Clap On, Clap Off: Usability of Authentication Methods in the Smart Home

Weijia He, Juliette Hainline, Roshni Padhi, Blase Ur
University of Chicago
{hewj, juliettehainline, padhi, blase}@uchicago.edu

ABSTRACT

Despite rapid advancements in authentication technologies, little user testing has been conducted on the various authentication methods proposed for smart homes. Users' preferences about authentication methods may be affected by their beliefs in the reliability of the method, the type and location of devices for which they must authenticate, the effort required for successful authentication, and more. In this paper, we provide insight into users' concerns with these methods through a 46-participant user study. In particular, we seek to understand users' preferences towards different authentication methods in terms of the perceived security and usability implications of each method.

1. INTRODUCTION

Smart-home devices are increasing in popularity. Many devices have versatile and multi-modal interfaces. For example, users can verbally tell their smart voice assistant to play music or set up a schedule to turn their smart lights off automatically at night. This functionality is convenient as many actions can be done without the user physically approaching the device. Despite the rich modalities of this interaction, many widely deployed smart-home devices rely on usernames and passwords for authentication [9].

It is well known that passwords can be risky without proper generation and management [8]. This dilemma worsens for smart-home devices because few of these devices have an interface for entering a username and password. As a result, users are forced to carry a smartphone with them to authenticate themselves. If authentication can only be performed when people are using their smartphone, though, authentication is inconvenient. It is also open to forgery if other members of the household pick up the smartphone.

In recent years, many researchers have tried to develop authentication alternatives to passwords that rely on using machine learning to recognize a user's immutable characteristics or tendencies. For example, facial recognition through photos or videos is a widely used approach already implemented by many manufacturers, such as the iPhone's Face ID [1]. Beyond face recognition, researchers have often relied on sound. Chauhan et al. developed an authentication method based on one's breathing sound [2]. The sound of footsteps has been researched as a way to increase the accuracy of identification by Chen et al. [3]. Similarly, there is also research about authenticating people by their gait [6], human-device interaction [10], body shape [5], and more.

Little research, however, has been conducted to understand users' interest in these novel authentication methods. Since the essence of these types of authentication methods involves collecting information about users, it is important to make sure that users are comfortable with these implicit authentication methods.

Therefore, we ask the following questions in this paper:

- What factors affect users' preferences in authentication methods in smart homes? What do they value most?
- What can we do to make these novel authentication methods more appealing to users?

In an effort to answer these two questions, we conducted an online user study with 46 participants from Amazon's Mechanical Turk to capture their perceptions towards five different authentication methods. These five authentication methods are categorized by the type of information they collect for authentication.

2. SURVEY AND RESULTS

In this section, we describe our survey design and our results.

2.1 Recruitment and Survey Structure

We recruited participants on Amazon's Mechanical Turk for an IRB-approved research study about "smart-home devices." We designed the survey to take about 25 minutes and compensated participants $5.00.

The survey was divided into three sections. The first section introduced participants to the survey scenario. After that, participants were introduced to an authentication method. Participants were asked to imagine that they were the primary owner of five smart-home devices, outlined in Table 1. We selected these five categories of devices because they are the top smart-home categories on Amazon. A specific product, link, and picture was given to help the participant understand the device. Though potentially biasing, our pilot testing suggested this was necessary.

Participants were then asked a series of questions which repeated for each of the five authentication methods outlined

USENIX Symposium on Usable Privacy and Security (SOUPS) 2018.
August 12–14, 2018, Baltimore, MD, USA.

Smart-Home Devices	Authentication Methods
Camera	Activity-based
Lights	Audio-based
Lock	Biometric
Thermostat	Camera-based
Voice assistant	Physical Possession

Table 1: The five devices we based the study around and the five authentication methods we tested.

in Table 1. The definition of these authentication methods, which was presented to participants at the beginning of each loop one at a time, can be summarized as follows:

- **Activity-based Authentication** is based on collecting users' motion data or interaction history.
- **Audio-based Authentication** is based on recording sound continuously.
- **Biometric Authentication** is based on collecting users' biometric features.
- **Camera-based Authentication** is based on videotaping surroundings continuously.
- **Authentication by Physical Possession** is based on tracking physical possession.

