Folk and Expert Mental Models of Security and Privacy

Wasif Altaf[1]*and Christian Tiefenau[1,2]†

[1] Department of Computer Science, Bonn University, Germany
wasif@uni-bonn.de
[2] Institute of Computer Science 4, Bonn University, Germany
tiefenau@cs.uni-bonn.de

Abstract

In this paper we predominantly reviewed recently published literature related to general end users', developers' and security and privacy professionals' mental models of security and privacy to explore current state of the art. We then extracted features of mental models of security and privacy for the aforementioned types of users and analyzed them in some detail to draw useful conclusions and trends. We conclude that there does not exist any design and development methodologies which implicitly address users' security and privacy concerns. However, development of such methodologies would be a challenging non-trivial task because users' mental models are ever evolving, diverse (based on the sophistication of their knowledge), gender biased and sometimes self-conflicting. Nonetheless, we found security and privacy professionals' guidelines provided in literature for improving users' mental models of security and privacy to be of paramount importance towards assessing and addressing risks.

1 Introduction

Mental models (MMs) are mental representations and associated processes for manipulating information related to entities or activities [14]. Also defined similarly by [5], mental models are models of reality created by mind to help understand, reason, explain and anticipate events. However, different users or stakeholders of a system may have various levels of knowledge regarding a subject under consideration. In this paper, we explore various stakeholders such as end-users, computer literate individuals, administrators and developers' mental models concerning security and privacy (SECAP) in different computer systems or computer related technologies.

We reviewed predominantly more recently published literature in the subject matter and extracted features related to mental models of security and privacy, and discussed as well as analyzed them in some detail. The features extracted from the literature reviewed have been used as basis for discussion, conclusions and future work.

The rest of paper has been organized as follows. In section 2, we discuss array of features for mental models of security and privacy considered in research work by various authors in subjects related to security and privacy of computer systems. In section 3, the results of features extraction have been discussed and analyzed. While in section 4, conclusions have been drawn from the analysis of features, relevant recommendations have been made, and possible lines of future work have been presented.

*Carried out the research and created document
†Supervised the research and reviewed the document

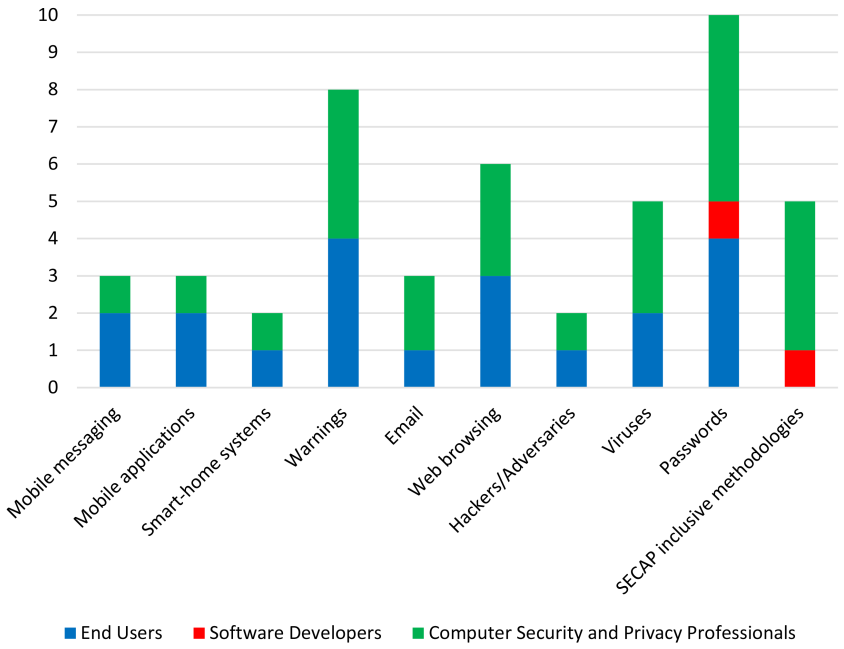

Figure 1: Distribution Of Users' Mental Models Of SECAP Regarding Different Application Domains.

2 Features for Mental Models of Security and Privacy

In this section, we present an exhaustive list of features related to different users' mental models of security and privacy, extracted from the literature reviewed. These features will be used for discussion and analysis of the prevalent security and privacy mental model issues and solutions.

