The TaPSI Research Framework - A Systematization of Knowledge on Tangible Privacy and Security Interfaces

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

Maximiliane Windl
LMU Munich
Munich, Germany
Munich Center for Machine Learning (MCML)
Munich, Germany
maximiliane.windl@ifi.lmu.de

Florian Alt
LMU Munich
Munich, Germany
University of the Bundeswehr Munich
Munich, Germany
florian.alt@ifi.lmu.de

Karola Marky
Ruhr University Bochum
Bochum, Germany
karola.marky@rub.de

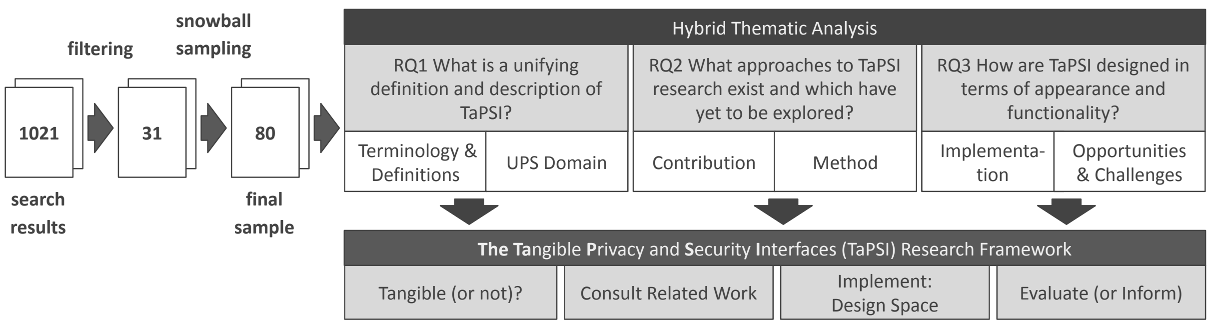


Figure 1: We searched for publications on *tangible privacy and security interfaces* (TaPSI) in 28 usable privacy and security (UPS) venues and used snowball sampling to broaden our sample further. Applying hybrid thematic analysis to our final sample ($n = 80$), we describe the used terminology and definitions, addressed UPS domains, contributions, methods, implementations, and opportunities or challenges inherent to TaPSI. Based on these findings, we present the TaPSI Research Framework, which gives recommendations for future researchers and describes a design space for TaPSI.

Abstract

This paper presents a comprehensive Systematization of Knowledge on tangible privacy and security interfaces (TaPSI). Tangible interfaces provide physical forms for digital interactions. They can offer significant benefits for privacy and security applications by making complex and abstract security concepts more intuitive, comprehensible, and engaging. Through a literature survey, we collected and analyzed 80 publications. We identified terminology used in these publications and addressed usable privacy and security domains, contributions, applied methods, implementation details, and opportunities or challenges inherent to TaPSI. Based on our findings, we define TaPSI and propose the TaPSI Research Framework, which guides future research by offering insights into when and how to conduct research on privacy and security involving TaPSI as well as a design space of TaPSI.

CHI '25, Yokohama, Japan

ACM ISBN 979-8-4007-1394-1/25/04
https://doi.org/10.1145/3706598.3713968

CCS Concepts

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

Keywords

tangible privacy, tangible security, tangible interface, TaPSI, framework

ACM Reference Format:
Sarah Delgado Rodriguez, Maximiliane Windl, Florian Alt, and Karola Marky. 2025. The TaPSI Research Framework - A Systematization of Knowledge on Tangible Privacy and Security Interfaces. In *CHI Conference on Human Factors in Computing Systems (CHI '25), April 26–May 01, 2025, Yokohama, Japan.* ACM, New York, NY, USA, 28 pages. https://doi.org/10.1145/3706598.3713968

1 Introduction

Tangible user interfaces give physical form to digital information by using artifacts to represent digital information or enable control by allowing for direct manipulation of digital information [121]. People can interact with these physical artifacts as they interact with any other physical object. Therefore, tangible interfaces offer unique opportunities, such as supporting intuitive and natural interaction (i.e., direct manipulation [67]), providing immediate tactile feedback [67], being fun or engaging to interact with [130], and enhancing users' feeling of being in control [141].

These advantages of tangible interfaces are particularly beneficial for usable privacy and security (UPS) solutions, which are often considered difficult to use, too abstract, or annoying [5, 129, 131]. Hence, tangible interfaces for privacy and security have long found their way into research and commercialization. Bank cards form one well-known example. They ensure that no unauthorized person can retrieve money from a bank account by restricting access to legitimate users only. Other examples of tangible interfaces for UPS include physical authentication tokens like YubiKeys [103], (smart) camera covers [43], network management devices that incorporate physical access restrictions [137] or educational boardgames [59]. Due to their tangible nature, these interfaces make it easy for users to understand when and where they are used.

Despite their clear advantages for human-centered security, no overarching conceptualization of usable tangible privacy and security interfaces exists today. Existing formalized approaches focus on specific sub-domains. For example, Mehta et al.'s *Privacy Care* framework [89] describes tangible privacy in the IoT. This lack of overarching formalization prevents researchers from gaining insights relevant to all types of tangible interfaces for privacy and security. We provide a solution to this problem by presenting the first overarching Systematization of Knowledge (SoK) on *tangible privacy and security interfaces* (TaPSI). Finding and comprehending literature on TaPSI can be challenging due to inconsistent and ambiguous terminology. For example, the terms *"tangible"*, *"graspable"*, and *"physical"* are frequently used interchangeably [121]. Our SoK facilitates the identification of relevant literature across UPS domains, fosters a common understanding for clearer discussions, and ensures that future publications are easily discoverable by answering the research question:

RQ 1 What is a unifying definition and description of *tangible privacy and security interfaces (TaPSI)*?

The decades-spanning literature on TaPSI [55, 102] and the lack of cross-references among publications from different UPS domains makes it particularly difficult to identify best research practices or avoid common pitfalls. This SoK, thus, guides researchers in investigating TaPSI by addressing the question:

RQ 2 What approaches to TaPSI research exist and which have yet to be explored?

In addition, our work assists researchers in the design of TaPSI and discusses their inherent opportunities and challenges for UPS by answering the question:

RQ 3 How are TaPSI designed in terms of appearance and functionality?

Analyzing 80 publications, we found that tangible solutions have been proposed frequently for authentication, privacy management, and access control. Research on TaPSI usually provides artifacts and empirical contributions that are optionally used to present theoretical insights. We also identified design dimensions of TaPSI in terms of their appearance, functionalities, and further impacting factors. Our work serves as a foundational resource for researchers exploring the unique opportunities and challenges associated with TaPSI. It provides a clear definition of TaPSI, reflects on existing research, and identifies new avenues for future research. Furthermore, it offers a comprehensive framework for designing research projects involving TaPSI and a design space for TaPSI.

Contribution Statement We contribute to research in the field of UPS by conducting the first SoK of tangible interfaces with privacy and security-related purposes. In particular, our contributions are:

(1) We used query-based and snowball sampling to identify 80 relevant publications, which we analyzed along seven dimensions: (1) usage of terminology, (2) corresponding UPS domains, (3) provided contributions, (4) applied methods, (5) implementation details, as well as (6) key opportunities and challenges inherent to TaPSI.
(2) We present our findings, derive a unified definition for future research of the term *tangible privacy and security interfaces (TAPSI)*, and present the TaPSI Research Framework that informs the design and evaluation of future TaPSI.

2 Related Work

Our work builds on SoKs on UPS and tangible user interfaces (TUIs).

2.1 SoKs for Usable Privacy and Security (UPS)

Garfinkel and Lipford [51] define UPS as *"the design, construction, and deployment of systems that people can use to secure computers and personal information"* [51, p. 7], identifying themes like authentication, adversarial modeling, system administration, consumer privacy, social computing, ecological validity, and education. Reutner et al. [23] emphasized the need for *tailorability and transparency*, noting that one-size-fits-all solutions often fail. They also stress that clear information is key to overcoming resistance to privacy and security measures. Alt and Zezschwitz [9] highlighted trends such as the impact of new technologies, stakeholder-specific designs, emerging methodologies, and interdisciplinary knowledge in UPS research. Distler et al. [40] reviewed empirical methods and risk representations, noting diverse methodologies and the importance of user-centric approaches. We adopted their categorization of UPS topics and study methods. Acquisti et al. [3] reviewed privacy and security decision-making with a focus on nudging techniques.

2.1.1 Usable Security. Di Nocera et al. [39] found that usable security research centers on evaluating authentication usability, supporting developers, understanding the impact of design decisions on security behavior, and developing formal evaluation models. Lennartson et al. [75] observed a focus on simplicity, task completion time, error rates, and error management. Nwokedi et al. [96] discussed the link between usability and security evaluation criteria. Other SoKs examine authentication mechanisms [97, 123].

2.1.2 *Usable Privacy.*

Iachello and Hong [65] summarize trends in the past usable privacy research and highlight promising yet underexplored directions for future research. In particular, they propose focusing on supporting users in managing their privacy, developing better analysis and evaluation methods, and focusing on theoretical contributions to understand the relationship between privacy and technological acceptance better. Acquisti et al. [4] identified three themes in empirical research on privacy behavior, that are uncertainty, context-dependence, and malleability. They argue that users are uncertain about their privacy preferences and the consequences of their privacy-related choices. Moreover, user's concerns are context-dependent and malleable (i.e., manipulable).

Summary. Prior SoKs provide a foundation for understanding the landscape of UPS. Moreover, they highlight the need for novel UPS interfaces that provide simplicity and transparency [4, 23, 75]. Tangible interfaces could be particularly well-suited to tackle these challenges, as they build upon pre-existing innate (i.e., reflexes and instincts) and sensorimotor (i.e., acquired in early childhood) knowledge and are, therefore, easy to understand and use [64, 89].

2.2 SoKs for Tangible User Interfaces (TUIs)

In 1997, Ishii and Ullmer [68] introduced the concept of "Tangible Bits", integrating digital information into the physical environment, laying the groundwork for TUI designs. Tangible bits can be applied to interactive surfaces, coupled with graspable physical objects, and implemented as ambient devices for peripheral awareness. In 2000, Ullmer and Ishii [121] presented the model-control-representation (physical and digital) interaction model (MCRpd), describing three key characteristics of TUIs based on their physical representations (i.e., the tangible artifacts): (1) computationally connected to underlying digital information, (2) embody interactive control mechanisms, and (3) perceptually related to actively transmitted digital representations. The authors discuss how the physical state of a TUI embodies key aspects of the system's digital state. In 2008, Ishii [67] contributed specific advantages inherent to TUIs. TUIs provide immediate tactile feedback, have conceding input and output spaces (i.e., they provide seamless information representation that spans the physical and digital domains), and have persistent physical states. Opposed to GUIs, TUIs are usually implemented for a specific purpose. They support space-multiplexed input, making them suitable for co-located and remote collaboration.

In addition to Ishii and Ullmer, other researchers have contributed excellent SoKs on TUIs. Fishkin [47] provided a taxonomy of TUIs, categorizing them based on their embodiment (i.e., the coupling between the user's tangible input and the interface's output) and the applied metaphor.

Hurtienne and Israel [64] defined intuitiveness in the scope of tangible interactions and its relationship to different knowledge categories. They describe the continuum of pre-existing knowledge, which includes innate (lowest level) knowledge, sensorimotor knowledge, culture, expertise, and tools (highest level). With increasing levels, the need for specialization increases, and the number of people with that knowledge decreases. Hurtienne et al. [64] argue intuitiveness can be assigned to any level of this continuum as long as users unconsciously apply the knowledge.

Shaer and Hornecker [110] reviewed the opportunities and challenges inherent to TUIs. They found that TUIs can (1) foster collaboration and discussions, (2) are physically and socially situated in the user's world, (3) support and stimulate reflection, (4) enable direct, integrated, and compatible space-multiplexed user input, (5) foster creativity by allowing designers to vary shapes, colors, weights, material and interactional constraints, and (6) provide rich tactile or embodied feedback even supporting eyes-free control. However, TUIs suffer from challenges regarding their scalability, bulkiness, lack of versatility, and create physical clutter. Users can get tired from performing tangible interactions [110].

Further SoKs explore tangible interactions and TUIs: Holmquist [62] categorized TUIs into *containers, tokens, and tools.* Hornecker and Buur [63] synthesize different frameworks on tangible interactions and present the key themes tangible manipulation, spatial interaction, embodied facilitation, and expressive representation. Shaer and Hornecker [110] introduced the token and constraints paradigm, defining TUIs in terms of pyfos (objects), tokens, constraints, variables (digital information and functions), and actions (possible manipulations). Mazalek and Van den Hoven [83] compared TUI frameworks and noted the scarcity of domain-specific insights. Wensveen et al. [130] argued that TUIs can influence emotions and enhance engagement. Other SoKs focused on TUIs in educational contexts, discussing their potential to enhance learning, cognition, memorability, and social development [77, 78, 104].

Summary. There is extensive research on TUIs, their advantages and limitations. TUIs can be described and clustered in different ways. In our work, we applied Fishkin's taxonomy [47] to the TaPSI presented in our sample of publications. We chose this taxonomy as it separates the individual categories particularly clearly, compared to others that tend to span continuums. TUIs also offer unique advantages over digital interfaces. In particular, they can be used independently or augment other objects [68]. They can be implemented as ambient displays [68]. They are intuitive to use and engaging [62, 64, 130], can foster collaboration, discussions, reflection, and creativity [110], and provide rich and immediate tactile or embodied feedback [67, 110]. Finally, they couple the physical and digital world [47, 63, 67, 68].

2.3 Formalizing Tangible Privacy

While there is no overarching conceptualization of TaPSI yet, we found publications focusing on IoT privacy.

Ahmad et al. [7] presented the term "tangible privacy", which describes *"privacy control and feedback mechanisms that are 'tangible,' i.e., manipulated or perceived by touch, and of 'high assurance,' i.e., they provide clear confidence and certainty of privacy to observers"* [7, p. 18]. Mehta et al. [89] present the *Privacy Care* framework which investigates privacy management through *"tangible and embodied style interactions"* [89, p. 7]. Their framework describes tangible privacy interfaces as direct, ready-to-hand, and customizable. Direct means that the interfaces allow for timely and intuitive interactions through metaphors. Ready-to-hand describes supporting ad hoc interactions that are not intrusive. Hence, they offer periphery-to-center attention transitions. Finally, customizable describes tangible privacy mechanisms that are adaptable to different usage contexts (e.g., by providing modular hardware or configurable software).

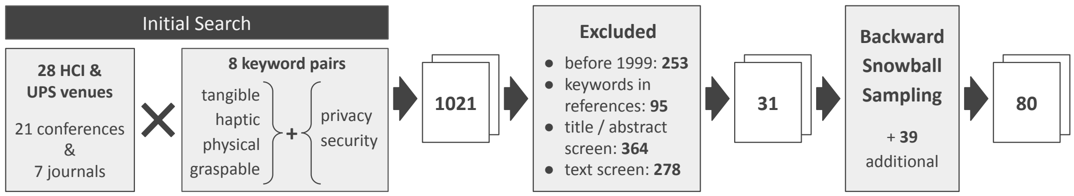


Figure 2: The data collection consisted of three steps. First, we collected 1021 publications from 28 different venues known for *usable privacy and security* and HCI publications. Next, we applied both automatic and manual filtering to focus on works that describe TaPSI. Through this, we identified 31 relevant publications, which we used for backward snowball sampling to broaden our initial search scope, finding 49 additional works.

Delgado Rodriguez et al. [31] used these publications to argue that tangible privacy mechanisms are physical objects that can be manipulated or perceived through tangible interaction. They increase awareness of privacy risks and communicate sensor states unambiguously, intuitively, and verifiably.

Summary. Since 2020, researchers have established the term *"tangible privacy"* to describe interfaces that help end-users protect their privacy in IoT environments and outlined the advantages of these mechanisms.

Summary: Research Gap

Our SoK demonstrates that many benefits described in tangible privacy for IoT research are also relevant to other security and privacy domains. However, the lack of formalization and inconsistent terminology impede researchers from leveraging existing findings on tangible interfaces across different UPS domains. *Our work is the first to distill findings on tangible interfaces from all areas of UPS research, creating a unified knowledge base. We provide a common definition, highlight promising open questions for future research, and outline both opportunities and common pitfalls.*

3 Literature Search: Data Collection

Figure 2 shows an overview of the data collection process that combined search-based and backward sampling.

3.1 Initial Search

3.1.1 Keywords and Targeted Venues. The four authors met to discuss potential search keywords and relevant target venues (conferences and journals) for HCI and usable security research. We also conducted test searches on Google Scholar and asked two further senior UPS researchers to review the list of venues.

Query. Starting with the term *"tangible privacy"*, presented by Ahmad et al. [7] in 2020 and since then used by other researchers [37, 89, 133], we collected synonyms for the word "tangible" to generate a broader set of search queries. This resulted in the following terms: *"tangible," "haptic," "graspable,"* or *"physical"*. As this paper focuses on privacy and security, we generated the following eight queries for our initial searches: *"tangible privacy"*, *"tangible security"*, *"haptic privacy"*, *"haptic security"*, *"graspable privacy"*, *"graspable security"*, *"physical privacy"*, and *"physical security"*.

Venues. During the brainstorming session, we came up with 28 relevant venues for publishing HCI (especially tangible user interfaces) or usable security-related research. This list included 21 conferences: CHI, CSCW, UIST, IUI, HCII, ICMI, CCS, Usenix Security, TEI, AHs, SOUPS, Symposium on S&P, NDSS, MUM, MuC, MobileHCI, DIS, NordiCHI, Interact, OzCHI, and ESORICS. It also included seven journals: IMWUT, TOCHI, International Journal of Human-Computer Studies, BIT, Computers & Security, IEEE Security & Privacy, and PoPETS. Refer to Appendix B for a glossary of all venue acronyms and their full names.

3.1.2 Paper Collection. Next, we conducted full-text searches (i.e., searches over the whole text body of publications) using the 8 queries across 28 venues, resulting in 224 independent searches (28 venues × 8 queries). To be able to specify a replicable cut-off date, all 224 searches had to be performed within a short time. Therefore, we developed Python scripts to automate these searches and store the results in tables. Our scripts accessed the content of the digital libraries' search result sites by using URLS generated through manual tests of their search interfaces as templates. Table 8 provides an overview of each venue's digital libraries or search tools and the search queries and filtering parameters. We used the venue title as a filtering parameter to focus on targeted venues. We used each publisher's digital library to make sure that our results are as complete and up-to-date as possible. However, we used Google Scholar for the few cases, where a digital library lacked adequate search functionalities. To ensure accuracy, we manually performed 50 randomly selected searches to compare the results with the automated table, finding no discrepancies. This initial search identified 1021 publications published until March 15, 2024.

3.1.3 Description of Search Results. The 1021 results were published between 1980 and 2024. 75% of them were published between 1999 and 2024. Furthermore, 931 (91.19%) of these results were obtained by searching for *"physical security"*. In comparison, *"physical privacy"* resulted in 69 (6.76%) publications, *"tangible privacy"* in 37 (3.62%), and *"tangible security"* in 29 (2.72%). Both, *"haptic privacy"* and *"haptic security"* were only found once. The venues in which most of our initial search results were published were Computers & Security (431; 42.21%), CCS (129; 12.68%), IEEE Security & Privacy (86; 8.42%), CHI (73; 7.15%), USENIX Security (64; 6.27%), and the SOUPS (73; 5.97%). All other venues contributed less than 5% of our results. For more details, we refer to Appendix A.2.

[1]Note that PoPETS is self-published since April 2022.

Table 1: We targeted 28 venues from different publishers with our initial full-text search. We used the digital libraries and search tools listed in this table. All search queries used a combination of 2 keywords separated by a whitespace, e.g., "tangible privacy" or "physical security." We used the venue title as a filtering parameter to restrict our searches to only targeted venues. Refer to Appendix B for a glossary of all venue acronyms and their full names.

Publisher	Digital Library	Venues	Search Query & Filter Parameters
ACM	ACM DL	CHI, CSCW, UIST, IUI, ICMI, CCS, TEI, AHs, MUM, MuC, MobileHCI, DIS, NordiCHI, OzCHI, IMWUT, TOCHI, MobileHCI, SOUPS	query: *"keyword1 keyword"*; URL parameters: *SpecifiedLevelConceptID* or *SeriesKey*; additional query for CSCW and MobileHCI: *"keyword1 keyword2"*and"venue" with SeriesKey *pacmhci*
Springer (see Appendix)	SpringerLink	HCII, Interact, ESORICS	query: *"keyword1 keyword2"&"venue"*; parameters: *Publication Title* has to contain venue
IEEE	IEEE-Explore	Symposium on S&P, IEEE Security & Privacy	query: *("Full Text & Metadata":"keyword1 keyword2") and ("Publication Title":"venue")*
Elsevier	ScienceDirect	International Journal of Human-Computer Studies, Computers & Security	query:*"keyword1 keyword2"*; parameters: *Journal or book title* has to contain the venue
Taylor & Francis	Taylor & Francis Online	BIT	query:*"keyword1 keyword2"*; searched on https://www.tandfonline.com/journals/tbit20
Usenix, Sciendo and Internet Society	Google Scholar	Usenix Security, SOUPS, PoPETS[1], NDSS	query:*"keyword1 keyword 2"*; URL parameter: *source:"venue"*

3.2 Filtering of Search Results

We filtered the publications for relevance.

3.2.1 Automatized Pre-Filtering. We excluded publications published before 1999 as the three works [5, 131, 142] initiating research on UPS were published in 1999 [23]. From the remaining publications, Python scripts excluded those without references to focus on evidence-based articles and those where the search keywords appeared only in the reference list and not in the main text. Two researchers reviewed the 195 publications where the script could not extract or locate the keywords applying the same criteria. To ensure consistency, 20% (39) was double-coded, with no disagreements found. This reduced the list to 673 publications.

3.2.2 Manual Filtering. Next, we manually filtered each of the remaining 673 publications to identify those in scope for our research.

