Security State of 802.11 Wireless Networks

A Study of WLANs in Five Norwegian Cities

Gaute Svendsen

Master of Information Science

Spring 2012

Faculty of Social Sciences
Department of Information Science and Media Studies

ABSTRACT

This thesis was written to promote awareness of wireless network security to the ICT industry and the general public. It gives an overview of the current security state in Oslo, Bergen, Kristiansand, Tromsø and Flekkefjord. The data was gathered through war-walking and war-driving in the mentioned cities, and the results were deduced from an analysis of 35 194 wireless networks. The findings showed that 36 % was either unencrypted or encrypted with the deprecated WEP protocol. Through the analysis of these and other findings, this thesis discusses the role of parties influencing wireless network security. It also provides a description of potential consequences, followed by counter-measures and recommendations. The magnitude of insecure wireless networks is a major risk to Norwegian citizens and to the society itself.

ACKNOWLEDGEMENTS

Through the process of creating this master's thesis I have not only been educated in WLAN security, but I have learnt a great deal about myself. I quickly found out that without the help of certain people, I would have gotten nowhere. I therefore wish to thank the important few that aided me on the way.

First and foremost, I would like to thank my supervisor Andreas L. Opdahl for his guidance and advice, and for helping me find an interesting direction for my thesis.

I wish to thank the people connected to the Aircrack-ng project for helping me choose technical equipment, and for directing me towards relevant literature. I also wish to thank Mike Kershaw, the developer of Kismet, for simplifying the process of harvesting network data.

Additionally, I would like to thank the representatives of the various Internet service providers, who willingly answered my tiresome questions.

Finally, my warmest gratitude goes to my fiancée, Eliane, for being so supportive and understanding, for motivating me in times of despair, and for brightening up my days.

Gaute Svendsen

Bergen, March 2012

TABLE OF CONTENTS

ABSTRACT II
ACKNOWLEDGEMENTS III
TABLE OF CONTENTS IV
LIST OF TABLES V
LIST OF FIGURES VI
LIST OF CHARTS VI
GLOSSARY VII

1 INTRODUCTION 1
RESEARCH QUESTIONS 2

2 BACKGROUND 3
2.1 Wireless Local Area Networks 3
2.1.1 Breaking WLAN Encryption 4
2.2 Internet Service Providers 8
2.2.1 Vulnerable Thomson SpeedTouch Routers 8
2.3 Security and Privacy in Households, Enterprises and Society 9
2.3.1 Criminal WLAN Exploitation 11
2.4 National and Societal Security Issues 13
2.5 Similar Studies 14

3 RESEARCH METHOD 16
3.1 Locations of Data Sampling 16
3.2 War-walking and Technical Equipment 17
3.2.1 Data Sampling: War-walking 18
3.2.2 Data Sampling: Hardware 19
3.2.3 Access Point Detection Software 20
3.3 Documentary Data 20
3.4 Preparation of Data 21
3.5 Reliability and Validity 23
3.5.1 Reliability 23
3.5.2 Validity 24
3.6 Ethical Concerns 27

4 RESEARCH FINDINGS: INSECURE WLANS AND VULNERABLE ISP ROUTERS 28
4.1 Routes of War-walking and War-driving 28
4.1.1 Oslo 29
4.1.2 Bergen 30
4.1.3 Kristiansand 31
4.1.4 Tromsø 32
4.1.5 Flekkefjord 33
4.2 Encryption Data 34
4.2.1 Cloaked SSIDs 35
4.2.2 Popular SSIDs 38

4.2.3 Popular Manufacturers 39
4.2.4 TKIP and CCMP 39
4.3 Internet Service Providers: Problematic Encryption Practices 40
4.3.1 ISP Routers: Altered or Unaltered Configuration 42

5 DISCUSSION 46
5.1 Encryption Usage in Norway 46
5.1.1 Comparison to Similar Research 47
5.1.2 Common SSIDs and Manufacturers 48
5.1.3 The IEEE 802.1X Standard 49
5.1.4 Temporal Key Integrity Protocol (TKIP) 50
5.2 The Role of the Internet Service Providers 51
5.2.1 Vulnerable ZyXEL Routers 52
5.2.2 Potentially Vulnerable Routers 54
5.2.3 Wired Equivalent Privacy (WEP) 55
5.2.4 Wi-Fi Protected Access Pre-shared Key (WPA-PSK) 56
5.3 Societal Challenges and Countermeasures 59
5.3.1 WLAN Breaches in Norway 61
5.3.2 Common Security Myths 62
5.3.3 Security Measures by State Institutions 64
5.3.4 Countermeasures and Recommendations 64

6 SUMMARY 68
6.1 Future Research 69

7 REFERENCES 70

LIST OF TABLES

Table 2.1 – PSK cracking rate with HD 6990 in EWSA and Pyrit 6
Table 2.2 – PSK cracking cost with Amazon, 0.28 USD/minute and 1 200 000 PSK/second .. 7
Table 4.1 – Encryption distribution in the sampled cities 34
Table 4.2 – Encryption distribution, Unencrypted+WEP vs. PSK+802.1X 35
Table 4.3 – Visible and cloaked networks in Oslo 36
Table 4.4 – Visible and cloaked networks in Bergen 36
Table 4.5 – Visible and cloaked networks in Kristiansand 36
Table 4.6 – Visible and cloaked networks in Tromsø 36
Table 4.7 – Visible and cloaked networks in Flekkefjord 37
Table 4.8 – Most common default SSIDs 38
Table 4.9 – Most common SSIDs by businesses and institutions 38
Table 4.10 – Most common manufacturers 39
Table 4.11 – Variables substituting characters in SSIDs 40
Table 4.12 – Circulation of WEP encryption in privatZ*, SpeedTouchZ* and ThomsonZ* .. 40
Table 4.13 – ISP preconfigured routers with WPA-PSK 41
Table 4.14 – SpeedTouch routers with default SSID 43

Table 4.15 – SpeedTouch routers with custom SSID 43
Table 4.16 – ZyXEL routers with default SSID..... 44
Table 4.17 – ZyXEL routers with custom SSID 44
Table 4.18 – Inteno routers with default SSID..... 45
Table 4.19 – Inteno routers with custom SSID 45
Table 5.1 – WPA passphrase strength of the largest ISPs that distribute wireless routers 57

LIST OF FIGURES

Figure 2.1 – MITM attack (Carpenter and Barrett 2008, 447)..... 11
Figure 3.1 – Bag containing GPS, 2 dBi and 7 dBi omnidirectional antennas 18
Figure 3.2 – Antenna coverage based on dB. For illustrative purposes only..... 19
Figure 3.3 – WLAN representation example from the GISKismet web page 22
Figure 4.1 – War-walking/war-driving route in Oslo 29
Figure 4.2 – War-walking route in Bergen 30
Figure 4.3 – War-walking route in Kristiansand..... 31
Figure 4.4 – War-walking/war-driving route in Tromsø..... 32
Figure 4.5 – War-driving route in Flekkefjord..... 33

