is the extra steps that the user must perform to log in [3]. For example, in Google 2-Step Verification (*G2SV*), the users enter their password and if it is correct, they receive a code in their phone via text, voice call, or mobile app. Then, they input this code to complete the login process. To minimize the steps required and the human interference, recent works have used radio-frequency transmitters [4], camera-based systems [2], acoustics and vision [11], acoustic signals [5], location-IoT [1] and ambient sounds [6, 9].

Focusing on sound-based 2FA, it works well in varying proximity scenarios both in indoor and outdoor environments [6], it is resilient to diverse attack types [5, 11], it supports cross devices [5], and it is easily deployable [9]. However, while it is usable [6, 9], audible (or near-audible) sounds could result unpleasant for people that are capable of hearing such sounds [9], ambient sounds could raise privacy issues [6], etc. To address such issues, in this late-breaking work, we present *UltraSonic Watch*, a 2FA mechanism based on ultrasound (i.e., the sound above human hearing range), which requires no interaction between the user and the device aiming to deliver seamless 2FA authentication. We also investigate whether ultrasound can be the basis of an efficient 2FA mechanism and we report on the user experience, perception, and acceptance of using such a mechanism.

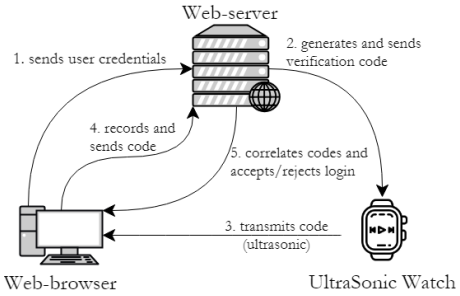

Figure 1: The conceptual architecture of the *UltraSonic Watch* 2FA system.

Figure 2: Testing the code transmission between the ultrasonic sensors.

Figure 3: Ultrasonic sensors were integrated into a traditional wristwatch to implement *UltraSonic Watch*.

PROTOTYPE

The conceptual architectural model of the 2FA scheme (Figure 1) consists of three main components: *Web-browser*, *Web-server*, and *UltraSonic Watch*. *UltraSonic Watch* is based on Arduino Uno and HC-SR04 ultrasonic sensors (Figures 2 and 3). *Web-server* is based on PHP and Apache; it is connected with a MySQL database. *Web-browser* is built with web technologies (HTML5, JavaScript); it communicates with *Web-server* via WebSocket. Considering that this paper focuses on the human-computer interaction aspect, we only provide an overview of the technical aspects of the *UltraSonic Watch*.

The scenario that our prototype employs is: i) the user enters their username and password in the client side (web-browser) application; ii) the user credentials are sent to the web-server; iii) the web-server verifies the credentials; iv) the web-server generates a verification code; v) the code is sent to the *UltraSonic Watch*; vi) the *UltraSonic Watch* transmits the encoded ultrasonic code to the client; vii) client records the encoded ultrasonic code and sends it to the web-server; viii) web-server extracts the code and compares it with the original one; ix) web-server notifies client whether the login is accepted or rejected; if rejected, a fallback code-based 2FA scheme is activated. In each communication channel, we considered security-related issues (e.g., code encryption).

We tested *UltraSonic Watch* in various conditions and we took precautions against diverse bad-case scenarios (e.g., communication loss between any of the components). Regarding positioning, *UltraSonic Watch* worked best (>99% success) for distance range: $[5cm, 60cm]$ and for relative angles range: $[-20^o, +20^o]$. After implementing *UltraSonic Watch*, we integrated it in a traditional wristwatch.

USER STUDY

We designed a controlled within-subjects experiment aiming to investigate whether *UltraSonic Watch*-based authentication performs better than a traditional 2FA scheme (we used *G2SV* scheme) and what the users' experience is (in terms of perception, preference, and willingness to adopt).

Method

Hypotheses.