Pre-Filtering Based On Title & Abstract. We first defined that in-scope publications should mention *objects/mechanisms that can be manipulated or perceived by touch and that specifically support users regarding security/privacy.* Using this criterion, two researchers independently reviewed the abstracts and titles of 50 random publications to decide which to confidently filter out. They discussed discrepancies to ensure a common understanding.

Both researchers subsequently reviewed 50 more publications independently in a second double-coding phase, with only 3 disagreements out of 50. This indicated a good understanding of the filtering criteria, allowing the first author to complete the pre-filtering of the remaining publications. After this step, 309 publications remained in the pool of potentially relevant sources.

Final Filtering Based On Full Text. We refined our filtering criterion before performing the final filtering step. Here, we considered publications that *describe, design, implement, or evaluate objects/mechanisms that can be manipulated or perceived by touch and that specifically support users in regard to their (cyber) security or privacy* to be in the scope of our literature survey. This includes publications that *focus solemnly on tangible solutions, as well as research that compares tangible to non-tangible solutions.* All publications not meeting this criterion were excluded from further analysis.

Four coders split up the remaining 309 publications for filtering. We took multiple steps to ensure consistency between coders. First, 15% (49 publications of 309) of publications were double-coded. We identified 5 disagreements (10%), which we resolved through discussions where all coders reviewed the papers in question together, clarified ambiguities in the criteria, and reached a consensus. This allowed us to refine the coders' common understanding of the inclusion criterion as follows:

Focus on Privacy or Security. We discarded publications that describe, design, or implement tangible mechanisms where the authors did not envision privacy- or security-related use cases as a primary usage scenario in the scope of our analysis. Hence, we filtered out publications where security and privacy were only considered after implementing or evaluating the tangible interface (e.g., as future work).

Tangible Mechanism Is A Core Theme. We did not include publications where tangible mechanisms were only peripheral to the conducted investigation. For example, we filtered out publications that merely conducted security analysis, described attack vectors, used image recognition on pictures of a tangible object, or implemented software for (tangible) devices. However, we considered publications in scope that mainly focused on such topics but additionally developed a physical prototype (for example, as a proof of concept).

Reference to a Specific TaPSI. We only analyzed publications describing, designing, implementing, or evaluating one or multiple specific tangible mechanisms. For example, we excluded publications on users' perception of generically described device types (e.g., unspecified webcam covers or smart locks) or the applicability of natural interactions with generic commodity devices (e.g., keyboards, mice, or smartphones) for authentication.

No Opinion and Literature Survey Contributions. Finally, we did not analyze opinion pieces and literature surveys. However, we did use these publications [85, 109, 114] as additional starting points for the snowball-sampling process.

All other unclear, or potentially in-scope publications were discussed between all coders in regular online meetings.

3.3 Snowball Sampling

Starting with the remaining 31 publications and three opinion/survey pieces [34, 86, 109, 114], we applied backward snowball sampling [135]. We noted any potentially relevant related work mentioned in these publications and screened them for inclusion by applying the criteria presented in Section 3.2.2. These steps were iteratively repeated for publications found during the snowball sampling process until we could no longer find any relevant additions. Again, we discussed all uncertainties in regular meetings. We did not focus on specific keywords or venues during this sampling phase. This allowed us to explore and collect publications not considered in our initial search, making our sample much broader and directed to publications that authors from our sample considered relevant. It also mitigated potential limitations from our initial selection of specific keywords and venues. Backward snowball sampling added 49 publications to our sample, along with an additional relevant position paper [34].

Summary: Data Collection

We first searched for publications on TaPSI from 28 HCI and UPS venues and filtered them. We then used the resulting 31 publications to perform backward snowball sampling to broaden our sample and mitigate selection bias. Our final sample included 80 publications.

4 Analysis Procedure

We identified relevant analysis dimensions to answer our research questions and then used a shared spreadsheet to collect relevant information and perform a hybrid thematic analysis.

4.1 Hybrid Thematic Analysis

Hybrid thematic analysis combines inductive and deductive methods to achieve both broad and in-depth insights [46]. Following a *deductive* (top-down) approach [27], we used existing categorizations from related work where applicable, particularly for scientific methods and tangible user interface classifications. The categorizations are detailed in Section 4.2. Three coders divided the sample and applied deductive coding. One author subsequently revised all assigned codes to check for plausibility and consistency. The coders met regularly to discuss and resolve disagreements.

For all other information, we used an *inductive* (bottom-up) method [18], where two authors independently created one codebook each using 20% of the publications (i.e., 16 publications). The authors met to discuss, compare their codes, and create a common codebook. One coder subsequently applied the resulting codebook to 80 publications. Any ambiguities and new themes were discussed with the other coder. As a result of the method we applied, we deliberately refrain from reporting measures of inter-rater agreement [84] for this exploratory work. Note that multiple codes from the same analysis categories could be assigned to a paper. Hence, the reported percentages do not add up to 100%.

4.2 Analysis Dimensions & Spreadsheet

Inspired by [40], we derived six analysis dimensions from our research questions to formalize and guide the process (see Figure 3).

To address RQ1, we examined how different TaPSI have been described or defined (i.e., their *terminology and definitions*), enabling us to derive a unifying definition of TaPSI and commonly used terminology. These findings can help researchers efficiently locate relevant literature and ensure their publications are both comprehensible and easily discoverable. We also describe the diversity of current TaPSI by specifying their use cases (i.e., *UPS Domains*). Our SoK also provides future researchers with fundamental insights on how to successfully research TaPSI. Hence, to answer RQ 2, we analyzed the *contributions* made by the publications in our sample, as well as the *methods* applied and indicate underexplored research approaches. For RQ3, we analyzed the extent and manner in which the TaPSI are *implemented*. Additionally, since the user interaction with TaPSI is fundamentally different from graphical user interfaces, we examined the inherent *opportunities and challenges*.

To ensure the collection of similarly broad information, we formalized which aspects of each publication are relevant to each analysis dimension as follows:

Terminology & Definitions: Terms used to describe the tangible interface, frequency of terminology (in the whole text), author-generated definitions of TaPSI

UPS Domain: UPS topic [40] (deductive), addressed specific UPS challenge (inductive), type of data that is being protected or managed (inductive), and targeted user group (inductive)

Contributions: Contribution type [134] (deductive), further themes on contributions (inductive), number of investigated TaPSI, and their technology readiness level [25] (deductive)

Methods: Number and type of formulated research objectives (inductive), research design [116] (deductive), number of studies, their location (deductive) and study methods [40] (deductive), number of participants

Implementation: Portability and form factor of TaPSI (inductive), materials used (inductive), means of interaction between user and interface (inductive), embodiment [47] (deductive), metaphor types [47] (deductive)

Opportunities & Challenges: Opportunities (inductive) and challenges (inductive) inherent to TaPSI

Three authors copied the relevant text segments from all 80 publications to a shared spreadsheet (see Supplementary Materials). One author then reviewed all publications again, adding additional segments. We used the resulting table for the next analysis steps.

4.3 Limitations

Our work is subject to selection bias and may have a limited sample representation. We combined a query-based sampling method with backward snowball sampling to mitigate such bias as much as possible. This allowed us to identify relevant publications that did not contain our search keywords or were published in venues we did not initially target. Our approach proved effective, as we were able to double our sample size through backward snowball sampling and our observations indicate that there are no search keywords more reliable than the ones we used for the initial search (see Sections 6.3 and 9.3.1). However, we decided against performing forward snowball sampling since some of the publications in our sample were cited by hundreds of other publications that we found to be largely not related to TaPSI (e.g., the over 1900 publications

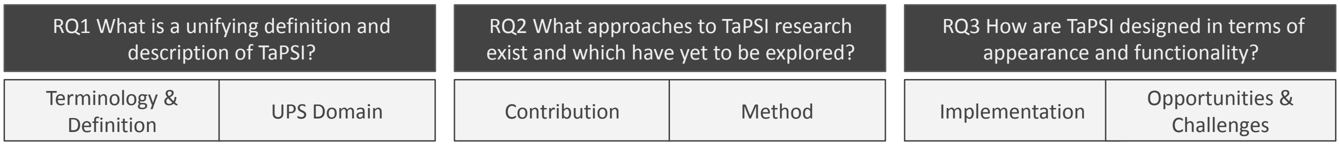


Figure 3: Our thematic analysis evolved around our three research questions. We further divided each research question into multiple analysis dimensions to collect more detailed information. In particular, we analyzed what TaPSI are, by identifying terminology used in the sample of publications and which usable privacy and security (UPS) domains they address. We also analyzed how TaPSI were investigated by reporting on contributions and applied methodologies. Furthermore, we investigated how TaPSI are implemented, as well as their inherent opportunities and challenges.

on the security of machine learning that cite [111]). As a result, the number of publications to review exceeded our available resources.

Like other qualitative research, the thematic analysis methods applied here might be affected by subjective interpretation. We took several steps to reduce subjectivity as much as possible (see Section 4.1). Nevertheless, despite our various efforts to achieve accurate insights, the frequencies reported in our work should be understood as trends rather than exact indicators.

Summary: Analysis Procedure

Using a shared spreadsheet, we applied *hybrid thematic analysis* to our sample [46]. Our findings were guided by knowledge from other systematic surveys, which we expanded, adapted, and refined to include the particular characteristics of TaPSI. Our analysis focused on the dimensions *UPS Domain, Terminology & Definitions, Contributions, Methods, Implementation, and Opportunities & Challenges.*

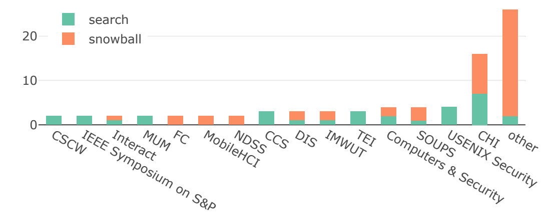
5 Description of the Sample

All 80 publications in our sample can be found in Appendix B.4. Figure 4 indicates when the publications were published and the most frequent publication venues (see also Appendix B.5).

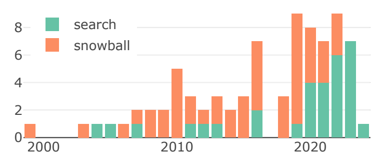
As mentioned before, we focused on publications from 1999 to March of 2024. Only one relevant paper was published from 1999 to 2002. In the following years, from 2003 to 2015, we found, on average, 2.23 relevant publications each year ($std = 1.17$, see Figure 4b). 67.5% of the analyzed publications were published from 2016 to 2024. Hence, from 2016 to 2023, an average of 6.63 works on TaPSI were published each year ($std = 3.38$). *This increase in interest in the research community during the last years indicates that TaPSI is a timely and growing topic.*

The 80 publications in our sample were published in 41 venues. However, for 26 of the venues, we only found one relevant publication each (see "other" in Figure 4a). 16 (20%) publications were presented at CHI. SOUPS[2], USENIX Security[3], and Computers & Security published 4 (5%) TaPSI publications each. We also found 3 publications in TEI[4], DIS[5], and CCS[6] publications. Therefore, *CHI was by far the most prominent venue for TaPSI publications.*

[2]Symposium on Usable Privacy and Security (SOUPS)
[3]USENIX Security Symposium
[4]International Conference on Tangible, Embedded, and Embodied Interaction (TEI)
[5]ACM Conference on Designing Interactive Systems (DIS)
[6]ACM Conference on Computer and Communications Security (CCS)



(a) Publications per venue



(b) Publications per year

Figure 4: We identified 31 publications in our initial search and 49 through additional snowball sampling. In subfigure (a), venues with only one publication – mostly found via snowball sampling – are grouped under "other." See Appendix B for a glossary of venue abbreviations and Appendix B.5 for a table of these results.

6 RQ 1 – What is a unifying definition and description of TaPSI?

6.1 Usable Privacy and Security (UPS) Domains

6.1.1 UPS Topics & Challenges. We adapted the categorization of *usable privacy and security* topics from Distler et al. [40]. In particular, we distinguish between "physical access control" and "digital access control" and added the categories "privacy indicators and warnings" and "security education and training" (see Table 2). In addition, we derived inductive codes to present insights into which UPS challenges TaPSI address.

Authentication. We found that 36.25% of the publications investigated authentication methods. These publications evaluated user perceptions of commercial physical authentication mechanisms (i.e., mostly authentication tokens, 16.35%), novel authentication methods involving tangible interactions (16.35%), or tactile-feedback-based secret entry methods that are not visually observable making them resistant to observation attacks (3.75%).

Privacy. Many publications described tangible interfaces for privacy-related topics, like privacy choice mechanisms (22.5%), privacy indicators and warnings (18.75%), or privacy-enhancing technologies (18.75%), often in conjunction. These publications mainly investigated challenges related to IoT privacy, either specific to microphones (mostly in smart speakers) (8.75%), cameras (5%), and location sensors (1.25%), or to multiple sensors (15%). In addition, 7.5% of the analyzed publications proposed privacy-enhancing technologies and/or choice mechanisms to address challenges resulting from the threat of shoulder surfing. Other presented privacy-enhancing technologies (3.75%) addressed unique challenges, such as remote collaboration and the impact of ubiquitous face-recognition or RFID tags on consumer products (1 publication each). Publications also investigated tangible privacy transparency mechanisms (4%) or privacy perceptions and behaviors (3.75%) usually in the context of IoT environments. One paper investigated peoples' privacy perceptions regarding tangible protections against observation (1.25%).

Access Control. Some publications described mechanisms for physical access control (8.75%) and addressed challenges around authentication mechanisms (3.75%) or tamper detection (3.75%). Tangible interfaces for digital access control (7.50%) supported users in setting up secure networks (3.75%), securely pairing devices (2.50%), or managing hardware crypto wallets (1.25%).

Other Security Topics. Seven publications presented tangible artifacts for security education and training (8.75%). Security perceptions, attitudes, and behaviors (8.75%) were investigated related to commercial authentication mechanisms (7.50%) or the verification of vaccination certificates (1.25%). Proposed security indicators and warnings (6.25%) were investigated to enhance users privacy in the IoT (3.75%), online privacy (1.25%), or protect them against scam calls (i.e., vishing, 1.25%). The only UPS topics from Distler et al. [40] that we could not assign to any publication were *security for admins and developers*, *encryption*, and *social engineering*.

6.1.2 Data Types Managed or Protected Through TaPSI. The tangible interfaces in our sample addressed a wide range of data management and protection challenges (see Table 2). Notably, 35% of the publications examined interfaces not tailored to any specific data type. Among those that did, 15% focused on safeguarding audio data (e.g., disabling smart speakers), while 13.75% targeted video or photographic data (e.g., camera covers). Interfaces dealing with location or presence data were discussed in 10% of the sample. Financial information was specifically protected in 8.75% of the studies, and 7.5% focused on managing data collected by IoT devices, with another 7.5% dedicated to secure network establishment and device pairing. Additionally, some interfaces managed authentication secrets (5%, such as passwords), screen-displayed private data (3.75%), or personal identity information (3.75%). Finally, 2.5% proposed TaPSI to ensure hardware integrity, and 5% addressed the protection or management of other data types.

6.1.3 Targeted User Groups. Most publications in our sample (82.5%) did not target specific user groups. However, some TaPSI were specifically designed for non-expert end users (10%), employees in general (7.5%), students (5%), developers/researchers (5%), expert end users (e.g., security experts, 3.75%), (shared-)office workers (3.75%), or older adults (2.5%).

6.2 Terminology & Definitions

6.2.1 Used Terminology. Overall, in 50% of the publications, authors gave their interface a specific name. Some examples of this are: TaPS Widgets [94], Posit [71], ICEbox [137], Play2Prepare [54], 3D-Auth [82], or PriKey [37]. Other terms used to refer to the presented tangible interfaces were: *"device," "prototype," "token," "game," "artefact"/"artifact," "indicator," "interface," "probe," "control," "object," "phidget," "tag,"* or *"tool"*. The investigated interfaces were also described as *"physical," "tangible," "haptic," "hardware,"* or *"wearable"*. We do not report term frequencies here, as a more precise automated term frequency analysis follows.

6.2.2 Term Frequency Analysis. For more insights into the terminology used in TaPSI publications, we analyzed the frequencies with which terms appeared in the publications' main parts (i.e., excl. references). For this, we established the following search terms:

- The above mentioned descriptive terms *"physical," "tangible," "haptic," "hardware,"* or *"wearable,"* as well as *"graspable,"* since we used this term in our initial search.
- All terms we identified that refer to the investigated TaPSI (i.e., *"device," "prototype," "token," "game," "artefact"/"artifact," "indicator," "interface," "probe," "control," "object," "phidget," "tag,"* or *"tool"*), as well as similar terms listed by Ullmer and Ishii [121] (i.e., *"prop," "phicon,"* and *"container"*).
- Further terms related to the usable privacy and security topics our sample addressed (see Table 2), like *"security," "privacy," "choice," "authentication," "warning," "education," "training," "access,"* or *"mechanism."*

We used a Python script to count how many publications included each keyword independently and all combinations of terms separated by whitespaces. Table 3 shows term frequencies.

One-Word Terms. More than 75% of the publications used the terms *"security"* (88.75%), *"device"* (87.5%), and *"physical"* (85%). Moreover, most (i.e., $>$ 50%) included the terms *"mechanism"* (72.5%), *"privacy"* (72.5%), *"interface"* (68.75%), *"control"* (68.75%), *"hardware"* (63.75%), *"access"* (58.75%), *"choice"* (57.5%), *"authentication"* (56.25%) and *"tool"* (51.25%). All other terms were mentioned in less than half of the publications (see Table 3a).

Multi-Word Terms. Out of the combined terms, *"physical security"* was the most frequently used in our sample (22.5%), followed by *"privacy control"* (22.5%), *"wearable device"* (15%), and *"access control"* (16.25%, see Table 3b). *"Authentication token," "physical access,"* and *"physical device"* were found in 15% of the publications. Some used the terms *"security mechanism"* (13.75%%), *"authentication mechanism"* (12.5%%), *"physical object"* (12.5%), and *"tangible privacy"* (11.25%). *"Hardware token," "physical control"* and *"physical privacy"* were all mentioned in 10% of our sample. No combination of three terms was found in more than 10% of our sample.

6.2.3 Related Definitions. As mentioned before, we could not find an existing definition of TaPSI. However, we identified some related definitions both inside our sample and outside of it.

Definitions of TaPSI In Our Sample. We first collected author-generated definitions of types of TaPSI from our sample.

Table 2: We analyzed the UPS domains of each of the 80 publications on TaPSI. We, therefore distinguish between the UPS topic they address [40], the type of the data that is being managed or protected by the different TaPSI, and the user group their design targets. We use bold font to highlight the largest portions of publications.

UPS Topics [40]		Managed or Protected Data		Targeted User Groups	
authentication	**36.25%**	**general data/not specified**	**35.00%**	**general/not specified**	**82.50%**
privacy choice mechanism	22.50%	audio	15.00%	non-expert end-users	10.00%
privacy-enhancing technologies	18.75%	video/photo	13.75%	employees in general	7.50%
privacy indicators and warning	18.75%	presence/location	10.00%	students	5.00%
security perceptions, attitudes, and behaviors	8.75%	financial	8.75%	developers/researcher	5.00%
security education and training	8.75%	general IoT-collected data	7.50%	expert end-user	3.75%
physical access control	8.75%	network connection/pairing	7.50%	(shared) office workers	3.75%
digital access control	7.50%	authentication secret	5.00%	older persons	2.50%
security indicators and warnings	6.25%	screen content	3.75%		
privacy transparency mechanism	5.00%	identity	3.75%		
privacy perceptions, attitudes, and behaviors	3.75%	integrity of hardware	2.50%		
		other	5.00%		

Table 3: We analyzed how many publications contained terms describing TaPSI. This includes descriptive terms, synonyms for *"tangible interface"* and privacy- or security-related terms. We did not include the publications' reference lists for this search. As we aim to identify commonly used terms, we only report on terms that appeared in at least 10% of the sample. The most frequently occurring terms are bolded.

(a) one-word

term	Frequency
security	**88.75%**
device	87.50%
physical	85.00%
mechanism	72.50%
privacy	72.50%
interface	68.75%
control	68.75%
hardware	63.75%
access	58.75%
choice	57.50%
authentication	56.25%
tool	51.25%

(b) multi-word

term	Frequency
physical security	**22.50%**
privacy control	21.25%
wearable device	16.25%
access control	16.25%
authentication token	15.00%
physical access	15.00%
physical device	15.00%

Tangible Privacy Ahmad et al. *"define 'tangible privacy' mechanisms as those privacy control and feedback mechanisms that are 'tangible', i.e., manipulated or perceived by touch, and of 'high assurance', i.e., they provide clear confidence and certainty of privacy to observers"* [7, p. 4].

Locators Song et al. *"define locators as feedback mechanisms that can be used to physically find IoT devices"* [113, p. 2].

Physical Authentication Devices (PADs) / Security Keys Nanda et al. define PADs as *"small physical tokens without a display screen that can be inserted into a USB port or kept in proximity to primary authentication devices, such as laptops or smartphones, for user login"* [95, p. 2]

Other Definitions of Similar Terms.

Physical Security Blythe et al. describe physical security as *"[s]trategies to physically protect infrastructures, information and information resources"* [17]

Physical Privacy Burgoon defined physical privacy as *"the degree to which one is physically inaccessible to others"* [19, p. 211]

6.3 Answering RQ1

To answer the question *"What is a unifying definition and description of TaPSI?"* (RQ1) we analyzed the UPS topics addressed in our sample, the used terminology, and presented definitions.

We found that TaPSI can be applied to a large variety of UPS domains. Most of the analyzed publications investigated *authentication*, *privacy*, and *access control*.

The terms *"security"* and *"privacy"* could be found in most publications. *"Tangible"* was only used in 36.25% of the publications. However, we found similar terms like *"physical"* and *"hardware"* in most works. Moreover, the term *"interface"* and similar terms, such as *"device," "mechanism,"* or *"control"* and *"tool"* were amongst the most frequently used terms. None of the analyzed combined terms was found in > 22.5% of the publications. Moreover, the most frequently used composed term *"physical security"*, also led to many false positives in our initial search. This is because the terms *"physical security"* and *"physical privacy"* are widely used but with meanings that differ from the description of TaPSI.