As different users or stakeholders may have different mental models concerning SECAP, we summarize those perceptions of SECAP in tabular form presented in Table 2, 3 and 4 for ease of understanding and analysis. General end users' (GEUs) and computer science students' (CSS), software developers' (Dev), and computer security and privacy professionals' (CSPP) mental models' of SECAP can be found in Table 2, 3 and 4 respectively. We provide the mental model feature along-with the respective source(s) for each of the stakeholders.

In this study, we have considered authors of literature reviewed as CSPP. We consider their conclusions, observations and analysis of mental models of GEUs' and software developers' as very important to the study. As it can be seen in Table 4 that CSPP's mental models' features of SECAP has significantly larger content as compared to GEUs and Developers' mental models, so we deem it critical towards understanding GEUs' and developers' mental models from CSPP's point of view.

3 Discussion and Analysis

As computer systems have a very large user-base with a number of stakeholders with varied levels of knowledge of computer systems and perceptions of SECAP. So it is of paramount

Application Domain	GEU	Dev	CSPP
Mobile messaging	[15, 6]	-	[12]
Mobile applications	[15, 6]	-	[12]
Smart-home systems	[25]	-	[25]
Warnings	[3, 8, 9, 1]	-	[3, 4, 8, 9, 1]
Email	[24]	-	[24, 12]
Web browsing	[24, 6, 20]	-	[24, 12, 20]
Hackers/Adversaries	[24]	-	[24]
Viruses	[24, 8]	-	[24, 12, 8]
Passwords	[21, 22, 13, 19]	[16]	[21, 22, 13, 19, 16]
SECAP inclusive methodologies	-	[2]	[10, 7, 23, 5]

Table 1: Different Users' Mental Models Of Security And Privacy Regarding Different Application Domains Along-With References.

importance to capture this diverse user base's mental models to make systems more resilient to the kinds of threats different stakeholders face. The papers we reviewed, discussed different application domains related to SECAP mental models of those stakeholders. In Table 2, we have summarized these application domains for each type of the stakeholders considered in this research, namely GEU, Dev and CSPP. The table provides references to the source materials, for each type of user against the application domain.

However, it is interesting to note that, the software developers' mental models of SECAP have not been explored much as compared to those of GEUs or CSPP. Also, it was noted during the literature review that, no research was carried out towards understanding system and/or web administrator's mental models of SECAP. We have also shown results of Table 2 as a distribution in Figure 1 for more clarity.

So, our discussion and analysis of the results obtained by literature review revolves around the mental models of end users, developers, and computer security and privacy professional, presented respectively in Table 2, 3 and 4. For each type of the above mentioned stakeholders, we present our observations based on the reviewed literature in following sections 3.1, 3.2 and 3.3 according to the respective order of their mention. These sections lay down basis on which we present our findings in some detail in conclusion and future work section.

3.1 End-Users' Mental Models

General End-Users (GEUs) who do not have formal computer science education believe that their messages can be eavesdropped by adversaries, so they avoid sending sensitive content over phones, and prefer communication in-person for conveying sensitive or private content [15]. GEUs also believe that government agencies, intelligence agencies, device manufacturers, hackers and service providers are their adversaries and have potential to use their information. But they are not worried about their adversaries because it is believed by them that they are not the target, they trust their adversaries that they would not do anything malicious with their information, and also because they are not doing anything illegal [15, 25].

GEUs also believed hackers were bad people who could break-into their computers and steal their financial and personal information, and once or if hackers were determined they could

No.	Mental Model Parameter	Applies To
1	Our messages can be eavesdropped by adversaries	GEU [15]
2	Avoid sending sensitive content over phones, and prefer face-to-face communication for that	GEU [15]
3	Consider intelligence agencies and governments as adversaries	GEU [15, 25], CSS [15]
4	Consider WhatsApp messaging insecure	GEU [15], CSS [15]
5	Consider system manufacturers or service providers as adversaries	GEU [25]
6	System manufacturers or service providers already know everything about me	GEU [25]
7	Multi-user systems pose added SECAP challenges	GEU [25]
8	Do not consider cyber crime to be a real threat	GEU [12]
9	Hackers break-in for getting financial and personal information	GEU [24]
10	Hackers can target anyone (normal people, companies, governments)	GEU [24]
11	Viruses are created by hackers, criminals or bad people	GEU [24]
12	Do not like system generated passwords or pass-phrases	GEU [21]
13	Parents lack understanding of teens' online privacy needs and management	GEU [6]
14	Understand which factors make a password strong	GEU [22]
15	Do not necessarily follow guidelines to make every password strong	GEU [22]
16	Condensing legalistic privacy policy information which GEUs don't already know, proves ineffective	GEU [9]
17	Creating passwords on mobile phones is frustrating, takes longer and more error prone	GEU [13]
18	Privacy extensions in web-browsers generally have overall positive SECAP-enhancing effect on GEUs	GEU [20]
19	Passwords with numbers and symbols are highly likely to be reused	GEU [19]
20	Users with large number of accounts mostly reuse their passwords, fully or partially	GEU [19]

Table 2: End Users' Mental Models Of Security And Privacy Along-With References.

