"When I am on Wi-Fi, I am Fearless:" Privacy Concerns & Practices in Everyday Wi-Fi Use

Predrag Klasnja[1], Sunny Consolvo[2], Jaeyeon Jung[2], Benjamin M. Greenstein[2], Louis LeGrand[2], Pauline Powledge[2], & David Wetherall[2]

[1]Information School & DUB Group
University of Washington
Seattle, WA 98195, USA
klasnja@u.washington.edu

[2]Intel Research Seattle
Seattle, WA 98105, USA
[sunny.consolvo, jaeyeon.jung, benjamin.m.greenstein, louis.l.legrand, pauline.s.powledge, david.wetherall]@intel.com

ABSTRACT

Increasingly, users access online services such as email, e-commerce, and social networking sites via 802.11-based wireless networks. As they do so, they expose a range of personal information such as their names, email addresses, and ZIP codes to anyone within broadcast range of the network. This paper presents results from an exploratory study that examined how users from the general public understand Wi-Fi, what their concerns are related to Wi-Fi use, and which practices they follow to counter perceived threats. Our results reveal that while users understand the practical details of Wi-Fi use reasonably well, they lack understanding of important privacy risks. In addition, users employ incomplete protective practices which results in a false sense of security and lack of concern while on Wi-Fi. Based on our results, we outline opportunities for technology to help address these problems.

Author Keywords

Privacy, security, Wi-Fi, wireless networks, user study.

ACM Classification Keywords

H.5.2 User Interfaces; K.4.0 (Computers and Society): General; H.1.2 Software Psychology

INTRODUCTION

Hundreds of millions of people use the Web for work, to look for information, romance, connect with friends and family, shop, and bank. Applications like to-do lists and word processors, which were traditionally standalone, now have popular online counterparts that enable users to access them from anywhere. Scores of new online services, such as social networking sites, have revolutionized how people stay in touch. Facebook, for example, has over 60 million active users and 65 billion page views per month [17].

Increasingly, when people go online, they do so wirelessly. With the proliferation of 802.11-based wireless networks (Wi-Fi), people can access the Internet from offices, cafés, hotels, airports, and even laundromats. Wigle.net, an online database of user-reported wireless networks, lists over 16 million networks worldwide [1], and that is likely a small fraction of the total number of Wi-Fi networks in use.

The trend toward doing more on wireless networks, however, comes at the price of diminished privacy [2]. First, to receive service, Web sites often require the user to provide personal data such as her name, age, ZIP code, or personal preferences. Many sites share this information with advertisers and other third parties. Additionally, as a recent study found, many services transmit such personal information without encryption (i.e., "in the clear") [13]. A majority of the large Web-based email services, for example, encrypt the login process, but not the contents of email messages. Anyone along the path between the user and the service's data center could intercept this information, opening users to privacy and security risks.

Second, the broadcast nature of Wi-Fi means that anyone within range of the network can receive and potentially read transmissions intended for any other device on the network. In addition, since anyone can set up a Wi-Fi network and name it whatever she wants, this raises the possibility of malicious access points spoofing legitimate services (e.g., "T-Mobile Hotspot") which can capture all transmissions from unsuspecting users who connect to them.

Combining these factors—accessing online services over Wi-Fi—magnifies the risks. Transmissions of unencrypted personal information becomes visible to anyone within range of the network, making it much easier to track users, aggregate information over time and possibly engage in identity theft. While standard Wi-Fi security mechanisms such as WEP and WPA help, Wigle reports that less than half of the Wi-Fi networks in their database use any kind of encryption [1]. Even these security systems can be bypassed, allowing eavesdropping of users' transmissions.

CHI 2009, April 4–9, 2009, Boston, MA, USA.

Worse, there is little users can do to find out how secure their communications are and who is able to view them.

Given the prevalence of wireless hotspots and the volume of sensitive information that users transmit over Wi-Fi, it is important to understand how aware people are of the risks related to its use and what measures they have in place to protect themselves. While the literature [14,16] provides indirect evidence that the risks are not well understood, these questions have not been directly investigated.

In this paper, we report on an exploratory, multi-method four-week study that we conducted to learn what Wi-Fi users from the general public understand about Wi-Fi, their Wi-Fi-related privacy and security concerns, and the practices they have put in place to protect themselves from the risks they perceive. The results show that participants' understanding of the risks associated with Wi-Fi use is limited. Despite living in a technologically sophisticated area of the U.S., the participants were not aware that information sent over Wi-Fi could be seen by others. At the same time, the practices that the participants had adopted to protect themselves from perceived risks gave them a potentially false sense of safety. Once they clearly understood the threats, however, the participants were willing to change practices to protect themselves from risk. In this paper, we describe the study methods, highlight important results, and discuss the implications of these results. We then discuss related work and conclude.

THE EXPLORATORY STUDY

In July and August 2008, we conducted a study with 11 participants from the general public to investigate their understanding of laptop computer Wi-Fi use. In this section, we describe our study procedures, the participants' profiles, and how we analyzed the data.

Study procedures

The study consisted of three components: (1) an initial in-person session, (2) four weeks of naturalistic laptop Wi-Fi use, and (3) a final in-person session. Both in-person sessions were conducted individually with each participant. All interviews were audio recorded and transcribed.

