Padlock, the Universal Security Symbol? – Exploring Symbols and Metaphors for Privacy and Security

Sarah Delgado Rodriguez
University of the Bundeswehr Munich
Munich, Germany
sarah.delgado@unibw.de

Anh Dao Phuong
LMU Munich
Munich, Germany
anh.dao@campus.lmu.de

Franziska Bumiller
University of the Bundeswehr Munich, LMU Munich
Munich, Germany
franziska.bumiller@unibw.de

Lukas Mecke
University of the Bundeswehr Munich, LMU Munich
Munich, Germany
lukas.mecke@unibw.de

Felix Dietz
University of the Bundeswehr Munich
Munich, Germany
felix.dietz@unibw.de

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

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

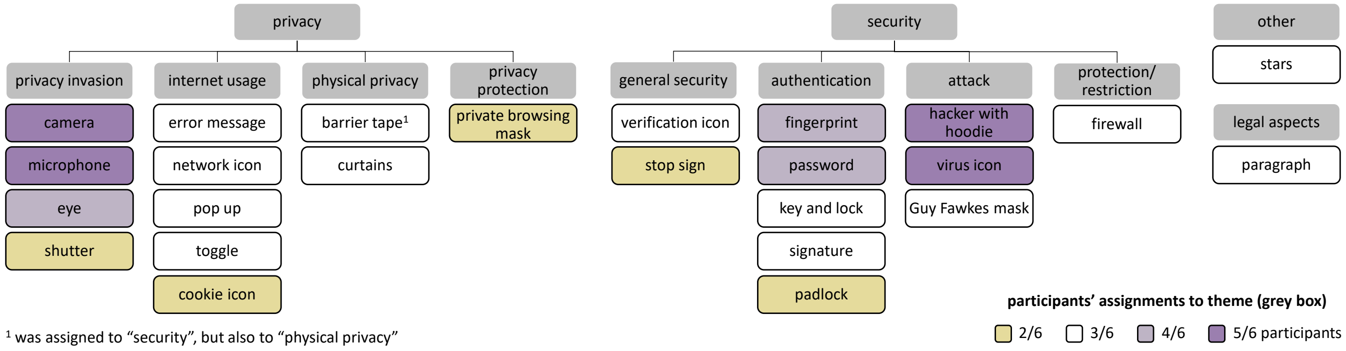


Figure 1: We conducted three studies ($n_{total} = 22$) and derived a symbol and metaphor space for privacy- and security-related topics. We first collected 32 symbols/metaphors and 5 colors which HCI-adepts associated with security and privacy in two brainstorming sessions ($n = 8$, each). Those were clustered into the themes visualized here (grey boxes) in a third study ($n = 6$).

ABSTRACT

The use of symbols and metaphors can be a fast and effective way of conveying abstract concepts. At the same time, misconceived symbols can lead to misunderstandings and errors. Therefore, when it comes to privacy and security, clear communication is essential to avoid putting users' personal data at risk. In this paper, we elicit 32 symbols and metaphors associated with privacy and security through two brainstorming sessions ($n = 8$, each). Six experts further separated this collection into security and privacy-related symbols and generated clusters based on similarity. Using participants' clusters, we derived underlying themes. As a result, we present a symbol and metaphor space for privacy and security and discuss their perceived meaning. Our findings can serve researchers, designers, and developers to find suitable symbols or metaphors for a given scenario (e.g., to decide on the interaction metaphor for a tangible security mechanism) and to understand if a symbol is ambiguous or how it may be understood (e.g., is an eye associated with privacy configurations?). Our work provides an initial knowledge base supporting effective communication in this field.

MUM '23, December 03–06, 2023, Vienna, Austria

ACM ISBN 979-8-4007-0921-0/23/12…$15.00
https://doi.org/10.1145/3626705.3627770

CCS CONCEPTS

• **Security and privacy → Usability in security and privacy**.

KEYWORDS

symbols, metaphors, privacy, security

ACM Reference Format:
Sarah Delgado Rodriguez, Anh Dao Phuong, Franziska Bumiller, Lukas Mecke, Felix Dietz, Florian Alt, and Mariam Hassib. 2023. Padlock, the Universal Security Symbol? – Exploring Symbols and Metaphors for Privacy and Security. In *International Conference on Mobile and Ubiquitous Multimedia (MUM '23), December 03–06, 2023, Vienna, Austria.* ACM, New York, NY, USA, 15 pages. https://doi.org/10.1145/3626705.3627770

1 INTRODUCTION

While real-world safety mechanisms such as helmets or handrails protect users from physical harm, cyber security and privacy mechanisms protect users from digital threats like ransomware or identity theft as well as from being observed without their knowledge. Such mechanisms are often designed to protect users transparently in the background and, due to being purely digital, can be hard to grasp and easy to misunderstand [5, 6, 15, 30]. Hence, it is essential for researchers and developers of such systems to communicate their functionality and state in an intuitive and unambiguous way.

Symbols and metaphors are powerful means to simplify and convey privacy- and security-related information [15]. Currently, commercial products use a lot of different symbols for security-related topics. For example, a lock icon (i.e., pictographic symbol [14]) might appear in a web browser's address bar, indicating that the visited website is secured using HTTPS [5, 25]. A pop-up icon with a red cross icon in the address bar might indicate that a pop-up has been blocked[1]. Similarly, related work has explored the usage and design of icons for further security-related applications such as encryption [5], warnings [29], privacy choices [15] or the description of attack scenarios [17]. Moreover, metaphors have been used to educate on cyber security [11] or to reduce complexity, e.g., when configuring firewalls [27]. However, users' understanding of symbols and metaphors may be influenced by pre-existing conceptions [4]. For example, people could assume that the ⏏ icon represents "eject", even though a developer might want to represent a house, leading to misunderstandings and confusion. This poses a major challenge to researchers and developers of novel privacy and security mechanisms who wish to use such symbolic representations. This challenge might prove even more difficult since there is still a lack of research on possible conflicting pre-existing associations of specific symbols to privacy vs. security and to different subtopics, resulting in more ambiguity. To support future researchers, designers, and developers on this front, our work captures known symbols for both security and privacy and their possible application areas. For this purpose, we conducted three exploratory studies ($n_{total} = 22$) – two brainstorming sessions and a third clustering study. We recruited HCI-adept participants for all three studies because the topics of privacy and security have shown to be abstract and hard to grasp for laypeople [13, 30]. We collected 32 unique symbols and metaphors, as well as 5 colors that 16 HCI-adept participants associated with privacy and security from the brainstorming sessions. Based on the majority votes of six recruited usable security researchers, we assigned 15 of these symbols to either security or privacy (i.e., $n > 3$ experts assigned them to this topic). Moreover, the experts freely created symbol clusters related to 17 underlying themes. Based on these findings, we derived an initial symbol and metaphor space for privacy- and security-related topics. We describe three example application scenarios for our symbol and metaphor space which demonstrate how it can support future researchers, designers, and developers. We envision our findings to be an initial fundament for future replications targeting varying user groups and diverse cultural backgrounds.

Contribution Statement. In this paper, we make a number of contributions that combine knowledge from two brainstorming sessions, and a subsequently conducted clustering study:

- We elicited 32 unique symbols for privacy and security from 16 HCI-adept participants in total. We then conducted an expert clustering study, to investigate the possible distinctions between privacy- and security-related symbols and metaphors as well as subgroups inside each of these topics.
- Based on the results of the studies, we derive an initial symbol and metaphor space for privacy- and security-related topics. We also discuss how our findings can be used by future designers, developers, and researchers.

2 BACKGROUND AND RELATED WORK

We present prior work on (1) symbols, icons, and metaphors in HCI, (2) symbols and metaphors for privacy and security, and (3) the challenges of designing such symbols. Finally, we explain the addressed research gap and used terminology.

2.1 Symbols, Icons, and Metaphors in HCI

Semiotics is a specialized subfield of HCI, which addresses symbols and icons. In his work from 1986, Gittens [14] defines icons as *"pictographic symbols which are used as part of the dialogue in order to represent processes and data in the computer"* (p. 523). His work covers different topics connected to icons like their design, characteristics or placement, and the use of metaphors laying the groundwork for the research to follow [14]. Islam [20], provides a broad overview of research in semiotics in his literature review. He presents symbols and icons as a subcategory of signs, which are defined as anything that can be interpreted by a human being [20]. More recently, Bühler et al. [4] focused on developing design guidelines for icons that are valid across cultures and thereby addressed a challenge that was pointed out in prior work [20]. The authors use human perception as a basis to develop design guidelines that are detached from cultural experiences. Even though symbols and metaphors are frequently used in combination, a separate field of research has formed for metaphors. In his work, Blackwell [3] examined the historical development of metaphors as well as common theories. He also discussed the widespread and well-known desktop metaphor and the usage of metaphors in HCI [3]. More recently, Reed et al. [28] investigated, how people can use metaphors to communicate content to each other.

In contrast to some of the aforementioned works [4], we primarily consider the content as well as the thematic assignment of

[1] https://support.google.com/chrome/answer/95472, last accessed June 2, 2023

symbols and metaphors rather than their exact design, representation, or wording. Moreover, we are particularly interested in the topics of security and privacy.