It is worth noting that by our definition, facial recognition in a security camera should be categorized as camera-based authentication instead of biometric authentication. To enable facial recognition, the camera has to keep videotaping, which gives the camera the ability to collect more information beyond users' faces. The same applies to voice recognition, which requires constant recording and thus should be categorized as audio-based authentication instead of biometric authentication.

Questions that followed focused on enabling the authentication method, the acceptability of data collection/storage requirements for the method, the acceptability of potential false accepts/rejects, and the comparative preference of using the method relative to traditional password-based authentication. Finally, participants reported the following demographic information: if they own any smart-home devices; gender; age; highest education completed; and if they have an education or job in a technical field.

2.2 Results

48 participants recruited from Amazon's Mechanical Turk filled out our survey. Two participants' responses had to be discarded due to unrelated content and incompleteness. Of the remaining 46 participants, 70.2 % identified as male, while 29.8 % identified as female. The age range of participants was 18-64, with 87.2 % of participants between 18 and 34. A majority, 68.1 %, reported a two-year or higher educational degree. Most participants (85.1 %) did not report having educational or job experience in a technical field. Finally, 62 % reported owning a smart-home device.

2.2.1 *Preference in Authentication Methods*

Figure 2 displays participants' stated desire to enable the different authentication methods we studied. Biometric authentication was the clear winner in participants' reported desires. Participants were most willing to use biometric authentication because of a sense of familiarity, security, and

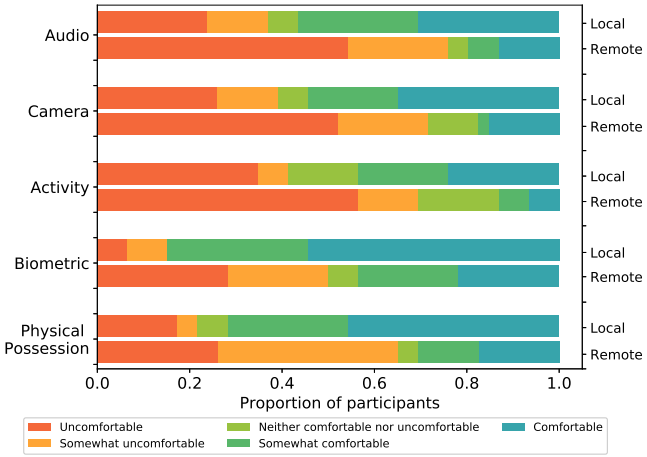

Figure 1: Participants' expressed comfort with local and remote storage for the authentication methods.

their stated perception that biometrics are difficult to fake, especially for fingerprints.

In contrast, activity-based authentication was the least desired authentication method. Participants were skeptical of the ability to detect activity or voice successfully. As P10 stated, "I don't think movements can be distinct enough to verify my identity. What if I come home drunk and don't walk the way I usually do?" For audio- and camera-based authentication methods, imitation attacks were participants' biggest concern. For instance, P15 wrote, "I do not trust this method of authentication, anyone can just copy my voice!"

A theme among all authentication methods was that participants felt some smart-home devices required more "secure" authentication methods than others. As P26 explained, "I think that an audio-based authentication for smart speaker, smart thermostat and smart lights is sufficient. It will increase the ease of use of these devices and I don't personally feel the security level needs to be significantly higher on these devices."

Interestingly, few participants mentioned privacy when they initially explained why they did not want to use audio- and camera-based authentication. After subsequent questions in the survey focused on data collection required by these two categories of authentication methods, 10-15 % of participants became less willing to use them. Most people considered these two authentication methods to be "too intrusive."