First component: Initial in-person session

During the initial in-person session, participants completed a consent form, background questionnaire, and three diagramming tasks. They were then interviewed, received the software for the second component of the study (described below), and provided us with personal information that our software would monitor for unencrypted exposure during the study's *in situ* portion.

The background questionnaire asked about basic demographics and Internet use, such as where and how they connect to the Internet, if and where they engage in various online activities, and if they had a Wi-Fi network at home. Following methods from prior work [7,18], we used diagramming to explore participants' understanding of Wi-Fi, and in particular, to assess how well they understood the visibility of data transmitted over Wi-Fi. Participants completed three diagrams. The first two assessed their understanding of what happens when two common Internet tasks—performing a Web search and viewing a checking account balance—are performed on a public Wi-Fi network. The third diagram assessed participants' understanding of the boundaries of public Wi-Fi networks.

Finally, participants were interviewed about their typical Wi-Fi use and familiarity with Wi-Fi and networking technologies. To minimize biasing the naturalistic Wi-Fi use during the second component of the study, we limited inquiries about privacy and security concerns. Following the interview, participants provided a list of personal data—for example, usernames, email addresses, home address, ZIP code, and the last four digits of their credit cards and social security number—about which they were curious to learn if they were visible to unintended parties. We then installed the study software on the participants' own laptops, and reviewed a sample questionnaire with them of the type that would be asked during the four weeks of naturalistic use.

Second component: Four weeks of naturalistic Wi-Fi use

The second component of the study included short questionnaires and logging on the participants' laptops over four weeks of naturalistic use. As participants used their laptops, they were presented with experience sampling-style [3] questionnaires (no more than 10 per day, but usually fewer) that asked several contextual questions (e.g., where they were, what they were doing, and the importance of the task).[1] Each questionnaire took one or two minutes to complete. In addition, the study software logged details about participants' online activities and application use. In particular, it logged information about networks to which they connected (e.g., SSID, encryption type, the number of active clients), network connections made by different applications, and the applications that were actively used.

Finally, we installed HTTP Analyzer[2] to inspect whether any personal information provided by the participants was being transmitted in the clear. Specifically, we used a simple exact string matching against HTTP GET request data and HTTP POST data and logged the URL, name of the application that produced the HTTP messages, and matching label (e.g., *username*) upon finding a match.

Our contact with participants during the four weeks was limited to diagnosing and fixing any technical problems with the study software and scheduling the final session. Other than completing the questionnaires, the participants were asked to not alter their usual behavior.

---

[1] When piloting the study, we found that asking privacy-related questions biased pilot testers' naturalistic Wi-Fi use, as they became concerned about issues they had not before considered.

[2] http://www.ieinspector.com/

Third component: Final in-person session

At the end of the four weeks, participants returned to our lab for the final session. During this session, they completed a questionnaire about the sensitivity of different types of information, repeated the three diagramming tasks from the first session, completed an additional diagramming task about the boundary of their *home* Wi-Fi networks, and were interviewed about their Wi-Fi-related privacy and security concerns and practices.

The focus of the final session was the interview, during which participants were asked about any risks they thought were associated with Wi-Fi use, and what, if any, concerns they had about using Wi-Fi. We specifically asked about risks such as network snooping and malicious access points if the participants did not mention those risks on their own. Participants were asked about how they chose which Wi-Fi networks they connected to, if and how they knew the network provider, and if the provider mattered to them.

After asking about their perceived risks and concerns, we showed participants a list of the personal information they provided in the first session that was sent unencrypted during their four weeks of naturalistic use. For each piece of information, the list showed on which Web sites the information was discovered and how many times the information was detected on each site during the four weeks. After participants reviewed the list, we asked if they were aware that this information was potentially visible to others and how they felt about it.

After the interview, participants were able to revise the diagrams from the beginning of the final session based on any change in their understanding that occurred during the interview. We then gave them the "correct answers" to diagrams one and two as determined by networking experts on our team, and explained the answers to them. We also uninstalled the study software from their laptops and compensated them up to $160 USD for their participation.

Participants

Eleven Wi-Fi users (six female), aged 19 to 63 years old (mean: 40.6, median: 38.5) were recruited by a market research agency from the Seattle Metropolitan area. Potential participants who worked in or studied technology-related fields were not invited to participate. Participants used their personal Windows XP laptop[3] as their primary computer, and claimed to use Wi-Fi several times per week in at least two different locations (e.g., home, work, school, or other public places such as cafés). Participants agreed to run our logging software and answer the questionnaires with which the study software prompted them.

Participants represented a range of professions including business owner, administrative assistant, surgery scheduler, sales manager, nanny, and teacher. One participant was a college student who had a part-time job working in a retail store's warehouse and another was a Master's student who was also working as a special education teacher. Participants' highest level of education were: High School Diploma (for one), some college or a certificate (for four); a Bachelor's degree (for one), some graduate work (for two), and a Master's degree (for three).

All participants used Wi-Fi at home, 10 of whom had a home Wi-Fi network (the eleventh used open networks in her neighborhood). Nine participants had Wi-Fi at work. All had used open public Wi-Fi hotspots prior to the study.

