Naïve Security in a Wi-Fi World

Colleen Swanson, Ruth Urner, Edward Lank

Naïve Security in a Wi-Fi World

Colleen Swanson, Ruth Urner, and Edward Lank

David C. Cheriton School of Computer Science
University of Waterloo
Waterloo, Ontario, N2L 3G1, CANADA
{c2swanso,rurner,lank}@cs.uwaterloo.ca

Abstract. Despite nearly ubiquitous access to wireless networks, many users still engage in risky behaviors, make bad choices, or are seemingly indifferent to the concerns that security and privacy researchers work diligently to address. At present, research on user attitudes toward security and privacy on public Wi-Fi networks is rare. This paper explores Wi-Fi security and privacy by analyzing users' current actions and reluctance to change. Through interviews and concrete demonstrations of vulnerability, we show that users make security choices based on (often mistaken) analogy to the physical world. Moreover, despite increased awareness of vulnerability, users remain ingenuous, failing to develop a realistic view of risk. We argue that our data present a picture of users engaged in a form of naïve security. We believe our results will be beneficial to researchers in the area of security-tool design, in particular with respect to better informing user choices.

Keywords: Wi-Fi, hotspot, security, behavior, privacy, trust.

1 Introduction

In March 2002, Network World ran an article entitled "Wi-Fi World," in which they hypothesize a world where wireless internet is ubiquitous. They describe a scenario in which people move from wireless at home to wireless at work, at cafés, and at airports. Helped along by inexpensive hardware, we now enjoy near-universal access to 802.11 wireless networks. While wireless hotspots have made accessing the internet more convenient, they also pose significant privacy and security risks to users.

Wireless network communication is particularly susceptible to eavesdropping (or packet sniffing) because an eavesdropper need not physically connect to a hardwired connection. They can sit in secluded locations within range of a wireless access point, but at some distance from their victim, and monitor all internet traffic being transmitted through the wireless signal. This allows them to easily determine websites users are visiting and any files, messages, or passwords used in the event users log into unsecured sites, use unencrypted email protocols (POP3 or IMAP) or unencrypted computer-to-computer connections (e.g. FTP, telnet, remote desktop). Furthermore, recent attacks on the SSL protocol [16] highlight the vulnerability of even encrypted—and therefore supposedly secure—connections.

This paper focuses on users' reactions to an awareness of their vulnerabilities when on Wi-Fi networks. To develop an understanding of whether people change with awareness of their vulnerabilities, we conducted a novel two-phase study of Wi-Fi users recruited from public cafés. This study included a demonstration of packet sniffing during the first phase and a follow-up study to determine whether and how users changed behaviors.

While we find that some participants do report an increased awareness of encrypted connections, changes in behavior were generally minor. We found an ingenuousness, a naïveté with respect to existing dangers, both before and after our demonstration of packet sniffing. Participants analyze dangers based on a set of simplistic assumptions: that they have nothing to hide; that no one would care to listen; that others on the network are honest; or that it is unlikely someone would target them. As a result, while they do take some steps to protect themselves, our participants engage in *naïve risk mitigation*, often basing their security strategies on faulty assumptions and analogies to the real world. Finally, we argue that by understanding users' perceptions of security, designers will be better able to train users to be secure and to communicate to users the risks and vulnerabilities that exist on their systems.

This paper is structured as follows. Section 2 contrasts our current research with related work. Section 3 outlines the details of our study. Sections 4 and 5 present the results, and Section 6 the design implications of our work.

2 Related Work

Research often paints a rather pessimistic image of users as having little understanding of current technology and the potential security risks involved. Even informed users often do not use available security tools, pay attention to browser indicators, or use secure passwords [3, 6, 10, 21].

In the past decade, there has been broad interest in user understanding and reactions to privacy and security issues that arise in the online world [1, 8–11, 13]); we will not attempt to address all related work, but rather highlight the most relevant. Flinn and Lumsden [9] conclude that although users try to educate themselves, they generally lack the basic knowledge necessary to assess privacy and security risks. Viseu [20] briefly touches on the theme of user behavior varying based on location, but only in the context of distinguishing between personal and public computers for online banking. Dourish et al. [8] highlight the need to make security more understandable, a theme we explore in our paper. We, however, focus on public Wi-Fi behavior with respect to both privacy and security, whereas Dourish is interested in security on a much broader level, focusing on how users view security relative to desired tasks. Finally, Dourish and Anderson [7] note that security is more than "economic rationality" and that general models of privacy and security are frequently borrowed from the physical world, a conclusion that echoes our observations of naïve risk management in the Wi-Fi world.

