Is the Future of Authenticity In Our Heads?

Moving Passthoughts From the Lab to the World

Nick Merrill, Max T Curran, John Chuang
BioSENSE, UC Berkeley School of Information
Berkeley, California, USA
ffff,mtcurran,john.chuang@berkeley.edu

ABSTRACT

Passthoughts authentication, in which a user thinks a secret thought to log in to services or devices, provides two factors of authentication (knowledge and inherence) in a single step. Since its proposal in 2005, passthoughts enjoyed a number of successful empirical studies. In this paper, we renew the promise of passthoughts authentication, reviewing the main challenges that passthoughts must overcome in order to move from the lab to the real world. We propose two studies, which seek different angles at the fundamental questions we pose. We conclude with future oppportunities, and challenges, for passthoughts' broader deployment as a tool for authentication. In doing so, we raise novel possibilities for authentication broadly, such as "organic passwords" that change naturally over time, or systems that reject users who are not acting quite "like themselves."

KEYWORDS

passthoughts, authentication, usable security

ACM Reference format:

Nick Merrill, Max T Curran, John Chuang. 2017. Is the Future of Authenticity In Our Heads?
Moving Passthoughts From the Lab to the World. In
Proceedings of New Security Paradigms Workshop, Islamorada, Florida, USA, October 2017 (NSPW '17), 10 pages.
DOI: 10.475/123_4

1 INTRODUCTION

Usable authentication is a long-standing problem in computer security. Traditional passwords are easy to guess and difficult to remember, while biometric authenticators like fingerprints are easy to steal and difficult to change. Possession of tokens or keys are susceptible to loss, and the use of multiple factors (such as password and SMS) require multiple steps, hindering wider adoption.

NSPW '17, Islamorada, Florida, USA

DOI: 10.475/123_4

First proposed by [39], "passthoughts" authentication allows users to to submit both a knowledge factor (i.e., a secret thought) and an inherence factor (i.e., the unique way that thought is expressed) in a single step, by performing a single mental task [20]. Since its original proposal, passthoughts has been validated in lab settings, even with consumer-grade devices [11] and in-ear EEG earbuds [14]. The protocol appears to be robust against impersonation attacks [20].

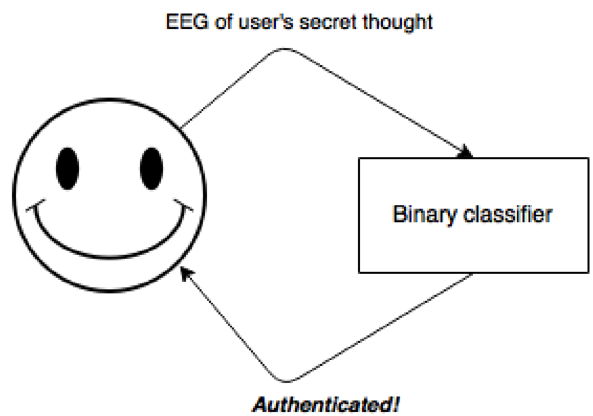

Figure 1: A passthought authenticator.

While recent work is heartening, passthoughts remains confined, for now, to the lab. This paper reviews the immediate questions that must be addressed if passthoughts is to move into everyday life. First, we must understand the real usability properties of passthoughts. The usability of passthoughts authentication will depend not only on its performance in ecologically valid contexts, but also on people's attitudes about brainwaves, EEG, and biosensing generally (Section 3). Second, we must test passthoughts in a variety of conditions: ambulatory settings, under different levels of stress, drowsiness, caffeine or alcohol, etc. This statistical analysis will help us understand the space of possible passthoughts, and how passthoughts change over time (Section 4).

This paper motivates and contextualizes two studies that could begin to address these challenges (Section 5). While these studies attack two sides of passthoughts' chances as a real-world technology this study serves not just to propose solutions, but to raise questions about what authentication could and should be able to do. While passthoughts is not without risks (Section 6), it raises the possiblity for several interesting paths, including exploration of systems that could enable novel types of authentication (Section 7).

2 BACKGROUND

Authentication seeks to prove that a user is who they claim to be. In computer security, authenticators are classified into three types: knowledge factors (e.g., passwords and PINs), possession factors (e.g., physical tokens, ATM cards), and inherence factors (e.g., fingerprints and other biometrics).

An ongoing problem in authentication lies in balancing strong security (i.e., multiple factors of authentication) with usability. As an example, major industry players such as Google and Facebook have strongly encouraged their users to adopt two-factor authentication (2FA), in which a user enters his or her password (a knowledge factor), and subsequently receives a code on their cellphone (a posession factor).

However, submitting two different authenticators in two separate steps has frustrated wide adoption due to its additional hassle to users. The Apple iPhone, for instance, already supports device unlock using either a user-selected passcode or a fingerprint. The device could very well support a two-step two-factor authentication scheme if desired. However, it is easy to understand why users would balk at having to enter a passcode *and* provide a fingerprint each time they want to unlock their phone.

2.1 One-step, multi-factor authentication

To assist with the usability issues surrounding multi-factor authentication, passthoughts aims to provide two factors of authentication in a single step. A single mental task, or passthought, provides both a knowledge factor (a chosen secret thought) with an inherence factor (the way that thought is expressed for an individual) [11, 20]. Using a custom sensing device, passthoughts could provide an additional posession factor, all in the same step.

Other work has attempted to provide multiple factors of authentication in one step. Some work has tested behavioral authentication methods such as keystroke dynamics, or voice. In both cases, the knowledge factor (password or passphrase) and inherence factor (typing rhythm or speaker's voice) are employed [28]. In contrast, the Nymi band supports one-step two-factor authentication via the inherence factor (cardiac rhythm that is supposed to be unique to each individual) and the possession factor (the wearing of the band on the wrist) [32]. Custom-built EEG devices could incorporate an added possession factor to the already two-step authentication provided by passthoughts [13].