LIST OF CHARTS

Chart 4.1 – Encryption distribution in the sampled cities, in percentage..... 34
Chart 4.2 – Encryption distribution, insecure vs. more secure..... 34
Chart 4.3 – Encryption distribution, Unencrypted+WEP vs. PSK+802.1X, in percentage 35
Chart 4.4 – Visible and cloaked networks in the sampled cities..... 37
Chart 4.5 – Unencrypted+WEP, visible vs. cloaked 37
Chart 4.6 – Unencrypted+WEP for sampled cities combined, visible vs. cloaked..... 38
Chart 4.7 – TKIP and CCMP in WPA/WPA2 39
Chart 4.8 – Circulation of WEP-encrypted Thomson routers from ISPs in percentage 41
Chart 4.9 – Tendencies to alter SSID on SpeedTouch, ZyXEL and Inteno routers..... 42
Chart 4.10 – SpeedTouch encryption, default SSID vs. custom SSID 43
Chart 4.11 – ZyXEL encryption, default SSID vs. custom SSID 44
Chart 4.12 – Inteno encryption, default SSID vs. custom SSID 45
Chart 5.1 – Private broadband subscriptions in percentage (SSB 2011c)..... 47

GLOSSARY

Brute force	Trying every possible combination of characters (e.g. aaa, aab, aac).
Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP)	Encryption protocol that uses the AES encryption standard. It was created to address the vulnerabilities presented by TKIP.
Cloud-based	Computational resources available from internet on demand.
CPU cluster	Linked computers that are able to work together on the same task.
Denial of Service	An attempt to make network resources unavailable to its intended users.
Dictionary attack	Trying values from a pre-arranged list as passphrases.
Extensible Authentication Protocol (EAP)	An authentication framework that provides an infrastructure for network access clients and authentication servers.
Internet Protocol (IP) address	A numeric label assigned to devices participating in a network such as a local area network or the Internet.
Internet Relay Chat (IRC)	A protocol for real-time Internet text messaging.
Internet service provider (ISP)	An organization that provides Internet access to its customers.
MAC address	A unique identifier for every network interface controller (network card or other network devices).
Monitor mode	Allows for packets to be captured without having to associate with the access point.
Packet analyser	A computer program that can intercept and analyse packets being transferred over the network.
Pairwise Master Key (PMK)	Hash of the network SSID and passphrase.
PHP	Service-side scripting language that produces dynamic web pages.
Pre-shared key (PSK)	A key shared between parties before it is being used.

Quality of Service (QoS)	Mechanisms for controlling traffic resources on a network.
Remote Authentication Dial In User Service (RADIUS)	A protocol for authentication, authorization and accounting management in networking.
Radio frequency (RF) signals	Radio waves that have been modulated to contain information.
Service set identifier (SSID)	The public name of a wireless network.
Temporal Key Integrity Protocol (TKIP)	A security protocol developed to replace the deprecated WEP protocol.
Urban canyon effect	Tall buildings blocking radio reception such as GPS signals.
War-walking / war-driving	The act of walking or driving with a portable computer in search of multiple wireless networks.
Wired Equivalent Privacy (WEP)	A deprecated encryption protocol for wireless networks.
Wi-Fi Protected Access (WPA)	An encryption protocol for wireless networks based on TKIP or CCMP.

1 INTRODUCTION

Norway is a modern nation with a population of 5 million citizens. It has a high standard of living and according to Statistic Norway[1], 93 % of the Norwegian population uses the Internet (SSB 2011b). Many are aware of the Internet network's dangers of malware, phishing attempts and e-mail scams, but not so many are aware of the dangers within their own local area network. As wireless network propagation is increasing together with the necessity of easy Internet access, the risk of attacks on local area networks must be taken seriously. Furthermore, the increasing information traffic over Internet, both in the private and public sector, makes the question of security and privacy highly pertinent. Additionally, the current development rate of electronic equipment requires a corresponding development of security measures. My understanding is that the customers' demand of a quick and easy gateway to Internet may lead manufactures and developers into giving security aspects a lesser priority.

This master's thesis aims to provide information about the current state of the security usage on wireless local area networks (WLANs[2]) in Oslo, Bergen, Kristiansand, Tromsø and Flekkefjord. The data that will be presented has been gathered by using wireless equipment to retrieve information from wireless access points[3] and routers. My intention is not only to find unencrypted and open networks, but also to look for networks with deprecated or insufficient encryption. By comparing my findings with older research I expect to see a large increase in the total number of wireless networks and also some improvement in terms of encryption usage. In accordance to this assumed development, I also find it interesting to investigate the role manufacturers, Internet service providers (ISPs) and other parties have in affecting encryption usage on wireless networks.

To investigate the mentioned concerns I have defined the following research questions:

[1] Statistisk sentralbyrå.
[2] The term *WLAN* will be used for any single access point or router found, even though some of them could be linked together and combined is creating a single WLAN.
[3] I will use the term *access point* when it is uncertain whether the device in question is an access point or a wireless router.

RESEARCH QUESTIONS

1. What is the current state of WLAN encryption in Norway?
    a. How secure are the wireless networks?
    b. Does city population or location affect encryption usage?
2. How are Internet service providers affecting the situation?
3. What consequences can poor WLAN encryption have for our society?
    a. Have encryption practices changed over the last few years?
    b. What can be done to improve today's situation?

Before I started my research, I had the understanding that a high number of WLANs were unencrypted or had encryption that could be easily broken. This assumption was based on various minor studies I had done in the past, as well as articles about encryption usage patterns in the 802.11 standards. The **first research question** in this master's thesis is based on that assumption, and I will try to answer it by looking at the magnitude of the various security protocols.

My **second research question** is based on increased media coverage of vulnerabilities in access points caused by the manufacturer or Internet service providers. It is common for many Internet users to have routers with encryption preconfigured by their ISP. If vulnerabilities in these router types are found, the large amount of exposed WLANs is problematic. This motivated me to investigate whether or not the Internet providers are actively trying to improve security in wireless networks.

In my **third research question** I will try to give an overview of the risks we face by not securing our WLANs properly. I also look for tendencies of improvement and suggest several methods of countermeasure.

In the following second chapter I will present background information beneficial to comprehend the results of my study. The chapter will explain basic vulnerabilities in 802.11 encryption methods, risks of wireless networking and present similar studies. In the third chapter I present my method of research from a theoretical and practical aspect as well as discussing reliability and validity. I then present my research results in the fourth chapter, followed by a discussion in chapter five. Finally, I summarize my thesis in chapter six and give suggestions for future research.

2 BACKGROUND

At the end of 2002 there were 224 000 active broadband subscriptions in Norway (SSB 2011d). Now there are more than 1 730 000 and 73 % of all households have broadband access (SSB 2011c). This is consistent with Internet usage prevalence of 35 % in 2002 rising to 77 % in 2010 (SSB 2011a). The increasing Internet dependence has led to increased broadband coverage and vice versa. Furthermore, introduction of handheld devices such as notebooks, smartphones and tablets has strengthened this dependence and many users now require wireless access to the Internet.

In this chapter I will introduce wireless networks and its history, followed by security flaws and methods to exploit them. I will then briefly introduce Internet service providers before I show examples of risks associated with wireless networking. Finally, I will present similar studies by other researchers.

2.1 Wireless Local Area Networks

In this thesis, WLAN refers to wireless networks under the IEEE 802.1 set of standards. IEEE stands for Institute of Electrical and Electronics Engineers and is the world's largest professional association dedicated to advancing technological innovation and excellence. While *wireless* is a superset of the Wi-Fi certification by the Wi-Fi Alliance, not every 802.11-compliant device is Wi-Fi certified.