No.	Mental Model Parameter	Source
1	Would Google to find solution(s) to security related requirement or problem	[2]
2	We rely on lawyers for handling privacy related matters	[2]
3	We rely on off-the-shelf or third party tools for security	[2]
4	We don't know exactly which data is collected by third party tools	[2]
5	We think of functionality implementation more than (in)secure implementation	[16]
6	We implement functionality securely if we are explicitly told to do so	[16]

Table 3: Developers' Mental Models Of Security And Privacy Along-With References.

hack anyone from normal people to companies, and governments [24]. GEUs believed viruses were created by hackers, criminals and bad people, and maybe used for various malicious acts such as accessing personal and financial information, breaking or slowing down the computers etc. GEUs also reported privacy concerns when using shared smart-home computer systems.

Additionally, Computer science students (CSS) were found to believe, like GEUs, that intelligence agencies and governments were their adversaries and also that WhatsApp messaging was insecure.

3.2 Software Developers' Mental Models

Developers mainly relied on finding solutions to security related problems and software requirements through online research using search engines such as Google. In order to meet software security requirements, developers resorted to third-party tools or off-the-shelf solutions, as opposed to building their own security software. However, developers were not exactly sure that which, or how much of their application's or users' information was gathered or was being used by third-party tools [2].

For privacy related issues or privacy related software requirements, developers relied on lawyers, mainly because they were not inclined to read (often obscure) legalistic privacy policies [2]. Moreover, software developers are more focused towards functionality implementation than considering or implementing secure solutions [16]. However, if developers are explicitly asked to implement secure solutions, then they consider security as a functionality requirement and implement secure solutions [16]. Which means that, it might be highly likely that security by-default may not be present in the implemented solutions.

3.3 Computer Security and Privacy Professionals' Mental Models

Computer Security and Privacy Professionals (CSPP), which in case of our study are SECAP researchers whose literature we reviewed, believe that extracting accurate SECAP mental models of GEUs is a complex task, because mental models are non-static. Moreover, there exist array of user groups with varied mental models of SECAP based on the sophistication of their knowledge, understanding and experience [10, 25].

No.	Mental Model Parameter	Source(s)
1	Existing SECAP control mechanisms are considered insufficient by users	[7]
2	Perception of SECAP control mechanisms varies between different users	[7, 25, 23]
3	Developers lack understanding of SECAP perceptions of different users	[7]
4	System development processes do not inherently consider SECAP concerns of users	[7, 5]
5	Privacy-by-design should be part of project life-cycle	[5]
6	GEUs MMs depend on sophistication of SECAP knowledge	[25]
7	GEUs think they are not being specifically targeted	[25]
8	GEUs trust adversarial actors not to do something malicious	[25]
9	Multi-user systems pose added SECAP challenges	[25]
10	GEUs smart-home choices don't consider their SECAP concerns	[25]
11	User friendly auditing features should be added to systems for gaining GEU's trust	[25]
12	Devices and services need to be designed for multi-users	[25]
13	Reputation systems maybe developed to help GEU's in decision-making regarding SECAP concerns	[25]
14	Best practices are needed to be developed to help GEUs' address SECAP concerns	[25]
15	Systems are required to be designed to be secure, robust and inter-operable	[25]
16	Trade-off between SECAP is required to be minimized	[25]
17	Methodologies need to be designed to measure user's MMs	[23]
18	Methodologies need to be developed to distinguish novice and expert users' MMs	[23]
19	Mental models approach could significantly improve risk communication to GEUs	[4]
20	Successful elicitation of GEU MMs is a complex task	[10], [11]
21	Formal verification of GEU's MMs may be useful for addressing SECAP concerns	[10]
22	Creating formal verification model for GEU MMs is a complex task	[10]
23	GEUs underestimate the value of their collective identification	[12]
24	Basic online security trainings are required to be held regularly for GEUs	[12]
25	Threat landscape is ever evolving (non-static)	[12]
26	Male GEUs were found to be better at detecting phising scams than females	[12]
27	Female GEUs appeared to be trusting downloading content from links from SMS, Email or IMs than males	[12]
28	GEUs are not aware which actions or options are counted as risky behaviour	[12]
29	GEUs do not largely report cyberattacks so threat perceptions maybe inaccurate	[12]
30	GEUs do not understand meaning of enabling or disabling web scripts	[24]
31	GEUs think they should not open email attachments from unknown people	[24]
32	GEUs think botnets do not harm the host computers	[24]
33	Only few developers have formal SECAP training	[2]
34	Developers do not read SECAP guidelines published by government agencies or other agencies	[2]
35	Privacy policies are not considered so valuable by developers	[2]
36	Very few developers know about existence of privacy tools	[2]
37	Developers consider SECAP versus costs and effort required for solutions as a tradeoff	[2]
38	GEUs generally ignore security related warnings	[3]
39	Advanced and novice users' MMs of SECAP are dissimilar	[3]
40	Novice users consider look and feel of security related warnings, and act accordingly	[3]
41	Advanced users are highly likely to examine URLs as compared to novice users	[3]
42	Developers should design warnings with fewer text, and accurate action options	[3]
43	Warnings should be presented to GEUs when highly necessary, not otherwise	[3]
44	GEUs do not like system generated passwords or pass-phrases	[21]
45	Engaged and disengaged users interact differently with SECAP software	[8]
46	SECAP nudges increase GEUs' SECAP enhancing behaviour	[1]

