"If HTTPS Were Secure, I Wouldn't Need 2FA"- End User and Administrator Mental Models of HTTPS

Katharina Krombholz
CISPA Helmholtz Center for Information Security

Karoline Busse
Bonn University

Katharina Pfeffer
SBA Research

Matthew Smith
Bonn University
FhG FKIE

Emanuel von Zezschwitz
Bonn University
FhG FKIE

***Abstract*—HTTPS is one of the most important protocols used to secure communication and is, fortunately, becoming more pervasive. However, especially the long tail of websites is still not sufficiently secured. HTTPS involves different types of users, e.g., end users who are forced to make security decisions when faced with warnings or administrators who are required to deal with cryptographic fundamentals and complex decisions concerning compatibility.**

In this work, we present the first qualitative study of both end user and administrator mental models of HTTPS. We interviewed 18 end users and 12 administrators; our findings reveal misconceptions about security benefits and threat models from both groups. We identify protocol components that interfere with secure configurations and usage behavior and reveal differences between administrator and end user mental models.

Our results suggest that end user mental models are more conceptual while administrator models are more protocol-based. We also found that end users often confuse encryption with authentication, significantly underestimate the security benefits of HTTPS. They also ignore and distrust security indicators while administrators often do not understand the interplay of functional protocol components. Based on the different mental models, we discuss implications and provide actionable recommendations for future designs of user interfaces and protocols.

I. Introduction

In the context of information technologies, protecting communication content at large scale has become more important than ever before. Almost twenty years after Whitten and Tygar's usability evaluation of PGP [1], reliable encryption still cannot be taken for granted even though adoption rates are growing [2]. In today's Internet ecosystem, HTTPS is the fundamental cryptographic protocol to secure information in transit and to ensure data integrity and privacy between two communicating parties. However, HTTPS is still not the default for all websites, especially when it comes to the long tail of websites [2], [3]. At the time of writing, Internet-wide scans from SSLPulse suggest that 36,3% of sites surveyed still have inadequate security[1]. Recent studies, e.g., by Krombholz et al. [4], show that this is, among other reasons, due to the fact that the deployment of cryptographic protocols is a difficult task even for knowledgeable users. Similar to message encryption, HTTPS confronts different types of (mostly technically adept) users with cryptographic algorithms and protocols which they do not fully understand – see, e.g., Krombholz et al. [4], Green and Smith [5], Acer et al.[3], Fahl et al. [6], Oltrogge et al. [7], and Reeder et al. [8]. In addition, users who are exposed to poorly configured sites are forced to make security-critical decisions and are often not aware of the respective consequences.

We argue that we still do not understand *why* these carefully designed protocols do not meet the needs of (knowledgeable) users to securely operate cryptographic applications. Therefore, this work employs an inductive approach to learn about the root causes for user misconceptions by formalizing mental models of end users and administrators. In particular, we focus on how users think that HTTPS works and against which types of attackers they think they are protected. By doing so, we get a detailed understanding of which knowledge gaps have to be filled in future protocol designs. We thereby contribute a qualitative study with 18 end users and 12 experienced administrators; our findings reveal interesting differences in the mental models of these two distinct user groups.

We found that many non-expert participants significantly underestimate the level of protection that HTTPS offers, whereas administrators generally have a good understanding of what HTTPS can or cannot protect against. We also discovered that most administrators have little conceptual knowledge of how the protocol works but are very familiar with the different steps of establishing a communication. Key elements are often considered as blackboxes and poorly understood. We further found that the distinction between authentication and encryption is unclear to many users–even to some experts. Based on our findings, we identified protocol components that diverge from user mental models and discuss implications and potential countermeasures.

The goal of this paper is to derive and compare mental models in order to understand if and how they deviate from the underlying functionality of HTTPS and their impact on security. The main contributions of this paper are as follows:

We conducted an in-depth qualitative study with $n = 30$ participants to **formalize user mental models** and **threat models** and to **understand users' perceptions, attitudes and misconceptions of how HTTPS works**. By focusing on

[1]https://www.ssllabs.com/ssl-pulse/, Accessed: 10/30/2018

different scenarios and studying two distinct groups of users, namely **end users and system administrators**, we were able to reveal group-specific differences.

II. Related Work

In this section, we examine related works on HTTPS/SSL/TLS from both the expert and non-expert user's perspective, message encryption, and mental model studies.

A. HTTPS From the Expert Users' Perspective

Krombholz et al. [4] identified major challenges in HTTPS deployment from an administrator's perspective and showed that the procedure is too complex. They identified usability issues and protocol components that are difficult to understand even for knowledgeable users who managed to deploy valid configurations. The results from Krombholz et al. [4] also suggest that administrators rely heavily on online sources and that the quality of these resources often leads to faulty implementation. Acar et al. [9] showed that this is also the case for API documentations, which influence code performance and security. Their findings suggest simplifying interfaces, providing more support for a broad range of tasks, and giving code examples to promote effective security in applications. These API documentations are among the primary sources that construct mental models.

Fahl et al. [10] studied reasons for webmasters to misconfigure security-critical X.509 certificates which do not validate on their website. They found that one third accidentally misconfigured those certificates and two thirds explained why they deliberately used non-validating certificates. Oltrogge et al. [7] studied the applicability of pinning for non-browser software and implemented a web-application to support the deployment of pining-protected TLS implementations. Manousis et al. [11] found that only 50% of the domains with Let's Encrypt certificates actually responded with a valid LE certificate on the standard HTTPS port which indicates that even automation does not obviate the need for administrators to deal with the complexity of the protocol, resulting in serious misconfigurations.

While these works [4], [10], [7] identified specific (protocol-related) tasks that are not sufficiently understood by knowledgeable users such as administrators and developers, they did not show *how* they are actually understood. Based on their findings, we measure user mental models to detect reasons for inadequately secured configurations and security misbehavior.

B. HTTPS From the End Users' Perspective

To ensure a safe usage of the HTTPS infrastructure, SSL warnings and connection security indicators serve as primary interaction components for end users. Related work in our field has significantly contributed to improving these UI components; Sunshine et al. [12] conducted the first study on the effectiveness on browser warnings. Harbach et al. [13] studied how linguistic properties influence the perceived difficulty of warning messages. Akhawe et al. [14] focused on the (in)effectiveness of different security warnings in browsers, which are strongly correlated to user experiences. Weber et al. [15] used participatory design to improve security warnings. Felt et al. [16] studied differences of SSL warnings between Google Chrome and Mozilla Firefox along with click-through rates. As a follow-up, Felt et al. [17] introduced new SSL warnings, which helped 30% of the tested users to stay safe. Those opinionated design-based warnings were released by Google Chrome. To provide users with further visual feedback, they proposed a new set of browser security indicators for HTTPS security in Google Chrome [18] based on a user study with 1,329 participants.

Even though adherence rates have improved, they could still be much higher. Reeder et al. [8] explored reasons for low adherence rates and misconceptions about browser warnings. They identified contextual misunderstandings that influence users in clicking through warnings and found that users are inconsistent in their perceptions and security assessments.

Acer et al. [3] studied over 2,000 Google Chrome browsing errors and classified their root causes. They showed that the majority of errors were caused on the client-side or by network issues and proposed mitigation for spurious certificate warnings. Chothia et al. [19] presented a security analysis of TLS used in UK banking apps that emphasized the importance of security by revealing privacy and security flaws.

Our work extends the state of the art by studying *how* connection indicators, warnings, and other UI cues contribute to the formation of valid mental models and perceptions of how to operate the system in the most secure manner. While related work has significantly improved security indicators and warnings and thus improved adherence rates, our results suggest that these UX components do not necessarily establish trust among end users.

C. Message Encryption

Already in 1999 Whitten and Tygar [1] had found that user interfaces for security applications need different usability standards to be effective. This led to a series of other studies, especially as messaging encryption became popular.

Fahl et al. [20] conducted a screening study on the usability of the message security of Facebook. Based on their findings that automatic key management and key recovery capabilities are important, they implemented a usable, service-based encryption mechanism. The effect of integration and transparency on users' trust was examined by Atwater et al. [21] and indicated that users have a stronger confidence in desktop applications and integrated encryption software than others. Different Instant Messaging applications were evaluated concerning their usability by Herzberg et al. [22], Schroder et al. [23], and Vaziripour et al. [24], concluding that the security mechanisms are impractical due to incorrect mental models, a lack of understanding, and usability problems.

Secure email exchange is desired by many users. However, as found by Ruoti et al. [25], the time component detains regular usage since simultaneous users are unsure at which point in time they use encrypted emails. Lerner et al. [26]

introduced a prototype for encrypting emails with Keybase for automatic key management and showed that lawyers and journalists were able to efficiently send encrypted e-mails with few errors. However, the operational constraints differ, and there is no one-size-fits-all solution.

Abu-Salma et al. [27] studied users' perceptions of secure communication tools and reasons for not adopting them, and revealed misconceptions of encryption concepts in users' mental models.

D. Mental Models

Users' mental models influence their behaviour and reactions in certain situations. Wash et al. [28] proposed a way to shape the mental models of non-experts to encourage security behavior irrespective of the users' technical understanding. Bravo-Lillo et al. [29] studied how users perceive and respond to security alerts. Renaud et al. [30] found that incomplete threat models, misaligned incentives, and a general absence of understanding of the email architecture lead to non-adoption of end-to-end encryption for emails. Oates et al. [31] explored mental models of privacy, and Wu et al. [32] explored end user mental models of encryption. Abu Salma et al. [33] quantified mental models and misconceptions of a hypothetical encrypted communication tool and found a large percentage of users underestimate the security benefits of E2E encrypted tools. Kang et al. [34] measured mental models about the Internet and its privacy and security challenges. Based on their findings, they proposed systems and policies which do not rely on the knowledge of users. Gallagher et al. [35] conducted a study with experts and non-experts on their mental models of the Tor network and found severe gaps in their knowledge which could lead to deanonymization. Zeng et al. [36] studied user understanding of smart-home technologies and revealed mismatches in users threat models compared to reality. Related works on mental models revealed severe misconceptions with respect to message encryption or specific tools. We replicate and confirm some conceptual misunderstandings on message encryption and extend the state of the art by investigating mental models of transport layer security from the end users' and administrators' perspective. In comparison to message encryption, especially, the configuration of the protocol from an administrators' perspective is complex and has a severe impact on the security of the Internet ecosystem.

III. Methodology

In the following, we describe our research questions and how we address them, i.e., the study design and procedure of our semi-structured interviews, recruitment, participants, and how we finally analyzed the resulting data. Our goal is to understand why end users and administrators make mistakes when using or configuring HTTPS that result in security-critical situations. Our approach is to construct theories by means of identification of patterns in the data [37] (inductive approach), which is why we opted for a qualitative interview study with a diverse sample of participants. In particular, we sought to answer the following research questions:

- What are people's expectations and perceptions of encryption and visiting sites via HTTPS?
- How well do users understand the associated threat models?
- What are the differences between end users' and administrators' mental models of HTTPS?

