A Comparison of American and German Folk Models of Home Computer Security

Michaela Kauer, Sebastian Günther, Daniel Storck, and Melanie Volkamer

ABSTRACT. Although many security solutions exist, home computer systems are vulnerable against different type of attacks. The main reason is that users are either not motivated to use these solutions or not able to correctly use them. In order to make security software more usable and hence computers more secure, we re-ran the study by Wash about "Folk Models of Home Computer Security" in Germany. We classified the different mental models in eleven folk models. Eight of the identified folk models are similar to the models Wash presented. We describe each folk model and illustrate how users think about computer security.

ACM Classification Keywords
H.5.2 Information Interfaces and Presentation: User Interfaces—evaluation/methodology, user-centered design; H.5.3Information Interfaces and Presentation: Group and Organization Interfaces—collaborative computing
General Terms
Human Factors, Security
Author Keywords
Home Security, Mental Models, Folk Models

1 INTRODUCTION

In the beginning of the computer era, computers were used by experts only and they were not connected to a worldwide network. Those experts were familiar with the use of the systems, knew the pitfalls, and knew how to protect their computers. Nowadays, computers and other devices, such as smartphones, are widely spread in Germany and nearly each and every household has a home computer. In contrast to the beginning, most users are not trained with the systems and have an incomplete mental model and knowledge of computer and Internet security many studies like [5, 6, 7, 8] show in different contexts. Correspondingly home computers are vulnerable against many different attacks with many different consequences, often although security software is used. Typical attacks against home computers are: malware infections while the consequence can be that users cannot access their data anymore or the computer is used as bot node in a botnet. The problem with security solutions is that they are often not usable and thus not able to protect users effectively e.g. because users

configure the security solution in insecure way [2]. In addition, there is often a small timeframe after a new attack has been deployed and the security solution being updated. Such attacks can only be detected and fraud can only be prevented if users become more aware, too. This awareness can either be communicated by the security solution or by independent trainings or information, e.g. on TV. However, both the more usable security solution as well as the awareness communication can only be successful if it takes the user's mental model and knowledge into account. Therefore, it is essential to understand users' mental models and group them in so called folk models, while folk models are mental models that are shared among several members of a culture [8].
In a first study Rick Wash investigated in a qualitative study the folk models on home computer security of North American home computer users living on the west coast. It can be expected that those model differ between cultures and therefore, this paper shows a re-run of the study in Germany and a comparison of the results. First, a short introduction to mental models in the context of Internet and Computer security is provided (section 2), followed by the description of the study methodology (section 3). In section 4 the results of our study are presented and compared to the results of the original study. The paper closes in section 5 with a discussion of the results.

2 Mental Models in Security

The idea to use folk models or mental models for a better understanding of user behavior in the security area is not new. Asgharpour and colleagues [1] used a closed card sorting to correlate security risks with mental models. For their approach they chose five existing mental models (e.g. physical safety, criminal behavior; cf. [3]) and instructed experts and non-experts to sort the security risks to the fitting mental model. The main finding of their work was the fact that experts and non-experts differ significantly in terms of their mental models. Therefore, the authors concluded that security advice should be adapted to the mental models of non-experts. Within their study they used predefined models, so that between 30% (non-experts) and 40% (experts) of the security terms were not categorized into the existing mental models. This is a clear hint that users do have additional/different mental models, which have to be identified.

One step towards the identification of occurring mental models for security was done by Rick Wash [8]. In his study about home computer security Wash [8] talks about folk models. In this context folk models are "[..]mental models that are not necessarily accurate in the real world, thus leading to erroneous decision making, but are shared among similar members of a culture"[8]. So it can be expected that if security software were designed to fit to folk models about possible threats, this software may have a decreased rate of unexpected behaviors for users. The study of Wash was conducted in America with 33 participants from a mixed citizenship. Overall, he indentified eight folk models that exist within the context of home computer security. Until now, no intercultural comparison was conducted to see if those folk models

identified by Wash may be generalized. Within this paper the study of Wash was re-run in Germany and the results of both studies are compared.