There is a small set of studies that focus on security, privacy and behavior on Wi-Fi connections. Kindberg et al. [12] investigate trust in Wi-Fi hotspots, observing that users willingly provided personal information in order to register for the authors' spoofed wireless service. Kowitz and Cranor [15] explore privacy in a lab setting by projecting excerpts from captured Wi-Fi packets onto a display. They report that participants felt uncomfortable while the display was on, but admit that participants may not have properly understood the relationship of the display to the functioning of the wireless network.

Klasnja et al. [14] investigate user understanding of Wi-Fi technology, current practices, and whether users send information they consider sensitive in the clear (accomplished by installing software to monitor participants' computers). They observe that users do not have a firm understanding of Wi-Fi security issues, and are surprised and concerned when presented with a list of released personal information. Users also indicated an intent to change their practices. Klasnja et al.'s primary focus, however, was on what users currently do to protect their privacy and whether users release information they wish to keep private.

Our study complements Klasnja et al.'s work in three ways. First, while Klasnja et al. look at what users currently do to protect their security, we expand significantly on this, exploring motivations for users' current Wi-Fi behaviors. Second, while Klasnja et al. observe a desire to change, they did not follow up to explore whether users actually changed, and why they did or did not change. Finally, our approach differs significantly from that of Klasnja et al. (and from Kowitz and Cranor) in that we did not involve participants' personal information in the demonstration of vulnerability. There is a distinction between a violation of privacy and an awareness of the possibility of privacy violation, especially with respect to user reactions and potential behavior changes. While both approaches have merit, we are most interested in how to encourage users to improve their privacy and security without first violating their security or privacy. In summary, we go beyond these and other previous works by not only exploring users' understanding of privacy and security practices, but also what effect increased knowledge of Wi-Fi actually has on behavior.

3 Methodology

Participants were recruited by word of mouth at local cafés offering free Wi-Fi and were only told we were interested in gathering information on general Wi-Fi behavior in public places. We interviewed 11 people of varying occupations and computer knowledge, P1–P11, and one security expert, S1, with ages ranging from 22–67; see Table 1. We remark that of the 12 participants, while most used their laptops frequently for work, study, and/or personal use, only S1 had extensive computer knowledge. Local recruitment and sample size may raise some concerns about the generalizability of these results. However, security and privacy researchers have found that geographic location and demographic characteristics have little effect on security/privacy behaviors [10]. As well, our sample size is not particularly small for a qualitative study [7].

Interviews were audio recorded and transcribed. For each round of interviews (initial and follow-up), once the data collection was complete, selected quotes were highlighted and analyzed using open coding; we refer the reader to [19] for a discussion of this technique. Quotes were organized using an affinity diagram by two of the researchers working collaboratively. A third researcher performed a separate coding of transcripts and validated clustering on the affinity diagram.

Table 1. Participant Demographics

ID	Occupation	Age, M/F
P1	Mathematics Ph.D. student	29/M
P2	English student/retail employee	22/M
P3	Retired sales manager	67/M
P4	Government employee	24/M
P5	MBA student	26/F
P6	MBA student	29/M
P7	Chemical engineering/MA student	23/F
P8	Investment analyst	23/M
P9	Physiotherapy/recreation student	24/F
P10	Sociology MA student	26/F
P11	Behavior therapist	30/F
S1	Security expert	35+/M

Our interviews were designed as follows. In the first interview, we gathered demographic information about the participants, as well as information on where participants use wireless internet. We conducted a walk-through of their most recent Wi-Fi session at a public place, then inquired whether and how often participants engage in various online activities at public Wi-Fi locations, all without reference to security. We transitioned into a discussion of privacy and security by asking about privacy and/or security concerns if participants had not already mentioned these topics on their own. We asked whether participants use any sort of protective measures while using wireless internet, explored their understanding and behavior with respect to SSL, and asked what information about their Wi-Fi activities might be available to other people.

We then moved to a brief explanation of how information is sent on wireless networks, introduced the concept of packet sniffing, and gave a brief demonstration using Wireshark (www.wireshark.org), a freeware network-monitoring program. Packet sniffing may be illegal by Canadian law, so we used two computers belonging to the researchers and avoided involving participants' or other café customers' computers. Instead, the demonstration consisted of using one computer to sniff the traffic of the other, while a researcher used the target computer to go to GoogleMaps and type in an address. Participants watched as the first computer captured this information, and were then shown how it was possible to recover exactly what had been typed and submitted to Google. Participants were allowed to ask questions as the demonstration progressed. In

case participants did not ask about activities such as online banking or online shopping, we briefly explained how SSL encryption disguises information and noted the URL indicator "https." Following the demonstration, we encouraged participants to discuss what they had seen, how they felt about it, and whether anything they had witnessed was likely to affect their Wi-Fi behavior.