Analysis

The results presented in this paper focus on our analysis of the interviews and diagramming tasks, as that data best addresses participants' privacy and security concerns, their understanding of privacy and security risks associated with Wi-Fi use, and strategies they employ to protect themselves from perceived risks. The interview transcripts were analyzed using open coding [20]. Diagramming tasks one and two (performing a Web search and viewing a checking account balance) were coded based on categories developed by a networking expert on our team to reveal important concepts that were clearly present in the diagrams. The categories included concepts such as *Broadcast Medium* (transmissions visible to other devices) and *End-to-End Encryption* (SSL). Diagrams three and four were analyzed based on whether the perceived range was contained to the location providing the network, the nearby surrounding area, or a much larger area. Logging data was analyzed for first order statistics (e.g., average number of Wi-Fi networks to which participants connected).

RESULTS

In this section, we briefly review how participants used Wi-Fi, and then describe their understanding of Wi-Fi, pre-existent concerns related to Wi-Fi use, practices they have adopted to mitigate perceived risks, and concerns that arose after they were presented with the list of their personal data that was sent in the clear during the study.

Overview of reported and observed Wi-Fi use

The survey and logging data indicate that the participants used a variety of applications while on Wi-Fi, and that they connected to multiple, often unencrypted networks. Consistent with previous findings [11], in their responses to the background questionnaire, participants reported using a wide range of online applications while on Wi-Fi. Our logging data confirmed these results. Table 1 shows popular online applications that the participants used during the study. We analyzed the log files and identified an application type using process names (e.g., msmsgs.exe, aim6.exe) and a Web site's URLs logged from the participant's machine. The table shows that the participants engaged in various online activities. All but one participant used Internet Explorer, four participants used Firefox

[3] Potential participants whose primary computer was a laptop provided by their employer were not invited to participate to limit our exposure to sensitive work-related information.

Application Type	Application and prevalence of use
Web-based Email	Hotmail (7), Yahoo! Mail (6), Gmail (3), webmail.psni.com (1)
Online Shopping	Amazon (8), AOL Shop (2), Walmart (1), Shopzilla (1), QVC (1)
Online Banking	Washington Mutual (2), Chase (1), ING Direct (1)
Photo Sharing	Photo Bucket (8), Flickr (4), MS Live (1), Snapfish (1)
Social Networking	MySpace (5), Facebook (5), Bebo (1)
Online Dating	Match.com (1), Eharmony.com (1)
Instant Messaging	MSN (4), AIM (2), Yahoo! Messenger (1), MySpace IM (1)

Table 1: Online application usage based on the logged data: The number in parentheses indicates the number of participants who used the service during the study.

(among whom only one exclusively used Firefox), and one participant used Flock for Web access.

During the naturalistic use component of the study, we logged that participants connected to from one to ten access points each (mean: 3.9, median: 4). Four participants never connected to an access point that used any type of encryption. Five participants connected to only one access point that used encryption. Only two participants connected to a network with WPA encryption; The other five connected to networks that used 40 bit WEP encryption.[4]

Six participants used open Wi-Fi networks when at least nine other users (or "clients") were connected to the same network. Four of those participants accessed open Wi-Fi networks while at least 45 other clients were active.

Finally, although only three participants logged online activity at five or more different networks, all of them went to their most frequently visited Web sites from nearly all networks to which they were connected. We have not found any systematic way in which participants' application and Web use varied from network to network.

Users' understanding of Wi-Fi

The interview and diagramming data suggest important subtleties in the participants' understanding of Wi-Fi. While they had a reasonably good understanding of how to use Wi-Fi, their understanding of how Wi-Fi works and the corresponding threats was very limited.

Understanding how to use Wi-Fi

Given that the participants were frequent Wi-Fi users, they had developed a sophisticated understanding of practical issues that affect their ability to use Wi-Fi, such as the network's range, signal strength, and signal propagation.

Network range. Diagrams three and four helped us assess participants' understanding of the boundaries of public and

[4] WEP is the weakest form of 802.11 encryption methods. WPA provides stronger security.

Figure 1: A participant's perceived range of a café's Wi-Fi network (the outline pointed out by the large arrow).

residential Wi-Fi networks. In diagram three, participants received a map of a shopping center which highlighted the location of a café that provided Wi-Fi. Participants were asked to draw the boundary of where they thought the range of the café's network was. The task was similar for diagram four, except that participants were given a map of either a single family home in a neighborhood or a unit in a multi-unit dwelling, depending on whether they lived in a house or an apartment/condominium.

For diagram three, all participants drew a network that extended beyond the café itself and into the shopping center. The size of the extension varied, with nine participants showing the range extending to nearby shops and the parking area around the café (Figure 1); another showed the network extending about halfway across the shopping center; and the last drew a network that extended to most of the shopping center. The diagrams suggest that the participants understood that Wi-Fi networks often extend beyond the physical boundary of the location that is providing it. We found similar results for diagram four. Here too, the drawings indicated that the network extends beyond the house or unit that provides it, to the properties and units of neighbors. Further, all three participants who lived in apartments/condominiums indicated that the network extends from side to side as well as up and down.

Signal strength and propagation. In diagram three, participants were also asked several questions about the ability to access the café's Wi-Fi network from other places within and outside of the shopping center. Their responses indicate a good understanding of how different elements such as distance and physical obstacles affect signal strength and the ability to connect to and use the network. Participants' confidence that they could connect to Wi-Fi generally went down as the distance from the café increased. For example, while 10 responded that someone would "definitely" be able to connect to the network from

the patio outside the café (one responded "probably"), nine thought that someone would "probably not" or "definitely not" be able to connect from a gas station two blocks away. Responses were mixed for the furniture store on the other side of the shopping center from the café, with six participants reasoning that the store was too far to have a usable signal. The participants' write-in rationales included: "*too far and too much interference*" {Participant 1, or "P1"}; "*outside of range*" {P8}; and "*parking lots not having obstacles aid in transmission of signal but distance is too long to allow signal use*" {P3}.