A. Study Design and Procedure

Kearney et al. [38] showed that humans commonly possess *tacit knowledge* about technology, i.e., superficial knowledge, of which they are not aware and which they cannot easily articulate. Nevertheless, this tacit knowledge determines people's decisions and responses to new situations. Our study is designed in a way that it supports participants in exploring and reporting their tacit knowledge by externalizing it. Based on related work on HTTPS usability, e.g., [4], [18], [2] and recent mental model studies from usable security, e.g., [34], [35], [36], [28], [30] we constructed an interview guideline for semi-structured interviews including a three-part drawing task and a short questionnaire with closed-ended questions covering demographics and questions on the participants' online communication behavior. The complete study material can be found in the Appendix, including the screening questionnaire in Section B and the interview guideline in Section C. Twenty-seven interviews were conducted in person in three different cities in Austria and Germany, namely Vienna, Bonn, and Hannover. The participants were invited to a quiet room at one of our labs or at a local hackerspace. In addition, three interviews were conducted via Skype.

All participants were informed about the purpose of the study and then signed a consent form. Then, depending on whether a participant was classified as end user or administrator, they were presented a questionnaire. After completion of the questionnaire, the main part of the study–namely the interview with the drawing tasks–was conducted. In order to elicit articulations and visualization of user mental models, the participants were guided through three drawing tasks based on different scenarios and asked to verbalize their thought process as they drew, consistent with traditional think aloud protocols [39]. The scenarios were (1) a general scenario of sending an encrypted message to a communication partner, (2) online shopping via HTTPS, and (3) online banking.

All but one interview were recorded after the participants gave their written consent. In addition to the audio recordings, the interviewers took notes.

Contrary to quantitative research, where the appropriate sample size can be determined by power calculations, the sample size in qualitative research is determined by the point at which no new themes or ideas emerge from the data. This metric is also referred to as saturation [40]. We conducted interviews until we reached saturation. As the sample of end users was more diverse in terms of demographics, education and technical experience (assessed in the screening questionnaire), a larger sample was required to reach saturation in comparison to the administrator sample. We validated our

study design with pilot interviews and a post-hoc validity study.

B. Expectations on User Mental Models

While our scientific principles encourage us to evaluate results from a neutral, non-involved standpoint, researchers introduce their own individual biases and preconceptions. To make these personal influences more transparent, we discussed a series of expectations on mental models prior to analyzing the data. We argue that mental models of both types of users are constructed based on the protocols and UX with which they interact. We therefore expected these components to be essential parts of their mental models. Mental models are also influenced by media articles, education, experience, and other factors. As we cannot isolate these factors, we do not build our expectations on them.

Consequently, we assumed security indicators (e.g., the https prefix or the padlock icon) as part of end user mental models. We did not expect deep knowledge about encryption concepts and keys, e.g., we did not expect awareness for metadata from end users or an understanding about additional network nodes. While all researchers agreed that end users should not confuse encryption with authentication, we did not agree on whether the absence of a centralized encryption component can be expected from end users.

We expected more in-depth knowledge from administrators, e.g., knowledge about symmetric and asymmetric encryption. We also expected keys, certificates, and certificate authorities to be components of their mental models. We also assumed that their tacit knowledge on data transport routes would contain intermediary nodes in the network. We expected more sophisticated threat models and awareness of metadata.

C. Pilot Interviews

Before the actual study, we conducted a series of pilot interviews, four in Vienna and two in Bonn. The first version of the interview guideline had only two different drawing tasks (message encryption in theory and visiting a site with HTTPS). As the results from our pilot interviews suggest, this was not enough to elicit a detailed articulation of the participants' mental models. We therefore decided to include a third drawing task (i.e., visiting an online banking site) that, from a technical perspective, presents a similar scenario but is often understood as a more security-critical task. Our results also suggested minor modifications to the order of questions.

D. Recruitment and Participants

In total, we recruited 45 participants. Since the first six and the last nine interviews were used for the pilot study and for the validation of the results, we excluded them from the final data set and thus had a final set of 30 participants, consisting of 18 end users and 12 administrators, respectively.

For the non-expert users, our goal was to recruit a diverse sample of participants. Hence, we used three separate recruiting mechanisms to build our sample: mailing lists, online forums, and personal contacts for recruitment. We especially limited the number of students in our sample and refrained from recruiting computer science students or IT professionals.

In contrast, the recruitment criteria for administrators was that they had to be in charge of administering systems and regularly-used services. We allowed both paid and voluntary work.

To recruit administrators, we contacted companies' IT departments directly (e.g. national newspapers) or used personal contacts as entry points to larger organizations and asked them to forward the announcement to their employers' IT department. Five administrators were recruited over this channel. Additionally, we posted advertisements on social media and a hackerspace mailing list to recruit another seven administrators. Sadly, we were unable to recruit female or non-binary administrators. Table III lists information of our participants. Table I presents a summary of demographics.

Table II summarizes the administrators' previous work experience and security-specific education. Four of the 12 administrators reported that they never received any security-specific education. Four administrators were employed at IT service providers, two at national newspapers, and the remaining ones were administrating servers in the fields of data protection, social services, advertisement, mobility, radio and television, and education. Eleven administrators were full-time administrators at a company, and one was voluntarily administrating at a non-profit organization.

The recruitment text did not include information on the actual purpose of the study in order to prevent the participants from informing themselves about HTTPS before participation. All participants were compensated with 10 Euros for their time.

TABLE I
PARTICIPANT DEMOGRAPHICS. TOTAL $N = 30$;

Demographic	**End users** $N_{End} = 18$	**Administrators** $N_{Admin} = 12$
Gender		
Male	7 (39%)	12 (100%)
Female	11 (61%)	0 (0%)
No Information	0 (0%)	0 (0%)
Age		
Min.	24	29
Max.	60	42
Median	28	34
Mean	34	34
Highest Completed Education		
Junior high	1	0
High school	4	5
University	13	7

TABLE II
ADMINISTRATORS' EXPERIENCE, AS ASKED IN THE INTRODUCTORY QUESTIONNAIRE. TOTAL $N_{Admins} = 12$;

	Number	**Percent**
Paid admin work	11	92%
Voluntary admin work	1	8%
Special IT-Sec Training	6	50%
Configured HTTPS Before	11	92%
Has written TLS-specific code	4	33%

Fig. 1. Example of a participant drawing (U09). Among other codes, this drawing was coded with F.5 scribbled line, G.4 local encryption component, J.5 not part of the model, N.5 model too sparse.

E. Data Analysis

We collected both qualitative and quantitative data. Our qualitative analysis is based on audio-recordings, hand-written notes, and the drawings that emerged from the drawing tasks.

For our analysis, we conducted inductive coding [41], [42], [43], [44], [45], [46] as commonly used to construct models and theories based on qualitative data in social sciences and usable security, e.g., [4], [47].

We applied two rounds of open coding to detect observable patterns. We then performed Strauss and Corbin's descriptive axial coding [45] and selective coding to group our data into categories and models. We also used selective coding to relate the categories to our research questions. Throughout the coding process, we used analytic memos to keep track of thoughts about emerging themes. The final set of codes is listed in Appendix A.

As a first step, three researchers independently coded all questions and drawings of mental models. Subsequently, the resulting codes were discussed and refined to agree on a final code book. As a second step, two coders independently coded the data and again conflicts were resolved in discussions. To code drawings along with the think-aloud protocol, the coders looked at the drawings and read the audio transcript aloud. After each item, one or more codes were assigned. Our goal was to code contextual statements instead of singular entities of the drawings. Figure 1 shows an example of a drawing and selected assigned codes.

We calculated Krippendorff's Alpha [48] to measure the level of agreement among the coders. Our $\alpha = 0.98$ indicates a good level of coding agreement since the value is greater than 0.8 [48]. A potential reason for the high α lies in the technical nature of the coding categories that have a limited scope of interpretation. Irrespective of the high level of coding agreement and in line with other qualitative research methodologists, we believe that it is important to elaborate how and why disagreements in coding arose and to disclose the insights gained from discussions about them. Each coder brought a unique perspective on the topic that contributed to a more complete picture. Most conflicts arose regarding the level of granularity of a drawing or representation. The conflicts were resolved based on discussions among all coders and additional consultation of the protocols and audio transcripts from the study.

Additionally, three researchers independently performed axial and selective coding to generate two models and two anti-models for HTTPS and message encryption. Then, the three coders met in person to reach agreement on these models and to resolve conflicts.

Our quantitative analysis is based on the close-ended questions from the questionnaire. We also evaluate quantitative aspects based on particular codes.

F. Pilot and Post-hoc Validity Study

We performed a series of pilot interviews to validate our study design prior to conducting the actual study. However, due to the lack of available ground truth, our exploratory study instrument may still be subject to bias and priming effects. During analysis, we observed that most participants naturally used the term encryption when articulating their understanding of HTTPS. Hence, it is natural to suspect a priming effect due to spatial task arrangement [49]. We conducted a post-hoc validity study with nine participants (four administrators [VA1-5] and five end users [VU1-5], demographics are shown in Figure III) and a different set of warm-up questions and task ordering. The goal was to completely avoid the word encryption and let participants start with the HTTPS drawing tasks. The modified interview guideline is presented in Appendix D. The additional data was again coded, but no new codes emerged from these data, indicating that saturation was reached with the original study protocol. Our results suggest that the term encryption did not emerge from the interview questions but is often used and understood as a synonym for security.

G. Ethical Considerations

Both our institutions located in central Europe do not have a formal IRB process but a set of guidelines to follow for this kind of user study. A fundamental requirement of our universities' ethics guidelines is to preserve the participants' privacy and limit the collection of person-related data as much as possible. Therefore, every study participant was assigned an ID, which was used throughout the experiment and for the questionnaire. All participants signed consent forms prior to participating in our study. The consent form explained the goal of our research, what we expected from them, and how the collected data was to be used. The signed consent forms were stored separately and did not contain the assigned IDs to make them unlinkable to their real identities. The study complied with strict national privacy regulations and the EU's General Data Protection Regulation (GDPR).

IV. Results

In the following we present both quantitative and qualitative results along with selected direct participant quotes.

A. Mental Models

Our qualitative analysis yielded four different types of mental models representing the lower and upper bound of correspondence to the technical concepts of message encryption (as collected via drawing task 1 and shown in Figure 2, Figure 3) and HTTPS (as collected via drawing tasks

2 and 3, shown in Figure 4 and Figure 5). In the following, we provide qualitative descriptions and visualizations of the models and discuss the differences between administrators and end users. These differences are color-coded in the visualizations. Section IV-B discusses quantitative aspects of these models based on particular codes. The corresponding codebook can be found in Appendix F.

