Human-centered Behavioral and Physiological Security

Florian Alt
florian.alt@unibw.de
University of the Bundeswehr
Munich, Germany

Mariam Hassib
hassib@fortiss.org
fortiss Research Institute of the
Free State of Bavaria
Munich, Germany

Verena Distler
verena.distler@unibw.de
University of the Bundeswehr
Munich, Germany

ABSTRACT

We propose a paradigm shift in human-centered security research in which users' objective behavior and physiological states move into focus. This proposal is motivated by the fact that many personal and wearable devices today come with capabilities that allow researchers to assess users' behavior and physiology in real-time. We expect substantial advances due to the ability to develop more targeted approaches to human-centered security in which solutions are targeted at individuals' literacy, skills, and context. To this end, the main contribution of this work is a research space: we first provide an overview of common human-centered attacks that could be better understood and addressed through our approach. Based on this overview, we then showcase how specific security habits can benefit from the knowledge of users' current state. Our work is complemented by a discussion of the implications and research directions enabled through this novel paradigm.

CCS CONCEPTS

• **Security and privacy → Human and societal aspects of security and privacy**.

KEYWORDS

usable security, human behavior, physiology

ACM Reference Format:
Florian Alt, Mariam Hassib, and Verena Distler. 2023. Human-centered Behavioral and Physiological Security. In *New Security Paradigms Workshop (NSPW '23), September 18–21, 2023, Segovia, Spain.* ACM, New York, NY, USA, 14 pages. https://doi.org/10.1145/3633500.3633504

1 INTRODUCTION

In the past 20 years, following seminal papers such as "Johnny can't encrypt" [90], "Users are not the enemy" [7] and "User-centered Security" [96], the usable security community has focused on obtaining a profound understanding of human habits in security-related situations. Application areas include research on password selection and maintenance [16, 34, 84–86], habits while being exposed to phishing emails [29, 36, 95], shoulder surfing [12, 18, 35], and warning messages [9, 19, 56]. Research in these areas is characterized by different research approaches, from controlled studies, yielding insights of high internal validity (for example, letting participants perform an email classification task in a lab environment) to in-the-wild studies with a stronger focus on ecologic validity (for example, observing real-world phishing habits in companies).

For decades, methods such as interviews and questionnaires have established themselves as the prevalent approaches to data collection [33], primarily due to their ability to capture subjective, in-depth insights into users' reasoning, motivations, and habits. At the same time, the proliferation of ubiquitous computing technologies is bringing sensing ever closer to the human body, be it through sensors integrated into personal devices (smartphones), wearables (smartwatches, HMDs), or tangibles. Those technologies have been appropriated by the Ubicomp and HCI community, not only as a novel means for data collection but also to build novel, adaptive user interfaces able to target users' context and state.

The technologies above allow insights into human behavior, physiology, and context in real time and without the need for interaction by the user. Still, there are only a few applications in security to date. A prominent example is behavioral biometrics, the approach of identifying humans based on their behavior [77], for example, as they walk [71], type [87], or interact with technology [37]. We propose a paradigm shift towards leveraging the opportunities of behavioral and physiological sensing in the context of human-centered security. We believe this shift can open novel opportunities both regarding *obtaining an in-depth understanding of security-related situations* and to *building novel human-centered security technologies*. One example could be exploring how user states (for example, fatigue, attention) and context influence the susceptibility to human-centered threats. An example of a novel physiological security interface would be identifying when users are at risk and providing in-situ guidance and means for protection.

The ability to personalize and contextualize security approaches will pave the way towards more targeted security interventions, that is, security designs not created for the average user but targeted towards individuals and their situative needs. Such designs will allow accounting for what users already know, for what their cognitive and physical abilities are, and for offering help and protection in situations in which security challenges arise.

To achieve this, we contribute a research space that charts how behavioral and physiological sensing can be leveraged to build and enhance the security of interfaces. Firstly, we introduce human-centered threats, that is, threats exploiting the vulnerabilities of humans. This list serves as a basis for identifying human security habits, much of which has been the focus of the research community for decades. We then explain how knowledge about humans' individual states, derived from behavior and physiology, can be leveraged during the design of security mechanisms. A discussion of the challenges and future research complements our work.

NSPW '23, September 18–21, 2023, Segovia, Spain

ACM ISBN 979-8-4007-1620-1/23/09.
https://doi.org/10.1145/3633500.3633504

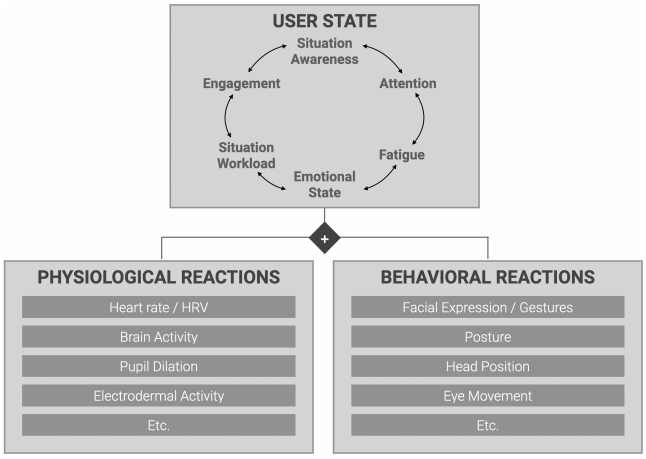

Figure 1: User State Model adapted from [83]: Physiological and behavioral reactions are predictive of user states.

2 BACKGROUND AND RELATED WORK

We introduce essential terms, explain the interplay of physiology and behavior, and shed light on how state-of-the-art approaches in human-centered security can benefit from this novel paradigm.

2.1 Terminology

We define *physio-behavioral security* as the use of sensor data with the objective of (1) improving understanding of how a technology user responds to a security-critical situation and (2) using this knowledge to improve the design of the system to increase security.

Depending on its objectives, a given study might make a stronger contribution to the first (understanding) or second (practical implications) part of this definition. Sensor data can include both behavioral data (e.g., typing behavior, mouse movement, touch targeting) as well as physiological data (e.g., heart rate, gaze, skin conductance). Types of sensor data are presented in section 4.3. Note that physio-behavioral data might be complemented with additional data types, allowing, for example, a particular context to be characterized (e.g., location data, presence of others, etc.).

We use the term *behavior* for any intentional user action that can be sensed. Well-learned user behavior (e.g., consistently using a password manager) will be referred to as *(security) habit*.

A *security-critical situation* refers to any moment in which a user's habits could substantially impact their security, regardless of their situational awareness. For instance, when creating a password, certain user habits would lead to better security (e.g., using a password manager). When receiving a phishing email, a user's action or inaction (clicking vs. not clicking on the phishing link) influences the risk of inadvertently downloading malware.

In these situations, physio-behavioral security can help understand the user's state in the moment and its security-relevant implications. A future perspective would be to use this knowledge to intervene in opportune moments and influence users' behavior.

In physio-behavioral security, a myriad of physiological and behavioral data streams can be relevant sources of information about the user's state. Physiological data collected by sensors placed on/around the human body include but are not limited to eye gaze data, heart rate, respiration rate, skin conductivity, and cortical activity (brain data), among others. Prior research in the areas of physiological sensing, affective computing, and cognitive systems provides a rich basis of how the body responds to external and internal stimuli and how these body signals can be used to infer user states such as attention, cognitive workload, stress, arousal, or emotions [83]. We discuss these signals in more detail in Section 4.3. Behavioral data refers to data collected due to actions from the users. These include typing and touching behaviors, mouse movement, body motion, and task performance behaviors (e.g., task accuracy and reaction time). We discuss behavioral data streams and the states that can be inferred in more detail in Section 4.3.

Both physiological and behavioral data can be collected through a wide variety of sensors that can be deployed either as wearables (for example, smart glasses, smart watches, on personal devices (for example, mobile phones), or in users' environments (for example, voice assistants, webcams, or eye trackers at users' desktops).

2.2 Research Methodology in Usable Security

A recent literature review investigated the methods used by the Usable Privacy and Security (UPS) community and found that interviews, experiments, and questionnaires were most frequently used by researchers [33]. The authors do not cite papers using behavioral or physiological measurements beyond click behaviors. Indeed, there are very few research papers in Usable Privacy and Security using these types of measurements so far (exceptions include [8, 64, 67, 93]), despite the potential these methods hold.

These frequently used self-reported methods hold some limitations. When self-reported methods are used to gain an understanding of security habits (as opposed to opinions, perceptions, etc.), the results rely on the research participants' ability to remember these habits. Researchers also often rely on hypothetical situations and study intentions rather than habits. When measuring, for instance, click behaviors, these measures are relatively simplistic and do not represent the details that can be represented in more nuanced behavioral or physiological measurements. In usable security, user states seem to play an important role. For instance, we know that people are more likely to fall for a phishing attack if they are stressed [78] or under a high workload [69] based on both in-situ observation and interview data [32] as well as research on the most successful phishing attacks, which use urgency cues (presumably causing time pressure) [91]. Using additional sensor data, we could obtain more fine-grained insights into situative user states.

2.3 Behavioral and Physiological Research in Usable Security

The use of behavioral and physiological data has been explored by research in usable security in the past decades. Still, it has, so far, been strongly driven by specific application areas and technology.

The most prominent and well-explored area is *behavioral biometrics*, that is, the use of behavior for uniquely identifying individuals. Much work has focused on understanding how accurately users can be identified based on different types of behavior. This includes, most importantly, keystroke dynamics [21, 23, 28, 30], touch targeting [24], and walking, but also behavior in virtual reality (VR)

[73] as well as gaze behavior [60]. Beyond specific application areas, researchers have looked at implications for the design of the user interface (e.g., smartphones [24]) and how data for training predictive models can be collected outside the lab [22]. From a security perspective, researchers have focused on threat models to behavioral biometrics [50, 65] and fallback authentication [66].