2.2 Symbols and Metaphors for Privacy and Security

Although symbols are a common way to communicate concepts easily across language and culture barriers, researchers have found that privacy concepts in particular prove challenging to convey through symbols [7, 15]. Researchers have explored a variety of symbols and metaphors to convey complex privacy concepts, in generic contexts [16, 26] as well as specific to particular domains such as the privacy of web links [22], social media [18], or webcams [7]. Prior work looked into variations between metaphors used in the physical world to convey privacy (e.g. doors and curtains) and in the digital worlds (e.g. illustration of a lock and key) and explored non-experts' view of these [26]. Efroni et al. [6] present an approach to visualize data processing using privacy icons to represent different levels of risks. Habib et al. [15] investigated ways to convey privacy choices to consumers on websites using different icons and link texts (e.g., a toggle which is a standard UI element for turning on or off settings, checkboxes, and a file folder representing personal data). They suggested simplifying the design of privacy icons and adding text to improve comprehension [15]. Further research explored the presentation of privacy notices, or privacy dashboards, which summarize and present information in a simplified manner that was otherwise available in long and jargon-filled privacy policies [15, 23]. Kelley et al. [23] proposed the privacy *nutrition label*, a concept that aims to provide users with concise and understandable information about data practices and empower them to make informed decisions about sharing their personal data. Overall, prior work primarily explored privacy icons focused on communicating current data practices [15, 31].

Moreover, prior research has explored visual representations of security aiming for improved user understanding and adoption of better security practices. Raja et al. [27] propose a physical security metaphor to improve the effectiveness of firewall warnings. They suggest that using metaphors – compared to usual text warnings – can enhance users' comprehension and decision-making when it comes to online security. Distler et al. [5] explored effective ways of representing encryption to non-experts using text and visuals. They mentioned security indicators in the context of secure emails such as closed envelopes, and torn envelopes, and used a padlock in front of ciphertext as a visual representation of encryption in their experiment. Besides symbols and words, Jeong et al. [21] emphasize the importance of colors in cybersecurity warnings which can enhance users' comprehension and their response to potential (online) risks. For example, different colors of warning imply varying levels of risk. However, the interpretation of different colors has also shown to be sometimes confusing for users, as their meaning might vary between different systems [1, 9, 27].

2.3 Challenges in Designing Symbols for Privacy and Security

While using symbols and metaphors offers promising opportunities for communicating privacy and security concepts, several challenges in research have been identified. The design of symbols should be based on users' knowledge and needs, employing well-known concepts, and closely mimicking real-world objects to increase memorability and recognition [6, 15]. Furthermore, standardization and consistency play a crucial role in symbol design for privacy and security communication [5, 15, 23]. Kelley et al. [23] emphasize the need for a standardized framework that provides concise and understandable information about data practices. Distler et al. [5] highlight the importance of consistent and accurate explanations. Related work has also established that implementing standardized indicators for privacy *choices* [15], as well as categorizing symbols based on context [26], would increase understanding.

2.4 Research Gap and Terminology

In summary, prior research investigated the use of symbols and metaphors for either privacy (e.g., communicating choices or visualizing risk), or for security (e.g., explaining encryption). In our work, we look at the distinction between privacy and security, aiming to create a clear understanding of these two topics and their symbolic representations. Throughout the paper, our use of the words *symbol* and *metaphor* is based on the definition from the Cambridge Dictionary[2]: *a symbol is "a sign, shape, or object that is used to represent something else"*. Moreover, we use *metaphor*, as *"an expression that occurs frequently in literature and describes a person or object by referring to something thought to have properties similar to that person or object"*. Hence, in line with Gittens [14], a symbol describes a more concrete subject, while a metaphor can refer to a whole situation or environment.

3 RESEARCH APPROACH

3.1 Research Questions

To address the previously discussed research gaps, we answer the following two research questions:

RQ1: *Which symbols and metaphors do HCI-adepts associate with privacy and security?*

RQ2: *How can such symbols and metaphors be distinguished between security- and privacy-related? Into which further groups can they be divided and to which themes can they be assigned?*

3.2 Methodology Overview

To answer our research questions, we conducted three studies (see Figure 2) with participants having expertise in HCI and interest in research on privacy or security (aka *HCI-adepts*, like researchers, students, and conference participants). Having such HCI-adept participants allowed us to rely on their pre-existing understanding of security and privacy, rather than on potentially biasing abstract definitions or specific example use cases. Drawing from experts' or adepts' feedback is a frequently applied strategy for exploratory research on usable security and privacy (e.g., [12] or [8]).

Collection of Symbols and Metaphors. To address RQ1, we first collected symbols for privacy and security in *two rapid ideation brainstorming sessions* ($n = 16$). We asked both groups of participants to speak out all symbols or metaphors they associate with

[2] https://dictionary.cambridge.org/dictionary/english/symbol and https://dictionary.cambridge.org/dictionary/english/metaphor, last accessed June 2, 2023

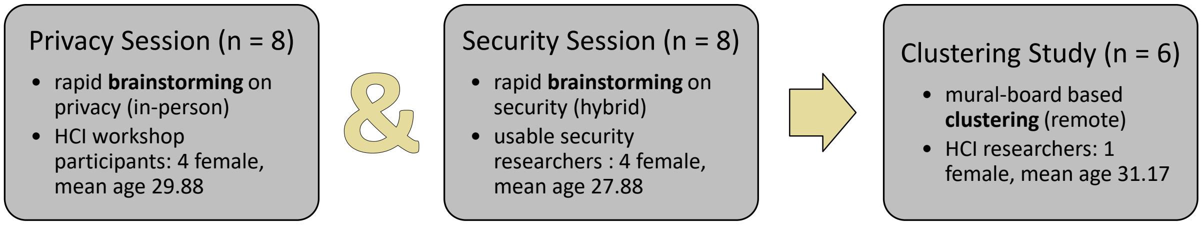

Privacy Session (n = 8)
rapid **brainstorming** on privacy (in-person)
HCI workshop participants: 4 female, mean age 29.88
&
Security Session (n = 8)
rapid **brainstorming** on security (hybrid)
usable security researchers : 4 female, mean age 27.88
Clustering Study (n = 6)
mural-board based **clustering** (remote)
HCI researchers: 1 female, mean age 31.17

Figure 2: We conducted two rapid brainstorming sessions, first on privacy and then on security. Participants of these sessions ($n = 16$) were asked to speak out all symbols and metaphors they associated with the corresponding topic. In the third study ($n = 6$), we asked participants to cluster the symbols resulting from the brainstorming sessions.

privacy or security respectively. One experimenter wrote all the mentioned ideas down for participants to see (i.e., on a poster or a projected Mural board). Both brainstorming sessions had different participants and lasted about 10 minutes each. The *privacy session* ($n = 8$) was conducted in person during a workshop at a German HCI conference. We conducted the *security session* ($n = 8$) using a hybrid setup with both in-person and online attendees.

Clustering. To expand upon the results of the brainstorming sessions and answer RQ2, we conducted a remote study ($n = 6$) with HCI researchers who predominantly work in the field of usable security. We asked these experts to review the list of symbols generated during the brainstorming session and to group them (a) based on whether they believe them to be representative of security or privacy and (b) freely into meaningful clusters. Each participant was provided with a link to a Mural board, which described the clustering tasks. Previous tests revealed an estimated completion time of roughly 15 minutes. Participants had one week to complete their own Mural board whenever they saw fit.

Ethical Considerations. Low-risk studies are exempt from approval by an IRB at our institution and residence country. However, we based our study design on instructions provided by our institutional ethics committee. Hence, participants were first provided with detailed information on which and how data would be collected, processed, and stored. We also informed them about the expected duration of each study, its purpose, and the compensation they could expect for their participation. Next, we asked them to formally consent to the participation and data collection.

Limitations. We acknowledge several limitations to our work. First, the security brainstorming session was done in a hybrid format and not in presence, where some participants were online and some were present. This might have deterred some of the online participants from speaking out their thoughts, even though the moderator of the hybrid session took special care to include remote participants, as much as possible. In the clustering study, we added icons to support comprehension of the textual labels of each symbol\metaphor whose specific design could have biased participants. We also did not provide definitions of the terms “privacy” and “security” to our participants, as we aimed to reflect their preexisting understanding as usable security and privacy researchers. Hence, we cannot be certain if their understanding of the terminology differs. Moreover, we recruited HCI-adepts applying direct recruitment, leading to small samples that were rather homogeneous in terms of culture (i.e., mostly inhabitants of Germany), which might affect the generalizability of our results to the general population. Recruiting HCI-adept participants also proved difficult, which is reflected in the sample sizes.

4 COLLECTION OF SYMBOLS & METAPHORS

We conducted two brainstorming sessions to collect symbols and metaphors associated with privacy and security respectively.

4.1 Procedure

In each session, we first distributed a consent form to participants and then asked them to fill out a brief questionnaire on their demographics. We then asked participants to speak out any symbols or metaphors they associated with privacy and security, respectively. In particular, we prepared a prompting slide that showed the question: *“Which symbols/metaphors do you associate with [privacy/security]?”* One experimenter directly wrote all mentioned ideas down for participants to see (on a poster in the privacy session and on a shared/projected Mural board in the security session).

