Creating 'Security Personas' to Support Security and Privacy Tool Design

ABSTRACT

Security and privacy researchers have recently turned their attention towards the user and are borrowing from the HCI community to further understand the user and their goals. However, we have observed, too often, that the user still becomes generalized to a small set of characteristics in security and privacy research. In this paper, through qualitative interviews, we explore how users' knowledge and motivation allows us to cluster users. Based on five groups of users, we create five "security personas", or prototypical users, to aid in the design of future security tools. We provide an evaluation of our personas by comparing them to data collected on another set of users and coded by independent researchers, and demonstrate the utility of these personas by analyzing two current security applications. Together, these results argue that our set of "security personas" provides a starting point for a richer description of users of online security and privacy tools.

Author Keywords

Persona, Security, Privacy, Interviews, User differences.

ACM Classification Keywords

Miscellaneous.

INTRODUCTION

Since 1999, Adams and Sasse have claimed that "users are not the enemy" and have promoted closer examination of security issues from a user point of view [4]. Despite this drive for a richer understanding of users, in privacy and security research, it is quite common to see a user community reduced to a single dimension based on some naïve observation from survey data. For example, authors state that "The average user has 6.5 passwords, each of which is shared across 3.9 different sites"[14], that "66% of respondents in a survey of 300 corporate users wrote down work-related passwords"[13]; or that, "given the right circumstances, online users easily forget about their privacy concerns and communicate even the most personal details without any compelling reason to do so"[6]. Essentially, researchers claim there exists a "generic user" who creates bad passwords, is naïve about privacy, or is undereducated about the security issues that affect them. [14,3,4].

A significant problem exists, however, when prospective users of technology are generalized to a single dimension. Software is designed for a generalized "user" who rarely exists in practice. Among many other researchers, Dourish and Anderson [11] highlight the dangers of this reductionist philosophy.

One challenge with analyzing any user community during design is that the goal of the analysis is, at heart, a reductionist approach to identifying user characteristics. Researchers look at practices [12] or demographics [15] or knowledge or motivation [11] to determine the characteristics of a user community and to express those consolidated characteristics for design. Unfortunately, we argue that much of the current research in security and privacy has attempted to distill users down to a single dimension by, for example, citing password practices [13, 14] or citing propensity to trade privacy and security for some perceived gain [6], but this trivializes user communities. The goal of this work is to begin to address online security and privacy attributes of users based on a view of users as a heterogeneous yet concrete community. Understanding the breadth of a user community enables better designs by tailoring any single design either to specific attributes of a subset of users, or by tailoring a design to broad attributes shared by all users of a software system.

In design, one technique used to ground discussions of unique user attributes, to explore differences between users, and to highlight the fact that certain classes of users are more central to any design endeavor than other users is personas [22]. Personas are common in product design, and as a design tool, have also been of interest to HCI researchers [16,19]. The specific goal of this research is to create, through qualitative data collected from a set of users, security personas that can aid in developing security

and privacy technologies for diverse users within the security and privacy domain.

Cooper wrote, "Personas are not real people, but they represent them throughout the design process. They are *hypothetical archetypes* of actual users. Although they are imaginary, they are defined with significant rigor and precision. Actually, we don't so much 'make up' our personas as *discover* them as a byproduct of the investigation process. We do, however, make up their names and personal details"[10].

To 'discover' these personas, we conduct semi-structured interviews with 13 subjects, and evaluate those subjects based on user knowledge and motivation. We choose knowledge and motivation as basic dimensions of our user community due to the pervasiveness of these themes in security and privacy research. Users do not know enough so make bad security decisions [3, 4, 14] is one common theme. Another is that users exist in groups, based on motivation; for example, there are minimalists, pragmatists, and purists [2].

Grouping users along these two dimensions creates five categories of users which we label: the struggling amateur, the lazy expert, the oblivious target, the paranoid expert, the aware technician. We evaluate these personas in two ways. First, we compare our personas to a set of participants from a colleague's security study. Then, we analyze the design of two popular security tools in light of our personas. Our hope is that these personas will spur more fine-grained discussion of who usable privacy and security researchers are designing for, and what role each design artifact will serve for various types of users within the space of possible users of these technologies.

This paper is organized as follows. First, we present related work on personas. We also provide a brief overview of some of the extensive body of work seeking understanding of users in security and privacy. We then describe the design of our qualitative interviews. Next, we present data from our interviews and cluster our participants. Finally, we present and analyze the personas created from these participants.

RELATED WORK AND MOTIVATION

Personas, introduced by Cooper, are defined as fictional characters created to represent different users within a design process[10]. While debate has existed on the benefits of personas during design [5,7,8], recent research has shown some benefit to their use during the design process[18]. Specifically, Long found that, in a controlled experiment within a university classroom, students using personas produced more usable designs than a control group. As well, Long argued that the personas encouraged more user-focus in design team communication. In this research, we aim to construct personas to describe various users within the security and privacy domain.