3 METHODOLOGY

Aim of this study was a comparison to the original study of Wash [9] and thereby to re-run the study of Wash as similarly as possible. The interviews were conducted face-to-face or via Skype in two rounds that followed each other with about four weeks break in between. Within this break, the interview data of the first round was analyzed and scenarios were deduced that focused on critical results from round one. It was tried to interview as different people as possible (e.g. level of education, age, security knowledge, social background) in order to reach a wide degree of variation in the folk models.

In round one 17 people participated and in round two 9 people participated in the interviews. About 25% of the participants were female. They were aged between 18 and 60 years. As in the original study, those participants represent a part of the German population but are by no means representative.

The first interview round focused on all kinds of general home computer security risks. Participants were first asked about their security behavior in general (use of passwords, updating software, using security software), followed by questions about their knowledge about security threats (known threats, countermeasures, source of security problem) and ended with questions about specific security threats (viruses, trojans, etc.). Each interview took about 90 minutes. Based on the results of the first round, a second interview was developed which included three different scenarios about general and current home computer security risks that were derived from critical aspects and misunderstanding in interview round one. Those scenarios were:

1) A friend tries to log on into Facebook on their computer and recognizes malicious software on their PC.
2) They became a victim of a hacker attack.
3) The police notified them about a theft of their identity.

For all three scenarios, participants were asked what they would do, if they believe the scenarios can be true and why they were a targeted. Additionally, the questions about specific threats from interview round one were asked. Each interview took about 90 minutes.

For data analysis two matrices were built that categorized the answers of the participants given in the interviews and summarized them into groups. Then, two matrices were created extracting the mental models from the interview results and describing them shortly to get an impression about each mental model. To avoid subjective notions, statements were not categorized as correct or false. It is believed that mental models are simplified representations of the environment that are helpful for the person who holds them and it is seldom the case that a mental model is either correct nor false, but often partially both. In a final step, the results of this study were compared to the results of the original study. Note, pseudonyms are used in this paper.

4 RESULTS: FOLK MODELS OF SECURITY THREATS

Folk models were categorized into models about Models of Viruses, Malware, Spyware and other malicious types of software and models of hackers and break-ins. Models were categorized as dealing with malicious types of software if the core of the model was about the functionality of the software. By contrast, models were categorized as dealing with hackers and break-ins if the core of the model was concerned with the person of the attacker. Each of the presented models was described by at least two participants and each of the participants had more than one folk model. Overall, 5 different models of viruses were found whereas 6 models for hackers and break-ins were identified. The next sections will present models of viruses.

4.1 Models of Viruses and other Malware

Security threats within this group are all associated with the term "virus", but not all of the participants thought a virus is concrete software. However, they described it at least as a generic term of all kinds of software related to home computer risks like trojans, spyware, computer worms, and malware. Almost every participant mentioned at least two different folk models of home computer security, but not everyone knew how they work in detail and what they could do to decrease the potential threats. In general only a few had a lack of security consciousness, while the rest, who named more than one model, had been informed by media or more experienced friends. A majority knew what countermeasures they can use to be more secure.

Viruses are Generically 'Bad'. The first model of viruses is based upon users' opinion that viruses are bad in general. The respondents described them as negative or annoying effects on their computers. All participants with this model were not sure how they can be infected by viruses, but mostly believed they could only catch a virus by visiting malicious or suspect websites or getting infected by physical media like USB flash drives. In all cases users agreed they have to actively download or execute the virus. For example Uma said "viruses come from dubious websites or links at Facebook", believing that if she does not click them, she does not get infected. In Olivia's opinion she can catch a virus by opening files on "infected USB flash drives" or "malicious attachments from spam emails". Users of this model are not in great fear of getting viruses with regard to their own behavior, but unlike the original study they all use anti-virus-software even if they never had a virus before because it makes them feel more comfortable. Paula and Julia have both had a virus (trojans), but did not know what the virus did or where it came from. They got informed by their anti-virus software which removed the Trojan automatically.