Our findings indicate a need to formalize and standardize terminology. We, thus, derive the term tangible privacy and security interfaces (TaPSI) and define it in the following Section (6.4).

6.4 Defining TaPSI

6.4.1 The Term "Tangible Privacy and Security Interfaces" (TaPSI). The publications we analyzed lie at the intersection of research on *usable privacy and security* and *tangible interfaces*. Thus, a combined term is most suited to adequately cover both aspects. The most frequently identified combined term was *"physical security."* Yet, as mentioned before, we observed that searching for *"physical security"* resulted in many results that do not fit into the scope of this survey.

We propose the term *"tangible privacy and security interfaces"*. It aligns well with the established terminology of *"tangible interfaces"* [67, 121] and the term *"tangible privacy"* which describes tangible interfaces for privacy management (i.e., control and awareness) in IoT environments [7, 89]. Moreover, *"tangible security"* was only found in 2.72% of the 1021 results from our initial search and 2.5% of the publications in our final sample. Thus, it has not been widely used in the area of UPS. Hence, we assume we are not creating conflicts with existing definitions.

6.4.2 Definition of TaPSI. TaPSI are described as being *"physical"* [95, 113] *"control and feedback mechanisms"* [7, p. 4] or interfaces that can be *"manipulated or perceived by touch"* [7, p. 4]. Accordingly, they are referred to as *interfaces for privacy or security management* [60, 71, 89, 137]. They can *"protect infrastructures, information and information resources"* [17], serve as *"smart physical barriers that protect against intrusive sensing"* [43, p. 3] or as an *"authentication factor (i.e., something the user has)"* [95, p. 2]. Hence, TaPSI *provide protection.* TaPSI are also *"of 'high assurance', i.e., they provide clear confidence and certainty"* [7, p. 4] and provide *"feedback for privacy awareness through visual cues, sound, haptics, or smell"* [89, p. 2] by *"appropriately alerting users about personal data privacy breaches"* [87, p. 2422]. Moreover, TaPSI can *"increase people's awareness of computer security needs and challenges, so that they can be more informed technology builders and consumers"* [38, p. 916] by *"educat[ing their users] on how to think as an attacker and then learn how to deter attacks"* [59, p. 3]. They, thus, impact *users' understanding of privacy and security-related concepts.*

Definition. Based on these descriptions, we define Tangible Privacy and Security Interfaces (TaPSI) *as "tangibles" – which means they exist in the physical world and can be manipulated or perceived by touch and potentially other senses – that help users manage, protect, and understand information privacy and/or security.* TaPSI, thus, describe the intersection between the research fields tangible user interfaces and usable privacy and security.

Summary: RQ1 – What is a unifying definition and description of TaPSI?

Researchers have proposed TaPSI to solve a broad variety of UPS problems. However, our analysis of the used terminology and presented definitions underline the need to formalize and standardize terminology in this research field. To close this gap, we propose for future researchers to use the term *"tangible privacy and security interfaces" (TaPSI)*, which we define *as "tangibles" – which means they exist in the physical world and can be manipulated or perceived by touch and potentially other senses – that help users manage, protect, and understand information privacy and/or security.*

7 RQ 2 – What approaches to TaPSI research exist and which have yet to be explored?

To understand how researchers investigate TaPSI, we analyzed (a) their works' contributions and (b) the applied research methods.

7.1 Contributions

7.1.1 Types of Contributions. We first applied the categorization of contribution types by Wobbrock and Kientz [134] to our sample (see Table 4). Most publications presented an artifact (72.5%) or empirically evaluated how people use an artifact (66.25%). They also made theoretical contributions (3.75%) and included empirical studies investigating people (8.75%). Our sample included one survey (1.25%) and one methodological contribution (1.25%).

Next, we conducted an inductive thematic analysis to gain detailed insights into the contributions of our sample. We found that *artifact contributions* included the development of novel tangible artifacts (55%), software complementing a tangible interface (22.5%), implementing and using a tangible interface to collect data for a subsequent technical evaluation (13.75%), or comparing developed software and tangible artifacts (5%). *Empirical studies that investigated how people use an artifact* either focused on a novel tangible interface presented in the same publication or commercial products, which included tangible interfaces provided to participants (7.5%) or owned by participants (6.25%). Some publications also compared perceptions of software and tangible products owned by them (3.75%). Moreover, the research in our sample also made *theoretical contributions*, such as implications for future designs (20%), design requirements for the design of the presented artifacts (16.25%), and design frameworks (2.5%).

7.1.2 Investigated Tangible Artifacts. Most publications either presented novel artifacts or investigated their use. Hence, all but one publication (98.75%) in our sample presented tangible interfaces. The number of TaPSI investigated in each publication ranges from 1 to 7 ($mean$ = 3.14%, std = 2.41%, see Table 4).

Their technology readiness levels (TRL) varied from TRL1 (define basic properties) to TRL9 (product on the market, see Table 4). The most frequent TRLs of the presented tangible interfaces were TRL5 (pre-prototype tested in lab, 35%), TRL9 (product on market, 26.25%), TRL3 (proof of concept, 11.25%), TRL4 (pre-prototype, 11.25%) and TRL6 (prototype tested in relevant environment, 10%). TRL1 and TRL8 were assigned to less than 10% of the publications.

7.2 Research Methods

To describe how TaPSI are investigated, we extracted the research methods used in the publications, see Table 5.

7.2.1 Research Objectives. We analyzed the publications for their research designs distinguishing between *descriptive, correlational, and experimental* research [116]. *Descriptive research* aims to capture a current situation (i.e., the current state of affairs). *Correlational research* analyzes how two or more variables relate to each other. *Experimental research* identifies the causal effects of experimental interventions on a dependent variable [116]. Most analyzed publications were descriptive (76.25%), 41.25% were experimental, and only one was correlational (1.25%). We also observed that 63.75% of the publications did not mention specific research questions, hypotheses, or goals. 13.75% contained research questions (2-7), 8.75% research goals (1-4), 7.5% hypotheses (1-6), and 6.25% freely formulated guiding questions (1-7).

7.2.2 Empirical Studies. 91.25% of the 80 publications conducted at least one empirical study, which involved human subjects (75%), technical evaluations (2.5%), or combinations of both (13.75%). On average, they reported on 1.75 (std = 1.33, range: 1-7) studies per publication. The number of participants for human subjects studies ranged from 2 to 50, 000. Only 11 studies had more than 100 human subjects. The remaining 106 presented studies had 19.82 participants on average (std = 18.66). Studies were frequently conducted in the lab (65%). However, researchers also performed studies online (21.25%) or in the wild (17.5%). We analyzed our sample for the study methods described in [40], as well as *"hands-on task"* (i.e., the

Table 4: We analyzed how the analyzed publications contribute to usable privacy and security research. For this, we distinguished the types of each publication's contributions [134], the number of tangible interfaces they present, and their technology readiness levels [25]. The largest percentages of publications per column are bolded.

Contribution Type [134]		Tangibles		Technology Readiness Level (TRL) [25] of Tangible	
Artifact	**72.50%**	0	1.25%	TRL1 Define basic properties	5.00%
Empirical: study about how people use an artifact	66.25%	**1**	**71.25%**	TRL3 Proof of concept	11.25%
Theroretical	30.00%	2	7.50%	TRL4 Pre-prototype	11.25%
Empirical: study about people	8.75%	3	13.75%	**TRL5 Pre-prototype tested in lab**	**35.00%**
Survey	1.25%	4	2.50%	TRL6 Prototype tested in relevant environment	10.00%
Methodological	1.25%	5	1.25%	TRL8 Pre-serial manufacturing	5.00%
		7	2.50%	TRL9 Product on market	26.25%

Table 5: We extracted the methods used in our sample and the underlying research objectives. Hence, we analyzed the research design [116] of each publication, how they formulated their research objectives in the text, the applied study method, and where the studies were conducted. The largest portions of publication per column are bolded.

(a) Research Objectives

Research Design [116]		Objective Types	
descriptive	**76.25%**	**none**	**63.75%**
experimental	41.25%	research question	13.75%
correlational	1.26%	research goal	8.75%
		hypothesis	7.50%
		guiding question	6.25%

(b) Conducted Studies

Study Method				Location	
hands-on task	**62.50%**	think-aloud	8.75%	**lab**	**65.00%**
survey	56.25%	diary study	6.25%	online	21.25%
interview	31.25%	storyboard study	3.75%	in-the-wild	17.50%
log analysis	22.50%	workshop	2.50%		
technical eval.	17.50%	observation study	2.50%		
focus group	10.00%	co-creation	1.25%		

participants had to use the investigated artifact), *"technical evaluation"*, *"think-aloud "*, and *"storyboard study"*. Most publications described studies involving hands-on tasks (62.5%) and surveys (56.25%). Many publications also conducted interviews (31.25%), analyzed logged data (22.5%), performed a technical evaluation (17.5%) or focus groups (10%). Some used think-aloud tasks (8.75%), diaries (6.25%), storyboards (3.75%), observation (2.5%), workshops (2.5%), and co-creation methods (1.25%).

7.3 Answering RQ2

We analyzed our sample's contributions and methods to answer the question: *"What approaches to TaPSI research exist and which have yet to be explored?"* (RQ2).

Most publications provided *artifact, empirical, and theoretical contributions.* They frequently described the design and implementation of one or multiple TaPSI, the conduction of an empirical study to inform the design of the TaPSI or evaluate it, and optionally theoretical insights. While most analyzed publications combined artifact and empirical contributions, some presented TaPSI and no empirical study (8.75%) or only an empirical contribution and no implementation of an artifact (23.75%). The latter usually involved the evaluation of commercially available TaPSI (21.25%) or a visual representation of an envisioned TaPSI (2.5%) [6, 88].

Most publications mentioned empirical studies including hands-on tasks (62.5%) and surveys (56.25%). Interviews (31.25%) and log analysis (22.5%) were also frequently applied study methods. Interestingly, most of the studies used a *descriptive design*, i.e., they did not compare multiple conditions or variables against each other.

Only 21.25% of the reviewed publications stated formal research questions or hypotheses, highlighting again the need for formalization to support more rigorous research approaches in the future.

Summary: RQ2 – What approaches to TaPSI research exist and which have yet to be explored?

Most publications provided a combination of artifact and empirical contributions and usually focused on a single interface with varying technology readiness levels. For many of the proposed TaPSI, there are no comparative insights. For example, it frequently remains unclear how users perceive them compared to digital alternatives. Moreover, many publications did not formulate specific research objectives hinting at a lack of formalization.

8 RQ3 – How are TaPSI designed in terms of appearance and functionality?

8.1 Implementation

As mentioned before, all but one of the analyzed publications examined at least one tangible interface. These interfaces were either developed by the authors or commercial products. This section describes their appearance, functionalities, and underlying metaphors. To extract the following findings, we applied Fishkin's taxonomy of tangible user interfaces (TUIs) [47] (deductive) as well as inductive thematic analysis. Fishkin proposes distinguishing TUIs based on the dimensions *embodiment* and *metaphor.*

8.1.1 Appearance. We examined TaPSI' appearance by analyzing the form factors and materials of the interfaces in our sample.

Form Factor. 33.75% of the publications investigated freestanding TaPSI. In particular, they were presented as tabletop interfaces (20%), tabletop games (10%), or other freestanding interfaces (5%). 31.25% were portable. As such, they could be transported in pockets

Table 6: We analyzed how TaPSI are implemented by describing their appearance (i.e., form factor and material) and interaction functionalities (i.e., their embodiment [47], user input, and system output to the user). The largest percentages are bolded.

(a) Appearance

Form Factor		Material	
freestanding	**33.75%**	**electronics**	**48.75%**
portable	31.25%	plastic	26.25%
attached or integrated	30.00%	paper/ cardboard	20.00%
wearable	6.25%	foil	3.75%
		wood	3.75%
		fabric	2.50%

(b) Interaction Functionalities

Embodiment [47]		User Input				Output to User	
full	**26.25%**	**push**	**16.25%**	approximate	12.50%	movement	8.75%
nearby	22.50%	**touch**	**16.25%**	attach or insert	11.25%	vibration	5.00%
distant	5.00%	move	13.75%	(dis)connect	8.75%	**screen**	**40.00%**
		rotate	6.25%	point	5.00%	light	13.75%
		hold	2.50%	cover	3.75%	sound	5.00%
		bend	1.25%	voice	2.50%	other visual	2.50%
		destroy	1.25%	digital	2.50%		

(20%, e.g., USB-Sticks, PDAs, or key fobs), bags (6.25%, larger than pocket format), or in a wallet (6.25%, (smart)cards or a sheet of paper). Moreover, 30% of the interfaces were attached or integrated into other devices (20%), furniture (6.25%), or non-tech objects (5%). Some of the presented interfaces were wearables (6.25%), like armbands (3.75%) or enhanced glasses (2.5%).

Material. The tangible interfaces were composed of different materials. We focus on the materials of novel interfaces developed by the authors of the publications rather than commercial products. We made this decision primarily to inspire future researchers in their choice of materials and because the materials of commercial products were often not specified in the publications. 48.75% of our sample developed a tangible interface containing electronics (e.g., sensors, actuators, wiring, microcontrollers, or power supplies). 26.25% included plastics (i.e., sturdy or flexible) and 20% were (partly) made of paper or cardboard. Some interfaces used different kinds of foils (3.75%, e.g., light-scattering foil [94], PDLC film [43], or copper tape [36]), wood (3.75%) or fabric (2.5%).

8.1.2 Functionalities. To describe the functionalities of the TaPSI, we first distinguished between active and passive prototypes (i.e., whether they require a power source). We then determined their embodiment and analyzed the supported interactions distinguishing between user input and system output functionalities.

Active vs. Passive. Most TaPSI presented in our sample were active (78.75%). Hence, they either contained a battery or needed to be connected to a power source to function (e.g., to wall sockets or USB ports on a PC). However, a subset (36.25%) of the analyzed publications (also) investigated passive TaPSI. Passive TaPSI included tabletop games, physical covers/seals, RFID or NFC-based interfaces, or conductive structures.

Embodiment. Embodiment of a TUI describes the cognitive distance between the user's input performed as a tangible manipulation and the interface's tangible output [47]. The embodiment of a TUI can be *full* (i.e., input and output in one device), *nearby* (i.e., the output takes place near the manipulated input device), *environmental* (i.e., the output is around the user, e.g., by changing ambient lighting), or *distant* (i.e., the output is *"over there"*, e.g., on another screen) [47]. 26.25% of the publications described TaPSI with full embodiment and 22.5% with a nearby embodiment, which indicates high levels of *"tangibility"* [47]. The embodiment of only 5% of the interfaces investigated was distant (i.e., low level of tangibility). Yet, this categorization did not apply to all interfaces in our sample for various reasons. In particular, 20% of the works presented an interface where the output was not directly observable by the user, 17.5% did not support (tangible) user input, and 11.25% were purely analog (e.g., tabletop games). In addition, in 7.5% of our sample, the user interactions with the TaPSI were not described in sufficient detail to identify their embodiment.

User Input. Most TaPSI supported direct tangible manipulation as user input, such as touching (16.25%), pushing (16.35%), moving (13.75%), rotating (6.25%), holding (2.5%), bending (1.25%) or destroying (1.25%) (parts of) them. Other tangible input modalities involved the arrangement of two artifacts by approximating them (12.5%), attaching or inserting them (11.25%), (dis)connecting them (8.75%), pointing them towards each other (5%), or covering them (3.75%). Few interfaces provided non-tangible user input, such as voice (2.5%), and digital controls (2.5%).

System Output. Most interfaces had non-tangible output functionalities, such as screens (40.0%), lights (13.75%), sound (5%), or other visual output (2.5%). However, some interfaces provided tangible output represented through movement (8.75%) or vibration (5%) of the interface or parts of it.

8.1.3 Metaphor. Fishkin's taxonomy [47] distinguishes TUIs based on the type of metaphor they apply. Interfaces that apply no metaphor are grouped into the *"none"* category. The category *"noun"* is applied if an interface's shape, appearance, or sound is based on a metaphor. *"Verb"* refers to analogies in the interactions. Interfaces can also make analogies to the interaction and the appearance/sound, described as *"noun and verb"* metaphors. The highest level of tangibility in the metaphor dimension *"full"* refers to interfaces where the virtual information and tangible representation are the same (i.e., really direct manipulation [48]).

Almost half of the publications in our sample presented TaPSI with no metaphor (47.5%). Others used primarily noun (25%) or verb metaphors (15%). 7.5% presented TaPSI with noun and verb metaphors. No interface could be assigned to the "full" category.

8.2 Opportunities & Challenges

Unlike digital interfaces, tangible interfaces provide a physical interaction layer that can support users but also introduce new challenges. We explored the resulting opportunities and challenges, to describe the potential of TaPSI.

8.2.1 Opportunities.

Intuitiveness Rooted in Pre-Existing Knowledge of the Physical World. *"A technical system is intuitively usable if the users' unconscious application of pre-existing knowledge leads to effective interaction"* [64, p. 128]. TaPSI are physical objects which leverage users' pre-existing knowledge and understanding of the physical world [7, 64, 89]. This results in a multitude of inherent opportunities. Authors in our sample argue that TaPSI support natural and intuitive interactions (25%) because users can interact with them in the same way they interact with any other object [64]. Therefore, TaPSI presumably offer a low threshold to get started, which can be particularly beneficial for inexperienced or novice users. Correspondingly, 16.25% of the analyzed works highlighted that TaPSI are inherently inclusive to diverse user groups.

Our sample also describes that physicalization supports the communication of clear and unambiguous information (13.75%). For example, users intuitively understand that a camera that is covered or pointed away, will not be able to record them [70]. This is particularly important for security and privacy interfaces, as it promotes the trust in the interface and self-efficacy necessary to support secure behavior in users [108]. Since tangible interfaces are part of the physical world, they can also be observed by anyone in their environment (e.g. by users, but also by potential bystanders) [132, 133]. We found that they, therefore, offer the opportunity to generate awareness about risks and adequate protective measures (12.5%).

TaPSI can leverage users' pre-existing knowledge through applying metaphors (7.5%). This can further increase intuitiveness [47, 89] and support reflection [119]. Going further, some publications in our sample suggested tangible interfaces that simulate real-world scenarios (2.5%) to provide a *"sandbox in which [users] can experiment with security risks, learn about decision-making and its consequences, and reflect on their own perception of security"* [49, p. 521].

TaPSI can also leverage their position in the physical environment (7.5%). For example, depending on the position of an interface, it can be perceived as peripheral or in the center of attention [55]. Moreover, placing TaPSI in a meaningful environment could increase usability [36, 106], encourage the adoption of protective behaviors [70, 102] or convey social meaning (i.e., it is okay to glance at something that is openly situated in a shared environment) [71].

Direct Ad-Hoc Interactions. The publications in our sample discuss that TaPSI support easy (18.75%) or quick (12.5%) usage and can allow grasping important information at a glance (3.75%). This is potentially rooted in the fact that most tangible interfaces are single-purpose devices. Hence, they are designed specifically for their intended use only. In contrast, digital mechanisms are usually installed on multi-purpose devices. Accordingly, with TaPSI users do not need to navigate different menus to find a specific functionality. Instead, TaPSI support *really direct ad hoc interaction* [48, 89].

To offer direct manipulation, users need to be able to immediately observe the effects of their actions [48, 112]. Hence, several works in our sample specifically highlight the need for real-time control (10%) or information features (5%) of TaPSI. They can further support directness by being *ready-at-hand* [89]. Correspondingly, some of the analyzed publications suggested mobile (8.75%), on-body (2.5%) or prominent placements of TaPSI (3.75%, e.g., on walls [137], in hallways [132] or on the packaging of devices [45]).

Support Cognitive Processes, Social Settings and Elicit Emotions. TaPSI can *"offer users a simple mental model of how it works and how to use it, which should help to improve security in practice"* [60, p. 999]. Hence, the authors of the analyzed works argue that TaPSI can support the user's understanding of protective measures (11.25%), as their behavior can be observed and contrasted with pre-existing knowledge of the physical world. This contrasts with digital privacy and security interfaces, which often operate opaquely to end users. As physical entities, TaPSI make *"abstract concepts more tangible and illustrative"* [119, p. 2] (7.5%), trigger reflection (6.25%), support decision making (2.5%), and leverage motor memory, making (potentially secret) interactions easier to remember (6.25%).

We also found that TaPSI can elicit emotions in their users. Users find them engaging (12.5%) and feel compelled to explore them through casual interaction (5%). TaPSI can also trigger creativity (2.5%) and trust in the protection provided through the interface (11.25%). In particular, some works in our sample argue that TaPSI can provide easy-to-verify assurance of the provided protection (11.25%), support users' sense of being in control (5%), and do not rely on untrusted software controls (3.75%). The positive impact of TaPSI on cognition and users' emotions can be even enhanced through customization, since this allows users to *"engage critically and personally with the medium, exercising a level of experimentation beyond that of typical digital [interfaces]"* [53, p. 3] (8.75%).

Consistent with research on tangible user interfaces, we found that TaPSI can positively impact social settings [78, 104]. In particular, the presence of such an interface can trigger discussion on security and privacy-related topics (12.5%), foster collaboration between users (7.5%), and bring people together (2.5%).

Save Resources and Forster Existing Setups. TaPSI also offer the opportunity to augment existing devices or non-tech objects to provide novel functionalities (15%), centralize the management of functionalities of devices (7.5%), or allow user interaction with devices, that do not have user interfaces (2.5%). They also often require few resources from their users, particularly in terms of time, effort, and dependency on other devices or objects (21.25%).

Security: Physical Separation, Presence and Barriers. TaPSI provide inherent opportunities when it comes to protecting data. In particular, while TaPSI might interact with other technological devices, they are frequently physically separate, which means that attacks might have to compromise both devices in order to be successful (16.25%). For example, Do et al's [43] smart webcam will cover a laptop's webcam, even if it was hacked. This is particularly beneficial if the tangible interfaces are also completely offline and, therefore, not susceptible to attacks via the internet (3.75%).

