End User and Expert Perceptions of Threats and Potential Countermeasures

Simon Anell
*Helmholtz Center for
Information Security (CISPA)
Saarland Informatics Campus
Saarbrücken, Germany
s9sianel@stud.uni-saarland.de*

Lea Gröber
*Helmholtz Center for
Information Security (CISPA)
Saarbrücken, Germany
lea.groeber@cispa.saarland*

Katharina Krombholz
*Helmholtz Center for
Information Security (CISPA)
Saarbrücken, Germany
krombholz@cispa.saarland*

***Abstract*—Experts often design security and privacy technology with specific use cases and threat models in mind. In practice however, end users are not aware of these threats and potential countermeasures. Furthermore, misconceptions about the benefits and limitations of security and privacy technology inhibit large-scale adoption by end users. In this paper, we address this challenge and contribute a qualitative study on end users' and security experts' perceptions of threat models and potential countermeasures. We follow an inductive research approach to explore perceptions and mental models of both security experts and end users. We conducted semi-structured interviews with 8 security experts and 13 end users. Our results suggest that in contrast to security experts, end users neglect acquaintances and friends as attackers in their threat models. Our findings highlight that experts value technical countermeasures whereas end users try to implement trust-based defensive methods.**

***Index Terms*—Usable Security and Privacy, Mental Models, Threat Models**

1. Introduction

Human error is considered among the main causes of many security problems. All types of users ranging from end users to knowledgeable experts such as administrators, developers, and designers are confronted with security decisions that they are incapable of making in an informed way. In fact however, every human in the chain who is considered an expert contributes to making the Internet ecosystem secure and user friendly. Their decisions when designing, developing, or configuring systems heavily impact how users perceive and understand the system. Such functional mental models are important for users to make technically sound security decisions. Each of these humans has a different perspective. While theorists who design cryptographic protocols aim for correctness, users at the more practical end of the spectrum value - in the broader sense of the meaning - a usable application.

Out of these diverse objectives and various backgrounds, different understandings and perceptions of security and threats emerge. On the one hand, users often do not understand the theoretical fundamentals behind systems, i.e., how and why they work and in particular, how IT-applications can be secured. On the other hand, back end-developers do not primarily consider how applications they develop are perceived and used by end users.

In this work, we explore how users and experts perceive security concepts and which threat models they have. We furthermore qualitatively describe the gap between experts' and lay users' perceptions.

In particular, we explore which threat models experts and end users consider relevant and how they perceive the potential damage associated with these threats. We also identify actors or beneficiaries of the threats and participants' reasoning behind potential intentions of attackers. We also study which methods both groups of participants consider as prevention techniques against these attacks.

Related work examined mental models of users regarding specific security technologies and topics, e.g., Krombholz et al. for HTTPS [7] and Wu et al. for encryption [13]- or focused on age groups - see Frik et al. for elderly people [2].

While all of these studies focused on specific technology or application areas, no other study considered general threats that users face in the Internet ecosystem. Our research follows an inductive approach; we conducted a formative interview study with 8 security experts and 13 end users and identify dimensions of perceived threats for each group of users. Although our study has a relatively small sample size, it provides insights to understand the gap between the end users' and the experts' understanding of relevant threat models. We are confident that the results of this formative interview study lay important foundations for future work with respect to specific technology and use cases.

2. Related Work

Mental models play a fundamental role in human decision making. How we understand the world influences how we behave and react. In this chapter, we examine related work that focuses on mental models w.r.t. security and privacy perception or the usability of deploying security or privacy increasing systems.

It is hard to change mental models in order to force or favor a specific behaviour. Wash et al. [11] presented ideas to influence mental models towards more secure behaviour even for non-tech-savvy end users.

The necessity to not only include end users but also experts is supported by findings of Krombholz et al. [8]: Even administrators struggle to deploy HTTPS securely and need to rely on online sources.

Also, Krombholz et al. [7] studied the mental models of both end users and administrators of HTTPS and conducted a study with 30 participants. Among others, they found severe misconceptions regarding it-security concepts such as authentication and encryption and discuss design implications for interfaces and protocols. Kang et al. [6] studied how laypeople and people with computer science background understand the internet and its effects on privacy and security decisions. The authors conclude that privacy and security decisions should not primarily rely on users' practices.

Additionally, Gallagher et al. [3] present a mental model study that exposes faulty mental models of experts and users w.r.t. Tor, which could lead to wrongful use with unwanted consequences of the tool. Wu et al. [13] explored users' mental models of encryption. They present a qualitative study with 19 semi-structured interviews that only focuses on this specific issue and come up with four mental models of encryption. The research of Zeng et al. [14] shows that mental models of end users often do not match with reality. They explore the mental models users have of threats regarding smart-home devices. Redmiles et al. [9] explored the decision making behind security-relevant decisions of end users with a qualitative study.

With a growing number of users of smart home devices, the number of people affected by privacy and security problems coming with this relatively new technology is growing, too. In their work, Tabassum et al. [10] showed that users tend to transfer threat models they have from other computing areas to the field of smart home. The authors give several recommendations for developers of smart home systems, such as providing more transparency and control and educating users about potential risks.

Wash et al. [12] surveyed United States Internet users in order to check causal beliefs regarding computer security and security promoting practices of the participants.

3. Methodology

As a first step to address user perceptions of security terminology and threat models from a holistic perspective, we chose an inductive research approach.