Authenticators are susceptible to a variety of attacks. One common attack on passwords is "shoulder surfing," in which an attack uses visual or other cues to steal, or improve the chances of guessing, a target's chosen secret. Passthoughts mitigates this attack by nature of the mental gesture: since the expression of a passthought is not externally visible, the authenticator is impervious to shoulder surfing attacks.

2.2 Passthought authentication

The use of EEG as a biometric signal for user authentication has a short history. In 2005, Thorpe et al. motivated and outlined the design of a passthoughts system [39]. Since 2002, a number of independent groups have achieved low (less than 1%) false acceptance rates using multi-channel sensors placed on the scalp [4, 26, 33, 34]. In 2013, one group showed that similar accuracy can also be achieved using a consumer-grade single-channel sensor [11]. In particular, the lack of signal diversity from multiple EEG channels can be overcome by allowing the users to choose their own personalized passthoughts (e.g., sing their favorite song in their head). There are two significant consequences of this result. First, the passthoughts approach is no longer constrained by the high cost (> $10,000 USD) and low usability (gel-based electrodes; aesthetic challenges of an EEG cap) of medical-grade multi-channel devices. Second, because users can choose and easily change their secret mental task, this approach can support one-step two- factor authentication via the simultaneous presentation of the inherence factor (brainwave signatures due to the unique folding structures of the cortex) and the knowledge factor (the secret mental task) [10].

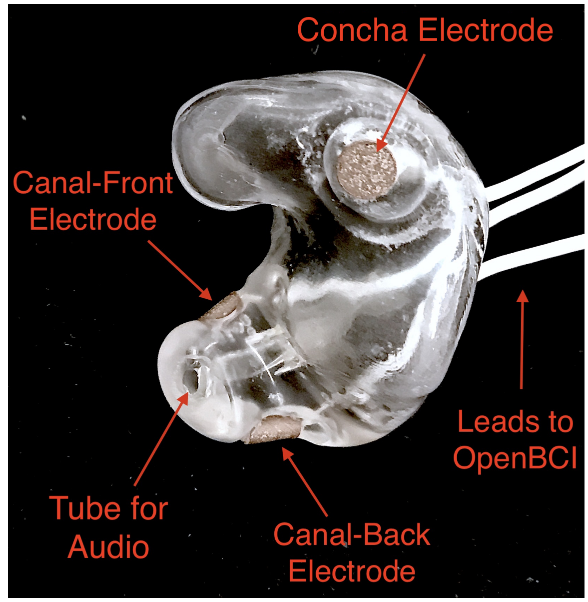

Figure 2: A custom-fit in-ear EEG device as used in Curran et al, 2017

2.3 Passthoughts using in-ear EEG

Even consumer-grade headsets can be uncomfortable to wear, and are awkwardly visible to outside observers. Earbuds present a more discreet, comfortable location for an EEG sensor, as earbuds are already commonly worn.

Research in in-ear EEG is only several years old. Nonetheless, the concept has attracted a lot of attention because of the discreetness factor of in-ear EEG over traditional scalp-based EEG. A research team at the Imperial College London and Aarhus University published a landmark paper in 2011 that introduced the concept of in-ear EEG, demonstrating for the first time the feasibility of recording brainwave signals from within the ear canal [25]. Follow-up work from the same group demonstrated its ability to produce signal-to-noise ratios comparable to those from conventional EEG electrode placements, robustness to common sources of artifacts, and use in a brain-computer interface (BCI) system based on auditory evoked potentials and visual evoked potentials [21, 22, 24].

[14] was the first to merge in-ear EEG with passthought authentication, using a modified consumer grade EEG device with a single electrode, achieving approximately 80 percent authentication accuracy. Ongoing work from the same authors investigates the use of custom-fit earbuds with multiple embedded electrodes 2.3. Lending credibility to that study's claim that in-ear EEG could one day become feasible in consumer devices, United Sciences recently announced a consumer "hearable" (in-ear wearable) called The Aware, which will measure EEG from the ear, among other biometrics.

3 USER ATTITUDES AND PERCEPTIONS

While past work makes passthoughts less visible with more discreet form-factors, a large question still remains: What sense would people make of passthoughts, as a technology, in their everyday life? This question begs not only user-centered design studies with passthoughts itself, but more general questions about what EEG means to people, and what people believe EEG data can reveal about them. Past work has established that people tend to ascribe almost magical abilities to brain-scanning devices, even subjects with specific training in the limitations of brain-scanners [2]. Will these attitudes scare away, or attract wider adoption? This section outlines common concerns around "mind-reading" machines, and how they relate to EEG and passthoughts specifically.

3.1 Contending with mind-reading machines

Biosensing devices in general raise many questions about privacy for end-users, typically around the meaning of the data produced by particular devices. For example, you might be eligible for an insurance discount if you wear a FitBit [5] (depending, of course, on what readings the FitBit produces [7]). But, would you wear a device in the workplace [35], if your manager used it to track your productivity? If biosensor data can be used in the courtroom [12], could not pervasive biosensing help to *predict* crime [38]? After all, one study suggests that probability of involvement in violent crime can be predicted from one's resting heartrate [23]. In all of these examples, biosensing technologies blur the line between *sensing bodies* and *sensing minds*. Now, when people decide to buy sensor-equipped consumer devices [36], or get sensed passively by devices integrated into the walls and ceilings [1] or city streets [40], end-users will need to contend with the prospect of mind-reading machines.

If people *think* a certain technology measures aspects of mind, it will certainly affect the way they engage with that technology, whether or not it works the way they expect [2]. Meanwhile, if they think that a given technology does *not* measure their mind, when in fact it does, users may suffer a breach of what Nissenbaum might call the "appropriateness of the flow of information" [15]. In both cases, knowing what people expect will help us anticipate their needs and concerns.

If we wish to understand what role passthought authentication *could* play in day-to-day life, we must view it both through the lens of potential privacy concerns, *and* through the lens of possible opportunities for self-reflection and self-understanding. Of course, users' attitudes will not be fixed: they will evolve over time, as users observe the device in action, and correlate its judgments with their own lived experiences [30]. In the next section, discuss how EEG as a sensing modality motivates questions around the meaning people may build around passthought authenticators.