1) Model of message encryption: This model incorporates mental representations that correctly abstract the underlying technology and is shown in Figure 2. The main properties of this model are

- encryption and decryption are performed on the devices at the **communication end-points**,
- the **data in transit** is protected from attackers and eavesdroppers,
- the existence of **keys** is acknowledged, well-articulated models acknowledge the existence of two different keys (public and private), and
- that a vaguely defined **key exchange** process is required.

While this model is conceptually correct and contains relevant entities of message encryption, the model for both administrators and end users is sparse when it comes to the purpose of these entities, especially regarding key exchange. Ten administrator participants mentioned that a key exchange via a key server or an in-person meeting needs to happen before sending encrypted messages, and 10 end users inferred during their think-aloud process that some kind of exchange needs to happen prior to communication. It is also notable that key creation is not at all reflected in this model. Only one participant vaguely mentioned that the key should be created at some point without being able to further articulate how the process works. None of our participants actually incorporated key creation. Our results indicate that administrators incorporated public and private keys more often than end users (as discussed in Section IV-B). Twenty-three participant drawings reflect properties of this model (thereof 12 by administrators and 11 by end users).

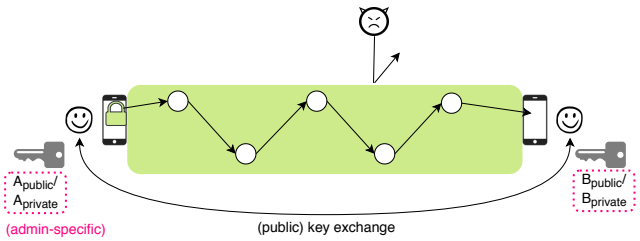

Fig. 2. Model of message encryption. Entities that are solely reflecting administrator mental models are visually highlighted (dashed box in pink).

2) Anti-model of message encryption: Contrary to the (correct) model, the anti-model incorporates all mental representations that deviate from the actual components and workflow of message encryption. The model is shown in Figure 3, and its key characteristics are

- a centralized authority is a major component of this model and acts as **authentication service**, **message relay**, or **centralized encryption service**.
- while encryption is handled by the **centralized authority**, decryption is not part of the model.
- data in transit **is not protected from attacks**.
- keys are not articulated as components. However, a vaguely defined **code** is exchanged between the communication end-points and the centralized service.

Our results suggest that the misconception of a centralized authority is more common and specific to end user mental models. Six participant drawings (0 administrators, 6 end users) feature elements of this *anti-model of message encryption*.

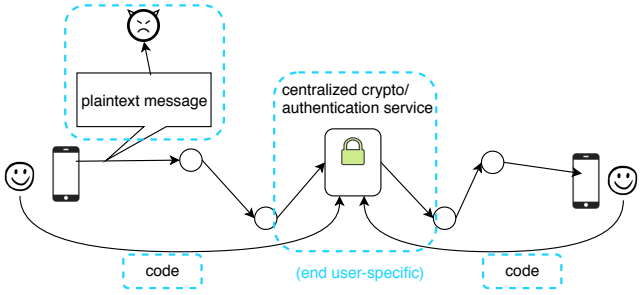

Fig. 3. Anti-model of message encryption. Entities that are solely reflecting end user mental models are visually highlighted (dashed boxes in blue).

3) Model of HTTPS: The best case model of HTTPS incorporates correct mental representations of the concept and components of HTTPS and is shown in Figure 4. Contrary to the correct model of message encryption, the correct model of HTTPS does not acknowledge the existence of keys (neither administrators nor end users mentioned them). This model is based on the data gathered through drawing tasks 2 and 3. The main properties of this model are:

- **data in transit** is encrypted and protected from attacks,
- the existence of a **CA**, but no awareness of its role and context,
- the **browser** is perceived as relevant entity,
- best-case representations contain **security indicators** like the "https" prefix or a lock icon.
- (Mostly) administrators' mental representations contain **protocol-related tasks** such as certificate checks, TLS handshakes, or HTTP GET requests that are articulated as check lists without any further understanding of their purposes and the involved entities.

Similar to the correct model of message encryption, this model contains multiple nodes between sender and receiver. Administrators' mental models generally contained more entities (e.g., CA's, different devices) and protocol-related tasks. Nineteen participant drawings substantially overlap with the *correct model of HTTPS*; 12 were articulated by administrators and seven by end users.

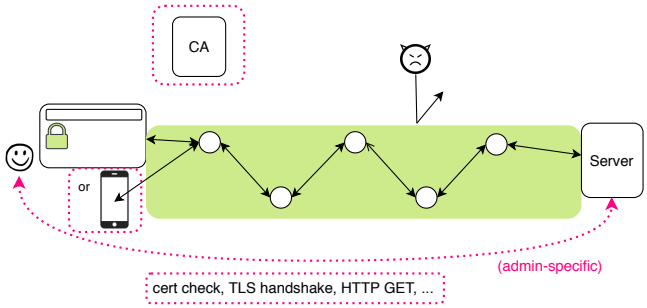

Fig. 4. Model of HTTPS. Entities that are solely reflecting administrator mental models are visually highlighted (dashed boxed in pink).

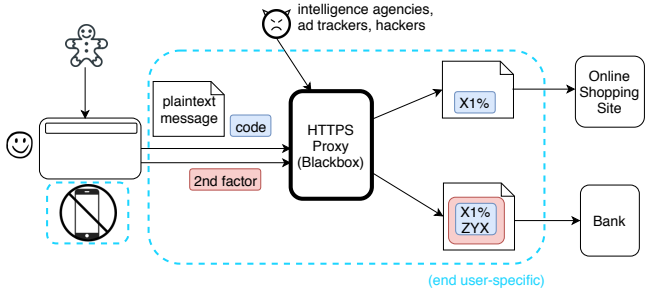

Fig. 5. Anti-model of HTTPS. Entities that are solely reflecting end user mental models are visually highlighted.

4) Anti-model of HTTPS: In contrast to the correct model of HTTPS but similar to the incorrect model of message encryption, the characteristics of this model are as follows:

- a **centralized blackbox HTTPS proxy** is responsible for authentication and/or encryption.
- the user's browser sends a **request/message along with a code** to the HTTPS proxy. The code is used to encrypt the data.
- if more security is required (e.g., in the case of online banking), the user sends an additional second factor to the HTTPS proxy, which then adds an **additional layer of encryption**.
- **decryption** is not part of the model. The server/website receives encrypted data, but it is unclear how it is then processed.
- **omnipotent attackers** such as intelligence agencies and surveillance programs, "hackers" but also ad trackers can attack the HTTPS proxy and eavesdrop information.
- **cookies** (represented by a gingerbread figure) may leak information via the browser.
- **smartphone** apps are generally perceived as insecure, regardless of whether HTTPS is used or not.

End users, especially, (8 participants) thought that mobile devices and apps are not safe to be used in this context, as sensitive information may be leaked. Also, the idea of multiple layers of encryption using a code and an additional 2nd factor was mostly part of end user mental models. Omnipotent attackers and a fairly negative security assessment are part of both administrators' and end users' mental models. This model underestimates the security of HTTPS and does not contain keys, certificates, or security indicators. Interestingly, this is the only of the four meta-models that acknowledges the existence of metadata. Twelve participant drawings feature elements from this *incorrect model of HTTPS* (10 end user models and 2 administrator models also contained elements of this model).

B. Mental Model Components and Emerging Themes

We discuss themes and particular aspects that emerged during the drawing tasks and corresponding think-aloud protocol. Table IV shows a selection of quantitative results per assigned codes where differences between groups are particularly interesting. The codes in parenthesis refer to the category codes (see Appendix F).

1) User Expectations of Security Tools: When asked of which **encrypted tools, apps or devices** they were aware, end users mostly referred to mobile apps (15 participants) and sensitive services such as banking services (14 participants) or phone calls (1 participant). At the same time, nine end users self-reported a lack of knowledge (see blue bars in Figure 9). In contrast, administrators (red bars) mentioned a broad spectrum of tools and applications, ranging from browsers (7 participants), email services (7 participants), and privacy preserving technologies such as VPN, SSH or Tor (6 participants) to local encryption such as disk encryption (1 participant) and remote encryption such as servers (4 participants). Interestingly, 8 end-users and 2 administrators explicitly stated that mobile apps are generally not encrypted and hence, untrustworthy. One end user (U04) reported to avoid mobile apps to handle sensitive data and that he accesses sensitive services, such as online banking, solely via the browser on his PC. This is in line with findings by Chin et al. [50] showing that users are commonly apprehensive about running sensitive tasks on their phones. Notably, eight non-experts and two administrators specifically brought up WhatsApp as a negative example of an application that is not or only partly encrypted. This implies that either the messaging app's initiative to offer end-to-end encryption did not yet reach all of its users or that users do not trust the service.

2) Mistrust in HTTPS and Browser Security Indicators: When it comes to **expectations of visiting a site with HTTPS**, nine end users reported a lack of knowledge, and some even claimed that they have never noticed the security indicator before as shown in Figure 6. One participant mixed up the HTTPS lock symbol with user authentication resp. authorization:

> "I think the lock symbol means that I have to authenticate myself. As I frequently forget my passwords, I usually try to click around to get rid of this symbol." (U12)

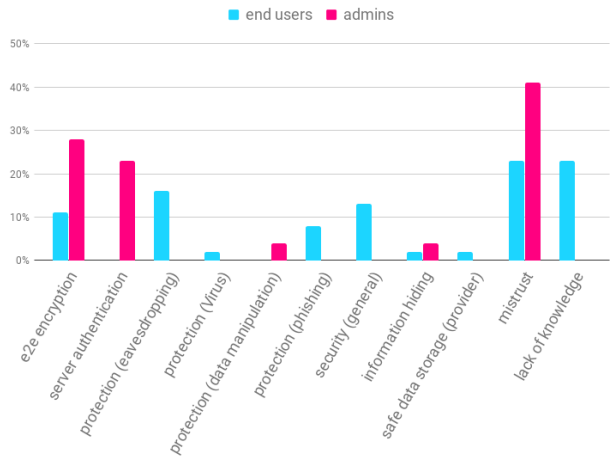

Fig. 6. Reported expectations on HTTPS. Each bar indicates how often a certain category was named in relation to all namings. (Multiple mentions per participant)

This shows that users still do not properly recognize the HTTPS security indicator, although much work has focused on improvements in this area. End users described their expectation of HTTPS on a superficial level, using general terms related to security and eavesdropping protection without further elaboration. Three participants wrongly assumed that HTTPS would protect against phishing, and one participant thought that HTTPS could ban viruses. Interestingly, one end user stated that

> "HTTPS prevents people from seeing what their partner did on the Internet or the employer from seeing whether employees were not working when they should have been." (U12)

None of the end users mentioned server authentication. In contrast, six administrators named end-to-end encryption and five server authentication. However, we observed that administrators described the two concepts decoupled from each other, which is in accordance with the finding from Fahl et al. [10] that administrators are not aware of the necessity of server authentication when establishing a secure encrypted channel.