In *802.11 Wireless Networks: The Definitive Guide*, Matthew Gast (2005) points out that wireless networks offer great advantages over wired networks in aspects such as mobility and flexibility. Users are no longer limited to a fixed position and "no cables means no recabling" (Gast 2005, XII). Before 1997, users who wanted to set up wireless networks were forced to "adopt single-vendor solutions with all of the risk that entailed" (Gast 2005, XIII). With the completion of the IEEE 802.11 standard that year, the ball had started rolling and everything became easier. Naturally, without wires it also became easier for intruders to eavesdrop on the data packets being sent over the network. To deal with this problem IEEE implemented a security protocol into the 802.11 ratification called *Wired Equivalent Privacy (WEP).* Despite the confident name, WEP was declared deprecated by IEEE in 2004 due to serious flaws in its algorithm (IEEE 2004). Nevertheless, WEP is still quite commonly used on wireless networks. To replace this faulty encryption, Wi-Fi Alliance created *Wi-Fi Protected Access (WPA)* that became ratified in 2004 (IEEE). WPA basically has two modes. The simpler one

called *WPA-PSK* or *WPA Personal* uses an 8 to 64 character long passphrase (63 ASCII or 64 hexadecimals) shared between the wireless clients on the network (Gast 2005). The other mode, *WPA-802.1X* or *WPA Enterprise*, is more difficult to configure as it relies on RADIUS servers and EAP for authentication (Gast 2005).

2.1.1 Breaking WLAN Encryption

There are several attacks on wireless networks that can damage the network itself or its users. For this thesis I will focus on attacks conducted to break into networks, rather than attacks to sabotage or deny accessibility. The process of cracking passwords for wireless networks depends on the encryption and authentication being used on the access point. WEP, WPA-PSK and WPA2-PSK are all possible to crack if given enough time. While there are attacks on the more secure authentication mechanism 802.1X, I have decided to focus on *pre-shared keys (PSK)* which is designed for home and small offices and where attacks are simpler to perform. I also expected the use of PSK to be far more common than 802.1X.

2.1.1.1 Wired Equivalent Privacy (WEP)

In 2001, Fluhrer, Mantin and Shamir (2001) presented weaknesses in the RC4 algorithm used in the WEP protocol. The same year their work led to the free tools AirSnort and WEPCrack being created, which allowed anyone to crack WEP keys on cheap hardware (AirSnort 2011; Rager 2011). Because AirSnort required 5 to 10 million encrypted data packets to be gathered, the process could take days on networks with little traffic. The cracking of the WEP password itself took less than a second (AirSnort 2011). A popular tool suite for cracking WLAN passwords today is called Aircrack-ng. This suite has the old *Fluhrer, Mantin, Shamir (FMS) attack* implemented but also takes advantage of more recent attacks such as the *KoreK chopchop* from 2004 that reduced the number of required packets to 300 000 – 1 000 000 depending on whether it was 64 or 128 bit encryption (Devine 2011). The most commonly used attack in Aircrack-ng however is the *PTW attack* which Tews, Weinmann and Pyshkin (2007) demonstrated could crack a 128 bit WEP key with a success probability of 50 % with less than 40 000 packets. For 95 % success probability they claimed only 85 000 packets was needed. Erik Tews, together with Martin Beck, later improved this attack to only need 24 200 packets for a 50 % success rate (Tews and Beck 2009). Nevertheless, as patiently waiting for packets still takes time on less trafficked networks, active attacks drastically reduce the time required to crack a WEP key. A popular active attack is called *ARP request replay* (Devine 2011). This attack listens for a packet that contains data needed to crack the key, and then retransmits it back to the access point (Carpenter and Barrett 2008). The access point will then

repeat the packet but with new data needed for the WEP cracking. By doing this over and over it is possible to generate almost 1 000 packets per second (Tews, Weinmann, and Pyshkin 2007). By using their PTW attack and replaying packets to the access point, Tews, Weinmann and Pyshkin (2007) showed that WEP could be cracked in less than 60 seconds.

2.1.1.2 Wi-Fi Protected Access PSK and Wi-Fi Protected Access II PSK

Cracking WPA-PSK and WPA2-PSK is normally not as easy as cracking WEP. The two encryption protocols used in WPA and WPA2 are called TKIP (Temporary Key Integrity Protocol) and CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol). Even though Tews and Beck (2009) and others have presented functional attacks on TKIP, the encryption has not been cracked in the same way as WEP. CCMP is on the other hand far more secure.

WPA-PSK and WPA2-PSK encryption relies on a *pairwise master key (PMK)* which is computed from the network name (SSID[4]) and the PSK (the passphrase) (Cache, Wright, and Liu 2010). To crack this PMK and end up with the PSK, the current method is a dictionary attack that matches words to the passphrase, or *brute-forcing* by trying every possible combination of characters, e.g. aaa, aab, aac... (Gast 2005). To be able to do this, it is necessary to monitor the network to capture the *handshake* that occurs when a user connects or reconnects (Gast 2005). Instead of waiting for this to happen it is possible to use an attack that disconnects a chosen user from the network, forcing him to reconnect (Devine 2011). When the handshake from this authentication has been gathered, there is no longer a need to monitor the network. The brute-force or dictionary attack can then be executed on a remote system where the cracking speed depends on the hardware of this system. A security researcher from Elcomsoft Co. Ltd. informed[5] me that their Windows software Elcomsoft Wireless Network Security (EWSA) is able to try 115 000 WPA passphrases per second by utilizing the new AMD Radeon HD 6990 graphics card (~5 000 NOK[6]). When considering that a standard[7] CPU (central processing unit) today is able to do only 4 000 passphrases per second, the contrast of using GPU (graphical processing unit) is vast. For UNIX-based operating systems there is an open source software called Pyrit that is also able to crack PSK using GPU. Online reports suggest that the combination of Pyrit and the HD 6990 graphics

[4] Service set identifier. Broadcasted network names for access points are sometimes called *ESSID*, but in this thesis I will use *SSID*.
[5] E-mail correspondence, 01.04.2011.
[6] 09.05.2011. Retail price in the United States: 699 USD.
[7] Intel Core i7 920 2.66 GHz.

card is able to process 170 000 passphrases per second. These rates lead to the following time periods of cracking PSK by brute-force:

Passphrase length and type of characters	EWSA	Pyrit
8 characters, only digits	15 minutes	10 minutes
8 characters, lower case alphabetic	22 days	14 days
8 characters, lower case alphabetic and digits	10 months	6 months
10 characters, only digits	25 hours	16 hours
10 characters, hexadecimals	110 days	75 days
10 characters, lower case alphabetic	40 years	26 years
10 characters, lower case alphabetic and digits	1 023 years	675 years

Table 2.1 – PSK cracking rate with HD 6990 in EWSA and Pyrit

This means that while a given passphrase "84150723" takes up to 15 minutes to crack, adding the letters "xy" to it increases the cracking period to 29 years.

There are also alternatives to running the cracking process on your own system, where you upload a file containing the handshake between client and access point to an online cracker. For instance, the web page of *WPA cracker*[8] offers a cracking service on a 400 CPU cluster that tries 286 million words in 55 minutes for 40 USD. This rate of password cracking equals 87 000 words per second. Another similar service is the *WPA Password Cracker*[9] by Question Defense that charges 10 USD to work through a password list of 982 million words in 3 hours. A third alternative is *Recover WPA*[10] which uses a dictionary of 700 million words and lets you check the encryption strength of a network for free. If the passphrase is found, they charge 15 GBP to reveal it.