4.2 Participants and Recruitment

For each brainstorming session, we recruited 8 participants. We conducted the sessions with different participants to avoid nudging participants to discuss specific distinctions between privacy and security. Our goal was to ensure that participants did not restrict their ideas based on such discussions. Participants of the *privacy session* were 25 − 35 years old ($mean = 29.88$, $std = 3.49$). Four participants identified as male and four as female. All participants were recruited during a workshop on tangible interactions at a German HCI conference. We did not prescreen participants for previous knowledge of privacy, however, workshop participants were asked to take part in our brainstorming session if they were interested in privacy research. For the *security session* we recruited 8 HCI-adepts (researchers and research assistants) through direct recruiting (i.e., writing e-mails or direct messages). Most participants of the security session were usable security researchers. They were 22 − 34 years old ($mean = 27.88$, $std = 4.19$). Four participants identified as male and four as female. We conducted this session in a hybrid manner with three online participants and five in-person participants. The hybrid setup allowed us to conduct the study without requiring extensive traveling. Online participants could participate in a raffle for a 10€ Amazon Voucher and in-person participants got a free lunch as compensation for their efforts. Please note that

Table 1: Symbols and metaphors associated with privacy, as mentioned by participants ($n = 8$) and their quotes.

symbol	quote
padlock	*“padlock, the universal security symbol.”*
eye	*“Maybe the contrary of observation, an eye.”*
camera	*“camera.”*
microphone	*“microphone.”*
fingerprint	*“fingerprint.”*
hacker with hoodie	*“typical hacker with a black hoodie.”*
shield	*“The shield. The protective shield.” – “Yes, that’s true. For anti-virus programs.”*
barrier tape	*“If you want people to form a queue, you use barrier tape.”; “black and yellow are also security.” – “[...]if you think about barrier tapes.”*
curtains	*“curtains” – “Yes, absolutely. So you can close them.”*
spotlight	*“A spotlight, when you illuminate the data.”*
shutter	*“the shutter of a camera.”*
signature	*“Maybe a signature. Since we also needed to sign before. [refers to consent form]”*
paragraph	*“paragraphs for privacy, especially for privacy policies.”*
password	*“passwords.”*
cookie icon	*“cookie icons.”; “’Accept all’ for cookie settings.”*
stop sign	*“stop sign.”*
toggle	*“True, also these small mini switches.” –“Toggles?” – “Yes, a toggle switch”*
pop-up	*“It reminded me of my anti-virus program. Each time I log into my pc a ’what is now active’ pops open.” – “You mean a warning message? A notification?” – “A notification, that your anti-virus is running.”*
VPN icon	*“I also associate VPN Icons with privacy.”*

this session was part of a larger focus group discussion on the topic “tangible security assistants”. Hence, the compensation refers to the complete focus group discussion (90 minutes).

4.3 Results

Both brainstorming sessions were audio recorded and subsequently transcribed. We first analyzed the data collected during each session independently. Two experimenters familiarized themselves with the data (i.e., transcripts and in-situ written-down symbols). One experimenter then created a spreadsheet, assigning all related statements from the transcripts to each written-down symbol or metaphor. Next, both experimenters agreed on descriptive labels for each symbol or metaphor based on participants’ quotes. In the final analysis step, the experimenters compared the results of both brainstorming sessions. We translated quotes from their original language where necessary.

4.3.1 Privacy Session.

Symbols and Metaphors. Table 1 lists all 19 symbols for privacy mentioned by our participants and how they described them. Overall, participants mentioned symbols representing privacy invasions but also protection:

> *“[..] there are two categories: Things that give me more ’privacy’ and the things that make ’privacy’ worse.”*
> *“[...] if you look at the terms that we’ve written down, [...] either they take away your ’privacy’ or they give you ’privacy’. They can both be metaphors. We have camera, microphone. On the other side, we have shield, which protects. Or a spotlight, as opposed to shield.”*

Table 2: Symbols and metaphors for security mentioned by participants ($n = 8$) during the second brainstorming session.

symbol	quote
key and lock	*“keys”; “the lock is more like a padlock [...] but you could also have like the keyhole in the door.”*
fingerprint	*“fingerprint.”*
padlock	*“padlock”*
ciphertext	*“For me, it’s also ciphertext. You know, that you have something that looks kind of encrypted.”*
firewall	*“The classic firewall.”*
hacker with hoodie	*“[...] I also associate, you know, a person with a black hat as the hacker with some kind of cyber security icon.”; “Yeah. Or some kind of attacker. You know, someone that has a hoodie, sitting in front of the computer [...]”*
private browsing mask	*“Also like the mask for Firefox when you go in private mode.”*
Guy Fawkes mask	*“Guy Fawkes masks I think they are called… Like the Anonymous masks”*
error message	*“Obscure and verbose error messages that you need to acknowledge every time.”; “I mean we have these red triangle shapes that are upside down.”*
verification icon	*“[...] this badges and whatever... trusted certificate, trusted shop. But also on Twitter you could have that “this account belongs to a real person”.”; “I think sometimes you also find badges for example, when your files are uploaded to a cloud [...] there’s also like a green check mark behind the file or whatever.”*
password	*“I think we have missed password up to this point.”*
stars	*“Also the [...] five star, yeah, could also be a symbol.”*
password strength indicators	*“[...] password strength indicators. [...] the colored ones [that] fill up, and tell you if it’s secure [...]”*
eye	*“If someone can see something you have an open eye [...] and if you want to hide something, you have an eye that’s crossed out.”; “ [...] So if something is maybe, you know, encrypted and safely stored away, [...] sometimes you also have the eye [indicating] that no one else can see it.”*
camera	*“There could be a surveillance camera.”*
safe	*“And I also thought about a safe [...]”*
guardian	*“And maybe also a guardian angel like somebody who is protecting you.”*
chain	*“[...] in Photoshop program you have these chains and if some layers are connected, there is like a connected chain and if not, it’s like a broken chain. So, you know, it’s like independent from the others. Something like this.”*
virus icon	*“What also comes to mind is a virus icon.”*
network icon	*“For me a network icon would also kind of indicate that there must be someone caring about the security of this network.”*

Colors. Moreover, participants discussed which colors they associate with privacy. They first mentioned *red and green*, where red represents *“danger or stop.”*, while green stands for the contrary:

> *“First I only thought of red, I thought ’stop, there is a barrier’, something like this. Interestingly, you could also see privacy from an ’I am protected perspective’, and then it would be green.”*

However, one participant mentioned: *“[...] green and red are more a warning for me and not security.”* Moreover, *blue*, which *“represents seriousness.”*, and *“black and yellow”* were also mentioned.

4.3.2 Security Session.

Symbols and Metaphors. Overall, participants of the security session mentioned 20 different symbols or metaphors. Table 2 lists all these symbols and the corresponding participant quotes.

Moreover, participants of the security session again briefly stated the difference between protecting and invading symbols:

> *"And I mean, does it have to be something that is secure? Because I also associate, you know, a person with a black hat as the hacker with some kind of cyber security icon."*

Colors. Similarly to the privacy session, participants of the security session also discussed the importance of different colors. Participants mostly mentioned again *red and green*:

> *"For me, it's, again, like a color thing. So some browsers, you know, when they have no HTTPS, they have, like, something red or some kind of alarm sign in red [...]. And when it's secure, it's kind of green."*

Another participant also mentioned *yellow*:

> *"[...] in some train stations, you have like a line where you're not supposed to stand and they have multiple like yellow lines. [...] you know, here it's probably less secure, so you have to behave differently."*

4.4 Final List of Symbols and Metaphors for Security and Privacy

Participants of both brainstorming sessions came up with a total of 32 unique symbols and metaphors. Common symbols and metaphors mentioned in both sessions were *padlock*, *eye*, *camera*, *fingerprint*, *password*, and a *hacker with a hoodie*. Another common metaphor was specific colors such as *red*, *green*, or *yellow*. Moreover, during both brainstorming sessions, we observed that participants did mix up the concepts of privacy and security where participants of the privacy session mentioned security and vice versa.

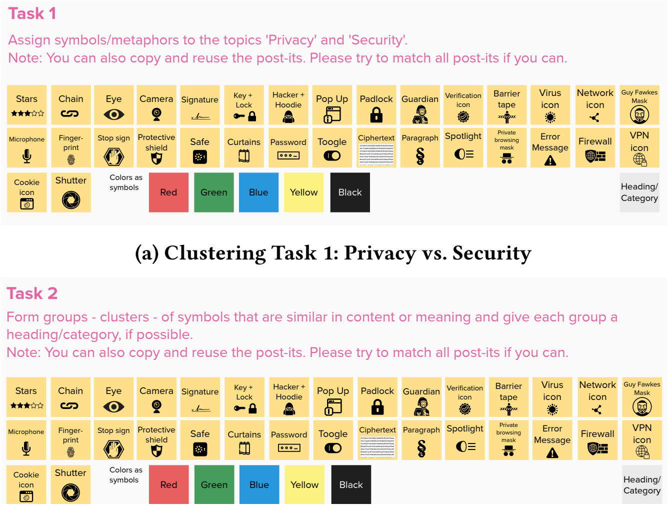
5 CLUSTERING OF SYMBOLS AND METAPHORS

After collecting symbols and metaphors for privacy and security, we conducted a third study to investigate possible clusters.

5.1 Procedure

The clustering study was conducted remotely. We recruited our six participants directly via email. Each participant was first asked to fill out an online consent form. Next, we asked them to follow the instructions provided on a Mural board[3]. We prepared one such Mural board for each participant of the clustering study. The boards included detailed task descriptions and further important instructions. Appendix A provides a screenshot of the Mural boards.

