USEable Security: Interface Design Strategies for Improving Security

Amanda L. Stephano
Indiana University
Amanda.Stephano@gmail.com

Dennis P. Groth
Indiana University
901 East Tenth Street
dgroth@indiana.edu

ABSTRACT
As people start depending more on technology and the internet they are opening themselves up to new risks. In this project, we specifically investigated wireless router interfaces to understand the needs of users when they configure security. Two studies were conducted: a baseline study comparing the interfaces of two routers on the market and a study comparing a prototype and the Linksys interface. The baseline study showed that there was no difference between the current interfaces. We then conducted a controlled experiment with a prototype that gave visual feedback. The prototype showed significant improvement in level of security achieved.

Categories and Subject Descriptors: H5.m. Information interfaces and presentation (e.g., HCI): Miscellaneous.

General Terms: Human Factors, Security

Keywords: Security, evaluation, visual interfaces, usability

INTRODUCTION
Computers and technology are becoming more prevalent these days, particularly in the average home. Along with the increase in the use of technology there is also a rise in the amount of people using the internet. Unfortunately, this also means that there are many people that are not secured when using their computer and connecting to the internet. There are several different aspects of security to consider, including physical security, information security, and then network security when using the internet. This makes computer security very complex for people [1]. This is one of the reasons why people do not bother trying to secure their computer. Another reason people do not secure their computers is simply that people do not understand fundamentally how computers work. If they do not know how it works how can they secure it? Finally, people just want to get their work done using their computer. Security is secondary to completing their tasks and usually not very important to them [5].

VizSEC'06, November 3, 2006, Alexandria, Virginia, USA.

In our investigation we decided to focus on the setup interfaces for wireless routers. This is because wireless networks are very prevalent not only in businesses, but also in the average home. Hence, a wide variety of people need to be able to set them up and secure them. A study done by Sandvig and Shah showed that, on average, 75% of wireless networks are not secured [7]. People that are not securing their networks are exposing themselves to the following risks:

- Reduced bandwidth
- Stolen Files
- Network used for illegal activities
- Locked out from own router

In most cases, people will not notice these things happening. The average person will not typically understand how fast their network is and how fast it should be. Also, in the case of stolen files, they are usually not actually stolen, just copied; so there is no way to know that something has actually been stolen. Furthermore, it is hard to detect other traffic on a network unless a person specifically knows what programs to use and how to monitor their network.

Why do people leave their routers unsecured? Most routers come with default settings that do not need to be changed for the router to work. Consequently, users may simply plug the router in and leave all of the defaults. Once again, the user just wants it to work, security is secondary. This shows that the problem is not only with the technology, but with the human factor. Therefore, we need to design the configuration tool so that the user can be aware of security levels while still being able to configure the router properly. This is where Human Computer Interaction (HCI) can help. HCI has been applied to other areas of security including securing email. Whitten and Tygar did a study on an application, PGP 5.0, to see if its interface was usable or not [8]. Garfinkel followed up this Whitten and Tygar's study with a more comprehensive study on secure email usability [4]. A lot of HCI research has also been conducted in the area of authentication which includes trying to find ways to create more secure passwords. Yan, Blackwell, Anderson, and Grant have done studies to determine how to get the

user to generate more secure passwords [9]. Other studies have been conducted in the area of mitigating error when using interfaces to setup of security. A study was done by Maxion and Reeder in attempt to mitigate human error by using a certain design principle called external subgoal support [6].

There have been previous studies conducted in the area of wireless networking security. Guo, Koh, and Tang from Carnegie Melon University conducted a study comparing the interfaces of a Linksys router, a Netgear Router, and a prototype they created. They had six users per router, three technical and three non-technical, try to set them up using the given interface. They measured success by the number of tasks they were able to complete using each interface. Their study showed that the participants were not able to complete as many tasks with the Linksys and Netgear routers as they were with the prototype [3].

Another study that was conducted in both Illinois and California sought to find out how secure wireless networks were out in the wild. In California, they found that 50% of routers they encountered had left all of the default settings on the router, meaning they were not secure at all. 25% of the networks they surveyed had only changed the administrative password. This study shows that 75% of the networks they found were not secured and could be used by anyone [6].