Furthermore, TaPSI can enhance security by requiring a user's physical presence for sensitive tasks (i.e., proximity or touch, 10%), making them again less susceptible to online attacks. TaPSI are also often single-purpose devices. Hence, it is much easier for developers to implement by-design data minimization (8.75%). Moreover, they can serve as physical barriers that protect sensitive information (7.5%) or recognize unauthorized users by measuring their tangible interactions and comparing them to the legitimate user's behavior patterns (i.e., behavioral biometrics, 7.5%)

Subtle Interactions. Security and privacy-related tasks are often perceived as interrupting or socially awkward [5, 37, 131, 138]. For example, cookie banners get in the way of users looking for information on a website and covering one's PIN entry while paying in a store can make other people feel distrusted. We found that TaPSI have the potential to be less interrupting and reduce social impacts, as they support subtle interactions (17.5%) and leverage multiple human senses (13.75%, i.e., vision, touch, audition). This subtleness makes interactions hard for bystanders to observe, increasing the users' privacy. Hence, the works in our sample leveraged this by supporting interactions that are non-obtrusive (i.e., peripheral [26, 89], 10%), invisible to others (6.25%), and inconspicuous (2.5%). Two works (2.5%) also discuss how TaPSI can change from being subtle to salient by making bigger or faster changes to the visual appearance, movement, and sound of the tangible [26, 55].

8.2.2 Challenges.

Limited Versatility and Scalability. A challenge of TaPSI is their limited versatility, as they are frequently designed for one very specific purpose [89]. Hence, 10% of the analyzed publications mentioned that the investigated TaPSI relies on specific additional hardware to work properly, and 7.5% discussed environmental factors that lead to malfunctions. The versatility of the TaPSI was also negatively affected by its incompatibility with other software (3.75%) and its insufficient adaptation to different usage scenarios (2.5%). Moreover, TaPSI can become quickly outdated (1.25%), as some of their functionalities can be hardware-based, limiting software updates' applicability. Accordingly, TaPSI can create physical clutter [89]. This makes users worry about carrying them (11.25%) and impacts their scalability (6.25%). Similarly, they can obstruct users when performing other tasks (2.5%).

No One-Fits-All Design. We found that designing TaPSI in a way that satisfies the expectations of users is very challenging. *"The dimensions of the [TaPSI] should be balanced on three levels: with the context, the user, and within the design itself"* [122, p. 12]. Hence, some TaPSI were perceived as too bulky (7.5%) and others as too small (1.25%). Small dimensions can improve portability but can also make TaPSI more prone to being misplaced and affect ergonomics [103, 122]. Larger dimensions can make it difficult to use TaPSI in environments where the space is limited and can hinder portability or usability [20, 37, 43]. Moreover, the publications in our sample reported that users might have varying preferences for the appearance of TaPSI (6.25%) and that aesthetics could hinder adoption (3.75%). Two works also mentioned that their participants were worried about breaking TaPSI (2.5%). Another challenge for TaPSI is that specific design choices limit how users interact with them (13.75%), which can collide with users' expectations [94]. Some publications also observed that TaPSI that incorporate a battery are limited in their performance (3.75%).

Inconvenient & Awkward Interaction. Using TaPSI can be tedious, especially if it requires frequently repeated tangible interactions [70, 89, 106]. In particular, the analyzed publications reported challenges such as taking too much time (16.25%) and too much effort (10%). In particular, when users had to consult usage instructions (5%). Some publications also mention that interacting with TaPSI could be inconvenient or disturbing for other nearby people (7.5%). For example, bystanders could think that the user is hiding something [71] or takes control away from them [7, 22, 37]. They could also be disturbed through the user's unexpected movements [20, 69]. Moreover, interaction with TaPSI was sometimes reported as not engaging (enough) (6.25%), difficult to remember (3.75%), and interrupting (2.5%). Purchasing and implementing TaPSI can also be costly (6.25%), especially if provided for larger groups (e.g., all employees from a company [74, 117]). TaPSI can provide easy-to-understand physical protections. However, users may still misunderstand how to use them depending on their specific design. Hence, the analyzed publications reported that users found functionalities of TaPSI difficult to understand (12.5%) and performed usage errors due to misunderstandings (8.75%). 6.25% mentioned that users had expectations not met by the investigated interface. Users in 3.75% of the publications in our sample did perceive no value in using token-based authentication TaPSI.

Security: Physical Access & Observability. TaPSI also face inherent security challenges. They could be lost, forgotten, or stolen, potentially preventing their users from using them or granting access to attackers (12.5%). Attackers could also observe the user's tangible input (11.25%). TaPSI might also put users' security at risk if misused (7.5%) or if they malfunction (5%). They can also be overlooked (5%) or occluded (2.5%). Few publications observed mistrust in TaPSI. In particular, participants did not trust LED indicators (2.5%) or would not use TaPSI for high-security use cases (1.25%). Some works discussed that designing TaPSI with intuitively verifiable protection features can be challenging (3.75%). For example, physical buttons should *"have reliable disconnects, in a way that is verifiable by either users or other experts"* [6, p. 20]. Instead of using LED indicators, users *"may need a more tangible mechanism, such as opaque covers or physical disconnects"* [7, p. 19]. This is because users *"may not, themselves, know how the circuitry works"* [41, p. 2483]. Interestingly, one work also discussed that users trusting the TaPSI too much could lead to more risky behavior [6] (1.25%).

Challenges When Evaluating TaPSI. 18.75% of the works mentioned that they used simplified TaPSI prototypes which impacted the validity of their results. 11.25% observed malfunctions of their prototypes during the evaluation process and 5% highlighted that specific design choices limit the generalizability of their findings.

8.3 Answering RQ3

We analyzed TaPSI implementations and the opportunities and challenges identified by researchers to answer the question: *"How are TaPSI designed in terms of appearance and functionality?"* (RQ3).

The TaPSI in our sample had diverse form factors affecting portability and size. They were integrated into or attached to devices, furniture, or non-tech objects or were freestanding, portable, and wearable. Most featured electronics, plastics, or paper/cardboard. They supported input through direct tangible interaction and arrangement of multiple objects or non-tangible voice or digital input. The interfaces' outputs were tangible, visual, and auditory. About half of the analyzed works presented TaPSI applying a metaphor.

The publications in our sample show that TaPSI inherently offer an intuitiveness rooted in users' pre-existing knowledge, support cognition, leverage social settings, and elicit emotions. They also allow easy and quick direct ad hoc interactions to augment existing environments with limited resources and leverage subtleness. Furthermore, they provide security benefits rooted in their physicality. However, they also come with inherent challenges, like their limited versatility and scalability or the difficulty of designing TaPSI that satisfy requirements from different stakeholders and use cases. Interacting with them can also be inconvenient or socially awkward, is prone to observation attacks, and requires physical access.

Summary: RQ3 – How are TaPSI designed in terms of appearance and functionality?

TaPSI usually require a power source, can be portable or stationary, and are made from various materials. They support both tangible and non-tangible interactions. The interaction with TaPSI can be intuitive, direct, and subtle, but also inconvenient or awkward. Their physicality supports cognition, social settings, emotions, and security benefits, but limits versatility, scalability, and universal applicability. They are also prone to observation or misplacement but can save resources by augmenting environments.

9 The TaPSI Research Framework

Condensing our findings into easy-to-use implications for future research, we present the TaPSI Research Framework to guide researchers in designing corresponding projects. The framework consists of six sequential steps, each accompanied by related recommendations and considerations. These steps are categorized into two primary categories: conceptual research design and technical research design [124]. *Conceptual research design* encompasses all steps required to define the goals of the research project, while *technical research design* outlines the actions necessary to achieve those goals [124]. Note that the framework's content and step order are not necessarily exhaustive or entirely precise, as they are based on the findings from our literature review. We encourage future researchers to further expand and adapt it.

9.1 Starting Point: UPS Problem

Research projects usually address a specific problem [124]. In our work, we observed that research on TaPSI addressed a large variety of UPS problems. In particular, our sample described TaPSI for *authentication, privacy, access control, warnings and education* (see Section 6.1.1), highlighting their potential across most UPS domains.

9.2 Step 1: Tangible (or Not)?

First, researchers should decide whether they want to address their specific problem through TaPSI or not. We recommend basing this decision on the opportunities and challenges inherent to TaPSI (see Section 8.2). In particular, some UPS problems can be (partially) solved by the intuitiveness of TaPSI, their effects on cognition, social settings, and emotions, the direct ad hoc interactions they offer, the fact that they are physically separate devices that can also serve as barriers, as well as their affordances for subtle interactions. We also found that the challenges inherent to TaPSI can be a relevant UPS problem [52, 95]. For example, works in our sample investigated usability challenges of authentication token [2, 28, 29, 56, 72, 128].

9.3 Step 2: Consult Related Work – What Did Others Do?

Consulting related work is another key step in defining research goals [124]. Therefore, we outline strategies for identifying TaPSI publications and uncover underexplored topics.

9.3.1 How to Search for TaPSI Publications?

Digital Libraries & Venues. As the publications in our sample stem from a large variety of venues, we recommend using a search engine not limited to a specific publisher, such as *Google Scholar*. If Google Scholar returns too many irrelevant results, the *ACM DL* is a good alternative for finding TaPSI-related publications, as most of the publications in our sample can be found there. Moreover, most analyzed works were published at HCI venues, like CHI, DIS, IMWUT, or TEI. The most promising (usable) privacy and security venues are Computers & Security, SOUPS, and USENIX Security.

Search Terms. "Security" was the most frequently used term in the analyzed publications, followed by *"device"* and *"physical."* (see Section 6.2). However, unspecific terms like *"device," "mechanism,"* or *"tool"* often describe potentially intrusive devices (e.g., IoT devices or smartphones [37, 76, 94]), rather than TaPSI. We also observed that many publications use *"physical"* or *"physical security"* in contexts unrelated to TaPSI (e.g., policies regulating access to infrastructure [11] or measures against physical harm [61]). Hence, it is currently impossible to determine a failure-proof set of search terms for TaPSI. However, combinations of *"physical", "security"* with *"device"*,*"mechanism"*, or *"interface"* are good starting points. More specific search terms matching the UPS problem are also helpful, such as: *"privacy control," "wearable device," "access control," "authentication token," "physical access,"* or *"physical device"*.

9.3.2 Open Questions For Future Research. Our SoK revealed underexplored questions, presenting promising directions for research.

TaPSI for Specific User Groups: Few TaPSI are tailored to the needs of specific user groups (see Section 6.1.3). However, related work has shown that personal attributes of users impact their perception of TaPSI [31].

Inclusive Security and Privacy: We found that TaPSI can be inclusive to diverse user groups. However, most TaPSI in our sample were not designed or validated for accessibility although research found that TUIs can be beneficial for some people with physical or learning disabilities [73, 140]. Hence, there is a need for future research on TaPSI for inclusive privacy and security management and education.

Insights into the Effects on Cognition: The works in our sample highlight a potential positive impact of TaPSI on cognition and the formation of mental models. Nevertheless, current literature lacks research on which aspects of TaPSI design enhance or hinder cognition.

Correlational Research: Only one publication in our sample used correlational research, which is essential for identifying relationships between variables and making predictions. For TaPSI, it could be used to explore relationships between interface size and user perception, verify security-usability trade-offs, or examine the impact of personal attributes (e.g., age, gender, technical affinity) on TaPSI perception [31].

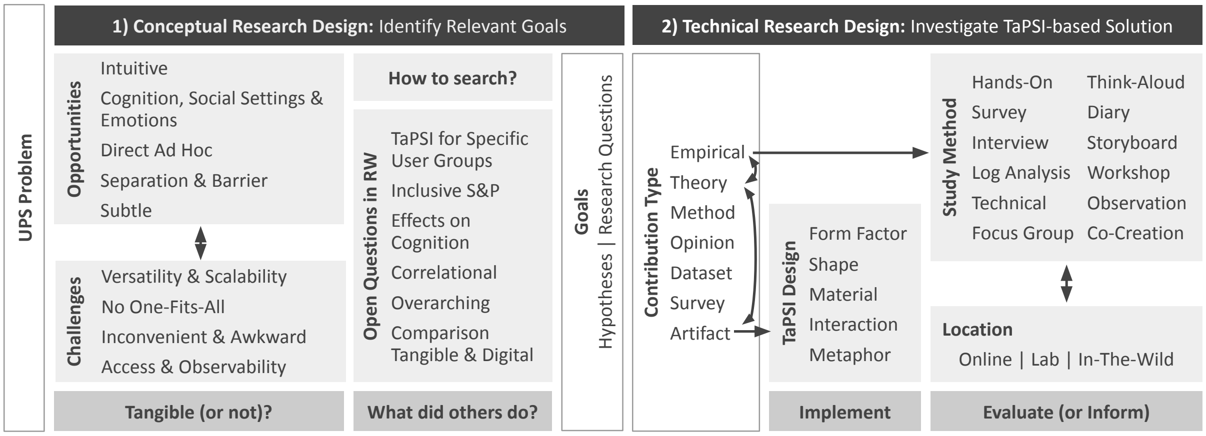


Figure 5: Our findings informed the TaPSI Research Framework. It describes important steps and information to consider when designing a research project on TaPSI. In particular, we provide guidance on how to first identify relevant research goals (i.e., conceptual research design [124]) and how to then investigate a TaPSI-based solution (i.e., technical research design [124]).

Overarching Questions: Most publications in our sample focus on a specific TaPSI sub-group, offering few comparative insights. For instance, it is unclear how users perceive TaPSI across different use cases. Comparative research could help identify which UPS topics are best suited for TaPSI.

Comparison Between Tangible and Digital: Some works in our sample compare tangible and digital solutions for the same application scenario, but most focus on authentication. There remains a lack of research comparing solutions across the digital-tangible spectrum for other use cases.

9.4 Step 3: Research Goals

The next step is to formulate relevant research goals [124]. Although not widely reported in our sample, defining clear research questions is advisable to focus and guide the research effectively [44, 80, 100].

9.5 Step 4: Contribution Type

The technical design of a TaPSI project largely depends on the intended contribution. The decision on contributions should be based on the conceptual research design. Most publications in our sample presented artifacts, made empirical contributions, and/or offered theoretical insights. Typically, projects involved designing and implementing TaPSI, conducting a user study, and optionally providing theoretical insights (see Section 7.1.1). Hence, we focused our framework on these types of contributions. The order of artifact implementation and empirical study can vary depending on whether the study was performed to evaluate the TaPSI or to inform its design. In our framework, we placed the empirical contribution after the artifact, as this is the more common order in our sample.

9.6 Step 5: Implementation & Design Space

Artifact contributions may require implementing a novel TaPSI, which involves key design considerations. To elaborate on this, we present a design space (see Figure 6) and discuss how some TaPSI from our sample apply to it (see Table 7).

9.6.1 Example TaPSI. TaPSI can be authentication mechanisms. For instance, the YubiKey U2F [103] is a commercial USB authentication token (aka. security key). The 3D-Auth Configuration Tangible [82] enables users to authenticate by possessing it (first factor) and rotating its parts to enter a PIN (second factor), before pressing it against a capacitive screen. Undercover [107] enables observation-attack-resistant secret entry at ATMs. Users input graphical passwords by pressing buttons, with the image-to-button mapping conveyed through a trackball hidden beneath their hand.

Moreover, TaPSI like Posit [71], an interactive calendar that lets users control schedule visibility by adjusting its placement, support privacy decisions. Privacy Itch and Scratch [87] is an armband that alerts users to smartphone app privacy intrusions via vibrations and allows them to respond through swiping gestures. In contrast, some TaPSI automatically protect user privacy without requiring their input. For example, ParaSight [42], a smart speaker add-on, locally filters raw audio data and transmits only the filtered information to the speaker via spoken utterances. ParaSight also impacts user awareness as they can hear the utterances.

The IoT Privacy and Security Labels [45] similarly enhance user awareness by providing transparent information about privacy risks. Printed on IoT device packaging, they help users make informed purchase decisions. The visual and auditory IoT Locators [113] are small add-ons for IoT devices that enhance awareness of nearby devices by blinking and beeping. The Moody Keyboard [30] delivers security and privacy warnings during PC interactions through light and vibration.

Other TaPSI provide access control. The ICEbox [137], a network management device, includes a physical lock, ensuring network access is restricted to users with the corresponding key. SenseHandle [33] is a sensor-enhanced door handle that identifies individuals by their door-opening behavior. It authenticates users and restricts entry to unauthorized individuals. TaPSI can also educate users on security topics: Riskio [59] is a tabletop game that teaches company employees about security risks and defensive strategies.

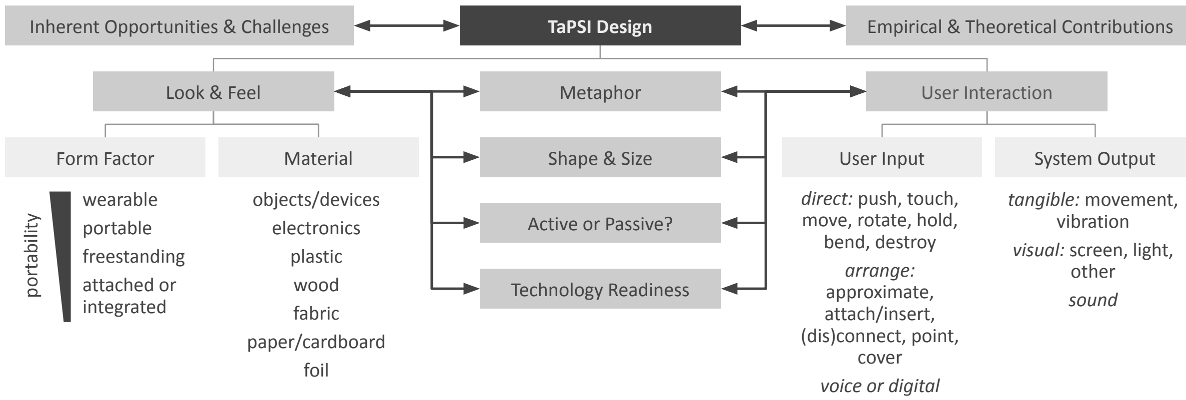


Figure 6: We present a design space for Tangible Privacy and Security Interfaces (TaPSI) that can be used by researchers and developers. We discuss why the design of TaPSI should be informed by reflections on the opportunities and challenges inherent to TaPSI, as well as on the potential findings of or plans for additional empirical or theoretical contributions. The design space describes different options for the look & feel of the TaPSI (i.e., its form factor and materials) and the supported user interactions (i.e., input and output). We also describe how the usage of metaphors, the shape, size, and technology readiness of the TaPSI, and its dependency on a power source (i.e., active or passive) affect the design.

Table 7: This table shows how our design space applies to exemplary TaPSI. For this, we selected a broad sample of TaPSI from different UPS domains. Note that we abbreviated centimeter with cm and decimeter with dm in the "Shape & Size" column.

	Impacting Factors				Look & Feel		User Interaction	
TaPSI	**Metaphor**	**Shape & Size**	**Active/ Passive**	**Technology Readiness**	**Form Factor**	**Materials**	**Input**	**Output**
YubiKey U2F [103]	-	cm-sized USB-stick	passive	TRL9: product on market	portable	device	push; (dis)connect	other device
3D-Auth Configuration Tangible [82]	interaction: *"configure parts"*	cm-sized combination lock	passive	TRL5: pre-prototype tested in lab	portable	plastic	touch; movement; rotate	other device
Undercover [107]	-	dm-sized banking terminal	active	TRL5: pre-prototype tested in lab	freestanding	plastic; electronics; object	push	movement; screen
Posit [71]	appearance: *"desktop calendar"*; interaction: *"position on desk"*	dm-sized desktop calender	active	TRL6: prototype tested in relevant environment	freestanding	electronics; plastic	movement	screen
Privacy Itch and Scratch [87]	interaction: *"itch and scratch"*	cm-sized arm band	active	TRL5: pre-prototype tested in lab	wearable	fabric; electronics	touch	vibration
ParaSight [42]	interaction: *"utterances"*	dm-sized add-on device	active	TRL3: proof of concept	attached	electronics; plastic	voice	sound
IoT Privacy and Security Label [45]	-	cm-sized label on packaging	passive	TRL5: pre-prototype tested in lab	attached	paper or cardboard	approximate (i.e.. scan QR)	other device
IoT Locators [113]	-	cm-sized IoT add-on device	active	TRL5: pre-prototype tested in lab	attached	electronics	digital	light; sound
Moody Keyboard [30]	appearance: *"moody"*	dm-sized PC keyboard	active	TRL4: pre-prototype	freestanding	device; electronics	push	vibration; light
ICEbox [137]	appearance and interaction: *"door lock"*	dm sized wall-mounted device	active	TRL5: pre-prototype tested in lab	attached	electronics	point; attach or insert; touch	screen; other visual
SenseHandle [33]	-	dm-sized door handle add-on	active	TRL5: pre-prototype tested in lab	attached	electronics; plastic	touch; movement	-
Riskio [59]	appearance: *"university fees office"*	dm-sized tabletop game	passive	TRL8: pre-serial manufacturing	freestanding	paper or cardboard	nothing digital	

9.6.2 *How to Decide on the Design?*

The design of TaPSI should be contrasted with two general considerations:

Inherent Opportunities and Challenges: Developers should consider which opportunities of TaPSI they aim to leverage and which of their challenges they want to mitigate.

Empirical or Theoretical Contribution: Researchers may investigate user preferences, empirically evaluate TaPSI, or proof the feasibility of theoretical considerations.

9.6.3 *Look & Feel.*

Form Factor. As described in Section 8.1.1 TaPSI can have different *form factors*. Wearable TaPSI are particularly appropriate for discreet and immediate warning and management interfaces that users need readily accessible (e.g., Privacy Itch and Scratch [87]). Portable TaPSI are suitable for use cases that require frequent interactions in different locations but without a constant exchange of information. They are often used for authentication, such as the YubiKey U2F [103], 3D-Auth tangibles [82], and others [81, 92, 122]. Freestanding TaPSI are designed to stay in specific, meaningful environments, such as desks for office-related privacy and security tasks (e.g., Posit [71], [13], [36], [55]), prominent spots at home (e.g., [22], [20], or [132]), or near devices they support (e.g., Moody Keyboard [30], [16], [15], [94]). Attached to or integrated TaPSI can serve two main purposes: augmenting the specific device (e.g., IoT Locators [113], ParaSight [42], [93], [43], [115], [126]) or object they are attached to (e.g., IoT Privacy and Security Label [45], SenseHandle [33], [50], [106]), or ensuring they remain consistently in the same location (e.g., ICEbox [137]).