Our results should be interpreted as a formative interview study with different types of users. We designed a semi-structured interview guideline; the full Interview guideline can be found in Appendix A. We recorded and transcribed all interviews and then two researchers performed independent open coding. We conducted interviews until no new themes emerged, until *saturation* was reached [4].

We conducted one interview via Skype, and the remainder of the interviews face-to-face. The same semi-structured interview guideline was used for end users and experts. Among all participants, we raffled a 50 Amazon voucher. Our university's ethical review board (ERB) approved our study.

3.1. Briefing

Before the audio recording started, we informed the participants about the interview topic and procedure. We emphasized that there are no right or wrong answers to our questions and that the aim of the study was to capture the genuine perceptions of the participants and not to examine technical understanding of IT-Security topics. We briefly explained the analysis of the interviews which includes the anonymous transcription of the recording. We informed them of their right to discontinue the interview at any point in time without giving a reason and that they can contact us at any point after the interview and request the deletion of their data. The participants were given a written informed consent form to sign that includes all of the previous information (see Appendix C).

3.2. Interview Guideline

The interview guideline was structured according to the following topics:

1) Internet usage and devices
2) Threats towards the participants and their devices.
3) Threats towards the interaction with a 3rd party e.g. the provider of an online shopping service.
4) Threats towards the 3rd party.

IT-security as a topic for an interview can be intimidating for end users. This is why we started with basic, non-technical questions about Internet and device usage. In order to collect genuine threat models (threats that are vital and obvious for the participant), we try not to restrict or influence the participants with our questions. This is why we ask briefly and openly to "*think of **threats** towards the end user and their devices*".

Based on the answers, it is necessary to clarify or to go deeper and query additional information about the mentioned threats and dimensions that are important parts of the threat landscape. Our intention is to capture dimensions and themes about potential **attackers** and their **intentions**, **maximum damage** than can be caused, **how** the attack is executed and finally what can be done by end users in order to **prevent** or **defend** against such a threat.

We continued by depicting a brief example scenario to introduce 3rd party IT-infrastructure. As a reference point, we mentioned a provider of a service that most likely everyone has used at some point: an online shop. Participants should think of threats that target the process of ordering an item in this shop. Additionally to the important information mentioned above, the participant should now both think of defensive actions carried out by themselves as customers and also by the provider.

Finally, the participant should think of threats directly targeting the providers and their infrastructure. Here, also both parties should be taken into account when thinking of defense methods.

3.3. Pilot Study

We conducted a pilot interview with one end user and found that the questions were too technical. The participant requested clarification for these questions several times. We dropped explanations of technical terms and added the online shop scenario to make the situation more tangible. Additionally, we collected feedback from a psychologist on the study design and the structure of the interview guideline.

3.4. Recruitment

We recruited thirteen end users; the main sampling criteria was to not have a background in computer science. End users were recruited via snowball sampling, word-of-mouth recommendations of acquaintances, and postings on the bulletin boards at the university campus. Participants could contact the interview coordinator via phone or email. The interview was announced as "Interview about IT Security". A familiarity distance of at least 1 to both of the interviewers was maintained which means that interviewers did not interview direct acquaintances. To counter social desirability bias and avoid intimidating influences, we did not conduct interviews with end users at our research institute but in a place of their choice where they felt comfortable. At the request of the participants, interviews were also conducted at their apartment, a neutral room at our university or their workplace.

For our sampling method, we define experts as persons that fulfill at least one of the following criteria:

1) an expert is a person that has at least 3 years of work experience as a security developer or security consultant, or
2) a person who studied computer science or cybersecurity and has work or research experience in the field.

We recruited experts via word of mouth and emails and interviewed eight experts, six of them were researchers from different research areas and different fields of work. All experts were male and aged between 23 and 39. We conducted the expert interviews either in our lab or via Skype.

Participants were asked to give their consent to the audio recording and the anonymous transcription and analysis of the interview.

3.5. Participants and Demographics

In total, our analysis is based on 21 interviews with experts (*N*=8) and end users (*N*=13). All interviews were conducted in German. The participants were German, Italian, Swiss, and Portuguese nationals and aged between 17 and 53 years, all spoke German at a native level. The interviews lasted between 11 and 34 minutes.

In the end user sample, we had seven female participants and six male (54% female). End users' age ranged from 17 to 53 (*avg*=27,2 years). Seven of them were working full-time, six were students (two at schools, four at different universities).

Experts were skewed to the younger side (*avg*=27,3) and age ranged from 23 to 39. Our expert sample included four security-focused grad students, three Ph.D. students concerned with IT-security, and one senior researcher. All experts had working and/or research experience in IT-security. Expert research and work fields ranged from web security over automotive security to mobile security, protocol verification, security consulting and penetration testing. Except for the group criteria, age, gender, citizenship and occupation, we did not query any demographic data and did not actively seek certain statuses of these characteristics. We refer to end users as U1,...,U13 and to experts as E1,...,E8.

