Is the Future of Authenticity In Our Heads?

Moving Passthoughts From the Lab to the World

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

ABSTRACT

While brain-computer interfaces are used by some individuals with disabilities, passthought authentication stands a chance at becoming the first brain-computer interface to reach wide, consumer adoption. However, to move passthoughts out of the lab and into the world, we will need both quantitative data about EEG signals and rich, qualitative data about user beliefs surrounding EEG specifically, and the possibility of mind-reading devices generally.

KEYWORDS

passthoughts, authentication, usable security

ACM Reference format:

Nick Merrill, Max 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),* **??** pages.
DOI: 10.475/123_4

1 INTRODUCTION

Usable authentication is a long-standing problem in 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.

Using EEG (electroencephalography), a user can submit both a knowledge factor (i.e., secret thought) and an inherence factor (i.e., brainwave signal unique to the individual) in a single step by thinking a single mental task, or *passthought* [**?**]. Even better, passthoughts have no externally visible "tell," making them impervious to shoulder surfing attacks. Data from consumer-grade EEG devices [**?**], or collected from an EEG earpiece [**?**], have been shown to work well with passthoughts.. [**?**] showed this protocol to be robust against impersonation attacks, even when the attack has learned the target's secret thought.

Recent work is heartening, but passthoughts remains confined, for now, to the lab. This paper reviews the immediate challenges passthoughts must overcome if it is move into everyday life. First, we must test passthoughts in a variety of conditions: ambulatory settings, under different levels of stress, drowsiness, caffeine or alcohol, etc. At the same time, we must build a better understanding of the statistical distribution of EEG signals that a person gives off during the course of their life, if we are to know how easy or difficult passthoughts are to guess (Section 3). Second, we must understand what people believe consumer-grade EEGs could reveal about them; past work indicates that people believe EEG can reveal what someone is thinking or feeling, which could scare off wider adoption (Section 4).

Passthought authentication stands a chance at becoming the first brain-computer interface to reach wider adoption. It is not without risks (Section 5.4), but, if future work can address the two challenges posed here, several interesting paths unfurl: closed-loop authentication, continuous and/or tacit authentication, and possible theoretical contributions to neuroscience, authentication and HCI (Section 6).

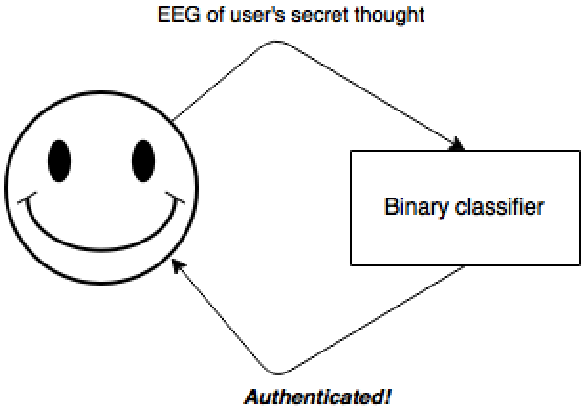

Figure 1: A passthought authenticator.

2 BACKGROUND

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). Using a custom sensing device, passthoughts could provide an additional posession factor, all in the same step.

2.1 One-step, multi-factor authentication

Other work has attempted to provide multiple factors of authentication in one step. Some work has tested behavioral authentication

NSPW '17, Islamorada, Florida, USA

DOI: 10.475/123_4

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 [?]. 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) [?]. Custom-built EEG devices could incorporate an added possession factor to the already two-step authentication provided by passthoughts [?].

2.2 Rubber-hose-proof authentication

Authentication protocols are often susceptible to a so-called *rubber-hose attack*, in which users are coerced into giving up their chosen secret (e.g. password), biometric, or unique token, voluntarily or not [? ?]. This attack is particularly effective against protocols that rely only on inherence factors, as inherent traits such as fingerprints are difficult to change without costly repercussions [?]. One defense against such an attack is *tacit authentication*, in which the user does not know exactly how s/he performs the authenticating action.