The board was divided into three parts. The first part introduced the purpose and context of the clustering study, followed by a brief demographic questionnaire. Each of the two other parts contained a set of sticky notes with the name and an icon of the symbol or metaphor (see Figure 3). As an aid to avoid participants misunderstanding the textual labels of the symbols and metaphors, we added one icon to each sticky note. We used the Mural board icon search feature to find fitting icons for all symbols\metaphors but for *ciphertext*, where we used an icon found on Google because it was not available in the Mural board search. Two experimenters discussed the selection of each icon to make sure that we used graphical representations illustrating the original quotes from participants of the brainstorming session as closely as possible. In the first clustering task, participants were asked to assign the sticky notes to either privacy or security. In the second task, they were requested to cluster the symbols and metaphors freely into groups and label these groups. Based on prior internal testing, we estimated the duration of the study to be 15 minutes. Participants could work on their boards on their own whenever they wanted. However, we asked them to finish the study in the course of one week. Participants could take part in a raffle of two 10€ Amazon vouchers.



Task 1

Assign symbols/metaphors to the topics 'Privacy' and 'Security'.
Note: You can also copy and reuse the post-its. Please try to match all post-its if you can.

(a) Clustering Task 1: Privacy vs. Security

Task 2

Form groups - clusters - of symbols that are similar in content or meaning and give each group a heading/category, if possible.
Note: You can also copy and reuse the post-its. Please try to match all post-its if you can.

(b) Clustering Task 2: Free Clustering

Figure 3: Using Mural boards, we asked the participants (n = 6) to first divide all symbols into security or privacy clusters and then group them freely. For this figure, we translated all texts from their original language.

5.2 Participants

We recruited six researchers (i.e., 4 Ph.D. students and 2 professors) as participants in the clustering study. Five participants identified as male and one as female. Moreover, our participants were 27-37 years old ($mean$ = 31.17, std = 3.92) and self-reported as experts in usable security and privacy ($median = 4 - agree$).

5.3 Data Analysis

To analyze the results, we first extracted all data from the online boards and organized the information in spreadsheets. We translated text entries from their original language to English where necessary. Next, we reviewed the assigned group for each symbol for both clustering tasks and identified recurring themes.

In the first clustering task, participants could assign each symbol to either "privacy" or "security", not assign it to any of those categories, or to both (see Figure 3a). This resulted in four possible assignments for each symbol. To analyze the agreement for each symbol, we analyzed how many participants assigned the most frequent category to each symbol. Additionally, we calculated measures of inter-rater agreement using the Fleiss' κ [2, 10].

[3] https://www.mural.co, last accessed June 2, 2023

Table 3: In the clustering study, we first asked our six expert participants to assign all 32 previously collected symbols to "privacy" or "security" using a Mural board. Each participant had their own board and did this task by themselves.

symbol	P1	P2	P3	P4	P5	P6	majority	assignments
stars	privacy	security	security	privacy	privacy	neither	privacy	3/6 (50%)
chain	security	privacy	security	security	security	neither	security	4/6 (67%)
eye	privacy	privacy	both	privacy	privacy	privacy	privacy	5/6 (83%)
camera	security	neither	privacy	privacy	privacy	neither	privacy	3/6 (50%)
signature	both	neither	security	security	security	privacy	security	3/6 (50%)
key and lock	security	neither	security	security	security	privacy	security	4/6 (67%)
hacker with hoodie	security	neither	security	security	both	both	security	3/6 (50%)
pop-up	privacy	privacy	privacy	privacy	privacy	neither	privacy	5/6 (83%)
padlock	both	security	security	security	security	both	security	4/6 (67%)
guardian	privacy	neither	privacy	both	privacy	both	privacy	3/6 (50%)
verification icon	security	privacy	privacy	security	both	security	security	3/6 (50%)
barrier tape	security	privacy	privacy	security	security	neither	security	3/6 (50%)
virus icon	security	neither	security	security	security	security	security	5/6 (83%)
network icon	privacy	neither	privacy	privacy	security	neither	privacy	3/6 (50%)
Guy Fawkes mask	security	neither	privacy	privacy	security	neither	-	2/6 (33%)
microphone	privacy	privacy	privacy	privacy	privacy	neither	privacy	5/6 (83%)
fingerprint	both	neither	security	security	security	privacy	security	3/6 (50%)
stop sign	security	neither	security	privacy	privacy	security	security	3/6 (50%)
shield	security	neither	privacy	privacy	both	both	-	2/6 (33%)
safe	security	privacy	security	security	security	neither	security	4/6 (67%)
curtains	privacy	privacy	privacy	privacy	privacy	privacy	privacy	6/6 (100%)
password	security	neither	security	security	security	both	security	4/6 (67%)
toogle	privacy	privacy	privacy	privacy	privacy	neither	privacy	5/6 (83%)
ciphertext	security	privacy	security	security	privacy	neither	security	3/6 (50%)
paragraph	security	neither	security	both	privacy	neither	-	2/6 (33%)
spotlight	security	neither	neither	security	privacy	neither	neither	3/6 (50%)
private browsing mask	privacy	privacy	privacy	privacy	privacy	privacy	privacy	6/6 (100%)
error message	both	neither	privacy	security	privacy	neither	-	2/6 (33%)
firewall	security	neither	security	security	security	both	security	4/6 (67%)
VPN icon	security	neither	privacy	privacy	privacy	both	privacy	3/6 (50%)
cookie icon	privacy	neither	privacy	privacy	privacy	neither	privacy	4/6 (67%)
shutter	privacy	privacy	privacy	privacy	privacy	neither	privacy	5/6 (83%)

The second task involved the free clustering and labeling of groups of symbols. To analyze the results of this task, we compared the number and labels of participants' clusters, as well as the symbols assigned to each cluster. We specifically sought to identify similarities and differences in participants' clustering of the symbols. Furthermore, we analyzed which clusters contained the same symbols, which allowed us to derive a hierarchical structure.

5.4 Results

As mentioned before, participants were asked to (1) distinguish between symbols for privacy and security, as well as, (2) freely group the symbols and label each resulting group.

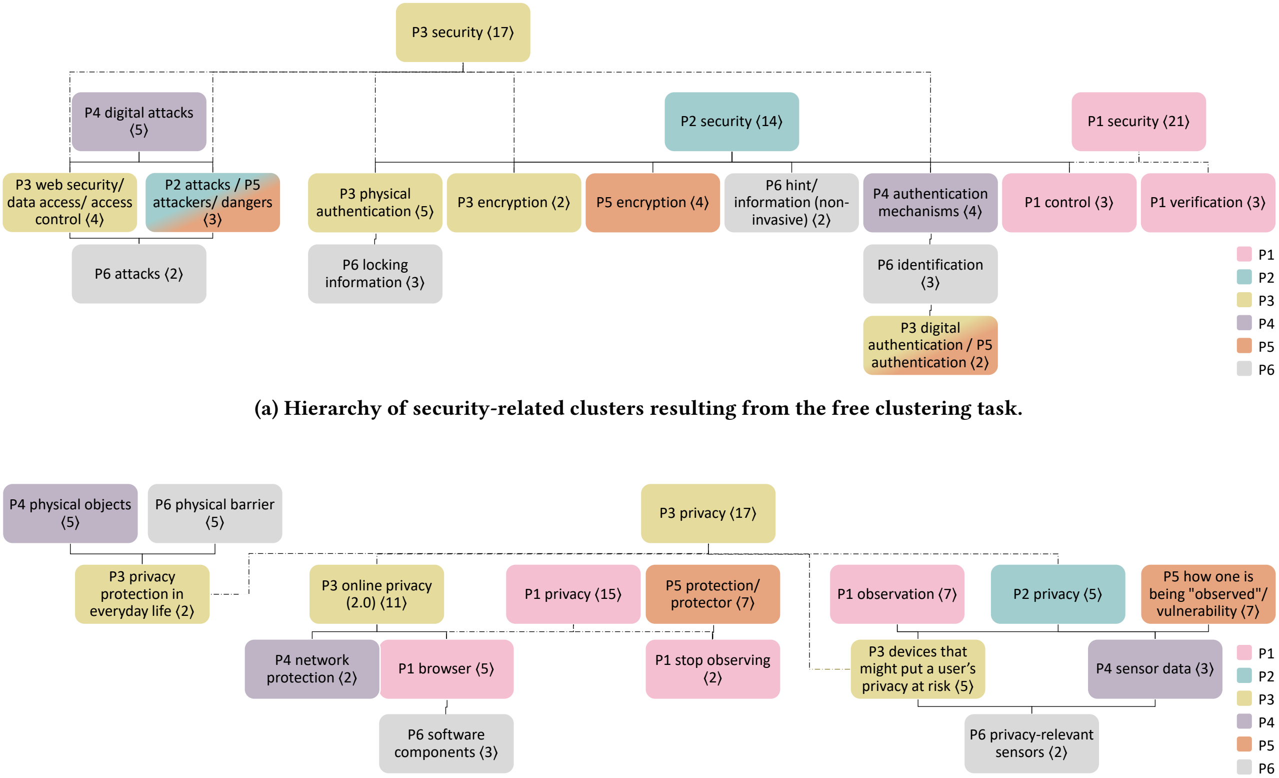
5.4.1 Security vs. Privacy. Table 3 summarizes how participants categorized each symbol when distinguishing between privacy and security. Overall, we found that Fleiss' $\kappa = -0.15$, indicating poor agreement between participants [10, 24]. However, the majority of participants (i.e., $n > 3$) selected the same categorization for fifteen symbols. All six participants assigned *curtains* and *private browsing mask* to privacy. Moreover, five participants agreed on the same categorization for six symbols: *eye* (privacy), *pop-up* (privacy), *microphone* (privacy), *toggle* (privacy) and *shutter* (privacy). Finally, seven symbols were assigned to the same category by four participants, namely *chain* (security), *key and lock* (security), *padlock* (security), *safe* (security), *password* (security), *firewall* (security) and *cookie icon* (privacy).