With the creation of personas in mind, we examine other research focused specifically on developing an understanding of users. User studies in security and privacy typically make use of either qualitative or quantitative methods to develop an understanding of users.

Focusing first on qualitative studies, these papers look deeply into their participants for reasoning or external factors in decision making. For example, Dorish et al. aimed to determine how end users manage security on daily basis[12]. Their research allowed them to create a set of practices that characterize a "typical user". Realizing there are differences in user's security behavior, two studies, Friedman et al.[15] and Dourish and Anderson[11] explored factors that might affect how users perceive security and privacy. Friedman et al.[15] looked at 72 individuals from three different communities in hopes of seeing some differences in security practices based on location demographics. However, what they observed was that "the high-technology participants did not always have more accurate or sophisticated conceptions of Web security than did their rural and suburban counterparts." They conclude that the differences in users are not a result of their demographic category. Dorish and Anderson[11] conducted an extensive literary review to demonstrate how social and cultural behaviors influence security and privacy rational. We build on this work, aiming to shed light on the security and privacy nuances that occur between people.

Beyond differences in behavior, users of security and privacy technologies often have different focuses. For example, when looking at privacy from a social behavior perspective, Acquisti and Gross[3] used survey data to assess students' privacy awareness levels and to determine if their intentions match their actions. They found that the majority of their sample was more concerned about controlling their information than censoring their information. They show that user goals vary in security and privacy protection. We argue that understanding this divergent focus is an important component of tool design.

Quantitative studies aim to determine what users do and understand about security and privacy issues[3,4,9,14]. Beyond these academic studies, many researchers have made use of media surveys to strengthen a security argument and demonstrate the need for a new technology. For example, when promoting graphical passwords statistics about writing down or forgetting passwords are quite commonly used as motivation. For example, Dunphy et al. note that "66% of respondents in a survey of 300 corporate users wrote down work-related passwords"[13].

While these quantitative studies are valuable in identifying *what* people do, we have found that, lacking motivations for action, it becomes difficult to interpret results. Frequency of writing down passwords is one statistic that is particularly difficult to interpret. For example, in our observations we found that many participants, including the most security conscious, reported writing down a password or even sharing a password; however, there was often specific

reason for needing to do so. For example, P1 notes that they share a password, but only when there is no other option.

[P1]At work if I need someone to take over for me when I'm gone or sick I'll write my password down, and in that case I don't really care that much
[Moderator]So if someone at work needs you password you'd just give it?
[P1]Um depending on the context, I'm reluctant to give it unless there is no other option.

P4 also reports sharing a password, but only with specific, trusted people in their personal life:

[Moderator]Have you ever shared a password?
[P4] Yes, a low security one... I have shared a higher security one in my personal life but only with trusted people like my parents.

Similar results apply for the statistic that "88% report having to reset a password after forgetting it"[20]. Among our participants these situations were rarely reported for an 'important password', like email or banking.

While quantitative studies may provide a snapshot of *what* people do, we argue that they are difficult to apply to design. Personas, in contrast, aim to reveal *who* people are. Their goal is to allow designers an understanding of *why* people do what they do.

We are not the first to claim that differences exist between users, and that understanding these differences may aid in design. Ackerman et al.[2] used opinion surveys to create three classifications of privacy awareness. Most of their respondents were considered the pragmatic majority; the others were either marginally concerned or were privacy fundamentalists. Our personas build on this previous work by incorporating both knowledge and motivation into a view of different sets of individuals. The goal of this paper is to explore the differences in users and to ground that exploration in a set of "security personas".

METHODOLOGY

In the book, "The User is Always Right", Mulder and Yaar, discuss practical ways to create and use personas[20]. In this book they also discuss the differences between qualitative and quantitative personas. Our aim is to create a set of qualitative security personas. Both Cooper & Mulder and Yaar provide tips and methods for making qualitative personas real. The standard methodology is to

1) Conduct interviews with potential users.
2) Create the segmentations based on the interview data.
3) Make the personas real and believable.

To begin constructing our personas, we conducted semi-structured interviews with thirteen participants. Participants were recruited online from across North America and interviewed over Skype. All the participants were aged 23-27 and four were female. All of the participants had a post secondary education but were no longer in school.

