Design and Evaluation Method for Secure 802.11 Network Configuration

Cynthia Kuo
Carnegie Mellon University
129 Baker Hall
Pittsburgh, PA 15213
cykuo@andrew.cmu.edu

Vincent Goh
Carnegie Mellon University
Pittsburgh, PA 15213
vgoh@andrew.cmu.edu

Adrian Tang
Carnegie Mellon University
Pittsburgh, PA 15213
bct@andrew.cmu.edu

1. INTRODUCTION

We examine how home users conceptualize wireless technologies; what they perceive to be the security issues in 802.11 networks; their level of concern about these issues; and their ability to successfully configure a secure wireless network. To show that vendors could do better without incurring major costs, we develop a configuration interface that helps users articulate and implement a security policy using existing tools and technology. We test this prototype against the two best-selling access points. In addition, we propose a methodology for assessing security interfaces. Traditional techniques for interface evaluation focus on one aspect of the user experience; we integrate several techniques to provide insight into which aspects are problematic for users.

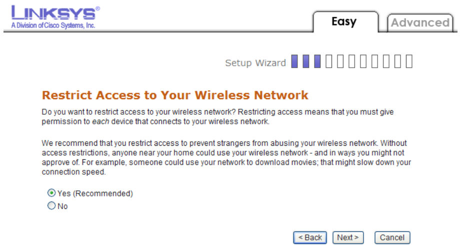
2. PROTOTYPE DESIGN

We implemented a prototype on a Linksys WRT54G. The prototype attempts to elicit a user's goals and values by asking general questions. It automatically maps these preferences to their technical features. This produces a recommended configuration for the user, which can be changed if desired. If the user's preferences produce a set of feature settings that conflict with one another, the wizard asks the user to resolve the conflict. The wizard only asks for information that needs to be input by a person. Any decisions that can be automated are automated.

3. EVALUATION METHODOLOGY

3.1 Target Population

Our study population consisted of the target market for 802.11 home networks. We defined the likely consumer as someone who: (1) uses wireless Internet access at home, school, or work place on a daily basis (5+ days per week); (2) has broadband access at home; and (3) uses a laptop as his primary computer. We included individuals who already had wireless networks at home, as well as individuals who did not.



Restrict Access to Your Wireless Network

Do you want to restrict access to your wireless network? Restricting access means that you must give permission to *each* device that connects to your wireless network.

We recommend that you restrict access to prevent strangers from abusing your wireless network. Without access restrictions, anyone near your home could use your wireless network - and in ways you might not approve of. For example, someone could use your network to download movies; that might slow down your connection speed.

● Yes (Recommended)
○ No

Figure 1: Access Restriction Wizard Screen

3.2 Tasks

We defined the ideal secure wireless network as one where the consumer has: (1) changed the default password; (2) changed the SSID; (3) generated or entered an encryption key on the access point; (4) entered the encryption key on a client; and (5) enabled MAC filtering.

3.3 Study Setup

Eighteen participants were randomly assigned an access point: the Linksys WRT54G, the Netgear WGT624, or the prototype (see Table 1).

Access Point	Low Expertise	High Expertise
Linksys WRT54G	3	3
Netgear WGT624	3	3
Prototype	3	3

Table 1: Participant Assignment

3.4 Evaluation Goal and Method

The Conceptualization-Attitude-Performance (CAP) evaluation method combines elements from different methodologies: mental models interviews, surveys, usability studies, and contextual inquiry. It is comprised of five sections (see Table 2). As much as possible, the experiment was designed so that participants would not realize that the focus of the study is security until they reached the tasks.

Section	Time	Purpose
Interview	25 minutes	Understand where participants use wireless Internet access, their attitudes towards unsecured wireless networks, and to what extent they understand that their data is being broadcasted.
Questionnaire	5 minutes	Gather participants' attitudes towards various aspects of wireless networks: availability, reliability, ease of use, use of open wireless networks, security, privacy, and health.
Tasks	45 minutes	Observe participants during wireless network setup. Ask participant to configure network as they would at home. Wait until participant declares that setup is finished, and then follow up with security-related questions. If participants have not set up basic wireless connectivity by 20 minutes, the experimenter steps in, setting up a wireless connection and asking the participant to continue.
Questionnaire	5 minutes	Repeat questionnaire. Used to measure within-subject changes in attitude.
Debriefing	10 minutes	Follow up with any remaining questions.

Table 2: Design of CAP Evaluation Method

4. RESULTS

We discovered that participants understood wireless technologies and the security threats posed by 802.11 networks fairly well. We also found that awareness of a security issue does not necessarily equate to higher levels of concern; this may be influenced by participants' value judgments. Last, we compared the performance of our prototype against that of the Netgear and Linksys products. Below, we show that low expertise users are able to configure fewer security features than high expertise users on commercial access points. This difference does not exist for our prototype. Furthermore, low expertise participants attempt to configure fewer features on commercial access points, and those use our prototype experience a positive change in attitude towards the ease of use of wireless networks.

A two-way Analysis of Variance (ANOVA) was used to test for group-mean differences in the number of tasks that participants completed. The effect of expertise level depended on the access point assigned, and vice versa. This effect was significant at the 10% significance level, $F(2, 12) = 3.15$, $p = .08$. The results are shown in Figure 2. Vertical bars represent the standard error of the mean.

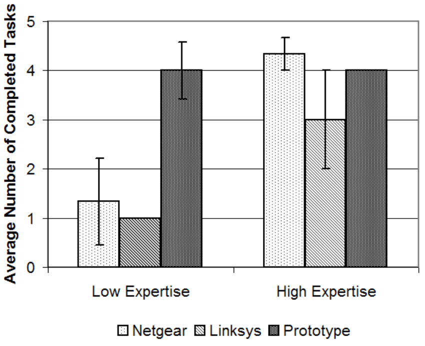


Figure 2: Average Number of Completed Tasks

Low expertise users completed fewer tasks than high expertise users on the commercial access points, $t(12) = 4.11$, $p = .001$. This difference did not exist for the prototype users. In addition, all prototype users performed as well as the high expertise users on the commercial access points. Low expertise users completed 2.8 more tasks on the prototype than with the commercial access points, $t(12) = 3.80$, $p = .003$. There was no significant difference for high expertise users, $t(12) = .45$, $p = .663$.

5. CONCLUSIONS

Many users have difficulty configuring secure wireless networks with today's 802.11 access points. We develop a configuration interface that helps users articulate and implement a security policy. To evaluate our prototype design, we developed a methodology based on several traditional human-computer interaction techniques. The method attempts to measure how well users understand the concept of wireless broadcasting, what they know about wireless security threats, how much they care about these security threats, and whether they are able to successfully protect themselves from these threats. Our results show that participants have a fairly good understanding of wireless technologies and security threats. However, users have difficulty translating this knowledge into security policies and implementing these policies in the configuration interfaces of today's access points. We show that low expertise users attempt to configure fewer features than high expertise users. Even if we prompt them to configure these features, low expertise users are also less able to succeed than high expertise users. Our prototype design removes this expertise barrier by eliciting users' values and automating their translation into policy and mechanism. Thus, our prototype encourages low expertise users to attempt as many changes as high expertise users, and enables them to accomplish as much as their high expertise counterparts. Finally, we show that better security can be achieved without developing new technology. We can dramatically improve the accessibility of security technologies by designing interfaces with the user in mind.

6. ADDITIONAL AUTHORS

Adrian Perrig (Carnegie Mellon University, email: `adrian@ece.cmu.edu`) and Jesse Walker (Intel Corporation, email: `jesse.walker@intel.com`)