Colors. We asked participants to assign the five colors mentioned during brainstorming sessions to the themes of privacy or security. P1 and P6 did not assign the colors to any theme. P4 assigned all colors to privacy. P3 assigned *red*, *green*, and *yellow* to, both, privacy and security while not making any decision for *blue* and *black*. Only P2 and P5 categorized specific colors to either privacy or security. Both only agreed on *blue* being associated with privacy.

5.4.2 Free Clustering. Participants could freely create and name clusters of symbols and metaphors during the second clustering task (see Figure 3b). We analyzed the results by investigating which clusters were created and how they relate to each other. This allowed us to identify the underlying themes of participants' clusters.

Created Clusters. Our participants created 4 – 8 clusters each ($mean = 6.83$, $std = 1.47$). A complete list of all 41 assigned clusters can be found in Appendix B. Participants also labeled a symbol directly without assigning it to any larger cluster five times. Three of these labels were associated with the paragraph symbol (*legislation*, *legal protection*, and *security of people*). The other two labels referred to the *stars* (*password meter*) and the *pop-up* (*ads*).

Structuring the Clusters. Two participants (P1 and P3) first distinguished between privacy and security and then grouped the symbols further. This finding inspired us to investigate possible hierarchical structures between clusters of different participants. Hence, we analyzed which clusters from different participants contained the same symbols. This allowed us to derive a hierarchical


P3 security ⟨17⟩
P4 digital attacks ⟨5⟩
P2 security ⟨14⟩
P1 security ⟨21⟩
P3 web security/ data access/ access control ⟨4⟩
P2 attacks / P5 attackers/ dangers ⟨3⟩
P3 physical authentication ⟨5⟩
P3 encryption ⟨2⟩
P5 encryption ⟨4⟩
P6 hint/ information (non-invasive) ⟨2⟩
P4 authentication mechanisms ⟨4⟩
P1 control ⟨3⟩
P1 verification ⟨3⟩
P6 attacks ⟨2⟩
P6 locking information ⟨3⟩
P6 identification ⟨3⟩
P3 digital authentication / P5 authentication ⟨2⟩
P1
P2
P3
P4
P5
P6
P4 physical objects ⟨5⟩
P6 physical barrier ⟨5⟩
P3 privacy ⟨17⟩
P3 privacy protection in everyday life ⟨2⟩
P3 online privacy (2.0) ⟨11⟩
P1 privacy ⟨15⟩
P5 protection/ protector ⟨7⟩
P1 observation ⟨7⟩
P2 privacy ⟨5⟩
P5 how one is being "observed"/ vulnerability ⟨7⟩
P4 network protection ⟨2⟩
P1 browser ⟨5⟩
P1 stop observing ⟨2⟩
P3 devices that might put a user's privacy at risk ⟨5⟩
P4 sensor data ⟨3⟩
P6 software components ⟨3⟩
P6 privacy-relevant sensors ⟨2⟩
P1
P2
P3
P4
P5
P6

(a) Hierarchy of security-related clusters resulting from the free clustering task.

(b) Hierarchy of privacy-related clusters resulting from the free clustering task.

Figure 4: We analyzed which clusters between participants are completely contained in other clusters. This figure illustrates the resulting hierarchies of clusters. Hence, the top clusters contain the connected bottom clusters. Clusters on the same level are not necessarily distinct from each other (i.e., can contain the same symbols). Dashed lines indicate hierarchies directly defined by participants during the clustering task. The number of symbols of each cluster is indicated in angle brackets. We used different colors to highlight the participants who created each cluster. Please note that the figure does not contain clusters that did not lay inside any other cluster.

structure of clusters that are completely contained inside other clusters. 32 of the 41 clusters could be sorted into such a structure. Our analysis resulted in two independent hierarchies, one for privacy and for security (see Figure 4).

Security-related clusters predominantly described authentication (6 clusters: *physical/digital authentication*, *authentication (mechanisms)*, *identification*, and *locking information*), encryption (2 clusters), or attacks (5 clusters: *(digital) attacks*, *attackers/ dangers*, and *web security/ data access/ access control*). Other security-related themes included *control*, *hint/information*, and *verification*.

Privacy clusters were related to internet usage (4 clusters: *online privacy*, *browser*, *network protection*, and *software components*), privacy-invasions (5 clusters: *observation*, *devices that might put a user's privacy at risk*, *how one is being "observed"/ vulnerability*, *sensor data* and *privacy-relevant sensors*), physical privacy (3 clusters: *physical objects*, *physical barriers*, and *privacy protection in everyday life*), as well as privacy protection (2 clusters: *protection/ protector* and *stop observing*).

As mentioned before, not all clusters could be structured into our hierarchies, as they did not fit into any other cluster. Instead, we thematically organized them into protection/restriction (*protection mechanisms*, *software protection measures*, and *restriction*), *browser features*, *trust*, warnings (*warning/problem/danger*) and *others* (3 clusters: *other stuff*, *other* and *UI elements*).

Colors. Of our six participants, two (P1 and P6) did not cluster the provided colors at all. Moreover, 3 participants created their own cluster, only for colors (P2: *colors, feedback for UI buttons*, P3: *certificate status*, and P4: *system state*). However, P3 did not assign all five provided colors to their cluster called *certificate status (expired, valid, soon-to-be expiring)*, but only the colors *red*, *green*, and *yellow*. Only P5 assigned colors to clusters that contained symbols. P5 assigned *red* to *warning/problem/danger* and *attackers/dangers*, *green* to *protection/ protector*, *protection mechanisms* and *authentication*, *blue* to *protection/ protector*, *protection mechanisms* and *trust*, *yellow* to *warning/problem/danger*, as well as *black* to *legal protection*, *how one is being "observed"/ vulnerability* and *attackers/dangers*.

6 SYMBOL AND METAPHOR SPACE

To conclude our analysis and render our results easily applicable for future researchers and designers, we derived an *symbol and metaphor space for security and privacy*. The presented symbol and metaphor space may be used right away as a tool for researchers, designers, and developers. In the future, we envision the space to be further replicated and expanded through research targeting varying user groups with diverse cultural backgrounds.

6.1 Derivation of the Symbol & Metaphor Space

Based on the results of the clustering study, we derived the underlying themes of participants' clusters (i.e., *authentication*, *encryption*, *attacks*, *general security*, *protection/restriction*, *internet usage*, *privacy invasion*, *physical privacy*, *privacy protection*, *legal aspects*, *browser features*, *trust*, *warnings* and *others*). We then analyzed which of the symbols collected during the brainstorming sessions participants associated with these themes. To do so, we determined to which theme most participants assigned each symbol. Using this method, we were able to assign 25 of the 32 symbols to a specific theme (see Appendix C). Next, we applied the results of both clustering tasks to distinguish between privacy- and security-related themes, if applicable. We found that the clustering hierarchies derived from the free clustering task rarely conflicted with the results of the privacy vs. security clustering. The only symbol with conflicting assignments was *barrier tape*, which was assigned to *security* in the first task and to *physical privacy* in the second task.

We represented our findings in a symbol and metaphor space for privacy and security shown in Figure 1. We included *barrier tape* in the theme *physical privacy* but annotated the possible conflict using a footnote. Seven symbols (*chain*, *guardian*, *shield*, *safe*, *ciphertext*, *spotlight* and *VPN icon*) could not be conclusively assigned, since they were clustered equally frequently into multiple themes. Hence, these symbols are not part of the symbol and metaphor space.

6.2 Interpreting the Symbol & Metaphor Space

Our space consists of 10 *themes* (grey boxes) and 25 *symbols and metaphors* (all other boxes). Eight themes are either associated with privacy or security, which is visualized through connecting lines. All *symbols and metaphors* were assigned by participants of our clustering task to the theme that is situated on top. We used colors to visualize how many participants assigned each symbol to its corresponding theme. *Yellow-colored* symbols were only associated with a theme by two of our six participants. Future users of our symbol and metaphor space should therefore have in mind that these symbols might not be as clearly related to their theme as others. *Violet-colored* symbols were assigned to their theme by the majority of participants ($n > 3$), making them a safer choice for future applications.

6.3 Applying the Symbol & Metaphor Space

To conclude the description of our symbol and metaphor space for security and privacy, we discuss its envisioned application based on a few exemplary projects.

Webshop Privacy. A web designer is developing a webshop that specifically minimizes data collection about customers to protect their privacy. To make possible customers aware of these efforts, brief descriptive texts that appear in tooltips and a specific subpage that indicates this in a more detailed manner were added to the webshop. To create a visually recurring theme between the different information sources, the web designer wants to add the same graphical symbol to each. Therefore, the designer focuses on the privacy-related symbols in our space and decides that the *privacy protection* theme is most appropriate for this purpose. The designer then sees that the *private browsing mask* might be a fitting symbol, searches online for graphical representations of this symbol, and finally decides on an icon.