During the interviews the questions revolved around three themes. First, we developed an understanding who the participant was and how they used computers. Second, we explored the participant's security and privacy background, including their knowledge of security issues and their security concerns. Finally, we examined their current security and privacy practices. As our goal was to assess both knowledge and motivation of participants, questions included both a mix of factual questions about security, open-ended questions about approaches participants took toward security, and scenario questions that asked participants what they would do in a given situation. Examples of factual questions, assessing knowledge, include the following:

- Can you tell me what a cookie is?
- Can you tell me what a security certificate is?
- Can you tell me what https means?

Questions that indicated aspects of both knowledge and motivation included more open-ended questions:

- Is your wireless network secure? How do you know?
- Can you tell if your neighbors have secured networks?
- Have you ever changed your browser's settings? How long ago and why?

We measured motivation specifically through participants desire to act on security concerns. Questions that helped us assess the participant's motivation included:

- Who would you say is more/less secure than you?
- What are some examples of things that you wouldn't want to have online?
- Where did you learn about your security measures?
- In terms of computers or the internet, who are the 'bad guys'?

We also asked some scenario questions that involved changes in behavior based on concrete examples. For example, we asked "If you knew there was a 50% chance, that at any given time, someone was watching everything you did on your computer, would you change your behaviors? How so?"

Once the interviews were completed, they were transcribed and quotes from open-ended questions were analyzed using an affinity diagram. Based on the affinity diagram, themes and persona segments were formed. We then mapped these themes and persona segments onto groups of participants.

Segmenting Participants - The Interaction of Knowledge and Motivation

To be useful, a persona is designed to represent a group of participants. As a result, one goal of our interview data was to develop an understanding of how motivation and knowledge interact to create different types of users. To group participants based on knowledge and motivation, we used transcripts of interviews. Answers to questions from raw interview data were used to grade the knowledge and

motivation of our participants on three levels: Low, Moderate, and High. The final clusters of participants produced the five groups that were eventually developed into personas. In the observation section we look at some of the responses that helped us place these participants.

OBSERVATIONS

As described in the methodology section we divided the participants into three levels of knowledge and three levels of motivation. While there are variations within each level, our goal was to provide a course view of participants in terms of both motivation and knowledge, and our 3-level categorization allowed that. The table below places the participants within their level of knowledge and level of motivation.

High Knowledge	P3, P13		P1, P8
Moderate Knowledge		P2, P4, P11	
Low Knowledge	P6, P5, P9	P7, P10, P12	
	Low Motivation	**Moderate Motivation**	**High Motivation**

Table 1: Knowledge and motivation of participants allows grouping into five user types.

Participants in the low motivation category clustered into two different knowledge levels. There were a group of three participants who had low knowledge, and two participants had good knowledge of security. As an example of the disparity in knowledge between these participants when asked "what is a cookie?" P9 said,

Something that takes up space on your computer and it comes from when you get things off the internet. I don't think it's the same as a virus type thing but I also don't think it's good for your computer.

P13, in response to the same question said

[A cookie] is a little file that the browser puts on your computer to store some kind of information about your visit or whatever you want to track…Every once in a while they will create a script that will pop up with a survey and if they have seen that survey once then it'll create a cookie and it won't show up again.

While there is a clear distinction in knowledge between P9 and P13, in both cases, we saw little motivation for security. Participants in the low knowledge, low motivation category had no knowledge of security procedures and didn't think it was a problem. An example of an assessment of the interaction of knowledge and motivation, P6 stated:

My old password that I got rid of maybe 4 months ago... was 123456. Everything was set to it, and the incredible thing is I've never had any problems what so ever... I have no fear when it comes to hackers and all that crazy stuff there is no reason for them to go after me, I'm not a target.

Participants in the more knowledgeable group were aware of what was wrong but still preferred convenience over all else. For example demonstrating both knowledge and motivation when ask about home wireless security, P3 said,

With WEP which is terrible but realistically is secure enough. If some Unix script kiddie wants to crack my WEP then he can get in because I've honestly had trouble with WPA just being a pain.

As we move across the table, participants of moderate motivation fell into two categories of knowledge, low and moderate. P7, P10 and P12 had similar answers on questions assessing knowledge to P5, P6 and P9. For example, consider the following interaction with P7:

[Moderator] Is your wireless secure?
[P7] Yes.
[Moderator] How do you know that?
[P7] I've been told that, and whenever anybody wants to go on it they have to get all the numbers and stuff like that.

Those with moderate knowledge were able to sufficiently answer most technical questions without trouble.

[Moderator] What is a security certificate?
[P4]A file that is defined by and certified by a trusted party.

Moderate motivation, like moderate knowledge, is particularly difficult to characterize. Within the moderate motivation group there are difference levels of knowledge, which further confounds characterization. P12 notes:

I have 3 passwords, It's a word and a number for all of them. The nice thing is that you usually get three tries on accounts before they lock you out so if I forget one I've used then I can usually get through the three of them.