2.2.2 *Storage*

We also measured participants' comfort towards different strategies for storing the data necessary for each method. Figure 1 shows that, for all methods, participants felt more comfortable about data being stored locally.

However, for many machine learning-based authentication methods, it is computationally expensive or even intractable to run the whole model locally, which means that storing the data on manufacturers' servers is inevitable. Under these circumstances, participants reported feeling better if the information stored is about their fingerprints or indoor location, instead of audio, video, and activities. With that being said, the idea of storing data somewhere else is still unsettling. Even for biometric authentication, the method that

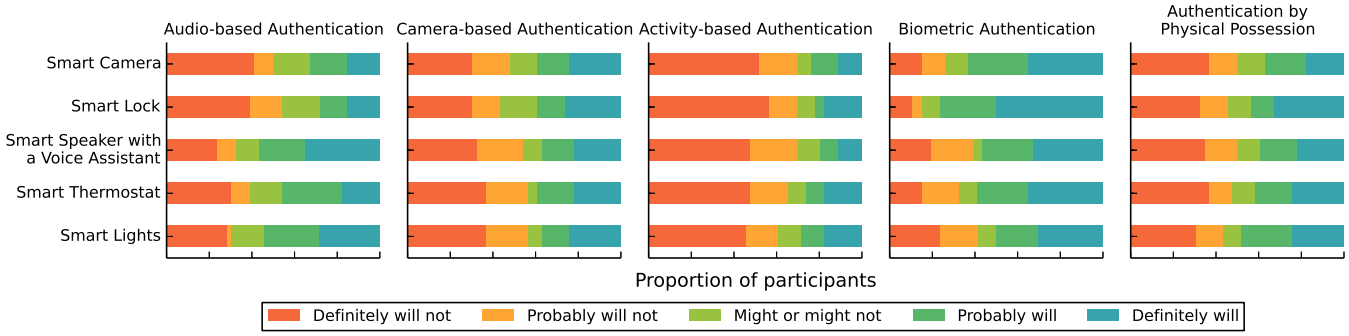

Figure 2: Participants' reported willingness to enable authentication methods on different smart devices before knowing details about the data that would need to be collected to enable that method.

inspired the least amount of concern, 50 % of participants felt at least somewhat uncomfortable with the idea.

2.2.3 *False Rejection*

Most participants reported a somewhat high tolerance of being falsely rejected by the smart-home device in a given authentication session. The majority of participants reported they would give up after at most three attempts, as shown in Figure 3. However, this answer may suffer from social desirability bias (meaning that they may have answered what they think they should have answered, instead of what they actually would do in real life). Even typing in a password three times while logging into a website is cumbersome, and making three attempts may be even more onerous for the authentication methods we studied.

Participants reported a low tolerance in terms of how frequently they could tolerate this false rejection occurring, as shown in Figure 4. We found that the participants' tolerated frequency should be less than one time per month. However, responses from participants also showed a relatively higher tolerance towards biometric authentication. This difference might be due to the ease of the authentication process.

2.2.4 *Account Authentication*

As shown in Figure 5, participants were more willing to use traditional account authentication (i.e., authentication with a username and password) than most of the alternative authentication methods we explored.

The exception was biometric authentication, which participants tended to report preferring over account authentication. Participants preferred biometric authentication because they felt it offered a more secure and convenient way of authenticating themselves. P29 wrote, "Having to enter usernames and passwords is obsolete in my opinion. Keeping it quick with biometric and audio authentication is the way that I'd wish to operate these devices."

For the other authentication methods, participants had a variety of reasons for preferring account authentication. For privacy reasons, participants preferred account authentication to audio and camera methods. For reliability reasons, participants preferred account authentication to audio, camera, and activity-based methods.

3. DISCUSSION

In this section, we discuss the limitations of our study, the implications of our results, and potential future directions.