H_1: *UltraSonic Watch* performs better than *G2SV*.
H_2: Participants have a better experience when using *UltraSonic Watch* than *G2SV*.

Instruments and metrics. To assess the performance (H_1) of each 2FA scheme, we measured the time to log in and the failure rates. To assess the users' experience (H_2), we used the questionnaire presented in [6], which collects information on the perceived quickness of the two schemes, participant's willingness to adopt any of the schemes, and participants' preference on the environment they would feel more comfortable to use the schemes.

Table 1: Information about the study participants.

Gender:	14 females, 15 males, 1 genderqueer
Age (in years):	$M = 24$, $SD = 5$, $min = 18$, $max = 45$
Occupation:	23 students, 7 industry employees
Experience with 2FA:	Only one participant had never used 2FA. The rest of the participants were familiar with 2FA, with *G2SV*-like schemes being the most common ones.

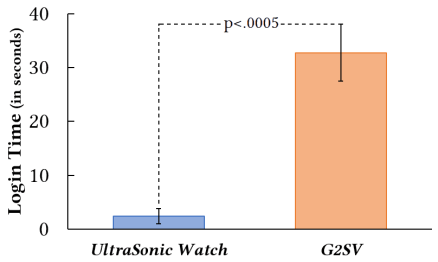

Figure 4: When using *UltraSonic Watch*, the users needed less time to log in the system (significant difference: $p < .0005$), than when using *G2SV*.

Participants. We recruited 30 participants of varying characteristics (Table 1). We used personal contacts and randomly invited people we came across at various study-cafés to take part in our study.

Procedure. After recruiting a participant, we provided them with information about the study process and the collected data (i.e., anonymous store, use only for research purposes) and they provided their consent. Then, we started the experiment. At first, each participant filled a form about demographic information, and then they logged into our system to read their emails and perform a visual search task using either the *UltraSonic Watch* or the *G2SV* scheme. Then, the participant performed the same task using the other scheme. We counterbalanced the sequence of the 2FA schemes to mitigate order effects. Thus, 15 participants used *UltraSonic Watch* first and then *G2SV*, and the other 15 participants vice versa. After using both 2FA schemes, each participant completed the questionnaire and performed an exit interview with a member of the research team.

Results

Login time. The paired-samples t-test revealed that when using *UltraSonic Watch*, the users needed 30.314 (95% CI, 24.913 to 35.716) fewer seconds to log in than when using G2VS, $t(29) = 11.479$, $p < .0005$, $d = 2.096$ (Figure 4). As expected, no order effects were found.

Failure rates. We did not witness any login failure for either of the two 2FA schemes. We speculate that this may be due to the participants' briefing, as we explained how the two 2FA schemes work.

Perceived quickness and security. The analysis of the post-test questionnaire answers (Wilcoxon signed-rank tests) revealed that *UltraSonic Watch* elicited a statistically significant median increase in perceived quickness compared to *G2SV* ($z = 4.761$, $p < .001$). Regarding the perceived security, most users (14/30) reported that they felt more secure when using *UltraSonic Watch* as the attackers could not track their actions (Table 2). The rest majority (13/30) reported no change in the security perception. Moreover, most of the participants (24/30) reported that they would prefer *UltraSonic Watch* to make an important transaction, such as a bank transfer.

Willingness to adopt. The Wilcoxon signed-rank tests revealed that *UltraSonic Watch* elicited a statistically significant median increase in willingness to adopt compared to *G2SV* if it was either mandatory ($z = 4.659$, $p < .001$) or optional ($z = 4.285$, $p < .001$). The main reasons for adopting *UltraSonic Watch* are that it is easy to use, it is quicker, it does not require human interference, and it feels more secure. Besides the positive aspects of the transparent and automatic process, the participants mentioned that the fact that they did not have any control of or feedback during the process could lead to doubts regarding the adoption of such schemes in critical scenarios (Table 2).

Table 2: Participants' comments.