Furthermore, the role of gaze has been the focus of research [46]. Prior work looked at how eye gaze can be leveraged for explicit [31, 57], implicit [17, 59, 61], and multimodal authentication [49, 57]. Also, researchers have looked at how gaze could be used more generally to enhance security mechanisms. For example, Arianezhad et al. [10] demonstrated that security expertise is correlated with gaze duration while looking at security indicators. Mihajlov et al. [63] explored how much time users spend looking at different fields upon account registration. In graphical authentication schemes, eye gaze has been used to create dictionaries of frequently selected positions (hot-spots) [58] and to personalize authentication schemes [47, 75]

Looking at other types of physiological and behavioral data, we find fewer examples of how they can be employed in security-critical situations. Yu et al. investigated using mouse movement behavior to detect phishing email awareness [93]. Hashem et al. explored using Electroencephalography (EEG) and Electrocardiography (ECG) to detect insider attacks [39]. Neupane et al. used EEG and eye gaze to infer user behavior toward malware warnings and phishing email detection. This provides a basis for future real-time alerts based on user physiological and neurological behavior [70].

2.4 The Interplay of Physiology and Behavior

Prior work has explored the complex relationship between context, individual factors, and user states. In our research, we build on Schwarz et al.'s user state model [83]. It identifies six basic human states: situational awareness, engagement, attention, workload, fatigue, and emotional state. Those states are of particular interest in human-centered security, as they have a profound influence on how humans react in specific situations. For example, prior research found that people believe to be more susceptible to shoulder surfing as they are under high workload [78] or in a particular emotional state, such as stress [69]. Another example is that knowledge of attention can be leveraged to assess whether users noticed specific elements in emails hinting at a phishing attempt [67]. What is equally interesting is that attackers often try to elicit certain user states. For example, in social engineering, attackers often try to evoke the emotional state 'fear' to make users take certain actions (e.g., frightening users to lose access to their bank accounts) [38]. As a result, (real-time) knowledge of users' states is a powerful means to not only better understand a security-related situation but this information can also serve as a trigger for interventions designed to protect users from cybersecurity attacks.

Schwarz's model implies that humans' physiological reactions and behavior are predictive of their state, that is, if a system is capable of assessing physiological reactions (such as heart rate, pupil dilation, or electrodermal activity) and certain behaviors (facial expressions, postures, eye movements), it is possible to predict the current user state as in [83]. Note that other individual factors influence a person's state. Those include long-term factors (e.g., knowledge, ability, skills, experience, and motivation) and short-term factors (e.g., sleep, well-being, and personal needs).

We argue that understanding this interplay – which is primarily enabled by the proliferation of technology allowing individuals' physiology and behavior to be assessed – will enable a profound shift in how we build approaches to mitigate cyber-attacks.

3 EXAMPLES

We sketch two motivating examples of novel research approaches enabled by the proposed paradigm shift (cf. Figure 2). The first example concerns secure password habits. Here, we investigated what can be learned from understanding a user's state while registering a password [5, 6]. The second example looks at user states while being exposed to phishing emails. These examples represent two spots in a design space, charted in Section 4.

3.1 Password Behavior

We assessed the *interplay of password strength and cognitive load* [6]. We hypothesized that as users create stronger passwords, this will increase their cognitive load. To this end, we collected eye gaze and pupil dilation data while users entered a series of strong and weak passwords. Our analysis of users' pupil dilation as a measure of cognitive load revealed that composing stronger passwords consistently led to a stronger change in pupil dilation than weaker passwords (3).

Our findings have interesting implications. Firstly, it enables the *design of novel technologies* to protect people from choosing weak passwords. One example could be a 'ubiquitous password meter'. Think about users in the future wearing AR glasses capable of assessing users' cognitive load as well as identifying situations in which users are exposed to a password registration interface. The AR glasses could now inform users that they are about to choose a weak password (a) without knowing the actual password and (b) independent of whether the underlying password system implements means to analyze the entered password for its strength.

Secondly, the approach allowed interesting insights into users' habits to be gathered, enabling subsequent research. Figure 3 reveals two interesting observations. (1) For the first created password, the mean pupil diameter change is considerably smaller than for the subsequent passwords. This effect is likely caused by participants reusing a password (though the difference to weak passwords is still strong enough to make a distinction). (2) The mean pupil diameter change decreases over time. The explanation for this is that users, over time, developed a strategy for creating passwords (such as making up a sentence and then composing the password as the sequence of the first letters of the words in the sentence). This demonstrates the rich insights obtainable from assessing users' physiology and behavior in security-related situations.

We followed up by more closely investigating *password reuse* [5]. We looked into whether it is possible to infer password reuse from behavior and physiology. To this end, we conducted an experiment in which we let participants create passwords for two different websites. During this process, we assess users' gaze behavior and keystroke dynamics. We found that about 30% of users reused passwords. This allowed us to compare user states for cases in which users reused passwords and cases in which they did not.

Figure 2: Examples of how security systems can benefit from knowing users' states: Eye gaze and keystroke dynamics hinting at password reuse (left). Mouse movement and eye gaze hint at exposure to a phishing email (right).

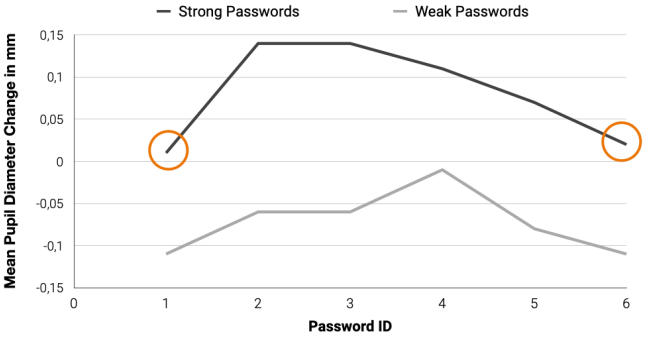

Figure 3: Influence of password strength on pupil diameter. When users are tasked to create a series of passwords, they often reuse a password (left circle), resulting in a lower cognitive load. After several passwords, they develop a strategy, resulting again in a decrease in cognitive load.

Our findings yield again interesting insights. We confirmed our hypothesis that a lower workload was associated with password reuse. However, we found that other gaze features had a stronger influence on the accuracy of the predictive model. More specifically, fixation duration had the most substantial influence, followed by saccadic duration, the number of fixations and saccades, and fixations on screen and keyboard. The latter two features are particularly interesting: The reason for which fixations on the screen and keyboard are a strong predictor is that for reused passwords, people have memorized finger movements (i.e., motor memory) and, hence, need to less frequently switch their gaze between the screen (password registration interface) and the keyboard. We also looked at user behavior, more specifically, their typing behavior. We found that differences between reusing a password and coming up with a new one were visible in the flight time between button presses, keystroke count, and typing duration.

Also here, the findings have some interesting implications from a practical perspective. While it is well-known that password reuse is the root cause for credential stuffing attacks, it is much less clear how to prevent such password choice habits, that is, how users can be supported in not reusing passwords. Existing approaches implemented by many password managers are to analyze the stored passwords for reused passwords and point this out to the user. However, this approach has been demonstrated to be hardly effective: changing a password once stored is cumbersome, and prior research showed that even in cases in which users become aware that their password has been part of a breach, only 13% of people changed their password within three months of the breach [15].

The findings of the work described above have the potential to address this in a fundamentally different way: knowing in real-time that users are about to reuse a password allows for intervening *before* users' finished the password registration process, that is, an intervention (e.g., real-time nudge) could point out the issues associated with password reuse in an opportune moment in which the cost for changing a password is minimal. We demonstrated that using gaze data, a prediction of password reuse from gaze data is possible already before users even start entering a password, as cognitive load as a result of making up a password can already be assessed before users start typing.

3.2 Exposure to Phishing Emails

In the third example, we investigate the influence of phishing emails on users' eye gaze and mouse movement behaviors [3]. To this end, we conducted a study in which participants engaged in a role-play scenario where users were asked to sort emails in their inbox into different folders (important, spam, neutral, bin) of a fictional character working in an IT company. During the role-play, gaze data and mouse movements were collected using remote eye tracking with the users' webcams. The collected gaze and mouse data was then analyzed, and features extracted.

Our findings demonstrate that certain features of mouse and gaze data were good indicators of whether or not a user has correctly detected a phishing email. Attention, as predicted through mouse hover speed and the number of gaze fixations on particular areas of interest, were significant indicators of whether a user was aware of phishing emails. As opposed to the aforementioned examples on password choice, reliable predictions were more difficult. The reason for this is, on the one hand, the complex nature of phishing emails. Here, the type of email, as well as the presence of indicators in emails hinting at phishing (e.g., ambiguous links), had a strong influence. On the other hand, individual differences across users played a role. For example, some users were more likely to click on links, which their risk-taking behavior could explain.

This example demonstrates both opportunities and challenges of building security approaches based on user states. The ability to predict exposure to a phishing email from user states that the user might not be consciously aware of or has learned to ignore could fundamentally change how we protect users from social engineering attacks. Rather than making users verify the legitimacy of every single email and making them think twice before they click a link or open an attachment, state-aware interventions would not only reduce warning fatigue. Still, they would also allow interventions to be highly individualized and tailored towards individual factors. At the same time, this example demonstrates the complexity of this approach due to the interplay of user state with context and individual factors, requiring further research.

3.3 Summary

The aforementioned examples show different application scenarios in which physiological and behavioral input, beyond biometrics for authentication, can be used in security-critical situations. The examples also surface some of the challenges and opportunities associated with such methods that should be explored in more detail. In the following section, we chart a research space meant to showcase the potential of the approach and help researchers identify interesting directions to explore.

4 A RESEARCH SPACE FOR PHYSIO-BEHAVIORAL SECURITY

In the previous section, we provided three examples of how human-centered security research can benefit from a shift of focus toward user behavior and physiology. The following section outlines a research space to demonstrate how the research community could systematically explore this area.

The research space (see Figure 4) consists of three dimensions: a human-centered attack space, human cybersecurity habits, and examples of behavior and physiological reactions to look at. It is worth noting that this research space is not but a snapshot in a constantly evolving threat landscape. It is intended as a scaffold based on which researchers can explore the potential of the approach and extend the space as novel threats emerge and as novel technologies to assess users' behavior and physiology become ubiquitous.

4.1 Human-Centered Attacks

The research space is centered around human-centered attacks aiming at obtaining sensitive information. Such sensitive information may be used to impersonate users or commit financial fraud. Account credentials, which attackers can exploit to authenticate, are of particular interest. User account access gives cybercriminals access to payment information (credit cards, bank accounts, PayPal), enabling them to commit financial fraud. Or it gives them access to a larger network, which they might explore and compromise. Common examples are (a) looking for and deleting backups, encrypting data, and demanding ransom in return for the decryption key (ransomware) or (b) ex-filtrating sensitive information and threatening to publish it unless the victim pays money (extortionware).