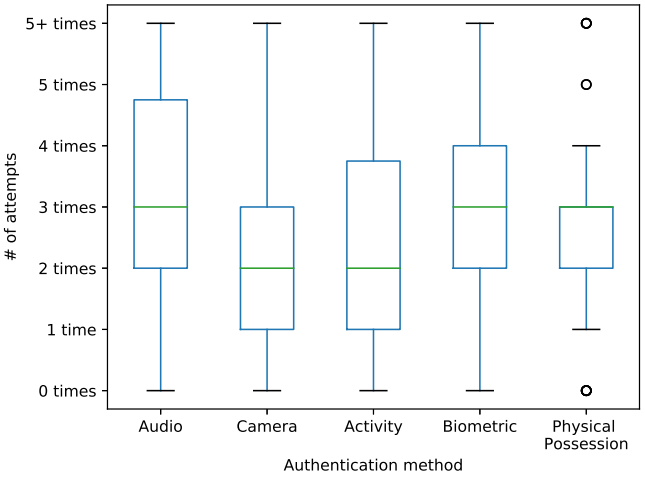

Figure 3: The number of falsely rejected authentication attempts participants reported being willing to tolerate for the different methods.

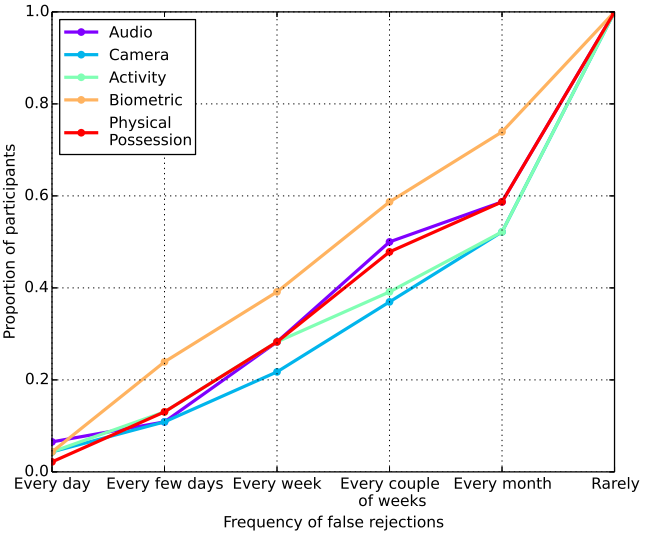

Figure 4: The proportion of participants who reported being willing to tolerate given frequencies of false rejections in authentication.

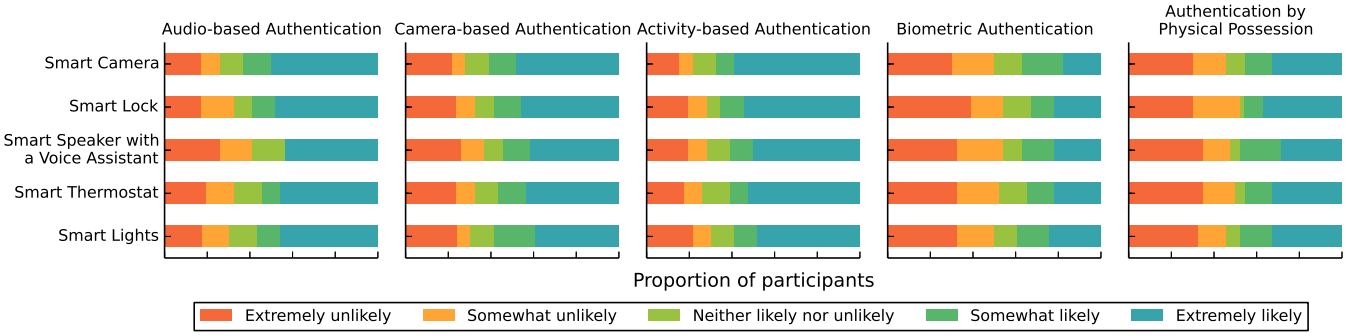

Figure 5: Participants' reported likelihood of choosing traditional account authentication (i.e., a username and password) *over* each of the alternative authentication methods shown for each type of device.