	Interview 1	Interview 2	Interview 3	Interview 4	Interview 5	Interview 6
Experts	0,81	0,82	0,89	0,86	0,9	0,93
End Users	0,74	0,92	0,7	0,9	0,86	0,8

TABLE 1. KRIPPENDORFF'S ALPHA FOR THE FIRST TWELVE INTERVIEWS AS A MEASUREMENT FOR INTER-RATER RELIABILITY

3.6. Evaluation and Coding

We sectioned the transcriptions into logical blocks which ideally consist of snippets of conversation that deal with distinct concepts. By the nature of an open conversation, concepts are distributed over several sections and one section includes several concepts. Two researchers iteratively coded primary codes for twelve interviews, six interviews of each group. After examining the first, randomly chosen interview, one researcher proposed the first draft of a codebook that was discussed and modified. After each interview, the two coders resolved conflicts and modified the preliminary codebook. The final version of the codebook can be found in Appendix B. The two coders achieved a Krippendorff's Alpha of 0.85 (0.88 for the expert interviews and 0.82 for the end user interviews, see Table1). After the first twelve interviews were coded, one of the two coders coded the remainder of the interviews with the established codebook. After finding the main themes for each interview, for both of the groups, we took a look at the set of interviews and merged the information to come up with a group-specific overview for each threat that includes the possible damage, the attackers and their objectives and methods to prevent or defend against the attack. This technique is known as axial coding. After this step, we are able to expose prominent concepts for each group and can qualitatively compare the groups.

4. Results

In this section, we provide an overview of all *threats* that the participants mentioned as well as an overview of the *attackers* that were identified and in addition *countermeasures* and preventive methods.

For every threat we include *damage* that is done by the respective threat, *attack vectors*, identified *attackers* and recommended *countermeasures*. We highlight all codes with italic font.

We provide figures to depict the information given by experts with dashed lines and the information given by end users with dotted lines. Table 2 shows how often each threat was mentioned by both the end user and the expert group.

4.1. Threats

4.1.1. Malware. The concept of *malware* [fig. 1] is prevalent in both groups - mentioned by nine end users and six experts. Participants brought up various ways of being infected by malware. These include malware being *downloaded and executed* unknowingly, and malware as a *byproduct of software*. End users mentioned access to the device and the following *data loss*, *not being able to use the device* and being included in a *botnet* as characterisations of malware.

Experts added *code-execution*, *being compromised* (e.g. via keylogger), reduced *performance* up to *not being able*

Threats		
Threat	End Users	Experts
Malware	9 (69%)	6 (75%)
Physical Theft	3 (23%)	3 (38%)
Phishing	6 (46%)	6 (75%)
Ransomware	0 (0%)	4 (50%)
XSS/Webattacks	2 (15%)	6 (75%)
Shoulder Surfing	0 (0%)	3 (38%)
Imitation	3 (23%)	5 (63%)
Data Loss	13 (100%)	8 (100%)
Denial of Service	3 (23%)	4 (50%)
Identity Theft	4 (31%)	4 (50%)
Stalking	2 (15%)	0 (0%)

TABLE 2. NUMBER OF THREATS MENTIONED BY END USERS AND EXPERTS

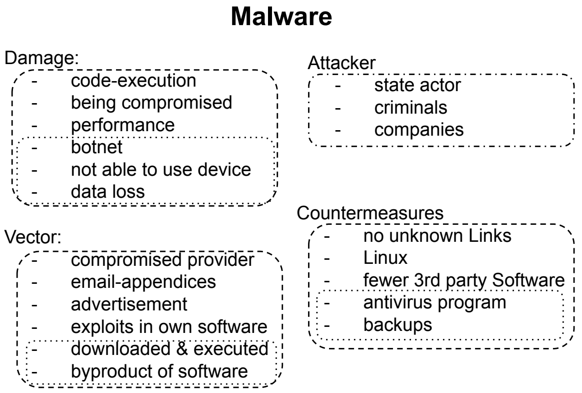

Figure 1. Malware (dashed lines for expert responses, dotted lines for end user responses)

to use the device and being included in a *botnet*.
Attackers were identified as *state actors*, *criminals* or *companies* by both groups. *Backups* and use of an *antivirus program* were the most prominent countermeasures mentioned. Using *Linux*, following *no unknown links* and using *fewer 3rd party software* was only recommended by experts.

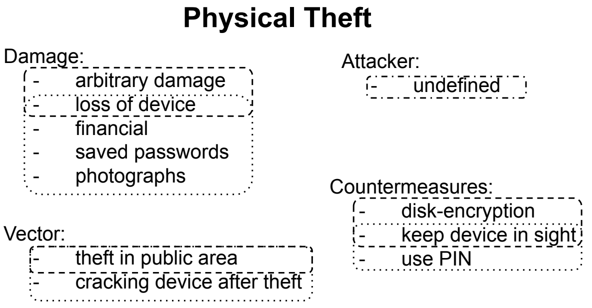

Figure 2. Physical Theft

4.1.2. Physical Theft. Consequences of *physical theft* [fig. 2] of a personal device were identified as the *loss of device* for both groups. *Financial* loss that comes with it, losing *saved passwords* and personal *photographs* was added by end users.
The device can be lost by *theft in public places* and, for end users, *cracking the device after theft*. Both groups did not specify the attacker. *Disk-encryption* to ensure data integrity after theft was mentioned by experts, *keep device in sight* by both groups and *using a PIN* for data integrity was added by end users.