An alternative that offers more customization was reported by Reuters in January 2011, where Thomas Roth, a computer security consultant, used 8 instances of Amazon's cloud-based computers to perform a WPA-PSK attack at 400 000 keys per second (Finkle 2011). For this computational resource, Amazon charged 0.28 USD per minute and the attack lasted about 20 minutes before Roth found the passphrase (Finkle 2011). According to Reuters, Roth has since then updated his software and believes he could hack the same network in just 6 minutes (Finkle 2011). Table 2.2 below shows time and cost of brute-forcing different strengths of passwords with Roth's updated software (estimated to be 3 times as fast as previous version). Even though Amazon offers reserved instances based on a yearly fee and a lower cost per

[8] The web page for *WPA cracker* can be found at: http://www.wpacracker.com/
[9] The web page for *WPA Password Cracker* can be found at: http://tools.question-defense.com/
[10] The web page for *Recover WPA* can be found at: http://www.recoverwpa.com/

minute, I have used 0.28 USD per minute for the sake of comparison. Amazon now allows the use of 64 simultaneous instances, which in theory should make it possible to reach almost 10 million passphrases per second, but subsequently to the cost of 2.24 USD per minute.

I contacted Roth several times in order to hear the current state of his approach, but unfortunately he did not respond to my enquiries.

Passphrase length and type of characters	Time	Cost
8 characters, only digits	83 seconds	0.39 USD
8 characters, lower case alphabetic	48 hours	806 USD
8 characters, lower case alphabetic and digits	27 days	10 886 USD
10 characters, only digits	2 hours	34 USD
10 characters, hexadecimals	11 days	4 435 USD
10 characters, lower case alphabetic	4 years	588 672 USD
10 characters, lower case alphabetic and digits	97 years	14 275 296 USD

Table 2.2 – PSK cracking cost with Amazon, 0.28 USD/minute and 1 200 000 PSK/second

Brute-forcing WPA-PSK works by taking the passphrase attempt in plain text, encrypting it, and then comparing the result to the encrypted hash (Cache, Wright, and Liu 2010). Because the encrypting process is the most processor-intensive part, pre-computed hash tables can speed up the password cracking dramatically. But since the PMK is a hash of both SSID and passphrase, the pre-computed hash table needs to be specified to a single SSID to work. Such tables are for that reason only useful if generated for popular network names (Cache, Wright, and Liu 2010). For the 1 000 most common SSIDs, *Church of Wifi*[11] has created 40 GB of hash tables from a list of 1 000 000 words. With the use of such tables it is possible to try millions of passphrases per second on a normal CPU.

Prior to Tews and Beck's TKIP attack in 2008, the only practical attack against TKIP was the previously mentioned PSK brute force attack which is also applicable to CCMP (Halvorsen et al. 2009). However, the TKIP attack by Beck and Tews, which was later improved by Halvorsen et al., is not a key recovery attack and should therefore not be compared to the FMS and PTW attacks. In practice, the TKIP attack makes it easy to perform Denial of Service (DoS) attacks on wireless networks, which prevents accessibility for the network's intended users (Halvorsen et al. 2009). Though not yet implemented, Halvorsen et al. (2009) also describe a theoretical approach to spoofing the DNS (Domain Name System) server. Simply put, when a user types in a web page address, DNS spoofing makes it possible to

[11] The Church of Wifi web page can be found at: http://www.churchofwifi.org/

redirect the user onto a fake web page created by the attacker (Cache, Wright, and Liu 2010). The fake web page can be a cloned version of the real web page that steals sensitive information, or it can contain malware that infects the victim. DNS spoofing also makes it possible to redirect and monitor e-mail traffic.

2.2 Internet Service Providers

The four largest Internet service providers in Norway are Telenor, NextGenTel, Get and Ventelo. Together they have a 74.2 % market share of Norwegian broadband subscriptions (PT 2011). Telenor has 48.8 %, NextGenTel 10.9 %, Get 10.3 % and Ventelo 4.2 %.

Most ISPs in Norway have a bundle that includes a wireless router when distributing broadband to their customers. In order to simplify the installation process, they often deliver the wireless routers preconfigured. Because the ISPs for several years have configured them to use WEP encryption, I expect there to be a significant number of such routers active. In the current practice, however, most ISPs configure their routers to use WPA-PSK encryption and attach the passphrase on a sticker underneath.

This practice of bundling wireless routers with broadband subscriptions has become quite customary. NextGenTel, for instance, estimates[12] to have delivered wireless routers to about 70 % of their broadband customers. That means that they have delivered 132 000 preconfigured WLANs in Norway, based on their 188 000 total broadband subscriptions (PT 2011). I will now show an example on how preconfigured routers can be problematic.

2.2.1 Vulnerable Thomson SpeedTouch Routers

In April 2008, Kevin Devine (2008) published a method on how to find the default WEP password on preconfigured Thomson SpeedTouch routers from only the SSID. Devine had obtained a copy of the setup wizard distributed on CDs in Spain by the French telecommunications company Orange. By reverse engineering this file he was able to find the link between serial number, SSID and password. Devine then created a tool that allowed users to look up SSID and retrieve the password. In the source code comments of this tool he has provided the following example with the serial number CP0615JT109 (53):

[12] E-mail correspondence with Morten Ågnes, Director of Marketing and Information in NextGenTel, 26.04.2011.

> The format of a serial number:
>
> CP YY WW PP XXX (CC)
>
> […]
>
> Remove the CC and PP values: CP0615109
>
> Convert the "XXX" values to hexadecimal: CP0615313039
>
> Process with SHA-1: 742da831d2b657fa53d347301ec610e1ebf8a3d0
>
> The last 3 bytes are converted to 6 byte string, and appended to the word "SpeedTouch" which becomes the default SSID: SpeedTouchF8A3D0
>
> The first 5 bytes are converted to a 10 byte string which becomes the default WEP/WPA key: 742DA831D2
>
> (Devine 2008)

Devine's tool is simply using brute-forcing to return the password when given the 6 byte string of the SSID. Due to convenience and the tool's simplicity there are now PHP versions on multiple web pages so that it no longer requires a download. The tool has also been ported to mobile platforms such as iOS and Android.

The largest Internet service provider in Norway, Telenor, has since 2003 offered various wireless routers to home users that subscribe to their broadband service (Telenor 2010). Thomson SpeedTouch is one brand they have used, and many customers are therefore affected by the vulnerability mentioned above.

2.3 Security and Privacy in Households, Enterprises and Society

Insecure WLANs pose risks to many different security aspects. By the term *insecure* I refer to wireless networks that can be exploited due to insufficient encryption. The term will primarily be applied to unencrypted and WEP-encrypted networks, but also to networks with weak WPA passphrases or vulnerable routers. Inspired by *Top 10 Wireless Network Risks* by the risk assessment firm Altius IT (2010), in this subchapter I will present notable risks that are faced by both enterprises and private users.

- *Bandwidth theft* – While perhaps not the most damaging risk, bandwidth theft is very common on unencrypted networks. Unauthorized users can steal Internet bandwidth to download content such as music, video and games, and thus be limiting the experience and productivity for authorized users. In a poll conducted in the United States in December 2010 for the Wi-Fi Alliance, 32 % of the respondents admitted to having

attempted to connect to someone else's network – an increase of 18 percentage points from a December 2008 poll (Wi-Fi Alliance 2011).