3.1 Limitations

Similar to most user studies, responses may be affected by self-report biases. In addition, participants may have answers affected by social desirability bias. Nevertheless, this formative study can help determine whether a user would consider using an authentication method. This information is crucial for researchers looking to innovate with new authentication methods or expand upon existing ones.

3.2 Security in Authentication

Based on their responses, many participants were aware of the potential for imitation attacks in audio- and camera-based authentication and expressed their concerns about them. To ease their concerns, we believe that liveness detection, which can tell if the biometric feature is from a present and real human being, should be an indispensable part of these mechanisms. However, current liveness detection for audio-based authentication usually requires an accessory (e.g. a smartphone [11, 12]) to achieve its goal, which violates users' preference for hands-free authentication and thus hampers adoption. Liveness detection for camera-based authentication may be insufficient because attackers can impersonate another person or bypass the authentication system by wearing specially crafted eyeglasses [7]. More research needs to be done to understand the attack space of such authentication methods, as well as how to cope with these potential attacks in a more usable way.

3.3 Privacy in Authentication

In our study, we discovered that participants mostly made their decisions based on security, convenience, and reliability. However, after revealing potential data collection required by these methods, more participants listed privacy as another concern they have towards these new authentication methods. This shows us that even though some people do value their privacy, they are not clear about the potential privacy threats existing in a smart-home environment, which is consistent with the findings from another study conducted by Gerber et al. [4]. Therefore, we believe it is important for researchers to approach continuous authentication with great care, clearly communicating underlying privacy issues and limiting unnecessary information collection.

Though the goal of continuous authentication is to provide an entirely immersive experience in a smart home, letting every smart home device know who is interacting with it and offering customized services accordingly, it is unnecessary to expose users to untrusted manufacturers all the time; users do not interact with these devices constantly. This is especially true when it comes to audio or video recordings that possibly contain very sensitive information. Contextual factors might help mitigate such situation. For example, because both audio- and camera-based authentication requires proximity, these authentication methods should not be activated when primary users are not in the same room with related devices. Such measurement can prevent unnecessary recording from happening. However, more research is required to solve the issue of unwanted recording.

Moreover, figuring out how to make users aware of existing privacy issues in their smart homes is another possible research direction. Without traditional modalities such as screens or keyboards, we can no longer inform users about potential information access in the same way as we do on our smartphones. It is impossible for users to take any action to protect their privacy when they are not actively aware of potential privacy threats imposed by smart devices.

3.4 Usability Evaluation for Authentication

Due to the fact that many of these novel authentication methods are based on machine learning, it seems intuitive and reasonable to adopt similar evaluation methods that are well accepted by research in machine learning.

However, designing authentication methods for a smart home is a specific application of machine learning, which has its own context and involvement with humans. To make these novel approaches fit into the context of this specific problem, it is important to analyze the context of a smart home and users' thought processes so that we can understand where the obstacles lies and which approach will be the best.

The first problem of current machine learning-based evaluation is that it is not clear how high precision and recall should be to match users' expectations. Frequent false rejections can easily annoy users and make them turn off the authentication process entirely, while false acceptances can impose security threats to users and can scare users away from trying these novel methods. Without measuring users' expectations of false accepts and false rejects, the only way to evaluate the result is through subjective judgment, which is hard to justify.

As discussed in Section 2.2, users have a relatively low tolerance towards false rejection in terms of frequency. False rejections should occur less than once per month. With this information at hand, we calculate the acceptable false reject

rate (FRR) based on estimation of usage frequency. For example, for a family with 3 people, they could use a smart lock 180 times per month if they have different schedules, which means the acceptable FRR for this family should be less than 0.55 %, which is lower than many proposed authentication methods. That said, if the feature itself is not very frequently used and not very sensitive, the standard could be looser than in the scenario above.

