UNIVERSITY OF OSLO
Department of Informatics

Wireless Security and User Attitude in SOHO environments

Master thesis

Ugo Santucci
Oslo University College
Norway

May 24, 2006

Abstract

Wireless telecommunications networks have been one of the outstanding success stories over the last decade or so. Wireless Local Area Networks (WLANs) are reaching the same success in a very short time.[1] Corporate and home users are avoiding the expenses and delays associated with installing wired networks.Many factors have contributed to their popularity and success, the low cost of wireless equipment, and the portability they offer. WLAN provides great mobility and flexibility but it also poses security risks that must not be overlooked.[2] The evolution of the wireless market has involved a growing attention towards security issues in wireless networks, both home networks and public networks.This is the reason why numerous novice users start to use such wireless technologies. However, the great majority of users is unaware of the real security issues.

At the time of writing there is no recorded study of user attitude and knowledge about securing wireless SOHO (Small Office/Home Office) environments. This study has the goal to feel this gap through a quantitative and qualitative study.

The author has been studying the difficulties and the problems novice users' computer have in installing , configuring and understanding the overall security policy of a Wireless Local Area Network. The research results reveals many of the behaviors, expectations and states of awareness among novice users towards the most common security threats, in a SOHO WLAN environment.The effort of this research has the goal to show a problem: the user satisfaction is related mostly with the perceived importance of certain technical issues more than a complete understanding of the related problem.

My research also revealed that wireless security is one of the most misunderstood aspects of wireless technologies. The biggest misconception is that a strong security mechanism is all that needed.This study concludes that wireless equipment manufacturers can contribute to the overall security by providing simple security oriented user interfaces and by keeping the equipment's firmware updated to latest standards.

"Through 2006, 70% of successful WLAN

attacks will occur because of misconfigured

access points or client software." [3]

General terms: Wireless Network Security, user attitudes.

Keywords: Wireless Security, human factor, user awareness, user satisfaction, user information satisfaction.

Dedication

To my parents and my brother, for their everlasting love and support.

***

In constant memory of Pierino Ruggiero.

Acknowledgments

I have never understood just why people write thank-you and acknowledgements sections.Who bothers to read them? Well, I have a better idea why now.

So I want to thank my family, who trusted me to find my own way and encouraged me to go after my passion.
My gratitude goes to Dr. Frode Eika Sandnes, my supervisor, for the help offered when he realized just how clueless I was; he was able to show me the road I was looking for and stimulate my mind.

Life situations change quickly, and two years of education here in Norway have passed.
Emotionally, mostly, I would like to thank Kyrre Begnum, Simen Hagen, Frode Eika Sandnes, and Maurice David Wrnhard, for the great moral support and professional help.

My sincere thanks go to my fellow graduated student in the M.Sc. In Network and System Administration: Jon Henrik, Maurice, Espen, Eivind, Gard, Alexander, Ilir, Sven, Akram, Stig, and Muhammad.

Finally, I thank all the International Students of the University Oslo College for the valid support.

Preface

This Master thesis is written in partial fulfillment of the requirements for the degree of Master of Science in Network and system administration at Oslo University College.

The technical knowledge and the technical skills acquired through the Master degree course at Oslo University gave me a solid technical background, but also the means to understand and analyze problematic of long range, incorporating the technical and the human side of science.
Network and System administration is about designing, running and maintaining a networked system consisting of hardware, software and users.

At the time of writing there is no recorded study of user attitude and knowledge about securing wireless networks.
Part of this research has been useful to create ,with my supervisor Frode Eika Sandnes, a paper for the conference that will be held in October 2006 in Dublin, Ireland.
The paper, which title is *"User Awareness and Attitude to WLAN Security: Effects to Gender, Age and Occupational Status"* has been submitted the 14th of May to the 6th IEEE International Workshop on IP Operations and Management , IPOM'2006 , waiting to be published.
I found interesting the knowledge acquired during this research; it reveals, in all its magnitude, the beauty of the human being.

Contents

List of Figures

Chapter 1

Introduction

Hewlett Packard tells us that 31 Million users worldwide will be accessing public wireless networks by 2007[4].

Marketing trends estimate that by the end of 2006, 21 million homes will have implemented a Local Area Network (LAN), and of those 21 million homes 65% will use wireless solutions [5].Today's society is more global and mobile than in the past years, and the technology has an important place in such a dynamic trend. Since the mid 90's Wireless local area networks, also called Wi-Fi, have assisted to the growth and proliferation among home users, organizations and Universities. A Wireless LAN (WLAN) is a local area network without physical interconnecting wires. The computing devices in a WLAN communicate with one another using radio frequency electromagnetic waves. While WLAN provides greater mobility and flexibility, it also poses several security risks that are not faced in a wired network. Unlike the wired network, the perpetrator does not need physical access to the WLAN, as the medium is shared radio frequency. In addition, the current WLAN security mechanisms used to ensure proper access control and confidentiality of wireless communication are inadequate. Users dislike wired technologies and prefer wireless ones and the popularity of the wireless LANs has been growing a lot in the past few years. Like their wired counterpart, wireless LANs are apt to security vulnerabilities, but also require different security measures. Unlike wired networks, WLANs provide the transmitted data to anyone with a receiver that is in the radio range. As a result, WLAN traffic is also delivered to adversary as well as the intended party, and the adversary with a transmitter has the ability to inject or forge packets into the network.[4]
With WLAN we need to examine threats in a different way: if you had cables extending outside the perimeter of your building would you feel insecure? This is the same feeling you could feel when your data are broadcasted over 'air' with such a WLAN technology. Various WLAN standards or specifications, such as IEEE 802.11a, IEEE 802.11b, OpenAir, HiperLAN, Bluetooth and HomeRF exist today. Among these standards, IEEE 802.11b is the most widely used in WLAN products. This standard counts

that the Service Set Identifier (SSID) ,used in controlling access to the WLAN , is usually broadcasted in clear or can be derived easily.The deprecated WEP and WPA1 have been replaced by the WPA2 standards, but not everyone uses encryption. With increasing deployments of WLAN it is essential to ensure that the deployment of WLAN will not compromise the confidentiality, integrity and availability of information and operations. Most of those vulnerabilities happen because not enough care and precautions are not taken to guarantee that a good security takes place. It can happen that companies sell wireless hardware which are not upgraded, or fail to integrate the latest encryption standards. Additionally, they are unconcerned about releasing updated firmware through the website. In fact the firmware of some models of routers, mainly those which are addressed to a home users, are not frequently available on the manufacturers' website. So, from a security point of view, such hardware is unsuitable for safe communication.

Surprisingly, deprecated encryption standards are still installed on the router firmware so that it is still possible to use them and broadcast "'unsafe"' data over the air channel. Home wireless users and security professionals in the world are all facing similar issues concerning the WLANs security. They both need to find a way to provide a secure working environment. But it is not easy, because the concept of security depends on the overall system policy more than the security of a single specific part of the system.

It is possible to prevent attacks, and a well-known example of security prevention would be a firewall device that restricts specific traffic or ports to or from specific hosts. Although this provides protection against unauthorized traffic, it has no means for determining if an attack is being attempted via an authorized port.[5] This shows already that a single procedure cannot cover the security need of the whole system. An element of security detection would be an IDS (Intrusion Detection System) device that contains a signature to identify a specific attack via authorized or unauthorized ports.

Security professionals often have the technology and resources to develop security solutions based on prevention, detection, or a combination of the two.[5] However, novice home wireless users do not have the time, the wish and often the experience of evaluating the best security policy for their network.They want to be connected in a short time and use the portability of such a technology.

The first part of this document will briefly review the basic home access point security mechanisms, and their weaknesses.

The second part will describe some of the behaviors, expectations and states of awareness of novice users towards the most common security threats happening in a small office/home office (SOHO) WLAN environment.

User awareness and attitudes were tested across different user groups with a special emphasis addressed to the methods that can be used to detect where the vulnerabilities reside and how to secure them.

The effort of this research has the goal to show a problem: the user satisfaction is related mostly with the perceived importance of a certain technical issues more than a

complete understanding of the related problem.
At last, the research points out that wireless LANs can be used safely, if safety measures are taken to install, configure and understand the way to secure them.

Chapter 2

Motivations

The author has been many times present to the installation of WLANs to friends' house and helped them out in understanding the securing techniques and the overall technology to use.
Since many of them were more attracted by the wireless handy technology, than by the technical issues , the security risks built-in in such a technology were ignored or simply undervalued.
Those episodes triggered in me the wish of deepen in the wireless techniques, in particular those related to a home environment/home offices , and to observe the behavior and unawareness of many novices in that field.
Attitude measurements have been used in research to understand individuals' beliefs and behaviors concerning computer usage.
Coldwell [6] (1995) investigated some specific computer issues like hacking and Landing and Slaughter (1999) investigated attitudes related with copyright and copying issues.
However, as far as I could search, there were no attitude measurements for defining issues in securing wireless SOHO environments.
This research has the goal to determine, by attitude measurements, the most common mistakes novice users do when installing, configuring and securing wireless LANs.

Chapter 3

Thesis structure

An overview of wireless Security fundamentals and its security breaches are presented in Chapter 4. The purpose of this section is to give the reader an understanding of the basics of the Wireless Internet technology and its evolution.
Chapter 4 points out the actual problem related with the Wireless security threats and the way to prevent them. It will be also highlighted the actual point where technology and research meet by giving temporary security solutions.
The Chapter 5 and 6 describe the related work, the methodology deployed in this thesis, and the experiments conducted.
The results obtained with the qualitative and quantitative approaches, are presented in Chapter 7.
Conclusion is presented in Chapter 8.
Chapter 9 presents the survey.
Chapter 10 presents the paper "'User Awareness and Attitude to Home WLAN Security: Effects of Gender and Age , *Frode Eika Sandnes and Ugo Santucci* "'

Chapter 4

Theoretical foundations

4.1 An introduction to the WLAN technology

All computer systems and communications channels face security threats that can compromise the overall system security.
The most common threats are[7]:

- Denial-of-service
- Interception
- Manipulation
- Masquerading
- Repudiation

Each threats present its own charateristics and weak points.Some of the listed security breaches are affecting also WLANs. Interception, Authentication, and Encryption are the weakest points of the WLANs[2].
Theoretically, it is well-known that every kind of traffic transmitted by radio signal is subject to interception.This is due to the fact that a Wireless router simply broadcasts the signal over the radio channels, allowing interception of the signal to all the clients situated in the range.In fact, in some cases, WLANs' attacks depend on the ability of an adversary to intercept wireless traffic.Interception of the signal and a subsequentally modification of the *shared-authentication key*, can allow a bad-intentioned user to masquerade its idententity and intercept a legitimate user's data stream.[5] A way to prevent this kind of attack is a form of strong authentication and encryption.These security measures prevent that the content of intercepted signals from being disclosed. [8], [2].In particular, the most weak points of Wireless Local Area Networks are in the *Authentication* between a station (i.e. a wireless device) and an AP (Access Point), and in the encryption mechanisms.

Five years have passed since the first defeat of the WEP security mechanism. The well known story recounts that in 2001, a group from the University of California, Berkeley presented a paper describing weaknesses in the 802.11 Wired Equivalent Privacy (WEP) security mechanism defined in the original standard; they were followed by Fluhrer, Mantin, and Shamir's paper entitled "**Weaknesses in the Key Scheduling Algorithm of RC4**"[9]. Not long after, Adam Stubblefield and AT&T publicly announced the first verification of the attack.The problem was in the key re-use, a familiar issue in cryptography: if the same key is used repeatedly to encrypt the same data, an attacker can easily discover the key. Before an attacker can acces a WEP protected network, the amount of data captured has to be quite large.If the wireless network could change the key periodically,it will make much harder to find crack the secret key[10].
In 2001, the Wi-Fi alliance began to quickly realize that consumers needed an alternative to WEP sooner, rather than later. Realizing that Task Group i, the IEEE working group in charge of 802.11i, would not be ready to ratify their standard in time to meet with consumer demands, the Wi-Fi Alliance decided to create their own subset of 802.11i called WPA or Wi-Fi Protected Access. WPA was based on portions of the 802.11i standard that were already decided on before ratification of the standard [9]. In fact, the 802.11i is the most recent standard for wireless local area networks (WLANs) that provides improved encryption for networks.The 802.11i specification offers a level of security sufficient to satisfy most government agencies. It has been tested and deployed for years in corporate, enterprise, private and public environments (e.g. hot-spot areas), and it should be one of the favoured technologies for home networking. 802.11i aims to enhance 802.11 security[11],[12],[13].

Today there are free tools available that exploit those vulnerabilities, enabling even novice hackers to be able to break the WEP encryption and hence gain unauthorized access to wireless networks[14].The most famous are Aircrack,Warlinux distribution and NetStumbler[15],[16],[17].

4.2 Existing products

In SOHO environments, vendors and manufacturers of WLANs routers must implemement all mandatory features of the security standards to prevent the communication from being intercepted.Unfortunately, this does not always happen. In a wireless router, one of the most important features, is to strongly authenticate and secure the communication.This means that products should always keep track of the latest security standards and known security breaches [7].The on-going development of the IEEE security standards has to be tracked by the hardware's components involved in a WLAN[18]. The point to be made is that all products involved in a Wireless Network should meet the latest standards; this is only possible if the vendors give the possibility to update the hardware's firmware.

4.3 Security concerns in SOHO

In order to penetrate a WLAN, an AP must be located. APs bridge wireless end users to the wired network, and are often located BEHIND the firewall.Improperly configured APs broadcast important informations of the message (frames) that contain security information about the WLAN. Hackers have built utilities to exploit this information. One such hacker utility is called NetStumbler. It is a Sniffer, so called because it "'gathers"' data[15].
In fact, it is possible to crack the WEP with only 300MB of gathered packets (the amount usually recommended for WEP cracking). Many tools are available on the Internet. Such tools can run on different platforms. They mainly gather informations about about the AP's present in the area and about the security breaches of the AP's.Once a "'weak"' APs is located, there are many possibilities of capturing the traffic and violating privacy. One of the most known distribution is WarLinux.It is a Linux distribution for WarDriving. Wardriving is searching for Wi-Fi wireless networks by moving vehicle. It involves using a car or truck and a Wi-Fi-equipped computer, such as a laptop or a PDA, to detect the networks. It is available on disk and bootable CD. It's main intended use is for systems administrators that want to audit and evaluate thier wireless network installations.Such a powerful tool, is intended to be handy for wardriving also[16].

4.4 Best security practices

It is not easy to properly design secure networks, so it is necessary to implement secure policies to obtain security.Security policies varies from place to place. They depend from the dimension of the network and from the number of clients served. A tipical SOHO environment is meant to give connectivity to a limited number of clients, generally not more than few tens. SOHO networks generally are confined to a single room, they generally use a router, small Ethernet switch and a Wi-Fi wireless network.Generally SOHO networks are used to share files and other information as well as to share an Internet access connection. A SOHO network may also have a server which needs to be accessed.
Because of their small scale, the security reccomendations can be easily covered, in order to have security on mind when designing and implementing the network.
Obviously, WLAN manufacturers are encouraged to think addressing their products and offers to an increasing number of novice users. For those interested in deepen into the subject, I would advice to read through an excellent paper that guides to WarDriving. It is available on the free press room of the SANS institute **(SysAdmin, Audit, Networking, and Security)** archives[19]. Novice users are also encouraged to focus on the Wireless 802.11 security, by reading the main guidelines available on the System Experts paper[20]. An easy overview of the main WLAN security best practices is reported.

- It is good to puchase WLAN products that are able to update their firware, automatically or through the manufacturers' website, in order to keep track of the 802.11i security standards.
  Many WLAN products start to have a proprietary security mechanism to overcome the shortcomings of the 802.11 security standards.

- It is important to utilize VPN tunneling technologies to ensure proper confidentiality and authentication of the WLAN usage. All data will be encrypted and it will safeguard the the network from intruders[5].

- It is a good practice to change the WLANs default SSID (Service Set Identifier) or hide it. In most Windows operating systems , the APs(Access Point) , by default, broadcast their SSIDs to connect themselves to the wireless clients.As consequence the client,when activating a wireless card,can have a list of all the APs in the range and try to connect and join them.This means that any wireless device,in the transmitting range of the AP,is able to join the network. Disabling SSID broadcasting makes APs harder to identify .A client will have to manually enter the SSID to join specific AP. This applies to all wireless technologies (802.11a/b/g).
  This measure is the first and the easiest step toward securing a wireless network.Moreover, the default setting SSID are available on the Internet from most WLAN manufacturers. An hacker would feel partially decouraged to gather and subsequentally attack the WLAN[21].

- It is adviced to power down the wireless station; to reduce the power transmitting range of the wireles station, when it is not used for a long time, helps in order to reduce the probability of an attack coming from outside the WLAN perimeter[11].

- Another feature available on most wireless APs is MAC (Media Access Control) Address Filtering. It give the possibility to the router administrator to create an ACL (Access Control List),which is a list of all the computer can connect to the network. It is basically a filter method,useful only in part. It select the computer by filtering them with the MAC address,which is easily spoofable today. This measure requires more effort since the administrator would need to collect the list of MAC addresses for all authorized wireless devices[10]. While a useful security measure for a small office, this may not be feasible for large organization.Allthough such a measure decourages only novice hackers, it can be useful in SOHOs .In fact, almost all access points allow the user to create access table allowing filtering the number of clients willing to reach the WLAN.Only registered and trusted clients can connect to the AP[5].