Viruses are Buggy Software. A very common folk model is "viruses behave like buggy software". They often lead to computer reboots, corrupted files or total system crashes and always slow down the computer. Users can only fix them by re-installing their operating system. Respondents of this model usually believe those viruses do not

have a special purpose and are just meant to annoy. Similar to the “viruses are generically bad” model, people thought to “catch” a virus they need to actively download or “click” a virus. Therefore, users feel mostly immune if they are careful and watch out in what kind of files they trust. Some participants said that viruses are often part of games or related things. For example, Xander, told us he can ”catch viruses as part of game cracks, but thought they are not as bad as ”normal” viruses so he will not stop downloading those programs. People who think viruses as some kind of “buggy software” are not sure about the purpose they have. Again, they all use anti-virus software and sometimes firewalls, because it makes them feel more comfortable.

Viruses Cause Mischief. The most frequent model is “viruses causing mischief”. These mischief activities have a very wide spectrum of how they affect computers and what their intentions are. Some of the respondents named unusual pop-ups with advertisements (Fiona and Neil) or massive data loss (almost everyone) as visible effects of the infection. Participants corresponding to this model have a better understanding of what viruses do and often have concrete images of who could have created them. Quinn mentioned an interesting aspect: “viruses can cause damage to the computer’s hardware”, so he has to buy new parts like a new hard drive. To get mischievous viruses, it is not necessary to actively download and execute them. Users can also get them passively by “visiting suspect websites like pornographic sites” (Lewis) or “sites with manipulated scripts” (Walter). Respondents with this folk model use security software, but do not totally rely on it, because “anti-virus tools do not know every virus ” (Gerrit).

Viruses Support Crime. Some of the respondents had the idea that viruses are part of criminal intents supporting organized criminals. The main goals of those viruses are identity theft, collecting personal data, opening backdoors for hackers and also extortionate robbery. Frequently this is combined with spyware like keyloggers to send the attackers passwords and other login information (Matt, Arthur). The model is directly connected to the models of hackers as professionals of criminal organizations. Most of the participants are worried about becoming victim of monetary robbery, but still Online-Banking is seen as very beneficial. Bob believed viruses often “take over [..]online banking or other financial accounts and automatically transfer money to criminals”. Also if they got robbed by viruses most of them thought it would be their own fault and not the fault of Online-Banking in general (Xander, Walter). Participants in this group have a distinct sense of privacy and are afraid of someone stealing and abusing their identity. This abuse was defined in multiple ways: a lot of the attendees only think about collected addresses, names and various personal data (e.g. Xander), while others also believe Online-Banking accounts are real parts of their identity(Robert). A last aspect of identity theft is creating digital movement profiles which do not directly harm them, but lead to more individual advertisements on websites or, combined with collected/stolen addresses, to more precise spam. Thomas came up with viruses which can “encrypt important files” on computers, which can only be decrypted if you send the authors of the viruses money (”extortion”). Neil had

the idea that some viruses were directly created by anti-virus software producers to convince more people to buy their security software.

Viruses are Governmental software. A completely new aspect which did not occur in the original study, were viruses created by governments or secret services. These types of viruses "will be installed on your computer by policemen at house searches" (Robert) or "secretly placed by police hackers" (Bob). Those viruses are not easily categorized as good or bad. David had the opinion only criminals such as terrorists will be a target to find potential risks for mankind or illegal activities. Steven thought that governmental viruses are looking for people who are tax dodging, while Robert believed those viruses could target every citizen to observe them. As an example for this extreme point of view, he referred to the "Bundestrojaner" and "Staatstrojaner" (engl. Federal Trojan horse), which are tools from German police to possibly monitor everyone, even if they have not done any criminal activity at all. A different threat Robert had in mind when thinking of the "Staatstrojaner" was its abuse by criminals due to badly written software. He stated it would be possible to take over or put mischievous files to computers.