In contrast, P11 and P4 display their somewhat superior knowledge:

[P11] If I'm actually entering my credit card number or something that is secure like that I will make sure that it's a secure site by looking for a padlock and https.

[P4] When I sign up for a new service with a website I'm definitely interested in what information it's going to share about me and what will be used in what way.

The primary characteristics of moderate motivation were participants' willingness to act on security or privacy concerns that were particularly relevant to them. For example, P10's Facebook account caused some worry:

On occasion [I worry about Facebook], but only because I have pictures of my nieces and nephews on there. That made me a little more cautious I know that Facebook has a thing that you can limit who see your pictures but I do know that there is one little trick that people can get around with that … and that's a little weird to me.

Our fifth group consisted of participants that were both highly motivated and highly knowledgeable. These participants were technically inclined and both worked in

the computer industry (though not specifically in security). These individuals were more motivated than any of our other participants in how they learned about security, in their actions, and in their concerns. First, these highly motivated participants would often go out of their way to learn about security. When asked 'where did you learn?' P8 and P1 had similar responses noting:

[P8]The internet actually, more specifically I guess tech sites... actually going and reading and looking for security information.

[P1]A lot of it through reading. Some advice through more knowledgeable friends. A lot of experience, Some in the classroom too.

Highly motivated participants are normally very knowledgeable. We attribute this both to the availability of security information online, and to a willingness to think about and act on aspects of security informed by their extensive knowledge:

[Moderator] Is your wireless secure?
[P1] As secure as it can be... I believe even WPA is cracked now, you know I do my best.

[P8] I think what bugs me the most is the authentication questions, the idea of having and easy question in case you can't get the hard question.
[Moderator] So what do you usually do when you encounter one of those?
[P8] I've considered just putting my password in there again but I'm concerned that they might just be storing them in plaintext … Um so now I just randomly generate a string, put it in there and store it in keychain.

In our participant population, we did not find any participants who were highly motivated but lacked knowledge of security. This makes almost intuitive sense: There is a wealth of practical advice and information about security available for those who are willing to look. As a characteristic of highly motivated participants was a willingness to proactively learn about a broad set of security issues, they would almost always have extensive knowledge of security and privacy risks.

PERSONAS

Our qualitative data and analysis represent the first two steps in constructing personas. By characterizing participants around knowledge and motivation, we observe five groups of potential users. We label these potential users as different types of security personas: The oblivious target, a security persona with low motivation and knowledge; The struggling amateur, a security persona of moderate motivation and low knowledge; The aware technician, of moderate knowledge and motivation; The lazy expert, with high knowledge but low motivation; The paranoid expert, with high knowledge and motivation.

While our qualitative results provide guidelines for the five security personas, to make personas real there is a set of information that must be synthesized from interview data. Qualitative personas typically consist of a name, a quote, personal demographic information, domain specific information including objectives and motivations, and a photo (which we obtained from online stock images). Each persona should also have a profile, which is "the meat of the persona; it summarizes all the key differentiators and attributes, while telling the story of who this person is and how he or she interacts with the company/product."[20] Once the personas have been specified, they can be used in the creation of scenarios and to focus the discussion of design. We now introduce each of our security personas.

Allison: The Struggling Amateur

- Moderate motivation
- Low knowledge

"I think I worry most about my bank account being hacked, but seeing the awards they have won [for security] makes me feel better"

Allison wouldn't really say she's tech savvy but she has been using a computer since high school, and bought her own when she left for university. She's also currently looking for a new job and is a little concerned about putting her phone number and address out there but she does it anyways.

Allison maintains three somewhat similar passwords that are usually a word or date that is meaningful to her. Most things about security she learned from her friend Henry, who she still relies on for advice even though he lives far away. Usually she doesn't like to online shop just because the shipping costs so much and she would rather just go to a store and pick it up. Overall her main concern is online banking but she has a lot faith in her bank to be secure.

Henry: The Lazy Expert

- Low motivation
- High knowledge

"I'm sure hackers are still a concern, just more for major corporations and not the average person"

Henry is a web designer at a large company in Silicon Valley. His work place is fairly strict on their security rules, which Henry is happy to comply with even though he thinks some of them are unnecessary. Some people give him a funny look when he puts his laptop in the trunk of his car instead of the empty seat beside him but he's okay with that.

To Henry's parents and friends, he's still considered the computer fix-it guy. Over the years Henry has given out lots of security advice to his friends and family, but some of it he

doesn't follow himself. For instance, he doesn't even have a virus scanner on his computer. When talking about security Henry may not know everything but he is fairly confident that he is not a target for any attacks. He tries to maintain a professional image on anything that is directly tied to his name, and for everything else he's just a face in the crowd.