In this paper we discuss a comprehensive evaluation that was performed using current wireless router interfaces and a prototype we developed. We performed an initial baseline study to compare two of the market leaders in wireless networking, Linksys and DLink. Based on the results of that study we then developed a prototype modeled after the original Linksys interface and conducted another user study. Both studies followed the same general form and procedure. After we conducted the study with the prototype we were able to compare those results with the results from the study conducted with the original Linksys interface. Finally, we discuss our conclusions from the studies and explain the future work that could be done in the area.

BASELINE STUDY

To better understand user needs we performed an initial baseline study to see how effective the current setup interfaces of wireless routers are. We chose two of the market leaders in wireless networking to test: Linksys and DLink.

Study Demographics

There were 21 participants in the study: 10 for the Linksys and 11 for the DLink. The number of users for the DLink was slightly larger to attain an equal number of women participants in each group. Each group had 5 women. Each group had 2 highly technical people, according to their field of study or career. We recorded each participant's age and average time per day that they spent working on a computer. Ages of participants ranged from 18-47. For the Linksys router the average computer usage was 3.65 hours per day. The average computer usage for DLink router was 7.6 hours per day.

Figure 1 - Screenshot of DLink Interface

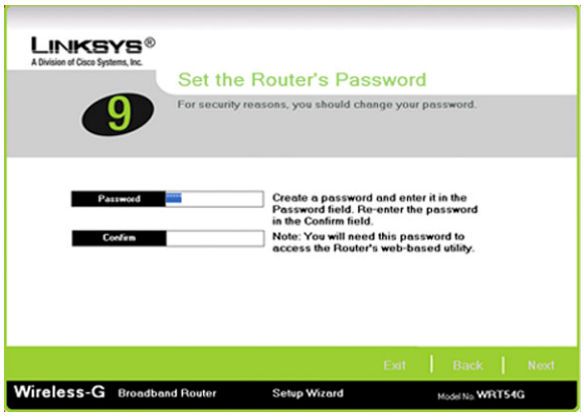

Figure 2- Screenshot of the Linksys Interface

Study Procedure

The users were provided with the router in the box with all of the materials that are included with it. All users used the same computer for the procedure, an IBM T40 Laptop Computer running Microsoft Windows XP. The specific user task was to set up the router like they would for their own home. During the experiment we observed the users, but did not offer assistance for completing the task. After they finished setting up the router, the users completed a post-experiment survey. The survey is based on the Questionnaire for User Interface Satisfaction (QUIS) [2] and is broken up into 6 different parts: Security, System Capabilities, Learning, Overall Reaction, Screen, and Terminology and System Information. Users were asked to rate items on a scale from 1 to 10 based on their experience. Afterwards, the users were asked a handful of open-ended questions. Specifically, the follow-up questions included asking why or why not the user did certain things while they were setting up and if they understood exactly what the different tasks were.

During the study, we measured achievement of the following four security tasks:

1) Changing the default administrative password
   - Allows the user to change the router settings.
2) Changing the default name of the network (SSID)
   - Uniquely identifies the network so that computers can connect by name.
3) Enabling Encryption
   - Allows access to the network with a specific key, which is like a password. It also disguises any data that is sent across the network so that information is not legible.
4) Enabling MAC Address Filtering
   - Allows only specific computers to access networks by using their MAC Address to uniquely identify them.

The security level the user was able to attain is based on how many of the four tasks that were successfully completed. For the purposes of the study we created the following ordered taxonomy of security levels:

Level 0 (weakest):

1) Default values not changed, security not enabled, or
2) Only the default SSID changed, or
3) Only MAC Address Filtering enabled.

Level 1:

1) Only the default admin password changed, or
2) The default admin password and the default SSID changed, or
3) MAC Address filtering has been enabled and the default SSID has been changed.

Level 2:

1) The default admin password has been changed and MAC address filtering has been enabled, or
2) The default SSID has been changed and Encryption is enabled.

Level 3:

1) MAC Address Filtering and Encryption have been enabled, or
2) The default admin password and SSID have been changed and MAC Address Filtering has been enabled, or
3) The default admin password and SSID have been changed and Encryption has been enabled, or
4) The default SSID has been changed and MAC Address Filtering and Encryption have been enabled.

Level 4 (strongest):

1) The default admin password has been changed and MAC Address Filtering and Encryption have been enabled, or
2) The default admin password and SSID have been changed and both MAC Address Filtering and Encryption have been enabled.

In summary, the dependent variables for the study were:

1) Time to complete set up of router.
2) Security level achieved during set up of router.
3) Subjective ratings of security and interface.