In the following, a non-comprehensive list of approaches to obtaining sensitive information is provided.

4.1.1 Guessing Attacks. Guessing attacks refer to cyber-attacks in which the impostor tries to obtain a secret (for example, a password, PIN, or lock pattern) through guessing. This usually happens during offline attacks where impostors try out many possible secrets. Example approaches include but are not limited to:

Brute Force Attacks In this attack, a malicious actor attempts to reveal account credentials by repeatedly trying different username and password combinations.

Dictionary Attack In this attack, a malicious actor attempts to reveal account credentials by trying words from a dictionary or a list of commonly used passwords.

Credential Stuffing Credential stuffing is an attack in which stolen usernames and passwords obtained from a data breach or phishing attack are used to gain access to multiple user accounts. This attack is becoming increasingly common as it is easy to conduct and can be used to access many accounts quickly and easily. The attack begins when malicious actors obtain a list of stolen usernames and passwords from a data breach or phishing attack. They then use automated programs to attempt to access multiple user accounts simultaneously using the same stolen credentials.

4.1.2 Observation Attacks. In observation attacks, impostors try to eavesdrop on credentials in the real world or the digital world.

Shoulder Surfing Shoulder surfing is an attack in which malicious actors observe users while entering information on a device without the user noticing. This attack is most commonly used to obtain passwords or other sensitive information, such as credit card numbers or bank account information. Shoulder surfing can be conducted in person or remotely via video surveillance. To protect against shoulder surfing attacks, users should monitor their surroundings when entering sensitive information. Other measures to counteract shoulder surfing are privacy screens, video surveillance, or physical barriers to prevent malicious actors from observing information.

Keyloggers Keyloggers are malicious programs that can capture keyboard input on a computer. Malicious actors use them to gain access to confidential information, such as passwords, credit card numbers, and other sensitive data. Keyloggers can be installed on a computer through malicious email attachments, websites, or software downloads. Once installed, the keylogger will capture all keystrokes on the computer, allowing the malicious actor to access confidential information. Keyloggers can also capture other information, such as screenshots of the computer's desktop or web activity. This allows malicious actors to access more information than just the keystrokes.

Sniffing Sniffing is an attack in which malicious actors use tools to capture and analyze data transmitted over a network. Tools such as WireShark can be used to capture confidential information, such as usernames, passwords, and credit card numbers. This information can then be used to access accounts and impersonate users. Sniffing attacks are difficult to detect, as the malicious actors are not actively attacking. Instead, they passively monitor the network traffic for any sensitive data being transmitted.

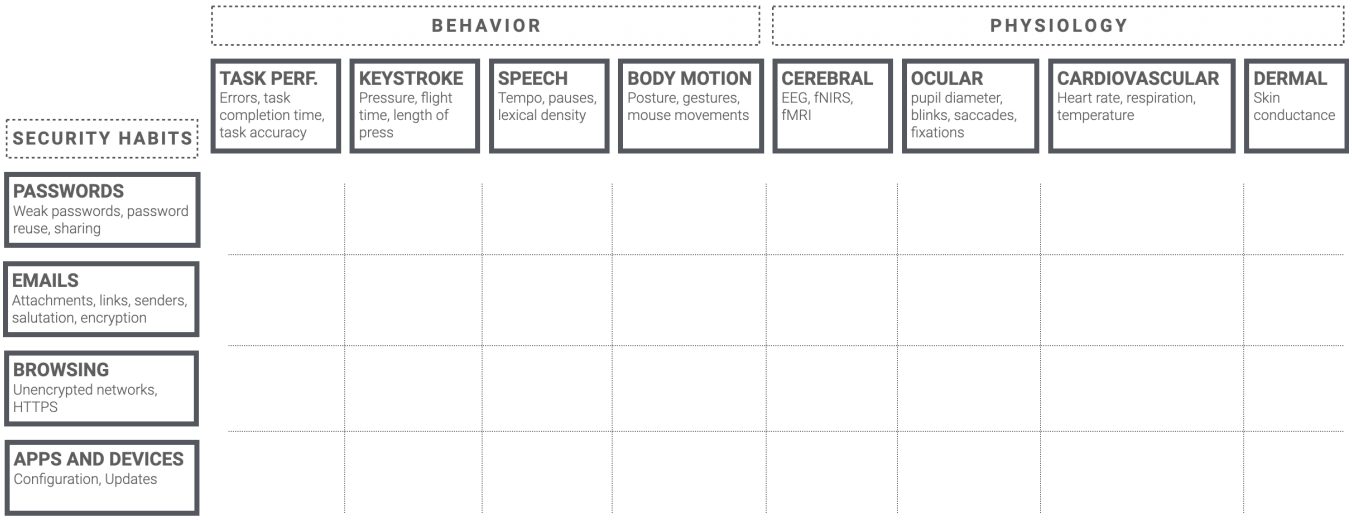

Figure 4: Research Space for User States in Security Tasks: Security habits lead to observable changes in user behavior and physiology. These changes can be used to target user interfaces to users' states better.

4.1.3 Social Engineering Attacks. Another approach is to make users reveal sensitive information, such as credentials, using a request that appears to be legitimate. Today, many different forms of social engineering exist. We focus here on very common ones:

(Spear) Phishing Spear phishing is a type of social engineering attack in which malicious actors target a specific individual or organization with a personalized and often convincing email. The email typically contains malicious links or attachments that, if clicked, will install malware on the user's computer or give the attacker access to sensitive information. Spear phishing is often difficult to detect, as the emails are carefully crafted to appear legitimate and often contain convincing information about the target. As spear phishing attacks are not sent in large numbers and are highly targeted, technical detection is also challenging.

Vishing Vishing is a social engineering attack in which malicious actors use voice communication, such as phone calls or voice messages, to manipulate victims into providing confidential information or taking action, such as transferring money from a bank account. These attacks typically begin with a phone call or voice message from an attacker, who may pose as a representative of a bank or other organization. The attacker will then attempt to manipulate the victim into providing confidential information or taking action, such as transferring money.

Further (sub)forms of social engineering exist, which mainly differ in the medium used. Prior years witnessed social engineering attacks through SMS (smishing), Twitter (twishing), pop-ups (pop-up phishing), and images (image phishing).

4.1.4 Reconstruction Attacks. Several forms of attacks exist in which impostors, once they obtain physical access to a device, try to reconstruct credentials.

Smudge Attacks Smudge attacks exploit the fact that skin fat produces a smudge trace whenever a user interacts with a surface. This trace is then clearly visible under slant incident light. Prior work has shown that this allows attackers to reconstruct the original password [13]. This type of attack is particularly critical for authentication systems in which the smudge trace can be directly matched to the secret.

Thermal Attacks As users enter credentials on a physical surface, thermal cameras can be used to reconstruct the password. Prior work has shown that, in particular, PINs and lock patterns are susceptible to this kind of attack [1], which could realistically occur in users' everyday lives as many opportunities for thermal attacks exist [14].

4.2 Human Cybersecurity Habits

The following section lists several possible target habits for more securely interacting in the digital world, specifically intending to mitigate the aforementioned attacks. The habits revolve around the choice of passwords, using emails, surfing the WWW, and application/device usage. Note, again, that this is not a comprehensive list. Still, this overview is meant to demonstrate the many application areas in which knowledge of the user state may open new opportunities to develop stronger means for protection.

4.2.1 Passwords. As described above, users' habits when it comes to creating, maintaining, and using passwords have a strong influence on human-centered attacks' success rate.

Weak Password Choice Weak passwords make them susceptible to guessing attacks. As a result, much work has been conducted on understanding users' password choices and how they can be supported in choosing stronger passwords. Several factors play a role here. Firstly, prior work has identified a lot of misconceptions users have about the strength of their passwords [88]. Hence, analyzing users' states might hint at such misconceptions and allow them to be addressed in a personalized manner. Secondly, the question is when there is an opportune moment to approach the user regarding choosing a strong password. For example, most online shopping websites require users to create an account and

password upon checkout. At this moment, however, the user is strongly focused on the checkout process with a presumably low motivation to invest effort in choosing a strong password. A better understanding of where and when users direct their attention during tasks might help identify more suitable moments for approaching users with the request to set a password.

Password Reuse Password reuse is a dangerous practice, as it enables credential stuffing attacks targeting multiple accounts protected with the same credentials. At the same time, this danger is unclear to many users. Services and tools, such as https://haveibeenpwned.com/, are attempts to address this but struggle with the fact that users would need to engage with them actively. With knowledge of users' behavior, it might be possible to build interventions that integrate both means to explain this threat to the user while at the same time guiding how to mitigate attacks resulting from password reuse.

Sharing Passwords Passwords can be shared. While an apparent challenge here is that sharing credentials makes it more difficult to keep track of who has access to the password, another challenge is that how the password is being shared may lead to malicious actors gaining access (e.g., sending a password through unencrypted email or text message). Here, knowledge of situational awareness might help mitigate cases in which password confidentiality is at risk.

Entering Passwords Finally, as explained in the attack space, passwords might be subject to observation or reconstruction attacks. Knowledge of where users are directing their attention upon password entry might help build interventions that protect users from attacks such as shoulder surfing. For example, Saad et al. showed how shoulder surfing attempts can be communicated to the user [79]. Yet, knowledge of the user state might help to minimize any harmful influence of interventions (warning fatigue, distraction).

4.2.2 Emails. The second category of security habits concerns users working on emails. As has been described above, phishing is an omnipresent threat to emails. Many phishing emails exploit users' states. For example, it is well known that phishing emails are often sent close to the end of a working day when users are tired or less engaged. Or they target situations of high workload, for example, close to public holidays. Or they elicit and target emotional states, such as fear or stress. In the following, several aspects of working on emails are described, alongside pointing out opportunities for better protecting users based on knowledge of their state. Of interest is the work of Pfeffel et al. [72], who assessed where users direct their attention when looking at emails. Their findings show users mostly looked at the header and body. Hence, interventions might focus on those areas.

Attachments Many phishing emails contain attachments with malicious software, for example, a keylogger subsequently monitoring and transmitting users' keystrokes.

Links A common approach in phishing emails is making users click on a link, directing them to a fake website on which they are supposed to enter their credentials. Email interfaces might benefit from the ability to assess users' attention towards suspicious elements, of which links are but one. An example of work in this direction is EyeBit [68], a browser extension using eye tracking to check whether users have looked at a URL (to check its legitimacy) and, before the user has done so, deactivates all input forms.