Materials. Most TaPSI incorporate *electronics* to support user interaction with digital information (e.g., Undercover [107], Posit [71], IoT Locators [113], ICEbox [137]). *Plastics* are commonly used due to their sturdiness and versatility, as they can be shaped into almost any form via, e.g., 3D printing (e.g., 3D-Auth [82], Posit [71], ParaSight [42], or SenseHandle [33],). *Wood* is also used for rapid prototyping with tools like laser cutters (e.g., [133], [132]) and for its traditional aesthetic (e.g., [22]). *Fabric* allows to implement wearable TaPSI (e.g., Privacy Itch and Scratch [107] or [88]). *Paper and cardboard* are ideal for quickly prototyping low-fidelity TaPSI (e.g., Undercover [107], [79], [41], [90]) and for creating disposable interfaces (e.g., Privacy and Security Labels [45], [52], [91], [60]). *Foils* can enhance TaPSI with their unique properties, such as light scattering [94], opacity modulation [43], or current conduction [36].

9.6.4 *User Interaction.*

Developers need to decide *how users will interact* with the TaPSI. We differentiate between user input to TaPSI and TaPSI' output to the user (see Section 8.1.2).

Usually, the *user input* consists of direct tangible manipulation, the arrangement of objects, voice, or digital input. Tangible user input is easy [28, 29, 60, 111], fast [12, 122, 137], and can act as a reflexive action, boosting user trust in the protections provided by TaPSI [43]. However, when used very frequently, it may be perceived as annoying and effortful [70, 89, 106]. In such cases, voice input could be a viable alternative [20].

The *system output* is either tangible, visual, or auditive. Tangible outputs, such as vibrations or small movements, are discreet and hard for bystanders to notice, making them effective for private communication, as seen in Privacy Itch and Scratch [87], Undercover [107], and other TaPSI [15, 16]. *Movements*, in particular, are intuitively verifiable and unambiguous system outputs, enhancing user trust in TaPSI [7, 43, 55].

9.6.5 *Factors That Impact the Look & Feel and User Interaction.*

We identified additional factors that impact the design of TaPSI.

Metaphor. Metaphors can be applied to the *appearance* of TaPSI or the *user interaction* [47] (see Table 7 and Section 8.1.3). For example, ICEbox [137] employs a *"door lock"* metaphor by integrating a physical lock. Users can manage home network access similarly to deciding who enters their home – by keeping ICEbox locked for restricted access or handing out a key for unlimited access. This makes interactions intuitive and supports cognition because users can apply familiar home security decision-making processes. Posit's [71] appearance is inspired by an analog desktop calendar. It also uses placement changes as an input modality for privacy management, based on the principle that *"if an object is placed in a space in the middle of the desk, it is more private[...][, but if it] is placed in a peripheral area of the desk, it is more legitimate [for bystanders] to focus on"* [71, p. 151]. Hence, Posit leverages users' familiarity with desk positioning for privacy reasons. Privacy Itch and Scratch [87] uses an *"itch and scratch"* metaphor to enable intuitive user interactions. Unlike the *"door lock"* or *"position on desk"* metaphors, however, this metaphor is not linked to privacy or security, and may therefore offer less cognitive support. Therefore, security-related themes (see [32] for examples) are likely better suited to support cognition in addition to intuitive interactions.

TaPSI could also implement personal metaphors if users are able to adapt their colors, shapes, or materials. Such personalized TaPSI leverage users individual experiences and preferences, which supports cognition better [36, 122], elicits emotional responses [36, 82] and potentially increases adoption [31, 82].

Shape & Size. The shape and size of TaPSI can have an impact on their portability, the materials they are made of, and the supported user interaction due to ergonomics and user expectations [37, 94, 122]. In particular, wearable TaPSI should not restrict movement or be uncomfortable to wear [21]. Portable TaPSI should be compact (centimeter-sized), thin, and easily attachable to commonly carried items like keys or wallets [21, 37, 82], but not too small. For instance, while both the YubiKey U2F and YubiKey Nano are portable, the Nano is too small to attach to a keychain, making it harder to transport securely [103]. Freestanding TaPSI are typically decimeter-sized (e.g., Undercover [107], Posit [71] or the Moody keyboard [30]). Nevertheless, their size and shape should be carefully designed to suit their intended environment. This consideration is even more critical for attached TaPSI, such as ParaSight [42], SenseHandle [33], or IoT Locators [113], which must seamlessly integrate with specific objects or devices without compromising functionality. Additionally, developers should consider ergonomics. For instance, Van Koningsbruggen et al. [122] developed TaPSI for embodied password input in various shapes and sizes to identify the optimal balance between security and usability.

Active or Passive? TaPSI are often *active* (i.e., use electrical power) as most user interactions with digital information require electronics. Hence, active TaPSI offer a wide range of interaction options but introduce the need for regular recharging or connection to power outlets. This can particularly affect the usability of wearable and portable TaPSI [21, 26, 82]. Passive TaPSI do not require a power source but rely on specific materials and support limited user interactions. For instance, the 3D-Auth tangibles [82] are designed for a single type of tangible interaction (e.g., configuring parts) and are made of conductive and insulating plastics. Passive TaPSI also often depend on active devices to function, making them suitable for scenarios where such devices are already in use. For example, 3D-Auth tangibles [82] must be pressed against a capacitive screen, the IoT Privacy and Security Label's [45] QR code requires scanning with a smartphone, and the YubiKey U2F [103] connects to a computer's USB port. Hence, passive TaPSI are well-suited for token-based authentication (e.g., YubiKey U2F [103], 3D-Auth tangibles [82]), add-on security or privacy features (e.g., IoT Privacy and Security Label [45], [133], [79], [106]), displaying static information (e.g., Riskio [59], [38], [52], [90]), or as disposable interfaces (e.g., IoT Privacy and Security Label [45], [10], [91]).

Technology Readiness. TaPSI can be implemented in different levels of *technology readiness* (see Section 7.1.2). Early prototypes like paper, click, or wizard-of-oz prototypes have low readiness, while fully functional prototypes and commercial products have high readiness. The readiness level of TaPSI affects its appearance, functionalities, and the study methods suitable for its evaluation. For instance, Undercover [107] is a pre-prototype created to gather user feedback in the lab. Its materials were not durable enough for repeated use in diverse environmental conditions, making it unsuitable for in-the-wild studies. In contrast, the YubiKey U2F [103] is a functional product suitable for in-the-wild studies but limits researchers' ability to influence the interface's design.

9.7 Step 6: Evaluate (or Inform)

Researchers might use empirical methods to evaluate or inform the design of TaPSI. As mentioned before, the choice of study methods or locations is typically linked to their technology readiness.

9.7.1 Study Method. The study methods in our sample correspond to typical HCI methods. However, it is important to note that most of the studies involved direct user interaction with the TaPSI (i.e., hands-on tasks). This was often combined with a collection of user feedback (e.g., through surveys, interviews, or think-aloud methods) or, interestingly, sometimes only used for data collection. In the latter case, the interaction with TaPSI was measured by various sensors in order to subsequently carry out purely technical performance evaluations (e.g. using machine learning). For example, Sharif et al. [111] developed eyeglasses that can avoid face recognition. To evaluate their approach, they took pictures of persons wearing these glasses and measured their effect on the performance of various face recognition models. Alsulaiman et al. [8] asked 16 participants to repeatedly perform their signature using a commercial handwriting device that measures the user's movements and exerted pressure. They subsequently used the collected data to train a machine-learning model for user identification purposes.

9.7.2 Study Location. Most publications in our sample conducted studies in the lab. This corresponds to our expectations of what the evaluation of TaPSI usually looks like. Other researchers performed in-the-wild studies (17.5%) to achieve more ecologically valid results. However, an in-the-wild evaluation might require the development of a prototype with a high technology readiness (i.e., high-fidelity), that is stable against misuse and environmental influences [105].

Interestingly, many publications also conducted studies online (21.25%). Online studies can help to achieve larger and more diverse participant samples, enhancing generalizability [98]. But how can studies involving TaPSI, which are inherently physical, be conducted online? Some performed such online studies by providing their participants with videos that show the TaPSI [43], virtual prototypes of the TaPSI (e.g., click-prototypes) [6, 36, 37, 90], and storyboards [70, 90]. Delgado Rodriguez et al. [37] sent Wizard-of-Oz prototypes to participants, enabling them to experience the interaction with and form factor of PriKey – an interface for configuring privacy settings in smart homes.

9.8 How to Apply the Framework?

Our framework consolidates recommendations for designing TaPSI research projects. To use it, researchers follow Figure 5 from left to right. Hence, the project design *starts with a UPS problem* one aims to address. Next, to *decide whether tangible solutions are suitable for this specific problem*, a researcher considers the inherent *opportunities and challenges of TaPSI.* If the researcher chooses to continue with a tangible approach, the next step involves *consulting related work on TaPSI.* Here, we also recommend *starting points for literature reviews* and discuss *open questions for future research* on TaPSI, as inconsistent terminology can make this process challenging. To conclude the conceptual research design [124], researchers should formulate research goals (i.e., research questions or hypotheses) [80, 124]. The *technical research design* [124] of a project that involves TaPSI strongly depends on the intended contributions. Most publications in our sample presented artifacts and empirical contributions, which they used to derive theoretical insights. Correspondingly, our framework presents a *design space for TaPSI* and discusses *particularities of empirical studies* involving TaPSI.

9.9 Future Extension of the Framework

We encourage future researchers to apply the TaPSI Research Framework to their projects to validate and refine it.

In addition, we envision our framework being replicated for digital privacy and security interfaces by *retaining its structure (i.e., steps and order) but adapting the content* with recommendations specific to digital solutions. The framework could also be similarly adapted to inform the research design of tangible interfaces for non-security topics. It could also be *extended* with insights on digital solutions to guide research on hybrid interfaces – those that allow users to choose between digital and tangible solutions, offering modular, adaptable, and interchangeable user interfaces [31].

Finally, we highlight the need for more research comparing tangible and digital solutions across UPS topics to better understand their respective benefits and challenges.

10 Conclusion

We present the first Systematization of Knowledge (SoK) on tangible privacy and security interfaces (TaPSI). We initially screened

1021 publications from 28 venues using a keyword search, supplemented by backward snowball sampling to minimize sampling bias. We analyzed 80 publications according to our research questions. Based on our findings, we introduce the TaPSI Research Framework to guide researchers in implementing and evaluating TaPSI. This framework outlines opportunities, challenges, a design space, open research questions, and recommendations for finding related work and evaluating TaPSI, making this SoK a foundational resource for future TaPSI research.

Acknowledgments

We thank Priyasha Chatterjee for her support in filtering and coding the publications, and Verena Distler and Sarah Prange for their input to methodological discussions. This project has been funded by the European Union – NextGeneration EU and the dtec.bw – Center for Digitization and Technology Research of the Bundeswehr as part of the project MuQuaNet, as well as the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Germany's Excellence Strategy - EXC 2092 CASA - 390781972.

References

[1] Svetlana Abramova and Rainer Böhme. 2023. Anatomy of a {High-Profile} Data Breach: Dissecting the Aftermath of a {Crypto-Wallet} Case. 715–732. https://www.usenix.org/conference/usenixsecurity23/presentation/abramova

[2] Claudia Ziegler Acemyan, Philip Kortum, Jeffrey Xiong, and Dan S. Wallach. 2018. 2FA Might Be Secure, But It's Not Usable: A Summative Usability Assessment of Google's Two-factor Authentication (2FA) Methods. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* 62, 1 (Sept. 2018), 1141–1145. https://doi.org/10.1177/1541931218621262 Publisher: SAGE Publications Inc.

[3] Alessandro Acquisti, Idris Adjerid, Rebecca Balebako, Laura Brandimarte, Lorrie Faith Cranor, Saranga Komanduri, Pedro Giovanni Leon, Norman Sadeh, Florian Schaub, Manya Sleeper, Yang Wang, and Shomir Wilson. 2017. Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online. *ACM Comput. Surv.* 50, 3, Article 44 (aug 2017), 41 pages. https://doi.org/10.1145/3054926

[4] Alessandro Acquisti, Laura Brandimarte, and George Loewenstein. 2015. Privacy and human behavior in the age of information. *Science* 347, 6221 (2015), 509–514. https://doi.org/10.1126/science.aaa1465 arXiv:https://www.science.org/doi/pdf/10.1126/science.aaa1465

[5] 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

[6] Imtiaz Ahmad, Taslima Akter, Zachary Buher, Rosta Farzan, Apu Kapadia, and Adam J. Lee. 2022. Tangible Privacy for Smart Voice Assistants: Bystanders' Perceptions of Physical Device Controls. *Proc. ACM Hum.-Comput. Interact.* 6, CSCW2 (Nov. 2022), 364:1–364:31. https://doi.org/10.1145/3555089

[7] 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 (Oct. 2020), 116:1–116:28. https://doi.org/10.1145/3415187

[8] Fawaz A. Alsulaiman, Jongeun Cha, and Abdulmotaleb El Saddik. 2008. User Identification Based on Handwritten Signatures with Haptic Information. In *Haptics: Perception, Devices and Scenarios*, Manuel Ferre (Ed.). Springer, Berlin, Heidelberg, 114–121. https://doi.org/10.1007/978-3-540-69057-3_12

[9] Florian Alt and Emanuel von Zezschwitz. 2019. Emerging Trends in Usable Security and Privacy. *i-com* 18 (2019), 189 – 195. https://api.semanticscholar.org/CorpusID:210714734

[10] Andrew W. Appel. 2011. Security Seals on Voting Machines: A Case Study. *ACM Trans. Inf. Syst. Secur.* 14, 2 (Sept. 2011), 18:1–18:29. https://doi.org/10.1145/2019599.2019603

[11] Wade H. Baker and Linda Wallace. 2007. Is Information Security Under Control?: Investigating Quality in Information Security Management. *IEEE Security & Privacy* 5, 1 (2007), 36–44. https://doi.org/10.1109/MSP.2007.11

[12] Dirk Balfanz, Glenn Durfee, Rebecca E. Grinter, Diana K. Smetters, and Paul Stewart. 2004. {Network-in-a-Box}: How to Set Up a Secure Wireless Network in Under a Minute. https://www.usenix.org/conference/13th-usenix-security-symposium/network-box-how-set-secure-wireless-network-under-minute

[13] Szilvia Balogh, Tobias Daniel, Sarah Delgado Rodriguez, Ismael Prieto Romero, and Florian Alt. 2022. Rubik's Cube Auth - A Tangible Authentication Mechanism Using A Standard Rubik's Cube. Gesellschaft für Informatik e.V., 10.18420/muc2022. https://dl.gi.de/handle/20.500.12116/39108

[14] Kristian Beckers and Sebastian Pape. 2016. A Serious Game for Eliciting Social Engineering Security Requirements. In *2016 IEEE 24th International Requirements Engineering Conference (RE)*. 16–25. https://doi.org/10.1109/RE.2016.39 ISSN: 2332-6441.

[15] Andrea Bianchi, Ian Oakley, and Dong Soo Kwon. 2010. The secure haptic keypad: a tactile password system. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '10)*. Association for Computing Machinery, New York, NY, USA, 1089–1092. https://doi.org/10.1145/1753326.1753488

[16] Andrea Bianchi, Ian Oakley, Jong Keun Lee, and Dong Soo Kwon. 2010. The haptic wheel: design & evaluation of a tactile password system. In *CHI '10 Extended Abstracts on Human Factors in Computing Systems (CHI EA '10)*. Association for Computing Machinery, New York, NY, USA, 3625–3630. https://doi.org/10.1145/1753846.1754029

[17] John M. Blythe, Lynne Coventry, and Linda Little. 2015. Unpacking security policy compliance: the motivators and barriers of employees' security behaviors. In *Proceedings of the Eleventh USENIX Conference on Usable Privacy and Security* (Ottawa, Canada) *(SOUPS '15)*. USENIX Association, USA, 103–122.

[18] R Boyatzis. 1998. *Transforming qualitative information: Thematic analysis and code development.* Sage.

[19] Judee K Burgoon. 2012. Privacy and communication. In *Communication yearbook 6*. Routledge, 206–249.

[20] Varun Chandrasekaran, Suman Banerjee, Bilge Mutlu, and Kassem Fawaz. 2021. {PowerCut} and Obfuscator: An Exploration of the Design Space for {Privacy-Preserving} Interventions for Smart Speakers. 535–552. https://www.usenix.org/conference/soups2021/presentation/chandrasekaran

[21] Yuxin Chen, Huiying Li, Shan-Yuan Teng, Steven Nagels, Zhijing Li, Pedro Lopes, Ben Y. Zhao, and Haitao Zheng. 2020. Wearable Microphone Jamming. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–12. https://doi.org/10.1145/3313831.3376304

[22] Yu-Ting Cheng, Mathias Funk, Wenn-Chieh Tsai, and Lin-Lin Chen. 2019. Peekaboo Cam: Designing an Observational Camera for Home Ecologies Concerning Privacy. In *Proceedings of the 2019 on Designing Interactive Systems Conference (DIS '19)*. Association for Computing Machinery, New York, NY, USA, 823–836. https://doi.org/10.1145/3322276.3323699

[23] Luigi Lo Iacono Christian Reuter and Alexander Benlian. 2022. A quarter century of usable security and privacy research: transparency, tailorability, and the road ahead. *Behaviour & Information Technology* 41, 10 (2022), 2035–2048. https://doi.org/10.1080/0144929X.2022.2080908 arXiv:https://doi.org/10.1080/0144929X.2022.2080908

[24] European Commission. [n. d.]. ABOUT TECHNOLOGY READINESS LEVELS. https://euraxess.ec.europa.eu/career-development/researchers/manual-scientific-entrepreneurship/major-steps/trl Last accessed 20 July 2023.

[25] European Commission. 2014. HORIZON 2020 – WORK PROGRAMME 2014-2015 General Annexes2 22. Extract from Part 19 - Commission Decision C(2014)4995. https://ec.europa.eu/research/participants/data/ref/h2020/wp/2014_2015/annexes/h2020-wp1415-annex-g-trl_en.pdf Last accessed 20 July 2023.

[26] Enrico Costanza, Samuel A. Inverso, Elan Pavlov, Rebecca Allen, and Pattie Maes. 2006. eye-q: eyeglass peripheral display for subtle intimate notifications. In *Proceedings of the 8th conference on Human-computer interaction with mobile devices and services (MobileHCI '06)*. Association for Computing Machinery, New York, NY, USA, 211–218. https://doi.org/10.1145/1152215.1152261

[27] Benjamin F Crabtree and William F Miller. 1992. A template approach to text analysis: developing and using codebooks. (1992).

[28] Sanchari Das, Andrew Dingman, and L. Jean Camp. 2018. Why Johnny Doesn't Use Two Factor A Two-Phase Usability Study of the FIDO U2F Security Key. In *Financial Cryptography and Data Security*, Sarah Meiklejohn and Kazue Sako (Eds.). Springer, Berlin, Heidelberg, 160–179. https://doi.org/10.1007/978-3-662-58387-6_9

[29] Emiliano De Cristofaro, Honglu Du, Julien Freudiger, and Greg Norcie. [n. d.]. A Comparative Usability Study of Two-Factor Authentication. https://www.ndss-symposium.org/ndss2014/ndss-2014-usec-programme/comparative-usability-study-two-factor-authentication/

[30] Alexander De Luca, Bernhard Frauendienst, Max Maurer, and Doris Hausen. 2010. On the design of a "moody" keyboard. In *Proceedings of the 8th ACM Conference on Designing Interactive Systems (DIS '10)*. Association for Computing Machinery, New York, NY, USA, 236–239. https://doi.org/10.1145/1858171.1858213

[31] Sarah Delgado Rodriguez, Priyasha Chatterjee, Anh Dao Phuong, Florian Alt, and Karola Marky. 2024. Do You Need to Touch? Exploring Correlations between Personal Attributes and Preferences for Tangible Privacy Mechanisms. In *Proceedings of the CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '24)*. Association for Computing Machinery, New York, NY, USA, Article 981, 23 pages. https://doi.org/10.1145/3613904.3642863

[32] 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 *Proceedings of the 22nd International Conference on Mobile and Ubiquitous Multimedia* (Vienna, Austria) *(MUM '23)*. Association for Computing Machinery, New York, NY, USA, 10–24. https://doi.org/10.1145/3626705.3627770

[33] Sarah Delgado Rodriguez, Lukas Mecke, and Florian Alt. [n. d.]. SenseHandle: Investigating Human-Door Interaction Behaviour for Authentication in the Physical World | USENIX. https://www.usenix.org/conference/soups2022/presentation/delgado-rodriguez-poster

[34] Sarah Delgado Rodriguez, Sarah Prange, and Florian Alt. 2021. Take Your Security and Privacy Into Your Own Hands! Why Security and Privacy Assistants Should be Tangible. https://doi.org/20.500.12116/37360

[35] Sarah Delgado Rodriguez, Sarah Prange, Pascal Knierim, Karola Marky, and Florian Alt. 2022. Experiencing Tangible Privacy Control for Smart Homes with PriKey. In *Proceedings of the 21st International Conference on Mobile and Ubiquitous Multimedia (MUM '22)*. Association for Computing Machinery, New York, NY, USA, 298–300. https://doi.org/10.1145/3568444.3570585

[36] Sarah Delgado Rodriguez, Sarah Prange, Lukas Mecke, and Florian Alt. 2024. Act2Auth – A Novel Authentication Concept based on Embedded Tangible Interaction at Desks. In *Proceedings of the Eighteenth International Conference on Tangible, Embedded, and Embodied Interaction (TEI '24)*. Association for Computing Machinery, New York, NY, USA, 1–15. https://doi.org/10.1145/3623509.3633360

[37] Sarah Delgado Rodriguez, Sarah Prange, Christina Vergara Ossenberg, Markus Henkel, Florian Alt, and Karola Marky. 2022. PriKey – Investigating Tangible Privacy Control for Smart Home Inhabitants and Visitors. In *Nordic Human-Computer Interaction Conference (NordiCHI '22)*. Association for Computing Machinery, New York, NY, USA, 1–13. https://doi.org/10.1145/3546155.3546640

[38] Tamara Denning, Adam Lerner, Adam Shostack, and Tadayoshi Kohno. 2013. Control-Alt-Hack: the design and evaluation of a card game for computer security awareness and education. In *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security (CCS '13)*. Association for Computing Machinery, New York, NY, USA, 915–928. https://doi.org/10.1145/2508859.2516753

[39] Francesco Di Nocera, Giorgia Tempestini, and Matteo Orsini. 2023. Usable Security: A Systematic Literature Review. *Information* 14, 12 (2023). https://doi.org/10.3390/info14120641

[40] 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

[41] Youngwook Do, Nivedita Arora, Ali Mirzazadeh, Injoo Moon, Eryue Xu, Zhihan Zhang, Gregory D. Abowd, and Sauvik Das. 2023. Powering for Privacy: Improving User Trust in Smart Speaker Microphones with Intentional Powering and Perceptible Assurance. 2473–2490. https://www.usenix.org/conference/usenixsecurity23/presentation/do

[42] Youngwook Do, Seong-Eun Moon, and Minsuk Chang. 2022. ParaSight: Enabling Privacy-preserving Sensing Data Sharing via Device-to-device Utterance-based Communication. In *Extended Abstracts of the 2022 CHI Conference on Human Factors in Computing Systems (CHI EA '22)*. Association for Computing Machinery, New York, NY, USA, 1–6. https://doi.org/10.1145/3491101.3519757

[43] Youngwook Do, Jung Wook Park, Yuxi Wu, Avinandan Basu, Dingtian Zhang, Gregory D. Abowd, and Sauvik Das. 2022. Smart Webcam Cover: Exploring the Design of an Intelligent Webcam Cover to Improve Usability and Trust. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 5, 4 (Dec. 2022), 154:1–154:21. https://doi.org/10.1145/3494983

[44] Renee Elio, Jim Hoover, Ioanis Nikolaidis, Mohammad Salavatipour, Lorna Stewart, and Ken Wong. 2011. About computing science research methodology. *Google Scholar Google Scholar Reference* (2011).