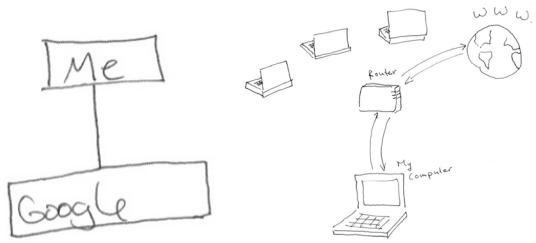
Network selection. Understanding of signal strength and propagation was closely tied to how participants chose Wi-Fi networks. Participants explained that signal strength was the main criterion they used when deciding to which Wi-Fi network to connect, preferring those with a strong signal. While a majority preferred free networks, some were willing to pay for "*a good signal*" {P2}. This group included a 19-year-old student, who previously had a subscription to T-Mobile hotspots and was willing to renew it in exchange for a *"reliable network"* {P5}. Another mentioned the frustration he experienced when he could not access email from networks with a weak signal.

Understanding how Wi-Fi works

Although they are able to connect to and use Wi-Fi effectively, the participants' understanding of how Wi-Fi and other networking technologies work was limited. Only three participants knew that *WEP* or *WPA* were types of Wi-Fi security. Even *IP address*, a fundamental networking concept, was understood by only five of the eleven participants, and then only partly. *Router* was the only term more or less correctly understood by most participants.

Diagrams one and two were used to help assess participants' understanding of what happens when common Internet tasks are performed on a public Wi-Fi network. For both diagrams, participants were instructed that they were accessing the Internet from a Wi-Fi network at a café, and that they could see at least three other café patrons using their laptops. Participants were given one scenario per diagram, (1) performing a search at *http://www.google.com* and (2) viewing their account balance at *https://bankofamerica.com*, and were asked to draw all of the people, computers, devices, and components that they thought were involved in performing these tasks. They were to highlight any that they thought may be able to see their search terms (diagram 1) or account balance (diagram 2).

The results showed that the broadcast nature of Wi-Fi and the role of SSL encryption were poorly understood. The diagrams of only four participants showed evidence of understanding that unencrypted information sent over an open network might be visible to other devices on the network (i.e., that Wi-Fi is a broadcast medium). Of these four, only one participant clearly understood that when SSL is used to secure transmissions (as when a person is accessing a Web site that uses https://), the content of those



(a) **(b)**

Figure 2: Diagram one (Web search from a café's network) for two participants with (a) no awareness of data visibility or the path that the search term takes; and (b) visibility to others implied in the diagram.

transmissions is not visible to other devices. One other participant's diagram seemed to suggest that SSL encrypted only passwords, while the diagrams of the remaining two participants from this group showed no difference between doing a Web search from Google and viewing a checking account balance from Bank of America.

Threat models

While the above analysis shows that most participants know how to use Wi-Fi, their limited understanding of the related technical aspects has consequences in the threat models that the participants have (and have not) developed of security and privacy risks related to Wi-Fi use. These threat models, in turn, have consequences for their ability to make informed decisions to protect themselves from a broader range of privacy and security risks.

Clever hackers. Participant's main pre-existing threat model was of hackers breaking into their computers to read their files and observe their desktop activities. Ten of the 11 participants considered someone breaking into their computer the main risk of using Wi-Fi. P10's explanation summarized how many participants understood this risk: "*other people can log onto your computer… and they can see what I'm seeing.*" However, the likelihood of this is generally seen as being very low, as the participants believed that hacking requires a great deal of expert knowledge. Break-ins are done by *"clever hackers"* {P1}, by *"some really high end person"* {P4}, and not by *"the average Joe Blow"* {P3}. Given that participants believe that hacking requires substantial expertise, the probability of it happening to them *"just seems unlikely"* {P5}.

Physical threats. Another common threat model, mostly related to privacy, was shared by nine participants and has to do with the physicality of using a laptop in a public place where someone could actually see their screen by looking over their shoulder. As P5 explained, "*I worry about people visually seeing over my shoulder*." The perceived risk ranges from someone seeing a sensitive email to striking up an unwanted conversation about a Web site that the participant is reading. Even if the content is not sensitive per se—a news article on CNN, for example—someone

looking over their shoulder is perceived as "*kind of weird*" {P5} and the act is seen as an invasion of privacy.

Privacy and security concerns about using Wi-Fi

Interviews revealed that participants' threat models went along with three classes of concerns about using Wi-Fi: loss of financial and personally identifiable information, impression management, and consideration for others.

Financial and personally identifiable information

The single most prevalent concern—and for several, the only concern prior to the study—was that someone could get their financial or other sensitive personally identifiable information. Credit card numbers, bank account information, and social security numbers constitute the core of this set of information. Ten participants claimed that someone stealing this information was their greatest concern about using Wi-Fi. The eleventh was unconcerned about this information because he does not perform any banking or financial transactions from his laptop. Rather, all of his family's finances are handled by his spouse. Even in his case, however, the information itself was deemed to be very sensitive. That participant is concerned about accidentally leaving his credit card at a coffee shop, and he also mentioned that he did not even put his social security number on his last job application, explaining that "*I don't generally throw that out there too easily*" {P2}. The fear of identity theft or financial damage (actually experienced by four participants) was everyone's main source of concern.