- *Masquerade* – Hiding under the name (in this case IP address) of the broadband owner could give access to services and benefits which should not be available to others.
- *Reputation* – Even a relatively innocent breach on an organization's wireless network could be damaging to the company's reputation if the breach becomes publicly known.
- *Confidentiality* – Wireless networks are often connected to in-house private networks. This may allow an intruder to bypass hardware firewalls between the private network and the broadband connection.
- *Litigation* risks – If an intruder uses the internet connection to conduct illegal actions such as distributing pirated software or child pornography, an investigation would trace the actions back to the wireless network and not the perpetrator. Obviously this also applies if the internet connection is used for malicious purposes such as hacking[13] or Denial of Service attacks. There are many incidents where WLAN owners have gotten in trouble due to criminal actions performed through their Internet connection. A recent example was reported by the Associated Press in April 2011, where a man in Buffalo, New York, got his home raided by federal agents with assault weapons (Thompson 2011). Convinced he was a paedophile, they took away his computer, iPads and iPhones to investigate. Within three days the investigators determined the homeowner was innocent. A week later, agents arrested a 25-year-old neighbour and charged him with distribution of child pornography. AP reports in the same article of two other incidents in 2009 and 2010 of similar character.
- *Clear text* – A large amount of information on wireless networks is transmitted in clear and unencrypted text. This makes it possible for an intruder to use a packet analyzer to gain access to confidential data such as e-mail accounts and web browser activity. Basically it lets the intruder monitor everything that is being transmitted over the network. This is commonly done through a man-in-the-middle attack which is illustrated in Figure 2.1 below.

[13] As the media commonly refers to *hacking* as breaking into computer systems or networks, I will also use it in this sense. Some may however argue that the correct term is *cracker*.

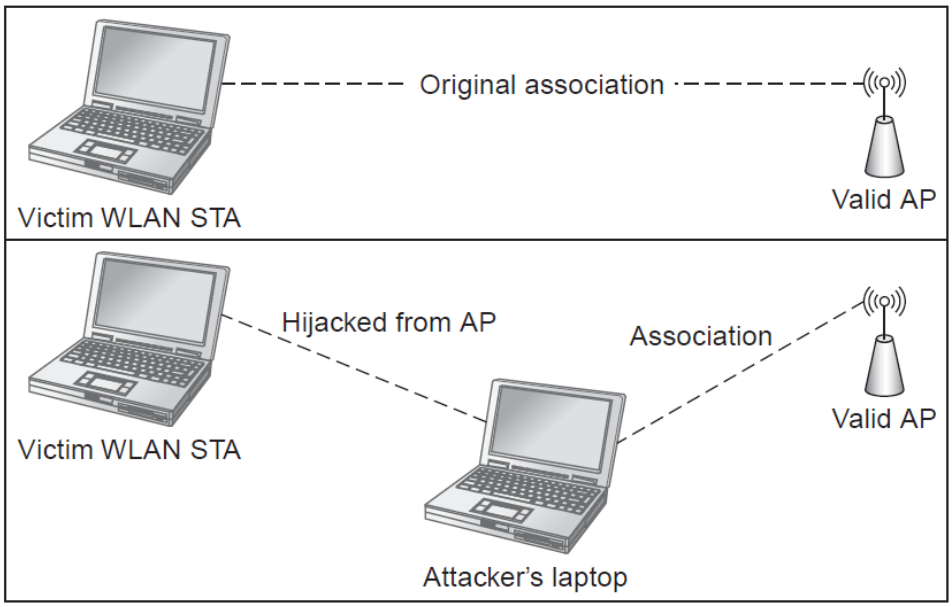

Figure 2.1 – MITM attack (Carpenter and Barrett 2008, 447)

- *Rogue access points* – Wireless access points installed on a company's network without explicit authorization. It can also refer to fake access points created by an adversary to monitor data traffic through man-in-the-middle attacks.
- *Information sensitivity* – Sensitive information such as client lists and trade secrets should not be accessible through wireless networks.

2.3.1 Criminal WLAN Exploitation

October 25, 2011, the Norwegian Broadcasting Corporation ran a documentary on the TV channel NRK that demonstrated how simple breaking into encrypted wireless networks really is. In this documentary Hans-Peder Torgersen, Assistant Chief of Police at Kripos[14], explained that they investigate several cases related to WLAN security. He said that criminals, typically in drug-related cases, use wireless networks to communicate with each other. In cases concerning sexual abuse, Torgersen pointed out that pictures and other content have been distributed through wireless networks. He also mentioned that threat messages are being sent out via WLANs.

The documentary, which partially took place in Sweden, also showed how easy it is to monitor the data traffic on networks that are unencrypted or broken into. To find out the magnitude of credit card trading they visited an online chat channel made for this purpose. The first contact that responded to their request to buy Swedish credit card information

[14] A Norwegian special police division under the Norwegian Ministry of Justice and the Police.

claimed that he had sold 160 Swedish credit cards that day. The journalist in the documentary bought the information for one Swedish credit card and it turned out to be perfectly valid.

2.3.1.1 Consequence of a WLAN Breach

In July 2005, one of the largest known theft of credit cards began outside a Marshalls clothing store in Minnesota (Pereira 2007). According to Joseph Pereira with the Wall Street Journal, investigators believe "hackers pointed a telescope-shaped antenna toward the store and used a laptop computer to decode data streaming through the air between hand-held price-checking devices, cash registers and the store's computers" (2007). This helped them retrieve at least 45.7 million stored credit and debit cards numbers from the central database of the clothing store chain's parent, TJX Companies, Inc. While a person familiar with the internal investigation claimed the number could be as high as 200 million, TJX denied this but admitted at the same time that they might never know precisely. Apparently TJX deleted the logs and was unable to crack the encryption on files left on the system by the hackers. In addition, the perpetrators also got access to 451 000 customers' personal information such as driver's license numbers, military identification and Social Security numbers.

According to Pereira, TJX was using the obsolete WEP encryption for their wireless networks. At the time of the breach, this encryption could easily be cracked within half an hour. Forrester Research analyst, Khalid Kark, expected the breach could cost TJX Companies Inc. somewhere between $500 million and possibly approach $1 billion (Kerber 2007). On the other hand, Sharon Gaudin (2007) reported in InformationWeek that IPLocks, a database security firm, estimated that the bill could reach as high as $4.5 billion ($100 per lost record). Both these estimations were done considering the initial number of stored payment card numbers at 45.7 million. Two years later, Reuters reported that the main perpetrator in the TJX case stole "more than 170 million" payment card numbers from different sources until he was sentenced to 20 years in prison in March 2010 (Finkle and Wahba 2009; Weil 2010).

Privacy Commissioner Jennifer Stoddart said that TJX "collected too much personal information, kept it too long and relied on weak encryption technology to protect it — putting the privacy of millions of its customers at risk" (Jewell 2007). Even though credit card associations have declined to disclose the total damages from the thefts, some banks have said that fraudulent purchases were conducted as far away as Sweden and Hong Kong (Jewell 2007).

In a paper from the wireless security company AirDefense Inc, now acquired by Motorola, several other retail data breaches involving wireless are exemplified (Sinha 2007). The author points out that "many data breaches are never reported as organizations try to minimize the negative publicity and business impact that would result from it" (Sinha 2007, 4).