4.2 Models of Hackers and Break-ins

The second important category of folk models deals with "Hackers and Break-ins". All participants had an – more or less concrete - idea of what a hacker is and what he does. A hacker can be any kind of person who can somehow get access to a system to which no access permission is granted. It is often not obvious which person it exactly is or what things he does in order to break into a computer system. In any case, hackers are considered to be persons who break into a system and do something. Most of the participants thought about several types of hackers. For some of them it was really difficult to clearly separate different hacker models, because they often did not exactly know how hackers operate and where they come from. Even though most of the participants had no idea how a hacker can break into a system, they all believed it is possible. In their opinion, after a hacker has gained access to their computer, he can do whatever the users could do with their computer. Within this study six folk models for hackers were found. They describe who is believed to be the attacker, what his motivation could be and how they chose their targets.

Hackers practice their hobby. One group of participants considered hackers to mainly be young technical "nerds" (i.e. Victor) and often "hobby hackers"(i.e. Kevin). When asked about the meaning of "nerds" participants described them as persons with a very good knowledge of computers and an addiction to them. The term "very good knowledge" was very generic but implied whatever it needs to break into a computer. Furthermore, they are very talented and intelligent (Olivia, Julia) and may be isolated, only having "little social competence" (Victor). Therefore they operate alone or only in small groups with only one or two other people. A "Hobby hacker" can be a "nerd" as well as a normal person who was not clearly specified. Some of the

respondents believed that hackers break into systems in order to impress others, which was interpreted as a sign of their social incompetence. Some hackers (hobby hackers) were described to only break into systems “just for fun”. Many participants also stated that hackers want to test their own skills and consider their break-in as a challenge. Olivia said “they hack into the school computer to delete or change grades”. The effects of hackers’ break-ins can cause annoying computer behavior or theft of personal data. Claus believed hackers always do damage and told us that damage does not implicitly mean ”physical” damage, but rather theft of personal information. Stealing of personal files like photos is considered a threat which “happens in the background”(Paula) and is thereby hard to detect. In Steven’s and Claus’s case they had a look at their router logs and noticed that something undefined has gained access from the Internet. Often, victims do not know they are actually targeted, meaning they only discover any harm caused afterwards. Thus it is very important to prevent a break-in. In this model, hackers choose their victims by accident or people they personally know. Participants claim “it is very unlikely to become a target if the hacker doesn’t know me”. Most of them do not know how to protect themselves from hackers, because they do not know how a break-in works.

Hackers are Intruders Who Break into Computers for Criminal Purposes. Another set of respondents believed hackers are criminal professionals that operate solo as well as in groups. They can be persons of all ages. Robert described them as “men from the 70s with long hair”, whereas Ilias imagined “younger persons”. Often a hacker was considered to be a male person. Some participants even believed that hackers come from a specific region. For example, Xander thought hackers are Asian or East-European people, whereas Neil believed they come from Russia. The hackers in this model are clearly criminal and very skilled. They are specialized persons with extensive computer knowledge. Break-ins are always conducted for criminal purposes, for that reason some participants stated “hackers operate solo so they don’t attract attention” (Olivia, Fiona). These hackers often create software which can help them to gain access or is placed on the compromised computer. Some attendees reckoned that hackers develop and distribute their own viruses and afterwards break into the infected systems. Attacked persons are always victims of a crime. These crimes are mostly personal information theft and sometimes system damage. Personal information theft is always associated with stealing of sensitive information (mainly banking information like credit card or online banking account) which the hacker uses to come into money. Identity theft is also possible. Kevin said “hackers steal personal information to buy something online with someone else’s identity”. Few participants believed that hackers intentionally cause system harm. They break into the computers and intentionally delete files or cause the systems to crash. Even though it is not clear why the hackers do this, some participants thought it to be likely. Users with this folk model consider everyone to be a potential victim. Nonetheless they think it is very unlikely they could be a target because they do not think they have valuable information on their PC (Fiona). About half of the participants did not know what to do if they become a victim. The only thing they would do while they are under attack was to disconnect from the Internet or to shut down their computers.