Impression management

Maintaining an image for others [9] and not being misunderstood by others based on one's online activities were concerns that influenced participants' Wi-Fi behavior. For example, one participant, a businessman who usually connects to the Wi-Fi network with the strongest signal, chose to not use a network named "Jane's Naked Lounge" which he could see from his hotel room in Las Vegas. He explained that he did not want that name in his preferred network list, because he did not want to have to explain to someone who sees it that he did not go to the lounge but rather only connected to their Wi-Fi network. Another participant does not play games or read celebrity gossip online at work, both because it would be inappropriate and because it is none of her coworkers' business to know that she reads gossip or plays games. A third participant commented that he would not want his wife to see his Web browsing history without being able to explain it for fear that she might misunderstand his behavior. Being able to control who sees what, even for those closest to the participants, was deemed important for managing how one is perceived both in professional and personal life.

Consideration for others

Not offending others or not putting them at risk by exposure to what one is doing online was another privacy concern that emerged from our analysis. One participant talked about tilting his screen in coffee shops so that other patrons do not have to see his gory online video games. "*I guess it's kind of like a courtesy thing, like I don't want people to be freaked out*" he explained {P5}. Another participant does not check certain work-related information in public places to prevent it from being seen over his shoulder and to protect confidentiality of people from whom he gets information. These anecdotes suggest that the participants sometimes keep their activities to themselves not just to protect their own privacy but also out of courtesy to others.

Practices for handling privacy and security concerns

The aforementioned concerns have resulted in participants employing a repertoire of practices that, they believe, address the risks and therefore mitigate their concerns.

Avoiding online financial transactions in public places

The participants consistently stated that they did not make online purchases or bank online from public locations such as cafés or airports unless they felt that the transaction absolutely could not wait until they got home. Seven participants claimed to use this practice routinely. For this group the main perceived threat was hacking, although two participants were just following advice from tech-savvy relatives or neighbors, without understanding the threats.

Trust in external safeguards

Some participants simply trusted that financial and commercial institutions made perfectly secure Web sites: "*I kind of trust my bank and my credit cards…when they say that this is hacker-proof, that it truly is*" {P4}. This participant looked for indications (e.g., hacker-proof seals) on the Web pages themselves, but was not familiar with more reliable indicators, such as "https://" in the URL [cf. 12]. Another participant mentioned that she assumes that her banking transactions are secure because her bank's site asks her "*secured questions*" {P8}. As suggested previously [4], such external indicators of security gave these participants what could be a false sense of safety.

Physical privacy and security

The threat of someone looking at one's screen over one's shoulder while at a public place was consistently handled by tilting or dimming the screen, or finding a seat against the wall. Nine participants did this as routine practice, both to prevent others from seeing their passwords or sensitive information, and to avoid unwanted conversations with "*weird people*" {P1}. As we mentioned, one participant also used this technique out of courtesy, so as not to expose others to the violent imagery of his video games while they are "*sitting here drinking* [their] *cappuccino*" {P5}.

Use of security software

All participants used some form of a firewall and antivirus software on their laptops. Several believed that this measure effectively protected their laptops from being hacked, alleviating their primary concern about using Wi-Fi.

These practices and beliefs seem to give participants a sense of security and to address their main privacy concerns. This might explain, at least in part, why when initially asked, the majority of participants did not think they had any concerns about using Wi-Fi. Hence, while the concerns do exist, the practices in which the participants already engage appear to mitigate them enough so that participants seldom think about their concerns. We return to this point below.

Limited understanding of risks

One consequence of participants' limited understanding of how Wi-Fi works is that it left them unaware of several risks to which they are exposed when they use Wi-Fi. In particular, two important threat models that are relevant to their privacy and security concerns were essentially absent from their awareness: malicious access points and the potential visibility of information sent in the clear.

Malicious access points

The concept of a malicious access point was something that had never occurred to most participants. All of them trusted that the names of Wi-Fi networks accurately reflected who was providing the networks. For example, a network called "Marriott Hotel" would be provided by the Marriott Corporation. Only one participant had ever been suspicious of a Wi-Fi network. In that case, the network had a similar name to his university's network. What made him suspicious was that when he connected to the network, he did not have to go through the standard university gateway Web page (it was not until he noticed the lack of the gateway that he realized the inconsistency in the name). Other participants showed no awareness that malicious Wi-Fi networks could exist. Even when asked if he thought that a network could be malicious, one participant replied that

> I just don't imagine that it's worth anybody's time to set up a phony server to send spam out to people when you're only going to collect from a couple of blocks. {P2}

The result is that the majority of participants connected to open Wi-Fi networks indiscriminately. Signal strength was the single most often mentioned criterion participants used to decide to which network to connect. The question of whose network they were connecting to and if the network might be malicious almost never arose, even for networks with names the participants did not recognize [cf. 14].

Visibility of unencrypted information

Only four participants had any idea that information transmitted over Wi-Fi could potentially be visible to other people. As we discussed above, only their diagrams showed any evidence that they understood that Wi-Fi was a broadcast medium and that others might be able to see the information that was transmitted over it.