2.4 National and Societal Security Issues

In 2002, the Norwegian Ministry of Justice and the Police[15] published a White Paper on national security that contained topics on safety measures and crisis management. In pursuant to §6.2.1, economic growth and welfare have been concurrent with the expansion of information and communications technology (ICT), and production and operations management in most social sectors is based on such technology (Ministry of Justice and the Police 2002). The White Paper further states that this dependency has made the society more vulnerable and that a functional ICT is of great importance to crisis management.

In their annual threat assessment for 2011, the Norwegian Police Security Service (PST)[16] reported that illegal intelligence services in Norway "are showing an increased interest in, and capacity for, exploiting the opportunities with cyber-intelligence" (PST 2011, 10). Opportunities are in this case referred to as retrieving sensitive information and acts of sabotage towards our digital society. The PST anticipates increasingly more sophisticated endeavours from foreign states against Norwegian computer networks. The assessment reported that computer network operations is of growing importance in assisting the intelligence services into retrieving sensitive information from both private and public sector in Norway.

NorCERT (The Norwegian Computer Emergency Response Team) reported in November 2011 that they handle 500 attacks on Norwegian computer systems every month (Staveland 2011). Assistant Director, Jeanette Tjaberg, pointed out that mobile phones, social media and tablets have made us more vulnerable to computer attacks than ever before. She also said that even though the threat level has increased significantly, there are few signs of improvement in security (Staveland 2011). Also Secretary General in ICT-Norway, Per Morten Hoff, is frustrated by the current situation. He has claimed that public computer security in Norway is simply a deception (Staveland 2011).

[15] Justis- og politidepartementet.
[16] Politiets sikkerhetstjeneste.

2.5 Similar Studies

Several researchers have already covered the flaws in the encryption aspects concerning wireless networks. The most notable is *Weaknesses in the Key Scheduling Algorithm of RC4* by Fluhrer, Mantin and Shamir (2001), a paper that was the beginning of today's complete breakdown of WEP encryption. Since then there have been several articles and books on exploiting the mentioned RC4 and more recently the encryption protocol TKIP. Due to the extensive research already done on these topics, I do not elaborate on the technical encryption details in this thesis. Instead, I have presented the security protocols superficially as they are the foundation for any research on WLAN security. I will now present studies that are more closely related to my own research.

Hole, Dyrnes and Thorsheim (2005) gathered WLAN data in Bergen in 2004. Their research was conducted in "the city center, which contains many shops and small businesses; Kokstad/Sandsli, an area close to the airport with large businesses; and Fyllingsdalen, a location outside the city centre with many large office buildings" (Hole, Dyrnes, and Thorsheim 2005, 29). Out of the 706 WLANs they detected by *war-walking* and *war-driving*, more than 500 were in city centre. By the terms war-walking and war-driving they refer to walking or driving with a portable computer in search of multiple wireless networks. Their article also says that 244 of the 706 networks were using WEP, but does not mention how many were using WPA. Thorsheim explained[17] that this was because the software they used at the time did not separate between WEP and WPA. If they came across any WPA encryption, it was probably a rarity as WPA was introduced the same year they did the research, and the encryption was not supported in older operating systems such as Windows 95 (NETGEAR 2011). Hole, Dyrnes and Thorsheim could not with certainty conclude that the remaining 462 networks "transmit in the clear" (2005, 29). However, random spot checks strongly indicated that many WLANs did not have any form of encryption.

While no similar war-drive has been publicly presented in Norway since then, internationally the situation is different. A notable study of WLAN security is conducted by PISA (Professional Information Security Association) and WTIA (Hong Kong Wireless Technology Industry Association) every year since 2002 in Hong Kong (PISA and WTIA 2011). Their latest research from December 2010 showed that 34 % of the WLANs they detected were using WEP encryption. Although it is a large decrease from 45 % in 2009, they point out that

[17] E-mail correspondence with Per Øyvind Thorsheim, 14.04.2011.

they are far from satisfied due to the simplicity of cracking WEP. Unencrypted networks went down only 2 percentage points to 14 %, but WPA/WPA2 went from 39 % to 52 %. Overall they concluded with “some improvement in WLAN security implementation in Hong Kong” over the previous year (PISA and WTIA 2011, 17). Additionally, the total number of detected access points was 16 462 – a slight increase from 15 753 in 2009. Only 7 388 WLANs were detected in 2008.

3 RESEARCH Method

In this thesis I make use of the quantitative research method which consists of "the collection of data in numerical form for quantitative analysis" (Jupp 2006, 250). The data obtained through this method is converted to numerical values through measurement methods such as counting and scaling (Punch 2005). As a result, comparisons are possible and the findings can be subject to statistical analysis.

To discover the scope of insecure WLANs I decided to use a quantitative sampling method to gather access point data in five cities in different geographical parts of Norway. In this chapter I explain the practical process and the reasons behind the selection of geographical areas to research. I also present the methods I employed to gather the data and the limitations and ethical concerns I encountered during the process.

3.1 Locations of Data Sampling

In my research I decided to focus on city centres where I was likely to find a high WLAN density. In some cases I was able to use the municipalities' own area plans as guidance to what was considered their city centre. Especially Bergen, Kristiansand and Tromsø provided good information and maps for this (Iversen 2011; Aardal 2011; Ledingham 2010). In some of the cities I also did research in additional areas with high population density.

Limited time and resources required me to make a strategic decision about where to collect my data material. The five cities I chose were Oslo, Bergen, Kristiansand, Tromsø and Flekkefjord. Oslo is the capital of Norway and with a population of 592 000 citizens, the largest city in Norway. It also has the highest population density. Bergen is the second largest city with 258 000 citizens and consequently largest on the west coast. With its 68 000 citizens, Tromsø is the largest city in the northern Norway, and Kristiansand is the largest city in the south with 82 000 citizens. Contrary to the rest of the cities in the selection, Flekkefjord is a small town with only 9 000 citizens.

The choice of cities was based on their location and population size. The capital, Oslo, was a natural choice due to its size, status and eastern location. While there are two large cities in the western part of Norway, namely Stavanger and Bergen, I chose the latter because it is larger and also the city where I currently live. In the northern part of Norway I chose Tromsø over the quite larger Trondheim for a couple reasons. First of all, Tromsø is more than 1 000

kilometres north of Trondheim and is thus a better representative for the northern population. Secondly, the practicality of having acquaintances in Tromsø who knew the city would be beneficial in terms of gathering network data in an efficient manner. In the south, Kristiansand was a natural choice due to its population size and the structural layout of the streets in the city centre. Despite its 110 kilometre proximity to Kristiansand, the last city I chose was my hometown Flekkefjord. As I lived there for almost 20 years, it was easy to decide in what areas to gather access point information. For that reason I also conducted initial testing in Flekkefjord to be able to gather data effectively and efficiently.

3.2 War-walking and Technical Equipment

Even though other research methods such as interviews or surveys were possible, tools that automatize the method of gathering WLAN data return a larger amount of raw data material. It would also have been possible to get information from data collected by others, but doing it myself gave me several advantages compared to the alternative. Wigle[18] is an example of a source with user-submitted data, where its database contains more than 50 million access points worldwide. But no removal of old submissions and not separating between encryption protocols were two critical reasons why I could not use its data. There were three factors that made me want to gather the data the way I did. First of all, I could choose the areas to conduct my research. While there are articles that present systematic data collections of access point information, these have rarely been conducted in Norway. Secondly, I would get all the raw data possible and thus be able to look for other interesting material and anomalies. Thirdly, my method of gathering data would be more relevant because it would be recent and conducted in a relatively short time span.