Category	Comment
Perceived security:	P3: "*UltraSonic Watch was more secure since attackers couldn't see if or what I was typing.*"
	P7: "*An attacker has no means to steal ultrasounds.*"
	P20: "*Undoubtedly ultrasonic is more secure, as it is novel technology. At least, for now.*"
Willingness to adopt:	P2: "*UltraSonic Watch was much faster, so I'd pick it for login.*"
	P12: "*For secure transactions, I'd use the UltraSonic Watch.*"
	P13: "*Ultrasonic sensors can be easily customized and deployed, right? I'd use them not only in my watch but also my mobile.*"
	P19: "*I'd use UltraSonic Watch especially for my e-banking, but shouldn't it send me some kind of notification or await me to confirm an action?*
	P20: "*UltraSonic Watch was fast, easy-to-use, and automatic. I did less, and I was more secure.*"
	P25: "*I am positive using the UltraSonic Watch, but at the same time, I'm skeptical as neither I was aware nor I had control of the login process.*"

(continues to the next page)

Preferred environment. Regarding the context that the users would prefer to use each 2FA scheme, the McNemar's tests revealed that *UltraSonic Watch* would be preferred in working environments ($p = .004$) and libraries ($p = .009$). The participants reported that in the workplace the authentication should be performed quickly in order to save time or do not get distracted by non-primary tasks. Regarding the libraries, they would prefer a scheme that is non-distracting for other library users.

DISCUSSION

In this paper we presented *UltraSonic Watch*, which helped users to complete a 2FA login process more quickly than when using a traditional 2FA scheme; they felt that the process was completed in less time and more securely and they had an increased willingness to adopt it, especially in places that time matters (e.g., workplace) and places that require quiet (e.g., library).

An issue raised by the participants was the absence of control or feedback during the authentication process. Seamless authentication is a desirable characteristic mainly due to its non-distracting nature but this feature raises a contradiction. To provide an increased feeling of control and increase the willingness to adopt the scheme, it is essential to further investigate whether and how much human intervention could and should be incorporated in the process. If 2FA is a continuum with the seamless 2FA at the one end and the traditional 2FA at the other, it is vital to investigate where the golden section between the user interference and the user control lies, whether this is dependent on the type of the authentication service, and the optimal control/notification type (e.g., message, vibration).

In contrast to other sound-based 2FA schemes, *UltraSonic Watch* overcomes privacy issues associated with ambient sounds, as there is no transmission of data that may leak private information (e.g., transmission of recorded conversation during authentication attempt) or compromise user location. Moreover, it does not disclose authentication-related actions (e.g., when the code is transmitted) which can be associated with audible sounds (e.g., the attacker is aware of when the authentication process is active as they can hear, record, and reproduce the transmitted sound).

Given the reported advantages of the seamless 2FA and the low cost and the easy integration of ultrasonic sensors in information systems, the use of ultrasound is not only promising for providing better authentication solutions but also contributes to designing multifunctional wearable devices, as ultrasound has been used to measure distances, to provide haptic feedback and perception [10], to support hand gesture recognition [8], etc.

Limitations and Future Work

Our study has limitations, which are related primarily to the small and non-diverse study sample. Moreover, the study participants did not use *UltraSonic Watch* in their real life, but the authentication

(continues from the previous page)

Category	Comment
Preferred environment:	P2: "*When in work, I want to do things fast, so I'd use the watch.*"
	P9: "*No sounds means no distraction or frustration for other people.*"
	P25: "*I think it would work well both in quiet and noisy places, as it's based on sounds beyond human hearing spectrum.*"
	P28: "*Checking my emails or purchasing online are not tasks of my job; so, when needed, I want to complete such tasks securely and quickly.*"

scenario was realistic; we expect that our results will be replicated in more ecologically valid and real-life settings. Our future work includes: i) performing a longitudinal study with increased sample size and diversity, ii) integrating *UltraSonic Watch* in real-life scenarios, iii) investigating possible threats and providing workarounds, iv) investigating means of making the users feel more in control of the authentication process, and v) coupling 2FA with other factors (e.g., human factors [7]). Moreover, considering that ultrasound is audible to some animals, we should investigate the impact of *UltraSonic Watch* on them in our future attempts.