- Using strong encryption mechanism is important as well. It is necessary to configure the Wireless router with the latest encryption standards, in order to

decourage any attempt of possible key-cracking[22].Let us remember that it is enough for a hacker, to gather 300MB of data to probably be able to crack WEP.

- WLAN users should not be allowed to set up their wireless stations in ad-hoc mode and communicate with each other without going through the access point. This is to prevent unauthorized access to the user's files if they are not protected. The user should power down the wireless station when it is not being used for a long period of time, e.g. after office hours. This will reduce the risk of attacks on the wireless station over the WLAN[11].Also the user's wireless station should not have concurrent direct connection to any untrusted network, e.g. the Internet, when the wireless station is connected to the internal wired network. This is to prevent any unauthorized access to the internal wired network via the wireless station.

4.5 Users and technology

Clearly, one needs certain technical insight to secure a wireless network. It is unrealistic to expect ordinary users to acquire sufficient insight. The responsibility of ensuring adequate security therefore falls onto the equipment manufacturers and software providers. There are several interesting studies on how novice users relate to security.
For instance, it has been demonstrated that novice users find it difficult to conduct an encryption task on a message[23] and hence find it difficult to protect e-mail messages. Another security feature that most users get in direct contact with is passwords and several studies have addressed how users compromise password security [24],[25]]. Attitude to security has also been studied and it has been found that age is an important factor as younger users are more pragmatic about security than more senior users [10]. Studies from different areas of computer science repeatedly confirm that technology have different effects on different user groups. Especially, in the field of human computer interaction (HCI) . Young users are more comfortable with the technology than older users, and young adults are again better than children. Gender has also been found to affect how users interact with technology. Male users perform better at spatial tasks relying on spatial memory than females and that females are more emotionally driven [**?**]Finally, practice results in learning and consequently better performance [26].
The hypothesis of this study is that different user groups have different attitudes towards wireless technology. It is also relevant to study this diverse set of groups as an increasing portion of the general population is setting up wireless networks in their homes. The expected results of this enquire is that males would be more familiar and aware of WLAN security than females and that young adults would more familiar with WLAN security than senior users.

Chapter 5

Quantitative study

This study is an investigation of novice Internet user's attitudes and awareness. The author has used questionnaires concerning computer Wireless security scenarios to gather informations about the general trends of the chosen demographic. User attitudes, user awareness, operator care/lessness and wireless security are the primary topics covered in the quantitative study. This chapter, which regards general trends, deals with the usage and practice of wireless networks in SOHO environments and important technical issues such as encryption standards, SSID broadcasting and MAC filtering.

5.1 Methodology

I have chosen a quantitative research method for investigating students' and employees' attitudes and responses, because it offers a effective method (with a valid feedback) to investigate attitudes of a large population. The quantitative study was realized using a questionnaire the purpose of which was to reveal general trends regarding user attitudes and reactions towards the concepts of wireless LAN networks, general Internet security, configuration and installation of wireless routers, security standards, and safety security measures. A total of 40 subjects completed the questionnaire. The general demographic was the international student population at the Oslo University College. The subjects were chosen to widely represent gender, age, profession and different technical Internet backgrounds.

5.2 Considerations

During the production of the survey, the following factors were consistent:

- **Number of questions.**

  The survey was composed by 20 multiple choice questions. The number of questions was small, not more than 20, because the subjects had to focus on 2-3 main topics related to wireless LAN Security, which required a high level of focus.

- **Length and simple layout.**

  It was important that the survey had to present a light easy reading content and should have not reminded students of any kind of examination test. I aimed to devise a survey which would be relatively enjoyable to take part in, and also potentially enhance the students' knowledge. Layout was as simple as possible in order to be read and submitted in no more than 20 minutes. Each question took, in average, one minute to respond to. The length of the survey was initially limited to 5 pages, for maximum concentration and focus.

- **Open questions.**

  Open questions were meant to increase the subject's participation in the test and to widen the possible feedback.

- **Life Scenarios.**

  Some questions had a joint-part, which required the subjects to put themselves in a real case scenario in which they were personally threatened, which heightened the sense of importance. Two different life cases were created, with the intent of stimulating the subject and producing a state of awareness of real possible threats. These kinds of questions amplifed the reactions and the awareness of the subjects. Moreover, the subjects better recognized the thin gap between theoretical eventuality and reality of a security threat.

5.3 Materials

The questionnaire has experienced five different production phases. The final version, the one submitted by the students, presented 20 multiple-choice questions written in English. The surveys were printed on six sheets of one-sided paper.
The final survey is available in the Appendix A.

- All the multiple choice questions had an open question option, where it was possible to fill in an acceptable reply, in case the provided responses would not satisfy the subject.

- The questions were constructed in a clear and simple jargon-free manner, in order to avoid questions being skipped. So the questionnaire offers open question and ”I do not know” response options.

- In many questions it was possible to choose more than one reply. The number of alternatives ranged from two to fourteen options.

- The questions were formulated for an audience comprised of subjects who had both expert and novice experience of computer security.

5.4 Subjects

The research subjects consisted of international students at the University of Oslo (UIO), Oslo University College (HIO), and some HIO employees and researchers.The majority of the population belonged to the international student population of the HIO.An important factor that motivated the interviewer in choosing the student population as a demographic was the fact that international students represented a wide mixture of students coming from all over the world.The different cultural backgrounds, technical skills and education, provided a rich, varied and heterogeneous response for analysis leading to a wide variety of results.Their help has been important especially because their diverse methods and views, made it possible to foresee a wide and experimental approach to wireless concepts.
All of the subjects taking part in the survey had to be unfamiliar with the latest changes and updates in wireless security or Internet security countermeasures.The main characteristics linking the subjects were an interest in knowing more about wireless techniques and potential practical dangers and threats. Students were encouraged to take part in the survey as it was a way for them to learn more about new technological issues and feel stronger and more aware of the problems they bring. The theoretical background they had was relevant because it radically changed their way of understanding

questions and the replies submitted. The subjects had the opportunity to show their knowledge in various different sub-fields of the wireless and their ability of criticizing the suggested questions was relevant in order to have new terrains and data to extend the research. If they thought some questions were inappropriate, they filled a blank field with a suggestion about what they thought about that relevant section. This is the reason why the ”open” questions have often been particularly pertinent. A minority of the population consisted of employees and researchers at the HIO, with some technical Internet background, but novices in the wireless field. They also showed a strong interest in the wireless technologies and they generally considered themselves ”unaware of the security risks that wireless brings”. That is the reason why four of them have also shown interest and participated at the interview in a second stage of the research.

The questionnaire was distributed in a time interval of 9 days, in the 3rd week of April 2006.

5.5 Analysis methods and data gathering

Each subject was contacted on a one-to-one basis and completed the survey under the supervision of the author. 95 % of the questions were collected in person on hard copies. The remaining 5% of the questions were collected via e-mail. Students took about 15-20 minutes to complete the questionnaire.Data were manually recorded from the questionnaires and input into Open Office Calc suite. Subsequentally, they were analyzed with statistical tools and plotted.
The number of questions replied to, was very high, suggesting that most people were interested in the survey and sufficiently motivated by the topics addressed.
General trends and combined quantitative analysis are presented.

5.6 General trends

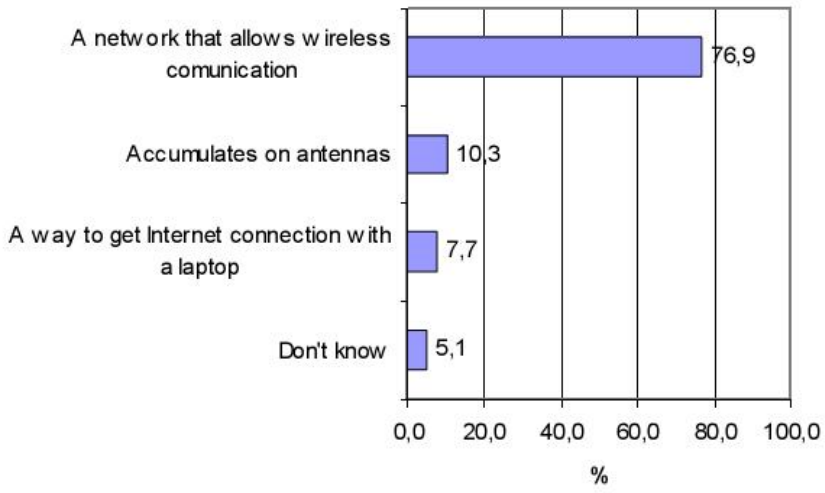


Figure 5.1: What is a WLAN ?

In this section only the most relevant observations are included, for the sake of brevity.
The figure 5.1 indicates a general opinion about what a WLAN is.
76.9 % of the subjects thought that a WLAN was a network allowing wireless communication to occur. This response was correct.
7.7% of the subjects were under the impression that a WLAN is a method of connecting over the Internet with a laptop computer.
This trend is understandable considering that laptop computers are the computer items most often connected to a wireless network and novices, probably, associated them with a WLAN.
An unusual 5.1% wrote that they did not even know what a WLAN is.
Such a trend is consistent, guessing that this is connected to unfamiliarity with the acronym WLAN (wireless Local Area Network) and not necessarily the concept of wireless communications.

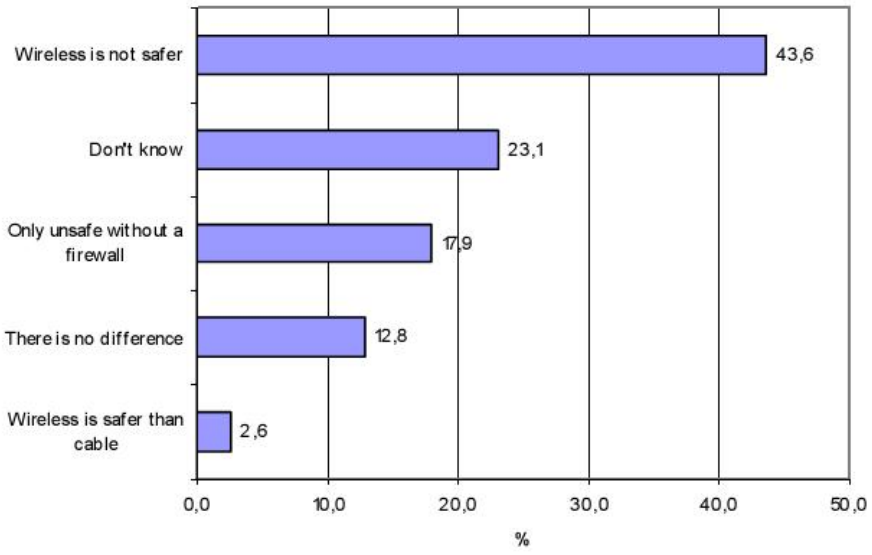


Figure 5.2: Is wireless communication safer than communication through a wire?

Fig 5.2 shows the tendency of responses to the question: ”is wireless communication safer than communication through a wire? ”.
Here 43.6% of the subjects correctly believed that wireless is not safer than a wired connection, only 2.6% support the claim.
Surprisingly, a massive 23.1% admit not to know, and the 12.8% claims that there is no difference. The 17.9% incorrectly believed that a firewall would provide the necessary Internet safety. Based on these results we can conclude that nearly the 50% of the respondents have a realistic notion that a wireless technology suggests that data is broadcasted over ’air’ and thus security is lost on the way. Half of the subjects have an unclear and mistaken understanding of the problem. I think that such a trend is influenced by heavy and inaccurate advertisement of media, in the Internet field. Media would be considered by the author to be partially responsible for this. For example, the high number of respondents trusting in firewalls to keep them secure may be due to the repeated mentioning of firewalls in connection with security during the last 5 years. Some of the subjects believed that there is no difference between a wired connection and a connection over the ’air’ channel. They are probably not aware of the fact that a radio signal cannot be sent only to a specific receiver, but it has to be broadcasted in the air, so it is possible for everyone to capture and analyze it.

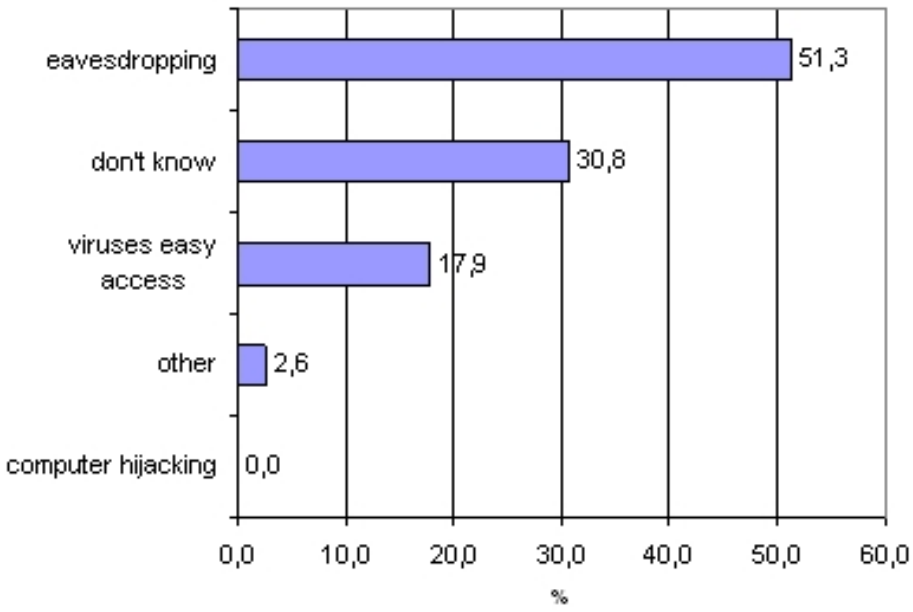


Figure 5.3: Disadvantages of unencrypted traffic.

Fig 5.3 reveals the subjects knowledge about the disadvantages of unencrypted traffic.
In this case the 51.3% correctly perceived eavesdropping, the intercepting of conversations by unintended recipient, as a possible problem. In the survey terms such as eavesdropping were replaced with clear explicit phrases like ”someone who secretly listens in on the conversations of others”, in order to make the questions more accessible to people who were less literate in English, or not aware of computer jargon.
Worryingly, 30.8% of the subjects indicated that they did not understand any threats were posed by unencrypted traffic.
Altogether, 17.9% of the subjects were aware that unencrypted traffic makes the system more vulnerable to virus attacks. This notion is unfounded, because it assumes that a malicious code has been injected in a captured packet, in a hijacked session. In addition, media and private companies have highlighted and stressed the risks related with viruses, and some users may associate them with any type of security problem.
It is very surprising that none of the subjects indicated the computer hijacking as a possible disadvantage related with an unencrypted traffic. In the survey, the term ”hijacking” is used when spyware or a virus alters a computer program so that whenever that program is being used, it performs tasks set by the creator of the virus.

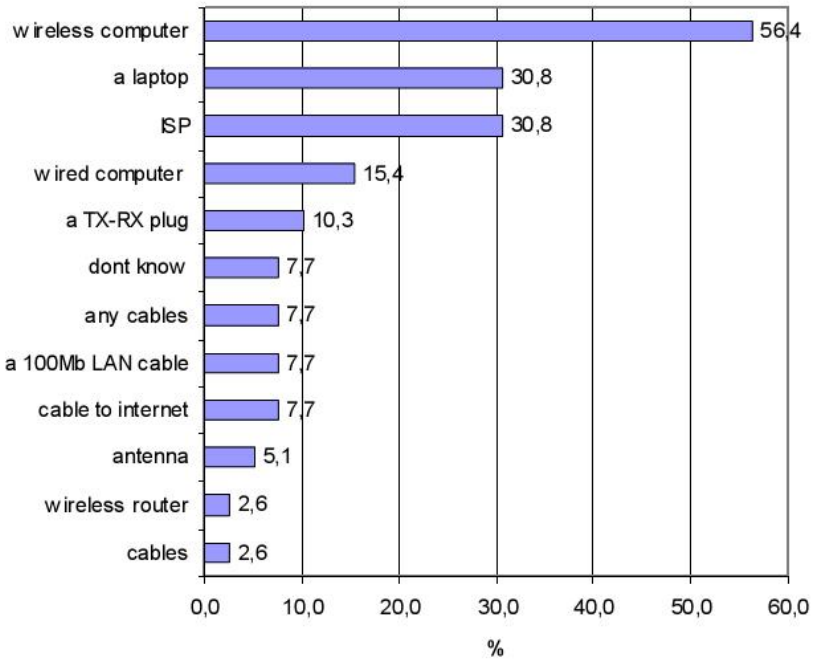


Figure 5.4: Items needed to set up a WLAN.

In the Fig 5.4, the plot shows the trend regarding the conceptions and misconception about the elements needed to set up a WLAN.
More than the half of the subjects, that is 56.4%, claimed that a wireless computer is needed. Although this is a common practice, it is not truth. It is surely possible to set up a wireless network, with only wired clients.
The 30.8% of the subjects stated that a Laptop is needed to set up a WLAN. In fact, either item is needed to use a wireless connection, but not to set it up.
Very surprisingly, only 2.6% of the population was aware that a wireless router and cables are needed, and only 5.1% of the subjects indicated the need of an antenna.
Although the antenna is usually integrated in the wireless router and in the wireless cards of the clients joining the WLAN, it is a basic element, because it gives possibility to a signal to travel into the air.
It is also surprising that the 10.3% of the subjects indicated the need of a transmitter-receiver plug.
Reassuringly, 30.8% correctly indicated an internet service provider (ISP) as a necessity.The subjects' responses show that there are confusion and misconception regarding the components of a wireless network.