While I could have used vehicles to cover a greater area and collect data from a larger number of WLANs, I mainly walked and prioritized network density instead. The reason for this was that I expect that in most scenarios where there is a security breach on a wireless network, the attack is likely coming from a neighbouring perpetrator. Commencing an attack from outdoors in open areas with few houses are also more likely to look suspicious. In addition, in areas with high WLAN density an attacker could receive sensitive information from more sources simultaneously than in areas with low density. Gathering data by foot also allowed me to detect wireless networks in areas unavailable to vehicles.

[18] The Wigle web page can be found at: http://www.wigle.net/

However, deciding how much time to spend on gathering data was not an easy task. Even though covering a big area could have been faster by using motorized vehicles, it would also have shown fewer wireless networks per distance. This is because wireless access points in Europe broadcasts on 13 different channels. In order to receive the information I needed, my wireless interface controllers (WLAN cards) had to listen on every channel for a certain period of time (Carpenter and Barrett 2008). Passing an access point in high speed could therefore cause my setup not to see the access point. I intended to reduce this problem by using two network cards and thereby be listening on two different channels simultaneously. Nevertheless, my tests and the aforementioned reasons led me to choose war-walking as the main method of data sampling.

3.2.1 Data Sampling: War-walking

In practice, my research was conducted by war-walking with a laptop computer, an extra battery, a USB connected GPS and two WLAN cards. USB connection for the GPS was specifically chosen over Bluetooth interface due to the potential interference in the 2.4 GHz spectrum. The GPS was pinpointing my positions where I detected the various access points and proved helpful in my analysis of the data afterwards. I decided to keep the laptop, WLAN cards and antennas inside a bag to avoid unsettling bystanders, and to be able to gather data without being interfered. Because the GPS device was much more discrete it allowed me to have it attached on the outside of the bag, which presumably made the reception better. Forcing the Wi-Fi antennas to work through an extra layer is not ideal, but I decided the minimal loss of gain to be an acceptable compromise. Due to the nature of the research I conducted I believe this compromise had little impact on my results.

Figure 3.1 – Bag containing GPS, 2 dBi and 7 dBi omnidirectional antennas

3.2.2 Data Sampling: Hardware

For convenience purposes I used a small netbook with 9” screen with a battery that lasted 5 hours. I expected this to be sufficient for a single day, but I also brought a two-hour battery for unexpected circumstances. The two different network cards I used both had the RTL8187L chipset from Realtek which performs very well in Linux. Unfortunately this chipset is only operating at 2.4 GHz frequencies and will not see access points that are only broadcasting at 5 GHz. This means that the new 802.11n access points that are only broadcasting at 5 GHz, as well as access points set to the old 802.11a standard, will not be detected by my network cards. Fortunately, most 802.11n WLANs only support 2.4 GHz and the dual band ones are typically broadcasting on both 2.4 GHz and 5 GHz simultaneously. At the time of my war-walk, 802.11n chipsets were poorly supported in war-walking software.

With these two network cards, I used an omnidirectional antenna with 2 dBi gain on one card and a 7 dBi omnidirectional antenna on the other card. Omnidirectional simply means a 360-degree horizontal radiation pattern, and gain is a measurement of directionality (Carpenter and Barrett 2008). While a 7 dBi antenna reaches relatively far, it is not good at picking up access points located on higher floors. There are, however, cases where WLANs on very high floors can be detected if their Radio Frequency (RF) signal is being reflected downwards. For instance will drywalls and windows absorbs less dB than concrete and metal (Carpenter and Barrett 2008). A 2 dBi antenna is better for detecting WLANs on higher floors, but does not reach as far horizontally as an antenna with higher gain. So by using two different antennas I would in theory detect more access points. Cisco Systems, Inc. (2007) compares this antenna radiation pattern to what happens when placing pressure on the top and bottom of a balloon. In doing so, the balloon will expand in an outward direction and cover more horizontal space and at the same time reduce vertical space. I made an illustration of this below in Figure 3.2:

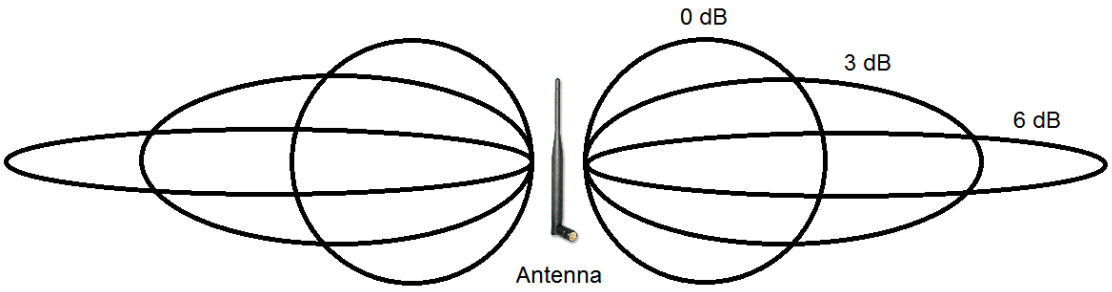

Figure 3.2 – Antenna coverage based on dB. For illustrative purposes only

3.2.3 Access Point Detection Software

In quantitative research, the use of software is beneficiary due to the magnitude of raw data material in need of post-processing (Marczyk, DeMatteo, and Festinger 2005). For my study, I used the Linux distribution Ubuntu and the open source software Kismet[19] to gather the wireless data packets. Kismet is an "802.11 wireless network detector, sniffer, and intrusion detection system" (Kershaw 2011). This software allowed me to automate the search for wireless access points and simultaneously save their GPS location. In addition, using a Linux distribution made it possible to set the network cards into *monitor mode*, which makes it possible to perform passive scanning in Kismet (Cache, Wright, and Liu 2010). Tools that can perform passive scanning only listen to the surrounding data packets and never transmit anything. This leads to better results than if I was to use a scanner in Windows such as NetStumbler where support for monitor mode is absent (Cache, Wright, and Liu 2010).

Kismet also let me have one network card listen on one channel and the other network card on another. As I used the default rate of hopping through 3 channels per second, in practice it meant 6 channels per second because of the two network cards. I also configured Kismet to stay longer on channels 1, 6 and 11 which are the most common by far. Overall, the Operating System and software I used to detect access points proved to be useful and consistent.

3.3 Documentary Data

Written historical and contemporary documents are important sources of information within social research. "In conjunction with other data, documents can be important in triangulation, where an intersecting set of different methods and data types is used in a single project" (Denzin 1989 in Punch 2005, 184). In my case, my documentary sources of data included expert statements, government papers, official statistics and online discussion forums.

The war-walk I conducted was intended to answer questions I had related to WLAN security in Oslo, Bergen, Tromsø, Kristiansand and Flekkefjord. While it answered most of my questions, including giving me a large amount of information concerning preconfigured routers from the ISPs, it was not sufficient. For that reason I had to seek information directly from the Internet service providers as well as from additional sources.

When researching ISP encryption practices I tried getting the information directly from the companies' spoke persons. While I had e-mail correspondences with Telenor, Canal Digital,

[19] The Kismet web page can be found at: http://www.kismetwireless.net/

NextGenTel, Ventelo and GET, it was limited as to what they were willing to reveal due to the sensitivity of the subject. This led me into retrieving supplementary data from media, online discussion forums and through private conversations via Internet Relay Chat (IRC).