The independent variables for the study were:

1) Type of router.
2) Gender.
3) Technical experience level.

Quantitative Results

Objective Results

Our results show that there is no significant difference between the two routers for the amount of time it takes to set up. The average time for the DLink router was 14.9 minutes, whereas the Linksys router took 17.2 minutes on average. See Table 1 for details of the results.

	Mean DLink	**Mean Linksys**	**P**
Time to Setup Router - all	14.9	17.2	0.34
Time to Setup Router - Women	16.2	16	0.95
Time to Setup Router -Men	13.4	18.4	0.27
Time to Setup Router - Technical	13.5	16.5	0.59
Time to Setup Router – Non-Technical	15.2	17.8	0.45
Security Level Achieved - all	1.3	1.4	0.76
Security Level Achieved - Women	1.2	1.3	0.52
Security Level Achieved – Men	1.4	1.3	0.72
Security Level Achieved – Technical	3.0	2.0	0.43
Security Level Achieved – Non Technical	0.9	1.3	0.28

Table 1 - Security level achieved (0-3) and time (in minutes) to setup router for both the DLink and Linksys routers.

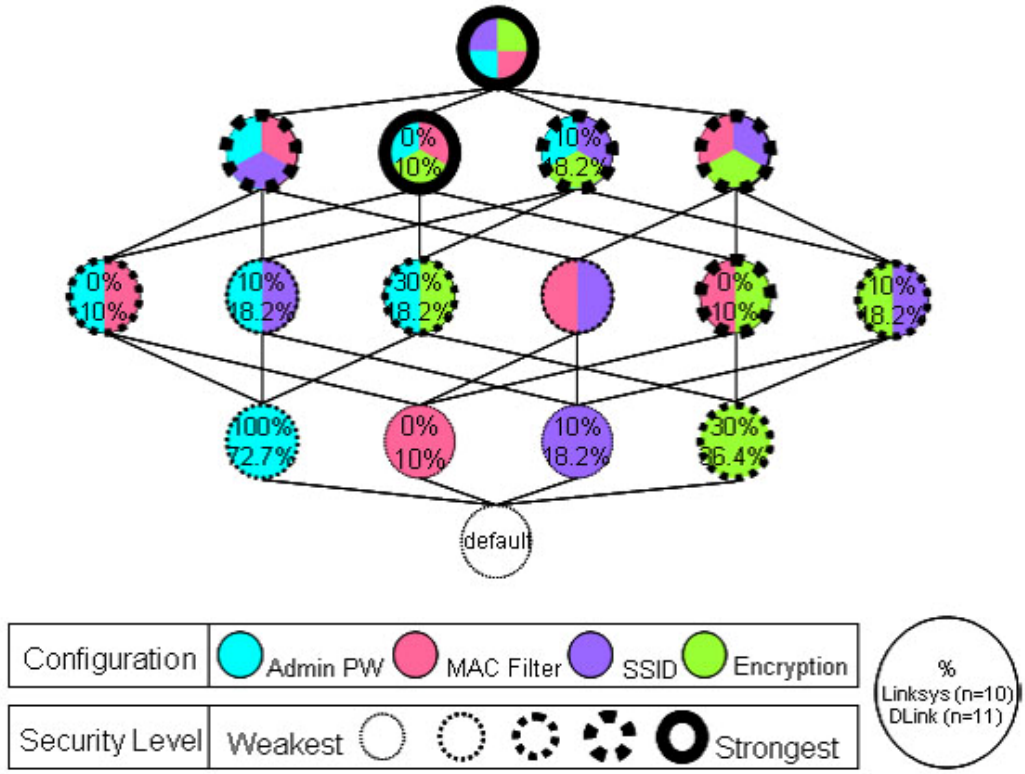

Figure 3 – Visual representation of security level results. The lattice represents the possible permutations of the security settings. The edge style for each node is an interpretation of the strength of the settings. Within each node is the percent of users that achieved that particular level of security.

Once again there was no significant difference between the security levels reached by users when they were setting up the different routers. Participants setting up the DLink router on average reached a security level of 1.3 and participants setting up the Linksys router achieved a security level of 1.4 (see Table 1). By looking at Figure 3, you can see that most users only achieved a security level of 1. The figure also shows that only 10% of the DLink users were able to achieve a level 4. The highest level Linksys users were able to achieve was 3. One reason why several of the DLink users did not change the admin password was because it appeared to be filled in already, so the users assumed they did not need to change it.