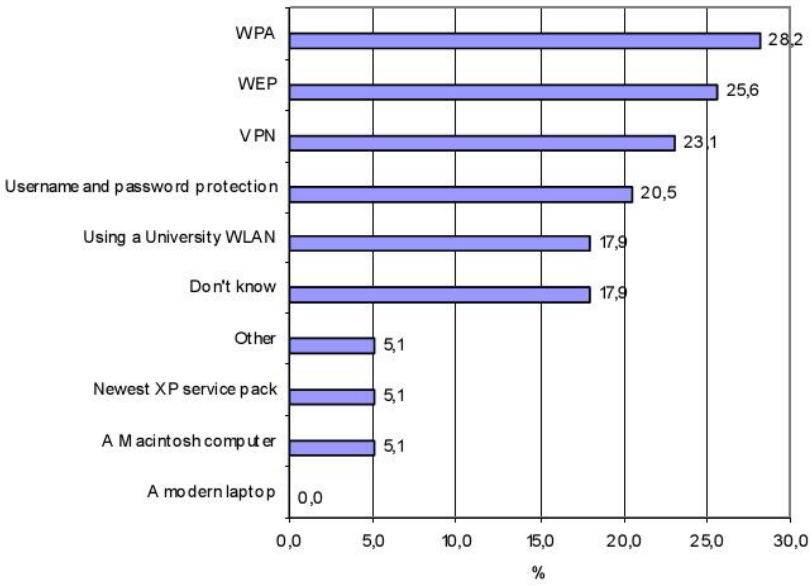
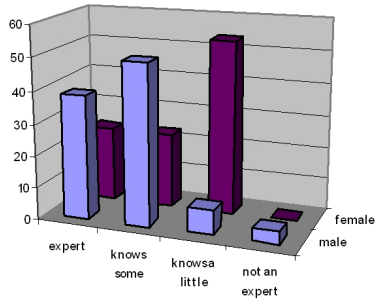
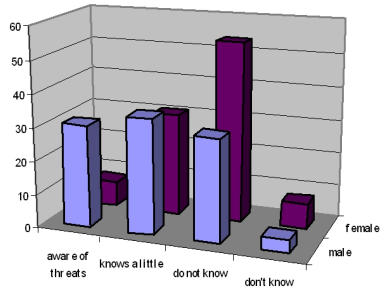


Figure 5.5: Elements that give security in a WLAN?

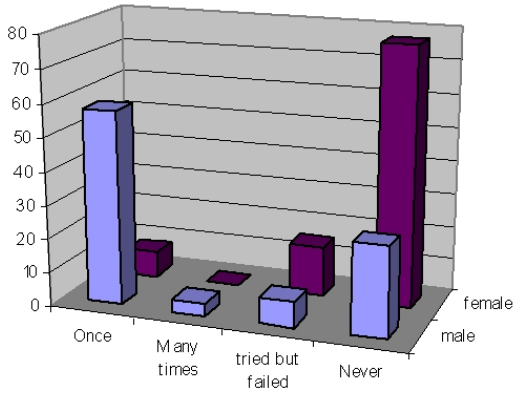
Fig 5.5 enumerates elements that provide security according to the subjects.
The results show that about a quarter of the subjects view WPA, WEP and VPN (Virtual Private Network) as technologies that provide security.
This is an encouraging trend because the encryption standard WPA2 and the tunnelling VPN technology are really elements providing security to the network.
Unfortunately, a 25.6% of the subjects still think that the now deprecated WEP encryption standard is a reassuring element.
A total of 17.9% of the subjects indicate that they do not know. Of the more ambiguous and misunderstood security practices included 20.6% of the subjects that believe that username and password protection adds security, 17.9% believe that using a University WLAN is safe (”its provided by the university so it must be safe”), 5.1% believe using a Apple Macintosh computer is safe and 5.1% believe that installing the most recent Microsoft Windows XP service pack will do the job.



(a) Self-assessed Internet skills



(b) Awareness wireless security threats



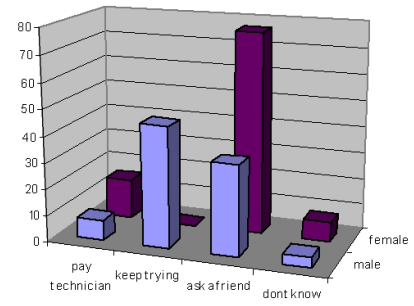
(c) Subjects that have installed a WLAN-gender breakdown

Figure 5.6: Combined quantitative analisys based on Internet skills, awareness of security threats and previous experience - Gender breakdown

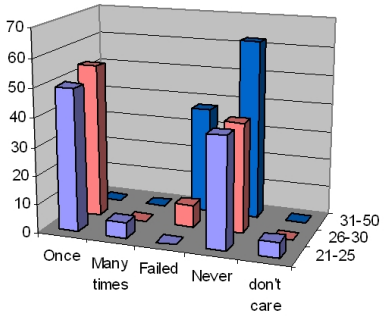
5.7 Combined quantitative analysis

5.7.1 Effect of gender

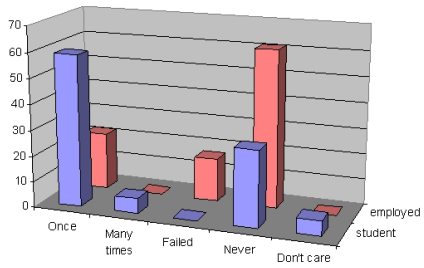
Not surprisingly, the largest cross-group difference was observed with respect to gender.



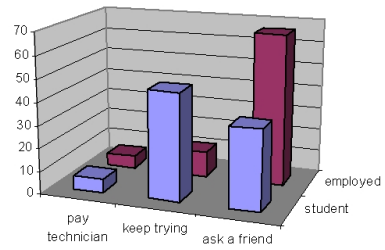
(a) How to tackle difficulties installing a WLAN



(b) Subjects that have installed a WLAN-age breakdown



(c) Subjects that have installed a WLAN-profession breakdown



(d) How to handle difficulties installing a WLAN

Figure 5.7: Combined quantitative analisys: difficulties, previous experience, capacity of handling difficulties - Professional and Age breakdown

Fig 5.6.a shows the breakdown of self-assessed Internet skills. There is a clear difference between males and females.
Males express more confidence than females as 38% of the males view themselves as expert Internet users, while only 23% of the females viewed themselves as experts. Similarly, 50% of all males claims to have ”some” Internet skills, while only 23% of females did so. However, females were in majority (58%) in terms of having ”little” Internet skills, while only 8% males thought the same.

Fig 5.6.b shows the subjects' self-assessed awareness of wireless security threats. Again, males indicated a stronger awareness of wireless security threats than females as 31% males and only 8% females indicated awareness of wireless security threats. The males and females where approximately equally divided on knowing a little about

security threats (35% males and 31% females) and females where in majority for the group that indicated no awareness (54% females and 31% males).

Fig 5.6.c shows the gender breakdown with respect to practical experience with setting up a wireless network.
Clearly, males express more familiarity with setting up a wireless network than females as a massive 58% males claim to have set up a wireless network once versus only 8% females.
Next, 77% females reported never having installed a wireless network compared to 27% of the males.
Only 4% males had set up a wireless network more than once. Next, 15% females and 8% males had attempted setting up a wireless network, but failed.

Fig 5.7.a shows how males and females would tackle difficulties while installing a wireless network.
The general trend is that males report a willingness to try themselves until they are successful (46% males, 0% females), while females are more likely to seek help.
Most subjects would ask a friend (77% females, 35% males). Others would be willing to pay a technician to complete the job (15% females, 8% males).

5.7.2 Effect of age

Results for the different age groups are similar to the ones obtained for the genders.
However, there was not much effect of age between the young age groups, i.e. 21-25 and 26-30 years of age.
There are, generally, more distinctive differences between subjects that are 21-30 and 31-50 years of age.
For example, Fig 5.7.b shows the differences between the different age groups with respect to experiences installing a wireless network. Generally, young adults have more experience with installing wireless networks than older subjects. There are not many differences between the two groups of young adults.

5.7.3 Effect of professional status

The differences between the user groups were smallest for the group of students versus employed. This again is probably an effect of a limited sample.
The current study should be expanded to include computer professionals versus non-computer professionals. The results in this section should therefore be viewed with some caution.

Fig 5.7.c shows the breakdown of experiences installing wireless networks with respect to being a student or being employed.
The results show that students have more experience with setting up wireless networks than employed individuals. Among students 59% had set up an wireless network once, 6% many times and 29% never, while among employed subjects 22% had installed a wireless network once, none several times and 61% never.
Furthermore, 17% of the employees reported having tried to install a wireless network but failed. None of the students reported failing to install a network.
One explanation of this could be that students have more time on their hands and are dependent on Internet access to conduct their studies. To save money they experiment themselves. Some employees are less dependent on Internet at home, and all required computer infrastructure is provided at work.

Fig 5.7.d shows the attitude these two user groups have towards problem solving during wireless network installation. Students (47%) are more likely to continue trying until they succeed than employees (11%), while employees (67% employees versus 35% students) are more likely to ask a friend. Students and employees are equally unlikely to pay technicians to do the work (6%).
Again, one possible explanation is that students have more free time than employees , and they are more willing in save money.

Chapter 6

Qualitative study

6.1 Methodology

Clearly, it is difficult to portend (and to predict) how a person reacts to a new technology never encountered before. Neither it is easy to foresee the way a person can react to different incentives. The approach to a new technology can stimulate curiosity, can be frustrating, funny, sad, and can provoke a sense of confusion. It happens it can also provoke interest and arouse the will of knowledge about that specific area of interest[27]. For the home wireless LANs, it usually happens that people are attracted by the portability and convenience of such a solution and also to the prices of the equipment encourage the trend. The interest in such a technology can be really strong and sometimes people cannot cope, in terms of technical knowledge, with the required expertise to set up safe and well-functioning networks. This is the challenge hundreds of novice users experience everyday in their home offices or home environments, when they want to use a wireless technology.
The author has used four real life experiments consisting of installing and securing a wireless LAN at the Oslo University College, Norway. Four novice users have been invited, on different days, to an interview at Oslo University College, from March to beginning of May 2006. During the interview, which lasted approximately one hour, they were asked to configure, install and make it work a relatively simple home WLAN. The experiment, thought and planned few weeks before the interviews, has been held in special equipped labs, where technical parameters (as LAN connectivity, frequency signal overlapping and wireless LANs) could be analyzed and kept under control. Obviously, other wireless LANs beacons are present all over the University perimeter, so special precaution has been required by the interviewer, when making the experiment. The goal of the experiment was to reproduce a SOHO (home office/small office) environment in which to test the user conveniences and reactions, based on an attitude measurement. The interview, in the beginning, was thought to generate and analyze outcomes on different levels. Data were supposed to be subsequently analyzed through statistical instruments and the theoretical help of a vast literature on the Hu-

man Computer Factors (HFC) affecting human choices. The author understood that many sides of the human behavior were involved in such a typology of research, and was humbly aware of the greatness of the human mind. Thus, both sides were taken into consideration through a statistical analysis. The two main outcomes focused on were the technical aspects, and the human side. On the technical side, it has been really interesting to witness the response users had to the technologies and technical environments they are immerse into. On the human side, special attention has been addressed to the attitudes and the expectations users had facing WLANs technologies.So, both the technical and the human outcome have been statistically analyzed after the interviews The subjects were asked to ”think aloud”, to express all the mental steps they were encountering during the experiment and all the technological lack of knowledge they felt during each single step of the procedure. Also, it was made clear, they had to communicate and express their impressions, some emotions, expectations, reactions, frustration and general feelings, by giving us the possibility to record and get insight to the states of awareness. Such a request has been fundamental for us to be able to register and analyze data. Additionally, the act of recording the interviews gave us the possibility to analyze data on a time line frame, which gives a clear indication of the reactions and reflexes times.

6.2 Subjects

Four subjects were selected and recruited for the qualitative study. Computer users, with a very tiny and superficial knowledge of Internet security, where chosen in order to acquire interesting qualitative data. Novice users had a narrow technical background, but they were willing to understanding and learning about wireless technology, and the main guidelines to make it work safely.

1. Ruth Calva, Spanish, female, 22 years old, international student of Telecommunication Engineering at the Oslo University College.

    - She uses her laptop for study.
    - She uses the Internet everyday at home, with a wireless connection. She has never been thinking about security problems related to the wireless networks she uses at home, because she says she has no private information to hide. Her Internet habits can vary from normal browsing to interactive games. She mostly uses multimedia applications.
    - She checks her mail few times per day.
    - She has never seen any AP (Access Point) at her place but she knows there is one.
    - She does not use any form of authentication in her home WLAN. She lives with three other international students in the house and she has never been thinking they could audit her confidential information.

2. Anya Zhuravkova, Russian, female, 23 years old, international student of Journalism at the University of Oslo.

    - She mainly uses computer 3 or 4 times per week for study reasons.
    - She writes articles and stories with Microsoft Word. She's got a laptop for 3 months and she has never connected it to the Internet.
    - Sometimes she uses the University student account to check her email on a well-known russian web server: *Yandex.ru*.
    - She has never used a wireless network in her life; neither has she known what the associated technical security issues are.

3. Mari Mehlen, Norwegian, female, a mathematic teacher at the faculty of Engineering at Oslo University College in her 50's.

    - She uses a networked computer on a daily basis, with the access over the Internet.

- She has never configured a wireless LAN but she has heard about it.
- She's aware of some security breaches over the Internet but she's unaware of the potential security threats of a wireless network.
- In the job environment, she does not worry at all about Internet security threats because she thinks that it's up to the security technicians of the University to work for giving security to the University employees.

4. Jorunn Fergus, Norwegian, female, member of the administrative staff at the Engineering Faculty at Oslo University College, also in her 50's.

    - She also uses the desktop computer at work, connected on the Internet, on daily basis.
    - She has access to the University Intranet.
    - A big percentage of her daily jobs rely on the Intranet. She uses specifically administrative software, among all the administration departments of the University backbone.
    - She's unaware of the security issues a wireless LAN can bring, and she has seen a wireless router before because her son has tried to install at homr, a wireless LAN few times (without succeeding).
    - She is really motivated to take part to the interview to acquire the means, she says, and understands the tools to install and secure a wireless network from scratch.

All subjects were female. The light Internet experience and the almost limited knowledge of network security, is a common feature for the subjects. The subjects use common office applications, University software, and some multimedia applications to browse on the Internet.
The differences in culture, age, educational background, and technical understanding merge into an interesting four study-cases the interviewed.

6.3 Precautions and materials

The Engineering Department at the College has kindly offered to finance the materials for the experiments. The lab environments where the interview sessions were held,all presented already a wireless working Network, the University one. Before getting started with the first interview, preparations were taken to ensure that no packets collision or networks conflicts were taking place. A virtual private network (VPN) is a private communications network usually used within a company or University to communicate over a public network. VPN message traffic is carried on public networking infrastructure (e.g. the Internet) using standard (often insecure) protocols[20]. The local University pre-built WLAN used the communication channel 6, not encrypted, tunneled through VPN (Virtual Private Network) technology, and serving a theoretical unlimited number of clients in the signal range.In fact, it was really likely that creating a WLAN in the same frequency range, with a similar client-server technology, would have lead to *a packet collision or ARP (Address routing Protocol) conflicts*[28].More in details, it can happen that two WLANs, with two different SSIDs, can travel on the same air channel and the same air range. They can use the same client-server authentication standard , so that two or more packets of the nets can overlap , damaging the quality of the connection. In the worst case, it is really likely to have a total shadowing of one of the WLANs [29].The technological policy of the University College has not interfered so far in the installation and configuration of our home WLAN. Besides, the physical location of the underground laboratories softened any possible potential collision.The simple home WLAN we were going to install used default channel 6 , a different SSID than the one used by the University, a high level of encryption 64-128bits, no use of tunneling technologies (i.e. VPN) and serving just one client.

Figure 6.1: D-Link wireless router. Picture imported from the manufacturer's manual

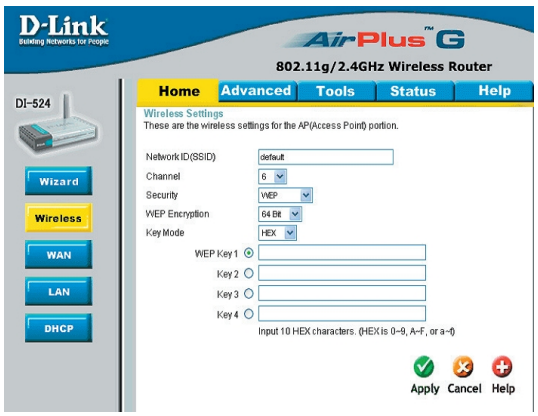
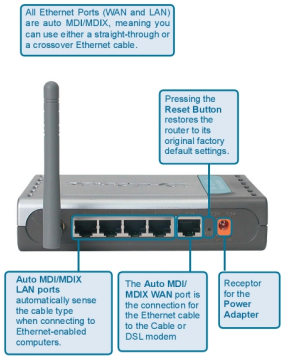


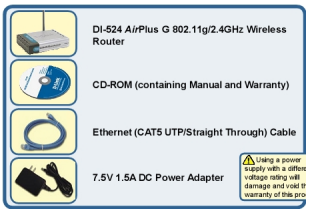
Figure 6.2: Router's web-interface. Screenshot captured during the configuration procedure.