Mark: The Oblivious Target

- Low motivation
- Low knowledge

"I only changed my password because when I was signing up it wouldn't let me use my normal one."

As an educational assistant, Mark is always so busy he barely has time access to a computer. What is most frustrating about using the computer at work is having to log into their system--they've made the password much more complicated than his regular password and require him to change it too often for, what feels like, no apparent reason. He likes to switch back and forth between two easy passwords that he can remember. At least the system always gives him a few tries if he can't remember it the first time.

Generally when Mark is using the computer he doesn't really think about security or privacy until someone brings it up (and even then it's a fleeting thought). Mark has only been using Facebook for a little while and worries about his ex-girlfriends (and his mom) being able to find him on it. He remembers trying to set his Facebook page to private when he signed up but isn't completely sure that it worked and keeps forgetting to check it again.

Robert: The Paranoid Expert

- High motivation
- High knowledge

"I try not to use any websites that might store my personal information in plaintext."

Robert went to university for software engineering and got some really cool co-op placements around the country. In his last year of university (even though he loved programming), his cyber ethics course really struck a cord with him. Since then he's added some security and privacy blogs to his RSS feeds. He tries to be diligent with regards to security and privacy within a reasonable degree (since he still uses Facebook and Google).

When signing up for new accounts Robert is very careful what information to give them and adds filters to his email address if he thinks he will get junk mail from the site. For the authenticating questions, Robert will often put in a computer generated password and save the password in Keychain with his other passwords. However, Robert also likes to try all the new web 2.0 services and creates new accounts just to try things out. He feels that if it is an account that wouldn't harm him if it was hacked, it's okay to use his throwaway password.

Patricia: The Aware Technician

- Moderate motivation
- Moderate knowledge

"I'm more worried about what other people are doing to protect themselves."

Patricia tends to read about computers and the internet in the news and always picks up on the problems that are reported. She is currently concerned about the people that do data mining like Facebook and Google. To help with this she has her browser delete history and cookies when she closes it.

On her own time, Patricia loves to shop online and is always amazed at the good deals. She tries to stick to trusted sites like Amazon but has recently fallen in love with sites like esty and Threadless. She was a little hesitant at first with these sites but read reviews and knew to look for the padlock before giving her information. Working for the bank she also has some confidence that if her credit card was stolen the bank would be able to reimburse her. Patricia feels like she's got the security/privacy thing figured out and worries about her parents who aren't as tech savvy.

EVALUATING PERSONAS

Researchers have frequently evaluated the use of personas in design, seeking to determine whether personas aid in the design process [5,7,8,18]. However, our goal is not to evaluate whether these security personas are valuable in design – a central premise of this work is that there does exist a value to personas. Instead, we wish to determine whether the security personas we have developed are a useful representation of the design space in security and privacy. We do this by answering two questions: Do the personas represent users? *and* Do the personas enable analysis of design?

Do the security personas represent users?

One way to evaluate our personas against the design space is to look at a separate set of participants. To perform this analysis, colleagues made available to us a set of participants collected from a study of WiFi security practices [1]. Table 2 describes these participants.

Study Method

This WiFi study was a two-part study. Participants, recruited at random from area cafés with open wireless access points, were questioned about their security practices, and given a demonstration of a packet sniffing attack in the first phase of the study. 3 – 4 weeks later, participants were re-interviewed to determine whether WiFi

behavior had changed, and what factors influenced whether participants did or did not change behavior.

Results

The participants were coded by independent researchers and we explain some of the observations that determined the participants' placement within the grid. As one component of the study, our colleagues questioned participants' on their knowledge of security technologies. One participant, W12, had extensive knowledge of security and privacy. Four other participants, W1, W2, W4, and W8 had moderate knowledge of security technologies. Other participants, W3, W5, W6, W7, W9, W10, and W11 had limited to no knowledge of technologies such as Secure Socket Layer (SSL) protocols and Virtual Private Network (VPN) Connections. Table 3, below, shows our placement of this set of WiFi participants on our knowledge to motivation grid.

ID	Occupation	Age, M/F
W1	Mathematics Ph.D. student	29/M
W2	English student/retail employee	22/M
W3	Retired sales manager	67/M
W4	Government employee	24/M
W5	MBA student	26/F
W6	MBA student	29/M
W7	Chemical engineering/MA student	23/F
W8	Investment analyst	23/M
W9	Physiotherapy/recreation student	24/F
W10	Sociology MA student	26/F
W11	Behavior Therapist	30/F
W12	Security expert	35+/M

Table 2: Participants in the WiFi study.