Past work has exploited tacit skills (skills we know how to do, but cannot readily explain our method for doing, e.g. riding a bike or walking [?]). In practice, these skills require time to learn, and the fact that they are performed visibly could open up opportunities for recording and replay attacks. In our work, we explore a different solution to rubber-hose attacks: a thought, which is secret (and thus changeable), but has a particular expression unique to an individual, the performance of which cannot be described (and thus cannot be coerced). Furthermore, the performance of the chosen thought is invisible to outside observers, making the actual act of authenticting impervious to shoulder-surfing.

2.3 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 [?]. Since 2002, a number of independent groups have achieved 99- 100% authentication accuracy using multi-channel sensors placed on the scalp [? ? ? ?]. In 2013, one group showed that 99% authentication accuracy can also be achieved using a consumer-grade single-channel sensor [?]. 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) [?].

2.4 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 many people already wear earbuds in day-to-day life.

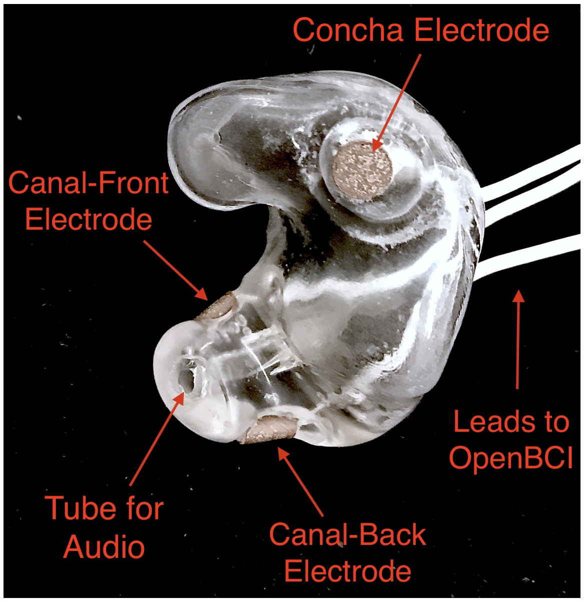

Figure 2: A custom-fit in-ear EEG device as used in Curran et al, 2017

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 [?]. 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 [? ? ?].

[?] 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 1. 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 [?].

2.5 Contending with mind-reading machines

Finally, a crucial thread of past work work concerns how users perceive the capabilites of devices that purport to "read" their "mind." Biosensing devices in general raise many questions for consumers. You might be eligible for an insurance discount if you wear a FitBit [?] (depending, of course, on what readings the FitBit produces [?]). But, would you wear a device in the workplace [?], if your manager used it to track your productivity? If biosensor data can be used in the courtroom [?], could not pervasive biosensing help to *predict* crime [?]? After all, one study suggests that probability of involvement in violent crime can be predicted from one's resting heartrate [?].

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 [?], or get sensed passively by devices integrated into the walls and ceilings [?] or city streets [?], 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 [?]. Meanwhile, if they think that a given technology does *not* measure their mind, when it fact it does, users may suffer a breach of what Nissenbaum might call the "appropriateness of the flow of information" [?]. In both cases, knowing what people expect will help us anticipate their needs, and concerns.

Crucially, there are some people who actually *want* their minds measured, e.g. for self-reflection. Consider the Spire, a breath sensor that claims to divine, from a person's patterns of in-breaths and out-breaths, what the user is calm, focused, or tense [?]. For the device to "work," not only must these detected signals match with end-users' intuitions, but users must also believe that a device like the Spire has the power to measure and detect these phenomena, given breath as input [?]. In general, technologies that claim to "measure the mind" must rely on end-users to define the criteria by which systems are deemed effective, or accurate.

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 [?].