Another emerging topic was mistrust in the security indicator and mistrust in HTTPS as a protocol. Generally, we were surprised about the high frequency of expressed mistrust against HTTPS and the security indicator coming from both end users (7 participants) and administrators (6 participants). One administrator stated that HTTPS does not offer eavesdropping protection, claiming

> "The lock symbol does not mean anything, it is pure marketing". (A06)

After this statement, we asked the participant a series of follow-up questions to allow him to clarify. As a result, the participant referred to powerful attackers and large (government) organizations and said that the arms race with powerful attackers is almost impossible to win for defenders.

Another dominant theme was the underestimation of the security benefits of HTTPS. For example, one end user articulated

> "The lock symbol puts security in people's mind with the purpose to build up trust. This does not mean that the website is secure." (P01)

As discussed by Felt et al. [18], **security indicators** are a critical UI component of modern browsers. The results from our study, however, suggest that security indicators are rarely part of user mental models. Twenty participants did not include security indicators in their drawings and the associated think-aloud protocol. One participant explicitly used an *insecurity* indicator in their drawing (note that the interviews were conducted shortly before Chrome started notifying users of unencrypted connections). The other participants referred to either the lock icon (5) and/or the HTTPS prefix (5) in their drawings.

3) Perceived Security Benefits of HTTPS: With respect to security perceptions, the elicited mental models were rather diverse. Eight out of the 18 end users from our study clearly underestimated the security benefit of HTTPS. Six end users had a realistic assessment of the security of HTTPS and understood that HTTPS encrypts the entire transport layer instead of just single data elements such as a username and a password, or a credit card number. U09 explicitly stated that he had no deeper understanding of keys, certificates, and other system components, but had a (correct) basic understanding of the underlying concept of transport layer encryption.

In the context of the two HTTPS-related drawing tasks, the participant said:

> "I expect the connection to the online shop to be secure (or insecure), irrespective of whether I want to buy a pen or a house." (U09)

A few participants also misunderstood the security benefits of HTTPS and assumed that it prevents any form of data leakage (2 non-experts) and can even prevent phishing attacks (3 non-experts). One participant imagined HTTPS to be a completely encapsulated system where all attempts to attack the sensitive information are bounced off.

> "HTTPS inhibits tracking, it is a completely encapsulated system that does not share the data." (U03)

Another participant (end user) perceived HTTPS as a tunnel between him and a server:

> "The connection between me and the server goes via a tunnel, and attempts to attack the data bounce off" (U09)

One administrator, also, described HTTPS and the attacker model as a tunnel:

> "SSL is like a tunnel, and data can be pushed through this tunnel." (A04)

Irrespective of security indicators, many participants expressed general distrust towards encrypted connections.

> "I always feel queasy, anyway. Nothing on the Internet is secure." (U01)

While for some types of attacks (e.g. phishing, malicious Javascript, or drive-by downloads) this is a true statement, this was not the type of attack to which the participants typically referred. Surprisingly, most participants questioned the protection mechanisms against attacks that HTTPS *can* protect them against (e.g., third parties stealing their passwords/credit card numbers when submitting a web form to an online shop).

Seven non-experts and six administrators expressed general doubts about whether cryptography can achieve what it promises. However, the participants considered cryptography necessary to protect various assets. Thirteen out of 18 end users mentioned sensitive data related to purchases or personal information as crucial to be protected by cryptography. Administrators again showcased a more diverse idea, referring to sensitive data (2 participants), protocol specific data (1 participant), as well as local data (1 participant) or data in transit (2 participants). Both end users and administrators had a similar picture of successful attackers, believing that the state respectively the police or secret service (26 participants) as well as hackers (19 participants) and big companies such as Apple, Facebook, or Google (18 participants) are the most persistent attackers.

4) Centralized Components and Authorities: Another emerging theme was centralization vs. decentralization and powerful authorities. Eleven end users included a **centralized encryption entity** in their drawings, i.e., a remote service that is responsible for encryption and then forwards the encrypted data to the communication partner (as in the first scenario) or to the online shop (second scenario). In other models, the centralized component acted as a message release point that 1) checks the message for suspicious content and validity, 2) encrypts it, and then 3) forwards it to the receiver. Comparing our findings to related work, we observe that end users perceive other de-centralized cryptographic tools as centralized systems, e.g., Tor [35] or use centralized components since they are perceived as more trustworthy, e.g., hosted wallets to manage bitcoins [51].

An interesting observation is that only one participant (U08) included key generation in their model. All other participants implicitly or explicitly assumed that the key was already there by default and did not include key generation in their models. Only a few participants discussed key exchange as part of their drawing and explanation as shown in Table IV.

5) Authentication vs. Encryption: Furthermore, misconceptions about the differences between encryption and authentication emerged as a theme for both groups of participants. Both end users and administrators from our sample confused encryption with authentication. In general, 13 users expressed concerns regarding the protocol's security promises. Especially when it comes to 2-Factor-Authentication (2FA), a common misconception of end users was that the secondary factor was used to add an additional layer of encryption. Participant U11 argued that 2FA is required for online banking to compensate the lack of security provided by HTTPS.

> "HTTPS is a bad protocol. If HTTPS were secure, I wouldn't need 2FA." (U11)

6) Differences between Administrators and End Users: For both groups of participants, mental models were diverse even among experienced administrators.

When asked about how they think **encryption works in theory**, 10 of 12 administrator drawings reflected concepts of end-to-end encryption. In comparison, fewer than 50% of the end user drawings clearly depicted end-to-end encryption. Four end users incorporated symmetric keys in their drawings and two explicitly mentioned private and public keys without being able to further elaborate why two keys are necessary. In contrast, seven administrators explicitly referred to asymmetric encryption in their drawings and the think-aloud protocol. More than half of the end user mental models referred to a third party that acts as encryption entity or proxy, or, referred to encryption as a blackbox. One participant (U03) used ephemeral keys and anther one (U15) thought that encryption was the same thing as obfuscation and steganography. In contrast, none of the administrators' drawings reflected such misconceptions.

While comparing the differences between administrators and end users, a theme emerged, protocol-based vs. conceptual. Our results suggest that expert mental models are mostly protocol-based instead of conceptual compared to non-experts. Most administrators were familiar with specific protocol characteristics, such as which messages are exchanged between server and client and how connections are established.

When asked to explain the underlying concepts, most administrators were unable to explain how HTTPS works and had sparse mental models of the underlying fundamentals and their interplay. This was often the case even for the first drawing task, which asked participants to depict how sending an encrypted message through any channel works in theory. Even in such a straight-forward scenario for knowledgeable users, some administrators showed and even admitted significant knowledge gaps. However, we also observed that administrators concealed these gaps more frequently and randomly dropped associated technical terms without being able to explain what they mean. Some participants, though (such as A09), explicitly admitted major knowledge gaps:

> "How HTTPS works... those are the things that I always forget. You should have asked me five years ago." (A09)

Another example of an administrator lacking conceptual knowledge but getting stuck on a configuration detail was participant A4, who said:

> "I am really not sure how Firefox validates certificates, but I know that Chrome uses the Windows Root CA." (A4)

In general, our results suggest that the administrators' level of expertise is rather diverse, much like that of end user participants. While some had sparse and incomplete mental models of encryption or HTTPS in particular (e.g., A09, A10,

A11), some were confident and able to articulate how HTTPS works in a very detailed and accurate way.

7) Mental Model Evolution: Figure 8 in the Appendix shows the mental model refinement over time across the three drawing tasks. The refinement between the first and second drawing task was equally distributed across our participants. In contrast, 26 participants had a constant level of detail of their mental models across drawing tasks 2 and 3.

8) Terminology and Visualization Components: While most administrators used *technical* terminology to elicit their mental models, end users sometimes created new terminology to compensate for missing technical terms in their vocabulary. The most frequently used technical term by the administrators was *cipher* followed by *session key* and *hash*. Twelve participants did not include a visualization of the encrypted message in their drawings. Five participants represented the encrypted message as scrambled text or numbers, four used a lock icon, three drew physical objects like an envelope or a treasure chest, and three marked the encrypted message with a different color. Others used scribbled lines, a different language, or chopped text.

For the first drawing task, 20 participants used an abstract example scenario. The remainder used an arbitrary messaging app or referred to apps and tools they knew from their everyday lives (Signal, WhatsApp, PGP/GPG).

Twenty-one participants clearly understood the connection between drawing tasks 2 (visiting an online shop) and 3 (visiting a bank's website).

Our results also suggest that only three participants were aware of the existence and associated risks of (unencrypted) metadata.

Regarding mental models of HTTPS, we classified 12 models as clearly conceptual, seven as protocol-based, and two with both conceptual and protocol-specific components. The remaining nine models were too sparse to classify them. Ten participants explicitly admitted their knowledge gaps and eight participants tried to cover them.

9) Structure-Behavior-Function (SBF) Model: The *Structure-Behavior-Function (SBF) framework* was proposed by Goel et al. [52] to describe complex systems based on three pillars: (1) *structure* (system components), (2) *behavior* (change of the system over time), and (3) *function* (effect of the system on the environment). It is often used by cognitive psychologists to describe mental models and compare them to actual system descriptions.

Hmelo-Silver et al. [53] applied the SBF framework in order to model novices and experts' understandings of complex systems. They found that the novices' system perceptions mostly focused on concrete aspects related to the structure of the system, often simplifying causality and assuming central control. In contrast, experts were more likely to discuss behavioral aspects.

Applying this model to HTTPS, we model an end user's computer or a server hosting a web page as structural components. We model behavioral aspects as perceivable browser indications, such as warning messages or security indicators. Functional aspects comprise authentication of end users and encryption of the communication path, resulting in a protection against various attack vectors such as eavesdropping or traffic injection.

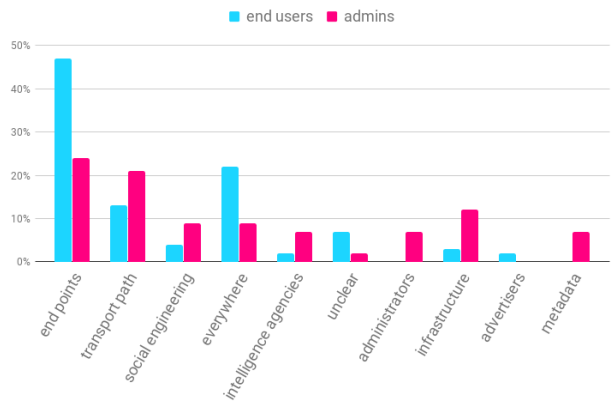

Fig. 7. Attacker models in participant drawings. Each bar indicates how many percent of all drawings feature a certain attacker type.