A D-Link wireless router, in Fig 6.1, model AirPlus G DI-524, was used for the experiments. It is known to have a pretty easy setup with a step-by-step configuration management support. The Router has all advanced firewalls and latest encryption standards built-in, to minimize the threats of hackers using penetration tools. It can be configured as a virtual server; it has a port redirection management interface, and all the newest filtering features. When it comes to encryption, it is furnished of the latest WPA-PSK standard, but it also gives the possibility of choosing a deprecated standard. All those features are accurately customizable through a web-interface (Fig 6.2) that the routers lays out.
Note: This way of configuring the router is for expert users acquainted with the latest technologies; the subjects participating to the interview have not used such a configuration method.Moreover the router presents one Input plug for the LAN Internet connection and four plugs to multiplex the band through normal crossover cables(Fig 6.3.a).During the interview the D-Link router was provided in the original packaging, as delivered from the shop.

- The router.



(a) Router's plugs. Picture imported from the manufacturer's manual



(b) Package content. Picture imported from the manufacturer's manual

(c) Dell Inspiron 1150

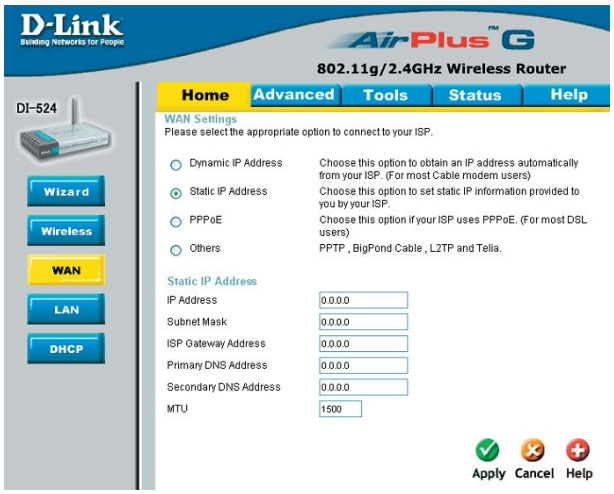
Figure 6.3: Materials used during the interviews

- The power supply.
- One blue LAN cable.
- An installation CD.
- The warranty.
- A quick instructions manual in five languages, including Spanish, Norwegian and English. Russian was not listed.

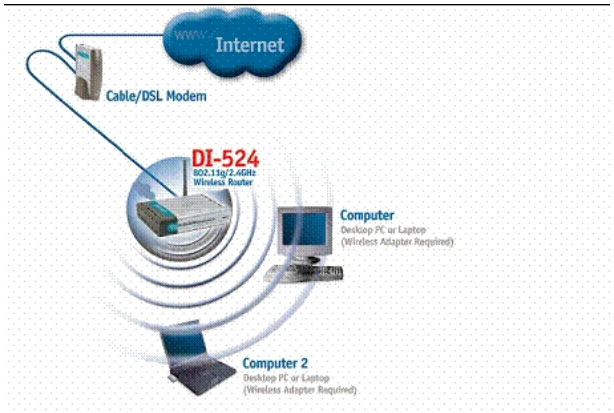
The package contained the following items (Fig 6.3.b): A Dell Inspiron notebook computer 1150 with OS Windows XP in Norwegian language, built-in WLAN card and a Cdrom drive (Fig 6.3.c), was used during all the interviews.
The interviews were carried out in three different laboratories, all of them had a desk next to the wall were it was possible to use the University LANs plugs.

6.4 Procedure

The subject was guided to the place of the interview and in the meantime asked what were her expectations and if she had a vague idea about what was going to happen in the lab. A short introduction of the interview was explained, in order not to adduce possible anxiety or any situations of uneasiness and discomfort for the subjects. The technical and the human outcome were going to be registered and subsequently analyzed. The subject was asked to think aloud and express the feelings she experienced. Sessions were recorded with a Video Camera (1st Interview) and with an MP3 player (2nd, 3rd, and last interviews).To configure the home WLAN, the subjects had to first install the router and then configure it. The two processes were made as easy as possible, by using the installation CD furnished in the start package.The CD drove them through the process, by the the visual help of some easy screenshots.The first steps consisted of unpacking the package of the WLAN router and explore its contents.On average this took five minutes. The investigator has always tried to minimize its involvement and focused on the subject's own reasoning. Of course hints were given when the subjects were obviously struggling. After unpacking the package and spreading all its content on the desk, the subject was asked to configure and install the wireless network. Then, the subject was driven through the steps to configure and install the router. These procedures varied from 20 to 35 minutes, depending on the technical background of the subject and of the overall understanding of the procedures. Subsequentally, once the router was successfully configured and installed, the connection of the WLAN was tested and the client was authenticated to the WLAN, through safe authentication steps. This procedure usually did not present any bottlenecks a part some basic knowledge about operating system Window XP, and how to join and connect to a wireless network. The authentication had, obviously, to be carried out by remembering the pre-created authentication keys. Finally, to verify that the client was connected to the Internet, a browser was opened and a random web page loaded. Most hacking tools do need a little bit of technical expertise, perhaps on Linux operating systems , so it was really unlikely novice users could run such a tests. Moreover, the possibilities to crack WEP keys, or analyze traffic, requires one to gather and capture wireless packets for hours and hours. Such an attempt would have been useless in such a short interview time.
I encourage researchers to investigate and further explore in such a direction.



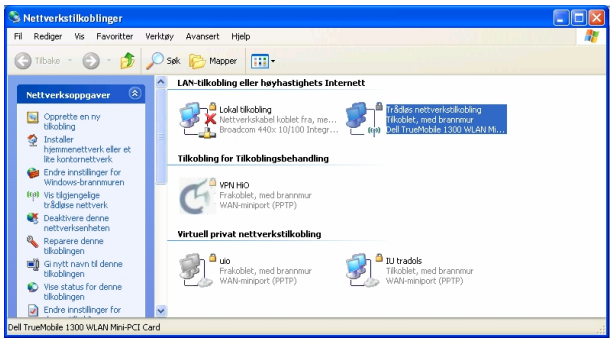
(a) Web - interface to control the router configuration



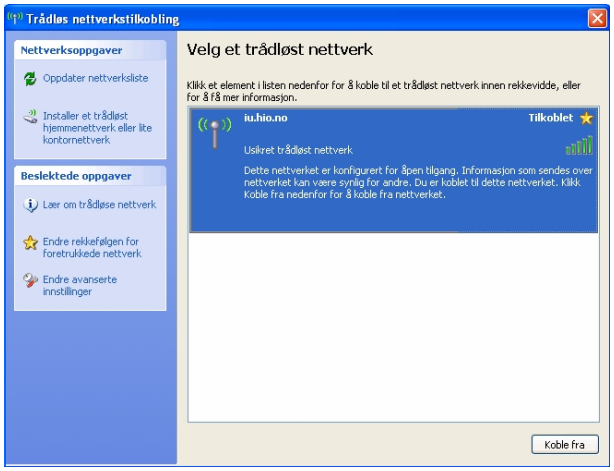
(b) Network topology

Figure 6.4: Web-interface and Network topology

Note: the configuration method used in the interviews is only a possibility among few others. It is surely the easiest one. In fact, the quick installation CD had been created by the manufacturers with the purpose to give the chance to novice users to configure the router through few guided steps. An expert would probably feel more comfortable using a Web Interface, there is more control and the environment is more customizable(Fig. 6.4.a).The subjects had to create the wireless network, as in the model shown in Fig (6.4.b).



(a) List of the networks



(b) List of wireless networks

Figure 6.5: Network configuration windows

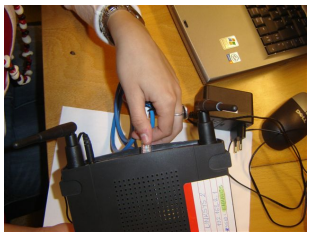
After successfully configuring the wireless router and having create a working WLAN, the subjects had to disconnect the laptop from any cable and they were asked to test the wireless connection by logging into the pre-created WLAN (6.5.a-b) This few steps are not so evident, especially when the subjects do not know a lot the operating system from the administrator point of view. It has to be said also that Windows XP it's not as easy as MAC OS X when it comes to connect to wireless networks. In particular the Windows interface does not ask to the user, to which wireless network he wants to connect. Macintosh OS X system, automatically capture the wireless beacons and propose to the user a list of the available networks. Surprisingly, Windows XP connects automatically to the most powerful wireless signal, without asking any user authorization. This could clearly compromise the security of the system and the user privacy.

Once the subjects were asked to log in into the network, they had to open the net-

work windows and choose one of the wirelesses access points present into the radio range (Fig 6.5.b)
The following section outlines observations made for the four subjects analyzed. The cases will be analyzed afterwards, showing the results and general trends.

(a) The subject reading the quick installation manual

(b) The subject investigating the package



(c) Where does the plug go ?

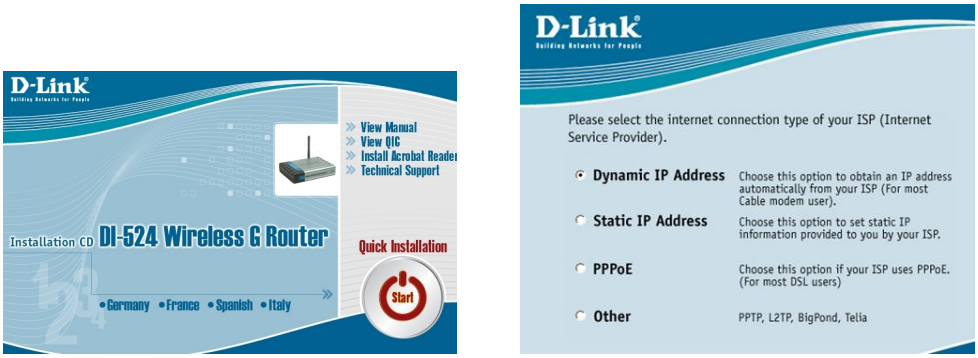
(d) Connection of the routher to the Internet

(e) Configuration process

Figure 6.6: Subject Ruth Calva

6.4.1 Subject 1 Ruth Calva, female, 21 years old, spanish international student

The interview takes place the 27th of March 2006, at 13.45. In the first 5 minutes it is necessary to make the subject feel comfortable with the interviewer and the new environment. It is asked to her what are her feelings and the expectations. She has no idea about the work that is waiting for her but she says she really hopes the experiment will be successful. The subject shows an evident interest in the interview. She rapidly unpacks the package and tries to spread all its components on the desk(Fig.6.6.b). She recognizes almost all the items and she plugs the power supply to the D-Link router. Then she starts reading the manual and expresses the feeling that the illustrations and the plots help her a lot(Fig. 6.6.a).She is happy to find the spanish section in the start-up guide, but she keeps on reading the english instructions.Such a behavior is probably explainable because she masters a good knowledge of the language and because the english section is the first one presented into the manual(Fig.6.6.a).



(a) Quick installation Graphical User Interface - Languages selection

(b) Quick installation Graphical User Interface - Internet connection selection

Figure 6.7: Quick installation GUIs

The plots and the quick guide help her lot to feel confident. She soon discovers the quick installation guides is not enough to configure the WLAN. In fact, it only contains some general information and then states to use the CD of installation.She claims there are no instructions in the manual and she feels lost, she would have liked to be driven more in the initial configuration steps.After 9 minutes from the beginning she has completed to read the installation guide and she has hit the wall(Fig.6.6.b). At that point she's suggested to use the installation CD. The auto start CD opens up a nice installation guide that leads through the process. At this point she notices on the router ports, a yellow label stating that the CD had to be run before starting configuring the WLAN(Fig 6.8.b). The subject feels now unaware of the steps will lead her to the final configuration. The quick installation CD starts automatically and a nice blue GUI (Graphical User Interface) pops up, showing 4 different languages, including Spanish.Fig.6.7.a). Once again the subject continues in English. The GUI leads her through all the configuration of the router. Cables are connected from the router to the University LAN plug and the router is switched on. The wireless laptop is connected to the router as well in order to be properly configured through the interface(Fig.6.6.d). The subject feels now happy and safe to be lead through the configuration. She likes the plots and the colors of the GUI.

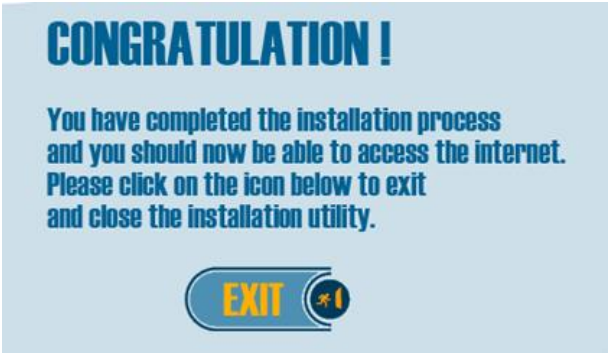
(a) Quick installation Graphical User Interface - Encryption and SSID , captured by the manufacturer's software.

(b) A yellow string,present on the router plugs, advices to run the CD first.

Figure 6.8: Quick installation GUIs

She is disoriented when the author asks what is really happening and which part of the WLAN that is being configured. After 26 minutes, the student starts noticing that the installation of WLAN has successfully been completed and now the CD leads through the important process of the configuration of WLAN. Right away the GUI asks information about the SSID and the frequency channels are going to be used. The subject chooses "Ruth "as SSID name(Fig.6.8.a).The subject feels a little bit disoriented but perseverance is shown during the process. At this point little tips about the meaning of some special initials are given. The subject shows the feeling that the so nice GUI was leading her few minutes before through a well explained installation procedure, is now becoming more detailed and requires a background theory that she does not have. The GUI takes for granted that many acronyms and initials are known already for the user. The subject then chooses the name for the WLAN, and comes to the encryption procedure. There are a few possibilities (None, WEP, 64-BIT or WPA-PSK) (Fig.6.8.a). She says there are no explanations about the encryption, so she thinks aloud saying that she chooses the default one, hoping not to cause any damage to the computer Laptop. Right away the subject is explained what is the encryption of a signal and that in case of a misconfiguration problem, it's not the laptop computer that is going to be damaged, but the WLAN will lack of the overall privacy of every data broadcasted in the air. The subject wonders how comes the manufacturers gives the possibility of choosing for the option "no encryption". She would like to automatically have the safest encryption already activate, without having the option of choosing. It is confusing and creates a lot of doubts. The subject chooses the password "toroloco". The subject has already conducted the interview for 42 minutes now. She has got no idea about the acronyms used in the encryption menu, and she asks information about

(a) Quick installation Graphical User Interface - router reboots , captured by the manufacturer's software



(b) Quick installation Graphical User Interface , captured by the manufacturer's software

Figure 6.9: Quick installation GUIs

such initials. She knows that default choice of "No encryption" is not going to be the safest one, so she chooses the one at the end of the list, probably thinking that they were ordered in an incremental security order. The late standards WPA-PSK, with a relative key word is chosen as encryption and the configuration information are saved in the router, which is going to be soon rebooted (Fig.6.9.a-b).

All the windows are closed and the user leaves the GUI. Now the subject is asked to connect to the created WLAN, but a language problem is soon revealed. The operating system WINDOWS XP is in Norwegian language, so that some help is basic for the perpetuation of the experiment. The browser Internet Explorer is launched but the user notices that no connection is available. She is stuck now. She thinks she should be able to surf the Internet. Few minutes are needed to understand she has only created a WLAN but now she needs to authenticate and login into the network. So she's helped to find the network connection window where it is possible to notice two WLANs, the one it has been just created and the University one(Fig.6.5.a-b). The user successfully connects to the WLAN (authenticating with the password she created) and shows a

congratulation into having been part of the interview. Few important observations are summarized before the interview is concluded:

- Essential theory is missing in the quick installation manual.
- Essential theory is missing in the quick installation CD as well ; this leads the user to not completely understand what the steps that the GUI suggests are. In fact the GUI is not addressed for a public does not know already some theory about WLANs standards. No theory is proposed to help during the installation and the configuration of the router.
- The quick installation CD turns out to be a good idea, with a nice GUI, few languages proposed.
- The user would prefer to buy a router that has an additional manual with some theory about the WLANs and their security standards. She thinks it is a MUST for the company to release products addressed to a wider audience.
- The quick installation manual is for beginners, and it could be perhaps probably better to improve the structure of the manual. A theory manual would be much more appreciated.

6.4.2 Considerations

The interview lasted for 49 minutes in total.The student wanted to have more control of what she was doing, and this is a priority for her. The engineering background influenced her behavior towards the configuration processes. So control and understanding were more important than the final result of 'being connected'. The student was unaware of the threats an open network posed. She believed there was need for information in the manual describing the importance of security matters. Moreover a general thirst for knowledge in this field was clearly shown. She would have liked to know more about the possibilities of customizing and configuring a large scale WLAN. The quick installation manual has deceived her and has probably worsened the perceived importance of what she was doing. Special technical skills where not really required in the configuration of the router through the installation CD. A lack of explanation of the theory is claimed by the subject. She wanted to be more aware of the most common security incidents happening. The subject has surely shown the strongest technical background among all the four subjects.
Below, the subject reports on her impressions of the interview.

Subject declarations

"In the beginning I felt very nervous, because I didn't really know the kind of experiment that I was supposed to do. "

"Then when the interviewer explained me what was it about, I felt very excited because I have never done something like this. However, in the same time I continued feeling nervous because I wanted to do it well. "

"In the moment I had the box in my hands I was very impatient, I only wanted to open it and to start to plug everything, but I talked with myself and I decided to keep calm and to start reading the manual. "

"The manual for me was not very useful, the only thing that it explains clearly was the components inside the package but otherwise it was a graphic, which helped me a lot. It explained how I should connect everything and it made the task easier. "

"Also the CD was very helpfully, I was happy when I saw the Spanish language.
The worst moment where I felt lost was when I had to choose between the different encryptions. The problem for me was that there was not any explanation about it. I knew that I did not want the option "no encryption", but then I had to choose between the others two, the 64-Bit and the 128-bit. Then I decided to choose the safest one, the one with more bit of encryption."