3 DIVERSITY AND CRACKABILITY OF PASSTHOUGHTS

To transition from the lab to the real world, passthoughts studies must collect larger, and more diverse corpora of EEG data. While past work on passthoughts has achieved excellent results on corpora of recordings from different users, these studies do not consider passthoughts from 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 [?], let alone subjects who are under the influence of caffeine, alcohol or marijuana.

Relatedly, these studies do not systematically investigate how these recordings relate statistically to non-passthoughts. That is, 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 blind-spot poses a possible challenge to passthought's vulnerability to dictionary-style cracking. If I have 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. Investigating this question could also help us understand how and why passthoughts work at all: Why are passthoughts unique, and how unique are they?

4 USER PERCEPTIONS OF EEG

The prior section outlined the first major challenge to passthought authentication: that of corpus diversity. The following section reviews a more subtle challenge: that of usability, as it relates to attitudes around sensing brainwaves.

What can machines know about a person's mind, even theoretically? This question is never more relevant than when speaking of attempts at quantitative measures of brain activity (e.g. brainwaves). Past work has established the almost magical abilities that people tend to ascribe to brain-scanning devices, even subjects with specific training in the limitations of brain-scanners [?]. This section outlines concerns around "mind-reading" machines, and how they relate to EEG and passthoughts specifically. We then move to a discussion for possible ways to address these concerns, and concerns about dataset diversity, in the following section.

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

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 [?]).

The survey I 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 [?]. 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 ??).

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? The following section describes one exploratory study that could investigate some aspects of this larger question.

5 A LONGITUDINAL STUDY ON EEG

As reviewed above, passthoughts currently faces two major challenges. First, we also do not have a sufficiently 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, we do not understand how people's beliefs about EEG might affect their behavior with a passthought authentication system.

A longitudinal study, such as a technology probe or diary study [?], could help address both of these issues at the same time A small group of subjects could wear a working, recording EEG device,