Hackers are Professionals of Criminal Organizations. This model is conceptually similar to “Hackers are intruders” and is also about hackers who steal users’ personal information or intentionally harm computers. The difference lies in the way the hackers select their victims. Within this model, hackers are part of criminal organizations. They operate in organized groups with hierarchical structures. Four respondents called one of these organizations “the Internet Mafia”(Neil, Fiona, Lewis, Quinn). They had never heard whether an “Internet Mafia” exists, thus it is more their imagination of a structured criminal institution. Such criminal organizations consist of professional hackers and other criminal persons without computer knowledge. The “professionals” select their victims according to their expected value. ”Stealing precious company secrets” was said by Lewis. Julia also believed they focus on “industrial spying or sabotage”. But also “rich people with a lot of money” (Robert and Lewis) might be targets of those hackers. Additionally, groups of individuals who perfectly fit the criminal intentions, like: “building a network [botnets] for spam mails with home computers” (Kevin) might be attacked. Another reason given by Olivia was to “cripple public authorities”. Subjects describing this folk model did not worry about these hackers because they did not consider themselves as worthy target and therefore did not aim to protect themselves.

Hackers are Contractors Who Support Criminals. In this folk model hackers are contractors supporting criminals. They aim not at harming others but to make profit by selling stolen information or are engaged by criminal groups. While some of our participants thought “hackers are absolute computer-freaks acting solo”(Julia), some others perceived “hackers are small groups operating for big companies” (Neil). It is not distinct who they are exactly, but at least a combination of hobby hackers and intruders. The main reason why these hackers break into systems is to collect big amounts of personal and financial information which they resell to spammers or other criminal organizations. Zelda, for example, described the hack of the “Playstation Network” as a hack by a small group gathering credit-card information for some masterminds behind. Participants with this model mostly did not think they are directly a target, rather having an account on a big website which gets hacked (Lewis, Yvonne). For example contractors attack e-commerce companies like Amazon and eBay or financial institutions like PayPal or Online-Banking in general. Those who thought they could be a victim also believed they were only randomly selected (Eve, Paula). Hence the majority of the users are very careful about the private data they publish to online services, and use different passwords for each website to minimize the risk for more services to get compromised.

Hackers are Governmental Officials. An additional folk model was the model “hackers engaged by governments and secret services”. It is directly associated with the “viruses are governmental software” folk model. People with this mental model are often more deeply interested in computer security and politics. Due to the rising attention by reading about it in the news, also “normal” computer users are into this topic. Almost all of them had a raised concern about hacker groups working for their

own government ”to observe citizens” (Steven) and also supposed to defend against ”cyber-war” (Robert) and online-terrorism(David), while Xander and Bob believed that governmental hackers also were the attacking party. In summary, all participants said that they only act if any type of suspicion of crime is going on. When asked about the term ”government hackers”, the majority responded they do not imagine very skilled hackers, but rather normal policemen with some kind of additional training in computer security and hacking. If people are concerned that they could be observed by their government, police or secret services, they only thought these hackers would create profiles and collect personal data. Neil had the idea that they could also hack into smartphones to produce movement profiles.

Hackers are Stakeholders with individual and opportunistic purposes. The last hacker folk model was hackers with opportunistic goals and targets. Those hackers are driven by their individual view on how the world should be, but may not be distinctly legal in all cases. Arthur and Kevin for example referred to ”Anonymous” and ”LulzSec” as stakeholders with arguable aims, but agreed they often operate in grey areas of law which may not be reasonable for everyone, ”especially for governments”. Another group of stakeholders named by Eve and Walter is the German lobby association “Chaos Computer Club” (abbr. “CCC”). This organized collective of hackers were described as primarily good people who want to help mankind by finding critical security vulnerabilities in administration or business systems without abusing them and “to point out deplorable circumstances in politics” (Claus).Although noted by a lot of participants, none of them were in fear to be targeted by stakeholders, since they are more interested in media-effective targets.