[45] Pardis Emami-Naeini, Yuvraj Agarwal, Lorrie Faith Cranor, and Hanan Hibshi. 2020. Ask the Experts: What Should Be on an IoT Privacy and Security Label?. In *2020 IEEE Symposium on Security and Privacy (SP)*. 447–464. https://doi.org/10.1109/SP40000.2020.00043 ISSN: 2375-1207.

[46] Jennifer Fereday and Eimear Muir-Cochrane. 2006. Demonstrating rigor using thematic analysis: A hybrid approach of inductive and deductive coding and theme development. *International journal of qualitative methods* 5, 1 (2006), 80–92.

[47] Kenneth P. Fishkin. 2004. A taxonomy for and analysis of tangible interfaces. *Personal Ubiquitous Comput.* 8, 5 (sep 2004), 347–358.

[48] Kenneth P. Fishkin, Anuj Gujar, Beverly L. Harrison, Thomas P. Moran, and Roy Want. 2000. Embodied user interfaces for really direct manipulation. *Commun. ACM* 43, 9 (sep 2000), 74–80. https://doi.org/10.1145/348941.348998

[49] Sylvain Frey, Awais Rashid, Pauline Anthonysamy, Maria Pinto-Albuquerque, and Syed Asad Naqvi. 2019. The Good, the Bad and the Ugly: A Study of Security Decisions in a Cyber-Physical Systems Game. *IEEE Transactions on Software Engineering* 45, 5 (May 2019), 521–536. https://doi.org/10.1109/TSE.2017.2782813 Conference Name: IEEE Transactions on Software Engineering.

[50] Kyosuke Futami, Akari Fukao, and Kazuya Murao. 2019. A method to recognize entering and leaving person based on door opening and closing movement using angular velocity sensor. In *Adjunct Proceedings of the 2019 ACM International Joint Conference on Pervasive and Ubiquitous Computing and Proceedings of the 2019 ACM International Symposium on Wearable Computers (UbiComp/ISWC '19 Adjunct)*. Association for Computing Machinery, New York, NY, USA, 57–60. https://doi.org/10.1145/3341162.3343798

[51] Simson Garfinkel and Heather Richter Lipford. 2014. *Usable security: History, themes, and challenges*. Morgan & Claypool Publishers.

[52] Dañiel Gerhardt, Alexander Ponticello, Adrian Dabrowski, and Katharina Krombholz. 2023. Investigating Verification Behavior and Perceptions of Visual Digital Certificates. 3565–3582. https://www.usenix.org/conference/usenixsecurity23/presentation/gerhardt

[53] Mark Gondree and Zachary N. J. Peterson. 2013. Valuing Security by Getting {[d0x3d!]}: Experiences with a Network Security Board Game. https://www.usenix.org/conference/cset13/workshop-program/presentation/gondree

[54] Ingrid Graffer, Maria Bartnes, and K. Bernsmed. 2015. Play2Prepare: A Board Game Supporting IT Security Preparedness Exercises for Industrial Control Organizations. https://api.semanticscholar.org/CorpusID:55543977

[55] Saul Greenberg and Hideaki Kuzuoka. 1999. Using digital but physical surrogates to mediate awareness, communication and privacy in media spaces. *Personal Technologies* 3, 4 (Dec. 1999), 182–198. https://doi.org/10.1007/BF01540552

[56] Nancie Gunson, Diarmid Marshall, Hazel Morton, and Mervyn Jack. 2011. User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking. *Computers & Security* 30, 4 (June 2011), 208–220. https://doi.org/10.1016/j.cose.2010.12.001

[57] Sandeep Gupta, Attaullah Buriro, and Bruno Crispo. 2019. SmartHandle: A Novel Behavioral Biometric-based Authentication Scheme for Smart Lock Systems. In *Proceedings of the 2019 3rd International Conference on Biometric Engineering and Applications (ICBEA 2019)*. Association for Computing Machinery, New York, NY, USA, 15–22. https://doi.org/10.1145/3345336.3345344

[58] Marian Harbach, Sascha Fahl, Matthias Rieger, and Matthew Smith. 2013. On the Acceptance of Privacy-Preserving Authentication Technology: The Curious Case of National Identity Cards. In *Privacy Enhancing Technologies*, Emiliano De Cristofaro and Matthew Wright (Eds.). Springer, Berlin, Heidelberg, 245–264. https://doi.org/10.1007/978-3-642-39077-7_13

[59] Stephen Hart, Andrea Margheri, Federica Paci, and Vladimiro Sassone. 2020. Riskio: A Serious Game for Cyber Security Awareness and Education. *Computers & Security* 95 (Aug. 2020), 101827. https://doi.org/10.1016/j.cose.2020.101827

[60] Eiji Hayashi, Bryan Pendleton, Fatih Ozenc, and Jason Hong. 2012. WebTicket: account management using printable tokens. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '12)*. Association for Computing Machinery, New York, NY, USA, 997–1006. https://doi.org/10.1145/2207676.2208545

[61] Duncan Hodges. 2021. Cyber-enabled burglary of smart homes. *Computers & Security* 110 (2021), 102418. https://doi.org/10.1016/j.cose.2021.102418

[62] Lars Erik Holmquist, Johan Redström, and Peter Ljungstrand. 1999. Token-Based Access to Digital Information. In *Handheld and Ubiquitous Computing*, Hans-W. Gellersen (Ed.). Springer Berlin Heidelberg, Berlin, Heidelberg, 234–245.

[63] Eva Hornecker and Jacob Buur. 2006. Getting a grip on tangible interaction: a framework on physical space and social interaction. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Montréal, Québec, Canada) *(CHI '06)*. Association for Computing Machinery, New York, NY, USA, 437–446. https://doi.org/10.1145/1124772.1124838

[64] Jörn Hurtienne and Johann Habakuk Israel. 2007. Image schemas and their metaphorical extensions: intuitive patterns for tangible interaction. In *Proceedings of the 1st International Conference on Tangible and Embedded Interaction* (Baton Rouge, Louisiana) *(TEI '07)*. Association for Computing Machinery, New York, NY, USA, 127–134. https://doi.org/10.1145/1226969.1226996

[65] Giovanni Iachello and Jason Hong. 2007. End-User Privacy in Human–Computer Interaction. *Foundations and Trends® in Human–Computer Interaction* 1, 1 (2007), 1–137. https://doi.org/10.1561/1100000004

[66] Vincent Immler, Johannes Obermaier, Kuan Kuan Ng, Fei Xiang Ke, JinYu Lee, Yak Peng Lim, Wei Koon Oh, Keng Hoong Wee, and Georg Sigl. 2019. Secure Physical Enclosures from Covers with Tamper-Resistance. *IACR Transactions on Cryptographic Hardware and Embedded Systems* (2019), 51–96. https://doi.org/10.13154/tches.v2019.i1.51-96

[67] Hiroshi Ishii. 2008. Tangible bits: beyond pixels. In *Proceedings of the 2nd International Conference on Tangible and Embedded Interaction* (Bonn, Germany) *(TEI '08)*. Association for Computing Machinery, New York, NY, USA, xv–xxv. https://doi.org/10.1145/1347390.1347392

[68] Hiroshi Ishii and Brygg Ullmer. 1997. Tangible bits: towards seamless interfaces between people, bits and atoms. In *Proceedings of the ACM SIGCHI Conference on Human Factors in Computing Systems* (Atlanta, Georgia, USA) *(CHI '97)*. Association for Computing Machinery, New York, NY, USA, 234–241. https://doi.org/10.1145/258549.258715

[69] Lukasz Jedrzejczyk, Blaine A. Price, Arosha Bandara, and Bashar Nuseibeh. 2010. "Privacy-shake",: a haptic interface for managing privacy settings in mobile location sharing applications. In *Proceedings of the 12th international conference on Human computer interaction with mobile devices and services (MobileHCI '10)*. Association for Computing Machinery, New York, NY, USA, 411–412. https://doi.org/10.1145/1851600.1851690
[70] Haojian Jin, Boyuan Guo, Rituparna Roychoudhury, Yaxing Yao, Swarun Kumar, Yuvraj Agarwal, and Jason I. Hong. 2022. Exploring the Needs of Users for Supporting Privacy-Protective Behaviors in Smart Homes. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems (CHI '22)*. Association for Computing Machinery, New York, NY, USA, 1–19. https://doi.org/10.1145/3491102.3517602
[71] Nari Kim, Juntae Kim, Bomin Kim, and Young-Woo Park. 2021. The Trial of Posit in Shared Offices: Controlling Disclosure Levels of Schedule Data for Privacy by Changing the Placement of a Personal Interactive Calendar. In *Proceedings of the 2021 ACM Designing Interactive Systems Conference (DIS '21)*. Association for Computing Machinery, New York, NY, USA, 149–159. https://doi.org/10.1145/3461778.3462073
[72] Kat Krol, Eleni Philippou, Emiliano De Cristofaro, and Angela Sasse. [n. d.]. "They brought in the horrible key ring thing!" Analysing the Usability of Two-Factor Authentication in UK Online Banking. https://www.ndss-symposium.org/ndss2015/ndss-2015-usec-programme/they-brought-horrible-key-ring-thing-analysing-usability-two-factor-authentication-uk-online/
[73] Adam A Kumpf et al. 2009. *Trackmate: Large-scale accessibility of tangible user interfaces.* Ph. D. Dissertation. Massachusetts Institute of Technology, School of Architecture and Planning ....
[74] Juan Lang, Alexei Czeskis, Dirk Balfanz, Marius Schilder, and Sampath Srinivas. 2017. Security Keys: Practical Cryptographic Second Factors for the Modern Web. In *Financial Cryptography and Data Security*, Jens Grossklags and Bart Preneel (Eds.). Springer, Berlin, Heidelberg, 422–440. https://doi.org/10.1007/978-3-662-54970-4_25
[75] Markus Lennartsson, Joakim Kävrestad, and Marcus Nohlberg. 2021. Exploring the meaning of usable security–a literature review. *Information & Computer Security* 29, 4 (2021), 647–663.
[76] Xiaopeng Li, Qiang Zeng, Lannan Luo, and Tongbo Luo. 2020. T2Pair: Secure and Usable Pairing for Heterogeneous IoT Devices. In *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security (CCS '20)*. Association for Computing Machinery, New York, NY, USA, 309–323. https://doi.org/10.1145/3372297.3417286
[77] Yanhong Li, Meng Liang, Julian Preissing, Nadine Bachl, Michelle Melina Dutoit, Thomas Weber, Sven Mayer, and Heinrich Hussmann. 2022. A Meta-Analysis of Tangible Learning Studies from the TEI Conference. In *Proceedings of the Sixteenth International Conference on Tangible, Embedded, and Embodied Interaction* (Daejeon, Republic of Korea) *(TEI '22)*. Association for Computing Machinery, New York, NY, USA, Article 7, 17 pages. https://doi.org/10.1145/3490149.3501313
[78] Meng Liang, Yanhong Li, Thomas Weber, and Heinrich Hussmann. 2021. Tangible Interaction for Children's Creative Learning: A Review. In *Proceedings of the 13th Conference on Creativity and Cognition* (Virtual Event, Italy) *(C&C '21)*. Association for Computing Machinery, New York, NY, USA, Article 14, 14 pages. https://doi.org/10.1145/3450741.3465262
[79] Linda Little, Pam Briggs, and Lynne Coventry. 2005. Public space systems: Designing for privacy? *International Journal of Human-Computer Studies* 63, 1 (July 2005), 254–268. https://doi.org/10.1016/j.ijhcs.2005.04.018
[80] Yiren Liu, Mengxia Yu, Meng Jiang, and Yun Huang. 2023. Creative Research Question Generation for Human-Computer Interaction Research.. In *IUI Workshops*. 58–66.
[81] Sana Maqsood, Sonia Chiasson, and Audrey Girouard. 2016. Bend Passwords: using gestures to authenticate on flexible devices. *Personal Ubiquitous Comput.* 20, 4 (Aug. 2016), 573–600. https://doi.org/10.1007/s00779-016-0928-6
[82] Karola Marky, Martin Schmitz, Verena Zimmermann, Martin Herbers, Kai Kunze, and Max Mühlhäuser. 2020. 3D-Auth: Two-Factor Authentication with Personalized 3D-Printed Items. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–12. https://doi.org/10.1145/3313831.3376189
[83] Ali Mazalek and Elise van den Hoven. 2009. Framing tangible interaction frameworks. *Artificial Intelligence for Engineering Design, Analysis and Manufacturing* 23, 3 (2009), 225–235. https://doi.org/10.1017/S0890060409000201
[84] Nora McDonald, Sarita Schoenebeck, and Andrea Forte. 2019. Reliability and inter-rater reliability in qualitative research: Norms and guidelines for CSCW and HCI practice. *Proceedings of the ACM on human-computer interaction* 3, CSCW (2019), 1–23.
[85] Vikram Mehta. 2019. Tangible Interactions for Privacy Management. In *Proceedings of the Thirteenth International Conference on Tangible, Embedded, and Embodied Interaction (TEI '19)*. Association for Computing Machinery, New York, NY, USA, 723–726. https://doi.org/10.1145/3294109.3302934
[86] Vikram Mehta. 2019. Tangible Interactions for Privacy Management. In *Proceedings of the Thirteenth International Conference on Tangible, Embedded, and Embodied Interaction* (Tempe, Arizona, USA) *(TEI '19)*. Association for Computing Machinery, New York, NY, USA, 723–726. https://doi.org/10.1145/3294109.3302934
[87] Vikram Mehta, Arosha K. Bandara, Blaine A. Price, and Bashar Nuseibeh. 2016. Privacy Itch and Scratch: On Body Privacy Warnings and Controls. In *Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems (CHI EA '16)*. Association for Computing Machinery, New York, NY, USA, 2417–2424. https://doi.org/10.1145/2851581.2892475
[88] Vikram Mehta, Arosha K. Bandara, Blaine A. Price, Bashar Nuseibeh, and Daniel Gooch. 2021. Up Close & Personal: Exploring User-preferred Image Schemas for Intuitive Privacy Awareness and Control. In *Proceedings of the Fifteenth International Conference on Tangible, Embedded, and Embodied Interaction (TEI '21)*. Association for Computing Machinery, New York, NY, USA, 1–13. https://doi.org/10.1145/3430524.3440626
[89] Vikram Mehta, Daniel Gooch, Arosha Bandara, Blaine Price, and Bashar Nuseibeh. 2021. Privacy Care: A Tangible Interaction Framework for Privacy Management. *ACM Trans. Internet Technol.* 21, 1 (Feb. 2021), 25:1–25:32. https://doi.org/10.1145/3430506
[90] Vikram Mehta, Daniel Gooch, Arosha Bandara, Blaine A. Price, and Bashar Nuseibeh. 2023. A Card-based Ideation Toolkit to Generate Designs for Tangible Privacy Management Tools. In *Proceedings of the Seventeenth International Conference on Tangible, Embedded, and Embodied Interaction (TEI '23)*. Association for Computing Machinery, New York, NY, USA, 1–13. https://doi.org/10.1145/3569009.3572903
[91] Paul A. Moskowitz, Andris Lauris, and Stephen S. Morris. 2007. A Privacy-Enhancing Radio Frequency Identification Tag: Implementation of the Clipped Tag. IEEE Computer Society, 348–351. https://doi.org/10.1109/PERCOMW.2007.11
[92] Martez Mott, Thomas Donahue, G. Michael Poor, and Laura Leventhal. 2012. Leveraging motor learning for a tangible password system. In *CHI '12 Extended Abstracts on Human Factors in Computing Systems (CHI EA '12)*. Association for Computing Machinery, New York, NY, USA, 2597–2602. https://doi.org/10.1145/2212776.2223842
[93] Kazuya Murao, Hayami Tobise, Tsutomu Terada, Toshiki Iso, Masahiko Tsukamoto, and Tsutomu Horikoshi. 2014. Mobile Phone User Authentication with Grip Gestures using Pressure Sensors. In *Proceedings of the 12th International Conference on Advances in Mobile Computing and Multimedia (MoMM '14)*. Association for Computing Machinery, New York, NY, USA, 143–146. https://doi.org/10.1145/2684103.2684116
[94] Max Möllers, Ray Bohnenberger, Stephan Deininghaus, Patrick Zimmer, Karin Herrmann, and Jan Borchers. 2011. TaPS Widgets: tangible control over private spaces on interactive tabletops. In *CHI '11 Extended Abstracts on Human Factors in Computing Systems (CHI EA '11)*. Association for Computing Machinery, New York, NY, USA, 773–780. https://doi.org/10.1145/1979742.1979632
[95] Ashish Nanda, Jongkil Jay Jeong, Syed Wajid Ali Shah, Mohammad Nosouhi, and Robin Doss. 2024. Examining usable security features and user perceptions of Physical Authentication Devices. *Computers & Security* 139 (April 2024), 103664. https://doi.org/10.1016/j.cose.2023.103664
[96] Ugochi Oluwatosin Nwokedi, Beverly Amunga Onyimbo, and Babak Bashari Rad. 2016. Usability and security in user interface design: a systematic literature review. *International Journal of Information Technology and Computer Science (IJITCS)* 8, 5 (2016), 72–80.
[97] L. O'Gorman. 2003. Comparing passwords, tokens, and biometrics for user authentication. *Proc. IEEE* 91, 12 (2003), 2021–2040. https://doi.org/10.1109/JPROC.2003.819611
[98] Aswati Panicker, Novia Nurain, Zaidat Ibrahim, Chun-Han (Ariel) Wang, Seung Wan Ha, Yuxing Wu, Kay Connelly, Katie A. Siek, and Chia-Fang Chung. 2024. Understanding fraudulence in online qualitative studies: From the researcher's perspective. In *Proceedings of the CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '24)*. Association for Computing Machinery, New York, NY, USA, Article 824, 17 pages. https://doi.org/10.1145/3613904.3642732
[99] Rebecca S. Portnoff, Linda N. Lee, Serge Egelman, Pratyush Mishra, Derek Leung, and David Wagner. 2015. Somebody's Watching Me? Assessing the Effectiveness of Webcam Indicator Lights. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI '15)*. Association for Computing Machinery, New York, NY, USA, 1649–1658. https://doi.org/10.1145/2702123.2702164
[100] Simmi K Ratan, Tanu Anand, and John Ratan. 2019. Formulation of research question–Stepwise approach. *Journal of Indian Association of Pediatric Surgeons* 24, 1 (2019), 15–20.
[101] Ken Reese, Trevor Smith, Jonathan Dutson, Jonathan Armknecht, Jacob Cameron, and Kent Seamons. 2019. A Usability Study of Five {Two-Factor} Authentication Methods. 357–370. https://www.usenix.org/conference/soups2019/presentation/reese

[102] J. Rekimoto, Y. Ayatsuka, Michimune Kohno, and Haruo Oba. 2003. Proximal Interactions: A Direct Manipulation Technique for Wireless Networking. https://www.semanticscholar.org/paper/Proximal-Interactions%3A-A-Direct-Manipulation-for-Rekimoto-Ayatsuka/cf9644103b94af4bcaf13cda5b07d6dcf8da9c6a

[103] Joshua Reynolds, Trevor Smith, Ken Reese, Luke Dickinson, Scott Ruoti, and Kent Seamons. 2018. A Tale of Two Studies: The Best and Worst of YubiKey Usability. In *2018 IEEE Symposium on Security and Privacy (SP)*. 872–888. https://doi.org/10.1109/SP.2018.00067 ISSN: 2375-1207.

[104] Lea Dujić Rodić and Andrina Granić. 2021. Tangible interfaces in early years' education: a systematic review. *Personal and Ubiquitous Computing* (2021), 1–39.