REFERENCES

[1] Ioannis Agadakos, Per Hallgren, Dimitrios Damopoulos, Andrei Sabelfeld, and Georgios Portokalidis. 2016. Location-enhanced Authentication Using the IoT: Because You Cannot Be in Two Places at Once. In *Proceedings of the 32Nd Annual Conference on Computer Security Applications (ACSAC '16)*. ACM, New York, NY, USA, 251–264.

[2] Mozhgan Azimpourkivi, Umut Topkara, and Bogdan Carbunar. 2017. Camera Based Two Factor Authentication Through Mobile and Wearable Devices. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 1, 3, Article 35 (Sept. 2017), 37 pages.

[3] Jessica Colnago, Summer Devlin, Maggie Oates, Chelse Swoopes, Lujo Bauer, Lorrie Cranor, and Nicolas Christin. 2018. "It's Not Actually That Horrible": Exploring Adoption of Two-Factor Authentication at a University. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (CHI '18)*. ACM, New York, NY, USA, Article 456, 11 pages.

[4] Alexei Czeskis, Michael Dietz, Tadayoshi Kohno, Dan Wallach, and Dirk Balfanz. 2012. Strengthening User Authentication Through Opportunistic Cryptographic Identity Assertions. In *Proceedings of the 2012 ACM Conference on Computer and Communications Security (CCS '12)*. ACM, New York, NY, USA, 404–414. https://doi.org/10.1145/2382196.2382240

[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 (MobiCom '18)*. ACM, New York, NY, USA, 401–415. https://doi.org/10.1145/3241539.3241574

[6] Nikolaos Karapanos, Claudio Marforio, Claudio Soriente, and Srdjan Čapkun. 2015. Sound-proof: Usable Two-factor Authentication Based on Ambient Sound. In *Proceedings of the 24th USENIX Conference on Security Symposium (SEC'15)*. USENIX Association, Berkeley, CA, USA, 483–498. http://dl.acm.org/citation.cfm?id=2831143.2831174

[7] Christina Katsini, Christos Fidas, George E. Raptis, Marios Belk, George Samaras, and Nikolaos Avouris. 2018. Influences of Human Cognition and Visual Behavior on Password Strength During Picture Password Composition. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (CHI '18)*. ACM, New York, NY, USA, Article 87, 14 pages.

[8] Jess McIntosh, Asier Marzo, Mike Fraser, and Carol Phillips. 2017. EchoFlex: Hand Gesture Recognition Using Ultrasound Imaging. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (CHI '17)*. ACM, New York, NY, USA, 1923–1934. https://doi.org/10.1145/3025453.3025807

[9] Prakash Shrestha and Nitesh Saxena. 2018. Listening Watch: Wearable Two-Factor Authentication Using Speech Signals Resilient to Near-Far Attacks. In *Proceedings of the 11th ACM Conference on Security & Privacy in Wireless and Mobile Networks (WiSec '18)*. ACM, New York, NY, USA, 99–110. https://doi.org/10.1145/3212480.3212501

[10] Graham Wilson, Thomas Carter, Sriram Subramanian, and Stephen A. Brewster. 2014. Perception of Ultrasonic Haptic Feedback on the Hand: Localisation and Apparent Motion. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '14)*. ACM, New York, NY, USA, 1133–1142. https://doi.org/10.1145/2556288.2557033

[11] Bing Zhou, Jay Lohokare, Ruipeng Gao, and Fan Ye. 2018. EchoPrint: Two-factor Authentication Using Acoustics and Vision on Smartphones. In *Proceedings of the 24th Annual International Conference on Mobile Computing and Networking (MobiCom '18)*. ACM, New York, NY, USA, 321–336. https://doi.org/10.1145/3241539.3241575