Between 3–4 weeks after the initial interview, we contacted participants for a follow-up. Participants were not informed in advance of the second interview, but had agreed to be contacted in case we had further questions. Out of the participants P1–P11, all but P6 met us for a follow-up.[1] In this interview, we asked participants if they had given the demonstration any further thought and whether their public Wi-Fi behavior had changed in any way. We inquired how likely participants felt a packet-sniffing attack was, and what, if anything, would prompt them to change their behavior. To complete the overall picture of user behavior, we also asked participants about privacy and security programs and whether they would use such tools to protect themselves.

4 Current Wi-Fi Beliefs and Practices

The overwhelming view of our participants, when asked to identify any concerns they might have using Wi-Fi, was that they had none. Most explained that they generally felt safe using public Wi-Fi. P1 explained that while "there is probably some security risk . . . ," he was not concerned, describing himself as a "careless Wi-Fi user." P5 justified her lack of concern by comparing public wireless with her previous work wireless connection: given that "it's secure enough to use Wi-Fi for business purposes," she felt public wireless must also be safe by association. Although P5 was aware that her work laptop had special security features installed, this did not affect her reasoning. Her comment is a first glimpse of participants making choices based on analogy to the real world: while in some circumstances, it might make sense to say that "if A can do activity x safely, so can B", this is often faulty reasoning in reality and certainly does not translate well to the wireless world, as different security settings and software will result in different levels of security.

An analysis of the typical online activities our participants engage in via unsecured wireless, however, reveals a more complicated view of safety and security. Indeed, almost all of our participants (with the exception of P8) acted to protect either their privacy or their security, most commonly in the form of deciding on a set of activities with which they were comfortable, a topic we discuss in Section 4.1. In addition, some of our participants actively sought to protect themselves via awareness of SSL or security certificates; we discuss our participants' behaviors with respect to these security tools in Section 4.2. These results are especially interesting in the context of what types of attacks our participants believed possible before the packet-sniffing demonstration, which

[1] We remark that given S1's area of expertise, we only conducted the first part of the initial interview, as we felt the packet-sniffing demonstration and second interview would be inappropriate.

ranged from the belief in all-powerful hackers who could access any information on users' computers to the belief that any attackers would have to physically look at the laptop screen to glean information; a common theme was the idea that any attack beyond shoulder-surfing would require "computer savvy" (P12). Regardless of how extensive participants thought an attacker's reach might be, their security behaviors were surprisingly similar.

4.1 Controlling Risk through Regulation of Online Activities

In the first component of the interview process, we paid special attention to the types of online activities participants engage in while using public Wi-Fi. We were particularly interested in activities participants claimed to avoid and attempted to determine the underlying cause. The overwhelming (and unsurprising) theme emerging from this was that participants were primarily concerned with the security of their financial information and therefore uncomfortable banking or shopping via public Wi-Fi. While this was the main focus of their security concerns, we also observed that participants viewed privacy and security based on a perception of context (i.e., a café) and what was appropriate in that context. Some of these participants were particularly concerned with protecting the impression others would have of them.

As we discuss in the following sections, participants' security choices are frequently informed by an understanding of typical behavior in the real world, a phenomenon we call *naïve risk mitigation*. For example, some think about impression management and try to ensure that nothing scandalous about them is released. Others, conditioned to protect financial information, apply this same notion to the online world. Finally, while many researchers have argued that participants "don't care" enough about security or privacy to alter their actions, it seems that (with the exception of P8) participants we interviewed accept and expect the need to adapt their behavior to protect themselves.

Avoiding Financial Transactions Almost all of our participants reported avoiding banking and shopping while on public Wi-Fi. P2 even expressed his lack of concern regarding public Wi-Fi in terms of this avoidance:

> [Public Wi-Fi has] never been a concern because ... I don't do online banking in public places or purchase anything in public. (P2)

Two participants who said they did not "really" have concerns about public Wi-Fi immediately mentioned a discomfort in banking while on public Wi-Fi. P6 mentioned that he was unsure whether he would access his online banking over an unsecured wireless connection and that he tried to pay attention to whether the network was "secure" or not, citing fear of identity theft. The other, who said she does occasionally connect to online banking in public if she has forgotten to at home, admitted:

> I feel like I don't want to do my banking, also, like sometimes at a public location, because I don't know how computers work very well. (P10)

Other reasons given for this discomfort or avoidance varied, but most were equally vague in nature. P11, in examining her security concerns, explained that she does not "do banking or anything" when she is at the café, as it "says it's unsecured." P1 said that he did not bank online in public, but rather preferred to connect at home (via his neighbor's unsecured Wi-Fi) or school, explaining that "somehow I think it's more secure, but it probably isn't." Others who expressed clear security concerns about financial transactions—"I do it at home, the same as online banking" (P7)—focused on physical security, not the security of the Wi-Fi connection. P7 worried her account number would be stolen; P5 explained:

> I'm not sure if it's [avoiding online shopping] primarily due to . . . security of the internet connection, or just because I don't like flashing my personal information [in public].