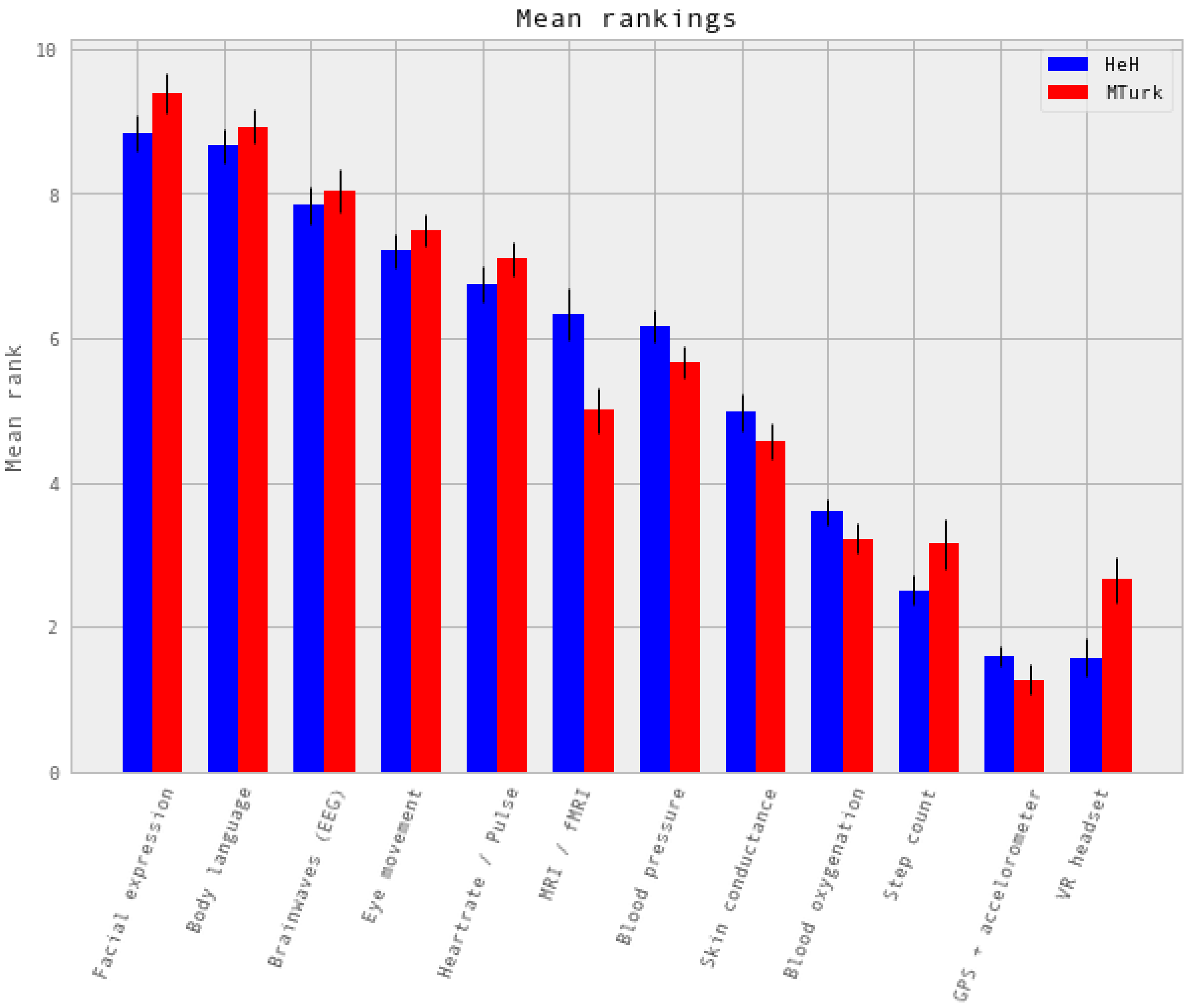

Figure 3: "Please rank the following sensors in how likely you believe they are to reveal what a person is thinking and feeling." Mean Likert responses (Not at all. . . Very informative). Lower bars mean higher rank (1 being the highest-ranked, or most likely to reveal what one is thinking or feeling."

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.

5.1 Usability and attitudes

By deploying a real sensing apparatus, be it a traditional consumer device such as the Muse [?] 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 [?]. Such a study presents a dual opportunity to understand user beliefs in a rich, qualitative sense, while simultaneously collecting the large, diverse and longitudinal corpus of EEG signals necessary if we wish to stand a chance at decent classification accuracy in the wild.

Of course, this study is 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 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.

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 multidimensional clustering algorithms such as tSNE [?] 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 rare or unlikely a given passthought is, and help shed light on why and 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 guarantees can be enforced.

6 PRIVACY, SECURITY: CHOICES, TRADEOFFS

After the study described above, future work should be able to start building more robust, world-ready passthought systems, which could offer improvements to the usability and security of authenticating. However, these opportunities do not come without risks. Indeed, some risks are unique to the application context, and to EEG as a class of biosignal. This section briefly reviews risks to user privacy and security that widespread passthought authentication may introduce. I do not pose specific challenges to passthoughts here, though many surely lurk; instead, I present broad class of categories from which questions may emerge.

6.1 Privacy

One clear risk comes to user privacy, as it is still not well understood what EEG signals might reveal about a person. EEG signals that are not anonymized could, at least theoretically, 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 [?] 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 datbase queries.

6.2 Security

Device security presents another risk to passthought authentication. Since EEG devices will transmit data, likely wirelessly [?], 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 large data repositories in which EEG data might be stored. Large data repositories are what Wolf [?] calls a "toxic asset"; infrastructures that must be maintained, lest the maintainer take liability for the potentially harmful fallout of poor data management. With biosignals, as with many kinds of data, it is not entirely clear what they might mean until they are already collected in aggregate. At this point, it is too late to decide on an appropriate data security policy. Good data 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 [?].