In terms of motivation for security, participant W12 was both highly knowledgeable and highly motivated, the Robert of our persona set. In transcripts, we observed that this participant describes how he avoids using webmail in a browser because of "man-in-the-middle" attacks. He also avoids doing online banking on public WiFi, noting that he "knows enough of security to know it's reasonable," but had some concerns about highly sophisticated potential attacks on SSL connections.

W1 and W8 both had moderate knowledge of security, but very little motivation. During the follow up interview, W8 noted that:

Well, the way I see it is, if somebody is out there logging what websites I visit and sells it, that's fine.

W1 initially noted that he was a "careless WiFi user" and saw little reason to change. After all, anyone who actually tried to eavesdrop on someone would have to have "psychological problems" according to W1, and so it just wouldn't happen. While these participants don't directly align with Henry, our lazy expert (they have slightly less knowledge) they share one important characteristic. Both Henry and our new participants believe that, regardless of the fact that they may be exposing themselves to risks and an awareness of those risks, the chances of something happening to them are low, and it's not worth the bother to change their ways. They are not a target, and so do not need to change.

High Knowledge			W12
Moderate Knowledge	W1, W8	W2, W4	
Low Knowledge	W5, W9	W3, W6, W7, W10, W11	
	Low Motivation	**Moderate Motivation**	**High Motivation**

Table 3: WiFi participants grouped according to motivation and knowledge.

W5 and W9 know very little about security, but do not see any reason to change, even in light of a packet sniffing demonstration. W9 notes:

I'm very flexible, so if people want to know where I'm going, OK. I don't care.

W2 and W4, both with moderate knowledge of security, were classified as having moderate motivation because of actions they took proactively to protect themselves. Both noted expired security certificates, and only went to websites they trusted with these expired certificates, a behavior echoed by W12. As well, both were aware of SSL connections and paid attention to 'https' and padlock icons to indicate secure web pages. While their area of interest is slightly different from Allison's, they share Allison's focus on a single area of concern.

Positioning W4 was somewhat challenging; identifying this participants motivation resulted in some back and forth between researchers. This participant was very careful about login prompts – checking for encrypted connections – and was reluctant to engage in online banking or other potentially risky behaviors on public WiFi. However, one characteristic of high motivation among our initial participants is that they proactively read about security through online publications and tutorials. Participant W4 did not proactively educate himself about security, and he was very focused on login security but did not consider other aspects of privacy and security. Because we defined high motivation as a set of participants who proactively learn and have broad concerns, he was placed in the moderate motivation category by independent raters. In the end, we feel the ranking is justified. W4 shares more characteristics with Patricia than with Robert.

W3, W10, and W11 all reported changes in behavior, particularly an increased caution using open WiFi as a result of the packet sniffing demo. W11 taught her

coworkers about SSL connections and worked with her peers to ensure everyone was being more secure. W3 was reassured about his online banking, and paid careful attention to connections after the demo. Finally, both W6 and W7, despite a lack of knowledge, proactively took steps to protect themselves, justifying their placement in moderate motivation. These participants knew little but all wanted to be secure. They typically welcomed advice from someone like Henry about how best to protect themselves, and generally tried to follow Henry's advice.

Do the personas enable analysis of design?

Another aspect of personas is there utility in discussions of security tool design. As validation of our personas in design, we perform a thought experiment examining two common pieces of security software bundled with modern operating systems. The first is User account control in Windows Vista, which notifies the user when any administrator-level task is initiated through a dialog, Figure 1. The second is Windows Firewall which has default settings and a set of customization screens.

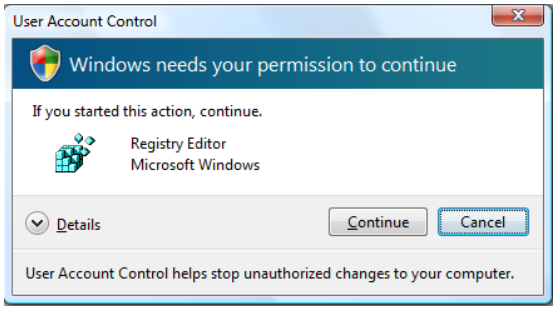

Figure 1: UAC Dialog Box in Vista

Consider, first Windows User Account Control. It is difficult to articulate how this control appeals to any security persona we specify – some (Robert, Patricia) because it doesn't provide them with enough information; others (Mark, Allison) because it asks questions that they cannot really answer; and Henry because it prompts him when he would rather ignore security and privacy as much as possible.

Windows Firewall, in contrast, allows low motivation personas (Mark and Henry) to generally ignore it. Allison is reassured by its presence, and only attends to it when she receives a security warning. Finally, Patricia finds the simple GUI for customizations useful. Only Robert might find the application of limited usefulness for him.