Subjective Results

Tables 2–7 show the questionnaire results. Like the quantitative results, the survey results show that there was no significant difference in opinion about the interface. Participants generally felt the same about both. For example, on average participants for the DLink router gave it a 6.5 for how easy it was to learn how to set up the system. The participants that used the Linksys router gave it a 6.6 on average for that category.

Security	**Mean DLink**	**Mean Linksys**	**P**
After setting up the router, do you feel your network is: not secure/very secure	6.2	6.6	0.60
Setting up security options: difficult/easy	5.5	5.7	0.79

Table 2 –Survey - Security (Max = 10)

System Capabilities	**Mean Dlink**	**Mean Linksys**	**P**
Correcting your mistakes: difficult/easy	5.9	5.5	0.70
Experienced and inexperienced users' needs are taken into consideration: never/always	5.1	5.7	0.62

Table 3 – Survey - System Capabilities (Max = 10)

Learning	Mean DLink	Mean Linksys	p
Learning to set up the system: difficult/easy	6.5	6.6	0.85
Tasks can be performed in a straight-forward manner :never/always	7.0	6.6	0.61
Help messages on screen: unhelpful/helpful	6.9	6.2	0.47
Supplemental reference materials: confusing/clear	6.6	6.2	0.60

Table 4 – Survey - Learning Results (Max = 10)

Overall Reaction	Mean DLink	Mean Linksys	p
Terrible/Wonderful	6.4	5.8	0.45
Difficult/Easy	6.5	6.1	0.65
Inadequate/Adequate Power	5.6	4.8	0.33
Frustrating/Satisfying	6.5	6.7	0.84
Dull/Stimulating	4.7	5.4	0.48
Rigid/ Flexible	5.1	5.5	0.69

Table 5 – Survey - Overall Reaction Results (Max = 10)

Screen	Mean DLink	Mean Linksys	P
Characters on the computer screen: hard/easy to read	7.9	7.5	0.62
Organization of information on screen: confusing/very clear	7.5	6.4	0.19
Sequence of screens: confusing/very clear	7.8	7.6	0.77

Table 6 – Survey - Screen Results (Max = 10)

Terminology and System Information	Mean DLink	Mean Linksys	P
Use of terms throughout the system: inconsistent/consistent	7.4	7.3	0.92
Computer terminology is related to the task you are doing: never/always	7.3	7.9	0.32
Position of messages on screen: inconsistent consistent	7.3	6.4	0.28
Messages on screen which prompt user for input: confusing/clear	7.6	5.7	0.04
Computer keeps you informed about what it is doing: never/always	6.5	6.3	0.80
Error messages: unhelpful/helpful	6.9	5.2	0.15

Table 7 – Survey - Terminology and Information (Max = 10)

The only significant difference in opinion about the two routers was how the users felt about the messages on screen prompting for input. The participants that setup the DLink router gave it on average a 7.6 for that category, whereas on average the users that setup of the Linksys router gave it a 5.7. The t-test result for the particular question had a p-value of 0.04 (see Table 7). There was no significant difference in subjective evaluation based on gender, or level of technical experience.

Observations

There are a few interesting observations that were made during the studies about both setup interfaces. Along with an online wizard, the DLink router came with a paper-based setup manual that guides users through the process. The participants found the manual to be a helpful reference. However, the screenshots of the different configuration screens showed all of the setting being left as default, so a lot of users inferred that this meant they should be left as default and hence did not change the settings at all. The Linksys router did not come with a supplemental paper-based manual. It only came with a CD that had a setup wizard. A lot of users actually looked for a paper manual when they were setting up the Linksys router and had some confusion. Users also took some of the diagrams in the Linksys interface literally which was a problem. Even though they knew they were setting the network up for a laptop they would around the testing room for a desktop computer since that is what the diagram showed.

Study Conclusions

The quantitative results show that the amount of time to setup both routers is roughly equivalent and the security level achieved is quite low on average, which indicates that the routers would not be secured. Based on these results we generated the following questions that need to be answered when designing a interface for setting up security:

- What level of support do users need?
- Can the interface have an effect on performance?
- How can an interface both educate and inform users about security?

PROTOTYPE STUDY

The prototype study was setup up in exactly the same way as the baseline study was. We developed a prototype interface based on the Linksys interface to see if we could improve the level of security the user could achieve, shorten the amount of time it takes to setup a router, and to make the interface overall more usable and enjoyable. We then compared the test results to the ones that we originally got when we had the users setup the Linksys router in the baseline study.