The results from our study suggest similar trends to those presented by Hmelo-Silver et al. [53]. End users' representations frequently include structural aspects and assume a central entity pursuing encryption. Furthermore, the end users from our study rarely included descriptions of behavioral or functional aspects, showing neither that their perception of security indicators is particularly strong nor that they are aware of the actual purpose of HTTPS.

In contrast, the administrators largely focused on behavioral aspects and delivered abstract representations of state transitions (such as sequence diagrams of protocols). Nevertheless, the administrators' system descriptions are lacking functional aspects. The administrators furthermore described the protocol behavior mainly decoupled from its actual purpose. An interesting observation from our study is that none of our expert participants clearly pointed out at which point of the protocol execution the encryption starts. Hence, our results show that neither end users nor administrators are able to link the structural aspects of HTTPS and behavioral aspects to the actual function that the protocol achieves.

C. Threat Models

After the participants finished all three drawing tasks, we asked them a set of warm-up questions about attacker models followed by another drawing task asking a participant to mark where an attacker could eavesdrop. We coded these vulnerable components and present the results in Figure 7.

The most mentioned component believed to be vulnerable to attacks were the communication endpoints, which 26 of 54 end user drawings and 10 of 35 expert drawings featured. Besides the endpoints, many end users stated that attackers could eavesdrop everywhere within the communication pro-

cess, while expert users tended to differentiate more and name concrete attackers or attack models.

Most participants visualized the attackers with arrows or circles indicating the vulnerable components of their drawings. However, some participants chose to insert attackers with a drawn representation, e.g., a set of eyes (A08), exclamation marks (A11), or stick figures as actual shoulder surfers (A10). Especially regarding the endpoint attackers, not only were malware or infected devices given as the enablers of eavesdropping, but also shoulder surfing (A10) and actual violence against human users (A11).

V. Discussion and Implications

In this section, we discuss our findings and derive potential implications on correct, incorrect, and sparse models (where essential components are missing for cases which put users directly at security or privacy risks).

Our analysis of mental models of HTTPS indicates differences between the two groups of participants. While administrator mental models were generally protocol-based and correct even if sparse, the mental models of end users were sometimes not only sparse but simply wrong or non-existent. Indeed, our user study was an opportunity for some end users to think about HTTPS and web encryption for the first time. However, we argue that fine-grained and fully correct mental models can and should not be expected from end users and partly not even from knowledgeable administrators. Thus, the following discussion places emphasis on misconceptions which crucially interfere with a secure and privacy preserving usage or configuration of HTTPS as well as actionable conclusions to mitigate these risks.

We also observed interesting corner cases which should not be ignored when discussing consolidated findings. Examples of such corner cases include contradictions, the confusion of authentication and encryption, or the assumption that publicly-available comments (i.e., consumer ratings) are not sent encrypted since this would prevent other consumers from reading them in plaintext. In contrast to the lower bounds of comprehension, we also found examples for the higher levels, e.g., an administrator who had a deep understanding of technical and operational details.

A. Implications from Correct Mental Models

The condensed representations of correct models show that participants of both user groups have a basic understanding of end-to-end encryption. In addition, the threat awareness was better than we initially expected. Many end users were aware that communication endpoints are often vulnerable (e.g. insecure devices like smartphones). This is a realistic assessment, since many smartphone vendors cease to ship security updates for their devices long before they reach their end of life. In contrast, administrators seem to focus on sophisticated but rare attacks, such as "man-in-the-middle." This may indicate an influence of tech news outlets and scientific publications which usually focus on more sophisticated attackers. Overall, we regard this as a benevolent effect since administrators should be aware of these attack types in order to deploy adequate countermeasures, and end users are currently held responsible for managing the security of their devices through, for example, regular OS and app updates.

Our results also indicate that mental models of end users may be influenced by media and marketing campaigns as the comprehension of message encryption (task 1) was often higher than the understanding of general HTTPS-encrypted traffic in web browsers. We hypothesize that one reason for this difference may be higher media coverage of message encryption in comparison to HTTPS. In addition, several app manufactures (e.g., WhatsApp) specifically point out end-to-end encryption when users start a new conversation.

Finally, the pictorial representations of mental models indicate interesting differences between end users and administrators: while end users' correct models were rather conceptual, administrators' models were mostly protocol-related and often illustrated operational details. The protocol-based representations reminded us of flow charts common to academic lectures and online tutorials, suggesting that many administrators tried to recall previously-seen educational material.

However, there is still room for improvement, since even correct representations were often sparse. For example, only the best representations pointed out security indicators, and important aspects like key exchange and certification authorities (CA) were hardly mentioned. Overall, the correct mental models indicate that media coverage, marketing, and education can help in forming folk models, even for complex processes like HTTPS.

B. Implications from Incorrect Mental Models

While correct mental models emphasized the value of end-to-end encryption, participants with incorrect mental models tended to underestimate the security benefits of HTTPS and furthermore assume that omnipotent attackers can eavesdrop at multiple stages of online communication. We hypothesize that this might be the result of press attention on misuse of SSL/TLS in mobile apps created by the work of Fahl et al. [10] and Cothia et al, among others. [19]. Consequently, end users are incapable of making informed security decisions as they do not trust the protocol in even its best-case configuration. As a consequence, end users do not demand proper configurations. Even though WhatsApp was already mentioned as an example of an application which explicitly advertises end-to-end encryption, some users might not even recognize such notifications (or simply mistrust them) as WhatsApp was constantly mentioned as an example for an app being not or only partly encrypted. While this seems to not prevent users from using WhatsApp, it shows that the security benefits of end-to-end encryption are often not perceived as such.

Even more worrisome, we identified corner cases of incorrect mental models which may directly put users at risk. For example, one end user thought that HTTPS can protect against phishing web sites. Such assumptions may lead to an unjustified sense of security whenever HTTPS connections are indicated by the browser. We also found that end users were

often not aware of security indicators or they were perceived as unimportant. Overall, the results show that the end users' interest in these indicators is mitigated by general mistrust in the protocol (i.e., the belief that cryptography/HTTPS cannot prevent attacks and eavesdropping). Similarly, we found that many users are not impressed by warnings of insecure connections, since they do not trust the protocol in the first place. While administrators generally have more correct mental models, their representations frequently lacked important parts and meaningful interconnections. Also, the administrators' statements indicated a high level of mistrust. As an example, one administrator (A06) claimed that "The lock symbol does not mean anything, it is pure marketing". Additionally, administrators frequently expressed mistrust in the PKI system. These two facts might explain a diminished interest in configuring certificates correctly.

In summary, the incorrect mental models indicate that end users do not trust the security that HTTPS can offer if deployed in a best-case working scenario. We argue that recent news reports about intelligence activities influenced perceptions about omnipotent attackers and that users need to build up trust before concepts like security indicators and warnings can be effective. The multi-step approach of our user study indicates that education and brain teasers can be promising in that they helped many users adjust their mental models even if considering some aspects of HTTPS for the first time. For example, we observed that thinking about threat models caused participants to review and refine their mental model drawings in some cases. End user participant U12 stated, "Now I see that I didn't think logically" before revising her drawing for task 1. The same was true for administrators who became more aware of metadata leakage after being asked about potential attacks.

C. Implications from Missing and Sparse Mental Models

In addition to correct and incorrect mental models, interesting implications can be derived from sparse models, as well. We found that keys and certificates are not part of the correct conceptional representations of most mental models, which implies that users do not understand their purpose within the concept. We argue that not being aware of their purpose reduces the chance that users verify certificates manually. The same is true for keys in other application scenarios: it is no surprise that key verification in mobile messaging apps is rarely performed, as users are not aware of its necessity nor the underlying threat model that this measure protects them from. Helping users understand the functional perspective of keys and certificates in HTTPS and encrypted messaging is thus one of the main challenges for future research. While not all conceptual parts need to be understood by users, it is essential that users are motivated to engage measures demanded by the security concept.

Even though some administrators mentioned keys and certificates with respect to HTTPS, they tended to use them as buzzwords in their articulations and were often unable to explain how these components contribute to a secure configuration. In addition, we found that most administrators were not aware that server authentication is a prerequisite for establishing a securely encrypted channel (which corresponds to the results from Fahl et al. [10]).

D. Potential Countermeasures and Improvements

While our data does not provide direct evidence for this, we hypothesize that education and online tutorials contribute to these mental models. This corresponds to the findings from Krombholz et al. [4], who showed that even administrators who successfully configure HTTPS strongly rely on online sources as they do not have a full understanding of the underlying concepts. For end users, our results have implications on security indicators, warnings and other UX cues that are designed to assist users in making informed security decisions.

1) Suggested Workflow Changes for Tools and APIs: We found that administrators often do not understand the interplay of functional protocol components (e.g. the CA, certificates for E2E, keys). In particular, our results suggest that the role of certificates and PKI as a whole for setting up an encrypted channel are poorly understood by administrators which indicates that administrators could benefit from a deployment process which more clearly illustrates the linkage between these components, resp. hides this complexity from them. Hence, as keys and certificates remain important functional components even in more user-friendly deployment concepts such as *Let's Encrypt*[2] and *Certbot*[3], it is necessary to provide tangible explanations to make their contribution to a secure configuration more intuitive. We acknowledge that Let's Encrypt and the ACME Protocol offer promising usability enhancements from the administrators' point of view, since they enable automatic issuance of certificates. However, these initiatives mainly simplify the process of obtaining a certificate, but do not completely obviate the need for its users to deal with certificates, keys and additional hardening measures. As our results show that the biggest challenge for administrators is to put these different components together in order to deploy a secure authenticated-encryption mechanism, we suggest that future protocol designs should aim at hiding this additional complexity from users.

Although we expected that server authentication was part of user mental models, our results suggest that this is rarely the case. Hence, the concept of server authentication along with its importance for communication security needs to be reflected in the user interface in order to make server authentication part of user mental models. Such UI components should also motivate users to verify the server's authenticity.

An example for a promising starting point in this regard is the NaCl API presented by [54], which provides one simple function referred to as *crypto_box* that comprises several functionality for authenticating and encrypting a message.

[2]https://letsencrypt.org – accessed: 05/08/2018.

[3]https://certbot.eff.org – accessed: 05/08/2018.

2) Trust Establishment: Our results suggest that especially end users need UX cues that help to construct valid mental models, as these are important to establish trust in the protocol and its security properties. In order to deal with general mistrust towards HTTPS, we argue that the protocols in today's Internet ecosystem and the upcoming Internet of Things should provide state of the art encryption by default and that insecure protocols such as HTTP should be abandoned to establish a more user-friendly distinction between best-case security and vulnerable connections. Also, a security-by-default state would obviate the need for users to regularly check HTTPS-specific UI components. For end users, mistrust in the protocol and misconceptions about the role of certificates can lead to wrong decisions when warnings are displayed, putting users at danger of privacy and security violation. This is in-line with latest innovations enforced by Google[4], who at the time of writing began to roll out a new version of the web browser Chrome not showing any security indicators for HTTPS secured websites anymore. At the same time, websites still using HTTP are marked as insecure by displaying a red insecurity indicator in the address bar. Google argued that users should expect a secure Internet by default, which is in-line with our findings. Also, our results suggest that security indicators are often not part of end user mental models, which is why we agree with Google's less ubiquitous yet more precise risk communication with indicators.