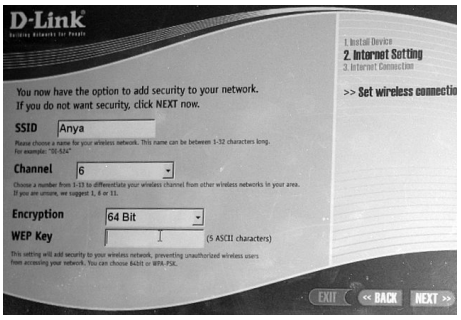
"In the moment the computer had connection, I felt really good, very satisfied with

me, but also I wanted to have more knowledge from the experiment, perhaps other kind of manual could help me more."

"The interviewer was there to help me, but not so much. At the end of the experiment, he explained to me everything, and it looked a lot easier."

(a) The subject being supervised by the author. The subject invetigates the user manual.

(b) The subject invetigates the wireless router.



(c) A screenshot of the quick installation wizard

(d) Where does the plug go?

Figure 6.10: Subject Anya Zhuravkova

6.4.3 Subject 2 Anya Zhuravkova, female, 23 years old, international Russian student

The interview takes place on the 26th of April 2006 at 12.27
She has no problem unpacking and identifying the various items present in the package and spread all its components on the desk. The quick instruction manual is being inspected but she finds it confusing. She states there are too many different languages and only 4 pages for each language.

(a) A screenshot from the quick installation wizard - Visual comparison between the theoretical case and the reality

(b) Wireless router's LEDs - Plug connectivity

(c) Pull-down menu

Figure 6.11: Visual comparisons - screenshots from the quick installation wizard

4th minute: she looks for the Internet LAN plug.
5th minute: she flips through the pages and abandons right away that manual, without have read into it and she focuses on the material in the box. She compares the few pictures of the manual with the material in the box. For few minutes she jumps from a material to another, she does not know how to get started at all! She finally goes back on the manual and she reads through, she understands she has to run the quick installation CD.

H: 12.37, she runs the CD and smoothly start the installation procedure. She notices that the LEDs are blinking, so she stops to be nervous, thinking that it is a good sign(Fig.6.11.b).

The installation CD shows her how to plug the power supply into the router and how the cables have to connect to the devices. She accurately compares the pictures in the GUI with the reality she's facing. 14th minute, 12.41: A picture in the GUI shows a case tower connected to the wireless router and she feels confused.(Fig 6.11.a)Then she understands that in our case the case tower is represented by the dell laptop computer. She continues the installation of the WLAN without any particular problems. It was the first time for the subject to plug in and out some cable and also to see so many LEDs blinking at the same time.(Fig.6.11.b) The installation of WLAN ends at 12.49.Then the configuration of the router starts at 12.52.She is confused about the differences between a dynamic IP address and a static IP address. She definitely has not found any theory about that in the guide, neither such a theory could come from her journalistic background. Few minutes are needed to explain her differences among the different IPs and then the she goes through the process of finding a name for the WLAN.The SSID is chosen without any problems(Fig.6.10.a). In fact she is able to read the little characters that are just below the main pull-down menu(Fig.6.11.c).

Those little words are a fast explanation of the upper menu and help a lot for the understanding of the acronyms. The user elegantly uses this GUI's help and goes on. In fact intuition for her is a good engine to carry on. When it comes to the channel frequency choice, she does not loose control. She checks the different channels frequencies, and observes that the pull down menu is really important for her to have the choice to browse through the items of the menus.She leaves the default channel 6 enabled, because she feels unsure.
32nd minute: Encryption configuration starts. She leaves the encryption disabled, without even browsing through the menu. In fact the encryption menu has NO ENCRYPTION as the default tag(Fig.6.10.a). At this point the subject feels a little bit disoriented but perseverance is shown during the process. A little tip about the importance of encryption is given in order to stress the importance of such a technique. Obviously the language used to define such a policy is simple, and an example in particular is used to make the subject deeply understand the importance of such a technique. The example is about a common language and diversification in languages. If someone does not want to be heard in a private conversation, he can switch into a language not easily understandable by the public. And so encryption works, and it is important to be used regularly.
34th minute: Anya asks an important question about the freedom of choosing or not an encryption standard.
It is definitely not easy to reply to such a question because a big dilemma stays: is the user adapting to the technology or vice versa? Where does the responsibility of an action fall? Is automatism better for the user or is the freedom of choice a right? Is the user responsible of knowing and adapting to the recent technologies? Or, does the technology the technology have to protect automatically the user from threats? People have surely had the option of free choice, but still novices should be lead in detail to a safe path. 36th minute: the password she chooses is "gosha". Right away the subject is explained what is the encryption of a signal, and that the WLAN will lack the overall privacy with regard to the data broadcasted in the air. Also this subject shows the feeling that the nice GUI was leading her few minutes before through a well explained installation procedure, is now becoming more detailed and requires a more detailed background. Now few the few encryption options (None, WEP, 64BIT or WPA-PSK) shock the subject, that wonders again about the fact that the company produces the router gives the possibility of choosing for the option "no encryption". She would like to have automatically had the safest encryption already activated, without having the option of choosing. It is just confusing and creates a lot of doubts. This is the 40th minute of interview and in few minutes the subject will finish the test. Few words to explain what is an ASCII character and the late standards WPA-PSK is chosen, with a relative key word and the configuration information are saved in the router, which is going to be soon rebooted(Fig.6.9.b).

(a) Password field.8-63 ASCII characters

Figure 6.12: ASCII - Hexadecimals password system

Note: The subject has some sometimes difficulties to choose the right length of the password and the digits type (ASCII or hexadecimal). In mathematics and computer science, **base-16, hexadecimal**is a numeral system with a radix or base of 16 usually written using the symbols 0-9 and A-F or a-f.(Fig.6.12.a) It allows the user to choose a password made of numbers and letters, while the ASCII method cannot allow the use of numbers. When users enter the pre-shared key as ASCII or hexadecimal characters it is important to know to differences.If they enter the key as ASCII characters, they have to enter between 8 and 63 characters, and the access point expanded the key using a special process, password based *described in the Password-based Cryptography Standard (RFC2898).*[30] If they enter the key as hexadecimal characters, they have to enter 64 hexadecimal characters, which is, perhaps too long to be remembered[31]. 42 minutes since the beginning of the interview have already pasted.All the windows are closed and the user leaves the GUI.

H: 13.13: the subject asks if the CD should be taken out of the laptop. H: 13.14: Investigator asks: Are you a tidy person? She says she is and she put the CD back into the envelope

Now the subject is asked to connect to the so-created WLAN . The operating system WINDOWS XP is in Norwegian language but the user does not really need any special help, she masters alone to perpetuate the experiment. The browser Internet Explorer is launched but the user notices that no connection is available. She is stuck now. She thinks she should be able to surf the Internet. She's been asked: why do you think you cannot connect to the network? She replies she cannot because there is any page available. Actually this is a consequence. Few minutes are needed to understand she has only created a WLAN but now she needs to authenticate and login into the network. She thinks aloud that at the end of the quick installation CD it was not explained how to connect to the WLAN after its configuration. So she's helped to find the networks connection window where it is possible to notice two WLANS, the one it has been just created and the University one.(Fig.6.5.a-b) The user successfully connects to the WLAN (authenticating with the password she created) and confesses that without the installation CD she would have never been able to create such a WLAN network alone.

Considerations

The interview lasted for 58 minutes.The student felt she wanted to have more control of what she was doing, and this was a priority for her. The journalistic background did not help a lot in such a technical experience. She wanted to be aware of the security threats and access control of the network. She understood that such issues are more important than the final result of 'being connected'. The student was unaware of the threats an open encryption would have caused. A lack of explanation of the theory is claimed by the subject. She wanted to be more aware of the most common security incidents happening. At this point few questions are made by the interviewer (I) to the subject (S):

- (I): Do you use or would you the Internet WLAN for banking purposes?
  (S): Probably !
- (I): Would you use the password to configure a WLAN again?
  (S): Sure I need it.
- (I): How often would you change your password?
  (S): I use to keep alwais the same, perhaps I would like to change it once a year.
- (I): If you install the same WLAN at your place, can your 'brother' connect to the WLAN with its own laptop? Does he need a password also?
  (S): He can connect only if he gets the password.
- (I): Would you see the traffic mixed somehow on the screen?
  (S): She feels embarrassed, she smiles, no reply given.

She concludes saying: "anyway I'll buy it (a WLAN router) soon, it's really useful!"

(a) The subject installs the WLAN

(b) Difficult moments: the subject is stuk

Figure 6.13: Subject Mari Mehlen

6.4.4 Subject 3 Mari Mehlen, female, Norwegian, teacher at the faculty of Engineering at HIO (University Oslo College).

The interview takes place the 5th of May 2006 at 12.27 in an administration office at the HIO. The subject does not present any problem unpacking and identifying the various items present in the package and spreads all of the components on the desk. The subjects does not present any sign of tension or stress for the interview. She says ”I will not read this manual until I have to ”. The subject obviously shows a reject of the reading part and an antipathy for the reading manuals (later it will be discovered some dyslexia in the subject). The first thing she does after unpacking the package is to detect all the items that are inside the box. On the back of the router, on the LAN ports, she finds a yellow string saying ”RUN THE CD FIRST ”(Fig.6.8.b). She does believe it was really important to find such an indication that advice to run the CD first. She opens the CD and put it into the Dell Laptop. Obviously she believes it is an installation software CD. Soon she discovers any software has to be installed and there are no windows with the icon ”next ”to click on. So when she realizes that an installation guide has opened she starts reading the quick installation manual. She flips through the pages and abandons that manual right away. The subject seems to be in hurry for something, as if she was in time competition. She reads the installation manual in english, and it takes few seconds for her to abandon it. She does not show any interest in the ”reading part”.She’s aware now of the fact that the CD will lead her through the process of installation and configuration of the router and she has not to use it to install any special software. After 4 minutes from the beginning of the interview she starts to be driven in the process by the installation CD. She connects the Internet cable from the LAN to the router but she does not understand what we should do with the second cable. We suggest giving a look again to the picture and then she understands that the second cable will connect the router to the Laptop. She asks why it is so important to check that LEDs are blinking , and it is replied that it is needed to check if the cable are broken for example or if there is an active connection between the Internet and the router or between two peripherals.8th minute: She has

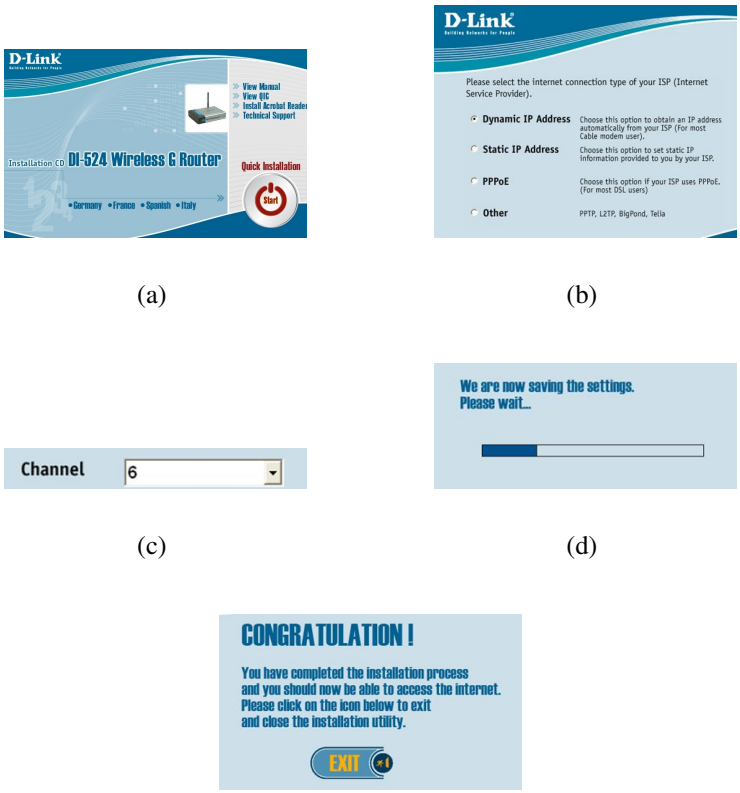
Figure 6.14: Subject during the installation process

some problem to realize that the Internet, the external world is represented by the little LAN plug that was on the wall.

11th minute: the cable presents two different colors and she does not know what color to use.

18th minute: She ends the installation of the cables and the setting up procedures that will lead her through the configuration of the WLAN.

She does not have any clue about the dynamic or static IP addressing steps.Since the interview takes place into an office of the HIO, and not in the usual lab room (as in the previous experiments), the subject is assisted in manually configuring a static IP to assigned to the LAN(Fig-6.7.b).She does not know anything about the SSID and the channel frequency. In fact she accepts all the default values. When it comes to the encryption of the signal, she chooses willfully to set no encryption for the WLAN she was going to create. Her point of view is clearly stated: ”I think the people working here are taking care already of the security, so I would just like to leave it without any encryption ”. The author replies that she should try to imagine such an experiment as it was at her place and then an interesting reaction of the subject takes places. She goes back to the previous configuration page and she starts to read again and choose a name for the network, the SSID and the channel frequency(Fig.6.8.a). Then when it comes to encryption she shows to know what that was for and that it is needed a kind of encryption when you use a network not in an already controlled environment, as the HIO. She does not know the differences between the different encryption standards, WEP, 64 Bit, WPA-PSK and she shows an interest in knowing more about this standards. A little ”break” is taken to explain her that the WEP is a deprecated security standard and that it has been hacked years ago already. We advice her to choose the latest standard: the WPA-PSK. Then she asks: ”Is it me who should choose an encryption key and a password? Should I then remember it? ” .



(a) (b)

(c) (d)

(e)

Figure 6.15: Configuration process: The most important GUIs lead the subject through the process. Screenshots are captured from the manufacturer's software

The first attempt of choosing a password is unsuccessful, the password is not accepted. She notices that she cannot write alphanumeric digits, but just ASCII, so changes the password back. The changes are saved in the router and then the router reboots.(Fig.6.15.d)

27th minute: she's been asked: "Do you like such an interface and such an installation procedure from the CD?" The subject replies that in the beginning she is instructed that she has to install a program on the computer, and that is the reason why she was not reading the manual and just focusing on installing the CD. She believes that it would be helpful if it was expressly stated by the firm to read the manual.

35th minute: the WLAN is well configured with a strong encryption and a unique name.

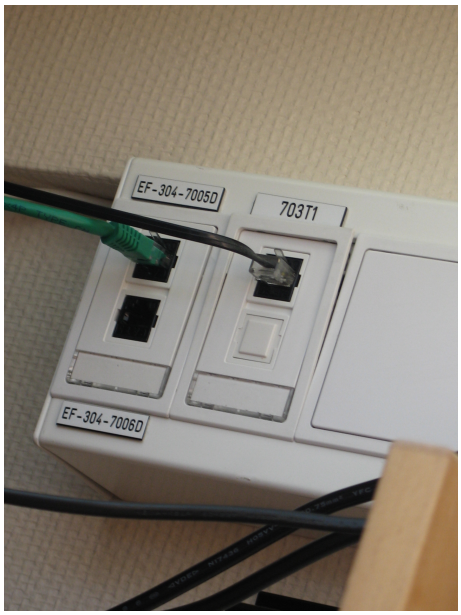
37th minute: When it comes to connect to the WLAN, she manages to find the network connections and she has no problem in the using the operating system in Norwegian. She gets connected to the WLAN but is not able to 'surf' on the Internet because we discover that the system administrator has disabled the connection from all

MAC addresses which are not registered. Such a policy is obviously taken for security reasons. This is explained to the subject.

The author asks:" Do you feel secure to use the Internet here at work?"

The subject replies:" Yes I do, people working here are taking care of the security."

The subject asks:" How can I know my IP number and who is giving it to me when I am at home? "



(a) Internet plug at HIO

Figure 6.16: Are the numbers on the IP's of the clients?

The subject asks:" what is a PPP (Point-to-Point Protocol) and what is a DSL connection? "

The subject asks:" Is it there a way to find the IP, the subnet mask and the main gateway and the names name server looking into the computer ? Is this information on the computer?

The subject asks: "If I am at University, is my IP that number that is shown on the plug? (Fig.6.16.a).The subject has problems in understanding that number available on the plug is not at all the IP number assigned to the computer.A reply is given to all the questions and.The author concludes: "How would you install it at home if you would not be able to manage it alone "?And then, "Would you call a technician "?

41st minute: She replies: "I would read through the installation guide book then! "

Figure 6.17: Subject Jorunn Fergus. Installation process

6.4.5 Subject 4 Jorunn Fergus, female, Norwegian, senior adviser at the faculty of Engineering at HIO (University Oslo College).