Even the security expert avoids banking online over a wireless connection, explaining that he "know[s] enough of the security to know it's reasonable, but [he] just [does not] do it." S1 further clarified this, mentioning the possible technical attacks on SSL sessions and the potential to be tricked when tired. He concluded the discussion, however, by reiterating the common theme of being more comfortable at a location perceived to be private and controlled: "It's one of those things I just don't bother doing, because I just wait until I get home."

As the security expert notes, it is reasonable to argue that participants' determination to avoid financial transactions is somewhat irrational. Online banking and e-commerce sites use SSL connections to transmit information, so the information is encrypted. However, with limited security knowledge, applying the age-old adage "better safe than sorry" is not an unreasonable choice. Users who do not understand how security works and do not have the knowledge to verify security before entering financial information are nevertheless confronted with the need to make a decision how to behave. "Just as you wouldn't take your wallet [out] to count your cash" (P2), online banking is viewed as an activity more appropriate to the supposedly safe environ of the home. Indeed, P2 gives perhaps the most direct explanation of this phenomenon, describing it as a result of external conditioning to protect one's financial information:

> It just strikes me as something you do in the privacy of your own home. . . . I guess I'm probably conditioned in some way to believe that yeah, you just don't . . . because it's dangerous or whatever. . . . I don't really believe that, but I can't explain why I wouldn't do [online shopping]. That's probably why.

Impression Management Some participants expressed concern about protecting their privacy while on public Wi-Fi; some of the approaches were rather unique, amounting to impression management. For example, P5 limits the information on her laptop to what she is comfortable sharing with her mother:

> My laptop is mum-safe. . . . There is nothing which I wouldn't show to my mum and my mum is very conservative. There is nothing that couldn't be given to pretty much anyone.

As P5 further explained, she does not perform activities or store information she deems private:

> So like when I'm in a coffee shop right now, I don't do anything really, which is going to be a concern of mine if somebody finds out.

A similar limitation on behavior to protect privacy was echoed by other participants. For example P1, P3, and P7 did not want to be caught doing something that others might consider inappropriate. Both P1 and P3, somewhat tongue-in-cheek, mentioned pornography as something they would not download, and P7 explained that she does not have privacy concerns because she "didn't do anything illegal, you know, anything wrong."

4.2 Views of Security Protocols: SSL and Security Certificates

Although many of our participants' behaviors fit the general impression that the public suffers from lack of awareness and concern, we did see some interesting responses to SSL and security certificate warnings. Of the four participants who actually knew what SSL was, only two, P2 and P4, claimed to actively look for the "https" indicator. Interestingly, the others, P1 and P8, admitted that they never checked, but rather assumed SSL was being used whenever they "needed it"; this reaction of trust was quite similar to other participants' security beliefs and is theme we discuss further in Section 5.3.

Participants had a mixed reaction to security certificate pop-ups. Many, including S1, ignored these warnings either all or "most of the time." Our more security-aware participants, P2 and P4, claimed to pay attention to the pop-up warnings, unless they were viewing websites they "trust" (P4). One participant, P7, said she would "rather just close [the site]." P3 noted he would be reluctant to visit the site, but that he has little of value on his computer, so it would not matter if the site was malicious. P9 said she generally goes to the site, but judges whether to remain by the website's appearance. Finally, P5 ignores the warnings if she recognizes the site and has never had any problems, but otherwise uses a friend's laptop to access the site if her fiancé says it is not safe.

5 Participant Responses to a Demonstration of Risk

One question we asked was how people would respond to a realistic depiction of their vulnerabilities. Does it spur them to learn more about security? To change their behavior? As we note earlier, past results in security research have rarely focused on concrete demonstrations of specific vulnerabilities, or whether such demonstrations have any lasting impact.

5.1 Initial Responses to Demonstration of Packet Sniffing

Beyond general statements of interest—comments like "Cool," "Awesome," or "Neat"—our participants expressed a range of responses to the packet-sniffing

demonstration. P1 was surprised by the demonstration, but noted that privacy was not "really a big deal" for him, and that if "something like that happened, I wouldn't really care that much." One participant stated he was "a little perturbed" (P4), but not overly concerned (although this participant later modified his behavior significantly, as described in Section 5.2). Others noted that the demonstration was "kind of scary" (P11) or "super creepy" (P10). Some expressed surprise that "people can actually see my info, personal things" (P9). Others questioned whether we could spy on anyone in the café, and when we explained how we could (though we did not spy on others), commented that this was "not good" (P3). More specific reactions to the demonstration can be grouped into four categories: participants were surprised at how easy packet sniffing was; participants wanted to know how packet sniffing could be prevented; participants had questions about the security of their own activities; and participants appreciated learning about packet sniffing.