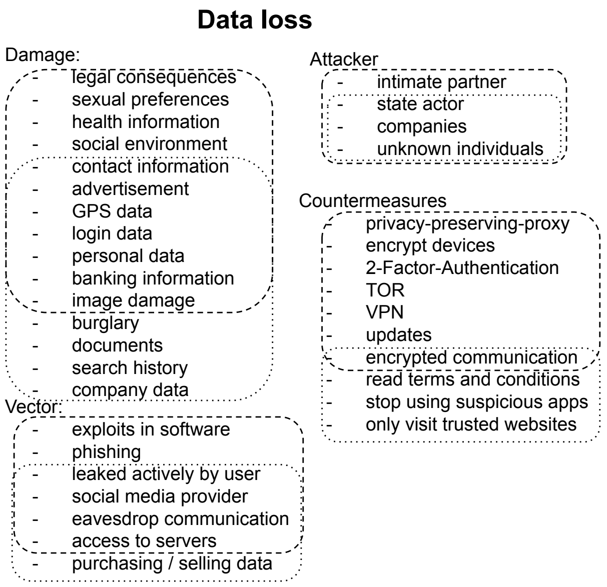

Figure 3. Data Loss

4.1.3. Data Loss. Attackers collecting all kinds of data is an omnipresent theme. All participants identified involuntary or unwanted *data loss* [fig. 3] as a threat. Various attackers, intentions, and procedures to get personal data were mentioned and categorized as *data loss*. Both groups mentioned data being lost to an adversary, e.g., *contact information*, *GPS data*, *login data*, *banking information* and *image damage* for companies. Personalized *advertisement* was mentioned as a consequence. Only experts mentioned *legal consequences* for companies that do not meet security standards. Also, experts brought up the loss of *health information*, *sexual preferences* and the exposure of ones *social environment* as dimensions of *data loss*. End users added being susceptible to *burglary* - if data about expensive online purchases and addresses are lost -, loss of *documents*, *search history* and *company data*. Attackers could act out of financial reasons, because of general surveillance for a state actor and out of curiosity and were identified as *state actor*, *unknown individuals*, *companies* and - only by one expert - *intimate partners*.
As countermeasures experts suggested using *privacy-preserving-proxies*, *encrypt devices*, *deploying 2-Factor-Authentication*, using *Tor* and *VPNs* and keeping systems *updated*. Both groups mentioned *encrypted communication*. End users added that it might help to *read the terms and conditions*, to *stop using suspicious apps* and to *only visit trusted websites*.

4.1.4. Identity Theft. Participant state that attackers require a *comprehensive profile* and *login data* for *identity theft* [fig. 4]. *Identity theft* was mentioned explicitly by several participants which is why we decided to treat this as an own relevant threat and as a possible consequence

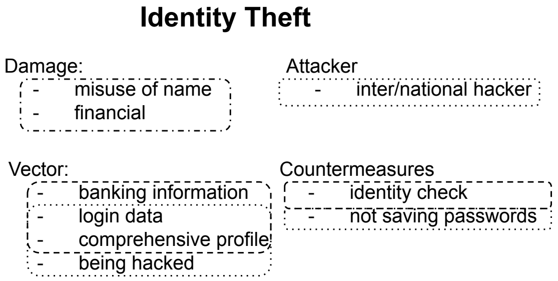

Figure 4. Identity Theft

of *data loss*. As previously stated, vast personal data and logins are crucial requirements mentioned by the participants. With sufficient *personal data* it is possible to build a *personal profile* that enables attackers to pose as the victim. The *misuse of name* then leads to *financial* damage.

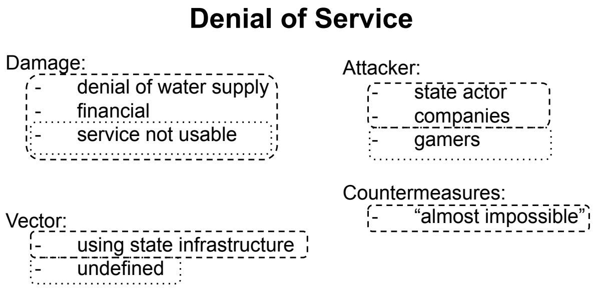

Figure 5. Denial of Service

4.1.5. Denial of Service. *Denial of Service* [fig. 5] was brought up by both groups. The targeted *service being not usable* anymore is the inherent consequence. End users did not specify how such an attack could be implemented and experts mentioned *state infrastructure* as a means. E4 mentioned the possibility of state-driven *denial of water supply* towards foreign states by *denial of service* attacks. *Companies* and *state actors* were identified as attackers by the experts. End users mentioned *gamers* as attackers. Experts thought that state-driven denial of service attacks as *almost impossible* to counter.

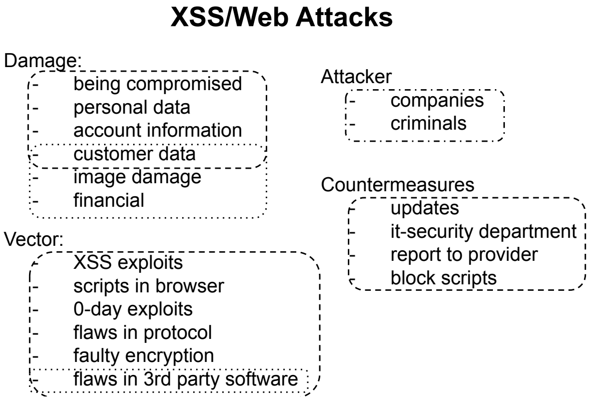

Figure 6. XSS and Web Attacks

4.1.6. XSS/Web Attacks. From both groups it emerged that *XSS and Web Attacks* [fig. 6] are a potential reason for *customer data* being lost. Only experts brought up loss of *personal data*, *account information* and *being compromised*. End users added *image damage* and *financial damage* for *companies*. Attack vectors mentioned by experts are using *XSS exploits* and *scripts in browsers*, *0-day exploits*, *flaws in protocols* and *faulty encryption*. Both groups mentioned *3rd party software* as a measure to attack. *Companies* and *criminals* were identified as attackers by both groups. While end users did not come up with countermeasures, experts suggested *updates*, a proper *it-security department* for companies, *reporting* suspicions to the provider and *blocking scripts* in the browser.