These findings were confirmed during the final interview when participants were shown a list of their personal data that was transmitted in the clear during the *in situ* study. While four participants said that they were not surprised to learn that their information might have been visible to others, even these participants acknowledged that they "*just don't think about that*" {P5} when they use Wi-Fi. The other seven had no idea that the Web pages they visited or the email messages they read through their Gmail or Yahoo! Mail accounts, for example, could have been seen by anybody else on the network. Understanding of this risk was minimal at best, and even when some understanding existed, this understanding generally did not translate into acute awareness of risk or taking of precautionary steps when Wi-Fi was actually in use (i.e., even those who included some notion of visibility in their diagrams do not think about that visibility as they use Wi-Fi).

Lack of in-the-moment awareness of risks and concerns

Combined, the practices that gave participants a sense of security and the lack of understanding of other threats to which they expose themselves might explain why eight participants responded that they do not think about privacy and security at all when they use Wi-Fi. While they are actually using Wi-Fi, privacy and security are rarely being considered. P4 expressed it best when she explained

> If you were to ask me, 'Are you concerned that people have your bank account number and your social security, and that they know what you're doing at all times?' I would say 'Sure, I'm very concerned about that.' But…when I go into my laptop and I go into a Wi-Fi, I just go…. I am fearless. {P4}

During typical Wi-Fi use, then, it is not that security and privacy risks are considered and then found to be acceptable in relation to potential benefits of using Wi-Fi, as economic theory would suggest (see [14]); rather, such risks, at least for the participants in our study, are just not being considered. Routine practices and beliefs on the one hand, and a lack of understanding of risk on the other, provide a sense of security that often keep such considerations from coming up.

Concerns raised by personal information exposure

At the end of the exit interview, all participants were presented with a printout listing the leaks of provided personal information, sorted by information type, the Web sites where the leaks occurred, and the frequency of transmission (e.g., for P4: "*ZIP*: www.mapquest.com, 88; maps.google.com, 17;…*username*: mail.yahoo.com, 23;…*first name*: mail.yahoo.com, 4…"). The number of exposures varied by information type and by Web site, but for some pieces of information, the number of times the information was transmitted during the study was quite high. For example, participants' *ZIP codes* were sent in the clear on average 1,171 times during the study (range: 13 to 10,268), and their *names* 1,280 times (range: 5 to 3,621).

Even though four participants were not surprised to learn that some of their information might be visible to others when they use Wi-Fi, all were unsettled when faced with

the list of the transmissions of their own personal data. When confronted with this list, two new types of concern emerged: aggregated information about themselves and inadvertently broadcasting other people's information.

Information aggregation

Even participants who initially did not think that it was problematic that their ZIP codes or first names might be visible in their Wi-Fi transmissions, quickly started thinking about the potential for someone to collect such information over time when they saw this seemingly harmless information about themselves in list form. As P1 noted, while her first name or ZIP code might be okay to be visible, "*piece* [it] *all together, though, you can find out who I am*." Connecting directly to the concern for their financial and personally identifiable information, the possibility of aggregation made participants think about even those Wi-Fi activities that previously seemed harmless, such as using map services to get driving directions from their homes or using their full name as their username or email address for various online services.

Exposing other people's information

Not only were the participants concerned about exposing their own information, but seeing what they had exposed about themselves made them realize that they were inadvertently exposing information about others. For some participants, this was even more problematic. P5 explained that by using online services, he is ultimately making the choice to expose his information, even though he had not realized the extent to which he was doing this. He could thus "*deal with it*" if someone were to see his information. However, he was quite bothered by the thought that simply by reading an email he might be exposing information about his friends or family. He felt that for someone to see that information would be "*100% inappropriate*" {P5}. Not surprisingly, information about elderly parents or under-aged children was considered to be particularly sensitive.

DISCUSSION & FUTURE WORK

Our results confirm two known issues about privacy and security that also apply to online activities performed over Wi-Fi. First, the threats are important and if not properly addressed, can cause anything from mild distress to serious problems. Second, users do not generally think about these issues while they are going about their work. Rather, they employ a set-it-and-forget-it strategy, adopting practices and tools that address the threats of which they are aware and then focus on sending email, writing reports, shopping, banking, running businesses, and so on [cf. 5]. Once they think that they have addressed the threats, users seem to forget about them until something—for example, a suspicious charge on a credit card statement—makes it clear that they are not adequately protecting themselves.

Results from our study also suggest that once the threats have been made clear to users, they appear to be willing to take action to mitigate the threats. For example, after learning about which personal information of theirs had been sent in the clear during the study, nine participants said that they intend to make at least some changes to their online behavior moving forward. The intended changes included being more careful with which networks they connect to, using Wi-Fi less often, being careful which emails they open while on public networks, and not using their full names as usernames. While we cannot be certain that the participants have actually employed these changes in practice, their plans show the intent to change behavior.

There is a clear opportunity for technologies to be developed to help users mitigate these threats. Two existing research trajectories hold particular promise for future work: (1) develop tools that help improve users' awareness of these threats, and perhaps even give them control over preventing certain types of data from being sent unencrypted or to unwanted parties, and (2) develop infrastructural solutions that improve Wi-Fi protocols and devices so as to eliminate the risks of intercepting and eavesdropping on Wi-Fi communications.