Many participants were not surprised by the demonstration itself, but were surprised by how easy it was:

> I probably would have thought something like this is possible. . . . I am surprised that there is a program that does that readily for you. (P8)

P2, P4, P5, P6, P8, and P9 all expressed similar sentiments, particularly some surprise at how easy it was for non-technical users. P6, for example, thought that it would "take some . . . technical skills, some programming or whatever."

An interesting role reversal took place at this point of the interview, where participants began to interview us. Participants were curious about how to prevent packet-sniffing attacks; they wanted to know "how you prevent that?" (P3), or "what [the café] would have to do to prevent this" (P8). Another common type of query involved the safety of online activities: online banking, e-commerce sites, Facebook, email, and others. Participants questioned us quite carefully on how security for online banking and e-commerce sites works. We provided a basic description of SSL protocols and how this protected participants from such attacks when connecting to these sites. Also, if participants did not ask about online banking or e-commerce, we proactively explained SSL connections to them. Several participants were reassured by this, noting that things were OK "as long as they can't find my banking information" (P10).

Finally, a common response was appreciation. P5 indicated that it "clearly shows that you can pretty much see everything." P4 always "thought it was that easy, but now that you showed me, [I'm more aware]." P2 noted:

> I'll certainly remain conscious of it, which is a good thing, obviously.

Participants also appreciated the ability to be able to act on information from the demonstration. P11 commented on getting laptops with wireless at work with "a lot of client info" on them and intended to verify that "those security measures" would be put in place. Another participant, P6, was concerned about "inside company information," noting that it was a "good thing" to see the demonstration because he was "doing this consulting project now" and "has a lot of financial documents" he sends "back and forth."

5.2 Behavioral Changes: The Plan and the Reality

When queried immediately after the demonstration about whether it would motivate behavior change, participants were split. Some participants expressed a desire to "be more cautious" (P11). Participants who queried us about online banking and security measures noted they would be more aware of the "https" indicator to ensure an SSL connection (P9, P10, P11). P5 explained that she was "probably gonna be a little bit more paranoid in terms of not using any ... personal information in public locations." Other participants were less concerned. P6 said he would not change his behavior because he does not "really have anything to hide." However, he also notes:

> Certainly if I were to work on some sensitive stuff, then that's definitely what I would probably think of. I would probably not send stuff from here on this wireless network.

P2 explained that despite a desire to remain conscious of the demonstration, "I don't think it would necessarily change my practices." This mixed message was common: participants indicated they were unlikely to change their practices, but also indicated that they would be more aware and take more care.

An analysis of reported participant behavior on follow-up confirms this notion: on the whole, any changes in behavior that occurred were minor and relegated to attempts to be more aware. Our main focus after the initial interview was determining whether participants had actually changed their behavior in any way. We wanted to see what they retained from the demonstration and if they reported being more aware. We conducted our follow-ups after 3–4 weeks, in our estimation enough time for participants to have re-established regular behaviors, but not so much that they would have difficulty recalling the demonstration.

We began the follow-up interviews by asking participants if they had given the demonstration any thought. Several participants mentioned having thought about the demonstration and all but one of the participants had discussed it. Some just told one or two of their friends, an unsurprising result. Some reported using their new knowledge to correct behaviors of their friends:

> I told [two of my friends] how it's not safe [to enter personal information in unsecured websites] because you showed me that what I typed in actually shows on your computer. (P9)

One participant (P11) taught all of her colleagues at work about the SSL protocol, claiming that they had all become more aware of the "s" in the browser and now tried to pay attention to it. P3, P5, P9, and P10 also reported remembering and thinking about SSL when online. Unfortunately, this did not necessarily translate into participants' behavior being more secure. While some (P3, P10, P11) reported checking for SSL when using sites they considered sensitive (e.g. banking), others only mentioned noticing the "https" when it was present:

> I haven't really investigated [whether sites I log into use "https"], but now I know [about "https"] so I probably know when it comes up and I feel more safe about it. . . . When it comes up it will automatically make me think it's a safe site, right. But then I didn't really [look] for it. (P9)

This last observation is particularly concerning, as from a security perspective, it is more important for users to notice the absence of a secure connection than its presence. P9's response to learning about SSL was to be reassured if she happened to notice its presence, rather than to actively check that SSL was being used. In this case, our user *felt* more safe online because she thought she was more aware, but in reality she had not improved her security.