Prototype Interface

We developed the prototype using the basic look of the Linksys interface and even used some of the same initial router setup screens. We altered the Linksys security configuration screens, however, to provide more feedback and information to the user. Specifically, we added a visual feedback bar at the bottom of the screen to let the user know what tasks they had completed and how secure they were. We also added a secondary form of feedback to the

administrative password screen (see Figure 4). We included MAC-filtering within the setup process, rather than an alternate advanced setting. Our design goal was to influence security by providing an informative display, which simply gave visual feedback on the security strength.

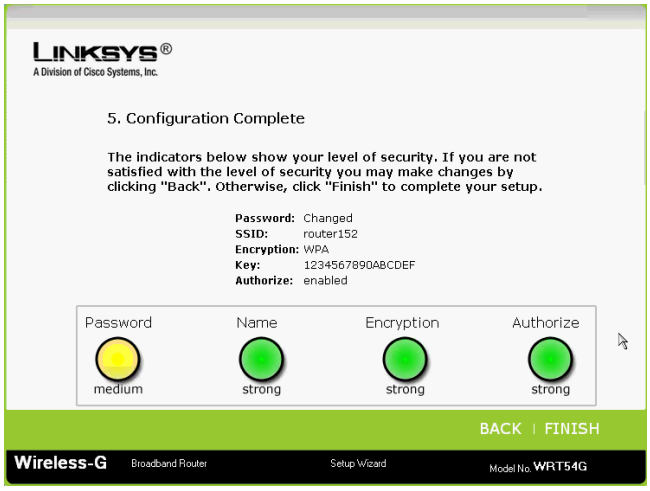

Figure 4 - Screenshot of Prototype

Study Demographics

Like the previous study, we had 10 participants test the prototype interface. Of the 10 people, 2 were technical and 8 were non-technical. Once again, by technical we mean that their area of study or career is technical. We also once again controlled participants by gendering, testing 5 men and 5 women on the prototype interface. Ages of the participants ranged from 19-25. The average computer usage of participants was 6.1 hours per day.

Study Procedure

For the prototype study we replicated the baseline study by giving the user the box with the Linksys router, but this time we had them use the prototype interface instead of the interface that comes with the router. Once again, they setup up the router using an IBM T40 Thinkpad laptop. We also specifically asked users to configure the router like they would for their own home. After the participants completed setting up the router they filled out the questionnaire and answered the same follow-up questions. We asked them questions like why or why not they did a particular task and if they found the feedback helpful.

In summary, the dependent variables for the study were:

1) Time to complete set up of router.
2) Security level achieved during set up of router.
3) Subjective ratings of security and interface.

The independent variables for the study were:

1) Type of router.
2) Gender.
3) Technical experience level.

Quantitative Results

Objective Results

The quantitative results from the study show that there is a significant difference between the prototype interface and the Linksys interface.

On average, the participants were able to complete the setup using the prototype interface in 6.1 minutes. This is a lot faster than the average amount of time it took to setup the Linksys router which was 17.2 minutes. By performing a t-test on the data we got a p-value of 0.0002 which means that it is highly significant difference between the two routers (see Table 8).

	Mean Prototype	Mean Linksys	P
Time to Setup Router	6.1	17.2	0.0002
Time to Setup Router – Women	7.4	16.2	0.012
Time to Setup Router – Men	4.8	20.0	0.012
Time to Setup Router – Technical	5.5	16.5	0.14
Time to Setup Router – Non-Technical	6.3	17.8	0.002
Security Level Achieved	3.3	1.4	0.0001
Security Level – Women	3.6	1.6	0.003
Security Level – Men	3.0	1.2	0.015
Security Level – Technical	3.5	1.5	0.32
Security Level – Non-Technical	3.3	1.2	0.0002

Table 8 – A comparison between the Prototype and the Linksys Interface.

The level of security attained also increased for the Prototype interface. On average, participants were able to achieve a security level of a 3.3. This is much better than the average security level achieved for the Linksys which was 1.4. By performing a t-test we showed that this result is highly significant since we have a p-value of 0.001 (see Table 8).