3.2 What (do you think) EEG can reveal about a person?

The survey we report on here, currently in-progress, examines how people's beliefs differ given device ownership, and their membership in one of two groups: Mechanical Turk workers, or people enrolled in Health-e-Heart, a massive (n > 40,000), longitudinal study, in which volunteers fill out surveys about themselves, and/or upload data from biomedical self-tracking devices, over the course of several years [17]. In one portion of the survey, we ask subjects to rate a number of different biosensors in order of how likely individual's believe each sensor is to reveal what "a person is thinking or feeling" (Figure 3.2).

In our preliminary findings, brainwaves (EEG) are seen as among the most revealing biosignals, just below body language and facial expression, in their capacity to reveal the goings on of a person's mind. More common sensors such as GPS and step count are seen as less revealing (despite empirical evidence suggesting such data can be quite revealing indeed [8]). What will this finding mean for wider adoption? Will people shy away from using their passthought authenticator in certain situations, or when they are feeling some type of way?

4 DIVERSITY AND SECURITY OF PASSTHOUGHTS

While the previous section outlined questions around user attitudes, empirical questions about passthoughts, as signals, also linger. This section outlines and motivates the major quantitative questions that have not been fully answered by past work on passthoughts.

While past work on passthoughts has achieved excellent results using recordings from different users, these studies do not consider a variety of different subject conditions. For example, sitting subjects may have different patterns of neural activity from subjects who are standing, walking or exercising [37], let alone subjects who are under the influence of e.g. caffiene or alcohol. Passthoughts studies must collect larger, and more diverse corpora of EEG data to examine how passthoughts change (or remain stable) throughout the dynamic contexts of daily life.

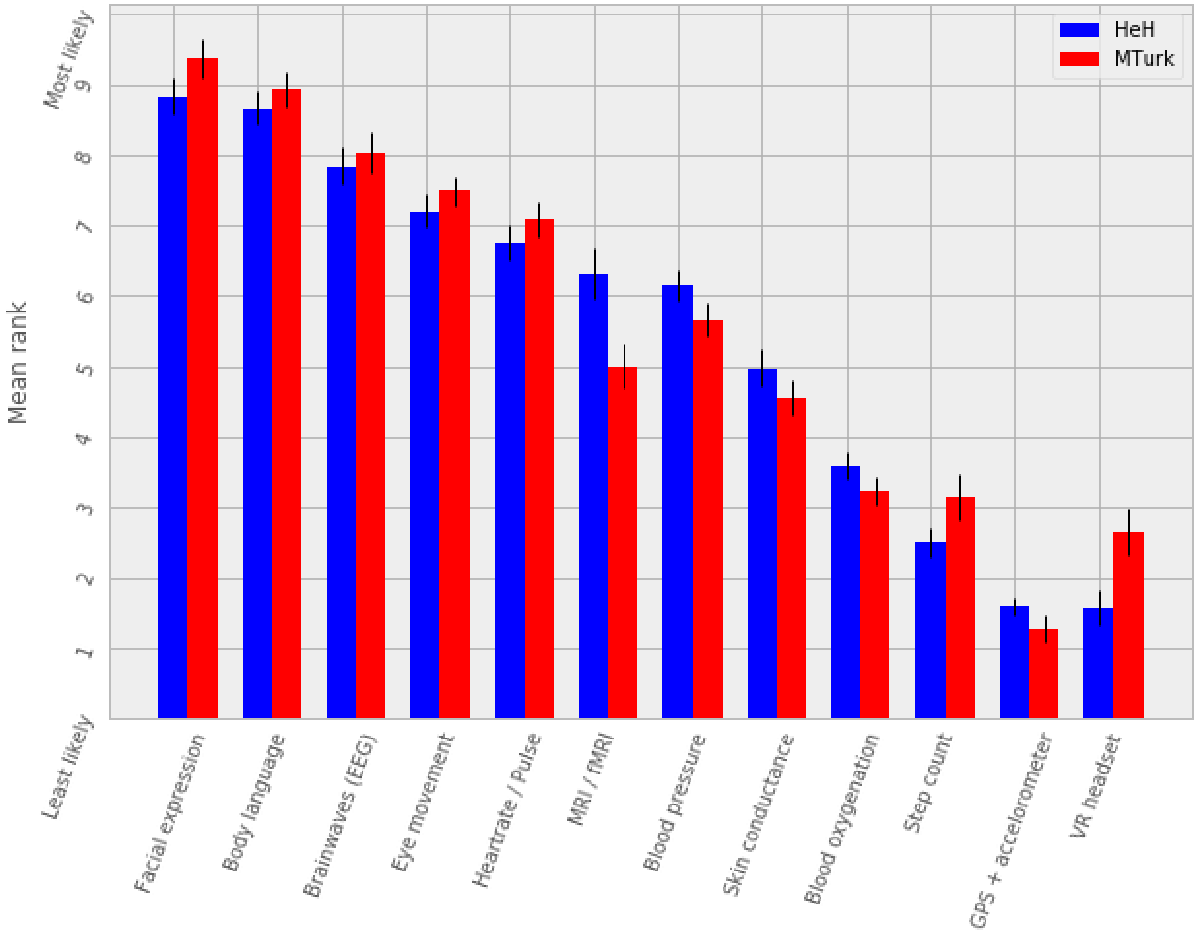

Figure 3: "Please rank the following sensors in how likely you believe they are to reveal what a person is thinking and feeling." Higher bars indicate higher rank, or higher likelihood of being revealing.

Investigating this topic could also help us understand how and why passthoughts work at all: Why are passthoughts unique, and how unique are they? A primary question in passthoughts surrounds how large the real space of possible passthoughts might be [39]. While the space of possible passthoughts is potentially unlimited, we do not yet know what passthoughts we stand a reasonable chance at observing consistently over time. A larger corpus of data might help shed light on this issue by allowing us to observe the distribution of signals that people produce over time.