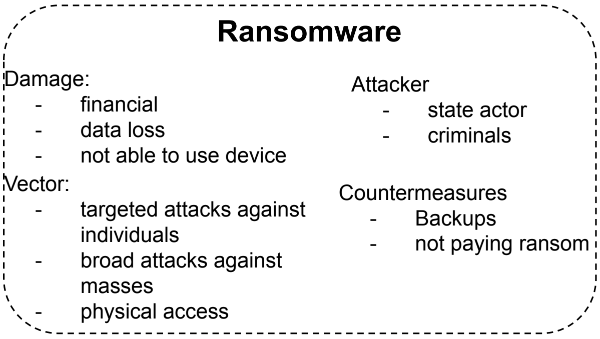

Figure 7. Ransomware

4.1.7. Ransomware. *Ransomware* [fig. 7] was only mentioned by experts. We categorize *ransomware* separately and not as *malware* because the characteristics are clearly qualifying for a individual treatment. Damage caused by by ransomware are *data loss* in cases where data cannot be decrypted, *financial* in case the ransom is paid or the *device cannot be used* anymore. Experts mentioned *targeted attacks against individuals* and *broad attacks against unspecified masses* as possibilities to distribute ransomware. Also, *physical access* by an attacker was added to the attack vectors. Participants identified *state actors* and *criminals* as possible attackers and suggested *not paying the demanded ransom*. One should rather keep consistent *backups* in order to set up the system again.

4.1.8. Phishing. *Phishing* [fig. 8] was one of the most prominent threats identified by both groups. Six participants recognized *phishing* as a threat, referring to broad attacks with *lists of emails* or *personalized, more targeted attacks* composed by using stolen data (spear-phishing). End users and experts mentioned *financial loss*, loss of *personal data*, *banking information* and *login data* as

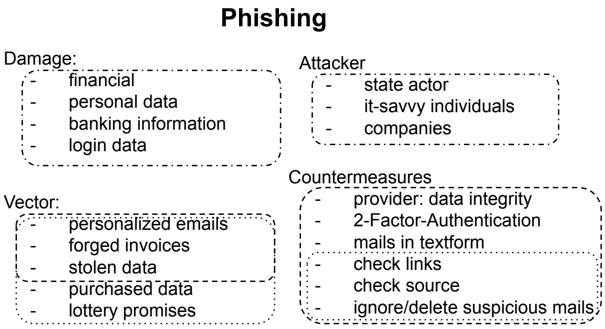

Figure 8. Phishing

damage done by *phishing*. Attackers would leverage stolen data to personalize deceiving emails and forge invoices. U5 mentioned using *bought data* to implement *phishing attacks*. U2 added using *lottery promises* as a method to deceive targets. Attackers can be *state actors*, *companies* and *it-savvy individuals*. In order to counter these attacks, participants express a general scepticism towards emails that query critical data. If an email comes with an invoice or payment request, participants stated that it is important to check if they actually purchased any item that would require such an invoice via email. Also, according to some participants, *suspicious mails* should be *ignored* and/or *deleted* right away. Others recommend *checking the source* and *links* provided before following them. In case login information is lost, experts propose *2-Factor-Authentication* such that the possible damage is limited.

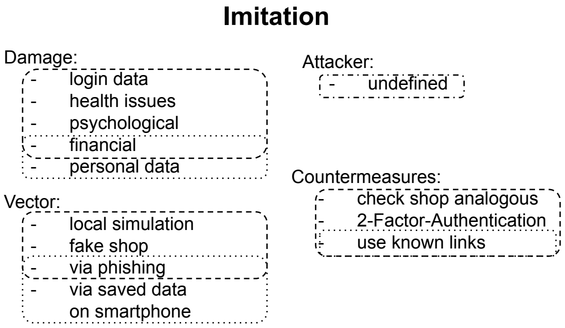

Figure 9. Imitation

4.1.9. Imitation. *Imitation* [fig. 9], the simulation of a service in the internet, was a threat mentioned by both groups. Since is it not necessary to use phishing mails to guide the victim to a *fake website*, we treated Imitation as an own threat. *Imitations* could be a copy of an existing shop or a *fake shop* in itself and try to catch *login data* and *money* from victims. Experts mentioned *health issues* as a consequence since a Patient could order medicine in a fake shop that would never arrive. Also, deceived buyers can be affected by *psychological* problems because they did fall for the scam. The attacker was not closer defined. A recommended countermeasure with both groups is only *using known links*. Experts again added using *2-Factor-Authentication*. E5 suggested *checking for the shop analogously*, e.g. in the commercial register of the state.