End-User Awareness Tools

Based on participants' reactions, we suggest that one effective way to improve awareness about Wi-Fi risks is to show users how their own data is being broadcast as they use Wi-Fi. The participants were less concerned about the risks *until* they saw the list of their very own names, usernames, addresses, etc. and just how many times this information was visible and to whom. This suggests that reflecting this type of information back to the user as they use Wi-Fi could be an effective strategy for making them more aware about certain threats and for motivating privacy- and security-conscious behavior. In this vein, and similar to the work by Kowitz & Cranor [16], we are currently working on a tool that would provide feedback to users about their unencrypted communications and give them some control over what is and is not sent in the clear.

Not surprisingly, however, the participants did not want these concerns to be a constant focus. One participant explained, "*if you think too much about it … you're just being paranoid"* {P5}. This suggests an important design challenge, about how such awareness tools should be designed so that they make risk visible without creating paranoia or inundating users with so much information that they become desensitized to it. Over-attention to privacy and security threats can lead to overly restrictive use of technology even when risks are low.

Infrastructural Solutions

Networking researchers are actively exploring technical solutions that could improve the security of 802.11 protocols. Proposals such as SlyFi [10] aim to eliminate all unencrypted communication, obfuscating even the process of network discovery and association as well as routing and network management messages. If successful, such work will considerably mitigate privacy and security risks

currently associated with Wi-Fi use. However, for such infrastructural solutions to be effective, they need both to be incorporated into wireless standards and to become widely deployed. With millions of Wi-Fi networks in existence, it will likely be years before infrastructural solutions can truly remedy the current state of Wi-Fi security. The fact that less than half of Wi-Fi networks use even the security schemes that are currently available [1]—and have been for years—vouches to the slow rate at which infrastructural improvements become widespread.

Therefore, we believe that what is needed in the interim is a better understanding of how end users understand and deal with Wi-Fi privacy and security threats, so that solutions, such as the aforementioned end-user awareness tools, can be developed that can help individuals become more informed users of Wi-Fi networks today and in the near future. The current study and the tools that our team is developing are steps in this direction.

RELATED WORK

Three areas of related work are particularly relevant to this paper: work that shows how users expose themselves to risk when they use Wi-Fi, studies that demonstrate a lack of understanding of privacy and security with other widely deployed technologies, and work that describes principles and tools for making privacy and security issues more visible to users during their work. We discuss these in turn.

Exposing themselves to Wi-Fi risks

Recent research has shown that Wi-Fi users expose themselves to very real privacy and security risks. In a field study, Kindberg et al [14] deployed spoofed access points in two cafés: one each in Bristol and London. The networks were given a legitimate-sounding name ("Fastnet") and configured with a Web gateway that asked users connecting to the network for their mobile phone number as a part of the authentication process. To complete connecting, users had to provide a unique PIN that was sent to their mobile phone, ensuring that the provided mobile numbers were legitimate. Kindberg et al found that nearly a third (32%) of 361 users who connected to the access points completed the authentication process by providing their mobile phone number. Though the researchers do not have data that would explain why their phishing attempt was so successful, results from our study suggest that their participants may have had a similar lack of awareness about malicious access points as the participants in our study.

Lack of understanding of privacy & security risks

Like our Wi-Fi-related findings, a number of studies have shown a similar lack of understanding of privacy and security issues with other widely used technologies. Friedman et al [7] found that only half of their interview participants (N=72) correctly recognized a secure Web connection from screenshots of a browser displaying a Web site with SSL encryption. More recently, Dhamija et al [4] showed that 23% of the participants in their lab study of phishing sites (N=22) did not look at the address bar or browser security indicators such as the padlock when evaluating if a site was legitimate. These participants only looked at the content of the Web page to evaluate site authenticity (similar to P4's comment above). In another lab study, Wu et al [21] showed that users did not understand phishing toolbars, widely used tools which visually indicate that the Web site the user visited might not be legitimate. Even when using a toolbar, their participants (N=20) were successfully spoofed over a third of the time.

In a different domain, an exploratory interview study of users' understanding of RFID (N=9) by King & MacDiarmid [15] found that their participants had serious misconceptions about how RFID chips worked, not realizing that the chips could be read without any auditory or visual feedback. Results such as these suggest that even established technologies like Web browsers and phishing toolbars are often misunderstood by non-technical users, and that the misunderstandings—and the associated privacy and security risks—run even deeper for technologies such as RFID (and, as we found, Wi-Fi) where easy ways to inspect security and privacy indicators are largely missing.

Principles and tools for improving user awareness

Potentially addressing findings like those described above, Dourish et al [5] argue that security is *"essentially, an end-user problem"* and advocate for making security technologies *"highly visible"*—so the user can always inspect and understand the current security configuration. Studies of tools that increase user awareness of privacy and security implications of their current activities show the promise of this approach. In a formative lab evaluation (N=8), Friedman et al [6] found that their *Cookie-Watcher* Mozilla extension was effective in helping users better understand what cookies are and do, and in making decisions about which cookies to accept while browsing. Similarly, in a lab study (N=20), Stoll et al [19] found that their *Sesame* system allowed users to make better security decisions about allowing network connections than a traditional firewall. Gideon et al's [8] *Privacy Finder* search engine allows users to quickly see whether an e-commerce site's privacy policy matches their preferences. In a lab study (N=24), the researchers found that the visibility of this information had an effect on the participants' shopping decisions.