A more subtle, but closely related question surrounds how passthought EEG recordings relate statistically to non-passthought EEG recordings. In other words, we do not know how the particular passthoughts observed in past work are drawn from the distribution of EEG signals that an individual produces over the course of their day. This blindspot poses a possible challenge to passthought's vulnerability to dictionary-style cracking. If an attacker has a large enough corpus of EEG readings, do some passthoughts start to look as guessable as *password1234*? By answering such questions, we could design data-driven policies for, e.g., how many retry attempts passthought authenticators should allow.

5 TWO STUDIES ON PASSTHOUGHTS

The prior two sections raise two main topics that future work could address. First, our limited understanding of passthoughts' usability, and user attitudes about the sensing modality present immediate questions for further development of this technology. Second, our limited knowledge of how passthoughts shift and change over time, and around the diversity of EEG signals as our (non-medical) devices sense them, raise questions about how frequently passthoughts would need to be calibrated, how accurate we can expect the protocol to be in different context, and how secure it might remain under threat from a motivated attacker.

This section proposes two studies on passthought authentication which, taken together, could make headway on these topics. One study, a controlled, lab-based experiment, seeks to raise fundamental questions about how the feedback of a real-time authentication system may affect the way users perform their passthoughts. It also begins to address certain, limited questions around the shifting nature of neural signals. The second study, a longitudinal deployment, seeks to collect a large and diverse corpus of EEG signals, while probing people's beliefs and attitudes about EEG and brainscanning in everyday life. Together, these studies address both long-term concerns about user attitudes and signal diversities, and also short-timescale questions about the usability and accuracy of passthoughts in realistic use scenarios.

5.1 A real-time passthought authenticator

Passthoughts promise more usable form multi-factor authentication compared to existing protocols, as they provide both a knowledge and an inherence factor in a single-step user action. However, no study yet has systematically evaluated passthoughts' usability. Here, we propose a study aimed at examining passthoughts' usability in an ecologically valid context.

5.1.1 Study protocol. This study would take place in a lab, under the supervision of an experimenter. First, the experimenter would calibrate a subject with a passthought authenticator, as in [11]. Through an automated cross-validation process, the participant's best-performing passthought would be selected. Next, the experimenter would present users with an online banking application, and ask them to perform their passthoughts. We can manipulate feedback such that users either see the real authentication accuracy (control), are always rejected by the authenticator, or always accepted by the authenticator.

After this task, subjects could take a post-questionnaire including various usability questions. After filling out this questionnaire, the experimenter might engage users in a brief, ten-minute semi-structured interview, in which subjects are asked to recount their experience with the authenticator. This interview could help gain some richer, qualitative data that traditional survey methods might fail to capture.

5.1.2 The effect of feedback. Through this study, we might find that passthoughts is considered usable, even when authentication attempts are always rejected. We might also find that passthoughts are not considered usable, even when authentication attempts are always accepted.

Furthermore, using the data collected during this study, we could perform an offline analysis to test for the effect of these conditions on the actual performance of users' passthoughts. When subjects are continuously rejected, do their passthoughts change in frustration (or in an attempt to gain access)? We might find that passthought performance remains stable, regardless of what feedback subjects are shown. Alternatively, we might find that performance changes when subjects are continuously rejected from their authenticator. Alternatively, performance may change, even when subjects are continually accepted by their classifier.

This study's findings could have far-reaching impacts for the future development of passthought authenticators. Its results would shed light on how passthoughts change as a response to authenticator performance on one hand, and how authenticator performance affects perceptions of passthoughts' usability on the other.

5.1.3 Exploring continuous re-calibration. In addition to these findings, the data generated during this study could help test a third hypothesis: that the continual re-training of passthought classifiers might help boost classification performance over time, especially in the face of shifting signals. Offline, we can train each classifier, for each subject, to achieve its post-calibration state. Next, we can run each reading recorded from a particular participant through the trained classifier. If the classifier accepts the reading, we can then re-train the classifier, adding this reading to the corpus of positive examples. In a separate, *negative calibration* condition, we also re-train the classifier with rejected readings as negative examples.

By comparing the final FAR and FRR for each subject using these strategies, compared to the one-time calibration strategy, we could begin to get an idea as to whether this strategy helps achieve superior performance, especially when signals change. This analysis could also act as a harbinger for some of the possible downsides of this approach: If a user is continually rejected, and the classifier is re-trained using those rejections as negative examples, will the user find themselves trapped in a negative spiral of ever-decreasing authentication accuracy?

5.2 A longitudinal study on brainwave monitoring

The study proposed above would help answer preliminary questions about the usability of a passthought authenticator in a short-term context, and possible ways for dealing with shifting neural signals, a few questions will still remain. First, the study above will not help us collect a large corpus of EEG signals, preventing us from investigating how robust passthoughts authentication performs in various user conditions, and from understanding how easy particular passthoughts are to guess or crack. Second, while the previous study helps us understand user attitudes over a short timescale, it will not help us understand how people's beliefs about EEG might change over longer periods of time, as they use their devices in day-to-day life.

Unfortunately, these challenges (particularly those around shifting neural signals) also make it difficult to produce a passthought authenticator that works with any reliability in real-life contexts. This makes a longitudinal study with a working authenticator impractical for the time being. However, we may still perform a longitudinal study that allows us to interrogate the usability aspects around (and attitudes about) passthoughts specifically, and EEG generally. In so doing, we may also collect a larger and more diverse corpus of passthoughts, which can be used to address the paucity of data we face today. A technology probe or diary study [18] could help address both of these issues at the same time.

Of course, this study would be no substitute for a working, online passthoughts authentication system. Instead, this study aims to collect useful data before such a system exists. It will not only elicit beliefs, but also allow us to collect larger datasets, and to catch technical issues in sensing devices and collection platforms.