7 FURTHER FUTURE DIRECTIONS

This paper so far has motivated a longitudinal study with EEG, and its importance even before a working passthought authenticator has been completed. I have also 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 open up after the immediate priorities described previously.

7.1 Closed-loop (real-time) passthoughts

Future work on passthoughts should look at closed-loop, or online authentication systems, in part to investigate the impact of human learning effects on passthought performance. What effect does the feedback (of a successful or unsuccessful authentication attempt) have on the way that people perform their passthoughts? Specific studies could, for example, provide false feedback in which passthought authentication appears to always either succeed or fail. In the always-fail condition, we might expect subjects to alter the way they perform the passthought across multiple attempts; data of how such a change occurs could enable us to pre-empt changes observable in the wild.

7.2 Continuous authentication

After immediate challenges are overcome, one further-out, though 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 [?]. 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 [?]; however, as a knowledge factor, it currently falls back on traditional passwords, which come with both 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. At the same time, individual login attempts can have sightly better security than traditional passthoughts alone, as the continuous inherence step provides an extra, ongoing validation to individual challenges.

7.3 Organic passwords

If EEG signals are nonstationary (changing over time), passthoughts will require online machine learning to maintain decent accuracy [**?**]. 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 gait, which may change more slowly for individuals, if it changes at all. Future work should investigate this claim, perhaps using a longitudinal corpus such as the one described above.

7.4 Neuroscience of authentication

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 on the Internet (i.e, using devices we have authenticated to). Can authentication ever verify not only your posession of your body, but of your "right mind"?

Many ask if passthoughts will 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, and legal questions. How does such a system conform to legal 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 I am aware, novel, and should be considered as we learn more about the strengths, weaknesses, and particular affordances of this still-novel method for authentication.

7.5 Mobile health

Neuroscience fuels some of the most chilling predictions in science fiction [**?**]. It also stands for some of the greatest possible advances in medicine, mental health, and understanding of animal behavior (including our own). By collecting unstructured or semi-structured EEG data in the wild, passthought systems could help build better BCIs [**?**], or as training data for larger systems of diagnosis or analysis. One ambitious goal is to detect or even predict seizures [**?**].

Again, these opportunities must strike a balance with the risks of individual users' privacy and security. Violations of security could undermine passthoughts as an authentication platform, while violations of privacy 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.

7.6 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 ideosynchratic (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).

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

[] 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

[] 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

[] 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

[] 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?

[] 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

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

[] 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

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

[] 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

[] 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/

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

[] Max T Curran, Jong-kai Yang, Nick Merrill, and John Chuang. Passthoughts Authentication with Low Cost EarEEG. *EMBC 2017* (????).

[] 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

[] 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

[] 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

[] 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

[] 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

[] 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

[] 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

[] 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

[] 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

[] 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

[] 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

[] 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

[] Ivan Martinovic, Doug Davies, Mario Frank, Daniele Perito, Tomas Ros, and Dawn Song. 2012. On the Feasibility of Side-Channel Attacks with Brain-Computer Interfaces. In *Usenixorg (Security'12)*. USENIX Association, Berkeley, CA, USA, 1–16. https://www.usenix.org/system/files/conference/usenixsecurity12/sec12-final56.pdf

[] 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

[] 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

[] 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

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

[] 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.

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

[] 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

[] 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.

[] 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

[] Steven Spielberg. 2002. Minority Report. (2002).

[] Spire, Inc. Spire is the first wearable to track body, breath, and state of mind. (????).

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

[] 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

[] 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

[] Julie Thorpe, P C Van Oorschot, and Anil Somayaji. 2005. Pass-thoughts: 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

[] 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

[] 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

[] 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

[] LLC. United Sciences. Aware Hearables - World's First Custom-Fit Bluetooth Headphones with Brain and Body Sensors. (????). http://efitaware.com

[] 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

[] 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

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

[] 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?