Attackers		
Threat	End Users	Experts
Companies	9 (69%)	6 (75%)
State Actor	2 (15%)	6 (75%)
Criminals	10 (77%)	6 (75%)
Acquaintances	2 (15%)	3 (38%)
Intimate Partners	0 (0%)	1 (13%)
Bystanders	0 (0%)	1 (13%)

TABLE 3. NUMBER OF ATTACKERS MENTIONED BY END USERS AND EXPERTS

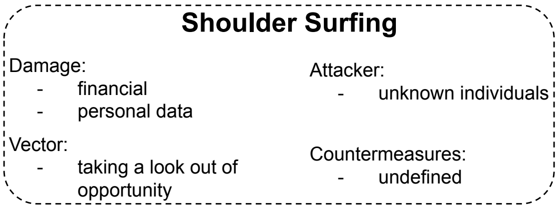

Figure 10. Shoulder Surfing

4.1.10. Shoulder Surfing. *Shoulder surfing* [fig. 10], the act of *taking a look at the screen* of someone else, was only mentioned by experts. As a consequence of people taking the opportunity to take a look and use the observed data later on were identified as *financial* consequences and the loss of *personal data*. Attackers were described as *unknown persons* that just happen to be near the victim. Countermeasures were not defined.

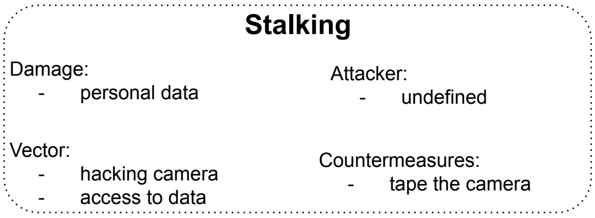

Figure 11. Stalking

4.1.11. Stalking. *Stalking* [fig. 11] was mentioned by two end users only. The intention of the attacker, who was not described in detail, was identified loosely as physically stalking someone or to search for certain *personal data*. This could be achieved by *hacking the camera* of a personal device and using *access to data* and could be countered by *taping* the laptop *webcam*.

4.2. Attackers

In this section, we provide an overview of the attackers that the participant imagined and elaborate on their intentions. Table 3 gives an overview of the number of mentions for each group. Participants often did not paint a clear picture of possible attackers. Even after requesting traits and details of an adversary for concrete threats, we often only got vague statements or the clear declaration: "I don't know."

A possible explanation for this is part of the discussion section. We identified the following attacker models, which include the attacking party, the intentions of this party, the methods used, and the damage done by the attacker. Still, we will not focus on the damage that these attackers cause with their actions - this was part of the previous section - but rather on the intentions.

4.2.1. Companies. End users and experts mentioned companies as beneficiaries behind attacks. The most prominent theme was *generating profit* out of end user data. This can be done *directly selling data* about the companies customers - U5 disclosed that they witnessed this first hand when working in a company. Participants also mentioned using data to improve advertising and by that *generating more profit*. Some end users rated *massive data collection in order to make money* as the right of the companies and U3 even stated that one could read the terms in conditions to be certain of those practices. In addition, both end users and experts mentioned companies illegally obtaining data from rival companies or targeting rivals with denial of service attacks *to harm them*.

4.2.2. State Actor. Both experts and end users mentioned state actors as attackers. While the possible intentions of state actors for end users were limited to *espionage*, experts could imagine additional reasons. Among them are *demonstration of power* with denial of service attacks or hacking big foreign companies *to cause financial harm*. Noteworthy is the idea that state actors could target the water supply of foreign states. Apart from a general description of a state as an attacker, both official state organs like intelligence agencies and covert groups that would work under government guidance were mentioned as possible actors. Participants also mentioned *general surveillance* by state institutions as an intention and E3 stated:

> *For states, gathering data is less about specific attacks and more like "Having more is better". They collect it in order to do Big Data stuff.*

Both groups described state actors as powerful attackers that are difficult to counter.

4.2.3. Criminals. Hackers and Criminals, be it individuals or groups, have one thing in common. The act and the intention is vicious from the beginning and involves planning. We clearly state that every other attacker described in this section also can have vicious intent and use illegal and/or immoral methods. Intentions mentioned were gaining *financial profit* or just *harming the attacked party*. We also include developers of software in this category who knowingly include malicious advertisements to their product.

4.2.4. Acquaintances. Friends and family were only seen as possible attackers by experts. Also, colleagues were not mentioned as possible attackers by end users. Experts identified attacks from friends, family, and colleagues as *less serious* with intentions like *playing a prank* on the victim or to *make somebody's day*.

4.2.5. Intimate Partners. Only E5 casually mentioned intimate partners as potential attackers. The intention was identified as the demand to *desire to know about the conversations* the partner is having.

4.2.6. Bystanders. Only E6 mentioned shoulder surfing as a threat and identified bystanders as attackers. These people would act out of *opportunity* or *curiosity*, there was no initial malicious intent or planning. Thus, they are not included in the *criminals* section.

4.3. Prevention and Defense Methods

Experts described prevention and defense methods in more detail and more extensively than end users. In this section we depict the most prominent countermeasures that were mentioned.

Both groups recommended checking links before clicking and ignoring or deleting suspicious emails. Experts' top advice was keeping systems updated and being mindful of HTTPS. 2-Factor-Authentication was only mentioned by experts for different threats. Backups were equally prominent with experts and end users. Encrypting physical devices was mentioned by half of the experts explicitly and not by end users. While encrypted communication was mentioned by both groups, HTTPS was only mentioned vaguely by U4:

> *Somehow there is this HTTPS at the beginning of the bar. I think, if there is something missing... i don't know. If something is missing it is not the genuine website. I think, if the S is missing at the end. Then one should be suspicious.*

Antivirus programs as a preventive method were mentioned by all but one end user and only by one expert who does not even use antivirus software. End users promoted only visiting known and trusted websites more prominently than experts.