Participants' perceptions of security and privacy changed in other ways as well. Increased knowledge of technology caused some participants to feel less safe overall, with some expressing doubts about their security even in the presence of security protocols. P3, at the end of his first interview, captured this feeling quite well: "I mean even the secure stuff, how secure is it?" P4 became so unsure of his online safety that he tried to avoid public Wi-Fi entirely, and if he did use public Wi-Fi did not do "anything that requires a login and a password." P9 explained that she now felt it was not "really safe to access [her] bank or you know, personal information," so she tried to avoid these activities while in public. P5 noted:

> Say if I was about to buy something and I had to enter all my credit card information. Although you said that if it says "s" it's safe, I probably would think about it twice, whether or not I want to use Wi-Fi.

Finally, nothing had changed for P1, P2, P7, and P8. P2, one of our more security-conscious participants, stressed that he had no reason to change as he had already been careful about his online activities. The others were also happy with their pre-demonstration behavior. As P8 explained:

> Nothing that I saw in there made me feel unsecure or threatened.

Given the limited effect of the demonstration, we asked participants what would motivate them to change their behaviors online. Most noted that the only thing that might prompt them to change their behavior would be if someone captured information from them:

> If I ever had a problem I'd change things, but . . . I have no reason to think that I'd do anything different right now. (P3)

Many participants echoed the sentiment that they would take action if something happened, but these behaviors were usually discrete, solving that specific problem rather than protecting themselves more generally. For example, P1 mentioned that if someone hacked into his email account, he would "have to change the password or something like that." P7 said that if she knew someone was spying on her, she would be "upset" and would stop using the Wi-Fi connection.

5.3 A Deeper Look: Underlying Motivations for (Lack of) Change

While we saw some change in behavior, we were surprised that, even with an awareness of how open information is on Wi-Fi, we did not see more awareness of privacy and security vulnerabilities. On the whole, participants were comfortable with their original Wi-Fi behavior. An analysis of the data reveals the following set of underlying assumptions that helps explain this: participants believed they had nothing to hide; participants felt people would lose interest pretty quickly; participants trusted others to not spy on them or to protect them; participants believed that packet sniffing did not happen often.

Nothing to Hide, Nothing to Fear Security researchers frequently quote the adage "The honest man has nothing to hide" as motivation for inertia when it comes to self-protection online. P1, P2, P5, P6, P7, P8, and P10 all mentioned variants of this. Participants felt that it was perfectly acceptable for someone to find out what they do online. P8 and P9 shared the sentiment that "if somebody is out there logging what websites I visit and sells it, that's all fine" (P8). P7 characterized her online activities as "not private," saying that she does "nothing super important." P5 echoed this sentiment when she explained that her "personal emails" were not "security sensitive."

I'm Not That Interesting P1 stated: "I'm not that interesting to begin with." Participants operated under a perception that the things they might reveal would be of limited value to other parties. P1, P2, P5, P6, P7, and P8 all noted the limited payoff someone would get from eavesdropping:

> The general notion of people that are invading your privacy isn't that much of a concern to me . . . I think they would lose interest pretty quickly in my case, anyway. There's not much to [know]. (P2)

I Can Trust Others There are two dimensions to trust that we found in responses. P1, P7, P9, and P10 all expressed trust that others would not spy—that others would be honest. P7 asked "What's the point of spying on what other people do?", while P1 explained that an eavesdropper would have to have "some psychological problems."

Both P7 and P9 attributed an honesty of intent to others, that people would do "their own stuff" (P9):

> I mean if people come in, they would do their own things, right? Normally people don't spying on purpose. (P7)

This trust extended to companies and institutions. For example, P10 trusted her internet service provider to monitor her home wireless network for intruders. P2 trusted the café to combat eavesdropping. Finally, P1, P4, and P6 assumed universities would protect the security of their communication on campus, an assumption faulty in reality. P1 and P3 both felt online banking must be all right because their banks were "legitimate" institutions.

It Would Never Happen to Me Some participants assumed the likelihood of network snooping was low, either because of a lack of interesting data or their understanding of the expense of the attack. P8 thought the odds are "slim to none":

> I just don't see what motive somebody would have to do that. To ... take your time, go out of your way, put all this software on and go to a public [place] ... and then sniff around.

Only P4 and P5 seemed to think eavesdropping more likely. P4 explained that "Enough of [his] friends have had some sorts of security issues that ... [he is] not willing to open [himself] up to that," and P5 took it as a "fact of life":

> I'm pretty sure people do it because it's available, it's there. I mean, for crying out loud, people peak on people in the change rooms, why won't they peak on somebody's laptop, which seems to be a little bit more useful to me.