Senders Attackers often send phishing emails from fake email addresses. They try to conceal this by using a different sender name (usually of a person being impersonated). While many email programs display the email address next to the sender's name, this is often not true for mobile email apps. Knowledge of user attention might be used similarly to make them verify an email's legitimacy.

Salutation The salutation is an important element hinting at the legitimacy of an email. Bad phishing emails often use a generic salutation (such as 'Dear Sir or Madam') to address the user. Again, knowledge of users' attention could serve as a means to assist users in spotting discrepancies in the salutation (e.g., approaching the user with their last name even though the impersonated person usually approaches the user with their first name).

Encryption The final habit is the use of email encryption to make it impossible for an attacker intercepting the email to read its content. Here, the user state might hint at whether users struggle with setting up email encryption in the first place or whether they have considered encrypting an email before sending a message.

4.2.3 Browsing. The third class of habits concerns users while browsing. Here, of particular interest are situations in which users are browsing in unfamiliar environments (hotels, public transport).

Encrypted Networks Many public WiFis, as found in hotels, at airports, and in trains, are unencrypted. While tools, such as VPN, help users protect themselves, these tools are often unknown to users, or they forget to enable them. Knowledge of the user state might help to build interventions that assist users in protecting their Internet connection.

HTTPS When accessing and, in particular, authenticating on websites, the use of HTTPS ensures the transmitted information is encrypted. Here, again, knowledge of users' states might hint at users' being unaware of this.

4.2.4 Applications and Devices. As users install new devices (e.g., a router or smart home appliance) or an app, these require proper setup and maintenance.

Configuration The first step is usually the device's configuration. Optimally, the manufacturer ships devices/apps with secure settings. Still, security settings might lead to devices not working properly, resulting in users deactivating more features than necessary. If a system identifies a high workload, this might hint at the user being overwhelmed with the current security task. Hence, information could be better targeted towards the knowledge/skills of the user.

Updates Updates are generally seen as annoying tasks, interrupting users' main tasks. Knowledge of users' situational awareness and attention might allow the request for an update to be targeted at an opportune moment.

4.3 Human State Detection

The following section provides an overview of human behavior and physiological responses that are predictive of user states.

4.3.1 Behavior. The user's behavior during interaction with a system can be used to infer their state. In the following, we provide a brief overview of various behaviors which can be captured and the potential user states that prior research has investigated.

Task Performance There are multiple metrics of task performance, including the number of errors, task completion time (TCT), task accuracy, and user reaction time while doing a given task. A large body of research shows these metrics to provide insight into cognitive load [55].

Keystroke Dynamics Keystroke dynamics refer to the users' behavior while typing, whether on physical buttons on a keyboard or virtual touch keyboards. Keystroke dynamics have been extensively researched as an authentication method (for a review, see [76]). Additionally, keystroke dynamics can be used to infer cognitive load [20, 55] and are useful indicators for emotion [62].

Speech Microphones are embedded in most devices we use today (laptops, mobile phones, voice assistants). A change in the users' cognitive load can be measured through many of the features of speech, such as tempo [25], pauses [51], or lexical density [51]. In addition to cognitive load, emotion recognition from speech is also a well-researched area [48].

Body Motion Movement of the whole or parts of the body is a relevant indicator for many user states. Capturing body movements can be done using on-body/on-device sensors or cameras in the environment. Body posture and gestures have been explored as an indicator for cognitive load [43]. Mouse Movement behavior during the interaction, such as the speed/pauses of mouse movements, have been shown to indicate attention [93] and cognitive load [11]. Additionally, Electromyography (EMG), which refers to measuring the activity of the muscles using on-body sensors, can indicate user states such as stress and emotion [89].

4.3.2 Physiology.

Cerebral Among many neuroimaging techniques used to collect brain data, Electroencephalography (EEG) and Functional Near Infrared Spectroscopy (fNIRS) are two common, non-invasive, and relatively light-weight methods that can provide insights about the cognitive processes of the brain. Both techniques are used to measure cortical activity [55]. In EEG, conductive electrodes placed on the scalp collect electrical potentials between 1 and 100 microvolts. The collected EEG data is then processed, and different features can be extracted. Using machine learning techniques, prior research has shown that EEG data can provide insights about users' cognitive load [55], engagement [42], and positive and negative valence [40]. In contrast to measuring electrical potentials with electrodes, fNIRS uses near-infrared light within a range of 650 nm to 1000 nm to measure changes in the concentration of Oxygenated (HBO) and Deoxygenated Hemoglobin (HbR) in the human brain [55]. The device comprises light emitters placed on the human scalp to measure the outcoming light, showing the amount of oxygen used. fNIRS has been shown to detect mental workload [55] successfully. While neuroimaging techniques had remained for decades confined to lab settings, portable and light-weight EEG/fNIRS sensors are becoming more available and enable their usage in more realistic setups (e.g., in workplaces [41], in lectures [42], while playing piano [94], and while driving [40]). Hence, we see the opportunity to use them in the context of human-centered security.

Ocular The eye provides a fascinating entryway to the state of the human body. Many types of eye movements (voluntary and involuntary) can be easily captured using eye trackers. Eye trackers can be stationary (attached to a display) or wearable as part of an HMD/smart glasses. Capturing eye movements has also been done on unmodified mobile phone devices using their cameras. Eye movements have long been researched as an interaction modality and for evaluation. Several eye movement features have been extensively explored in prior research, including eye blinks, fixations (voluntary movements focusing on an area of interest), saccades (the shifting movement between two areas of interest), smooth pursuit movements (following a moving object), and pupil dilation, among others. Prior research has shown all these eye features can be used to predict cognitive load [53–55]. Furthermore, eye gaze data has been extensively studied as an (additional) form of multi-modal input for authentication schemes [49], or as an indicator for password strength and reuse (cf. examples in Section 3 [5, 6]). Having been a technology constrained to lab settings for decades, eye tracking is today affordable and robust enough for real-world deployment, for example, in workplaces [45].

Cardiovuscular, Respiratory, and Nervous Systems The systems of the human body work closely together and influence one another. Heart rate, its derived metrics (e.g., Heart Rate Variability), breathing rate, and body temperature are all influenced by the human state (e.g., stress and emotional state) and have strong relations to one another [55]. Additionally, measuring and collecting these signals has become accessible to novice and expert users. Heart rate can be measured using electrocardiography (ECG) and photoplethysmography (PPG) in the time and frequency domains unobtrusively using wearable devices (e.g., chest band, smartwatch). Prior research showed that heart rate can give insight into users' mental workload during different tasks, for example, in the work context [27]. The respiratory system is responsible for breathing and its regulation. Like heart rate, breathing rate can be easily captured using wearable sensors. Research has shown that cognitive workload impacts respiration [44]. Prior research has also shown that combining Heart Rate Variability and breathing rate features and applying machine learning classifiers can lead to a good classification of emotions such as joy [52]. Finally, body temperature, regulated by the nervous system and in close relation with the cardiovascular system, can be an indicator of states, such as stress and cognitive load. Body temperature can easily be

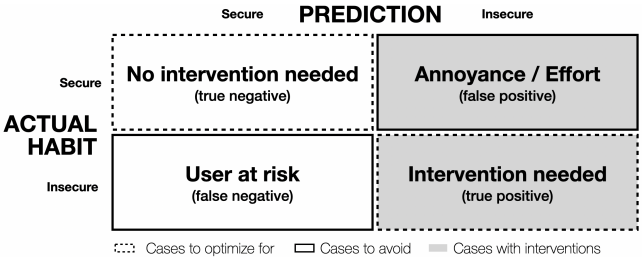

Figure 5: Our paradigm enables novel interventions. Due to the probabilistic nature, there is a possible mismatch between users' actual habits and system predictions based on the user state. Interventions must balance being annoying / creating effort (top right) and putting users at risk (bottom left).

captured using thermal imaging cameras or using on-body temperature sensors and combined with other smart wearable sensors (e.g., HR). Prior research explored the use of thermal cameras to detect levels of cognitive load [2] and stress [92]. Commercial smartwatches can capture many of the aforementioned metrics, making these applicable in organizational settings.

Dermal Another physiological response related to the nervous system is electrodermal activity (EDA), measurable by applying currents to assess the conductance or resistance of the skin [55]. EDA has been found to be successful at detecting stress and emotional arousal in various scenarios such as office work [81], driving [82], or during interaction in VR [26]. EDA can be detected by many commercial smartwatches, such as the Fitbit Sense.

4.4 Using the Research Space

We believe that the high-level perspective on physio-behavioral security offered by the research space will be useful for researchers moving forward. When positioning the described work on physio-behavioral measurements in the research space (Figure 4), we can see that most existing work is limited to certain quadrants. For instance, the quadrant at the intersection of passwords and ocular measurements would include comparatively many studies (e.g., [5, 6, 49]), whereas most quadrants are, so far, unexplored or under-explored. We suggest that researchers could use the research space to position the novelty of their research ideas but also use the present paper to find usable security research that used, for instance, similar sensor measurements but with a different security task.

Broadly, three major research directions can benefit from this work. Firstly, behavioral and physiological data can enhance our *theoretical understanding* of security habits, for example, through understanding phenomena and deriving theories. Secondly, we support building *enabling technologies*; that is, researchers can explore how meaningful data can be collected, which features are suitable to make predictions, to build predictive models, and to assess how accurately those work. Thirdly, researchers can build *interventions*, that is, user interfaces using knowledge of user states. One purpose of those interventions could be to protect users by helping them take meaningful action (for example, pointing out the risks of a weak password or raising awareness of a potential phishing attack).

An emerging challenge concerning interventions is coping with probabilities. Figure 5 visualizes this challenge. Generally, any intervention built on knowledge about user states tries to maximize prediction accuracy to support making a correct prediction (top left, bottom right). In cases where a system predicts secure user habits and this is true, no intervention is needed. The most interesting case is where the users' habits are insecure, and this is correctly predicted by the system. In this case, an intervention can be expected to be most effective. Challenging cases are a mismatch between what the system predicts and how users behave: If the system predicts a secure habit but it is in fact insecure, this puts the user at risk. Vice versa, if the system predicts an insecure habit but it is in fact secure, then this is annoying for the user. Future work could explore how, depending on the application area, a balance can be found between those two cases. One approach to address this could be to outsource edge cases: for example, if the system is not sure about a threat (for example, an email being phishing), then the response email by a user could be checked by a security expert from the IT department. This would reduce the burden on the user. At the same time, this raises ethical concerns, and researchers should answer when and how users should be informed about and consent to such practices.