The author asks:" Do you have any idea what are we going to do?" The subject replies:" I have an idea, but that is about all!".The first minutes are useful to make the subject feel at ease. Once the package is unpacked, the subject starts right away to read the installation quick guide.She does notice that there is also the Norwegian language, but she does not mind at all, she just keeps on reading the English part, probably because it is the first one offered on the guide. Several minutes are taken to carefully read the few pages in the manual, and to get acquainted with the items in the package. She reads loudly and she thinks aloud also, showing a nice mood, and a positive attitude towards the interview taking place. She starts to spread out on the desk all the items and to detect all the functionalities of each item. She connects the router to the power supply and switches on the Laptop. She asks if it is normal LEDs are blinking on the router. 9th minute, she runs the CD and the GUI comes up. She likes the interface and it gives her a sense of safety. She detects the WLAN ports on the router, with the different numbers and connects the cable from the router to the Laptop. She is not sure if the blinking lights are a good sign or not. She says that the LEDs of the router the son has at home are blinking all the time, so it should be fine if they are blinking. She reads the CD guidelines then she notices that the lights blinking are a good sign! The next 5 minutes are used to compare the pictures on the guide to the items at hand,

and to connect all the hardware together through the cables. Once everything looks connected and ready, she clicks on the NEXT button on the GUI. An error message pops up, and she needs few seconds to understand that the cables were connected to the wrong ports. So she switches the cables behind the router, giving to the possibility to the router to be configured. In fact, the case is that the Laptop's cable is plugged into the INPUT line of the router when the Internet cable is supposed to be connected, thust it was impossible to configure the wireless router. It is important to remark that the first router configuration has to be done through the cable procedure. Once the router is configured and the user has administrative privileges on it, then it is possible to reconfigure or modify settings even only with the wireless connection.

15th minute: everything is well connected and the installation of the router has ended. The subject starts the configuration procedure and she confirms she has no idea about the dynamic and the static IP configuration(Fig.6.15.d). She leaves the default configuration, the dynamic one and she continues to the next page, where she chooses the name for the wireless connection. She is not sure if such a name should be a difficult name or an easy name. In fact, the novice users are aware of the fact that a strong password can be more effective than an easy one, but perhaps sometimes they mixed concepts. In this case, probably the SSID was mixed with the secret password.
24th minute: The SSID chosen is "jorunnf". The channel frequency is left as default and the encryption is choose on purpose , because the subject says she is going to use the Net bank , which is a service Norwegian banks offer to the customers in order to login from remote to a bank service , giving the possibility to carry out the usual banking operations. The subject declares to have no idea about encryption standards and the interviewer explains to the subject the differences among the different standards and the strength in number of bits. She uses the one that has the biggest number of bits.

34th minute: The author asks:" where all this data are going to be saved? " The subject replies:" on the diskette isn't it or on the router." The procedure ends successfully and the data are finally stored in the router, which is rebooted. 37th minute: Internet connection procedure starts.

The author asks:" do we still need the cables ?" The subject replies: "I should not, because the connection is wireless " The author asks:" All the cable?" The subject replies:" yes, it is wireless "

The subject thinks that also the cable connecting the wireless router to the Internet should be unplugged, because the connection is surely a wireless one and this means that no cable should be needed.

The author asks:" Where do you think the router can get the connection?" The subject replies:" Well, at home at least it is connected to the incoming telephone line."The mistake is explained to the subject through few practical examples.

43rd minute: The user runs the IE browser to check the connection and the connection does not work.The user goes back on reading the quick installation guide, but in vain. The author asks:" how would you connect to a wireless network, in your home, at the University?" The subject replies:" Should not it be automatically?"

The standards procedure is explained to the subject. The network connections are opened and the wireless nets menu are shown on the screen , the one from the University (an open one , not encrypted) and the one she made , HOME, encrypted with 128-Bit , WPA-PSK.The user clicks on the HOME network and a password is asked. The user has not idea about which password it is.This shows an important common aptitude of novice users towards technology.They do not make any difference between the user side and the administrator side. In fact the user does not know that the passwords she creates and stores in the router, are the one she has to use to authenticate to the WLAN she has created.She types in the password, she confirms it, and the connection then is successfully. The user took 52 minutes to be connected.

At that point few other questions are made by the interviewer:

- What is this list of wireless networks with the names aside? What they represent?
  (S): We have two networks here, the University one and our, the one we created.

- (I): In which one would you feel safer, the University network or the one you created? (It has to be remember that the University WLAN did not have any encryption enabled)
  (S): I would feel more secure in ours, because we use a strong encryption and then there is the lock that means it is a secure network.

- (I): Should the university technicians use any encryption?
  (S): Yes definitely, I hope they will do that, because otherwise I will use my network I created now.

- (I): Do you use or would you the Internet WLAN for banking purposes?
  (S): Yes, why not, if it works!

- (I): Would you use the password to configure a WLAN again?
  (S): Sure, I need it.

- (I): How do you feel now that everything works?
  (S): I hope I learnt a little bit.

- (I): If you would not be able to install a WLAN alone, how would you do?
  (S): I would try to persevere.

The user lastly states that the terminology it is used in the manuals and in the quick installation CD guideline is not so clear, and she is not familiar with it. She thinks it is interesting to learn how to use computers and she will start soon.
The interview totally lasted 57 minutes.

Chapter 7

Discussion

The subjects had no problems in unpacking the contents of the wireless router package. The process of identifying the various items was varying from subject to subject. One of the subjects took quite long time to detect and understand the function of each item. It is understandable that the first time such a set of technical items are discovered, it takes few minutes to get acquainted with all the different objects.

7.1 Installation Process

Two of the subjects complained about the scarcity of explanations in the manual, while one was found to be happy about its existence. Only one subject showed not interest at all about the manual. In fact, she was trying to avoid as much as possible the reading part. Besides, the quick installation CD contained a lot of useful pictures and graphs that helped during the configuration procedure. Everyone has found that interesting. Subjects were lead through the configuration process, by having the possibility of making visual comparison among illustrations schemes. One of the subjects was confused by the visual comparison, as the illustration showed the case tower of a PC instead of the Laptop Dell used in the interview. Abstraction is common capacity that, with fantasy, gives birth to art. However, novices are more willing to stick to the rules! It should be left no possibility of perplexity and abstraction to novice users, manuals should not give any possibility of confusion!The unique plaint is regarding the lack of sufficient background theory and explanations of technical terms, acronyms and initials.Three of the subjects quickly identified the quick-start installation CD, by reading the installation manual or by noticing a yellow string on the back of the wireless router, giving the warning: ”Run CD First ”. Only one of the subjects had problems in detecting the quick guide functionality of the CD, thinking that the CD was meant to be used to install some software. Subjects generally appeared confused about how things had to be connected, showing a sense of panicking. In fact, the function of each item present in the package was not evident. Then, **three** of the subjects left the crossover

cable plugged into the laptop, after the configuration of the router and **one** of them , motivated such a choice by stating that the router needed to be not plugged anywhere, because the connection was wireless and subsequently no cables are needed for such a technology. After the installation process, a few problems were encountered also in the configuration process.

7.2 Configuration Process

Users had to choose a SSID, although no explicit explanation of these initials was provided. Three of the subjects had chosen its own name as WLAN SSID, or the world "HOME". Only one of subjects skipped that choice, by leaving the default SSID. The next step was the choice of the channel frequency and the encryption options. All subjects left the frequency channel to default. It was a choice suggested by the interviewers. In fact, the privacy of information about the specific of configurations of the University WLAN left no possibility to use different radio channels than the auto default one, which audits possible packets drops and tunes up automatically, by searching for a "clear channel". During the choice of the encryption standards, the biggest level incertitude affected the interviewed. The choice of encryption standards were the following:

- No encryption (Default)
- WEP
- 64-Bit
- WPA-PSK

None of them had any explanations of the acronyms, neither the impacts nor the consequences they could have provoked on the network privacy.

It is important to notice that such a quick installation CD has been made on purpose to lead novice users through a semi-automatic configuration process, and it tries to leave them with as few choices as possible. Deprecated wireless standards and no encryption should have been not mentioned, with an exception to for the Web-Interfaced configuration process (reserved for advanced users).

One of the subjects left the default 'no encryption' choice activated. This subject, once warned of the possible risks related to such a choice, opted for a strong encryption mechanism.

All subjects asked why the manufacturer of the wireless router used such an encryption method available and it was replied that is a policy chosen to preserve the user's freedom.One possible explanation to the fact that the manufacturer gave the possibility of choosing the 'No encryption' standard, was the possible to aid in the installation of net device on a network containing old machines.

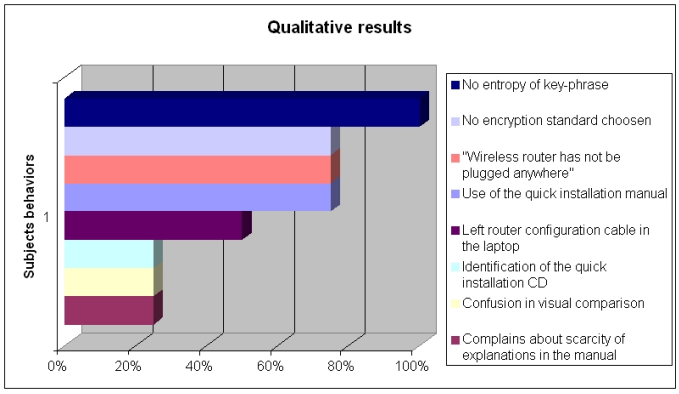
7.2.1 Related topics and possible manufacture policies

Modern computers have a strong computational power. Old machines can run out of resources when big encryption mechanisms are activated. Strong encryptions (from 32 to 128 or more bits), augment the clock cycles and the CPU load of the client and in certain cases it has been showed that the CPU is also over heated[8].Another possibility, more unlikely than the first one, would be that the manufacturers gives the possibilities of using No encryption methods (or deprecated ones), because they are faster to configure and they do not require any authentication procedure on the clients side.Once the subjects were lead to choose the strongest encryption standard, a key-seed had to be chosen. The subject had some difficulties to choose the right length of the password and the digits type (ASCII or hexadecimal).Such a key-seed would have been transformed by the router, in an authentication password the user had to use to connect to the WLAN, later on.The key length varies depending on the number of bits needed for the encryption, so the users had slight differences of response for each of the standards.It was a little bit confusing, anyway, to have the possibility to choose between ASCII and hexadecimal characters.Few words are needed to explain what an ASCII and hexadecimal character is.When they entered the pre-shared key as ASCII or hexadecimal characters it was important to know the differences. If they entered the key as ASCII characters, they had to enter between 8 and 63 characters, and the access point expanded the key using a special process, password based (described in the *Password-based Cryptography Standard (RFC2898)* [30].

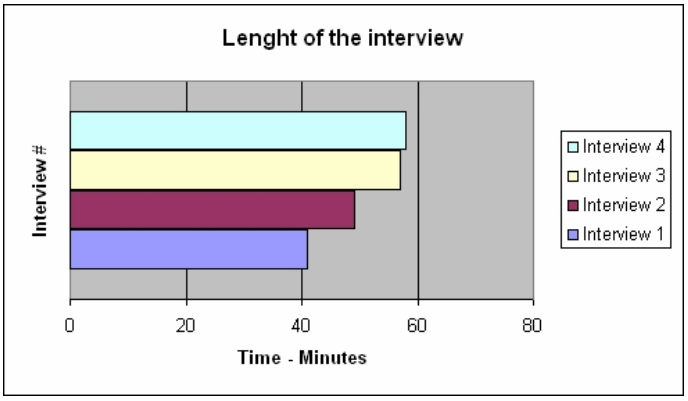
If they entered the key as hexadecimal characters, they had to enter 64 hexadecimal characters, which it was too long to be remembered.

all subjects selected a password made of ciphers (not numbers) showing a weakness (small entropy) in such a choice 1 of them declared to have never changed its login web mail password in 1 year.

Upon completing the installation, the subjects should have to disconnect the laptop computer from the wireless and then test the wireless network. No instructions on how to do this was provided. The entire group of subjects tried to connect to the WLAN using the Internet explorer browser, but obviously in vain. No instructions about how to connect to the WLAN was provided. The user had explicitly be told to connect to the WLAN by selecting the SSID in the in the wireless network list and then to authenticate through the password they created. 1 of the subjects did not know which password to use in the authentication interface. In fact they did not remember that the password they created during the configuration process would have needed in the authentication.



(a) Most common mistakes, and insecure habits



(b) Time users needed to make a working WLAN

Figure 7.1: General trends - Qualitative results.

7.3 General trends

The Fig.7.1.a shows the most common mistakes novice users perpetrated , when installing the WLAN.

Surprisingly, all the users have been choosing a password with a low level of security (the password did not contain any numbers or capital letters).
Unfortunately, a total of three users did not choose the signal. Although the GUI is configured with a default "'no encryption"' , it gives the possibility to choose between different encryptions models.

Of the most ambiguous security practices, the 75% of the subjects left the router cabled to laptop, after successfully have configured the WLAN.

Reasssuringly, only one subject had problems in visual comparison between the installation manual and the reality case.

All subjects think they could never have made it without the guideline CD.

Fig.7.1.b shows the time novice users deployed to install a WLAN from scratch. All the subjects had set up the WLAN in a time range of 40-60 minutes.Such a reassuring result, is partially influenced by the presence of the author during the interview.

In summary the installation and the configuration procedures suffered from the following general problems:

1. The subjects had too little background information to understand the terminology and acronyms used to configure the router
2. The quick paper manual did not represent a valid help, although the 75% of the subjects used it.
3. Half population complained about the scarcity of explanations in the quick installation CD manual.
4. The users were presented with too many choices, and too many instructions, to complete, didn't have time to understand all the decision they were making
5. The quick guide CD did not help the users, beyond installing and configuring the router.They had difficulties in understanding all the acronyms used today and the differences in technologies.
6. All the users chose an "easy password", without alphanumeric digits (hexadecimal)
7. The router was unplugged from the Internet LAN, because wireless technologies work without any wires.
8. The laptop was used with the configuration cable, used with the router.

Chapter 8

Conclusion

The results suggest that most users have insufficient knowledge about wireless network security to be able to install and configure a secure WLAN, even with the help of specific helping software.
Differences could also be attributed to gender and age. In particular, males are more confident about their wireless security knowledge than females, while females are more likely to seek professional help. Will females therefore end up with safer wireless networks than males?
There is clearly much to be desired from the wireless communication equipments manufacturers. The provision of quick-start help program is a good initiative, but these must be very simple, leaving no choice for the user in terms of security policy. Best practices should be followed to strengthen security. In addition, it should also be possible to configure the router for advanced users. One cannot rely on users to adapt to recent advances in technology - instead the technology must adapt itself to the users. One solution would be to preset the wireless routers with a high security setting such as WPA as default, where the device is given a unique random SSID and a random password, also provided on a piece of paper in the packaging. This would perhaps increase unit costs, but would greatly improve the security for novice users. Impatient novice users would then be able to immediately deploy relatively secure wireless networks in their homes. Contrary to the opinions of many, it is possible to create secure WLANs , but like any other IT system or network, they take time, study and proprer planning.Current security tools,if properly deployed, offer a robust protection against possible threats. It is only by imporving the knowledge and to educate the users that we can improve security and achieve secure cummunication on WLAN networks.Following secure measures to prevent WarDrives is a must.
With carefull planning and due diligence, a wireless network can be as secure as a wired network.

There are more of them than us, so we have to work smarter and harder than they do.

Bibliography

[1] WLAN Systems Lead Wireless Market Growth.
http://www.highfrequencyelectronics.com/archives/jul02/hfe0702-techreport.pdf.

[2] WLAN Security Threats and Senior Consulting Engineer Cisco Systems Brussels Belgium Solutions, Franjo Majstor.
http://csdl2.computer.org/comp/proceedings/lcn/2003/2037/00/20370650.pdf.

[3] Airwave, Gartner Group Wireless LAN's, and HIPAA.
http://airwave.com/docs/brochures/amp-hipaa.pdf.

[4] Go Wireless: Open up new possibilities for work and play.
http://h20331.www2.hp.com/hpsub/downloads/356395-001-web.pdf.

[5] Intercepting Mobile Communications: The Insecurity of 802.11.
http://www.isaac.cs.berkeley.edu/isaac/mobicom.pdf.

[6] R.A. "'Australian Attitudes Towards Intervention into Hacking"' Coldwell. Communications of the acm, november 1995.

[7] Robert E. Mahan Sans Institute : Security in Wireless Networks.
http://www.sans.org/rr/whitepapers/wireless/157.php.

[8] An Intrusion Detection System for Battery Exhaustion Attacks on Mobile Computers.
http://scholar.lib.vt.edu/theses/available/etd-05252005-140924/unrestricted/dcn-etd.pdf.

[9] Itsik Mantin Weaknesses in the Key Scheduling Algorithm of RC4, by Scott Fluhrer and Adi Shamir.

[10] et al. Security in the wild: user strategies for managing security as an everyday practical problem. Pers. Ubiquit. Comput. 2004. 8: p. 391-401. Dourish, P.

[11] May 5 2003 CyberScience Lab Report: Security Threats to the 802.11 Wireless Network.
shttp://www.nlectc.org/pdffiles/security-threats-to-802.11-networks.pdf.

[12] Y. BZahur, Wireless LAN security A. Yang, and 2003. 19(3): p. 44-60. laboratory designs. Journal of Computing Sciences in Colleges.

[13] W.C. Summers Bhagyavati and USA: ACM press A. DeJoie. Wireless Security Techniques: An Overview. in InfoSecCD Conference '04. 2004. Kennesaw.

[14] Wikipedia:IEEE 802.11 Security
http://en.wikipedia.org/wiki/802.11.

[15] WarDriving with NetStumbler
http://www.netstumbler.com.

[16] WarDriving with WarLinux
http://sourceforge.net/projects/warlinux/.

[17] Aircrack. Devine, C. http://www.aircrack-ng.org.

[18] Borisov Intercepting Mobile Communications: The insecurity of 802.11 and Wagner.