Table 4: Computer Security and Privacy Professionals' Mental Models Of Security And Privacy Along-With References.

Moreover, CSPPs also believe that GEUs trust their adversaries (governments, intelligence agencies, manufacturers, service providers and hackers), and think that they will not be specifically targeted because they are not doing anything illegal or malicious, or they are not high valued targets [25]. So, GEUs believed that SECAP control mechanisms were insufficient in general, yet different GEUs had various perceptions about SECAP control mechanisms [7, 25, **?**].

Additionally, CSPPs think that system developers lack understanding of GEUs SECAP perceptions and the system development methodologies used by developers did not consider or address SECAP concerns of GEUs [7, 5]. CSPPs also held that SECAP should be part of system design or system architecture processes [5].

CSPPs think that even though GEUs have SECAP concerns, but those concerns are not reflected by the choices GEUs made regarding smart-home systems [25]. However in order to gain GEUs' trust there should be user friendly auditing features, and guidelines to train users toward secure usage of smart-home systems. In this regard, reputation systems might be developed to guide GEUs towards right decision-making in smart-home systems choices. Nonetheless GEUs' privacy concerns in case of multi-user environment remain, because smart-home systems lack such features and pose further challenges towards addressing GEUs' SECAP concerns [25].

Moreover, it was found that GEUs underestimate the value of their identity in case of their systems were being attacked or their data was stolen, and they do not largely report cyber-attacks [12]. Basic online security trainings are required to be held regularly in order to inform GEUs about secure online behaviour because GEUs are not aware that which actions or options counted as risky behaviour. It was also found that males were better than females in detecting phising scams, and they were also less trusting in downloading content from links contained in SMS, Email or instant messages (IM) than females [12]. So GEUs' mental models of SECAP may also be affected or differentiated based on gender difference.

End users do not understand the meaning of and implications of enabling or disabling web scripts, and they think botnets do not harm their computers because they are not high value targets. However they think that they should not open email attachments from unknown people [24].

End users generally ignore security related warnings, so actionable warnings should be carefully designed and developed for situations when they are really necessary. In order to minimize effort required on GEUs' side, warnings should be created with fewer text, and having accurate actionable available options so that GEUs can make better informed and secure decisions as opposed to ignoring warnings all-together. Moreover, advanced and novice GEUs' behaviours towards security related warnings may also be different, as advanced GEUs are highly like in examining URLs or certificates as compared to novice users [3].

Software developers having expertise in development tools, technologies and solutions, only few developers receive formal SECAP training. So developers are not inclined towards reading privacy policies or reading government agencies' or other agencies' SECAP guidelines. Even though very few developers know about existence of of privacy tools, still they are highly likely to consider building SECAP features in solutions versus effort required for solutions as a tradeoff [2].