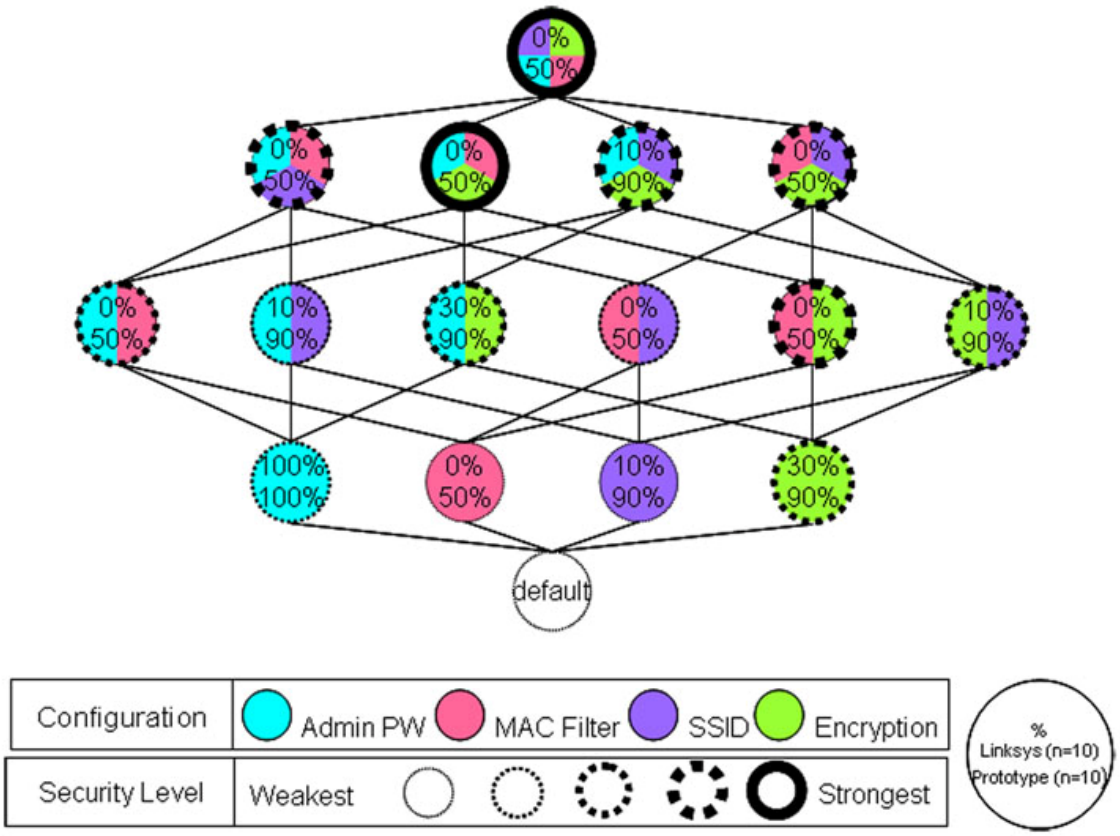

Figure 5 - Visual Representation of Security Level Results for the Prototype. The lattice represents the possible permutations of the security settings. The edge style for each node is an interpretation of the strength of the settings. Within each node is the percent of users that achieved that particular level of security.

Subjective Results

Like the objective results, the subjective results also show a significant difference between the Prototype interface and the Linksys interface. We once again gathered survey data using the QUIS. Due to space constraints, we only show results that had a significant difference are shown in Tables 9 and 10.

Overall Reaction	**Mean Prototype**	**Mean Linksys**	**p**
Terrible/Wonderful	7.4	5.8	0.034
Difficult/Easy	8	6.1	0.015
Inadequate/Adequate Power	7.8	4.8	0.005
Frustrating/Satisfying	7.9	6.7	0.05
Dull/Stimulating	5.9	5.4	0.62
Rigid/ Flexible	5.7	5.5	0.86

Table 9 – A comparison of the questionnaire results for the Prototype and Linksys interfaces for the Overall Reaction category.

In the Overall Reaction category, there was a significant difference between participants opinion of the interface overall (see Table 9). Participants seemed to like the interface more, found it easier, and more satisfying to use. We used a t-test on the data to determine its significance and all of the differences were all significant.

The Learning category also showed a difference between the interfaces. Users felt that Prototype was easier to set up than the Linksys interface. We once again performed a t-test on the data to determine if the difference was significant and we got a p-value of .003 which means that the difference was indeed significant (see Table 10).