[19] SANS Institute 2002: A guide to Wardriving and Andrew Etter. Detecting Wardrivers.

[20] System Experts: Wireless 802.11 Security: Questions and Answers to get started.

[21] SANS Institute 2004: Securing Your Wireless Access Point: What all those settings mean anyways ?
joe scolamiero, 4/20/04.

[22] Keng Hoe. SANS Institute 2005: Security Guidelines for Wireless LAN implementation.

[23] A. Whitten and Colorady. J.D. Tiger. Why Jhonny can't encrypt: a usability evaluation of PGP 5.0. in 9th USENIX security symposium. 2000. Denver.

[24] A. Adams, Users are not the enemy: why users compromise security mechanisms M.A. Sasse, and 1999. 42(12): p. 40-46. how to take remedial measures. Communications of the ACM.

[25] M.A. Sasse Adams, A., P. Lutt. Making passwords secure, usable. in HCI'97 conference on people, and UK: Springer. computers XII. 1997. Bristol.

[26] A. Newell, Mechanisms of skill acquisition P.S. Rosenbloom, the power law of learning. In Cognitive Skills, and Editor. 1981 L. Erlbaum Associates. p. 1-55 Their Acquisition, J.R. Anderson.

[27] Gender differences in way-finding strategies: Relationship to spatial ability Lawton, C.A. and 1994. 30(11-12): p. 765-779. spatial anxiety. Sex Roles A Journal of Research.

[28] Wireless Coexistence Probability of BT WLAN Collision: IEEE P802.19. http://www.ieee802.org/19/pub/2006/19-06-0021-00-0000-probability-of-bt-wlan-packet-collision.doc.

[29] Cover Story: ARP spoofing and Traffic Tricks poisoning. https://www.linux-magazine.com/issue/56/arp-spoofing.pdf.

[30] Password-Based Cryptography Specification. http://mirror.switch.ch/ftp/doc/standard/pkcs/pkcs-5v2/pkcs-5v2-0a1d1.pdf.

[31] Cisco IOS Software Configuration: Configuring Authentication Types. http://www.cisco.com/univercd/cc/td/doc/product/wireless/airo1100/accsspts/i1232ja/i1232sc/s32auth.pdf.

Chapter 9

Appendix A

University Oslo College
Survey

1. **Please state your sex**

☐ Male ☐ Female

2. **Please state your age**

☐ 15-20 ☐ 31-40
☐ 21-25 ☐ 41-50
☐ 26-30 ☐ More than 50

3. **Nationality : _____**

4. **What is your profession ?**

☐ Student ☐ Unemployed
☐ Employed ☐ Other_____

5. **How often do you use the Internet?**

☐ Every day ☐ Never
☐ Once per week ☐ Do not know
☐ More than once per week

6. **Are you an expert Internet user?**

☐ Yes ☐ No
☐ A little ☐ Do not know

7. What is a WLan?

☐ A network that allows wireless data communications
☐ A way of connecting to the Internet with a Laptop
☐ A new telephony 3G standard technology, as Infrared and Blue Tooth
☐ An electrical phenomenon that takes place when charge accumulates on antennas
☐ Do not know

8. Are you aware of today's most common security threats in WLan ?

☐ Yes
☐ A little
☐ No
☐ Do not know

9. Wireless communication over the Internet is safer than communication through cables?

☐ True ☐
☐ False ☐
☐ There is no difference between a cabled and a wireless communication
☐ Unsafe only if I don't use a firewall
☐ I do not know

10. Have you ever tried to install and/or configure an home WLan?

☐ Yes
☐ Yes many times
☐ I tried but I failed
☐ No
☐ I am not interested
☐ I do not know

11.What do you need to set up a home Wireless connection?

(You can select several items)

☐ One ore more antennas
☐ Any cable
☐ Any wireless computer
☐ Internet wired connection
☐ A 100 MBit cable LAN
☐ One or more cables
☐ An ISP (Internet Provider)
☐ Other_____
☐ Wireless Router
☐ A Laptop
☐ I do not know
☐ Any wired computer
☐ Router
☐ A TX-RX Plug

12.What do you do if you have any difficulties configuring a home WLan?

☐ Give up and pay a technician to do the job for you
☐ You keep trying until you succeed
☐ Give up and call a friend that knows how to do
☐ Do not know
☐ Give up and think the instruction manual is faulty or not well written
☐ Other_____

13.What are the major disadvantages of an unencrypted traffic?

☐ The connection is slow
☐ Viruses could easily get into my computer
☐ The computer starts to overheat
☐ Someone could take control of my computer
☐ Anyone could read my sensitive informations
☐ I do not know
☐ Other_____

14.Are you aware of the security threats happening within WLan Networks?

☐ No I do not know
☐ I know some of the problems
☐ I would like to know more about them
☐ Yes I am an expert
☐ It does not interest me

15.Security breaches over Internet WLAN are caused by:

☐ Bad weather and loss of signal in the air waves
☐ Lack of supporting safe technologies
☐ Hardware that overheat
☐ Bad overall security policy
☐ I do not know
☐ Old computer model
☐ Other_____

In the following question you have to imagine yourself in such a scenario :

Scenario : You want to buy an airplane ticket to Australia. You access your Bank over the Internet and verify your balance. You buy the ticket using your credit card number.
A few days later,you notice that your card has been used overseas, but you never traveled abroad...

16.Which of the following could be a reasonable cause ?

☐ Banks can make mistakes, no one has used my money abroad ☐ Someone has stolen my credit card number and used it without any authorization
☐ I do not know
☐ Other_____

17.Which of the following elements make you feel safer when you use an Internet wireless connection?

☐ A Macintosh computer ☐ A modern laptop
☐ Using a VPN tunnel client ☐ I don't know
☐ An encrypted connection WEP
☐ An encrypted connection WPA)
☐ Connecting from the University Wireless
☐ Having an user name and a password
☐ Newest version of Microsoft Windows XP (with the service packs included)
☐ Other _____

18.A Wireless security breach is caused by:

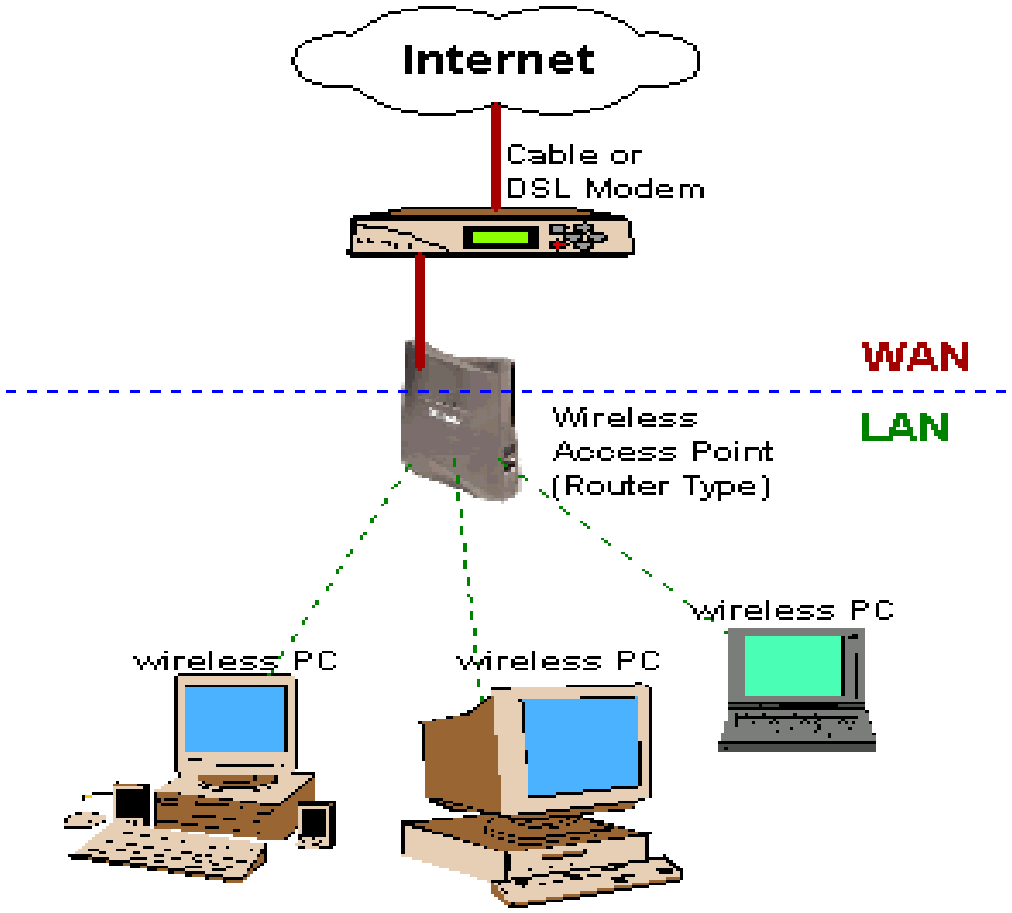
☐ A hardware problem
☐ Both hardware problems and human error
☐ The misconfiguration configuration of the network
☐ An human error
☐ I do not know
☐ Other _____

TEST

19.Are you willing be part in a real-life experiment that could improve your knowledge in how to secure a WLAN network?

☐ Yes
☐ No
☐ May be

20.What is the weakest point of the following network :



☐ The Internet
☐ The cable ADSL modem
☐ The wireless access point
☐ The group of Wireless clients
☐ The Wireless Laptop
☐ I do not know
☐ Other_____

Additional comments

_____
_____
_____
_____
_____

Chapter 10

Appendix B

User Awareness and Attitude to Home WLAN Security: Effects of Gender and Age

Frode Eika Sandnes and Ugo Santucci

Faculty of Engineering, Oslo university College,
P.O. Box 4, St. Olav's plass, N-0130 Oslo, Norway
frodes@iu.hio.no

Abstract. Recent advances in technology and efficient manufacture has lead to the wide availability of low cost wireless networking equipment. An increasing number of households are acquiring wireless networks. The low cost and convenience of not having wires around the house is appealing to users who want a tidy and clutter-free home environment. Simultaneously, there has been a growing attention towards security in wireless networks – both home networks and public networks. However, at the time of writing there is no recorded study of user attitude and knowledge about securing wireless networks. This study sets out to fill this gap through a quantitative and qualitative investigation. This study addresses wireless security with respect to age and gender. The results suggests that wireless equipment manufacturers can contribute to overall wireless security by providing simple security oriented user interfaces where options that violate best practices are hidden from the users.

Keywords: wireless security, user awareness, user attitude, wireless network management.

1 Wireless technology and convenience

An increasing number of households around the world have access to the Internet and many of these have some form of broadband access [1, 2]. Recently, WLAN (wireless local area network) equipment has become very affordable, fast and reliable. WLAN equipment include wireless routers which can be purchased for around 50 US$ (at the time of writing), and wireless networking interfaces for computers for around 10 US$, such as WLAN USB-sticks, WLAN PCMCIA cards, or WLAN PCI cards.

The WLANs are attractive for a number of reasons. The absence of physical wires is both aesthetically pleasing and convenient. The average home has limited space and its residents usually want a homely environment different from the office and not cluttered by wires. The lack of wires means that equipment can be placed nearly everywhere and the range of current wireless routers is sufficiently large to cover an entire apartment, including all its rooms. Speeds of 56 Mbps and more are common even for entry level equipment. Such data-rates are more than enough to support several users, with the exception of heavy-duty multimedia-processing.

Most of the wireless routers that can be bought today will work straight out of the box. This is convenient for most users who expect immediate deployment of their newly acquired equipment. If one walks around a residential neighbourhood with a WLAN enabled device, such as a PDA, it is common to se WLAN access points with the SSID “default”. Such SSIDs indicate that the router is simply connected to the nearest internet socket provided by the ISP (Internet Service Provider) and all default wireless router settings are used. The default is to impose no security (with the exception of the SSID itself which indicates to the client which access point it is connecting to). The consequences of this lack of security can be severe.

1.1 Wireless security threats, hacking tools and remedies

Recently, there has been focus on wireless security, and much have been written about WLAN security [1, 3]. The main issues include unconsolidated eavesdropping, denial of service attacks and man in the middle attacks [1]. With unencrypted traffic anyone within range of the WLAN network is able to eavesdrop on the communication and record all the contents. This is obviously not desirable when communicating sensitive information, such as credit card numbers etc. Furthermore, with an open network anyone within range can potentially access all the computing resources on the network, such as inspecting contents of files, e-mails, etc. Finally, perhaps the most severe threat is identity theft whereupon someone in range can pretend to be the user and do various illegal transactions such as downloading child pornography, etc. The owner of the network will be accountable as it is the owner’s Internet line that has been used to commit the crime.

To overcome these problems most routers are equipped with a set of security mechanisms. Encryption is used to prevent eavesdropping and authentication is used to limit access to the network. First generation WLAN equipment was equipped with WEP (Wireless Equivalent Protocol) which is considered unsafe. Second generation equipment are equipped with WPA (Wi-Fi Protected Access) which is considered safer than WEP, but still has problems. New technology is emerging such as TKIP and AES [1].

Moreover, filters can be set up such that only machines with certain MAC-addresses are allowed to access the WLAN (each computer is associated with a unique MAC address). Another challenge is that shops may with to get rid of old merchandise by selling older models at lower prices. These will typically be models without the most recent security features. Furthermore, shops such as large electronics chains do not always provide the necessary customer support. They may not help customers upgrade to more recent versions of firmware – a task that seems daunting to most novice computer users.

When setting up a new access point experts recommends four basic steps [1]. First, broadcasting of the SSID should be turned off. Second, MAC based access control should be activated. Third, WEP encryption should be enabled, and finally the power level of the access point should be lowered to prevent connections from outside the specified boundary. One way to achieve this is to set the maximum allowable communication rates to 5.5 Mbps.

There are several freely available security tools available that can be used for compromising the security of wireless networks. Some of these include AirCrack [4] which is a program that can be run on both Linux and Windows that allows the wireless traffic to be monitored and WEP keys to be cracked. Another tool is WarLinux [5] which can be downloaded as a bootable CD-image. WarLinux is a preconfigured linux installation that is designed for checking the strength of wireless networks.

1.2 Users' and technology

Clearly, one needs certain technical insight to secure a wireless network. It is unrealistic to expect ordinary users to acquire sufficient insight. The responsibility of ensuring adequate security therefore falls onto the equipment manufacturers and software providers.

There are several interesting studies on how novice users relate to security. For instance, it has been demonstrated that novice users find it difficult to conduct an encryption task on a message [6] and hence find it difficult to protect e-mail messages. Another security feature that most users get in direct contact with is passwords and several studies have addressed how users compromise passowrd security [7, 8]. Strategies for making more usable password systems include pass faces [9] and images [10]. Attitude to security has also been studied and it has been found that age is an important factor as younger users are more pragmatic about security than more senior users [11].

Studies from different areas of computer science repeatedly confirm that technology have different effects on different user groups. Especially, in the field of human computer interaction (HCI) it has been found that age has an impact on mobile phone usage [12]. Young users are more comfortable with the technology than older users, and young adults are again better than children. Gender has also been found to affect how users interact with technology [13]. Male users perform better at spatial tasks relying on spatial memory than females and that females are more emotionally driven. Finally, practice results in learning and consequently better performance [14].

The hypothesis of this study is that different user groups have different attitudes towards wireless technology. It is also relevant to study this diverse set of groups as an increasing portion of the general population is setting up wireless networks in their homes. The expected results of this study is that males would be more familiar and aware of WLAN security than females and that young adults would more familiar with WLAN security than senior users.

2 Quantitative study

The quantitative study was realised using a questionnaire and the purpose was to acquire general trends regarding user awareness and attitude towards wireless security.

2.1 Method

A total of 38 subjects completed the questionnaire. The subjects were hand-picked to widely represent gender and age. Subjects were mostly recruited from the international student population at Oslo University College.

The questionnaire comprised 20 multiple choice questions. The number of alternatives ranged from two to fourteen options. The questionnaires were printed on six sheets of one-sided paper and the text was written in English.

Subjects where contacted on a one-to-one basis and completed under the supervision of the second author. Some of the questionnaires were collected via e-mail and the others in person on hardcopies. It took about 10-15 minutes to complete the questionnaire.

The analysis was manually recorded from the questionnaires and input into Microsoft Excel which was used for subsequent statistical analysis and graphing.

2.1 General trends

Fig. 1 shows the general opinions about what a WLAN is. A total of 76.9 % of the subjects correctly identified a WLAN as a network that allows wireless communication. Interestingly, 7.7% of the subjects associate WLAN with laptops. This is understandable from the fact that laptop computers are the computer item most often connected to a wireless network. Surprisingly, 5.1% indicated that they did not know what a WLAN is. It is out guess that this is connected to unfamiliarity with the WLAN acronym WLAN and not necessarily the concept of wireless communication.

Fig. 2 shows the breakdown of responses to the trick question “Is wireless communication safer than communication through a wire?”. Here, 43.6% of the subjects correctly reject this claim, while only 2.6% support it. Surprisingly, a massive 23.1% admit that they do not know, 12.8% claim that there is no difference and 17.9% think that a firewall will provide the necessary security. Based on these results we conclude that nearly 50% of the respondents have a correct fundamental understanding of wireless security while over half of the respondents have a distorted and inaccurate understanding of the problem. It is possible that the media is partially to blame for this. For instance, the high number of respondents with total faith in firewalls may be due to the repeated mentioning of firewalls in connection with security in the mass media in recent years.