Tangible Authentication. A researcher is developing a tangible user interface for authentication on PCs. To enhance the user experience, the researcher wants to convey the functionality of the tangible user interface through its shape and the way people interact with it. Therefore, the researcher quickly focuses on the authentication theme in our symbol and metaphor space. First, the researcher excludes *fingerprint*, *signature*, and *password* because they are difficult to represent through the shape of a tangible user interface. The researcher then sees that *padlock* was only assigned to authentication by two of our six participants and, therefore, decides on a less ambiguous symbol, which is *key and lock*. Hence, the researcher develops a tangible user interface for authentication that involves having to insert a key-shaped authentication token in a device that resembles a keyhole.

App with Privacy Mode. An app developer deployed a new app that allows their users to share their location with others. The app includes a privacy mode that turns the tracking off. However, customers use this option less than expected. The developer now wants to make sure that the used eye icon was an adequate choice for indicating the privacy mode. Therefore, the developer searches for *eye* in our symbol and metaphor space and realizes that it was indeed assigned to *privacy* and more concretely to the theme of *privacy invasion*. Since this matches the functionality of the privacy mode well, the developer starts to look for possible other causes for the unexpected usage.

7 DISCUSSION

7.1 Unambigious: Perpetrators & Privacy

Some symbols were assigned to specific themes (almost) unanimously ($n >= 5(83\%)$), indicating very little ambiguity However, our participants were rarely in agreement when it came to symbols for security. Only the *virus icon*, was assigned to *security* by five of the six participants. When it comes to privacy, five of six participants agreed to the *eye*, *microphone*, *shutter*, *toggle*, and the *pop-up*. All six participants assigned *curtains* and *private browsing mask* to privacy. Our results further indicate even fewer strong agreements between participants when it comes to the free clustering task. This can be explained by the unrestricted nature of this task and the resulting large number of possible assignments to the 17 identified themes. Nevertheless, four symbols and metaphors were again assigned almost unanimously ($n = 5$). Both *camera* and *microphone* were associated with the theme of *privacy invasion*. A *hacker with a hoodie* and the *virus icon* were assigned to *attacks*, a security-related theme.

Hence, there seems to be large unanimity in the categorization of *perpetrator*-related symbols. Both the themes of privacy invasion and attack, represent perpetrators (i.e., a hacker, a virus, a microphone, and a camera). Therefore, we argue that **the application of perpetrator-representing symbols and metaphors could serve well for designs of future privacy and security mechanisms**, as already applied in related work [27]. However, future research is needed to investigate if such symbols elicit undesired negative emotions. Moreover, the above-observed trend of a more frequent agreement for privacy-related symbols and metaphors could not be clearly replicated for the free clustering task, since the four mentioned symbols were equally distributed between the themes *privacy invasions* and *attacks* (a security-related theme). However, it should be mentioned that cyber-attacks frequently lead to an invasion of the victim's privacy. Correspondingly, the *hacker with a hoodie* was assigned to both *privacy* and *security* by two of our six participants. This leads us to tentatively interpret that **privacy-related symbols might indeed be less ambiguous**. This observation should be, however, further investigated in future work, to come to a definite conclusion.

7.2 Most Ambiguous: Spotlights and Shields

Other symbols were interpreted very ambiguously. The *Guy Fawkes mask*, *shield*, *paragraph*, *error messages*, and the *spotlight* were not assigned to either security or privacy more frequently. However, while the *Guy Fawkes Masks* and *error messages* were not clearly associated with privacy or security, they were assigned to the same underlying themes by three of our six participants (i.e., *attacks* and *internet usage*). Thus, these two symbols nevertheless evoked similar associations in our participants. The symbol *paragraph* was assigned by half of the participants to its own cluster, describing *legal aspects*. This indicates that while this symbol is perceived as quite different from the others, it still usually evokes specific associations. However, ***spotlight* and *shield* were neither clearly assigned to privacy or security, nor to one of the free clustering themes**. We conclude that these two symbols are the most ambiguous. This is particularly surprising since shield icons are already widely used as security indicators [9].

7.3 Beyond Graphical User Interfaces

The symbols and metaphors we collected came both from the *digital world* (e.g., icons such as network, cookie, VPN, verification, and virus icons) and *physical world* (e.g., barrier tape, curtains, a hacker with a hoodie or a signature), since we asked our participants to speak out every symbol and metaphor that came to their mind and did not restrict the brainstorming. Therefore, **our results can be used beyond typical graphical user interfaces (GUIs) for other security and privacy mechanisms.** We envision our symbol and metaphor space to be used e.g., for tangible user interfaces, mixed reality applications, or purely analog objects (e.g., signs).

7.4 Implications of Recruiting Local HCI-adepts

We recruited HCI-adept participants for our studies to ensure a previous understanding of the topics of privacy and security. This allowed us to not rely on frequently rather abstract definitions of these topics or to refer to specific example use cases, which could have biased our participants. Nevertheless, the targeted recruiting of such participants proved much more difficult, which led to small sample sizes. Moreover, experts' perceptions of security might vary from non-experts [19]. Most participants of our studies were also (previously) affiliated with research labs situated in German-speaking countries. Therefore, the extent to which our results generalize to the general population – especially with diverse cultural backgrounds – needs to be investigated in future work [20].

7.5 Usage of Colors

Participants of both brainstorming sessions associated colors with security and privacy. *Red*, *green*, and *yellow* were mentioned in both sessions, *black* and *blue* were only discussed during the privacy session. Participants of both sessions further stated that *red* indicates danger, stop, or alarm, while *green* indicates the contrary (i.e., protected and secure). Similar distinctions between *green and red* have been implemented into security mechanisms, such as HTTPS indicators [9, 21]. However, participants of our clustering study did not associate colors with privacy or security or any specific free theme. Moreover, related work found that users might struggle with interpreting the meaning of colors in regard to security and privacy mechanisms, especially since they vary between systems [1, 9, 27].

7.6 Reflections on the Methodology

We conducted each of the three studies in a different format (i.e., in-person, hybrid, and remote). We based this decision on which format would allow us to recruit the largest possible sample of distinct (expert) participants. Nevertheless, we made interesting observations with regard to the various formats during the preparation and execution of each study, which we would like to share.

7.6.1 Preparing the Study Apparatus. We prepared a prompting slide for both brainstorming sessions (i.e., "Which symbols/metaphors do you associate with [privacy/security]?"), as well as consent forms and demographic questionnaires. Moreover, we brought a large poster, sticky notes, pens, and printed consent forms to the in-person session. For the hybrid session, we created a shared Mural board, tested the necessary hard- and software, and also prepared online consent and demographic forms. For both sessions, we previously discussed the planned procedure between all experimenters. **Hence, the preparation effort for the in-person and hybrid brainstorming sessions was quite similar.** However, we could use an already set up environment for the hybrid session, which contained an installed webcam, a microphone, and a large display. The preparation effort for the hybrid study would have increased otherwise. For the remote clustering study, we first developed the design of the Mural board and iteratively tested and discussed it involving multiple experimenters. This was necessary to make sure that participants would understand all task instructions correctly, without the presence of an experimenter. After deciding on a final design, we prepared one Mural board for each participant of the study (see Appendix A). Furthermore, we prepared an online consent form. **Overall, the preparation effort for the remote study was larger.** On the one hand, this resulted from having to prepare two clustering tasks rather than one brainstorming task. On the other hand, the effort was multiplied by the need to develop a much more stable and thoughtful study apparatus due to the absence of an experimenter.

7.6.2 Conducting the Study. Both brainstorming sessions were conducted with 2 or 3 experimenters present. One experimenter served as the main moderator (i.e., explaining the procedure and answering questions) and the others made sure that all participant feedback was correctly recorded and collected. For the hybrid session, the experimenters had to make sure that all participants could access/see the shared Mural board, where the ideas were collected. Moreover, the moderator had to ensure that online participants could participate in the discussion as equally as possible, as well as understand all instructions and comments made by in-person participants. *Hence, the hybrid study did require additional steps and a slightly different moderation style, compared to the in-person session.* Both sessions required all participants to be (virtually) present for the duration of the session and therefore also implied previous scheduling. **To conduct the remote study, it was only necessary for one experimenter to send the links to the mural boards to all participants, answer possible questions (no participant had questions), and check after one week if all participants had completed the study.** Moreover, participants could do the tasks whenever they saw fit, which was especially appreciated.

8 CONCLUSION

The usage of symbols and metaphors for security and privacy can support users' understanding, as they are an effective means to convey complex topics. With this paper, we build a knowledge base for future designers, developers, and researchers who aim to integrate such symbols or metaphors into security and privacy mechanisms. Therefore, we presented 32 symbols and metaphors – from a padlock and shield to fingerprint and eye – 16 HCI-adepts associated with privacy and security. Furthermore, we presented the results of a clustering study ($N = 6$), that shed light on how symbols for privacy might be distinct from symbols for security, as well as on how the symbols and metaphors can be clustered into 17 underlying themes. We then derived an initial symbol and metaphor space and demonstrated how it can be applied to different use cases. Our findings have practical implications for researchers, designers, and developers, as they support them in creating better-understood mechanisms that address the challenges of privacy and security.

ACKNOWLEDGMENTS

We thank our study participants for their time and valuable feedback. This project has been funded by the European Union – NextGeneration EU and the dtec.bw – Center for Digitization and Technology Research of the Bundeswehr.