GEUs mental models extraction can significantly improve SECAP risk communication to GEUs [4]. As successful and accurate elicitation of GEUs' mental models is a complex task, formal verification of GEU's mental models may be useful in managing SECAP concerns, however creating a formal verification model of GEUs' mental model is a complex task itself [10]. CSPPs think that methodologies should be proposed to measure GEUs' mental models, and such techniques are required which can differentiate between novice and expert users' mental

models [23].

4 Conclusion, Recommendations and Future Work

Eliciting accurate mental models of computer security and privacy of end users is a complex task because mental models are ever evolving. One big hindrance in eliciting accurate mental models of SECAP is the fact that different GEUs have various mental models based on the sophistication and complexity of their knowledge of SECAP concerns. While researchers have tried capturing various user's mental models of SECAP for different computer systems, applications and use cases, their results have not yet lead to design and development of such methodologies which have security and privacy as system design features. Nonetheless, researchers have provided guidelines for designing such systems which enhance SECAP behaviour and risk assessment of GEUs.

Moreover, even though software developers may have significant knowledge of development tools and technologies, but they normally lack understanding of SECAP concerns of GEUs. Also, they are not inclined towards reading or understanding privacy policies, instead, they would rather trust lawyers to handle privacy related matters. As far as security related software requirements are concerned, developers are highly likely to use off-the-shelf solutions or third-party tools, even when they are not sure the specific third-party tools which they are using might be collecting or gathering which or how much data about their systems' users. However, large firms have dedicated resource persons for guiding developers in security and privacy related software requirements and solutions.

As GEUs trust their service providers or device manufacturers, but if developers, system/web administrators do not have SECAP related knowledge or skills, such situation increases risk factors. More and focused research work needs to be done towards understanding developers' and administrators' mental models of SECAP. This should lead towards more usable SECAP guidelines and tools for developers and administrators. For example, integrated development environments could have plugins guiding developers towards implementing securer solutions.

Additionally, we also conclude from analysis of the aforementioned users' mental models towards security and privacy that the actual threat assessment is not possible. This assessment is also supported by an GEU argument that if adversarial intelligence agencies can hack into or compromise governments' systems which have top level security teams and systems, they can access or intrude in our systems too. In light of Edward Snowden's global surveillance disclosures of 2013, and the recent revelations of hackers attacking German governments' various departments over an extended period of time, more merit is brought to GEUs' claims that adversaries do have the required capabilities to infiltrate any systems, whenever they wish [18, 17].

In order to address GEUs' SECAP concerns and nullify the claim that adversaries have the required capabilities to infiltrate any systems, it is also important to understand attackers' mental models. As shown by the recent revelations, German governments' agencies allowed malware to operate in a controlled environment, in order to understand attackers' behaviour, and trace and track the attacker [18]. However, it has also been reported that considerable information may have been leaked during the process [17].

It is imperative that governmental intelligence, information security, and law enforcement agencies take necessary actions to revive GEUs trust in information security and privacy by thwarting such high level attacks within time. Moreover, information security and privacy trainings for GEUs should be held, in common language, regularly, in order to keep GEUs' risk and threat perceptions to realistically possible minimal levels. Such measures are necessary,

because the guidelines or updates issued by information security departments or agencies are generally not read by GEUs.

In future, we would like explore developers' and system/web administrators' mental models of SECAP in more depth. We would also like to evaluate the very few existing SECAP inclusive system design and development methodologies, and possibly propose improvements.

References

[1] Alessandro Acquisti, Idris Adjerid, Rebecca Balebako, Laura Brandimarte, Lorrie Faith Cranor, Saranga Komanduri, Pedro Giovanni Leon, Norman Sadeh, Florian Schaub, Manya Sleeper, et al. Nudges for privacy and security: Understanding and assisting users choices online. *ACM Computing Surveys (CSUR)*, 50(3):44, 2017.

[2] Rebecca Balebako, Abigail Marsh, Jialiu Lin, Jason I Hong, and Lorrie Faith Cranor. The privacy and security behaviors of smartphone app developers. 2014.

[3] Cristian Bravo-Lillo, Lorrie Faith Cranor, Julie Downs, and Saranga Komanduri. Bridging the gap in computer security warnings: A mental model approach. *IEEE Security & Privacy*, 9(2):18–26, 2011.

[4] L Jean Camp. Mental models of privacy and security. *IEEE Technology and society magazine*, 28(3), 2009.

[5] Kovila PL Coopamootoo and Thomas Groß. Mental models for usable privacy: A position paper. In *International Conference on Human Aspects of Information Security, Privacy, and Trust*, pages 410–421. Springer, 2014.