Fig. 3 reveals the respondents’ conception of the disadvantages of unencrypted traffic. Here 51.3% correctly perceive eavesdropping as a potential problem. Note that the term eavesdropping was replaced with an explanatory phrase on the questionnaire to make the option more clear to the less technical savvy respondents. An alarming 30.8% indicated that they do not know the disadvantages of unencrypted traffic. A total of 17.9% of the subjects indicated that unencrypted traffic makes the system more vulnerable to virus attacks. Although this is true in theory, it is less of a problem in practice. Again, the media has given computer viruses significant attention and some users may associate viruses with any type of security problem. It is very surprising that none of the subject indicated computer hijacking as a potential danger of unencrypted traffic.

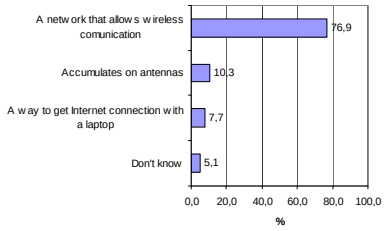


Fig. 1. What is a WLAN?

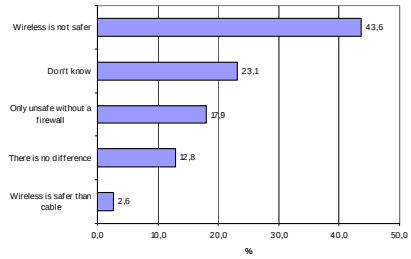


Fig. 2. Is wireless communication safer than communication through a wire?

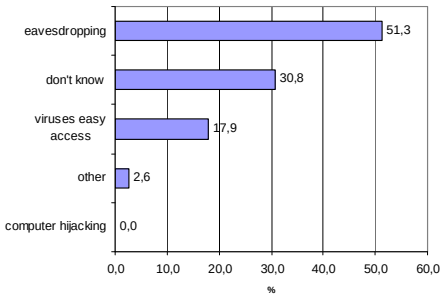


Fig. 3. Disadvantages of unencrypted traffic.

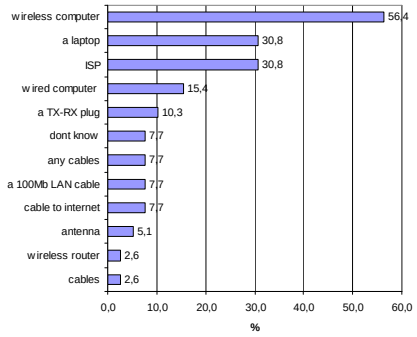


Fig. 4. Items that are needed to set up a WLAN.

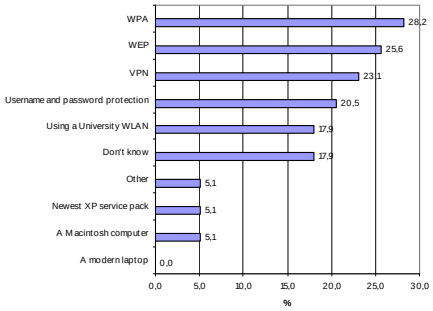


Fig. 5. Elements that give security

Note that a more elaborate explanation of computer hijacking was used in the questionnaires.

Fig. 4 shows the responses related to items that are required to set up a wireless network. More than half of the subjects, namely 56.4% of the subjects, claim that one needs a wireless computer and 30.8% that one needs a laptop to set up a wireless network. In fact, both items can be used for connecting to a wireless connection, but neither of them can be used to set it up.

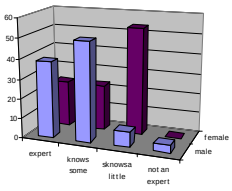


Fig. 6. Self-assessed Internet skills.

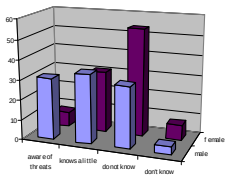


Fig. 7. Awareness of wireless security threats.

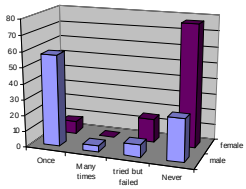


Fig. 8. Subjects that have installed a WLAN – gender breakdown.

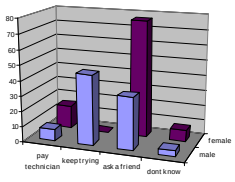


Fig. 9. How to tackle difficulties installing a WLAN.

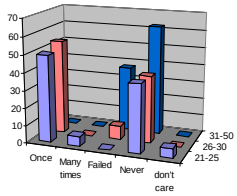


Fig. 10. Subjects that have installed a WLAN – age breakdown.

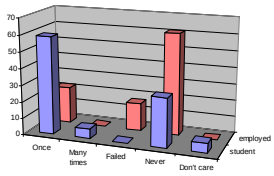


Fig. 11. Subjects that have installed a WLAN – profession breakdown.

Surprisingly, only 2.6% of the subjects were aware that one needs a wireless router and cables, and only 5.1% of the subjects indicated the need for an antenna. Although, the antenna is usually integrated into the wireless routers, they are clearly visible. It is surprising that as much as 10.3% of the subjects indicated the need for the fictitious and technical sounding TX-RX plug. Reassuringly, 30.8% correctly indicated an internet service provider (ISP) as a necessity.

The respondents' responses suggest that there are confusion and misconception regarding the components of a wireless network. However, there is also some element of noise as the users probably know more than what the questionnaire reveals. Some users may be conceptually aware of what is needed, but not familiar with the technical jargon or acronyms used on the questionnaire.

Fig. 5 enumerates elements that provide security according to the subjects. The results show that about a quarter of the subjects view WPA, WEP and VPN (Virtual Private Network) as technologies that provide security. The more recent WPA technology is also ranked before more dated WEP technology. A total of 17.9% of the subjects indicate that they do not know. Of the more ambiguous and misunderstood security practices included 20.6% of the subjects that username and password protection adds security, 17.9% believe that using a University WLAN is safe ("its provided by the university so it must be safe"), 5.1% believe using a Apple Machintosh computer is safe and 5.1% believe that installing the most recent Microsoft Windows XP service pack will do the job (assuming they are using Windows XP).

2.3 Effect of gender

Not surprisingly, the largest cross-group difference was observed with respect to gender.

Fig. 6 shows the breakdown of self-assessed Internet skills. There is a clear difference between males and females. Males express more confidence than females as 38% of the males view themselves as expert Internet users, while only 23% of the females viewed themselves as experts. Similarly, 50% of all males claims to have "some" Internet skills, while only 23% of females did so. However, females were in majority (58%) in terms of having "little" Internet skills, while only 8% males thought the same.

Fig. 7 shows the subjects' self assessed awareness of wireless security threats. Again, males indicated a stronger awareness of wireless security threats than females as 31% males and only 8% females indicated awareness of wireless security threats. The males and females where approximately equally divided on knowing a little about security threats (35% males and 31% females) and females where in majority for the group that indicated no awareness (54% females and 31% males).

Fig. 8 shows the gender breakdown with respect to practical experience with setting up a wireless network. Clearly, males express more familiarity with setting up a wireless network than females as a massive 58% males claim to have set up a wireless network once versus only 8% females. Next, 77% females reported never having installed a wireless network compared to 27% of the males. Only 4% males had set up a wireless network more than once. Next, 15% females and 8% males had attempted setting up a wireless network, but failed.

Fig. 9 shows how males and females would tackle difficulties while installing a wireless network. The general trend is that males report a willingness to try themselves until they are successful (46% males, 0% females), while females are more likely to seek help. Most subjects would ask a friend (77% females, 35% males). Others would be willing to pay a technician to complete the job (15% females, 8% males).

2.4 Effect of age

Results for the different age groups are similar to the ones obtained for the genders. However, there was not much effect of age between the young age groups, i.e. 21-25 and 26-30 years of age. There are generally more distinctive differences between subjects that are 21-30 and 31-50 years of age.

For example, Fig. 10 shows the differences between the different age groups with respect to experiences installing a wireless network. Generally, young adults have more experience with installing wireless networks than older subjects. There are not many differences between the two groups of young adults.

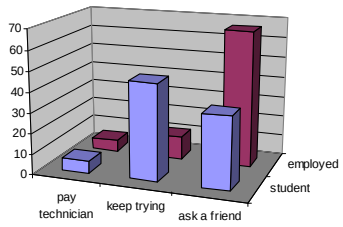


Fig. 12. How to handle difficulties.

2.5 Effect of professional status

The differences between the user groups were smallest for the group of students versus employed. This again is probably an effect of a limited sample. The current study should be expanded to include computer professionals versus non-computer professionals. The results in this section should therefore be viewed with some caution.

Fig. 11 shows the breakdown of experiences installing wireless networks with respect to being a student or being employed. The results show that students have more experience with setting up wireless networks than employed individuals. Among students 59% had set up an wireless network once, 6% many times and 29% never, while among employed subjects 22% had installed a wireless network once, none several times and 61% never. Furthermore, 17% of the employees reported having tried to install a wireless network but failed. None of the students reported failing to install a network.

One explanation of this could be that students have more time on their hands and are dependent on Internet access to conduct their studies. To save money they experiment themselves. Some employees are less dependent on Internet at home, and all required computer infrastructure is provided at work.

Fig. 12 shows the attitude these two user groups have towards problem solving during wireless network installation. Students (47%) are more likely to continue trying until they succeed than employees (11%), while employees (67% employees versus 35% students) are more likely to ask a friend. Students and employees are equally unlikely to pay technicians to do the work (6%).

3 Qualitative study

3.1.1 Subjects

Four subjects where recruited for the qualitative study. Computer users with no technical knowledge beyond office applications where chosen in order to acquire interesting qualitative data. Subject-A was a foreign student of journalism in her early 20s. Subject-B was a mathematics teacher in the faculty of engineering in her 50s.

Fig. 13. The subject being supervised by one of the investigators. The subject investigates the user manual.

Fig. 14. The subject investigates the wireless router.

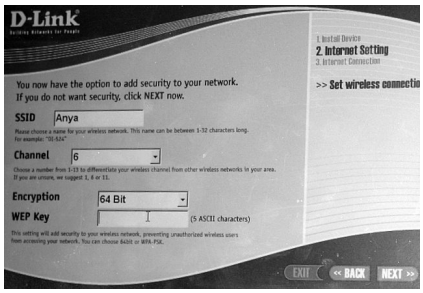


Fig. 15. A schreenshot of the quick install wizard.

Fig. 16. Where does that plug go?

Subject-C was a member of the administrative staff in the faculty of engineering also in the 50s. Subject-D was an international exchange student taking part in an European Project Semester. All the subjects where female.

3.1.2 Materials

A DLink AirLink G DI-524 wireless router was used for the experiment, and a Dell Inspiron 1150 notebook computer with Microsoft Windows XP installed (Norwegian language edition). The laptop had built in LAN and WLAN network cards and a CDROM drive. The wireless router was provided in the original packaging as delivered from the shop. The package contained the Wireless router, a power supply, a blue network cable, a quick installation CD with the router warranty and an instruction manual with instructions in five major languages including Norwegian, Spanish and English (see Fig. 13). The experiment was carried out on a desk next to wall with a university LAN socket. The university had also a WLAN with a unique SSID.

3.1.3 Procedure

The subjects were guided to the place of the experiment and told to set up a secure wireless network. The subjects were asked to unpack the contents of the WLAN router package and explore its contents (see Fig. 14).

Next the subjects where guided through the configuration. After successfully configuring the wireless router, and disconnecting the laptop from the Internet, the subjects where asked to test the wireless connection by logging into the configured network. The user had to open a webpage in browser to confirm the connection.

The subjects were asked to "think aloud" and the sessions were recorded using a portable mp3 recorder. A digital camera was used to pictorially document the session.

The investigators attempted to minimise their involvement and focused on observing the subjects, but would give gentle hints when the subjects were obviously struggling. Each session lasted for approximately one hour.

3.2 Results

In this discussion only the major observations are included for the sake of brevity. The subjects had no problems unpacking the contents of the wireless router package and identifying the various items. Two of the subjects looked at the installation manual but none of the subjects found the installation manual useful. The subjects complained that the manual did not contain sufficient background and explanation of terms and acronyms.

All the subjects quickly identified the quick-start installation CD with a yellow label giving the warning "insert into CD-ROM first" and successfully started the quick installation program that guided the users through the subsequent steps. However, one subject discovered the CD with the yellow warning after having attempted to install the router from the instruction manual.

Subjects generally appeared uncertain about how things were to be connected. First, the laptop computer was to be connected to the wireless modem for configuration, and later connected to the LAN (see Fig. 16).

The setup CD was quite helpful in instructing the users how to connect things together. Illustrations were used allowing the subjects to make visual comparisons. One subject was confused by an illustration showing a tower computer case instead of a laptop computer but eventually deduced that the tower case was analogous to the laptop computer.

After guiding the subjects through the connections the router had to be configured. The user had to select a SSID, although no explicit explanation of this was provided. Next the subject had the choice to setup a security mechanism. The choices were no security (default), WEP, 64BIT and WPA-PSK, but no explanations of these were given (see Figure 15). One subject initially ignored this setting and had to be corrected. All subjects had to ask which option to choose and WPA-PSK was recommended by the investigators with a simple explanation of why it is recommended. There was also a field for providing a password. Some subjects found the password field confusing when they were experimenting with the different encryption schemes as the allowable password characters are slightly different for each scheme.

Upon completing the installation, the subjects were asked to disconnect the laptop computer from the wireless router and test the wireless network. No instructions on how to do this was provided. The subjects initially tried the connection by opening internet explorer, but with no effect. The users had to explicitly be told to establish a wireless connection by selecting the SSID they had set up and provide the password for the connection. The fact that there was two SSIDs (the subject's access point and the university access point) did not cause any particular problem.

In summary, the installation procedure suffered from the following general problems: a) the subjects did not adhere to the specified order of the installation steps, b) the subjects had too little background information to understand the terminology and acronyms used, c) the printed manual provided no useful information and was only a disturbing element, d) the user was presented with too much choice and not enough insight to make a sensible decision, e) the setup CD did not help the users beyond installing the router as the subjects were totally on their own with regards to establishing a connection to the wireless network after completing the installation, f) the default option was no encryption and users are accustomed to accept the default settings when they are in doubt.

4 Conclusions

This paper addresses user awareness and attitude to wireless security. The results suggest that most users have insufficient knowledge about wireless network security to adequately install a secure WLAN, even with a quick start help program. Differences could also be attributed to gender and age. In particular, males are more confident about their wireless security knowledge than females, while females are more likely to seek professional help. Will females therefore end up with safer wireless networks than males? There is clearly much to be desired from the wireless communication equipments manufacturers. The provision of quick-start help program is a good initiative, but these must be very simple, leaving no choice for the user in terms of security policy. Best practices should be followed to strengthen security. In addition it should also be possible to configure the router for advanced users. One cannot rely on users to adapt to recent advances in technology – instead the technology must adapt itself to the users. One solution would be to preset the wireless routers with a high security setting such as WPA as default, where the device is given a unique random SSID and a random password, also provided on a piece of paper in the packaging. This would perhaps increase unit costs, but would greatly improve the security for novice users. Impatient novice users would then be able to immediately deploy relatively secure wireless networks in their homes.

References

1. Bhagyavati, W.C. Summers, and A. DeJoie. *Wireless Security Techniques: An Overview*. in *InfoSecCD Conference '04*. 2004. Kennesaw, USA: ACM press.

2. Schmidt, T. and A. Townsend, *Why Wi-Fi Wan't to be Free.* Communications of the ACM, 2003. **46**(5): p. 47-52.
3. Zahur, Y. and A. Yang, *Wireless LAN security and laboratory designs.* Journal of Computing Sciences in Colleges, 2003. **19**(3): p. 44-60.
4. Devine, C., *Aircrack*. http://www.aircrack-ng.org
5. *WarLinux*. http://sourceforge.net/projects/warlinux/
6. Whitten, A. and J.D. Tiger. *Why Jhonny can't encrypt: a usability evaluation of PGP 5.0*. in *9th USENIX security symposium*. 2000. Denver, Colorady.
7. Adams, A. and M.A. Sasse, *Users are not the enemy: why users compromise security mechanisms and how to take remedial measures.* Communications of the ACM, 1999. **42**(12): p. 40-46.
8. Adams, A., M.A. Sasse, and P. Lutt. *Making passwords secure and usable*. in *HCI'97 conference on people and computers XII*. 1997. Bristol, UK: Springer.
9. Brostoff, S. and M.A. Sasse. *Are passfaces more usable than passwords? A field trial investigation*. in *HCI 2000 conference on people and computers XIV - usability or else!* 2000. Sunderland, UK: Springer.
10. Dhamja, R. and A. Perrig. *Deja vu: a user study using images for authentication*. in *9th USENIX security symposium*. 2000. Denver Colerado, USA.
11. Dourish, P., et al., *Security in the wild: user strategies for managing security as an everyday, practical problem.* Pers. Ubiquit. Comput., 2004. **8**: p. 391-401.
12. Ziefle, M., S. Bay, and A. Schwade, *On keys meanings and modes: The impact of navigation key solutions on children's efficiency using a mobile phone (in press).* Behaviour and Information Technology, 2005.
13. Lawton, C.A., *Gender differences in way-finding strategies: Relationship to spatial ability and spatial anxiety.* Sex Roles A Journal of Research, 1994. **30**(11-12): p. 765-779.
14. Newell, A. and P.S. Rosenbloom, *Mechanisms of skill acquisition and the power law of learning. In Cognitive Skills and Their Acquisition*, J.R. Anderson, Editor. 1981, L. Erlbaum Associates. p. 1-55.