5. Discussion

End user and expert perceptions vs. the technical reality. Our findings on countermeasures and preventive methods for the use of *antivirus programs*, *updates*, *trusted websites* and being mindful of *HTTPS* are in line with the findings of Ion et al. [5]: End users would promote visiting trusted websites and using antivirus software whereas experts advice to use updated software and HTTPS connections.

Recent works on shoulder surfing suggest that close acquaintances are also likely to be shoulder surfers [1]. It is particularly noteworthy that the end users that we interviewed for our study did not consider friends, colleagues, or intimate partners as potential attackers. We hypothesize that this is due to the following reasons: In our study, end users were confronted with a possibly intimidating topic in an intimidating interviewing situation. We tried to make them feel as comfortable as possible, but still, social desirability could have affected the participants' responses. For a study about IT-security, attackers that would be educated in information technology such as *hackers* might be obvious choices for end users. Also, after several data scandals caused by social media companies (e.g. Facebook and Cambridge Analytica), that were covered by the main-stream media, might add up to end users considering these companies as possible attackers. In fact, companies and rudimentary described criminals or hackers were the most common attackers for end users.

Although ransomware has been quite present in recent years and has been widely covered in the media (e.g. WannaCry 2017), it was not mentioned by any end user and only by 4 experts. U4 mentioned hospitals being hacked and blackmailed but identified stolen data as leverage. This could indicate a low technical understanding of the characteristics of ransomware.

End users vs. experts. End users did not mention device encryption explicitly as experts did. U4 mentioned using a PIN code to secure the device when being stolen which actually enables the encryption for the iPhone model of the respective user. In the same context, U4 stated that using the PIN would still not help in case an attacker has access to a personal computer. This suggests that end users have misconceptions about the security of PINs.

Experts were more consistent than end users when reporting on their reasoning about potential threats. This means every threat that was mentioned by the expert group was mentioned by at least three experts.

Design challenges and future work. Based on our findings, we hypothesize that end users are often not motivated to perform a security measure as the associated threat models and their impact on device security are not clear to end users. Our results suggest that in some cases, end users and experts perceive entirely different attackers as likely. Based on the findings from this study we argue, that our community should start to incorporate prospective users in the design process to tie security technology more to their needs; either (1) to better understand which threats actually matter to them, and (2) if these perceived threats do not correspond with the technical reality, design security technology that helps them to understand the actual benefits of security technology and actually relevant threats. As mental models are mostly informed by experience and design, we argue that future work should focus on the interplay of mental models and the design of security technology. We therefore plan to explore user-centered and value-centered design methods.

Limitations of our study. We recognize that our convenience sample is all male and see the emerging problems. Unfortunately, it is still hard to find female experts in information security-related fields. We tried to recruit experts with different backgrounds and recognize that we should also have focused more on recruiting female experts and practitioners. While we state that valuable results have been found and we reached saturation, a larger, more diverse sample of participants for both groups could have resulted in additional findings. Due to our inductive approach and the qualitative nature of our study, our results have informed models and theories about end user and expert mental models. Thus, we cannot draw conclusions on quantitative aspects, such as the prevalence of mental models in different user groups. Hence our provided numbers can only be interpreted as rough indicators that need further testing with larger quantitative studies. We are aware of biases, e.g. social desirability bias, that come with qualitative research based on interviews with end users and which we are not able to counter completely.

6. Conclusion

In this work, we presented a formative interview study to explore mental models of threat models of both end users and experts in a technology-agnostic and holistic way. We found deep insights into the threat models for both groups.

We discovered differences in attacker models and revealed preventive methods and countermeasures used by end users and experts. Experts would consider state actors as attackers far more prominently than end users.

We found that end users would not consider close acquaintances and intimate partners as potential attackers. End users value trust-based countermeasures whereas experts overall promote more technical measures such as using 2-Factor-Authentication. Future work could include querying samples with participants from different regions. We did not target participants who use smart home devices and none of our participants mentioned threats related specifically to these systems. Future work should explore mental models of privacy and security of smart home devices sampling participants using these devices.

In addition, such work could shed light on the fact that acquaintances, friends, and especially intimate partners are not present in end user mental models of potential attackers.

References

[1] Malin Eiband, Mohamed Khamis, Emanuel von Zezschwitz, Heinrich Hussmann, and Florian Alt. Understanding shoulder surfing in the wild: Stories from users and observers. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, CHI '17, page 4254–4265, New York, NY, USA, 2017. Association for Computing Machinery.

[2] Alisa Frik, Leysan Nurgalieva, Julia Bernd, Joyce Lee, Florian Schaub, and Serge Egelman. Privacy and security threat models and mitigation strategies of older adults. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*, Santa Clara, CA, August 2019. USENIX Association.

[3] Kevin Gallagher, Sameer Patil, and Nasir Memon. New me: Understanding expert and non-expert perceptions and usage of the tor anonymity network. In *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*, pages 385–398, Santa Clara, CA, July 2017. USENIX Association.

[4] Greg Guest, Arwen Bunce, and Laura Johnson. How many interviews are enough?: An experiment with data saturation and variability. *Field Methods*, 18(1):59–82, 2006.