A general question is how to choose areas in the research space to focus on first. This choice could be guided by considering the likeliness and severity of attacks. For example, automated attacks, such as credential stuffing, are likely to cause more damage as opposed to cases where, for example, attackers need to be physically present (cf. shoulder surfing).

5 DISCUSSION

In the previous sections, we have sketched a research space, showcasing the interplay between human-centered attacks and human security habits to mitigate these attacks on one side and human states and how they can be predicted on the other side.

Based on prior research and our reflections about the research space, the following section will sketch and discuss a set of open research directions.

5.1 Relevance of User States to Security Contexts and Transfer Between Security-Relevant Situations

So far, only isolated spots in the research space have been explored. It is an open question of which user states are relevant to which security habits and which human-centered attacks can be prevented. It appears that for attacks such as social engineering, the emotional state, fatigue, and attention are of particular interest. For security habits, engagement, and situational awareness seem promising states to focus on. Workload and situation awareness seem to be relevant across many areas, on one hand, because security is typically a secondary task and on the other hand. After all, most threats in the digital world are not directly perceivable.

Once researchers have obtained a better understanding of how different research areas inside usable security can benefit from an understanding of user states, it is relevant to consider the extent to which the knowledge gained in one area of UPS can be transferred to other security-relevant situations.

5.2 Privacy

Security and privacy often require a trade-off. Think, for example, about the use of VPNs. While VPN offers security when using an unencrypted network, it comes at the expense of privacy, as the VPN provider will inevitably be able to observe the traffic. We expect that there will be a similar trade-off between the security that may be provided by collecting and utilizing sensor data and new privacy risks while doing so. Future work could look at, but not limit itself to, user concerns and privacy concerns emerging from data sharing and data inference.

5.2.1 User Concerns. Research is needed to better understand end users' concerns regarding using physiological and behavioral data. Prior work in the HCI community has looked at people's views towards novel sensing technologies, for example, thermal imaging [80] and the use of EEG [74]. Methodologically, prior work generally demonstrated to users both opportunities and challenges emerging from using the technology. To the best of our knowledge, the opportunities of behavioral and physiological data for cybersecurity have not been assessed in prior work. It will be interesting to see how perceive view this trade-off.

5.2.2 Data Sharing. Third parties could be interested in physiological and behavioral data, including employers or insurance companies. It is an open question how people would negotiate the boundaries around their physio-behavioral data in the various spheres of their lives. We see a particular need to explore how the interests of users and employees could be preserved, be it through policy or technical means. This closely relates to how technical means could be implemented to protect users' privacy. While protection might work in cases where approaches are targeted towards a specific context (at home, at work) or a user group (elderly, children), this might become much more difficult in cases using personalization (e.g., mechanisms adapting to the specific needs, skills, and level of knowledge of an individual user).

5.2.3 Data Inference. Using sensors to capture behavioral and physiological data creates large sets of personal data (e.g., distribution of workload and fatigue over the day, people's interests, and emotional state), which can create novel privacy concerns. The generated datasets might, for instance, reveal health conditions still unknown to study participants or end users (e.g., heart rate abnormalities). Such ethical concerns are rather new in Usable Security and Privacy research but well-known in the medical field. Hence, collaborations with medical staff and researchers are advisable.

5.3 Stakeholder View

Many stakeholders would be involved in the design, implementation, use, and maintenance of security approaches based on physio-behavioral data. For *designers and developers*, the system complexity may play a role. How can the required data be collected? Where is data being stored? Where are classifiers trained? Where are models being stored? How often do models need to be retrained?

From a *marketing* point of view, a relevant question concerns suitable business models. The development, deployment, and maintenance of strong security mechanisms come at a cost. The question remains whether it will, at some point, become a legal requirement to provide secure systems and whether a high level of security protection could become a purchase argument for end users.

From an *end users'* perspective, future work should look at the value proposition. At the moment, it is unclear how users would judge the trade-off between added security and the use of sensitive data, as well as the potential loss of control. This is likely to influence their motivation to use such approaches. At this same time, Adams et al. have shown that clearly communicating why certain types of behavior and mechanisms are useful from a security perspective increases users' motivation [7].

The various stakeholders will likely have different views on what "successful" physio-behavioral security interventions would imply. Such indicators of success could include organizational cost, behavior changes over time, and user experience.

5.4 Validity of Inferences Based On Sensor Data

It is an open challenge to understand and validate the inferences that can be made based on various sensor measurements. Some concepts that could potentially be inferred from sensor data are highly complex. For instance, while various existing smartwatches claim to measure stress, device manufacturers are not transparent about how such indicators are calculated, making it difficult for researchers to investigate the validity of these indicators, including their limitations. More research into the meaning one can infer from sensor measurements is needed, and interdisciplinary collaborations seem especially promising.

5.5 Methodological Challenges

Our paradigm holds a variety of methodological challenges.

5.5.1 Ecologic Data Validity. A fundamental challenge is how data of high ecologic validity can be collected for systems built on behavioral and physiological data, that is, data reflecting users' natural behavior. Much prior work has focused on collecting data under controlled conditions in the lab. Still, it is unclear to which degree user behavior in the lab is comparable to user behavior in the real world. This challenge has been recognized by researchers, leading to an attempt to collect unbiased, real-world data. Examples are the work of Buschek et al., who built an Android keyboard to collect the natural typing behavior of users over several weeks [22] as well as a research project funded by the German National Research Foundation (DFG) exploring behavioral biometrics in the real world[1].

5.5.2 Access to High-Quality Measurement Devices. It can be costly for researchers to acquire the needed measurement devices (e.g., eye trackers, wearables) and get access to sufficiently large participant pools to gain quantitative insights. It seems promising to build and strengthen collaborations with industrial partners to gain access to realistic settings in which human-centered physio-behavioral security might make important contributions.

From a research perspective, medical-grade devices could be used to demonstrate the general feasibility of approaches. However, whether or not these approaches will be put into practice depends on whether off-the-shelf end-user technology will be ready to deliver data at the required level of detail and quality.

[1] Scalable Biometrics Project: https://gepris.dfg.de/gepris/projekt/425869382

5.5.3 Uncertainty of Predictions. Future work should also address the question of which approaches to predictive modeling are most suitable in the context of physio-behavioral security. Here, a significant challenge concerns the communication of uncertainty associated with predictions. For instance, there is a likelihood of false positives (e.g., warnings that are triggered based on a physiological state when it is not warranted), which need to be explained and communicated to research participants as well as potential end users to avoid a loss of trust in the security system.

An interesting question in this regard is balancing accuracy and privacy. For example, systems could be built based on user-independent models; that is, a predictive model would use data of several users with a certain profile. This would allow for anonymization. At the same time, such user-independent models likely yield lower accuracy. In contrast, a higher accuracy may be achievable using user-dependent models. However, this would require data on a per-user basis. Future work should explore when to prioritize which approach. One idea here would be to consider different 'risk profiles': for example, to some, a bank account might seem more sensitive and thus worthy of stronger protection than a social media account. usually requires stronger protection than a social media account. Hence, the former account might rather be protected through a user-dependent model. User-centered methods (e.g., co-design) should be used to collaboratively define acceptable vs. unacceptable predictive models in collaboration with end users.

5.5.4 Social Desirability. Research participants' knowledge about data collection might influence their behavior. For instance, knowing that one's physical activity is being recorded by researchers might increase the desire to move more to seem more active. Such effects need to be carefully studied and quantified so that researchers can estimate how much an observation setting influences the participants' behavior and situate study results accordingly.

5.6 Novel Threat Models

An open question is which novel threat models the paradigm enables. Regarding behavioral biometrics, prior research explored so-called mimicry attacks [65], that is, attackers trying to mimic the victim's behavior. Beyond this, fine-grained knowledge about user states might provide valuable information to attackers when and how to perform attacks best. Still, such knowledge is first and foremost valuable for end-users as they could use it to adapt their habits based on their states (for example, working on emails at times of the day when they are likely to spot phishing emails best).

5.7 Other Application Areas

The approach has implications beyond security applications.

5.7.1 Privacy Research. Using sensor data could also be helpful in the context of privacy habits, as research on privacy shares many security research challenges. For example, privacy-related tasks, such as setting privacy permissions, are also secondary tasks for which a relatively low user motivation can be assumed. Certain measurement data could correlate with more or less privacy-preserving habits, and by understanding such correlations, we might tailor interventions to a person's behavior or physiological state. Privacy tasks might equally benefit from knowledge of the user state. Future work might set out from our research space and replace the categories 'human-centered attacks' with 'privacy violations' and 'human security habits' with 'human privacy habits'. Interesting aspects to investigate include how people's states are influenced while setting, managing, or revoking privacy permissions. Various applications exist, including smartphone permission, browser permissions, and permissions for IoT devices.

5.7.2 Fake News. An equally interesting research area is fake news. Prior research examined how users' gaze and mouse movement behavior differs when perceiving fake content compared to legitimate content [4]. Future research could expand upon this to understand how user states are affected beyond the perception of fake news, for example, during verifying and reporting fake news.

5.7.3 Deep Fakes. Deep Fake research might benefit from the proposed paradigm shift. Researchers might explore how situations in which users are exposed to deep fakes influence their state. An increase in attention towards the video of a participant in an online meeting could hint at deep fakes and be used to propose strategies for other meeting attendees to verify the participant's identity.

5.8 Need for Interdisciplinary Research

In this paper, we take a view from the usable security and privacy perspective towards the proposed paradigm. However, this paradigm is of interest and can strongly benefit from the involvement of different disciplines. On one hand, this includes other research areas in computer science: novel user interfaces will benefit from the expertise of the HCI community; privacy researchers can help with protecting users' privacy; and AI researchers can help with creating more accurate (predictive) models. On the other hand, this work can strongly benefit from joint work with the social sciences, medicine (cf. Section 5.2.3), as well as policymakers.

6 CONCLUSION

We proposed a paradigm shift towards physio-behavioral approaches to security, that is, approaches leveraging knowledge of human behavior and physiology with the ultimate goal of building novel, human-centered security interfaces. After providing three motivating examples, we sketched a research space introducing three dimensions and explaining their interplay. The research space is meant as a starting point for the research community to explore the proposed paradigm. We complement our work by elaborating on opportunities and challenges that could be explored in future work and briefly discussing application areas beyond security.