Most centrally relevant for this paper, Kowitz & Cranor [16] found that their public display that presented Wi-Fi users (N=11) in a campus computer lab with selected words from their transmissions made them more conscious about what they were typing even when they were not communicating sensitive information. Kowitz & Cranor suggest that increased visibility of what is going on when information is transmitted can have effects on user's decisions about how they use technology. Results from our study confirm a desire for these types of tools.

CONCLUSIONS

This paper makes two main contributions. First, to our knowledge this is the first study that examined how users from the general public understand and deal with privacy threats associated with Wi-Fi use. We found that the participants considered the threat of expert hackers breaking into computers to be the most serious. They were largely unaware of other more immediate risks, such as the visibility of unencrypted communications. The lack of awareness of such threats, combined with the existence of established but insufficient practices aimed at reducing perceived risks, led them to a false sense of security that reduced how much they thought about privacy and security while using Wi-Fi. And second, we outlined two trajectories, end-user awareness tools and infrastructural improvements, that seem to hold promise for addressing privacy and security problems with Wi-Fi use. Pursuing these trajectories could greatly improve users' ability to use Wi-Fi safely and effectively. Finally, our study combined multiple methods—interviews, diagrams and logged data—to tap into users' understanding and concerns. It was seeing the logs of personal information that they sent in the clear that made the participants truly realize the risks. Thus, we conclude that multi-method studies could greatly increase our understanding of users' privacy and security behavior as well as of the understanding that drives that behavior.

ACKNOWLEDGMENTS

We would like to thank the study participants and our friends, family, and colleagues who piloted the study software and instruments and provided support—particularly Anmol Sheth, Dan Halperin, and Keith Mosher. We also thank the reviewers for their helpful feedback.

REFERENCES

1. Anonymous. Wigle.net, http://wigle.net.

2. Cranor, L.F. 'I didn't' buy it for myself': Privacy and ecommerce personalization. In *Proc. WPES '03*, ACM Press, (2003).

3. Csikszentmihalyi, M. and Larson, R. Validity and reliability of the Experience Sampling Method. *Journal of Nervous and Mental Disease*, *175, 9*, (1987), 526-536.

4. Dhamija, R., Tygar, J.D. and Hearst, M. Why phishing works. In *Proc. CHI '06*, ACM Press, (2006).

5. 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 and Ubiquitous Computing*, *8, 6*, (2004), 391-401.

6. Friedman, B., Howe, D.C. and Felton, E. Informed consent in the Mozilla browser: Implementing value-sensitive design. In *Proc. 35th Hawaii International Conference on System Sciences*, IEEE, (2002).

7. Friedman, B., Hurley, D., Howe, D.C., Felten, E. and Nissenbaum, H. Users' conceptions of web security: a comparative study. In *Proc. CHI '02: CHI '02 extended abstracts on Human factors in computing systems*, (2002).

8. Gideon, J., Cranor, L., Egelman, S. and Acquisti, A. Power strips, prophylactics, and privacy, oh my! In *Proc. SOUPS '06*, (2006).

9. Goffman, E. *The presentation of self in everyday life*. Doubleday, Garden City, NY, 1959.

10. Greenstein, B., McCoy, D., Pang, J., Kohno, T., Seshan, S. and Wetherall, D. Improving wireless privacy with an identifier-free link layer protocol. In *Proc. MobiSys '08*, (2008).

11. Horrigan, J.B. Home broadband adoption 2008, Pew Internet & American Life Project, Washington, DC, 2008, http://www.pewinternet.org/pdfs/PIP_Broadband_2008.pdf.

12. Jensen, C., Potts, C., & Jensen, C. Privacy practices of Internet Users: Self-report versus observed behavior. *IJHCS, 63, 1-2*, (2005).

13. Jung, J., Sheth, A., Greenstein, B., Wetherall, D., Maganis, G. and Kohno, T. Privacy oracle: A system for finding application leaks using black-box differential testing. In *Proc. CCS 2008*, ACM Press, (2008).

14. Kindberg, T., O'Neill, E., Bevan, C., Kostakos, V., Fraser, D.S. and Jay, T. Measuring trust in Wi-Fi hotspots. In *Proc. CHI '08*, ACM Press, (2008).

15. King, J. and McDiarmid, A. Where's the beep? Security, privacy, and user misunderstandings of RFID. In *Proc. Usenix*, (2008).

16. Kowitz, B. and Cranor, L. Peripheral privacy notifications for wireless networks. In *Proc. WPES '05*, ACM Press, (2005).

17. Owyang, J. Social network stats: Facebook, MySpace reunion (Jan, 2008), 2008, http://tinyurl.com/ywnsgv.

18. Poole, E.S., Chetty, M., Grinter, R.E. and Edwards, W.K. More than meets the eye: transforming the user experience of home network management. In *Proc. DIS '08*, ACM Press, (2008).

19. Stoll, J., Tashman, C.S., Edwards, W.K. and Spafford, K. Sesame: Informing user security decisions with system visualization. In *Proc. CHI 2008*, ACM Press, (2008).

20. Strauss, A. and Corbin, J. *Basics of qualitative research: Techniques and procedures for developing grounded theory*. SAGE, Thousand Oaks, 1998.

21. Wu, M., Miller, R.C. and Garfinkel, S.L. Do security toolbars actually prevent phishing attacks? In *Proc. CHI '06*, ACM Press, (2006).