VI. Limitations

While we refrained from recruiting computer science students, our sampling method still has limitations. We aimed to recruit a diverse sample of users, however our sample is still skewed towards the more educated social class. Furthermore, our end user sample skewed female, but we did not manage to recruit a single non-male administrator. Sadly, female administrators are very rare in our region. Our sample was recruited in Central Europe which is generally privacy-aware, and HTTPS adoption rates are generally higher than e.g., in Japan [2]. Our results are therefore impacted by cultural effects. As research on perceptions of cryptographic tools and algorithms is still in its early stages, we followed an inductive approach and opted for a qualitative study to construct models and theory grounded in the data. Naturally, our methodology also has its limitations. The data is self-reported and qualitative in nature. While our sample is still sufficiently large to perform basic statistic tests, further investigations are necessary to determine large-scale effects and hence obtain significant results with larger effect sizes. We refrained from asking closed-ended knowledge questions. Also, the results from our pre-study showed that participants like to litter buzzwords which is why we designed our study to get a deeper context of their understanding. Our goal was to allow our participants to openly articulate how they think the protocol works. We decided to group our participants based on their role of being an administrator instead of their knowledge to avoid biasing effects by previously defined answer options.

[4]https://blog.chromium.org/2018/05/evolving-chromes-security-indicators.html

VII. Conclusion and Future Work

In this paper, we presented the first qualitative study on user mental models of HTTPS. In examining 18 end users and 12 administrators, our approach revealed four types of user mental models of HTTPS and (abstract) message encryption. We furthermore revealed misconceptions about threat models and protocol components that lead to decisions that influence the security of the systems and, as a result, directly put users at risk.

Additionally, we shed light on differences between end users' and administrators' perceptions; while end user mental models were mostly conceptual, administrators' mental models frequently contained protocol components and technical terms without accompanying understanding of their functionality and purpose within the protocol configuration. Among other insights, our findings suggest that 1) many users confuse encryption with authentication, 2) end users assume the omnipotence of attackers and significantly underestimate the security benefits of HTTPS, and 3) many users of both types generally ignore or even distrust security indicators.

Our work reveals reasons for the usability challenges determined by Krombholz et al. [4] that are often responsible for vulnerable HTTPS configurations. Our results, furthermore, explain why users often fail to correctly assess the implications of clicking through warnings. And, finally, we provide foundations for future designs of cryptographic protocols that are easier for administrators and developers to deploy or implement related code in the most secure manner and therefore minimize the exposure of end users to security-critical decisions when communicating online.

As future work, it remains to show how our findings can be used to inform the design of future cryptographic protocols. We think that our results can inform a larger (quantitative) study which could make use of closed-ended questions. Such future work could also include questions on administrator qualifications and knowledge questions to measure large-scale effects and to perform multivariate analyses.

Acknowledgments

We would like to thank the reviewers and our contact point Rob Reeder for their constructive feedback, and the Leitstelle 511 e.V. for providing an interview location in Hannover. This work was partially funded by the ERC Grant 678341: Frontiers of Usable Security and by the FFG grant no. 863129: IoT4CPS. The competence center SBA Research (SBA-K1) is funded within the framework of COMET Competence Centers for Excellent Technologies by BMVIT, BMDW, and the federal state of Vienna, managed by the FFG. The financial support by the Christian Doppler Research Association, the Austrian Federal Ministry for Digital and Economic Affairs and the National Foundation for Research, Technology and Development is gratefully acknowledged.

REFERENCES

[1] A. Whitten and J. D. Tygar, "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0." in *USENIX Security Symposium*, 1999.

[2] A. P. Felt, R. Barnes, A. King, C. Palmer, and C. Bentzel, "Measuring HTTPS Adoption on the Web," in *USENIX Security Symposium*, 2017.

[3] M. E. Acer, E. Stark, A. P. Felt, S. Fahl, R. Bhargava, B. Dev, M. Braithwaite, R. Sleevi, and P. Tabriz, "Where the Wild Warnings Are: Root Causes of Chrome HTTPS Certificate Errors," in *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security (CCS)*, 2017.

[4] K. Krombholz, W. Mayer, M. Schmiedecker, and E. Weippl, ""I Have No Idea What I'm Doing" - On the Usability of Deploying HTTPS," in *USENIX Security Symposium*, 2017.

[5] M. Green and M. Smith, "Developers are not the enemy!: The need for usable security apis," *IEEE Security & Privacy*, vol. 14, no. 5, pp. 40–46, 2016.

[6] S. Fahl, M. Harbach, H. Perl, M. Koetter, and M. Smith, "Rethinking ssl development in an appified world," in *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*. ACM, 2013, pp. 49–60.

[7] M. Oltrogge, Y. Acar, S. Dechand, M. Smith, and S. Fahl, "To Pin or Not to Pin-Helping App Developers Bullet Proof Their TLS Connections." in *USENIX Security Symposium*, 2015.

[8] R. W. Reeder, A. P. Felt, S. Consolvo, N. Malkin, C. Thompson, and S. Egelman, "An Experience Sampling Study of User Reactions to Browser Warnings in the Field," in *Proceedings of the CHI Conference on Human Factors in Computing Systems*, 2018.

[9] Y. Acar, M. Backes, S. Fahl, S. Garfinkel, D. Kim, M. L. Mazurek, and C. Stransky, "Comparing the Usability of Cryptographic APIs," in *Symposium on Usable Privacy and Security (SOUPS)*, 2017.

[10] S. Fahl, Y. Acar, H. Perl, and M. Smith, "Why eve and mallory (also) love webmasters: a study on the root causes of SSL misconfigurations," in *Proceedings of the 9th ACM symposium on Information, Computer and Communications Security*. ACM, 2014.

[11] A. Manousis, R. Ragsdale, B. Draffin, A. Agrawal, and V. Sekar, "Shedding light on the adoption of let's encrypt," in *arXiv preprint arXiv:1611.00469*, 2016.

[12] J. Sunshine, S. Egelman, H. Almuhimedi, N. Atri, and L. F. Cranor, "Crying Wolf: An Empirical Study of SSL Warning Effectiveness." in *USENIX Security Symposium*, 2009.

[13] M. Harbach, S. Fahl, P. Yakovleva, and M. Smith, "Sorry, I don't get it: An analysis of warning message texts," in *International Conference on Financial Cryptography and Data Security*. Springer, 2013.

[14] D. Akhawe and A. P. Felt, "Alice in Warningland: A Large-Scale Field Study of Browser Security Warning Effectiveness." in *USENIX Security Symposium*, 2013.

[15] S. Weber, M. Harbach, and M. Smith, "Participatory design for security-related user interfaces," in *Workshop on Usable Security (USEC)*, 2015.

[16] A. P. Felt, R. W. Reeder, H. Almuhimedi, and S. Consolvo, "Experimenting at scale with google chrome's SSL warning," in *Proceedings of the CHI Conference on Human Factors in Computing Systems*. ACM, 2014.

[17] A. P. Felt, A. Ainslie, R. W. Reeder, S. Consolvo, S. Thyagaraja, A. Bettes, H. Harris, and J. Grimes, "Improving SSL warnings: Comprehension and adherence," in *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*. ACM, 2015.

[18] A. P. Felt, R. W. Reeder, A. Ainslie, H. Harris, M. Walker, C. Thompson, M. E. Acer, E. Morant, and S. Consolvo, "Rethinking Connection Security Indicators." in *Symposium on Usable Privacy and Security (SOUPS)*, 2016.

[19] T. Chothia, F. D. Garcia, C. Heppel, and C. M. Stone, "Why Banker Bob (still) Cant Get TLS Right: A Security Analysis of TLS in Leading UK Banking Apps," in *International Conference on Financial Cryptography and Data Security*. Springer, 2017.

[20] S. Fahl, M. Harbach, T. Muders, M. Smith, and U. Sander, "Helping Johnny 2.0 to encrypt his Facebook conversations," in *Symposium on Usable Privacy and Security (SOUPS)*. ACM, 2012.

[21] E. Atwater, C. Bocovich, U. Hengartner, E. Lank, and I. Goldberg, "Leading Johnny to Water: Designing for Usability and Trust." in *Symposium on Usable Privacy and Security (SOUPS)*, 2015.

[22] A. Herzberg and H. Leibowitz, "Can Johnny Finally Encrypt? Evaluating E2E Encryption in Popular IM Applications," in *ACM Workshop on Socio-Technical Aspects in Security and Trust (STAST)*, 2016.

[23] S. Schröder, M. Huber, D. Wind, and C. Rottermanner, "When SIGNAL hits the Fan: On the Usability and Security of State-of-the-Art Secure Mobile Messaging," in *European Workshop on Usable Security. IEEE*, 2016.

[24] E. Vaziripour, J. Wu, M. O'Neill, R. Clinton, J. Whitehead, S. Heidbrink, K. Seamons, and D. Zappala, "Is that you, Alice? A Usability Study of the Authentication Ceremony of Secure Messaging Applications," in *Symposium on Usable Privacy and Security (SOUPS)*, 2017.

[25] S. Ruoti, J. Andersen, S. Heidbrink, M. O'Neill, E. Vaziripour, J. Wu, D. Zappala, and K. Seamons, "We're on the Same Page: A Usability Study of Secure Email Using Pairs of Novice Users," in *Proceedings of the CHI Conference on Human Factors in Computing Systems*. ACM, 2016.

[26] A. Lerner, E. Zeng, and F. Roesner, "Confidante: Usable Encrypted Email: A Case Study with Lawyers and Journalists," in *Security and Privacy (EuroS&P), 2017 IEEE European Symposium on*. IEEE, 2017.

[27] R. Abu-Salma, M. A. Sasse, J. Bonneau, A. Danilova, A. Naiakshina, and M. Smith, "Obstacles to the Adoption of Secure Communication Tools," in *Security and Privacy (SP), 2017 IEEE Symposium on (SP'17). IEEE Computer Society*, 2017.

[28] R. Wash and E. Rader, "Influencing mental models of security: a research agenda," in *Proceedings of the 2011 Workshop on New Security Paradigms*. ACM, 2011.

[29] C. Bravo-Lillo, L. F. Cranor, J. Downs, and S. Komanduri, "Bridging the gap in computer security warnings: A mental model approach," in *IEEE Security & Privacy*, vol. 9, no. 2. IEEE, 2011, pp. 18–26.

[30] K. Renaud, M. Volkamer, and A. Renkema-Padmos, "Why doesn't Jane pProtect Her Privacy?" in *International Symposium on Privacy Enhancing Technologies*, 2014.