ACKNOWLEDGMENTS

This work has received funding from dtec.bw – Digitalization and Technology Research Center of the Bundeswehr [Voice of Wisdom]. dtec.bw is funded by the European Union – NextGenerationEU. Furthermore, this work has received funding from the DFG under grant number 425869382.

REFERENCES

[1] Yomna Abdelrahman, Mohamed Khamis, Stefan Schneegass, and Florian Alt. 2017. Stay Cool! Understanding Thermal Attacks on Mobile-based User Authentication. In *Proceedings of the 35th Annual ACM Conference on Human Factors in Computing Systems (CHI '17)*. ACM, New York, NY, USA. https://doi.org/10.1145/3025453.3025461

[2] Yomna Abdelrahman, Eduardo Velloso, Tilman Dingler, Albrecht Schmidt, and Frank Vetere. 2017. Cognitive Heat: Exploring the Usage of Thermal Imaging to Unobtrusively Estimate Cognitive Load. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 1, 3, Article 33 (sep 2017). https://doi.org/10.1145/3130898

[3] Yasmeen Abdrabou, Felix Dietz, Ahmed Shams, Pascal Knierim, Yomna Abdelrahman, Ken Pfeuffer, Mariam Hassib, and Florian Alt. 2023. Revealing the Hidden Effects of Phishing Emails: An Analysis of Eye and Mouse Movements in Email Sorting Tasks. arXiv.org. arXiv:2305.17044 [cs.HC]

[4] Yasmeen Abdrabou, Elisaveta Karypidou, Florian Alt, and Mariam Hassib. 2023. Investigating User Behaviour Towards Fake News on Social Media Using Gaze and Mouse Movements. In *Proceedings of the Usable Security Mini Conference 2023 (USEC'23)*. Internet Society, San Diego, CA, USA. https://doi.org/10.14722/usec.2023.232041

[5] Yasmeen Abdrabou, Johannes Schütte, Ahmed Shams, Ken Pfeuffer, Daniel Buschek, Mohamed Khamis, and Florian Alt. 2022. "Your Eyes Say You Have Used This Password Before": Identifying Password Reuse from Gaze Behavior and Keystroke Dynamics. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems (CHI '22)*. ACM, New York, NY, USA. https://doi.org/10.1145/3491102.3517531

[6] Yasmeen Abdrabou, Ahmed Shams, Mohamed Omar Mantawy, Anam Ahmad Khan, Mohamed Khamis, Florian Alt, and Yomna Abdelrahman. 2021. GazeMeter: Exploring the Usage of Gaze Behaviour to Enhance Password Assessments. In *ACM Symposium on Eye Tracking Research and Applications (ETRA '21)*. ACM, New York, NY, USA, Article 9, 12 pages. https://doi.org/10.1145/3448017.3457384

[7] Anne Adams and Martina Angela Sasse. 1999. Users Are Not the Enemy. *Commun. ACM* 42, 12 (dec 1999), 40–46. https://doi.org/10.1145/322796.322806

[8] Abdulaziz Almehmadi. 2021. Micro-Behavioral Accidental Click Detection System for Preventing Slip-Based Human Error. *Sensors* 21, 24 (2021). https://doi.org/10.3390/s21248209

[9] Bonnie Brinton Anderson, Anthony Vance, C. Brock Kirwan, Jeffrey L. Jenkins, and David Eargle. 2016. From Warning to Wallpaper: Why the Brain Habituates to Security Warnings and What Can Be Done About It. *Journal of Management Information Systems* 33, 3 (2016), 713–743. https://doi.org/10.1080/07421222.2016.1243947 arXiv:https://doi.org/10.1080/07421222.2016.1243947

[10] Majid Arianezhad, L. Jean Camp, Timothy Kelley, and Douglas Stebila. 2013. Comparative Eye Tracking of Experts and Novices in Web Single Sign-On. In *Proceedings of the Third ACM Conference on Data and Application Security and Privacy (CODASPY '13)*. ACM, New York, NY, USA, 105–116. https://doi.org/10.1145/2435349.2435362

[11] Syed Arshad, Yang Wang, and Fang Chen. 2013. Analysing Mouse Activity for Cognitive Load Detection. In *Proceedings of the 25th Australian Computer-Human Interaction Conference: Augmentation, Application, Innovation, Collaboration (OzCHI '13)*. ACM, New York, NY, USA, 115–118. https://doi.org/10.1145/2541016.2541083

[12] Adam J. Aviv, John T. Davin, Flynn Wolf, and Ravi Kuber. 2017. Towards Baselines for Shoulder Surfing on Mobile Authentication. In *Proceedings of the 33rd Annual Computer Security Applications Conference (ACSAC '17)*. ACM, New York, NY, USA, 486–498. https://doi.org/10.1145/3134600.3134609

[13] Adam J. Aviv, Katherine Gibson, Evan Mossop, Matt Blaze, and Jonathan M. Smith. 2010. Smudge Attacks on Smartphone Touch Screens. In *Proceedings of the 4th USENIX Conference on Offensive Technologies (WOOT'10)*. USENIX Association, USA, 1–7.

[14] Paul Bekaert, Norah Alotaibi, Florian Mathis, Nina Gerber, Aidan Christopher Rafferty, Mohamed Khamis, and Karola Marky. 2022. Are Thermal Attacks a Realistic Threat? Investigating the Preconditions of Thermal Attacks in Users' Daily Lives. In *Nordic Human-Computer Interaction Conference (NordiCHI '22)*. ACM, New York, NY, USA, Article 76, 9 pages. https://doi.org/10.1145/3546155.3546706

[15] Sruti Bhagavatula, Lujo Bauer, and Apu Kapadia. 2020. (How) Do people change their passwords after a breach? *arXiv preprint arXiv:2010.09853* (2020).

[16] Robert Biddle, Sonia Chiasson, and P.C. Van Oorschot. 2012. Graphical Passwords: Learning from the First Twelve Years. *ACM Comput. Surv.* 44, 4, Article 19 (sep 2012), 41 pages. https://doi.org/10.1145/2333112.2333114

[17] Ralf Biedert, Mario Frank, Ivan Martinovic, and Dawn Song. 2012. Stimuli for Gaze Based Intrusion Detection. In *Future Information Technology, Application, and Service*, James J. (Jong Hyuk) Park, Victor C.M. Leung, Cho-Li Wang, and Taeshik Shon (Eds.). Springer Netherlands, Dordrecht, 757–763.

[18] Leon Bošnjak and Boštjan Brumen. 2020. Shoulder surfing experiments: A systematic literature review. *Computers & Security* 99 (2020), 102023. https://doi.org/10.1016/j.cose.2020.102023

[19] Cristian Bravo-Lillo, Lorrie Faith Cranor, Julie Downs, and Saranga Komanduri. 2011. Bridging the Gap in Computer Security Warnings: A Mental Model Approach. *IEEE Security & Privacy* 9, 2 (2011), 18–26. https://doi.org/10.1109/MSP.2010.198

[20] David Guy Brizan, Adam Goodkind, Patrick Koch, Kiran Balagani, Vir V. Phoha, and Andrew Rosenberg. 2015. Utilizing linguistically enhanced keystroke dynamics to predict typist cognition and demographics. *International Journal of Human-Computer Studies* 82 (2015), 57–68. https://doi.org/10.1016/j.ijhcs.2015.04.005

[21] Ulrich Burgbacher and Klaus Hinrichs. 2014. An Implicit Author Verification System for Text Messages Based on Gesture Typing Biometrics. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '14)*. ACM, New York, NY, USA, 2951–2954. https://doi.org/10.1145/2556288.2557346

[22] Daniel Buschek, Benjamin Bisinger, and Florian Alt. 2018. ResearchIME: A Mobile Keyboard Application for Studying Free Typing Behaviour in the Wild. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (CHI '18)*. ACM, New York, NY, USA, 1–14. https://doi.org/10.1145/3173574.3173829

[23] Daniel Buschek, Alexander De Luca, and Florian Alt. 2015. Improving Accuracy, Applicability and Usability of Keystroke Biometrics on Mobile Touchscreen Devices. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI '15)*. ACM, New York, NY, USA, 1393–1402. https://doi.org/10.1145/2702123.2702252

[24] Daniel Buschek, Alexander De Luca, and Florian Alt. 2016. Evaluating the Influence of Targets and Hand Postures on Touch-based Behavioural Biometrics. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (CHI '16)*. ACM, New York, NY, USA, 1349–1361. https://doi.org/10.1145/2858036.2858165

[25] Rui Chen, Tiantian Xie, Yingtao Xie, Tao Lin, and Ningjiu Tang. 2016. Do Speech Features for Detecting Cognitive Load Depend on Specific Languages?. In *Proceedings of the 18th ACM International Conference on Multimodal Interaction (ICMI '16)*. ACM, New York, NY, USA, 76–83. https://doi.org/10.1145/2993148.2993149

[26] Francesco Chiossi, Robin Welsch, Steeven Villa, Lewis Chuang, and Sven Mayer. 2022. Virtual Reality Adaptation Using Electrodermal Activity to Support the User Experience. *Big Data and Cognitive Computing* 6, 2 (2022). https://doi.org/10.3390/bdcc6020055

[27] Burcu Cinaz, Bert Arnrich, Roberto La Marca, and Gerhard Tröster. 2013. Monitoring of mental workload levels during an everyday life office-work scenario. *Personal and ubiquitous computing* 17 (2013), 229–239.