In summary, Windows user account control is poorly designed. Even its target persona, arguably Patricia, receives insufficient information to make informed decisions. In contrast, Windows Firewall seems functional for most users. Even paranoid experts like Robert recognize the fact that, for other people who know less than him, it's probably a good idea to have a basic firewall with simple settings.

DISCUSSION

In any work that tries to generalize across a set of users there will be characteristics of users that are fuzzy, lost or ignored. In our evaluation of personas above, we note that our personas do capture important characteristics. There are also other characteristics of our participants that we found interesting but hard to capture. In particular, within an individual participant, there were occasionally multiple identities that caused the individual's motivation levels to shift within the table. Changing contexts – work and home – or changing roles – from user to helper – influence users' attitudes toward security and had an effect on participants' motivation level.

Multiple Identities - Context

During the course of the interview some participants seemed to change their motivation based on the context of the discussion. It was common for participants to be more motivated in their workplace than in their personal life. For example, when discussing passwords P13 said

I have different levels of passwords for each of [the sites I visit]. Like some that I don't care about, like Facebook is less secure than my work. Work forces me to have a secure password and changes it every couple of months. So work naturally is going to be the highest for everything. Facebook and such I don't care about because there's nothing anyone can really do with that except slander me.

There are also external motivators, from social pressure, to being reprimanded, to job loss, that enforce protecting oneself at work. P2 said

Because I know that [work] can monitor pretty much anything you do on the computer, sometimes I don't even use my Google reader because there may be things that aren't entirely professionally appropriate.

When we asked P4 what he wouldn't put on his Facebook he said,

[P4] There's lots of stuff that I work on that's confidential and I can't talk about it or post pictures or share in any sort of public or even private way. So yes I definitely censor some stuff.
[Moderator] Do you have concern for your information?
[P4] Ummm. I guess I wouldn't post about my relationships so I guess it's not exclusive to my work.

Together, we group these together as context-based motivations, and note that an increase in motivation based on context is a potential characteristic of every persona except our paranoid expert, Robert. These characteristics are most predominantly demonstrated in the depiction of Henry.

Multiple Identities - Role

A few of the participants had an additional role to play when it came to security and privacy issues. Not only were these participants responsible for protecting themselves, but they were often the technician for their friends or family.

These helpers were often responsible for fixing other people's computers and for giving advice and guidance in questionable situations.

[P13] My mom, I dunno, she gets a virus every other week. She'll call me up and is like 'It says I have a Trojan horse what's that?' and I'll look at it and see if I can fix it. She doesn't even do that much online, she just browses and ends up with viruses.

The helpers were often much more motivated to help others than they were in securing themselves. P13 fell into this category, and P4, based on experience helping others, had concern for the general population,

[P4] I might be concerned for other people who do not understand the internet as well. Like I think there should be a better awareness of online privacy issues.

Participants who changed motivation based on role typically have moderate or high security knowledge and low to moderate motivation.

LIMITATIONS OF THIS WORK

As we note earlier, the personas we develop here are qualitative personas based on a relatively small set of interviews. The participants from whom our personas were developed were all 23 – 27 year-old, educated professionals. To partially address this, we evaluated our personas with participants from a separate WiFi study, where participants were recruited in person from area internet cafés. While this allowed us to develop an intuition on the generalizability of our personas, any set of personas covers only a subset of the total user community. Future work includes expanding qualitative and quantitative aspects of these personas.

Another avenue to explore with persona work in this area is the concept of anti-personas. The project would really describe the different threats that are out there. It would be helpful to understand how the threats are really perceived, how common they are, and how often people are anticipating them. It always helps to better understand the enemy when designing a secure system. For example it would be easier to protect against the script hacker than it would be to protect against the social engineer. Allowing the researchers to really focus on who these people are, may allow them extra insights into how to protect against them.

CONCLUSION

The hypothesized value in personas is the ability it gives designers to describe who the target user is, to connect to that target, and to ground discussion of users in details of a "real" person, rather than in abstract attributes. Past work in understanding users in the security and privacy domain has, we feel, focused too specifically on generalizations across all users. As well, much research has been grounded in survey data, without attending to the deeper motivations and knowledge that are pare of diverse participants.

Through qualitative interviews we have observed an interesting interaction between the motivation and knowledge of our participants. By clustering a set of participants around levels of motivation and knowledge, we identify five prototypical users. Using characteristics of these users drawn from affinity diagrams, we craft five unique personas. Our goal is to present the personas as a starting point for a discussion about the different types of target users in the design of security and privacy technologies.

ACKNOWLEDGMENTS

We would like to thank our participants and funding agencies.