[5] Iulia Ion, Rob Reeder, and Sunny Consolvo. "...no one can hack my mind": Comparing expert and non-expert security practices. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, pages 327–346, Ottawa, July 2015. USENIX Association.

[6] Ruogu Kang, Laura Dabbish, Nathaniel Fruchter, and Sara Kiesler. "my data just goes everywhere:" user mental models of the internet and implications for privacy and security. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, pages 39–52, Ottawa, July 2015. USENIX Association.

[7] Katharina Krombholz, Karoline Busse, Katharina Pfeffer, Matthew Smith, and Emanuel von Zezschwitz. "if https were secure, i wouldn't need 2fa" - end user and administrator mental models of https. In *S&P 2019*, May 2019.

[8] Katharina Krombholz, Wilfried Mayer, Martin Schmiedecker, and Edgar Weippl. "i have no idea what i'm doing" - on the usability of deploying HTTPS. In *26th USENIX Security Symposium (USENIX Security 17)*, pages 1339–1356, Vancouver, BC, 2017. USENIX Association.

[9] Elissa Redmiles, Amelia Malone, and Michelle Mazurek. I think they're trying to tell me something: Advice sources and selection for digital security, 01 2015.

[10] Madiha Tabassum, Tomasz Kosinski, and Heather Richter Lipford. "i don't own the data": End user perceptions of smart home device data practices and risks. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*, Santa Clara, CA, August 2019. USENIX Association.

[11] Rick Wash and Emilee Rader. Influencing mental models of security: A research agenda. In *Proceedings of the 2011 New Security Paradigms Workshop*, NSPW '11, pages 57–66, New York, NY, USA, 2011. ACM.

[12] Rick Wash and Emilee Rader. Too much knowledge? security beliefs and protective behaviors among united states internet users. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, pages 309–325, Ottawa, July 2015. USENIX Association.

[13] Justin Wu and Daniel Zappala. When is a tree really a truck? exploring mental models of encryption. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*, pages 395–409, Baltimore, MD, 2018. USENIX Association.

[14] Eric Zeng, Shrirang Mare, and Franziska Roesner. End user security and privacy concerns with smart homes. In *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*, pages 65–80, Santa Clara, CA, July 2017. USENIX Association.

Appendix A. Interview Guideline

A.1. Introduction

I would like to start the interview with questions on your internet usage behaviour.

1) How much time do you spend in the internet daily, including social media, news, surfing, watching videos, working?
2) Which devices do you use?

A.2. Personal IT-Infrastructure Related

Now, I would like to ask you about threats towards your infrastructure. Keep in mind that there are no wrong answers.

1) What threats can you imagine for these devices?
2) Who do you think could have an interest in attacking you?
3) What do you think are the attacker's intentions?
4) How do you think they could do that?
5) What do you think could be the maximum damage dealt?
6) How do you think you can defend yourself against these attacks?
7) Which of these techniques are you using? If you are not using a technique, why?

A.3. Interaction with 3rd-Party Infrastructure

Thank you for your answers so far. I would now like to ask you about dangers regarding the communication between you and a third party. Let's say that you are communicating with one of your devices with the provider of an online service. This could be a online shop or a bank.

1) Can you think of threats when communicating with the provider?
2) Who do you think could have an interest in an attack?
3) What do you think are the attacker's intentions?
4) How do you think they could do that?
5) What do you think could be the maximum damage dealt?
6) How do you think you can defend yourself against these attacks?
7) Which of these techniques are you using? If you are not using a technique, why?

A.4. 3rd-Party-Infrastructure Related

Thank you. Now i would like to ask you about threats directly towards the third party, like the provider of the online service.

1) What threats can you think of that target the provider directly?
2) Who do you think could have an interest in an attack?
3) What do you think are the attacker's intentions?
4) How do you think they could do that?
5) What do you think could be the maximum damage dealt?
6) How do you think the provider can defend against these attacks?
7) How do you think you can contribute to the safety of the provider?

Appendix B. Codebook - Primary Codes

- Affected Party: User, Provider, Others (e.g. 'communication')
- Affected Devices: Smartphone, Laptop, PC, Tablet, Smart Home Device
- Phishing Mail
- XSS and Webattacks
- Malware
- Ransomware
- Imitation
- Shoulder Surfing
- Physical Theft
- Data Loss
- Identity Theft
- Stalking
- Denial of Service
- Damage
- Attacker
- Usability
- Attacker Intention
- Attack Method
- Countermeasure
- Security Assessment

Appendix C.
Consent Form

Research purpose: In this interview we look at the understanding and perception of participants in IT security terminology and attacker models.

Voluntarily: Your participation in this study is voluntary. You can revoke your consent at any time and without giving reasons. You can also cancel the interview at any time without giving reasons, or request the deletion of your data after completing the study.

Benefits and Compensation: There are no direct benefits for you from participating in the study other than participating in the lottery for a shopping voucher. However, your experience contributes as a basis to a better understanding of the perception of IT security terminology and to make secure applications more usable.

Data protection: [institution redacted] considers data protection issues as highly important. Our procedures in this regard are in accordance with the relevant [country redacted] data protection laws and regulations. Apart from your age, gender (voluntary information) and educational background, no personal data is collected. The data collected during the survey is used exclusively within the framework of the research project. The data will not be passed on to third parties or used in any other way.

With my signature I confirm that I have read this declaration of consent and declare my voluntary participation in this study. I have understood that I can cancel the study at any time.