5.2.1 Study protocol. A small group of subjects could wear a working, recording EEG device, whether or not it provides feedback, in a variety of settings for some number of days, having subjects journal their experiences and asking them specifically what they feel someone might be able to know about them from the EEG signals they record. At the same time, we could use this study as an opportunity to collect a much larger, and more diverse corpus. To aid in the collection of signals that are specific to our problem of passthought authentication, subjects in this study might be prompted to perform a variety of tasks at a few checkpoints throughout the day. With the data collected during this study, we could easily simulate passthought accuracy on a much more realistic (and representative) sample of readings.

Such a study would trade a large population size for a large corpus of diverse data. This tradeoff allows us to closely investigate the diversity of EEG signals within subjects. The diverse readings encountered in day-to-day life could help us understand how such signals change as a function of time, and/or in different psychophysical states. At the same time, our user diaries and interviews could enable a rich, qualitative understanding of users attitudes.

5.2.2 A more diverse corpus. While subjects wear their EEG device and diary about their experience, we should also ask subjects to perform targeted mental tasks (potential passthoughts) in a variety of contexts (ambulatory, under the influence of caffeine or alcohol, etc). This diverse corpus should allow us to both evaluate performance in ambulatory settings, and to investigate the possibility that past works' models overfit for subjects who are sitting down in a lab. How do an individual's EEG signals change throughout various activities, and mental states?

This corpus will, of course, also include unlabeled non-task data from similarly diverse settings, perhaps concurrent with streams of GPS or accelorometer data. Unlabeled data represents another fruitful source of data for passthoughts. The unlabeled samples in this corpus also allow us to examine properties of EEG signals in general, helping us build more robust models which should help us prevent overfitting in the future.

5.2.3 The space of possible passthoughts. In another potentially fruitful analysis, such a corpus will allow us to perform statistical analysis of how passthoughts are drawn from the overall distribution of EEG signals. Using multi-dimensional clustering algorithms such as t-SNE [43] could assist us in understanding how particular passthoughts relate to other EEG signals that an individual expresses involuntarily throughout the day. These clusters will help us understand how likely or unlikely we are to observe a given passthought in context of a particular person's neural signals Such analysis between subjects could help shed light how given passthoughts are expressed uniquely between individuals.

Leveraging the statistical clusters of EEG data generated by these algorithms, it might also be possible to generate a "passthoughts cracker," capable of generating plausible passthoughts. Feeding these algorithms into pre-trained passthought classifiers, we can begin to generate realistic models of classifiers' resistance to cracking attempts. These cracking experiments could lead to defenses against cracking attempts, by enforcing retry attempt timeouts or other methods for limiting break-in risk, such that strong security guarantees can be enforced.

5.2.4 Usability and attitudes. By deploying a real sensing apparatus, be it a traditional consumer device such as the Muse [27] or a more experimental piece of equipment such as an earbud, and having people record EEG data in their daily life, we could learn more about the interpretative qualities of these data [31]. This study presents a dual opportunity to understand user beliefs with rich, qualitative data, while simultaneously collecting the large, diverse and longitudinal corpus of EEG signals necessary if we wish to stand a chance at decent authentication accuracy in the wild.

6 PRIVACY, SECURITY: CHOICES, TRADEOFFS

After the studies described above, we will have a much better grasp on the usability, and security properties of passthought authentication. However, there may still be unexplored risks, challenges, and tradeoffs, especially around user privacy. Indeed, some of these risks are unique to the application context of biometric authentication, and to EEG as a class of biosignal. This section briefly reviews risks to user privacy and security that widespread passthought authentication may introduce. We present broad class of categories from which such risks may emerge.

6.1 Privacy

As of yet, it is still not well understood what EEG signals might reveal about a person. EEG signals that are not anonymized could come to be seen as private in the face of new methods of analysis. (If your brainwaves can authenticate you, could they also uniquely identify you, even if your name is redacted?) Differential privacy [16] presents one approach to dealing with the risk of privacy breaches with EEG signals. By adding noise to datasets, differentially private databases can make strong guarantees about the likelihood of a de-anonymization attack on particular database queries.

6.2 Security

Device security presents another risk to passthought authentication. Since EEG devices will transmit data, likely wirelessly [27], their data may be intercepted, depending on the security properties of the underlying transit protocol. When transferring authentication credentials in passthoughts, the ability to snoop on authentication attempts could present a dangerous attack vector.

There is also the question of the security of data infrastructures in which EEG data might be stored. Large data repositories are what Wolf [46] calls a "toxic asset"; they must be maintained, lest the maintainer take liability for harmful fallout of poor data management. With biosignals, as with many kinds of data, it is not clear what they might mean until they are already collected in aggregate. By then, it is too late to decide on an appropriate data security policy.

Strong encryption policies should be built into collection systems from the very beginning, It remains an open question what specific protections and access controls will yield robust security. Homomorphic encryption, in which computation such as database queries can be performed on encrypted data, provides one interesting path for future work [41].

6.3 Tradeoffs between security and privacy

In some cases, passthoughts could present direct tradeoffs between security and privacy. For example, end-user privacy could be enhanced by storing all data locally, on the phone. All classification, and the training of all classifiers, could occur locally, so that users never need to disclose their private biosensory data to a third party. However, security might be improved by aggregating user data so as to construct more robust, reliable classifiers. Aside from classifier accuracy, training classifiers in the cloud could help with the speed of calibration, and prevent undue battery drain on user devices.

These factors suggest a possible tension between the accuracy (and thus security) of passthought authentication, and the locality (and thus privacy) of potentially sensitive user data. Future work should explore this tradeoff empirically, using real data and simulations from a variety of different users. Future work might also explore metrics by which to judge such tradeoffs. Whereas security might be measured straightforwardly using false-acceptance and false-rejection rates, user privacy might be more challenging to quantify, as might the tradeoffs between the two. However, future work will need to address these issues if we are to balance users' security requirements with their privacy requirements.

7 FURTHER FUTURE DIRECTIONS

This paper so far has motivated two future studies on passthoughts, and discussed potential risks intrinsic to the development of passthoughts systems. With these risks in mind, the present section explores some of the exciting possibilities that could unfold after the immediate priorities described in the prior sections.