REFERENCES

1. Authors Anonymized, ''Who would spy on me?' Naïve Security in a WiFi World'. Under review for CHI 2010
2. Ackerman, M.S. and Cranor, L.F. and Reagle, J. Privacy in ECommerce: Examining User Scenarios and Privacy Preferences, in Proceedings of the 1st ACM conference on Electronic commerce, (Denver, CO, US, 1999), ACM, 1-8
3. Acquisti, A. and Gross, R. 'Imagined communities: Awareness, information sharing, and privacy on the Facebook'. Lecture Notes in Computer Science, 6th Workshop on Privacy Enhancing Technologies, Vol. 4258, 2006, 36-58
4. Adams, A. and Sasse, M.A. 'Users are not the enemy'. Communications of the ACM, Vol 42, n 12, 1999, pp 40-46
5. Aquino Jr, P.T and Filgueiras, L.V.L. 'User Modeling with Personas'. Proceedings of the 2005 Latin American conference on Human-computer interaction, (Cuernavaca, Mexico, 2005), ACM, pp 277-282
6. Berendt, B. and Günther, O. and Spiekermann, S. 'Privacy in e-commerce: stated preferences vs. actual behavior'. Communications of the ACM. Vol 48, n 4, 2005, ACM, pp 101-106
7. Chang, Y. and Lim, Y. and Stolterman, E. 'Personas: From Theory to Practices'. NordiCHI '08: Proceedings of the 5th Nordic conference on Human-computer interaction, (Lund, Sweden, 2008), ACM, pp 439-442
8. Chapman, CN, Love, E, Milham, RP, ElRif, P, and Alford, JL. (2008). Quantitative evaluation of personas as information. Proceedings of the Human Factors and Ergonomics Society 52nd Annual Meeting, New York, NY, September 2008, pp. 1107-1111.
9. Conti, G. and Sobiesk, E. 'An honest man has nothing to fear: user perceptions on web-based information disclosure'. SOUPS '07: Proceedings of the 3rd symposium on Usable privacy and security (Pittsburgh, Pennsylvania, USA, 2007), ACM, pp. 112-121

10. Cooper, A. The Inmates are Running the Asylum. Macmillan Publishing Co., Inc., Indianapolis, IN, USA 1999.
11. Dourish, P. and Anderson, K. ‘Collective information practice: exploring privacy and security as social and cultural phenomena’. Human-computer interaction, vol 21, n. 3, Taylor & Francis, 2006, pp 319-342
12. Dourish, P. and Grinter, E. and Delgado de la Flor, J. and Joseph, M. ‘Security in the wild: User strategies for managing security as an everyday, practical problem’. Personal Ubiquitous Computing, vol 8, n.6, Springer-Verlag, 2004, pp 391-401
13. Dunphy, P. and Nicholson, J. and Olivier, P. ‘Securing passfaces for description’. SOUPS '08: Proceedings of the 4th symposium on Usable privacy and security. (Pittsburgh, Pennsylvania, USA, 2008), ACM, 24-35
14. Florêncio, D. and Herley, C. ‘A large-scale study of web password habits’. WWW '07: Proceedings of the 16th international conference on World Wide Web, (Banff, AB, Canada, 2007), ACM, 657-666
15. Friedman, B. and Hurley, D. and Howe, D. C. and Felten, E. and Nissenbaum, H. Users’ Conceptions of Web Security: A Comparative Study in CHI '02: CHI '02 extended abstracts on Human factors in computing systems, (Minneapolis, MN, USA, 2002), ACM, 746-747.
16. Grudin, J. and Pruitt, J. Personas, participatory design and product development: an infrastructure for engagement. Proc. of the Participatory Design Conference, CPSR 2002, 144-161
17. Hart, D. ‘Attitudes and Practices of Students towards Password Security’. Journal of Computing Sciences in Colleges, Vol. 23 n. 5 Consortium for Computing Sciences in Colleges, 2008, pp 169-174
18. Long, F. 'Real or Imaginary: The Effectiveness of using Personas in Product Design'. Proceedings of the Irish Ergonomics Society Annual Conference, May 2009, pp1-10 Dublin.
19. Miaskiewicz, T., Sumner, T., and Kozar, K. A. A latent semantic analysis methodology for the identification and creation of personas. In Proceeding of the SIGCHI Conference on Human Factors in Computing Systems, CHI '08, 1501-1510.
20. Mulder, S. and Yaar, Z. The User is Always Right - A Practical Guide to Creating and Using Personas for the Web. New Riders Publishing Thousand Oaks, CA, USA, 2006.
21. Ponemon, L. Perceptions About Passwords, CSO Online,March 01, 2006, Retrieved August 8, 2009, from CSO online: http://www.csoonline.com/read/030106/ponemon.html
22. Pruitt, J. and Adlin, T. The persona lifecycle: keeping people in mind throughout product design. Morgan Kaufmann, San Francisco, CA, USA, 2006.