3.5 Access Sharing

Because of the nature of a smart home, adding new users to the system is an essential part of using smart-home devices. However, training smart devices to know a new person can be very troublesome. Features used for identification may vary under different situations. Therefore, it is important for the devices to capture as much data as they can to train the model so that they can identify users in different environmental contexts, which could require a huge amount of time and effort. It is not realistic to require someone to go through all of this trouble just for temporary access.

Admittedly, making the registration process easy for machine learning-based authentication is difficult. However, the effort that a user is willing to make should be proportional to the rewards they receive from it. Therefore, it would be better to authenticate users with permanent and temporary access differently. As a permanent resident in the house, it is possible that people are more willing to put more effort into registering. For visitors who only stay in the house for a limited time-span, a temporarily enabled physical token might be sufficient.

4. CONCLUSION

In this paper, we began to examine what factors will affect users' preferences for post-password authentication methods in the smart home, as well as what we can do to make these authentication methods more appealing to users. For the first question, we ran a user study to understand users' reasoning behind their choices. We discovered some commonly shared standards, such as security, speed, reliability, and familiarity. After understanding the factors that will affect users' preferences, we briefly discussed how we can improve authentication methods in both design and evaluation to ease users' distrust toward new methods.

5. ACKNOWLEDGMENTS

We thank Heather Zheng for her assistance and feedback. This material is based upon work supported by the National Science Foundation under Grant No. CNS-1756011.

6. REFERENCES

[1] Apple. About Face ID advanced technology. `https://support.apple.com/en-us/HT208108`, 2017. Accessed: 2018-05-31.

[2] J. Chauhan, Y. Hu, S. Seneviratne, A. Misra, A. Seneviratne, and Y. Lee. BreathPrint: Breathing Acoustics-based User Authentication. *Proceedings of the 15th Annual International Conference on Mobile Systems, Applications, and Services - MobiSys '17*, pages 278–291, 2017.

[3] Y. Chen, W. Dong, Y. Gao, X. Liu, and T. Gu. Rapid: A multimodal and device-free approach using noise estimation for robust person identification. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, 1(3):41, 2017.

[4] N. Gerber, B. Reinheimer, and M. Volkamer. Home sweet home? Investigating users' awareness of smart home privacy threats. 2018.

[5] A. Kalyanaraman, D. Hong, E. Soltanaghaei, and K. Whitehouse. Forma track: Tracking people based on body shape. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, 1(3):61, 2017.

[6] M. Muaaz and R. Mayrhofer. An analysis of different approaches to gait recognition using cell phone based accelerometers. In *MoMM*, 2013.

[7] M. Sharif, S. Bhagavatula, L. Bauer, and M. K. Reiter. Accessorize to a crime: Real and stealthy attacks on state-of-the-art face recognition. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pages 1528–1540. ACM, 2016.

[8] B. Ur, J. Bees, S. M. Segreti, L. Bauer, N. Christin, and L. F. Cranor. Do users' perceptions of password security match reality? In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, pages 3748–3760. ACM, 2016.

[9] B. Ur, J. Jung, and S. Schechter. The current state of access control for smart devices in homes. In *Workshop on Home Usable Privacy and Security (HUPS)*. HUPS 2014, 2013.

[10] X. Wang, T. Yu, M. Zeng, and P. Tague. Xrec: Behavior-based user recognition across mobile devices. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, 1(3):111, 2017.

[11] L. Zhang, S. Tan, and J. Yang. Hearing your voice is not enough: An articulatory gesture based liveness detection for voice authentication. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, pages 57–71. ACM, 2017.

[12] L. Zhang, S. Tan, J. Yang, and Y. Chen. Voicelive: A phoneme localization based liveness detection for voice authentication on smartphones. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pages 1080–1091. ACM, 2016.