REFERENCES

[1] Imtiaz Ahmad, Rosta Farzan, Apu Kapadia, and Adam J. Lee. 2020. Tangible Privacy: Towards User-Centric Sensor Designs for Bystander Privacy. *Proc. ACM Hum.-Comput. Interact.* 4, CSCW2, Article 116 (oct 2020), 28 pages. https://doi.org/10.1145/3415187

[2] Mousumi Banerjee, Michelle Capozzoli, Laura McSweeney, and Debajyoti Sinha. 1999. Beyond kappa: A review of interrater agreement measures. *Canadian Journal of Statistics* 27, 1 (March 1999), 3–23. https://doi.org/10.2307/3315487

[3] Alan F. Blackwell. 2006. The Reification of Metaphor as a Design Tool. *ACM Trans. Comput.-Hum. Interact.* 13, 4 (dec 2006), 490–530. https://doi.org/10.1145/1188816.1188820

[4] Daniel Bühler, Fabian Hemmert, and Jörn Hurtienne. 2020. Universal and Intuitive? Scientific Guidelines for Icon Design. In *Proceedings of Mensch Und Computer 2020* (Magdeburg, Germany) *(MuC '20)*. Association for Computing Machinery, New York, NY, USA, 91–103. https://doi.org/10.1145/3404983.3405518

[5] Verena Distler, Tamara Gutfleisch, Carine Lallemand, Gabriele Lenzini, and Vincent Koenig. 2022. Complex, but in a good way? How to represent encryption to non-experts through text and visuals – Evidence from expert co-creation and a vignette experiment. *Computers in Human Behavior Reports* 5 (March 2022), 100161. https://doi.org/10.1016/j.chbr.2021.100161

[6] Z. Efroni, J. Metzger, L. Mischau, and M. Schirmbeck. 2019. Privacy Icons:. *European Data Protection Law Review* 5, 3 (2019), 352–366. https://doi.org/10.21552/edpl/2019/3/9

[7] Serge Egelman, Raghudeep Kannavara, and Richard Chow. 2015. Is this thing on? Crowdsourcing privacy indicators for ubiquitous sensing platforms. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems.* 1669–1678.

[8] Matthias Fassl and Katharina Krombholz. 2023. Why I Can't Authenticate — Understanding the Low Adoption of Authentication Ceremonies with Autoethnography. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems* (Hamburg, Germany) *(CHI '23)*. Association for Computing Machinery, New York, NY, USA, Article 72, 15 pages. https://doi.org/10.1145/3544548.3581508

[9] Adrienne Porter Felt, Robert W. Reeder, Alex Ainslie, Helen Harris, Max Walker, Christopher Thompson, Mustafa Embre Acer, Elisabeth Morant, and Sunny Consolvo. 2016. Rethinking Connection Security Indicators. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*. USENIX Association, Denver, CO, 1–14. https://www.usenix.org/conference/soups2016/technical-sessions/presentation/porter-felt

[10] Joseph L Fleiss. 1971. Measuring nominal scale agreement among many raters. *Psychological bulletin* 76, 5 (1971), 378.

[11] D.A. Frincke and M. Bishop. 2004. Guarding the castle keep: teaching with the fortress metaphor. *IEEE Security & Privacy* 2, 3 (May 2004), 69–72. https://doi.org/10.1109/MSP.2004.13 Conference Name: IEEE Security & Privacy.

[12] Nina Gerber and Karola Marky. 2022. The Nerd Factor: The Potential of S&P Adepts to Serve as a Social Resource in the User's Quest for More Secure and Privacy-Preserving Behavior. In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*. USENIX Association, Boston, MA, 57–76. https://www.usenix.org/conference/soups2022/presentation/gerber

[13] Nina Gerber, Verena Zimmermann, Birgit Henhapl, Sinem Emeröz, and Melanie Volkamer. 2018. Finally Johnny Can Encrypt: But Does This Make Him Feel More Secure?. In *Proceedings of the 13th International Conference on Availability, Reliability and Security* (Hamburg, Germany) *(ARES 2018)*. Association for Computing Machinery, New York, NY, USA, Article 11, 10 pages. https://doi.org/10.1145/3230833.3230859

[14] David Gittins. 1986. Icon-based human-computer interaction. *International Journal of Man-Machine Studies* 24, 6 (June 1986), 519–543. https://doi.org/10.1016/s0020-7373(86)80007-4

[15] Hana Habib, Yixin Zou, Yaxing Yao, Alessandro Acquisti, Lorrie Cranor, Joel Reidenberg, Norman Sadeh, and Florian Schaub. 2021. Toggles, Dollar Signs, and Triangles: How to (In)Effectively Convey Privacy Choices with Icons and Link Texts. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems.* ACM, Yokohama Japan, 1–25. https://doi.org/10.1145/3411764.3445387

[16] Leif-Erik Holtz, Katharina Nocun, and Marit Hansen. 2011. Towards displaying privacy information with icons. In *Privacy and Identity Management for Life: 6th IFIP WG 9.2, 9.6/11.7, 11.4, 11.6/PrimeLife International Summer School, Helsingborg, Sweden, August 2-6, 2010, Revised Selected Papers 6.* Springer, 338–348.

[17] Hilary H Hosmer. 2000. *Visualizing risks: Icons for information attack scenarios.* Technical Report. DATA SECURITY INC BEDFORD MA.

[18] Renato Iannella, Adam Finden, and Stacked Creations. 2010. Privacy awareness: Icons and expression for social networks. In *Proceedings of the 8th Virtual Goods Workshop and the 6th ODRL Workshop.* 1–15.

[19] Iulia Ion, Rob Reeder, and Sunny Consolvo. 2015. "...No One Can Hack My Mind": Comparing Expert and Non-Expert Security Practices. In *Proceedings of the Eleventh USENIX Conference on Usable Privacy and Security* (Ottawa, Canada) *(SOUPS '15)*. USENIX Association, USA, 327–346.

[20] Muhammad Nazrul Islam. 2013. A systematic literature review of semiotics perception in user interfaces. *Journal of Systems and Information Technology* 15, 1 (March 2013), 45–77. https://doi.org/10.1108/13287261311322585

[21] Rebecca Jeong and Sonia Chiasson. 2020. 'Lime', 'Open Lock', and 'Blocked': Children's Perception of Colors, Symbols, and Words in Cybersecurity Warnings. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems.* ACM, Honolulu HI USA, 1–13. https://doi.org/10.1145/3313831.3376611

[22] Saraschandra Karanam, Janhavi Viswanathan, Anand Theertha, Bipin Indurkhya, and Herre Van Oostendorp. 2010. Impact of placing icons next to hyperlinks on information-retrieval tasks on the web. In *Proceedings of the Annual Meeting of the Cognitive Science Society*, Vol. 32.

[23] Patrick Gage Kelley, Joanna Bresee, Lorrie Faith Cranor, and Robert W. Reeder. 2009. A "nutrition label" for privacy. In *Proceedings of the 5th Symposium on Usable Privacy and Security.* ACM, Mountain View California USA, 1–12. https:

//doi.org/10.1145/1572532.1572538

[24] J. Richard Landis and Gary G. Koch. 1977. The Measurement of Observer Agreement for Categorical Data. *Biometrics* 33, 1 (1977), 159–174. http://www.jstor.org/stable/2529310

[25] Joscha Lausch, Oliver Wiese, and Volker Roth. 2017. What is a Secure Email?. In *Proceedings 2nd European Workshop on Usable Security*. Internet Society, Paris, France. https://doi.org/10.14722/eurousec.2017.23022

[26] Maggie Oates, Yama Ahmadullah, Abigail Marsh, Chelse Swoopes, Shikun Zhang, Rebecca Balebako, and Lorrie Faith Cranor. 2018. Turtles, Locks, and Bathrooms: Understanding Mental Models of Privacy Through Illustration. *Proceedings on Privacy Enhancing Technologies* 2018, 4 (Oct. 2018), 5–32. https://doi.org/10.1515/popets-2018-0029

[27] Fahimeh Raja, Kirstie Hawkey, Steven Hsu, Kai-Le Clement Wang, and Konstantin Beznosov. 2011. A brick wall, a locked door, and a bandit: a physical security metaphor for firewall warnings. In *Proceedings of the Seventh Symposium on Usable Privacy and Security*. ACM, Pittsburgh Pennsylvania, 1–20. https://doi.org/10.1145/2078827.2078829