[31] M. Oates, Y. Ahmadullah, A. Marsh, C. Swoopes, S. Zhang, R. Balebako, and L. Cranor, "Turtles, Locks, and Bathrooms: Understanding Mental Models of Privacy Through Illustration," in *Proceedings on Privacy Enhancing Technologies*, vol. 2018, no. 4. De Gruyter Open, 2018.

[32] J. Wu and D. Zappala, "When is a Tree Really a Truck? Exploring Mental Models of Encryption," in *Symposium on Usable Privacy and Security (SOUPS)*, 2018.

[33] R. Abu-Salma, E. M. Redmiles, B. Ur, and M. Wei, "Exploring User Mental Models of End-to-End Encrypted Communication Tools," in *8th USENIX Workshop on Free and Open Communications on the Internet (FOCI 18)*, 2018.

[34] R. Kang, L. Dabbish, N. Fruchter, and S. Kiesler, "My Data Just Goes Everywhere: User Mental Models of the Internet and Implications for Privacy and Security," in *Symposium on Usable Privacy and Security (SOUPS)*, 2015.

[35] K. Gallagher, S. Patil, and N. Memon, "New Me: Understanding Expert and Non-Expert Perceptions and Usage of the Tor Anonymity Network," in *Symposium on Usable Privacy and Security (SOUPS)*, 2017.

[36] E. Zeng, S. Mare, and F. Roesner, "End User Security & Privacy Concerns with Smart Homes," in *Symposium on Usable Privacy and Security (SOUPS)*, 2017.

[37] C. Herley and P. van Oorschot, "SoK: Science, Security and the Elusive Goal of Security as a Scientific Pursuit," in *IEEE Symposium on Security and Privacy (SP)*. IEEE, 2017.

[38] A. R. Kearney and S. Kaplan, "Toward a Methodology for the Measurement of Knowledge Structures of Ordinary People: The Conceptual Content Cognitive Map (3CM)," in *Environment and Behavior*, vol. 29, no. 5, 1997, pp. 579–617.

[39] K. A. Ericsson and H. A. Simon, "Verbal reports as data." in *Psychological review*, vol. 87, no. 3. American Psychological Association, 1980, p. 215.

[40] G. Guest, A. Bunce, and L. Johnson, "How many interviews are enough? An experiment with data saturation and variability," in *Field Methods*, vol. 18, no. 1, 2006, pp. 59–82.

[41] S. B. Merriam and E. J. Tisdell, *Qualitative Research: A Guide to Design and Implementation*. John Wiley & Sons, 2015.

[42] K. Charmaz, *Constructing Grounded Theory: A Practical Guide through Qualitative Research*. SagePublications Ltd, London, 2006.

[43] J. Lazar, J. H. Feng, and H. Hochheiser, *Research Methods in Human-Computer Interaction*. Morgan Kaufmann, 2017.

[44] B. G. Glaser and A. L. Strauss, *The Discovery of Grounded Theory: Strategies for Qualitative Research*. Transaction publishers, 1967.

[45] A. Strauss, J. Corbin *et al.*, *Basics of qualitative research*. Newbury Park, CA: Sage, 1990, vol. 15.

[46] B. G. Glaser, *Emergence vs forcing: Basics of grounded theory analysis*. Sociology Press, 1992.
[47] A. Naiakshina, A. Danilova, C. Tiefenau, M. Herzog, S. Dechand, and M. Smith, "Why Do Developers Get Password Storage Wrong?: A Qualitative Usability Study," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, 2017.
[48] K. Krippendorff, *Content Analysis: An Introduction to Its Methodology*. SAGE Publications, 2004.
[49] S. Moreno-Ríos and J. A. García-Madruga, "Priming in Deduction: A Spatial Arrangement Task," in *Memory & Cognition*, vol. 30, no. 7. Springer, 2002, pp. 1118–1127.
[50] E. Chin, A. P. Felt, V. Sekar, and D. Wagner, "Measuring User Confidence in Smartphone Security and Privacy," in *Symposium on Usable Privacy and Security (SOUPS)*, 2012.
[51] K. Krombholz, A. Judmayer, M. Gusenbauer, and E. Weippl, "The Other Side of the Coin: User Experiences With Bitcoin Security and Privacy," in *International Conference on Financial Cryptography and Data Security*, 2016.
[52] A. K. Goel, S. Rugaber, and S. Vattam, "Structure, Behavior, and Function of Complex Systems: The Structure, Behavior, and Function Modeling Language," in *Artif. Intell. Eng. Des. Anal. Manuf.*, vol. 23, no. 1. New York, NY, USA: Cambridge University Press, Feb. 2009, pp. 23–35.
[53] C. Hmelo-Silver and M. Green Pfeffer, "Comparing Expert and Novice Understanding of a Complex System From the Perspective of Structures, Behaviors, and Functions," in *Cognitive Science*, vol. 28, 02 2004, pp. 127–138.
[54] D. J. Bernstein, T. Lange, and P. Schwabe, "The Security Impact of a New Cryptographic Library," in *Proceedings of the 2Nd International Conference on Cryptology and Information Security in Latin America*, ser. LATINCRYPT'12, 2012, pp. 159–176.

APPENDIX

A. Additional Tables and Figures

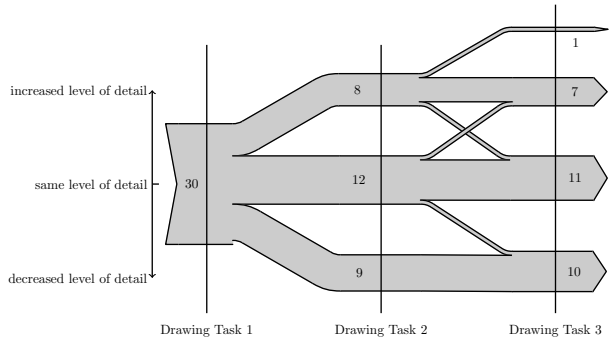

Fig. 8. Development of user mental models across the 3 drawing tasks.

TABLE III
STUDY PARTICIPANTS (ADMINISTRATORS, END USERS, PILOT/VALIDITY STUDY PARTICIPANTS)

ID	Age	Gender	Education	Employment	IT-education
Administrators ($N_A = 12$)					
A01	29	m	high school	employed	no
A02	40	m	university	self-employed	no
A03	29	m	university	employed	yes
A04	34	m	high school	employed	no
A05	nA	m	university	employed	yes
A06	42	m	high school	employed	no
A07	31	m	university	employed	no
A08	35	m	high school	employed	yes
A09	31	m	university	employed	yes
A10	31	m	high school	employed	no
A11	37	m	university	employed	yes
A12	30	m	university	employed	yes
End users ($N_U = 18$)					
U01	56	f	junior high	self-employed	no
U02	24	m	high school	self-employed	no
U03	24	f	high school	employed/student	no
U04	41	m	university	employed	no
U05	26	f	university	employed	no
U06	35	f	university	employed/student	no
U07	43	f	university	employed	no
U08	28	f	university	employed	no
U09	60	m	university	employed	no
U10	27	m	university	student	no
U11	24	m	university	student	no
U12	56	f	university	employed	no
U13	28	f	university	employed	no
U14	32	f	university	student	no
U15	28	m	university	employed	yes
U16	24	f	high school	employed/student	no
U17	27	f	university	employed	no
U18	28	m	high school	employed	no
Pilot study participants ($N_P = 6$)					
P01	36	m	university	employed	no
P02	28	f	university	employed	no
P03	28	f	high school	employed	no
P04	21	m	high school	employed	no
P05	36	f	university	employed	yes
P06	29	m	junior high	employed	no
Validity study participants ($N_V = 9$)					
VA1	24	m	university	employed	no
VA2	36	m	university	employed	no
VA3	27	m	high school	employed	no
VA4	40	m	high school	self-employed	yes
VU1	52	f	university	employed	no
VU2	27	m	high school	employed	no
VU3	30	m	university	employed	yes
VU4	23	f	university	employed/student	no
VU5	24	f	university	employed/student	no

TABLE IV

SELECTION OF MENTIONED CONCEPTS AND IDENTIFIED CODES. PERCENTAGES MAY NOT SUM TO 100 AS SOME PARTICIPANTS MENTIONED MULTIPLE ASPECTS. P VALUES ARE CALCULATED WITH TWO-SIDED FISHER'S EXACT TESTS COMPARING END USERS AND ADMINS, ϕ DENOTES THE MEAN SQUARE CONTINGENCY COEFFICIENT. LINES WHERE $p < 0.05$ ARE HIGHLIGHTED IN GREY.

Code	End users	%	Admins	%	Total	%	ϕ (if $p < 0.05$)
Cryptographic concepts							
End-to-end (B.1)	11	61,1%	12	100,0%	23	76,7%	$\phi = 0.45$
Symmetric encryption (B.2)	3	16,7%	3	25,0%	6	20,0%	
Assymmetric encryption (B.3)	1	5,6%	8	66,7%	9	30,0%	$\phi = 0.1$
Blackbox (B.6)	2	11,1%	0	0,0%	2	6,7%	
Obfuscation or steganography (B.7)	2	11,1%	0	0,0%	2	6,7%	
Authentication (B.8)	1	5,6%	0	0,0%	1	3,3%	
Model too sparse (B.9)	5	27,8%	4	33,3%	9	30,0%	
Key generation and exchange							
Web of trust (D.2)	0	0,0%	1	8,3%	1	3,3%	
PSK: key server (D.3)	1	5,6%	1	8,3%	2	6,7%	
PSK: in-person key exchange (D.4)	2	11,1%	3	25,0%	5	16,7%	
PSK: undefined (D.6)	2	11,1%	6	50,0%	8	26,7%	
Shared knowledge (D.5)	3	16,7%	0	0,0%	3	10,0%	
Model too sparse (D.1)	11	61,1%	3	25,0%	14	46,7%	
Security indicators							
HTTPS (J.1)	4	22,2%	3	25,0%	7	23,3%	
Lock icon (J.2)	3	16,7%	5	41,7%	8	26,7%	
Checkmark (J.3)	0	0,0%	2	16,7%	2	6,7%	
Insecurity indicators (J.4)	0	0,0%	1	8,3%	1	3,3%	
No indicator (J.5)	13	72,2%	7	58,3%	20	66,7%	
Perceived security benefit of HTTPS							
Underestimated (K.1)	8	44,4%	1	8,3%	9	30,0%	$\phi = -0.39$
Realistic assessment (K.3)	6	33,3%	6	50,0%	12	40,0%	
Model too sparse (K.4)	3	16,7%	6	50,0%	9	30,0%	
No control (K.5)	1	5,6%	1	8,3%	2	6,7%	
Meta observations							
More buzzwords (T.1)	3	16.7%	7	58.3%	10	33.3%	$\phi = -0.43$
Conceptual model (V.2)	10	55.6%	3	25.0%	13	43.3%	
Protocol-based model (V.1)	1	5.6%	6	50.5%	7	23.3%	$\phi = -0.51$
Third Parties							
Centr. encryption/auth. service (M.1, M.9)	11	61.1%	0	0.0%	11	36.7%	$\phi = -0.62$