[105] Yvonne Rogers, Helen Sharp, and Jenny Preece. 2011. *Interaction Design: Beyond Human-Computer Interaction.* John Wiley & Sons.

[106] Matthew Rueben, Frank J. Bernieri, Cindy M. Grimm, and William D. Smart. 2016. User feedback on physical marker interfaces for protecting visual privacy from mobile robots. In *2016 11th ACM/IEEE International Conference on Human-Robot Interaction (HRI)*. 507–508. https://doi.org/10.1109/HRI.2016.7451829 ISSN: 2167-2148.

[107] Hirokazu Sasamoto, Nicolas Christin, and Eiji Hayashi. 2008. Undercover: authentication usable in front of prying eyes. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '08)*. Association for Computing Machinery, New York, NY, USA, 183–192. https://doi.org/10.1145/1357054.1357085

[108] M. Angela Sasse, Jonas Hielscher, Jennifer Friedauer, and Annalina Buckmann. 2023. Rebooting IT Security Awareness – How Organisations Can Encourage and¬†Sustain Secure Behaviours. In *Computer Security. ESORICS 2022 International Workshops*, Sokratis Katsikas, Frédéric Cuppens, Christos Kalloniatis, John Mylopoulos, Frank Pallas, Jörg Pohle, M. Angela Sasse, Habtamu Abie, Silvio Ranise, Luca Verderame, Enrico Cambiaso, Jorge Maestre Vidal, Marco Antonio Sotelo Monge, Massimiliano Albanese, Basel Katt, Sandeep Pirbhulal, and Ankur Shukla (Eds.). Springer International Publishing, Cham, 248–265.

[109] Florian Schaub and Pascal Knierim. 2016. Drone-based Privacy Interfaces: Opportunities and Challenges. https://www.usenix.org/conference/soups2016/workshop-program/wfpn/presentation/schaub

[110] Orit Shaer and Eva Hornecker. 2010. Tangible User Interfaces: Past, Present, and Future Directions. *Foundations and Trends® in Human–Computer Interaction* 3, 1–2 (2010), 4–137. https://doi.org/10.1561/1100000026

[111] Mahmood Sharif, Sruti Bhagavatula, Lujo Bauer, and Michael K. Reiter. 2016. Accessorize to a Crime: Real and Stealthy Attacks on State-of-the-Art Face Recognition. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS '16)*. Association for Computing Machinery, New York, NY, USA, 1528–1540. https://doi.org/10.1145/2976749.2978392

[112] Ben Shneiderman. 1983. Direct manipulation: A step beyond programming languages. *Computer* 16, 08 (1983), 57–69.

[113] Yunpeng Song, Yun Huang, Zhongmin Cai, and Jason I. Hong. 2020. I'm All Eyes and Ears: Exploring Effective Locators for Privacy Awareness in IoT Scenarios. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–13. https://doi.org/10.1145/3313831.3376585

[114] Sarah Spiekermann and Sergei Evdokimov. 2009. Critical RFID Privacy-Enhancing Technologies. *IEEE Security & Privacy* 7, 2 (March 2009), 56–62. https://doi.org/10.1109/MSP.2009.31 Conference Name: IEEE Security & Privacy.

[115] Paul Staat, Johannes Tobisch, Christian Zenger, and Christof Paar. 2022. Anti-Tamper Radio: System-Level Tamper Detection for Computing Systems. In *2022 IEEE Symposium on Security and Privacy (SP)*. 1722–1736. https://doi.org/10.1109/SP46214.2022.9833631 ISSN: 2375-1207.

[116] Charles Stangor and Jennifer Walinga. 2014. *Introduction to psychology.* BCcampus.

[117] Dennis Strouble, Gregory Shechtman, and Alan Alsop. 2009. Productivity and Usability Effects of Using a Two-Factor Security System. *SAIS 2009 Proceedings* (March 2009). https://aisel.aisnet.org/sais2009/37

[118] Ke Sun, Chen Chen, and Xinyu Zhang. 2020. "Alexa, stop spying on me!": speech privacy protection against voice assistants. In *Proceedings of the 18th Conference on Embedded Networked Sensor Systems (SenSys '20)*. Association for Computing Machinery, New York, NY, USA, 298–311. https://doi.org/10.1145/3384419.3430727

[119] Marc Teyssier, Marion Koelle, Paul Strohmeier, Bruno Fruchard, and Jürgen Steimle. 2021. Eyecam: Revealing Relations between Humans and Sensing Devices through an Anthropomorphic Webcam. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (CHI '21)*. Association for Computing Machinery, New York, NY, USA, 1–13. https://doi.org/10.1145/3411764.3445491

[120] Christian Tiefenau, Maximilian Häring, Eva Gerlitz, and Emanuel Zezschwitz. 2019. *Making Privacy Graspable: Can we Nudge Users to use Privacy Enhancing Techniques?*

[121] B. Ullmer and H. Ishii. 2000. Emerging frameworks for tangible user interfaces. *IBM Syst. J.* 39, 3–4 (jul 2000), 915–931. https://doi.org/10.1147/sj.393.0915

[122] Rosa van Koningsbruggen, Bart Hengeveld, and Jason Alexander. 2021. Understanding the Design Space of Embodied Passwords based on Muscle Memory. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (CHI '21)*. Association for Computing Machinery, New York, NY, USA, 1–13. https://doi.org/10.1145/3411764.3445773

[123] Ignacio Velásquez, Angélica Caro, and Alfonso Rodríguez. 2018. Authentication schemes and methods: A systematic literature review. *Information and Software Technology* 94 (2018), 30–37. https://doi.org/10.1016/j.infsof.2017.09.012

[124] Piet Verschuren, Hans Doorewaard, and MJ Mellion. 2010. *Designing a research project.* Vol. 2. Eleven International Publishing The Hague.

[125] Vanessa Voigt, Raffael Wiethe, Chanakarn Sassmann, Moritz Will, Sarah Delgado Rodriguez, and Florian Alt. 2023. Safe Call: A Tangible Smartphone Interface That Supports Safe and Easy Phone Calls and Contacts Management for Older People. In *Proceedings of the 22nd International Conference on Mobile and Ubiquitous Multimedia (MUM '23)*. Association for Computing Machinery, New York, NY, USA, 562–564. https://doi.org/10.1145/3626705.3631878

[126] Wei Wang, Lin Yang, and Qian Zhang. 2016. Touch-and-guard: secure pairing through hand resonance. In *Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp '16)*. Association for Computing Machinery, New York, NY, USA, 670–681. https://doi.org/10.1145/2971648.2971688

[127] Catherine S. Weir, Gary Douglas, Martin Carruthers, and Mervyn Jack. 2009. User perceptions of security, convenience and usability for ebanking authentication tokens. *Computers & Security* 28, 1 (Feb. 2009), 47–62. https://doi.org/10.1016/j.cose.2008.09.008

[128] Catherine S. Weir, Gary Douglas, Tim Richardson, and Mervyn Jack. 2010. Usable security: User preferences for authentication methods in eBanking and the effects of experience. *Interacting with Computers* 22, 3 (May 2010), 153–164. https://doi.org/10.1016/j.intcom.2009.10.001 Conference Name: Interacting with Computers.

[129] Dirk Weirich and Martina Angela Sasse. 2001. Pretty Good Persuasion: A First Step towards Effective Password Security in the Real World. In *Proceedings of the 2001 Workshop on New Security Paradigms* (Cloudcroft, New Mexico) *(NSPW '01)*. Association for Computing Machinery, New York, NY, USA, 137–143. https://doi.org/10.1145/508171.508195

[130] Stephan Wensveen, Kees Overbeeke, Tom Djajadiningrat, and Steven Kyffin. 2004. Freedom of fun, freedom of interaction. *Interactions* 11, 5 (2004), 59–61.

[131] 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* (Washington, D.C.) *(SSYM'99)*. USENIX Association, USA, 14.

[132] Maximiliane Windl, Alexander Hiesinger, Robin Welsch, Albrecht Schmidt, and Sebastian S. Feger. 2022. SaferHome: Interactive Physical and Digital Smart Home Dashboards for Communicating Privacy Assessments to Owners and Bystanders. *Proc. ACM Hum.-Comput. Interact.* 6, ISS (Nov. 2022), 586:680–586:699. https://doi.org/10.1145/3567739

[133] Maximiliane Windl, Albrecht Schmidt, and Sebastian S. Feger. 2023. Investigating Tangible Privacy-Preserving Mechanisms for Future Smart Homes. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems (CHI '23)*. Association for Computing Machinery, New York, NY, USA, 1–16. https://doi.org/10.1145/3544548.3581167

[134] Jacob O. Wobbrock and Julie A. Kientz. 2016. Research Contributions in Human-Computer Interaction. *Interactions* 23, 3 (apr 2016), 38–44. https://doi.org/10.1145/2907069

[135] Claes Wohlin. 2014. Guidelines for snowballing in systematic literature studies and a replication in software engineering. In *Proceedings of the 18th International Conference on Evaluation and Assessment in Software Engineering* (London, England, United Kingdom) *(EASE '14)*. Association for Computing Machinery, New York, NY, USA, Article 38, 10 pages. https://doi.org/10.1145/2601248.2601268

[136] Zhenyu Yan, Qun Song, Rui Tan, Yang Li, and Adams Wai Kin Kong. 2019. Towards Touch-to-Access Device Authentication Using Induced Body Electric Potentials. In *The 25th Annual International Conference on Mobile Computing and Networking (MobiCom '19)*. Association for Computing Machinery, New York, NY, USA, 1–16. https://doi.org/10.1145/3300061.3300118

[137] Jeonghwa Yang and W. Keith Edwards. 2007. ICEbox: Toward Easy-to-Use Home Networking. In *Human-Computer Interaction – INTERACT 2007*, Cécilia Baranauskas, Philippe Palanque, Julio Abascal, and Simone Diniz Junqueira Barbosa (Eds.). Springer, Berlin, Heidelberg, 197–210. https://doi.org/10.1007/978-3-540-74800-7_15

[138] Yaxing Yao, Justin Reed Basdeo, Oriana Rosata Mcdonough, and Yang Wang. 2019. Privacy Perceptions and Designs of Bystanders in Smart Homes. *Proc. ACM Hum.-Comput. Interact.* 3, CSCW, Article 59 (Nov. 2019), 24 pages. https://doi.org/10.1145/3359161

[139] Affan Yasin, Lin Liu, Tong Li, Rubia Fatima, and Wang Jianmin. 2019. Improving software security awareness using a serious game. *IET Software* 13, 2 (2019), 159–169. https://doi.org/10.1049/iet-sen.2018.5095 _eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1049/iet-sen.2018.5095.

[140] Matej Zajc and Andreja Istenic Starcic. 2012. Potentials of the Tangible User Interface (TUI) in Enhancing Inclusion of People with Special Needs in the ICT-Assisted Learning and e-Accessibility. In *Agent and Multi-Agent Systems. Technologies and Applications*, Gordan Jezic, Mario Kusek, Ngoc-Thanh Nguyen, Robert J. Howlett, and Lakhmi C. Jain (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 261–270.
[141] Oren Zuckerman and Ayelet Gal-Oz. 2013. To TUI or not to TUI: Evaluating performance and preference in tangible vs. graphical user interfaces. *International Journal of Human-Computer Studies* 71, 7 (2013), 803–820. https://doi.org/10.1016/j.ijhcs.2013.04.003
[142] Mary Ellen Zurko and Richard T Simon. 1996. User-centered security. In *Proceedings of the 1996 workshop on New security paradigms*. 27–33.

A Initial Keyword-based Search

A.1 Applied Filtering Keys for the ACM Digitial Library

Table 8: Specified Level Concept IDs and Series Keys of ACM venues. See Appendix B for a glossary on venue acronyms.

venue	ACM SpecifiedLevelConceptID/ SeriesKey
CHI	*119596*
CSCW	*119481* and *pacmhci* + additional keyword *cscw*
CSCW	*119481*
UIST	*119271*
IUI	*119544*
ICMI	*120199*
CCS	*119372*
TEI	*119522*
AHs	*122392*
SOUPS	*118553*
MUM	*119644*
MuC	*122483*
MobileHCI	*119708* and *pacmhci* + additional keyword *mobilehci*
DIS	*119568*
NordiCHI	*119269*
OzCHI	*119294*
IMWUT	*imwut*
TOCHI	*tochi*

A.2 Descriptives of Search Results

Table 9: We initially conducted a keyword-based search for publications from 28 different venues. This table describes the results of this initial search. See Appendix B for a glossary on venue acronyms.

publication year		keywords		venues	
MIN	1980	tangible security	29	Computers & Security	431
MAX	1980	tangible privacy	37	CCS	129
		physical security	931	IEEE Security & Privacy	86
25% Quartille	1999	physical privacy	69	CHI	73
Median	2013	graspable security	0	USENIX Security	64
75% Quartille	2024	graspable privacy	0	Symposium on S&P	61
		haptic security	1	SOUPS	43
		haptic privacy	1	ESORICS	30
				CSCW	15
		—————		OzCHI	11
		Note that this categorization contains duplicated publications.		International Journal of Human-Computer Studies	11
				IMWUT	10
				BIT	10
				Interact	7
				TEI	6
				NordiCHI	6
				MUM	6
				PoPETS	6
				DIS	5
				UIST	3
				MobileHCI	3
				TOCHI	2
				HCII	2
				MuC	1

B Venue Acronyms

We provide a glossary of all venue acronyms.

B.1 Conferences

AHs Augmented Humans International Conference
CCS ACM Conference on Computer and Communications Security
CHI ACM Conference on Human Factors in Computing Systems
CSET Cyber Security for Energy & Transport Infrastructure International Conference
CSCW ACM SIGCHI Conference on Computer-Supported Cooperative Work & Social Computing
DIS ACM Conference on Designing Interactive Systems
ESORICS European Symposium on Research in Computer Security
FC Financial Cryptography and Data Security
UIST ACM Symposium on User Interface Software and Technology
IUI ACM Conference on Intelligent User Interfaces
HCII International Conference on Human-Computer Interaction (HCI International)
HRI ACM/IEEE International Conference on Human-Robot Interaction
ICBEA International Conference on Biomedical Engineering and Applications
ICMI ACM International Conference on Multimodal Interaction

Interact IFIP Conference on Human-Computer Interaction
MobiCom International Conference on Mobile Computing and Networking
MobileHCI ACM Conference on Human-Computer-Interaction with Mobile Devices and Services
MoMM International Conference on Advances in Mobile Computing & Multimedia Intelligence
MuC Mensch und Computer Conference
MUM International Conference on Mobile and Ubiquitous Multimedia
NDSS Network and Distributed System Security Symposium
NISK Norwegian Information Security Conference
NordiCHI Nordic Conference on Human-Computer Interaction
OzCHI Australian Conference on Human-Computer Interaction
PerCom International Conference on Pervasive Computing and Communications
RE Requirements Engineering
SAIS Southern Association for Information Systems Research Conference
SenSys ACM Conference on Embedded Networked Sensor Systems
SOUPS Symposium on Usable Privacy and Security
Symposium on S&P IEEE Symposium on Security and Privacy
TCHES IACR Transactions on Cryptographic Hardware and Embedded Systems
TEI International Conference on Tangible, Embedded, and Embodied Interaction
TOIT ACM Transactions on Internet Technology
TOPS ACM Transactions on Information and System Security
USENIX Security USENIX Security Symposium

B.2 Journals

BIT Behaviour & Information Technology
Computers & Security
IEEE Security & Privacy
IEEE Transactions on Software Engineering
IET Software
LNCS Lecture Notes in Computer Science
IMWUT ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies
Interacting with Computers
International Journal of Human-Computer Studies
PACMHCI Proceedings of the ACM on Human-Computer Interaction
Personal and Ubiquitous Computing
Personal Technologies
PoHFES Proceedings of the Human Factors and Ergonomics Society Annual Meeting
PoPETS Proceedings on Privacy Enhancing Technologies
ToCHI ACM Transactions on Computer-Human Interaction

B.3 Final Sample

B.4 Analyzed Publications

(1) [1] Abramova, S., & Böhme, R. (2023). Anatomy of a High-Profile Data Breach: Dissecting the Aftermath of a Crypto-Wallet Case. 715–732. https://www.usenix.org/conference/usenixsecurity23/presentation/abramova
(2) [2] Acemyan, C. Z., Kortum, P., Xiong, J., & Wallach, D. S. (2018). 2FA Might Be Secure, But It's Not Usable: A Summative Usability Assessment of Google's Two-factor Authentication (2FA) Methods. Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 62(1), 1141–1145. https://doi.org/10.1177/1541931218621262
(3) [6] Ahmad, I., Akter, T., Buher, Z., Farzan, R., Kapadia, A., & Lee, A. J. (2022). Tangible Privacy for Smart Voice Assistants: Bystanders' Perceptions of Physical Device Controls. Proc. ACM Hum.-Comput. Interact., 6(CSCW2), 364:1-364:31. https://doi.org/10.1145/3555089
(4) [7] Ahmad, I., Farzan, R., Kapadia, A., & Lee, A. J. (2020). Tangible Privacy: Towards User-Centric Sensor Designs for Bystander Privacy. Proc. ACM Hum.-Comput. Interact., 4(CSCW2), 116:1-116:28. https://doi.org/10.1145/3415187
(5) [8] Alsulaiman, F. A., Cha, J., & El Saddik, A. (2008). User Identification Based on Handwritten Signatures with Haptic Information. In M. Ferre (Ed.), Haptics: Perception, Devices and Scenarios (pp. 114–121). Springer. https://doi.org/10.1007/978-3-540-69057-3_12
(6) [10] Appel, A. W. (2011). Security Seals on Voting Machines: A Case Study. ACM Trans. Inf. Syst. Secur., 14(2), 18:1-18:29. https://doi.org/10.1145/2019599.2019603
(7) [12] Balfanz, D., Durfee, G., Grinter, R. E., Smetters, D. K., & Stewart, P. (2004). Network-in-a-Box: How to Set Up a Secure Wireless Network in Under a Minute. 13th USENIX Security Symposium (USENIX Security 04). https://www.usenix.org/conference/13th-usenix-security-symposium/network-box-how-set-secure-wireless-network-under-minute
(8) [13] Balogh, S., Daniel, T., Delgado Rodriguez, S., Prieto Romero, I., & Alt, F. (2022). Rubik's Cube Auth—A Tangible Authentication Mechanism Using A Standard Rubik's Cube. 10.18420/muc2022. https://dl.gi.de/handle/20.500.12116/39108
(9) [14] Beckers, K., & Pape, S. (2016). A Serious Game for Eliciting Social Engineering Security Requirements. 2016 IEEE 24th International Requirements Engineering Conference (RE), 16–25. https://doi.org/10.1109/RE.2016.39
(10) [15] Bianchi, A., Oakley, I., & Kwon, D. S. (2010). The secure haptic keypad: A tactile password system. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 1089–1092. https://doi.org/10.1145/1753326.1753488
(11) [16] Bianchi, A., Oakley, I., Lee, J. K., & Kwon, D. S. (2010). The haptic wheel: Design & evaluation of a tactile password system. CHI '10 Extended Abstracts on Human Factors in Computing Systems, 3625–3630. https://doi.org/10.1145/1753846.1754029
(12) [20] Chandrasekaran, V., Banerjee, S., Mutlu, B., & Fawaz, K. (2021). PowerCut and Obfuscator: An Exploration of the Design Space for Privacy-Preserving Interventions for Smart Speakers. 535–552. https://www.usenix.org/conference/soups2021/presentation/chandrasekaran
(13) [21] Chen, Y., Li, H., Teng, S.-Y., Nagels, S., Li, Z., Lopes, P., Zhao, B. Y., & Zheng, H. (2020). Wearable Microphone Jamming. Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems, 1–12. https://doi.org/10.1145/3313831.3376304
(14) [22] Cheng, Y.-T., Funk, M., Tsai, W.-C., & Chen, L.-L. (2019). Peekaboo Cam: Designing an Observational Camera for Home Ecologies Concerning Privacy. Proceedings of the 2019 on Designing Interactive Systems Conference, 823–836. https://doi.org/10.1145/3322276.3323699
(15) [26] Costanza, E., Inverso, S. A., Pavlov, E., Allen, R., & Maes, P. (2006). Eye-q: Eyeglass peripheral display for subtle intimate notifications. Proceedings of the 8th Conference on Human-Computer Interaction with Mobile Devices and Services, 211–218. https://doi.org/10.1145/1152215.1152261
(16) [28] Das, S., Dingman, A., & Camp, L. J. (2018). Why Johnny Doesn't Use Two Factor A Two-Phase Usability Study of the FIDO U2F Security Key. In S. Meiklejohn & K. Sako (Eds.), Financial Cryptography and Data Security (pp. 160–179). Springer. https://doi.org/10.1007/978-3-662-58387-6_9
(17) [29] De Cristofaro, E., Du, H., Freudiger, J., & Norcie, G. (2014). A Comparative Usability Study of Two-Factor Authentication. NDSS Symposium. Retrieved July 11, 2024, from https://www.ndss-symposium.org/ndss2014/ndss-2014-usec-programme/comparative-usability-study-two-factor-authentication/
(18) [30] De Luca, A., Frauendienst, B., Maurer, M., & Hausen, D. (2010). On the design of a "moody" keyboard. Proceedings of the 8th ACM Conference on Designing Interactive Systems, 236–239. https://doi.org/10.1145/1858171.1858213
(19) [33] Delgado Rodriguez, S., Mecke, L., & Alt, F. (2022). SenseHandle: Investigating Human-Door Interaction Behaviour for Authentication in the Physical World | USENIX. Retrieved July 11, 2024, from https://www.usenix.org/conference/soups2022/presentation/delgado-rodriguez-poster
(20) [35] Delgado Rodriguez, S., Prange, S., Knierim, P., Marky, K., & Alt, F. (2022). Experiencing Tangible Privacy Control for Smart Homes with PriKey. Proceedings of the 21st International Conference on Mobile and Ubiquitous Multimedia, 298–300. https://doi.org/10.1145/3568444.3570585
(21) [36] Delgado Rodriguez, S., Prange, S., Mecke, L., & Alt, F. (2024). Act2Auth – A Novel Authentication Concept based on Embedded Tangible Interaction at Desks. Proceedings of the Eighteenth International Conference on Tangible,