[28] Heather Crawford. 2010. Keystroke dynamics: Characteristics and opportunities. In *2010 Eighth International Conference on Privacy, Security and Trust*. 205–212. https://doi.org/10.1109/PST.2010.5593258

[29] Avisha Das, Shahryar Baki, Ayman El Aassal, Rakesh Verma, and Arthur Dunbar. 2020. SoK: A Comprehensive Reexamination of Phishing Research From the Security Perspective. *IEEE Communications Surveys & Tutorials* 22, 1 (2020), 671–708. https://doi.org/10.1109/COMST.2019.2957750

[30] Alexander De Luca, Alina Hang, Frederik Brudy, Christian Lindner, and Heinrich Hussmann. 2012. Touch Me Once and i Know It's You! Implicit Authentication Based on Touch Screen Patterns. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '12)*. ACM, New York, NY, USA, 987–996. https://doi.org/10.1145/2207676.2208544

[31] Alexander De Luca, Roman Weiss, and Heiko Drewes. 2007. Evaluation of Eye-Gaze Interaction Methods for Security Enhanced PIN-Entry. In *Proceedings of the 19th Australasian Conference on Computer-Human Interaction: Entertaining User Interfaces (OZCHI '07)*. ACM, New York, NY, USA, 199–202. https://doi.org/10.1145/1324892.1324932

[32] Verena Distler. 2023. The Influence of Context on Response to Spear-Phishing Attacks: An In-Situ Deception Study. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems (CHI '23)*. ACM, New York, NY, USA, Article 619, 18 pages. https://doi.org/10.1145/3544548.3581170

[33] Verena Distler, Matthias Fassl, Hana Habib, Katharina Krombholz, Gabriele Lenzini, Carine Lallemand, Lorrie Faith Cranor, and Vincent Koenig. 2021. A Systematic Literature Review of Empirical Methods and Risk Representation in Usable Privacy and Security Research. *ACM Trans. Comput.-Hum. Interact.* 28, 6, Article 43 (dec 2021), 50 pages. https://doi.org/10.1145/3469845

[34] Reyhan Düzgün, Naheem Noah, Peter Mayer, Sanchari Das, and Melanie Volkamer. 2022. SoK: A Systematic Literature Review of Knowledge-Based Authentication on Augmented Reality Head-Mounted Displays. In *Proceedings of the 17th International Conference on Availability, Reliability and Security (ARES '22)*. ACM, New York, NY, USA, Article 36, 12 pages. https://doi.org/10.1145/3538969.3539011

[35] Malin Eiband, Mohamed Khamis, Emanuel von Zezschwitz, Heinrich Hussmann, and Florian Alt. 2017. Understanding Shoulder Surfing in the Wild: Stories from Users and Observers. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (CHI '17)*. ACM, New York, NY, USA, 4254–4265. https://doi.org/10.1145/3025453.3025636

[36] Anjuli Franz, Verena Zimmermann, Gregor Albrecht, Katrin Hartwig, Christian Reuter, Alexander Benlian, and Joachim Vogt. 2021. SoK: Still Plenty of Phish in the Sea — A Taxonomy of User-Oriented Phishing Interventions and

Avenues for Future Research. In *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*. USENIX Association, 339–358. https://www.usenix.org/conference/soups2021/presentation/franz

[37] Hugo Gamboa and Ana Fred. 2004. A behavioral biometric system based on human-computer interaction. In *Biometric Technology for Human Identification*, Anil K. Jain and Nalini K. Ratha (Eds.), Vol. 5404. International Society for Optics and Photonics, SPIE, 381 – 392. https://doi.org/10.1117/12.542625

[38] Christopher Hadnagy. 2010. *Social engineering: The art of human hacking*. John Wiley & Sons.

[39] Yassir Hashem, Hassan Takabi, Mohammad GhasemiGol, and Ram Dantu. 2015. Towards insider threat detection using psychophysiological signals. In *Proceedings of the 7th ACM CCS International Workshop on Managing Insider Security Threats*. 71–74.

[40] Mariam Hassib, Michael Braun, Bastian Pfleging, and Florian Alt. 2019. Detecting and influencing driver emotions using psycho-physiological sensors and ambient light. In *Human-Computer Interaction–INTERACT 2019: 17th IFIP TC 13 International Conference, September 2–6, 2019, Proceedings, Part I 17*. Springer, 721–742.

[41] Mariam Hassib, Mohamed Khamis, Susanne Friedl, Stefan Schneegass, and Florian Alt. 2017. Brainatwork: Logging Cognitive Engagement and Tasks in the Workplace Using Electroencephalography. In *Proceedings of the 16th International Conference on Mobile and Ubiquitous Multimedia (MUM '17)*. ACM, New York, NY, USA, 305–310. https://doi.org/10.1145/3152832.3152865

[42] Mariam Hassib, Stefan Schneegass, Philipp Eiglsperger, Niels Henze, Albrecht Schmidt, and Florian Alt. 2017. EngageMeter: A System for Implicit Audience Engagement Sensing Using Electroencephalography. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (CHI '17)*. ACM, New York, NY, USA, 5114–5119. https://doi.org/10.1145/3025453.3025669

[43] Heinke Hihn, Sascha Meudt, and Friedhelm Schwenker. 2016. Inferring mental overload based on postural behavior and gestures. In *Proceedings of the 2nd workshop on emotion representations and modelling for companion systems*. 1–4.

[44] M Sazzad Hussain, Rafael A Calvo, and Fang Chen. 2014. Automatic cognitive load detection from face, physiology, task performance and fusion during affective interference. *Interacting with computers* 26, 3 (2014), 256–268.

[45] Stephen Hutt, Angela E.B. Stewart, Julie Gregg, Stephen Mattingly, and Sidney K. D'Mello. 2022. Feasibility of Longitudinal Eye-Gaze Tracking in the Workplace. *Proc. ACM Hum.-Comput. Interact.* 6, ETRA, Article 148 (may 2022), 21 pages. https://doi.org/10.1145/3530889

[46] Christina Katsini, Yasmeen Abdrabou, George E. Raptidis, Mohamed Khamis, and Florian Alt. 2020. The Role of Eye Gaze in Security and Privacy Applications:Survey and Future HCI Research Directions. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (CHI '20)*. ACM, New York, NY, USA. https://doi.org/10.1145/3313831.3376840

[47] Christina Katsini, Christos Fidas, George E. Raptis, Marios Belk, George Samaras, and Nikolaos Avouris. 2018. Eye Gaze-Driven Prediction of Cognitive Differences during Graphical Password Composition. In *23rd International Conference on Intelligent User Interfaces (IUI '18)*. ACM, New York, NY, USA, 147–152. https://doi.org/10.1145/3172944.3172996

[48] Ruhul Amin Khalil, Edward Jones, Mohammad Inayatullah Babar, Tariqullah Jan, Mohammad Haseeb Zafar, and Thamer Alhussain. 2019. Speech emotion recognition using deep learning techniques: A review. *IEEE Access* 7 (2019), 117327–117345.

[49] Mohamed Khamis, Mariam Hassib, Emanuel von Zezschwitz, Andreas Bulling, and Florian Alt. 2017. GazeTouchPIN: Protecting Sensitive Data on Mobile Devices Using Secure Multimodal Authentication. In *Proceedings of the 19th ACM International Conference on Multimodal Interaction (ICMI '17)*. ACM, New York, NY, USA, 446–450. https://doi.org/10.1145/3136755.3136809

[50] Hassan Khan, Urs Hengartner, and Daniel Vogel. 2016. Targeted Mimicry Attacks on Touch Input Based Implicit Authentication Schemes. In *Proceedings of the 14th Annual International Conference on Mobile Systems, Applications, and Services (MobiSys '16)*. ACM, New York, NY, USA, 387–398. https://doi.org/10.1145/2906388.2906404

[51] M Asif Khawaja, Natalie Ruiz, and Fang Chen. 2007. Potential speech features for cognitive load measurement. In *Proceedings of the 19th Australasian conference on computer-human interaction: Entertaining user interfaces*. 57–60.

[52] R Benjamin Knapp, Jonghwa Kim, and Elisabeth André. 2010. Physiological signals and their use in augmenting emotion recognition for human–machine interaction. In *Emotion-oriented systems: The Humaine handbook*. Springer, 133–159.

[53] Thomas Kosch, Mariam Hassib, Daniel Buschek, and Albrecht Schmidt. 2018. Look into My Eyes: Using Pupil Dilation to Estimate Mental Workload for Task Complexity Adaptation. In *Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems (CHI EA '18)*. ACM, New York, NY, USA, 1–6. https://doi.org/10.1145/3170427.3188643

[54] Thomas Kosch, Mariam Hassib, Paweł W Woźniak, Daniel Buschek, and Florian Alt. 2018. Your eyes tell: Leveraging smooth pursuit for assessing cognitive workload. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. 1–13.

[55] Thomas Kosch, Jakob Karolus, Johannes Zagermann, Harald Reiterer, Albrecht Schmidt, and Paweł W. Woźniak. 2023. A Survey on Measuring Cognitive Workload in Human-Computer Interaction. *ACM Comput. Surv.* 55, 13s, Article 283 (jul 2023), 39 pages. https://doi.org/10.1145/3582272

[56] Kat Krol, Matthew Moroz, and M. Angela Sasse. 2012. Don't work. Can't work? Why it's time to rethink security warnings. In *2012 7th International Conference on Risks and Security of Internet and Systems (CRiSIS)*. 1–8. https://doi.org/10.1109/CRISIS.2012.6378951

[57] Manu Kumar, Tal Garfinkel, Dan Boneh, and Terry Winograd. 2007. Reducing Shoulder-Surfing by Using Gaze-Based Password Entry. In *Proceedings of the 3rd Symposium on Usable Privacy and Security (SOUPS '07)*. ACM, New York, NY, USA, 13–19. https://doi.org/10.1145/1280680.1280683

[58] Daniel LeBlanc, Alain Forget, and Robert Biddle. 2010. Guessing click-based graphical passwords by eye tracking. In *2010 Eighth International Conference on Privacy, Security and Trust*. 197–204. https://doi.org/10.1109/PST.2010.5593249

[59] Chunyong Li, Jiguo Xue, Cheng Quan, Jingwei Yue, and Chenggang Zhang. 2018. Biometric recognition via texture features of eye movement trajectories in a visual searching task. *PLOS ONE* 13, 4 (04 2018), 1–24. https://doi.org/10.1371/journal.pone.0194475

[60] Jonathan Liebers and Stefan Schneegass. 2020. Gaze-Based Authentication in Virtual Reality. In *ACM Symposium on Eye Tracking Research & Applications (ETRA '20 Adjunct)*. ACM, New York, NY, USA. https://doi.org/10.1145/3379157.3391421

[61] Andrey V. Lyamin and Elena N. Cherepovskaya. 2015. Biometric student identification using low-frequency eye tracker. 191–195. https://doi.org/10.1109/ICAICT.2015.7338544

[62] Aicha Maalej and Ilhem Kallel. 2020. Does keystroke dynamics tell us about emotions? A systematic literature review and dataset construction. In *2020 16th International Conference on Intelligent Environments (IE)*. IEEE, 60–67.