5 DISCUSSION AND OUTLOOK

The participants of this study were widely interested in how they can protect themselves. But, “the vulnerability of home computers is a security problem for many companies and individuals who are the victims of these crimes, even if their own computers are secure.” Within this study eight out of the eleven folk models were equal to those from the original study [8]. But additionally, three new folk models were discovered during the re-run of the study in Germany. Those models were “viruses are governmental software”, “hackers are governmental employees”, and “hackers are stakeholders with individual opportunistic purposes”. It can be assumed, that those new models evolved due to the higher presence of the topic computer security in media during the last three years. For example, some well noticed events of the past few years were: governmental spyware, Wiki-leaks, Stuxnet (virus by a secret service), changing Facebook privacy and the German ”Staatstrojaner”. This indicates that users are concerned with current developments in IT security and the associated risks. Additionally, the new models show that this concern leads to new ideas about threats and that it is possible to influence the ongoing folk model by accurate reporting in the media. This fact could be used to actively change the folk models on computer security and thereby, not only promote more correct models but also promote

appropriate countermeasures. Another source of those differences might be simple accounted for by the different cultural backgrounds in which the two studies were conducted. A good summary was mentioned by Politics & Policy: "[..] the E.U. generally allowing more rights to the individual. With no single law providing comprehensive treatment to the issue, America takes a more ad-hoc approach to data protection, often relying on a combination of public regulation, private self-regulation, and legislation." [4] Also the ongoing discussion in Germany about privacy policies of Facebook and Google may play a bigger role in the way the participants described their mental models. Seeing it from a cultural point of view there might be additional folk models out of the U.S. and Europe.

To develop the best possible security software it is necessary to consider those folk models to prevent misuse of it. The authors of this paper would suggest a two-step procedure: 1) Use media to arouse interest in computer security. In this step, it might be helpful to especially address those people who think that they do not need security software (e.g. people with the "hackers are professionals of criminal organizations" or "hackers are stakeholders" models) and inform about threats that might occur that are not person specific (e.g. botnets). 2). Design security software that emphasizes the potential dangers, gives action advices and supports self-reflection of security behavior.

6 ACKNOWLEDGMENTS

We would like to thank Rick Wash, author of the original study, and our participants.

7 REFERENCES

1. F. Asgharpour, D. Liu, and L. J. Camp. Mental models of computer security risks. In Workshop on the Economics of Information Security (WEIS), 2007.
2. D. Balfanz, G. Durfee, D.K. Smetters, and R.E. Grinter. In Search of Usable Security: Five Lessons from the Field. In IEEE Security & Privacy, pp. 19-24, 2004.
3. L. J. Camp and C. Wolfram. Pricing security. In Proc. of the Information Survivability Workshop, 2000.
4. K. Hudson, T. Herr, A. Blanche and A. Cross. The european union and internet data privacy. Politics & Policy publication, http://politicsandpolicy.org/article/european-union-and-internet-data-privacy.
5. P. Johnson-Laird, V. Girotto, and P. Legrenzi. Mental models: a gentle guide for outsiders. Available at http: //icos.groups.si.umich.edu/gentleintro.html, 1998.
6. D. Liu, F. Asgharpour, and L.J. Camp. Risk communication in Security Using Mental Models. 2008
7. F. Raja, K. Hawkey, and K. Beznosov. Revealing Hidden Context: Improving Mental Models of Personal Firewall Users. In Proc. of the fifth Symposium On Usable Privacy and Security, SOUPS '09, pp. 1:1--1:12, July 15-17, 2009, Mountainview, CA, USA.
8. R. Wash. Folk models of home computer security. In Proc. of the Sixth Symposium on Usable Privacy and Security, SOUPS '10, pp. 11:1–11:16, New York, NY, USA, 2010.