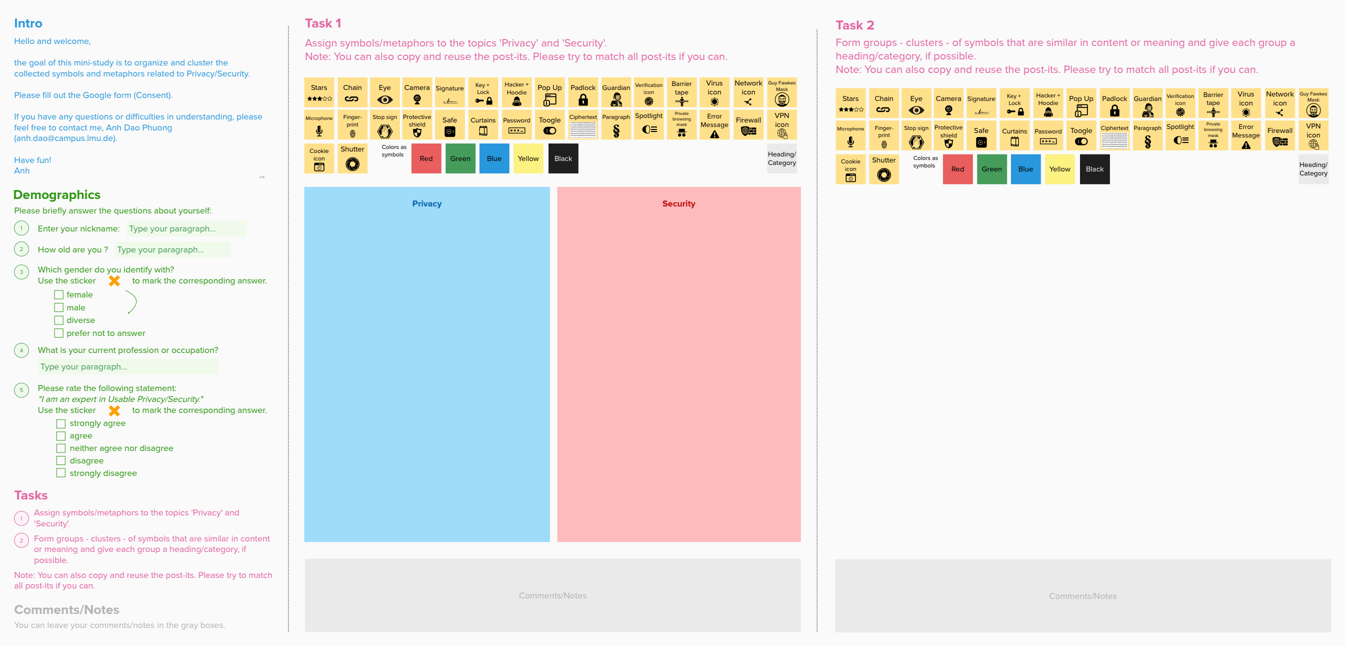
[28] Courtney N. Reed, Paul Strohmeier, and Andrew P. McPherson. 2023. Negotiating Experience and Communicating Information Through Abstract Metaphor. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems* (Hamburg, Germany) *(CHI '23)*. Association for Computing Machinery, New York, NY, USA, Article 185, 16 pages. https://doi.org/10.1145/3544548.3580700

[29] Nur Farhana Samsudin, Zarul Fitri Zaaba, Manmeet Mahinderjit Singh, and Azman Samsudin. 2016. Symbolism in Computer Security Warnings: Signal Icons and Signal Words. *International Journal of Advanced Computer Science and Applications* 7, 10 (2016).

[30] Alma Whitten and J Doug Tygar. 1999. Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0.. In *USENIX security symposium*, Vol. 348. 169–184.

[31] Maximiliane Windl, Anna-Marie Ortloff, Niels Henze, and Valentin Schwind. 2022. Privacy at a Glance: A Process to Learn Modular Privacy Icons During Web Browsing. In *Proceedings of the 2022 Conference on Human Information Interaction and Retrieval* (Regensburg, Germany) *(CHIIR '22)*. Association for Computing Machinery, New York, NY, USA, 102–112. https://doi.org/10.1145/3498366.3505813

A MURAL BOARD



Intro

Hello and welcome,

the goal of this mini-study is to organize and cluster the collected symbols and metaphors related to Privacy/Security.

Please fill out the Google form (Consent).

If you have any questions or difficulties in understanding, please feel free to contact me, Anh Dao Phuong (anh.dao@campus.lmu.de).

Have fun!
Anh

Demographics

Please briefly answer the questions about yourself:

1. Enter your nickname: Type your paragraph...
2. How old are you ? Type your paragraph...
3. Which gender do you identify with?
   Use the sticker ✗ to mark the corresponding answer.
   - □ female
   - □ male
   - □ diverse
   - □ prefer not to answer
4. What is your current profession or occupation?
   Type your paragraph...
5. Please rate the following statement:
   "I am an expert in Usable Privacy/Security."
   Use the sticker ✗ to mark the corresponding answer.
   - □ strongly agree
   - □ agree
   - □ neither agree nor disagree
   - □ disagree
   - □ strongly disagree

Tasks

1. Assign symbols/metaphors to the topics 'Privacy' and 'Security'.
2. Form groups - clusters - of symbols that are similar in content or meaning and give each group a heading/category, if possible.

Note: You can also copy and reuse the post-its. Please try to match all post-its if you can.

Comments/Notes

You can leave your comments/notes in the gray boxes.

Task 1

Assign symbols/metaphors to the topics 'Privacy' and 'Security'.
Note: You can also copy and reuse the post-its. Please try to match all post-its if you can.

Task 2

Form groups - clusters - of symbols that are similar in content or meaning and give each group a heading/category, if possible.
Note: You can also copy and reuse the post-its. Please try to match all post-its if you can.

Figure 5: Mural boards we prepared for each participant of the clustering study. After providing demographic information about themselves, participants had to first divide a given list of symbols into security- or privacy-themed and then group them freely. We translated the task descriptions from their original language where necessary for this figure.

B FREE CLUSTERING RESULTS

Table 4: Free clustering of all 32 symbols mentioned during both brainstorming sessions.

P1	P2	P3	P4	P5	P6
restriction: *chain, signature, padlock, barrier tape, fingerprint, stop sign, shield, firewall*	security: *chain, signature, key and lock, padlock, guardian, verification icon, fingerprint, stop sign, shield, safe, password, ciphertext, firewall, VPN icon*	online privacy (2.0): *pop-up, guardian, verification icon, network icon, Guy Fawkes mask, shield, toogle, private browsing mask, error message, VPN icon, cookie icon*	browser features: *pop-up, stop sign, shield, safe, private browsing mask, error message, cookie icon*	protection/ protector: *chain, guardian, shield, safe, curtains, toogle, private browsing mask*	physical *barrier: guardian, barrier tape, shield, curtains, shutter*
observation: *eye, camera, hacker with hoodie, guardian, Guy Fawkes mask, microphone, shutter*	other stuff: *stars, network icon, curtains, toogle, paragraph, spotlight, error message, cookie icon, shutter*	physical authentication: *signature, key and lock, padlock, stop sign, safe*	physical objects: *chain, padlock, barrier tape, curtains, spotlight*	how one is being "observed"/ vulnerability: *eye, camera, pop-up, network icon, microphone, spotlight, cookie icon*	software protection measures: *private browsing mask, firewall, VPN icon, cookie icon*
browser: *pop-up, network icon, toogle, error message, cookie icon*	privacy: *eye, camera, barrier tape, microphone, private browsing mask*	devices that might put a user's privacy at risk: *eye, camera, Guy Fawkes mask, microphone, shutter*	digital attacks: *hacker with hoodie, guardian, virus icon, Guy Fawkes mask, firewall*	encryption: *key and lock, padlock, ciphertext, VPN icon*	software components: *pop-up, toogle, error message*
other: *stars, virus icon, ciphertext, spotlight*	attacks: *hacker with hoodie, virus icon, Guy Fawkes mask*	web security/ data access/ access control: *eye, hacker with hoodie, virus icon, firewall*	authentication mechanisms: *signature, key and lock, fingerprint, password*	warning/ problem/ danger: *barrier tape, stop sign, error message*	identification: *signature, fingerprint, password*
control: *key and lock, safe, VPN icon*	ads: *pop-up*	*digital authentication: fingerprint, password*	sensor data: *eye, camera, microphone*	protection mechanisms: *firewall, VPN icon, shutter*	locking information: *key and lock, padlock, safe*
verification: *verification icon, password, paragraph*		encryption: *chain, ciphertext*	network protection: *network icon, VPN icon*	trust: *stars, signature, verification icon*	hint/ information (non-invasive): *verification icon, stop sign*
stop observing: *curtains, private browsing mask*		privacy protection in everyday life: *barrier tape, curtains*	UI elements: *stars, toogle*	attackers/ dangers: *hacker with hoodie, virus icon, Guy Fawkes mask*	attacks: *hacker with hoodie, virus icon*
		security of people: *paragraph*	legislation: *paragraph*	authentication: *fingerprint, password*	
		password meter: *stars*		legal protection: *paragraph*	

C SYMBOLS ASSOCIATED WITH CLUSTER GROUPS

Table 5: Symbols assigned to each group of clusters (i.e., had more corresponding assignments to this group than any other). The relative agreement between participants is shown in the last column. Hence, symbols with an agreement score of >= 50% were assigned to the same group of clusters by the majority of participants. Seven symbols could not be assigned unambiguously to any group (here: cluster group "-").

symbol	most frequently assignedgroup	assignments
stars	other*	3/6 (50%)
chain	-	
eye	privacy invasion	4/6 (67%%)
camera	privacy invasion	5/6 (83%%)
signature	authentication	3/6 (50%)
key and lock	authentication	3/6 (50%)
hacker with hoodie	attacks	5/6 (83%%)
pop-up	internet usage	3/6 (50%)
padlock	authentication	2/6 (33%)
verification icon	general security	3/6 (50%)
barrier tape	physical privacy	3/6 (50%)
virus icon	attacks	5/6 (83%)
network symbol	internet usage	3/6 (50%)
Guy Fawkes mask	attacks	3/6 (50%)
microphone	privacy invasion	5/6 (83%%)
fingerprint	authentication	4/6 (67%%)
stop sign	general security	2/6 (33%)
curtains	physical privacy	3/6 (50%)
password	authentication	4/6 (67%%)
toogle	internet usage	3/6 (50%)
paragraph	legal aspects*	3/6 (50%)
private browsing mask	privacy protection	2/6 (33%)
error message	internet usage	3/6 (50%)
firewall	protection/ restriction*	3/6 (50%)
cookie icon	internet usage	2/6 (33%)
shutter	privacy invasion	2/6 (33%)