6 Discussion

6.1 Practicing Naïve Security

In our observations, we bring to light two trends. First, we note that many participants' actions are (mis)informed by drawing mistaken analogy to real-world practices. Second, lacking knowledge, our participants believe that they have little of value, trust that others would not victimize them, and believe that something bad is unlikely. Together, these data lead to a view of our participants as both naïve (making decisions based on feelings, impressions, ideas, and not facts) and ingenuous (guided by a false sense of security). We draw a likeness between our participants' views of security and the concept of naïve, or 'folk' physics. Computers and computer security are incomprehensible to our participants. Therefore, our participants exhibit a naïve Wi-Fi behavior—they avoid things that may be dangerous, but they do so without knowing what is truly risky behavior. Participants practice naïve Wi-Fi Security based on their perceptions of risk and vulnerability.

Participants' activities are rife with instances of naïve security. When discussing security certificates, P9 went to websites and trusted the site based on if it "looked safe." P6 stated he would use any unsecured access point he could find to "check email," but not to browse the web. Finally, P8 does not believe people have "time to log hundreds of people." Unfortunately, malicious websites are designed to look trustworthy, unsecured access points are trying to get users to release passwords and other personal information, and logging and then parsing large data sets is trivial with simple scripting. Participants felt snooping did not happen because others would be honest, that their online financial transactions would be all right because they trusted the companies in question. P8, who never looked for SSL, was perfectly comfortable in the assumption that it was there if he "needed it."

Naïve security is also evident when we examine the more complicated behaviors of our participants. For example, recall P5's method of off-loading risk when confronted with security certificate warnings: If she recognizes a site and has never had any problems, she ignores the warnings. Otherwise she asks her more technically-minded fiancé if it is safe to go on, transferring responsibility. If he tells her it is not, she then "call[s] up [her] friend and use[s] his laptop" (P5), thereby transferring risk.

To overcome the misunderstandings in the naïve security paradigm, one valuable avenue for our participants seemed to be interaction with experts. They valued the packet-sniffing demonstration and in some cases acted on it appropriately. Just as concepts from naïve physics are addressed through education and enhanced understanding, additional discussions with experts could help our participants address security issues like email client setup, Gmail and Facebook use, malicious access points, and other potential Wi-Fi threats. However, it is challenging to engage participants to this extent. Beyond the limited resources of computer experts—we cannot spend individual time with everyone who uses public Wi-Fi—participants have an "it won't happen to me" attitude. Like those who believe theorems from folk physics, participants lack interest in developing a full and sophisticated understanding of the Wi-Fi world and how to protect themselves there:

> I did mention [the demonstration] to my fiancé, and I had to stop him at some point, because he ... tried to explain in detail, but .... I'm really not interested in technical details. (P5)

6.2 Creating Wi-Fi Security and Privacy Tools

Participants' reluctance to break from the naïve security paradigm might, at first, seem frustrating. However, through a better understanding of the paradigm of naïve security, one can imagine designing tools that educate users about risks based on analogies that they understand. Moreover, our results suggest that users appreciate learning about security via concrete, non-technical demonstrations, indicating the potential usefulness of such tools. Consider the following example. In spoken communication, we monitor our privacy by looking around to see who is close enough to overhear our conversation. Tools like Wi-Fi Radar that provide users with a radar display of nearby access points and the signal strengths associated with these access points could also display other wireless network interface cards (NICs) on the network. Combining this idea with Kowitz and Cranor's projected packet excerpts [15] could let Wi-Fi users know what others can hear and that others might be listening.

The challenge with tool design is that users still do not place a sufficiently high premium on privacy and security. When we explored attributes of security tools that participants might adopt during our interviews, participants noted that tools need to be cheap. Participants also did not want tools that slow their computer or require frequent interaction, describing security software as "just plain annoying" (P8):

> If [that tool] is not really expensive to buy .... Pretty sure I'll get it. If it's a product like a virus detector, a program that I [just] need to put in my computer. (P9)

> I mean, given that nothing happened to me yet, I think my priorities would still be as long as it's convenient, it doesn't slow my computer down, stuff like that, right? (P1)

While challenges in tool design may seem insurmountable, some tools have met with broad consumer acceptance. Most users hate the User Account Control dialog in Vista ("A program needs your permission to continue ...") because it prompts them at what seems to be foolish times, but the "set and forget" attributes of Windows Firewall and most virus scanners have met with broad acceptance. Research has consistently demonstrated that if users can understand explanations, they are much more accepting of software [5]. Coupling explanations that incorporate concepts of naïve security with technologies such as peripheral or ambient displays [17], better awareness of user interruptibility [4], or more intelligent "detail on demand" could enhance acceptance of security tools.