7.1 Continuous authentication

After immediate challenges are overcome, one potentially exciting possibility is that of using EEG for *continuous authentication*. Continuous authentication schemes seek to authenticate a user using ongoing streams of data or activity, sometimes by giving a probability that a person's identity is authentic [6]. Such schemes are a natural match for wearables, which can continuously collect and process biometric data. A recent startup, Unify.ID, has begun to perform cross-device continuous authentication as a service [42]; however, as a knowledge factor, it currently falls back on traditional passwords, which come with both well-known risks and annoyances to usability.

A continuous passthought authenticator could incorporate both knowledge and inherence factors (along with, optionally, the posession factor of a unique sensing device). Subjects could perform secret passthoughts for certain unlocking actions, while the authenticator could fall back on inherence in the base case (e.g. as an additional check on sites where the user's logged-in session would otherwise be remembered). In theory, this strategy provides better security properties than saved sessions or cookies, which, after initial authentication, establish only posession. Individual login attempts also offer security improvements over traditional passthoughts alone, as the continuous inherence step provides an ongoing validation against individual authentication attempts.

7.2 Organic passwords

If EEG signals are nonstationary (changing over time), passthoughts will require continuous re-calibration to maintain decent accuracy [44]. This feature of BCIs could have an unexpected benefit to security. If an individual's expression of their passthought in EEG is always changing, passthoughts themselves are effectively evergreen, automatically replaced or updated by nature of the authentication paradigm. This feature could improve security, as an attacker able to compromise a passthought's EEG signature may not be able to log into the system in a few weeks time, unless they are able to realistically mutate the signal over authentication attempts. This feature of EEG also gives passthoughts a possible advantage over other methods for behavioral authentication, such as voice or keystroke dynamics [28], which may change more slowly for individuals, if they change at all. Future work should investigate this claim, perhaps using a longitudinal corpus such as the one described above.

7.3 Authentication and the self

Where authenticity is nominally concerned with proving that you are who you say you are, a less-frequently-asked question in the authentication literature is, "are you really yourself?" We all sometimes do or say regrettable things when we are feeling "not quite ourselves," sometimes using devices or services with which we have authenticated ourself. Can authentication ever verify not only your possession of your body, but of your "right mind"?

A question raised earlier surrounds where passthoughts could still work if a person is drunk, having a migraine, or in distress (Section 3). Even if passthoughts fails when a user is in such an "off-baseline" state, passthoughts still may have utility (perhaps even *added* utility) in certain authentication contexts. For example, one may wish to allow themselves access to certain resources (e.g. bank accounts) when one's resting EEG state is not too much different from a pre-recorded baseline.

Such a scenario raises serious ethical, legal, and even philosophical questions. How does such a system conform to accepted definitions of a "person"? Who is a person to make decisions for their future self? What are possible vectors for abuse? In any case, this property of an authentication is, as far as we are aware, novel, and should be considered as we learn more about the strengths, weaknesses, and particular affordances of this developing method for authentication.

7.4 Passthoughts by any other sensor?

At the end of the day, past passthoughts work has collected electromagnetic signals from the body at the surface of the skin. What is important about passthoughts is not so much the EEG per se, but that it is both secret and idiosyncratic (knowledge and inherence), that its performance had no tell, and that its performance was not easily explained to others. EEG itself brings a variety of challenges: it is a low-magnitude signal, prone to noise, and inconvenient to capture without special equipment.

There is no theoretical reason why the same criteria cannot be met with, e.g., EMG from the face, or a mixture of EEG and EMG. Muscular activity associated with thoughts might, after all, be both difficult to view and consistent between trials. Future work could investigate such claims further, or use different types of sensors that may have a similar effect (EKG, fNIRs).

7.5 Health, neuroscience and BCIs

Neuroscience fuels some of the most chilling predictions in science fiction [45]. It also stands for some of the greatest possible advances in medicine, mental health, and understanding of human behavior. One ambitious goal is to detect or even predict seizures [29].

However, the original, and most active areas of research in BCI surround the creation of tools for persons with muscular disabilites [9]. By collecting unstructured or semi-structured EEG data in the wild, passthought systems could help improve the development of such BCIs [19]. The small size of data repositories, limited mostly by the clinical trials needed to build BCIs for persons with disabilities, has consistently frustrated attempts to improve on algorithms and protocols in this field [3].

Though the application context for passthoughts is quite different from wheelchairs, and although passthought users may not have muscular disabilities, pursuing passthoughts as an area of research will inevitably yield larger repositories of EEG data than have been collected to date. This data could prove invaluable for the development of EEG-based BCIs across a variety of fields, including (but not limited to) assistive technologies.

Again, these opportunities must strike a balance with the risks of individual users' privacy and security. Violating user privacy by revealing EEG data, even to researchers, could undermine any chance of wider BCI adoption in the long-term. Striking this balance will require a deeper understanding of the statistical properties of signals. How much data will users really need to give up? What counts as an "anomalous" reading? Answers to these questions could themselves inform neuroscientific inquiry. This balance will also require a deeper understanding of individuals' attitudes about the meaning of such signals, and how private people believe them to be.

8 CONCLUSION

In general, as sensors grow smaller and cheaper, devices more connected, and machine learning more sophisticated, people will build increasingly high-resolution models of human physiology "in the wild." Passthoughts present just a microcosm of the good such advances might bring, along with some of the most pressing anxieties: What does pervasive physiological recording mean for our privacy, security, safety? The balancing act between these risks and opportunities will prove recurring theme for decades to come. In the meantime, probing the outer limits of ubiquitous, pervasive sensing can shed light on both the good and bad that our near future may bring.