[6] Lorrie Faith Cranor, Adam L Durity, Abigail Marsh, and Blase Ur. Parents and teens perspectives on privacy in a technology-filled world. In *Proc. SOUPS*, 2014.

[7] Denis Feth, Andreas Maier, and Svenja Polst. A user-centered model for usable security and privacy. In *International Conference on Human Aspects of Information Security, Privacy, and Trust*, pages 74–89. Springer, 2017.

[8] Alain Forget, Sarah Pearman, Jeremy Thomas, Alessandro Acquisti, Nicolas Christin, Lorrie Faith Cranor, Serge Egelman, Marian Harbach, and Rahul Telang. Do or do not, there is no try: user engagement may not improve security outcomes. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*, pages 97–111, 2016.

[9] Joshua Gluck, Florian Schaub, Amy Friedman, Hana Habib, Norman Sadeh, Lorrie Faith Cranor, and Yuvraj Agarwal. How short is too short? implications of length and framing on the effectiveness of privacy notices. In *12th Symposium on Usable Privacy and Security (SOUPS)*, pages 321–340, 2016.

[10] Adam M Houser and Matthew L Bolton. Formal mental models for inclusive privacy and security. In *Symposium on Usable Privacy and Security (SOUPS)*, 2017.

[11] Ding-Long Huang, Pei-Luen Patrick Rau, and Gavriel Salvendy. A survey of factors influencing peoples perception of information security. In *International Conference on Human-Computer Interaction*, pages 906–915. Springer, 2007.

[12] James Imgraben, Alewyn Engelbrecht, and Kim-Kwang Raymond Choo. Always connected, but are smart mobile users getting more security savvy? a survey of smart mobile device users. *Behaviour & Information Technology*, 33(12):1347–1360, 2014.

[13] William Melicher, Darya Kurilova, Sean M Segreti, Pranshu Kalvani, Richard Shay, Blase Ur, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, and Michelle L Mazurek. Usability and security of text passwords on mobile devices. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, pages 527–539. ACM, 2016.

[14] M David Merrill. Knowledge objects and mental models. In *Advanced Learning Technologies, 2000. IWALT 2000. Proceedings. International Workshop on*, pages 244–246. IEEE, 2000.

[15] Alena Naiakshina, Anastasia Danilova, Sergej Dechand, Kat Krol, M Angela Sasse, and Matthew Smith. Poster: Mental models-user understanding of messaging and encryption. In *Proceedings of European Symposium on Security and Privacy. http://www. ieee-security. org/TC/EuroSP2016/posters/number18. pdf*, 2016.

[16] Alena Naiakshina, Anastasia Danilova, Christian Tiefenau, Marco Herzog, Sergej Dechand, and Matthew 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*, pages 311–328. ACM, 2017.

[17] Associated Press News. Hack of german government network caused considerable damage, March 2018.

[18] Deutsche Welle News. Hack on german government network 'ongoing', March 2018.

[19] Sarah Pearman, Jeremy Thomas, Pardis Emami Naeini, Hana Habib, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, Serge Egelman, and Alain Forget. Let's go in for a closer look: Observing passwords in their natural habitat. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, pages 295–310. ACM, 2017.

[20] Florian Schaub, Aditya Marella, Pranshu Kalvani, Blase Ur, Chao Pan, Emily Forney, and Lorrie Faith Cranor. Watching them watching me: Browser extensions impact on user privacy awareness and concern. In *NDSS Workshop on Usable Security*, 2016.

[21] Richard Shay, Patrick Gage Kelley, Saranga Komanduri, Michelle L Mazurek, Blase Ur, Timothy Vidas, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. Correct horse battery staple: Exploring the usability of system-assigned passphrases. In *Proceedings of the eighth symposium on usable privacy and security*, page 7. ACM, 2012.

[22] Blase Ur, Jonathan Bees, Sean M Segreti, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. Do users' perceptions of password security match reality? In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, pages 3748–3760. ACM, 2016.

[23] Melanie Volkamer and Karen Renaud. Mental models–general introduction and review of their application to human-centred security. In *Number Theory and Cryptography*, pages 255–280. Springer, 2013.

[24] Rick Wash. Folk models of home computer security. In *Proceedings of the Sixth Symposium on Usable Privacy and Security*, page 11. ACM, 2010.

[25] Eric Zeng, Shrirang Mare, and Franziska Roesner. End user security & privacy concerns with smart homes. In *Symposium on Usable Privacy and Security (SOUPS)*, 2017.