7 Conclusion

In this paper we explore the rationale behind current Wi-Fi security practices and the factors that limit changes in user behavior. Together, our observations of naïve risk mitigation and user ingenuousness depict a domain of naïve security, where users apply superficial concepts of real-world privacy and security and real-world likelihood of risk to the Wi-Fi world. We argue that by understanding how and why users rationalize actions, we can approach security-tool design from a more user-centric perspective, educating users based on their current understanding and presenting information in new, more effective ways.

Acknowledgments We thank the participants in our study. Funding for this research was provided by the Natural Science and Engineering Research Council of Canada, NSERC.

References

1. Ackerman, M. S., Cranor, L. F., and Reagle, J.: Privacy in E-commerce: Examining User Scenarios and Privacy Preferences. In: ACM Electronic Commerce, EC 1999. 1–8 (1999)
2. Acquisiti, A. and Grossklags, J.: Privacy and Rationality in Individual Decision Making. In: IEEE Security and Privacy. 26–33 (2005)
3. Adams, A. and Sasse, M. A.: Users Are Not the Enemy. ACM Commun. 42(12), 40–46 (1999)
4. Avrahami, D., Fogarty, J., and Hudson, S. E.: Biases in Human Estimation of Interruptibility: Effects and Implications for Practice. In: CHI 2007. 50–60 (2007)

5. Bunt, A., Conati, C., and McGrenere, J.: Supporting Interface Customization Using a Mixed-initiative Approach. In: IUI 2007. 92–101 (2007)
6. Dhamija, R., Tygar, J. D., and Hearst, M.: Why Phishing Works. In: CHI 2006. 581–590 (2006)
7. Dourish, P. and Anderson, K.: Collective Information Practice: Exploring Privacy and Security as Social and Cultural Phenomena. Human-computer Interaction. 21(3), 319–342 (2006)
8. Dourish, P., Grinter, R., Delgado de la Flor, J., and Joseph, M.: Security in the Wild: User Strategies for Managing Security as an Everyday, Practical Problem. Personal Ubiquitous Comput. 8(6), 391–401 (2004)
9. Flinn, S., and Lumsden, J.: User Perceptions of Privacy and Security on the Web. In: PST 2005 (2005), http://www.lib.unb.ca/Texts/PST/2005/
10. Friedman, B., Hurley, D., Howe, D. C., Felten, E., and Nissenbaum, H.: Users' Conceptions of Web Security: A Comparative Study. In: CHI 2002 Extended Abstracts, 746–747 (2002)
11. Hart, D.: Attitudes and Practices of Students towards Password Security. J. Comput. Small Coll. 23(5), 169–174 (2008)
12. Kindberg, T., O'Neill, E., Bevan, C., Kostakos, V., Stanton Fraser, D., and Jay, T.: Measuring Trust in Wi-Fi Hotspots. In: CHI 2008. 173–182 (2008)
13. Kindberg, T., Sellen, A., and Geelhoed, E.: Security and Trust in Mobile Interactions: A Study of Users' Perceptions and Reasoning. In: UbiComp 2004. LNCS, vol. 3205, pp. 196–213, Springer, Heidelberg (2004)
14. Klasnja, P., Consolvo, S., Jung, J., Greenstein, B. M., LeGrand, L., Powledge, P., and Wetherall, D.: "When I am on Wi-Fi, I am Fearless": Privacy Concerns & Practices in Everyday Wi-Fi Use. In: CHI 2009. 1993–2002 (2009)
15. Kowitz, B. and Cranor, L.: Peripheral Privacy Notifications for Wireless Networks. In: WPES 2005. ACM, 90–96 (2005)
16. Marlinspike, Moxie.: Null Prefix Attacks against SSL/TLS Certificates (2009), http://www.thoughtcrime.org/papers/null-prefix-attacks.pdf
17. Sankarpandian, K., Little, T., and Edwards, W. K.: Talc: Using Desktop Graffiti to Fight Software Vulnerability. In: CHI 2008. 1055–1064 (2008)
18. Solove, Daniel J.: 'I've Got Nothing to Hide' and Other Misunderstandings of Privacy. San Diego Law Review, vol. 44 (2007), http://ssrn.com/abstract=998565
19. Strauss A. and Corbin J. M..: Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory (3rd edition). Sage Publications (2007)
20. Viseu A., Clement A., and Aspinall J.: Situating Privacy Online: Complex Perceptions and Everyday Practice. Information Communication and Society. 7(1), 92–114 (2004)
21. Wu, M., Miller, R. C., and Garfinkel, S. L.: Do Security Toolbars Prevent Phishing Attacks? In: CHI 2006. 601–610 (2006)