Embedded, and Embodied Interaction, 1–15. https://doi.org/10.1145/3623509.3633360
(22) [37] Delgado Rodriguez, S., Prange, S., Vergara Ossenberg, C., Henkel, M., Alt, F., & Marky, K. (2022). PriKey – Investigating Tangible Privacy Control for Smart Home Inhabitants and Visitors. Nordic Human-Computer Interaction Conference, 1–13. https://doi.org/10.1145/3546155.3546640
(23) [38] Denning, T., Lerner, A., Shostack, A., & Kohno, T. (2013). Control-Alt-Hack: The design and evaluation of a card game for computer security awareness and education. Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security, 915–928. https://doi.org/10.1145/2508859.2516753
(24) [41] Do, Y., Arora, N., Mirzazadeh, A., Moon, I., Xu, E., Zhang, Z., Abowd, G. D., & Das, S. (2023). Powering for Privacy: Improving User Trust in Smart Speaker Microphones with Intentional Powering and Perceptible Assurance. 2473–2490. https://www.usenix.org/conference/usenixsecurity23/presentation/do
(25) [42] Do, Y., Moon, S.-E., & Chang, M. (2022). ParaSight: Enabling Privacy-preserving Sensing Data Sharing via Device-to-device Utterance-based Communication. Extended Abstracts of the 2022 CHI Conference on Human Factors in Computing Systems, 1–6. https://doi.org/10.1145/3491101.3519757
(26) [43] Do, Y., Park, J. W., Wu, Y., Basu, A., Zhang, D., Abowd, G. D., & Das, S. (2022). Smart Webcam Cover: Exploring the Design of an Intelligent Webcam Cover to Improve Usability and Trust. Proc. ACM Interact. Mob. Wearable Ubiquitous Technol., 5(4), 154:1-154:21. https://doi.org/10.1145/3494983
(27) [45] Emami-Naeini, P., Agarwal, Y., Faith Cranor, L., & Hibshi, H. (2020). Ask the Experts: What Should Be on an IoT Privacy and Security Label? 2020 IEEE Symposium on Security and Privacy (SP), 447–464. https://doi.org/10.1109/SP40000.2020.00043
(28) [49] Frey, S., Rashid, A., Anthonysamy, P., Pinto-Albuquerque, M., & Naqvi, S. A. (2019). The Good, the Bad and the Ugly: A Study of Security Decisions in a Cyber-Physical Systems Game. IEEE Transactions on Software Engineering, 45(5), 521–536. IEEE Transactions on Software Engineering. https://doi.org/10.1109/TSE.2017.2782813
(29) [50] Futami, K., Fukao, A., & Murao, K. (2019). A method to recognize entering and leaving person based on door opening and closing movement using angular velocity sensor. Adjunct Proceedings of the 2019 ACM International Joint Conference on Pervasive and Ubiquitous Computing and Proceedings of the 2019 ACM International Symposium on Wearable Computers, 57–60. https://doi.org/10.1145/3341162.3343798
(30) [52] Gerhardt, D., Ponticello, A., Dabrowski, A., & Krombholz, K. (2023). Investigating Verification Behavior and Perceptions of Visual Digital Certificates. 3565–3582. https://www.usenix.org/conference/usenixsecurity23/presentation/gerhardt
(31) [53] Gondree, M., & Peterson, Z. N. J. (2013). Valuing Security by Getting [d0x3d!]: Experiences with a Network Security Board Game. 6th Workshop on Cyber Security Experimentation and Test (CSET 13). https://www.usenix.org/conference/cset13/workshop-program/presentation/gondree
(32) [54] Graffer, I., Bartnes, M., & Bernsmed, K. (2015, December 15). Play2Prepare: A Board Game Supporting IT Security Preparedness Exercises for Industrial Control Organizations. https://api.semanticscholar.org/CorpusID:55543977
(33) [55] Greenberg, S., & Kuzuoka, H. (1999). Using digital but physical surrogates to mediate awareness, communication and privacy in media spaces. Personal Technologies, 3(4), 182–198. https://doi.org/10.1007/BF01540552
(34) [56] Gunson, N., Marshall, D., Morton, H., & Jack, M. (2011). User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking. Computers & Security, 30(4), 208–220. https://doi.org/10.1016/j.cose.2010.12.001
(35) [57] Gupta, S., Buriro, A., & Crispo, B. (2019). SmartHandle: A Novel Behavioral Biometric-based Authentication Scheme for Smart Lock Systems. Proceedings of the 2019 3rd International Conference on Biometric Engineering and Applications, 15–22. https://doi.org/10.1145/3345336.3345344
(36) [58] Harbach, M., Fahl, S., Rieger, M., & Smith, M. (2013). On the Acceptance of Privacy-Preserving Authentication Technology: The Curious Case of National Identity Cards. In E. De Cristofaro & M. Wright (Eds.), Privacy Enhancing Technologies (pp. 245–264). Springer. https://doi.org/10.1007/978-3-642-39077-7_13
(37) [59] Hart, S., Margheri, A., Paci, F., & Sassone, V. (2020). Riskio: A Serious Game for Cyber Security Awareness and Education. Computers & Security, 95, 101827. https://doi.org/10.1016/j.cose.2020.101827
(38) [60] Hayashi, E., Pendleton, B., Ozenc, F., & Hong, J. (2012). WebTicket: Account management using printable tokens. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 997–1006. https://doi.org/10.1145/2207676.2208545
(39) [66] Immler, V., Obermaier, J., Ng, K. K., Ke, F. X., Lee, J., Lim, Y. P., Oh, W. K., Wee, K. H., & Sigl, G. (2019). Secure Physical Enclosures from Covers with Tamper-Resistance. IACR Transactions on Cryptographic Hardware and Embedded Systems, 51–96. https://doi.org/10.13154/tches.v2019.i1.51-96
(40) [69] Jedrzejczyk, L., Price, B. A., Bandara, A., & Nuseibeh, B. (2010). "Privacy-shake",: A haptic interface for managing privacy settings in mobile location sharing applications. Proceedings of the 12th International Conference on Human Computer Interaction with Mobile Devices and Services, 411–412. https://doi.org/10.1145/1851600.1851690
(41) [70] Jin, H., Guo, B., Roychoudhury, R., Yao, Y., Kumar, S., Agarwal, Y., & Hong, J. I. (2022). Exploring the Needs of Users for Supporting Privacy-Protective Behaviors in Smart Homes. Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems, 1–19. https://doi.org/10.1145/3491102.3517602
(42) [71] Kim, N., Kim, J., Kim, B., & Park, Y.-W. (2021). The Trial of Posit in Shared Offices: Controlling Disclosure Levels of Schedule Data for Privacy by Changing the Placement of a Personal Interactive Calendar. Proceedings of the 2021 ACM Designing Interactive Systems Conference, 149–159. https://doi.org/10.1145/3461778.3462073
(43) [72] Krol, K., Philippou, E., De Cristofaro, E., & Sasse, A. (2015). "They brought in the horrible key ring thing!" Analysing the Usability of Two-Factor Authentication in UK Online Banking. NDSS Symposium. Retrieved July 11, 2024, from https://www.ndss-symposium.org/ndss2015/ndss-2015-usec-programme/they-brought-horrible-key-ring-thing-analysing-usability-two-factor-authentication-uk-online/
(44) [74] Lang, J., Czeskis, A., Balfanz, D., Schilder, M., & Srinivas, S. (2017). Security Keys: Practical Cryptographic Second Factors for the Modern Web. In J. Grossklags & B. Preneel (Eds.), Financial Cryptography and Data Security (pp. 422–440). Springer. https://doi.org/10.1007/978-3-662-54970-4_25
(45) [76] Li, X., Zeng, Q., Luo, L., & Luo, T. (2020). T2Pair: Secure and Usable Pairing for Heterogeneous IoT Devices. Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security, 309–323. https://doi.org/10.1145/3372297.3417286
(46) [79] Little, L., Briggs, P., & Coventry, L. (2005). Public space systems: Designing for privacy? International Journal of Human-Computer Studies, 63(1), 254–268. https://doi.org/10.1016/j.ijhcs.2005.04.018
(47) [81] Maqsood, S., Chiasson, S., & Girouard, A. (2016). Bend Passwords: Using gestures to authenticate on flexible devices. Personal Ubiquitous Comput., 20(4), 573–600. https://doi.org/10.1007/s00779-016-0928-6
(48) [82] Marky, K., Schmitz, M., Zimmermann, V., Herbers, M., Kunze, K., & Mühlhäuser, M. (2020). 3D-Auth: Two-Factor Authentication with Personalized 3D-Printed Items. Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems, 1–12. https://doi.org/10.1145/3313831.3376189
(49) [87] Mehta, V., Bandara, A. K., Price, B. A., & Nuseibeh, B. (2016). Privacy Itch and Scratch: On Body Privacy Warnings and Controls. Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems, 2417–2424. https://doi.org/10.1145/2851581.2892475
(50) [89] Mehta, V., Bandara, A. K., Price, B. A., Nuseibeh, B., & Gooch, D. (2021). Up Close & Personal: Exploring User-preferred Image Schemas for Intuitive Privacy Awareness and Control. Proceedings of the Fifteenth International Conference on Tangible, Embedded, and Embodied Interaction, 1–13. https://doi.org/10.1145/3430524.3440626
(51) [90] Mehta, V., Gooch, D., Bandara, A., Price, B. A., & Nuseibeh, B. (2023). A Card-based Ideation Toolkit to Generate Designs for Tangible Privacy Management Tools. Proceedings of the Seventeenth International Conference on Tangible, Embedded, and Embodied Interaction, 1–13. https://doi.org/10.1145/3569009.3572903
(52) [89] Mehta, V., Gooch, D., Bandara, A., Price, B., & Nuseibeh, B. (2021). Privacy Care: A Tangible Interaction Framework for Privacy Management. ACM Trans. Internet Technol., 21(1), 25:1-25:32. https://doi.org/10.1145/3430506
(53) [94] Möllers, M., Bohnenberger, R., Deininghaus, S., Zimmer, P., Herrmann, K., & Borchers, J. (2011). TaPS Widgets: Tangible control over private spaces on interactive tabletops. CHI '11 Extended Abstracts on Human Factors in Computing Systems, 773–780. https://doi.org/10.1145/1979742.1979632
(54) [91] Moskowitz, P. A., Lauris, A., & Morris, S. S. (2007). A Privacy-Enhancing Radio Frequency Identification Tag: Implementation of the Clipped Tag. 348–351. https://doi.org/10.1109/PERCOMW.2007.11
(55) [92] Mott, M., Donahue, T., Poor, G. M., & Leventhal, L. (2012). Leveraging motor learning for a tangible password system. CHI '12 Extended Abstracts on Human Factors in Computing Systems, 2597–2602. https://doi.org/10.1145/2212776.2223842
(56) [93] Murao, K., Tobise, H., Terada, T., Iso, T., Tsukamoto, M., & Horikoshi, T. (2014). Mobile Phone User Authentication with Grip Gestures using Pressure Sensors. Proceedings of the 12th International Conference on Advances in Mobile Computing and Multimedia, 143–146. https://doi.org/10.1145/2684103.2684116
(57) [95] Nanda, A., Jeong, J. J., Shah, S. W. A., Nosouhi, M., & Doss, R. (2024). Examining usable security features and user perceptions of Physical Authentication Devices. Computers & Security, 139, 103664. https://doi.org/10.1016/j.cose.2023.103664
(58) [99] Portnoff, R. S., Lee, L. N., Egelman, S., Mishra, P., Leung, D., & Wagner, D. (2015). Somebody's Watching Me? Assessing the Effectiveness of Webcam

Indicator Lights. Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems, 1649–1658. https://doi.org/10.1145/2702123.2702164

(59) [101] Reese, K., Smith, T., Dutson, J., Armknecht, J., Cameron, J., & Seamons, K. (2019). A Usability Study of Five Two-Factor Authentication Methods. 357–370. https://www.usenix.org/conference/soups2019/presentation/reese

(60) [102] Rekimoto, J., Ayatsuka, Y., Kohno, M., & Oba, H. (2003). Proximal Interactions: A Direct Manipulation Technique for Wireless Networking. IFIP TC13 International Conference on Human-Computer Interaction. https://www.semanticscholar.org/paper/Proximal-Interactions%3A-A-Direct-Manipulation-for-Rekimoto-Ayatsuka/cf9644103b94af4bcaf13cda5b07d6dcf8da9c6a

(61) [103] Reynolds, J., Smith, T., Reese, K., Dickinson, L., Ruoti, S., & Seamons, K. (2018). A Tale of Two Studies: The Best and Worst of YubiKey Usability. 2018 IEEE Symposium on Security and Privacy (SP), 872–888. https://doi.org/10.1109/SP.2018.00067

(62) [106] Rueben, M., Bernieri, F. J., Grimm, C. M., & Smart, W. D. (2016). User feedback on physical marker interfaces for protecting visual privacy from mobile robots. 2016 11th ACM/IEEE International Conference on Human-Robot Interaction (HRI), 507–508. https://doi.org/10.1109/HRI.2016.7451829

(63) [107] Sasamoto, H., Christin, N., & Hayashi, E. (2008). Undercover: Authentication usable in front of prying eyes. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 183–192. https://doi.org/10.1145/1357054.1357085

(64) [111] Sharif, M., Bhagavatula, S., Bauer, L., & Reiter, M. K. (2016). Accessorize to a Crime: Real and Stealthy Attacks on State-of-the-Art Face Recognition. Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, 1528–1540. https://doi.org/10.1145/2976749.2978392

(65) [113] Song, Y., Huang, Y., Cai, Z., & Hong, J. I. (2020). I'm All Eyes and Ears: Exploring Effective Locators for Privacy Awareness in IoT Scenarios. Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems, 1–13. https://doi.org/10.1145/3313831.3376585

(66) [115] Staat, P., Tobisch, J., Zenger, C., & Paar, C. (2022). Anti-Tamper Radio: System-Level Tamper Detection for Computing Systems. 2022 IEEE Symposium on Security and Privacy (SP), 1722–1736. https://doi.org/10.1109/SP46214.2022.9833631

(67) [117] Strouble, D., Shechtman, G., & Alsop, A. (2009). Productivity and Usability Effects of Using a Two-Factor Security System. SAIS 2009 Proceedings. https://aisel.aisnet.org/sais2009/37

(68) [118] Sun, K., Chen, C., & Zhang, X. (2020). "Alexa, stop spying on me!": Speech privacy protection against voice assistants. Proceedings of the 18th Conference on Embedded Networked Sensor Systems, 298–311. https://doi.org/10.1145/3384419.3430727

(69) [119] Teyssier, M., Koelle, M., Strohmeier, P., Fruchard, B., & Steimle, J. (2021). Eyecam: Revealing Relations between Humans and Sensing Devices through an Anthropomorphic Webcam. Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems, 1–13. https://doi.org/10.1145/3411764.3445491

(70) [120] Tiefenau, C., Häring, M., Gerlitz, E., & Zezschwitz, E. (2019). Making Privacy Graspable: Can we Nudge Users to use Privacy Enhancing Techniques?

(71) [122] van Koningsbruggen, R., Hengeveld, B., & Alexander, J. (2021). Understanding the Design Space of Embodied Passwords based on Muscle Memory. Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems, 1–13. https://doi.org/10.1145/3411764.3445773

(72) [125] Voigt, V., Wiethe, R., Sassmann, C., Will, M., Rodriguez, S. D., & Alt, F. (2023). Safe Call: A Tangible Smartphone Interface That Supports Safe and Easy Phone Calls and Contacts Management for Older People. Proceedings of the 22nd International Conference on Mobile and Ubiquitous Multimedia, 562–564. https://doi.org/10.1145/3626705.3631878

(73) [126] Wang, W., Yang, L., & Zhang, Q. (2016). Touch-and-guard: Secure pairing through hand resonance. Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing, 670–681. https://doi.org/10.1145/2971648.2971688

(74) [127] Weir, C. S., Douglas, G., Carruthers, M., & Jack, M. (2009). User perceptions of security, convenience and usability for ebanking authentication tokens. Computers & Security, 28(1), 47–62. https://doi.org/10.1016/j.cose.2008.09.008

(75) [128] Weir, C. S., Douglas, G., Richardson, T., & Jack, M. (2010). Usable security: User preferences for authentication methods in eBanking and the effects of experience. Interacting with Computers, 22(3), 153–164. Interacting with Computers. https://doi.org/10.1016/j.intcom.2009.10.001

(76) [132] Windl, M., Hiesinger, A., Welsch, R., Schmidt, A., & Feger, S. S. (2022). SaferHome: Interactive Physical and Digital Smart Home Dashboards for Communicating Privacy Assessments to Owners and Bystanders. Proc. ACM Hum.-Comput. Interact., 6(ISS), 586:680-586:699. https://doi.org/10.1145/3567739

(77) [133] Windl, M., Schmidt, A., & Feger, S. (2023). Investigating Tangible Privacy-Preserving Mechanisms for Future Smart Homes. Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems, 1–16. https://doi.org/10.1145/3544548.3581167

(78) [136] Yan, Z., Song, Q., Tan, R., Li, Y., & Kong, A. W. K. (2019). Towards Touch-to-Access Device Authentication Using Induced Body Electric Potentials. The 25th Annual International Conference on Mobile Computing and Networking, 1–16. https://doi.org/10.1145/3300061.3300118

(79) [137] Yang, J., & Edwards, W. K. (2007). ICEbox: Toward Easy-to-Use Home Networking. In C. Baranauskas, P. Palanque, J. Abascal, & S. D. J. Barbosa (Eds.), Human-Computer Interaction – INTERACT 2007 (pp. 197–210). Springer. https://doi.org/10.1007/978-3-540-74800-7_15

(80) [139] Yasin, A., Liu, L., Li, T., Fatima, R., & Jianmin, W. (2019). Improving software security awareness using a serious game. IET Software, 13(2), 159–169. https://doi.org/10.1049/iet-sen.2018.5095

B.5 Overview Table of Analyzed Publications per Venue or Per Year

Table 10: Overview tables showing the number of analyzed publications per venue and per year. The total amount of analyzed publications is 80.

(a) Publications per Venue

venue	search	snowball	both
CHI	7	9	16
USENIX Security	4	0	4
SOUPS	1	3	4
Computers & Security	2	2	4
IMWUT	1	2	3
TEI	3	0	3
CCS	3	0	3
DIS	1	2	3
IEEE Symposium on S&P	2	0	2
CSCW	2	0	2
FC	0	2	2
Interact	1	1	2
NDSS	0	2	2
MobileHCI	0	2	2
MUM	2	0	2
HRI	0	1	1
PoHFES	0	1	1
PoPETS	0	1	1
RE	0	1	1
CSET	0	1	1
SAIS	0	1	1
Personal Technologies	0	1	1
SenSys	0	1	1
TCHES	0	1	1
TOIT	0	1	1
TOPS	0	1	1
Personal and Ubiquitous Computing	0	1	1
NISK	0	1	1
PerCom	0	1	1
PACMHCI	0	1	1
NordiCHI	1	0	1
ICBEA	0	1	1
MuC	0	1	1
MoMM	0	1	1
LNCS	0	1	1
International Journal of Human-Computer Studies	1	0	1
Interacting with Computers	0	1	1
IET Software	0	1	1
IEEE Transactions on Software Engineering	0	1	1
IEEE Security & Privacy	0	1	1
MobiCom	0	1	1

Table 11: Publications per year

year	search	snowball	both
1999	0	1	1
2003	0	1	1
2004	1	0	1
2005	1	0	1
2006	0	1	1
2007	1	1	2
2008	0	2	2
2009	0	2	2
2010	0	5	5
2011	1	2	3
2012	1	1	2
2013	1	2	3
2014	0	2	2
2015	0	3	3
2016	2	5	7
2018	0	3	3
2019	1	8	9
2020	4	4	8
2021	4	3	7
2022	6	3	9
2023	7	0	7
2024	1	0	1

C Definition of the Technology Readiness Level

Table 12: Technology readiness level (TRL) as defined by the European Commission [24, 25]

level	general description [25]	exemplary description for software/hardware [24]
TLR 1	basic principles observed	Define basic properties: Scientific research that is translated into applied activity, having paper studies of basic properties.
TLR 2	technology concept formulated	Analytical study: The resulted applications are mainly speculative, with no proof of concepts to support assumptions. At this level, technology is limited to analytical studies.
TLR 3	experimental proof of concept	Proof of concept: Active R&D activities, including analytical and laboratory studies to physically validate the previous analytical predictions and assumptions. the first proof of concept.
TLR 4	technology validated in lab	Pre-prototype: The resulting system integrates basic technological components that work together in a low fidelity compared with the eventual system. This "ugly prototype" or "pre-prototype" includes integration of ad hoc hardware in the laboratory environment
TLR 5	technology validated in relevant environment (industrially relevant environment in the case of key enabling technologies)	Pre-prototype tested in lab: Integration of components with reasonable and realistic supporting elements for testing in a simulated environment. High fidelity is achieved in laboratory.
TLR 6	technology demonstrated in relevant environment (industrially relevant environment in the case of key enabling technologies)	Prototype tested in relevant environment: The technology is tested in a relevant environment. It starts to be considered as a representative prototype to be tested in a high-fidelity laboratory environment or in a simulated operational environment
TLR 7	system prototype demonstration in operational environment	Approved prototype: Testing is moved to operational environments such as a vehicle or machines. This is the first fully approved prototype
TLR 8	system complete and qualified	Pre-serial manufacturing: Technology is proven to work in its final form and under expected operational conditions. Tests and evaluation of the system are made in its intended or pre-production configuration. Design specifications, including quality and safety conditions along with operational suitability are evaluated. At this stage pre-serial manufacturing is intended to overcome any future mass production issues.
TLR 9	actual system proven in operational environment (competitive manufacturing in the case of key enabling technologies; or in space)	Product on market: Technology is shaped in its actual application, meeting production configuration and under real conditions such as those identified during operational tests and evaluation.