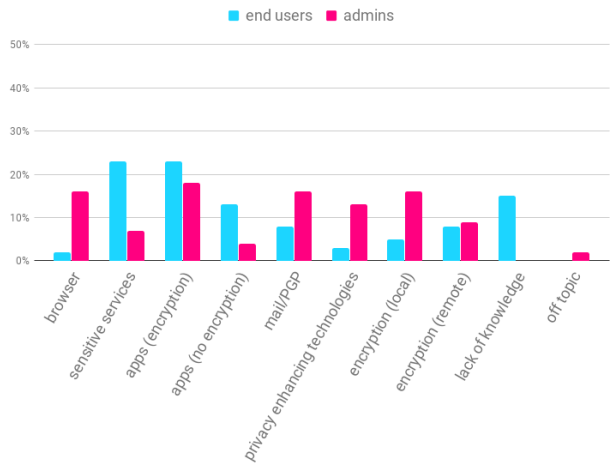

Fig. 9. Reported knowledge of encrypted tools, apps or devices. Each bar indicates how often a certain category was named in relation to all namings. (Multiple mentions per participant)

B. Screening Questionnaire

Demographics:

- Age/ Gender/ Profession/ Highest completed level of education/ Recent professional status
- Do you have an IT-security background? If yes, please specify: ...
- Are you a software developer? If yes, since:...
- Are you a system administrator? If yes, since: ...
- Technical Score: I have a good understanding of Computers and the Internet: Likert Scale from 1 (agree) - 7 (disagree)
- I often ask other people for help when I am having problems with my computer: Likert Scale from 1 (agree) - 7 (disagree)
- I am often asked for help when other people have problems with their computer. Likert Scale from 1 (agree) - 7 (disagree)

1) Technology use:

- Which of the following technologies and services below have you used in the past year? (Check all that apply.)
  - Social Networks (Facebook, Twitter, Instagram, LinkedIn, etc)
  - Online Audio and Video Conferencing (Skype, FaceTime, Google Hangout, etc.)
  - Office Software (Word, Excel, PowerPoint, etc.)
  - Mobile Messaging (Signal, Threema, Whatsapp, etc.)
  - Online Banking
  - Online Shopping (Amazon, Zalando, etc.)

Expert-specific questions:

- Have you ever written non-browser TLS code? (e.g. for TLS certificate validation?)
- Have you ever configured HTTPS?
- How long have you been working as admin/developer?
- How big is the company that you are working for?
- What is your company's scope?
- Security plays an important role in my everday work. (7-point-Likert, strongly agree - strongly disagree)
- When you are confronted with security-critical decision, do you make them mostly alone or mostly with a team?

C. Interview Protocol

General:

- In your daily life, are you aware of any tools, apps or devices where cryptography is used?
- why do you choose to use them?
- Was cryptography part of your education?
- If yes, where did you learn about it? If possible, briefly outline the basic content and topics that you heard of.
- What are your expectations when you visit a site with HTTPS and you see the green lock next to the URL in your browser?
- What is encryption?

1) Mental Models: In the following, I'm going to ask you to explain your perceptions and ideas about how encryption on the Internet works. The purpose of this interview is to understand your views, opinions, and understanding regarding how encryption works with respect to the technology you use in your everyday life. Please keep in mind that there is no correct answer to these questions - please just answer these questions based on your knowledge and experiences. Also, please think aloud and explain your thought process while drawing.

- **Phase 1: encryption in theory.** Please draw a picture of how you think encryption works, when you send an encrypted message to your friend. Remember to include all relevant persons and components into the drawing.
- **Phase 2:** Visiting a site with HTTPS. Imagine you are visiting a website with the HTTPS prefix (e.g. your favorite online shop). Please make a drawing of what makes such a site different to a site with the HTTP prefix.
- **Phase 3: Online Banking.** Imagine you log into your online banking. Usually, those sites are encrypted and you see a green lock next to the URL in your browser. Can you please make a drawing of what happens when you log into your bank account. Focus on what happens between you and your bank's website.

2) Attacker Models:

- Why is cryptography used on the Internet?
- What information does cryptography protect?
- Who is the attacker that encryption protects you against? [Images of NSA, person in the same WiFi, Teenage hacker in the basement, Google, Apple, Facebook]
- Please take your drawings (from before). Can you maybe mark where an attacker could eavesdrop?

D. Post-hoc Validity Study Protocol

General:

- In your daily life, which security practices do you apply to stay secure online?
- Do you sometimes pay attention to the green lock icon in the browser?
- Have you ever thought about what the green lock next to the URL means?
- What are your security expectations when you visit a site with HTTPS and you see the green lock next to the URL in your browser?

1) Mental Models: In the following, I'm going to ask you to explain your perceptions and ideas about how ~~**encryption**~~ **security** on the Internet works. [...]

- **Phase 1*: Visiting a site with HTTPS.**
- **Phase 2*: Online banking.**
- **Phase 3*: encryption in theory.**

2) Attacker Models: [...]

E. Final Set of Codes for General Questions/ Attacker Models

A. tools	**C. expectations on HTTPS**	**E. administration responsibility**	**G. info to protect**
A.1 browser	C.1 e2e encryption	E.1 academic	G.1 data: sensitive/personal/purchase
A.2 app	C.2 server authentication	E.2 service/industry IT	G.2 data: protocol specific
A.3 service: mail/PGP	C.3 safe data storage at provider	E.3 service/industry other	G.3 data: governmental/business
A.4 service: sensitive calls	C.4 information hiding/targeted advertisements	**F. crypto motivation**	G.4 data: in transfer
A.5 privacy enhancing technologies	C.5 security: general	F.1 authenticity communication partner	G.5 data: local
A.6 encryption: local	C.6 protection: data manipulation	F.2 integrity	G.6 data: remote
A.7 encryption: remote	C.7 protection: phishing	F.3 protection: privacy/anonymity	G.7 data: general
A.8 negative: mobile apps have no encryption	C.8 protection: virus	F.4 protection: third party	G.8 data: no protection
A.9 lack of knowledge	C.9 protection: eavesdropper	F.5 protection: malware	G.9 metadata: no protection
A.10 off topic	C.10 mistrust: no eavesdropping protection	F.6 protection: eavesdropper	G.10 lack of knowledge
B. education content	C.11 mistrust: meta data leakage	F.7 protection: sensitive data	G.11 off topic
B.1 work experience	C.12 mistrust: general	F.8 protection: general	**H. successful attacker**
B.2 lecture/academic	C.13 lack of knowledge	F.9 mistrust	H.1 state/police/secret service
B.3 aspect: encryption applied	**D. definition crypto**	F.10 no comment	H.2 hacker
B.4 aspect: cryptography theoretical	D.1 data obfuscation		H.3 big player
B.5 self education: books/videos/internet	D.2 data modification		H.4 insider
B.6 self education: programming	D.3 data tunnel		H.5 provider
B.7 non technical	D.4 en-/decryption keys		H.6 attacker omnipresent
B.8 no education	D.5 symbolic explanation		H.7 no attacker
B.9 cannot remember	D.6 mathematical concept		
	D.7 protection from eavesdroppers		
	D.8 lack of knowledge		

F. Final Set of Codes for Mental Models

A. communication path	**F. visualization of encrypted message**	**K. perceived security benefit of HTTPS**	**P. connection between 1 and 2?**
A.1 direct path	F.1 not part of the model	K.1 underestimated	P.1 yes
A.2 additional nodes as system components	F.2 scrambled text/numbers	K.2 overestimated	P.2 no
A.3 additional nodes as relays	F.3 color	K.3 realistic assesment	P.3 unclear
A.4 model too sparse	F.4 physical object (envelope, treasure chest)	K.4 model too sparse	**Q. certificates are introduced in 2**
B. cryptographic concepts	F.5 scribbled line	K.5 no control	Q.1 yes
B.1 end-to-end	F.6 encoded text/digits	**L. communication partner leaks data**	Q.2 implicitely (reference to 2nd drawing)
B.2 symmetric encryption	F.7 lock	L.1 no data leakage	Q.3 no
B.3 assymetric encryption	F.8 different language	L.2 leaks credit card data	Q.4 "stronger" certificates
B.4 ephemeral keys	F.9 chopped text	L.3 undefined data leakage	Q.5 yes, but they are misinterpreted
B.5 transport encryption	**G. provider role**	L.4 general distrust	**R. encryption point in 2**
B.6 blackbox	G.1 not part of the model	L.5 model too sparse	R.1 directly (local machine)
B.7 obfuscation or steganography	G.2 keyserver	**M. third parties**	R.2 crypto proxy
B.8 authentication	G.3 remote encryption component	M.1 centralized encryption service/proxy	R.3 after remote validation at remote service
B.9 model too sparse	G.4 local encryption component	M.2 PKI/CA	R.4 undefined
C. definiton quality	G.5 message release point	M.3 (ad) tracker	R.5 model too sparse
C.1 accurate model	G.6 in-software encryption	M.4 credit card provider/bank	**T. More technical buzzwords**
C.2 model too sparse	G.7 omnipotent observer	M.5 metadata leakage	T.1 yes
C.3 passphrase exchange	**H. confusion of concepts**	M.6 insiders	T.2 no
C.4 authentication	H.1 encryption equals authentication	M.7 successful intruders	T.3 conceptual representation
C.5 message is recognizable	H.2 encryption is a distinct service	M.8 unsuccesful intruders	**U. Distraction from knowledge gaps**
D. key generation and exchange	H.3 encryption is well-defined	M.9 authentication proxy	U.1 yes
D.1 model too sparse	H.4 model too sparse	M.10 model too sparse	U.2 no
D.2 Web of Trust	**I. model refinement (1-2)**	**N. HTTPS specific components**	U.3 knowledge gaps are explicitely admitted
D.3 PSK_keyserver	I.1 increased level of detail	N.1 certificates	**V. Representation**
D.4 PSK_in-person key exchange	I.2 decreased level of detail	N.2 keys	V.1 protocol-based
D.5 shared knowledge	I.3 constant level of detail	N.3 codebook (PKI)	V.2 conceptual
D.6 PSK_Undefined	**J. security indicators**	N.4 not part of the model	V.3 both
E. example scenario	J.1 https	N.5 model too sparse	V.4 model too sparse
E.1 abstract	J.2 lock icon	**O. model refinement (2-3)**	W. **Awareness of metadata**
E.2 arbitrary messaging app	J.3 check mark	O.1 increased level of detail	W.1 yes
E.3 WhatsApp	J.4 insecurity indicator	O.2 decreased level of detail	W.2 no
E.4 Signal	J.5 not part of the model	O.3 constant level of detail	
E.5 PGP/GPG			
E.6 not part of the model			