REFERENCES

[1] Fadel Adib, Hongzi Mao, Zachary Kabelac, Dina Katabi, and Robert C Miller. 2015. Smart Homes that Monitor Breathing and Heart Rate. *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems - CHI '15* (2015), 837–846. DOI:http://dx.doi.org/10.1145/2702123.2702200

[2] Sabrina S Ali, Michael Lifshitz, and Amir Raz. 2014. Empirical neuroenchantment: from reading minds to thinking critically. *Frontiers in human neuroscience* 8, May (may 2014), 357. DOI:http://dx.doi.org/10.3389/fnhum.2014.00357

[3] B Allison. 2009. The I of BCIs: Next Generation Interfaces for Brain—Computer Interface Systems That Adapt to Individual Users. In *Proceedings of HCII'09*, Julie A. Jacko (Ed.). Vol. 5611. Springer Berlin Heidelberg, Berlin, Heidelberg, 558–568. papers3://publication/uuid/443373BE-AE9B-40FB-B2BA-CF67CD92FCFE

[4] Corey Ashby, Amit Bhatia, Francesco Tenore, and Jacob Vogelstein. 2011. Low-cost electroencephalogram (EEG) based authentication. In *2011 5th International IEEE/EMBS Conference on Neural Engineering, NER 2011*. 442–445. DOI:http://dx.doi.org/10.1109/NER.2011.5910581

[5] Tara Siegel Bernard. 2015. Giving Out Private Data for Discount in Insurance. (2015). http://www.nytimes.com/2015/04/08/your-money/giving-out-private-data-for-discount-in-insurance.html?

[6] Hristo Bojinov, Daniel Sanchez, Paul Reber, Dan Boneh, and Patrick Lincoln. 2012. Neuroscience Meets Cryptography : Designing Crypto Primitives Secure Against Rubber Hose Attacks. *Proceedings of the 21st USENIX conference on Security symposium* (2012), 1–13. DOI:http://dx.doi.org/10.1145/2594445

[7] Tega Brain and Surya Mattu. 2015. Unfit Bits. (2015). http://www.unfitbits.com/http://www.unfitbits.com/index.html

[8] Luca Canzian and Mirco Musolesi. 2015. Trajectories of depression. *Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing - UbiComp '15* (2015), 1293–1304. DOI:http://dx.doi.org/10.1145/2750858.2805845

[9] Francesco Carrino, Joel Dumoulin, Elena Mugellini, Omar Abou Khaled, and Rolf Ingold. 2012. A self-paced BCI system to control an electric wheelchair: Evaluation of a commercial, low-cost EEG device. In *2012 ISSNIP Biosignals and Biorobotics Conference: Biosignals and Robotics for Better and Safer Living, BRC 2012*. 1–6. DOI:http://dx.doi.org/10.1109/BRC.2012.6222185

[10] John Chuang. 2014. One-Step Two-Factor Authentication with Wearable Bio-Sensors. (2014). https://cups.cs.cmu.edu/soups/2014/workshops/papers/biosensors

[11] John Chuang, Hamilton Nguyen, Charles Wang, and Benjamin Johnson. 2013. I think, therefore I am: Usability and security of authentication using brainwaves. In *International Conference on Financial Cryptography and Data Security*. 1–16. DOI:http://dx.doi.org/10.1007/978-3-642-41320-9_1

[12] Kate Crawford. 2014. When Fitbit Is the Expert Witness. *The Atlantic* (nov 2014). http://www.theatlantic.com/technology/archive/2014/11/when-fitbit-is-the-expert-witness/382936/

[13] Max T Curran, Nick Merrill, Swapan Gandhi, and John Chuang. 2017. One-Step, Three-Factor Authentication with Custom-Fit, In-Ear EEG. In *In submission*.

[14] Max T Curran, Jong-kai Yang, Nick Merrill, and John Chuang. Passthoughts Authentication with Low Cost EarEEG. *EMBC 2016* (????).

[15] Tony Doyle. 2011. Helen Nissenbaum, Privacy in Context: Technology, Policy, and the Integrity of Social Life. *The Journal of Value Inquiry* 45, 1 (2011), 97–102. DOI:http://dx.doi.org/10.1007/s10790-010-9251-z

[16] Cynthia Dwork and Aaron Roth. 2014. The Algorithmic Foundations of Differential Privacy. *Foundations and Trends in Theoretical Computer Science* 9, 2013 (2014), 211–407. DOI:http://dx.doi.org/10.1561/0400000042

[17] Deborah Estrin and Ida Sim. 2010. Health care delivery. Open mHealth architecture: an engine for health care innovation. *PLoS Medicine* 10, 2 (2010), e10011395. DOI:http://dx.doi.org/10.1126/science.1196187

[18] Bill Gaver, Tony Dunne, and Elena Pacenti. 1999. Design: Cultural probes. *interactions* 6, 1 (jan 1999), 21–29. DOI:http://dx.doi.org/10.1145/291224.291235

[19] Mick Grierson and Chris Kiefer. 2011. Better brain interfacing for the masses. In *Proceedings of the 2011 annual conference extended abstracts on Human factors in computing systems - CHI EA '11 (CHI EA '11)*. ACM Press, New York, NY, USA, 1681. DOI:http://dx.doi.org/10.1145/1979742.1979828

[20] Benjamin Johnson, Thomas Maillart, and John Chuang. 2014. My thoughts are not your thoughts. *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing Adjunct Publication - UbiComp '14 Adjunct* (2014), 1329–1338. DOI:http://dx.doi.org/10.1145/2638728.2641710

[21] P. Kidmose, D. Looney, L. Jochumsen, and D. P. Mandic. 2013. Ear-EEG from generic earpieces: a feasibility study. *Conference proceedings : ... Annual International Conference of the IEEE Engineering in Medicine and Biology Society. IEEE Engineering in Medicine and Biology Society. Annual Conference* 2013 (2013), 543–546. DOI:http://dx.doi.org/10.1109/EMBC.2013.6609557

[22] Preben Kidmose, David Looney, Michael Ungstrup, Mike Lind Rank, and Danilo P. Mandic. 2013. A study of evoked potentials from ear-EEG. *IEEE Transactions on Biomedical Engineering* 60, 10 (2013), 2824–2830. DOI:http://dx.doi.org/10.1109/TBME.2013.2264956