Learning	**Mean Prototype**	**Mean Linksys**	**p**
Learning to set up the system: difficult/easy	8.3	6.6	0.003
Tasks can be performed in a straight-forward manner: never/always	8.1	6.6	0.06
Help messages on screen: unhelpful/helpful	7.8	6.2	0.12
Supplemental reference materials: confusing/clear	7.7	6.2	0.14

Table 10 – A comparison of the survey results for the Prototype and Linksys interfaces for the Learning category.

Observations

In most cases, users would use the visual feedback mechanism to see how secure they were. In fact users would actually go back and change settings after seeing that the indicator showed that the security level for a particular task was weak or medium. This was very different behavior from participants who used the Linksys and DLink interfaces. They would rarely go back and make changes to the settings. It also seemed that in most cases, the feedback gave people an idea of what affected the security level for a particular task, even if they did not exactly understand what that setting did for them.

CONCLUSION AND FUTURE WORK

The initial study that we conducted showed how lacking current security setup interfaces for Wireless Routers are. They do not give the user any idea of how secure they are nor do they really explain what the different security options are. We tried to address one of these issues by developing a prototype which involved adding a feedback mechanism to it. Our results show that adding a feedback mechanism to the interface greatly improved the level of security the user was able to achieve. Even if the user did not quite understand what each security option was, they had an idea of how secure they were and they could easily go back and change their level of security. Both our objective and subjective results support this conclusion. The average time it took to setup the router was significantly decreased for the prototype interface and they were able to achieve a much higher level of security using it. Although the prototype is instructive in uncovering some of the possibilities that more effective interface design principles may provide, two specific questions remain open: **Why are users so much faster with such similar interfaces? Given the enhanced feedback mechanism, why did users not feel more secure?**

These studies were really just the beginning of a great deal of research that could be done in this area. In our study, we only tried one type of feedback for the user. There are many different variations of feedback that can be tested including real time feedback. Also, placement of the feedback mechanism and the type of indicator might also be important as well. Another area that one could pursue would be the addition of a wizard to give the user more thorough information. Our interface did not give the user a detailed explanation of each security option and it did not walk them through each task. It only gave them an idea of how secure each option made them. This type of interface would be more helpful for the technically inexperienced user, whereas our Prototype interface could be used by both technical and non-technical users. Enabling encryption and MAC address filtering were the most difficult tasks for inexperienced users and it would probably help a lot to have a walkthrough for them. An alternative style of interface based on objective setting might also be interesting. Such an interface might ask the user how secure they would prefer their network to be and then guide them accordingly. This technique would seek to better match the outcomes of the configuration with the goals of the user.

ACKNOWLEDGMENTS

We would like to thank Mark Christensen, Kristy Streefkerk, and Ryan Varick for their help. Also, we would like to thank all of the participants in our studies.

REFERENCES

1. Bishop, M. “Psychological Acceptability Revisited”, in Security and Usability edited by Cranor, L.F., Garfinkel, S., 2005, pg 1-11.
2. Chin, J. P., Diehl, V., A, Norman, K. “Developing of an Instrument Measuring User Satisfaction of the Human Computer Interface”, Proceedings of ACM CHI 1988, pp. 213-218, 1988.
3. Guo, C., Koh, V., Tang, A. “Design and Evaluation for Secure 802.11 Network Configuration”, SOUPS, 2005.
4. Garfinkel, S, Miller, R. “Johnny 2: A User Test of Key Continuity Management with S/MIME and Outlook Express”, SOUPS, 2005.
5. Karat, C., Brodie, Karat, J. “Usability Design and Evaluation for Privacy and Security Solutions”, in *Security and Usability* edited by Cranor, L.F., Garfinkel, S., 2005, pg 47-73.
6. Maxion, R., Reeder, R. “User-Interface Dependability Through Mitigation of Human Error” Int. J. Hum.-Comput. Stud. 63, 1-2, July 2005, pg 25-50.
7. Sandvig, C., Shah, C. “Software Defaults as De Facto Regulation: The Case of Wireless APs”, in Proceedings of the 33rd Telecommunications Policy Research Conference (TPRC) on Communication, Information, and Internet Policy, Arlington, Virginia, USA, 2005.
8. Whitten, A., Tygar, J.D. “Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0”, in Proceedings of the 8th USENIX Security Symposium, August 1999.
9. Yan, J, Blackwell, A., Anderson, R., Grant, A. “The Memorability and Security of Passwords”, in Security and Usabilty edited by Cranor, L.F., Garfinkel, S., 2005, pg 129 -1.