[63] Mihajlov Martin, Trpkova Marija, and Arsenovski Sime. 2013. Eye tracking recognition-based graphical authentication. In *2013 7th International Conference on Application of Information and Communication Technologies*. 1–5. https://doi.org/10.1109/ICAICT.2013.6722632

[64] John McAlaney and Peter J. Hills. 2020. Understanding Phishing Email Processing and Perceived Trustworthiness Through Eye Tracking. *Frontiers in Psychology* 11 (2020). https://doi.org/10.3389/fpsyg.2020.01756

[65] Lukas Mecke, Daniel Buschek, Mathias Kiermeier, Sarah Prange, and Florian Alt. 2019. Exploring Intentional Behaviour Modifications for Password Typing on Mobile Touchscreen Devices. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS'19)*. USENIX, Santa Clara, CA, 303–317. https://doi.org/10.5555/3361476.3361499

[66] Lukas Mecke, Sarah Delgado Rodriguez, Daniel Buschek, Sarah Prange, and Florian Alt. 2019. Communicating Device Confidence Level and Upcoming Re-Authentications in Continuous Authentication Systems on Mobile Devices. In *Proceedings of the Fifteenth Symposium on Usable Privacy and Security (SOUPS'19)*. USENIX, Santa Clara, CA, 289–301. https://doi.org/10.5555/3361476.3361498

[67] Daisuke Miyamoto, Takuji Iimura, Gregory Blanc, Hajime Tazaki, and Youki Kadobayashi. 2014. EyeBit: Eye-Tracking Approach for Enforcing Phishing Prevention Habits. In *2014 Third International Workshop on Building Analysis Datasets and Gathering Experience Returns for Security (BADGERS)*. 56–65. https://doi.org/10.1109/BADGERS.2014.14

[68] Daisuke Miyamoto, Takuji Iimura, Gregory Blanc, Hajime Tazaki, and Youki Kadobayashi. 2014. EyeBit: Eye-Tracking Approach for Enforcing Phishing Prevention Habits. In *2014 Third International Workshop on Building Analysis Datasets and Gathering Experience Returns for Security (BADGERS)*. 56–65. https://doi.org/10.1109/BADGERS.2014.14

[69] Rosana Montañez, Edward Golob, and Shouhuai Xu. 2020. Human Cognition Through the Lens of Social Engineering Cyberattacks. *Frontiers in Psychology* 11 (2020). https://doi.org/10.3389/fpsyg.2020.01755

[70] Ajaya Neupane, Md Lutfor Rahman, Nitesh Saxena, and Leanne Hirshfield. 2015. A multi-modal neuro-physiological study of phishing detection and malware warnings. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*. 479–491.

[71] Mark Nixon. 2008. Gait biometrics. *Biometric Technology Today* 16, 7 (2008), 8–9. https://doi.org/10.1016/S0969-4765(08)70103-6

[72] Kevin Pfeffel, Philipp Ulsamer, and Nicholas H. Müller. 2019. Where the User Does Look When Reading Phishing Mails – An Eye-Tracking Study. In *Learning and Collaboration Technologies. Designing Learning Experiences*, Panayiotis Zaphiris and Andri Ioannou (Eds.). Springer International Publishing, Cham, 277–287.

[73] Ken Pfeuffer, Matthias Geiger, Sarah Prange, Lukas Mecke, Daniel Buschek, and Florian Alt. 2019. Behavioural Biometrics in VR - Identifying People from Body Motion and Relations in Virtual Reality. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (CHI '19)*. ACM, New York, NY, USA, 11 pages. https://doi.org/10.1145/3290605.3300340

[74] Sarah Prange, Sven Mayer, Maria-Lena Bittl, Mariam Hassib, and Florian Alt. 2021. Investigating User Perceptions Towards Wearable Mobile Electromyography. In *Proceedings of the 18th IFIP TC 13 International Conference on Human-Computer Interaction (INTERACT '21)*. Springer, Berlin-Heidelberg, Germany. https://doi.org/10.1007/978-3-030-85610-6_20

[75] George E. Raptis, Christina Katsini, Marios Belk, Christos Fidas, George Samaras, and Nikolaos Avouris. 2017. Using Eye Gaze Data and Visual Activities to Infer Human Cognitive Styles: Method and Feasibility Studies. In *Proceedings of the 25th Conference on User Modeling, Adaptation and Personalization (UMAP '17)*. ACM, New York, NY, USA, 164–173. https://doi.org/10.1145/3079628.3079690

[76] Nataasha Raul, Radha Shankarmani, and Padmaja Joshi. 2020. A comprehensive review of keystroke dynamics-based authentication mechanism. In *International Conference on Innovative Computing and Communications: Proceedings of ICICC 2019, Volume 2*. Springer, 149–162.

[77] Kenneth Revett. 2008. *Behavioral biometrics: a remote access approach*. Wiley.

[78] Emils Rozentals. 2021. *Email load and stress impact on susceptibility to phishing and scam emails*. Student Thesis, Lulea, Sweden.

[79] Alia Saad, Michael Chukwu, and Stefan Schneegass. 2018. Communicating Shoulder Surfing Attacks to Users. In *Proceedings of the 17th International Conference on Mobile and Ubiquitous Multimedia (MUM '18)*. ACM, New York, NY, USA, 147–152. https://doi.org/10.1145/3282894.3282919

[80] Lipsarani Sahoo, Nazmus Sakib Miazi, Mohamed Shehab, Florian Alt, and Yomna Abdelrahman. 2022. You Know Too Much: Investigating Users' Perceptions and Privacy Concerns Towards Thermal Imaging. In *Proceedings of the 2022 Privacy Symposium (Privacy'22)*. http://www.florian-alt.org/unibw/wp-content/publications/sahoo2022privacy.pdf

[81] Florian Schaule, Jan Ole Johanssen, Bernd Bruegge, and Vivian Loftness. 2018. Employing Consumer Wearables to Detect Office Workers' Cognitive Load for Interruption Management. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 2, 1, Article 32 (mar 2018), 20 pages. https://doi.org/10.1145/3191764

[82] Stefan Schneegass, Bastian Pfleging, Nora Broy, Frederik Heinrich, and Albrecht Schmidt. 2013. A data set of real world driving to assess driver workload. In *Proceedings of the 5th international conference on automotive user interfaces and interactive vehicular applications*. ACM, New York, NY, USA, 150–157. https://doi.org/10.1145/2516540.2516561

[83] Jessica Schwarz, Sven Fuchs, and Frank Flemisch. 2014. Towards a more holistic view on user state assessment in adaptive human-computer interaction. In *2014 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*. 1228–1234. https://doi.org/10.1109/SMC.2014.6974082

[84] Sophie Stephenson, Bijeeta Pal, Stephen Fan, Earlence Fernandes, Yuhang Zhao, and Rahul Chatterjee. 2022. SoK: Authentication in Augmented and Virtual Reality. In *2022 IEEE Symposium on Security and Privacy (SP)*. 267–284. https://doi.org/10.1109/SP46214.2022.9833742

[85] Viktor Taneski, Marjan Heričko, and Boštjan Brumen. 2019. Systematic overview of password security problems. *Acta Polytechnica Hungarica* 16, 3 (2019), 143–165.

[86] Viktor Taneski, Marjan Heričko, and Boštjan Brumen. 2014. Password security — No change in 35 years?. In *2014 37th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*. 1360–1365. https://doi.org/10.1109/MIPRO.2014.6859779

[87] Pin Shen Teh, Andrew Beng Jin Teoh, and Shigang Yue. 2013. A survey of keystroke dynamics biometrics. *The Scientific World Journal* 2013 (2013).

[88] Blase Ur, Fumiko Noma, Jonathan Bees, Sean M. Segreti, Richard Shay, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. 2015. "I Added '!' at the End to Make It Secure": Observing Password Creation in the Lab. In *Proceedings of the Eleventh USENIX Conference on Usable Privacy and Security (SOUPS '15)*. USENIX Association, USA, 123–140.

[89] Chang Zhi Wei. 2013. Stress emotion recognition based on RSP and EMG signals. In *Advanced Materials Research*, Vol. 709. Trans Tech Publ, 827–831.

[90] Alma Whitten and J. D. Tygar. 1999. Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. In *Proceedings of the 8th Conference on USENIX Security Symposium - Volume 8 (SSYM'99)*. USENIX Association, USA, 14.

[91] Emma J. Williams, Joanne Hinds, and Adam N. Joinson. [n. d.]. Exploring susceptibility to phishing in the workplace. *International Journal of Human-Computer Studies* 120 ([n. d.]), 1–13. https://doi.org/10.1016/j.ijhcs.2018.06.004

[92] Takehiro Yamakoshi, Ken-ichi Yamakoshi, Shinobu Tanaka, Masamichi Nogawa, Mariko Shibata, Y Sawada, P Rolfe, and Yukio Hirose. 2007. A preliminary study on driver's stress index using a new method based on differential skin temperature measurement. In *2007 29th Annual International Conference of the IEEE Engineering in Medicine and Biology Society*. IEEE, 722–725.

[93] Kun Yu, Ronnie Taib, Marcus A Butavicius, Kathryn Parsons, and Fang Chen. 2019. Mouse behavior as an index of phishing awareness. In *Human-Computer Interaction–INTERACT 2019: 17th IFIP TC 13 International Conference, Paphos, Cyprus, September 2–6, 2019, Proceedings, Part I 17*. Springer, 539–548.

[94] Beste F Yuksel, Kurt B Oleson, Lane Harrison, Evan M Peck, Daniel Afergan, Remco Chang, and Robert JK Jacob. 2016. Learn piano with BACh: An adaptive learning interface that adjusts task difficulty based on brain state. In *Proceedings of the 2016 CHI conference on human factors in computing systems*. 5372–5384.

[95] Sijie Zhuo, Robert Biddle, Yun Sing Koh, Danielle Lottridge, and Giovanni Russello. 2023. SoK: Human-Centered Phishing Susceptibility. *ACM Trans. Priv. Secur.* 26, 3, Article 24 (apr 2023), 27 pages. https://doi.org/10.1145/3575797

[96] Mary Ellen Zurko and Richard T. Simon. 1996. User-Centered Security. In *Proceedings of the 1996 Workshop on New Security Paradigms (NSPW '96)*. ACM, New York, NY, USA, 27–33. https://doi.org/10.1145/304851.304859

Received 18 May 2023; revised 29 August 2023; accepted 1 October 2023