[23] Antti Latvala, Ralf Kuja-Halkola, Catarina Almqvist, Henrik Larsson, and Paul Lichtenstein. 2015. A Longitudinal Study of Resting Heart Rate and Violent Criminality in More Than 700000 Men. *JAMA Psychiatry* 72, 10 (oct 2015), 917–8. DOI:http://dx.doi.org/10.1001/jamapsychiatry.2015.1165

[24] David Looney, Preben Kidmose, Cheolsoo Park, Michael Ungstrup, Mike Rank, Karin Rosenkranz, and Danilo Mandic. 2012. The in-the-ear recording concept: User-centered and wearable brain monitoring. *IEEE Pulse* 3, 6 (2012), 32–42. DOI:http://dx.doi.org/10.1109/MPUL.2012.2216717

[25] D. Looney, C. Park, P. Kidmose, M. L. Rank, M. Ungstrup, K. Rosenkranz, and D. P. Mandic. 2011. An in-the-ear platform for recording electroencephalogram. In *Proceedings of the Annual International Conference of the IEEE Engineering in Medicine and Biology Society, EMBS*. 6882–6885. DOI:http://dx.doi.org/10.1109/IEMBS.2011.6091733

[26] Sébatien Marcel and José del R Millan. 2007. Person authentication using brainwaves (EEG) and maximum a posteriori model adaptation. *IEEE Transactions on Pattern Analysis and Machine Intelligence* 29, 4 (2007), 743–748. DOI:http://dx.doi.org/10.1109/TPAMI.2007.1012

[27] Vojkan Mihajlovic, Bernard Grundlehner, Ruud Vullers, and Julien Penders. 2015. Wearable, wireless EEG solutions in daily life applications: What are we missing? *IEEE Journal of Biomedical and Health Informatics* 19, 1 (2015), 6–21. DOI:http://dx.doi.org/10.1109/JBHI.2014.2328317

[28] F. Monrose and a. Rubin. 1997. Authentication via keystroke dynamics. *Proc. of the 4th ACM Conf. on Computer and Communications Security* (1997), 48–56. DOI:http://dx.doi.org/10.1145/266420.266434

[29] Florian Mormann, Christian E Elger, and Klaus Lehnertz. 2006. Seizure anticipation: from algorithms to clinical practice. *Current opinion in neurology* 19, 2 (2006), 187–193. DOI:http://dx.doi.org/10.1097/01.wco.0000218237.52593.bc

[30] Dawn Nafus (Ed.). 2016. *Quantified: Biosensing Technologies in Everyday Life*. Vol. 9. The MIT Press, Cambridge, MA. 116–131 pages.

[31] Jaime Nafus, Dawn; Sherman. 2014. This One Does Not Go Up to 11 : The Quantified Self Movement as an Alternative Big Data Practice. *International Journal of Communication* 8 (2014), 1–11.

[32] Nymi. Nymi Band - Always-On Authentication. (????). https://nymi.com

[33] Ramaswamy Palaniappan. 2008. Two-stage biometric authentication method using thought activity brain waves. *International journal of neural systems* 18, 1 (2008), 59–66. DOI:http://dx.doi.org/10.1142/S0129065708001373

[34] M Poulos, M Rangoussi, N Alexandris, and a Evangelou. 2002. Person identification from the EEG using nonlinear signal classification. *Methods of information in medicine* 41, 1 (2002), 64–75.

[35] Olivia Solon. 2015. Wearable Technology Creeps Into The Workplace. *Bloomberg* (aug 2015). http://www.bloomberg.com/news/articles/2015-08-07/wearable-technology-creeps-into-the-workplace

[36] James Stables. 2016. The best biometric and heart rate monitoring headphones. (2016). http://www.wareable.com/headphones/best-sports-headphones

[37] Robert T. Thibault, Michael Lifshitz, and Amir Raz. 2016. Body position alters human resting-state: Insights from multi-postural magnetoencephalography. *Brain Imaging and Behavior* 10, 3 (2016), 772–780. DOI:http://dx.doi.org/10.1007/s11682-015-9447-8

[38] Kalee Thompson. 2011. The Santa Cruz Experiment: Can a City's Crime Be Predicted and Prevented? *Popular Science* (oct 2011), 1–18. http://www.popsci.com/science/article/2011-10/santa-cruz-experiment?nopaging=1

[39] Julie Thorpe, P C Van Oorschot, and Anil Somayaji. 2005. Passthoughts: authenticating with our minds. *Proceedings of the 2005 workshop on New security paradigms* (2005), 45–56. DOI:http://dx.doi.org/10.1145/1146269.1146282

[40] Nigel Thrift. 2014. The 'sentient' city and what it may portend. *Big Data and Society* 1, June (apr 2014), 1–21. DOI:http://dx.doi.org/10.1177/2053951714532241

[41] Stephen Tu, M. Frans Kaashoek, Samuel Madden, and Nickolai Zeldovich. 2013. Processing analytical queries over encrypted data. *Proceedings of the VLDB Endowment* 6, 5 (2013), 289–300. DOI:http://dx.doi.org/10.14778/2535573.2488336

[42] UnifyID. 2017. UnifyID, a service that can authenticate you based on unique factors like the way you walk, type and sit. (2017). https://unify.id

[43] L J P Van Der Maaten and G E Hinton. 2008. Visualizing high-dimensional data using t-sne. *Journal of Machine Learning Research* 9 (2008), 2579–2605. DOI:http://dx.doi.org/10.1007/s10479-011-0841-3 arXiv:1307.1662

[44] C. Vidaurre, A. Schl??ogl, R. Cabeza, R. Scherer, and G. Pfurtscheller. 2006. A fully on-line adaptive BCI. *IEEE Transactions on Biomedical Engineering* 53, 6 (jun 2006), 1214–1219. DOI:http://dx.doi.org/10.1109/TBME.2006.873542

[45] Brian Welsh. 2011. Black Mirror: The Entire History of You. (2011).

[46] Gary Wolf. 2010. The Data-Driven Life. (apr 2010). http://www.nytimes.com/2010/05/02/magazine/

02self-measurement-t.htmlhttp://www.nytimes.com/2010/05/02/magazine/02self-measurement-t.html?