To find relevant information on WLAN encryption usage in Norway, I started out by searching through academic databases, master's theses, various web pages and other relevant sources. As I found little research done on WLANs in Norway, I contacted several institutions and persons connected to ICT security. While none of them were aware of related work, there was a large amount of interest towards my research. I also contacted Hole, Dyrnes and Thorsheim to get more information about their research from 2004, but their raw data was unfortunately not available anymore.

3.4 Preparation of Data

Collected data material should be "organized into a database that will facilitate accurate and efficient statistical analysis" (Marczyk, DeMatteo, and Festinger 2005, 199). Consequently, to be able to analyse my data in an efficient manner, I initially created a Java-based tool that parsed information from the raw files made by Kismet. I then discovered the python application GISKismet[20], which stores the data from Kismet into a SQLite database (Cache, Wright, and Liu 2010). Being able to use SQL queries simplified the process of analysing the data material considerably. The database contained the following variables: SSID, MAC address of router, manufacturer, broadcast channel, cloaked/visible, encryption, first and last time seen, minimum and maximum in addition to best (measured from signal reception) latitude, longitude and altitude. The database also contained more technical details, as well as MAC address and manufacturer of clients connected to the networks. For the post processing analysis I used SQLite Expert Personal[21] to run the SQL queries. This software proved very useful in looking for patterns and irregularities in WLAN security practice.

GISKismet also lets you use the Kismet logs to create files that show the access points in a graphical view on Google Earth, and I used this graphical view to verify the exact routes I took when gathering data. In addition to the GPS data from Kismet, I used the smartphone application RunKeeper that also logged my positions via GPS. This made it possible to have location data available even if the logging system in Kismet were to fail. I also considered a more practical alternative in the iPhone application WiFiFoFum, presented by Cache, Wright

[20] The GISKismet web page can be found at: http://www.giskismet.org/
[21] The SQLite Expert Personal web page can be found at: http://www.sqliteexpert.com/

and Liu (2010) in *Hacking Exposed Wireless: Wireless Security Secrets & Solutions*. But after some testing I found that Kismet, combined with good wireless equipment on a notebook, detected significantly more WLANs.

I originally intended to present the wireless networks graphically. Figure 3.3 below is an example from the GISKismet web page that shows how WLANs can be represented in Google Earth. The various colours of the circles indicate the encryption being used.

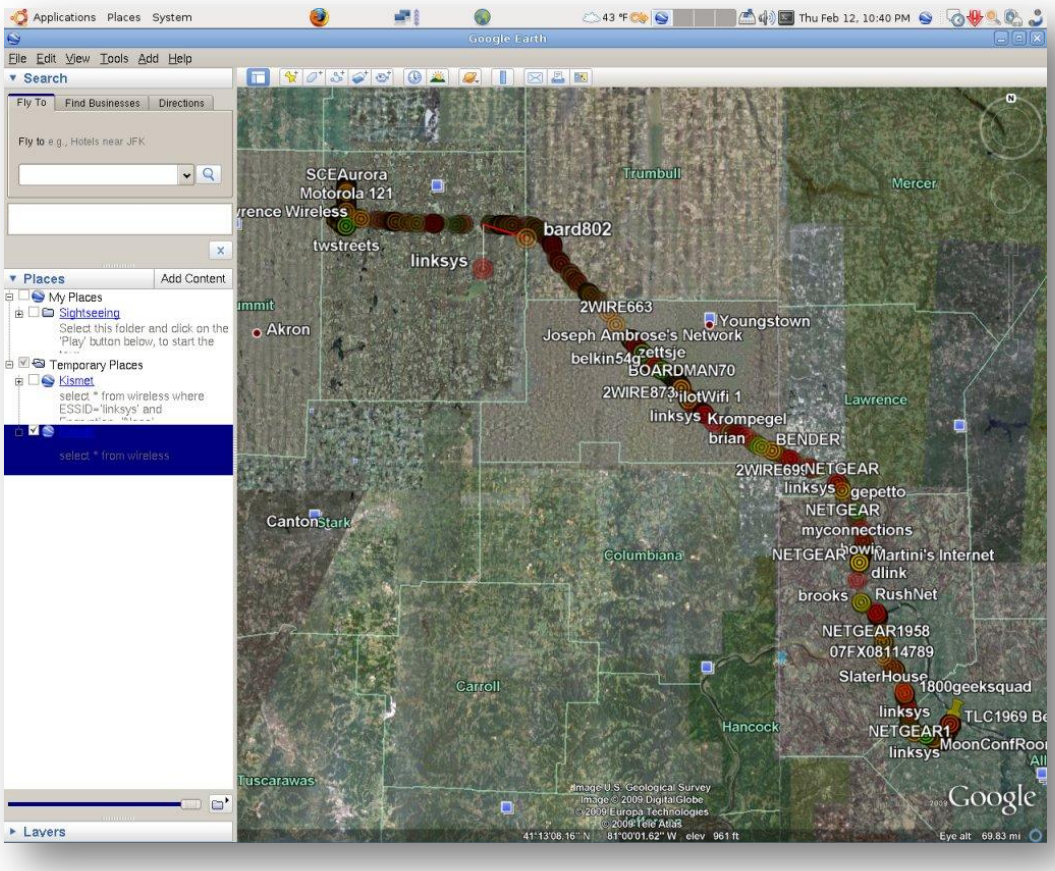

Figure 3.3 – WLAN representation example from the GISKismet web page

However, I decided that protection of privacy had to be preserved. Instead of doing a compromise of scrambling information such as SSID or GPS position that could identify the WLAN owners, I opted for a map visualisation of routes and areas I covered. This would also circumvent potential erroneous GPS readings caused by the urban canyon effect. In order to measure the distance of the routes, I used Google Maps' Distance Measurement Tool. This tool calculates the distance of drawn lines in Google Maps, and allowed me to estimate WLAN density in the various locations. To be sure of reliable estimates I compared these measurements to the distance results I got from RunKeeper.

3.5 Reliability and Validity

In order to support and consolidate my study and findings, this sub-chapter explores the *reliability* and *validity* of my research. I will first present reliability and its correlation to my research, followed by three categories of validity.

3.5.1 Reliability

Reliability depends on the accuracy and consistency of gathering data and its post-processing (Johannessen, Tufte, and Kristoffersen 2004). A reliable measurement returns a lesser chance of the results being prone to random factors and measurement error. Hence, the need for stable hardware and software, as well as testing rounds, is imperative. Johannesen, Tufte and Kristoffersen (2004) explain that a common testing method to check for data reliability is to repeat the research on the same group, for instance after 2-3 weeks. If the results are the same, the data has high reliability. This testing method in particular is called *test-retest* reliability. There is also high reliability if other researchers who investigate the same phenomena retrieve the same results. The term for this is *inter-rater* reliability (Johannessen, Tufte, and Kristoffersen 2004).

The unforeseen aspects of wireless technology would prevent some networks from being seen in a second run, but would also find networks I did not find in the first run. Such aspects include uncontrollable factors such as weather (even though its impact is mild) and moving objects such as cars and humans. Nevertheless, the encryption usage ratios should be fairly accurate. In terms of hardware and software, I already possessed knowledge regarding compatibility and the wireless equipment that would return accurate results. Furthermore, both the chipset (RTL8187L) and the software (Kismet and GISKismet) I used were recommended in *Hacking exposed wireless: wireless security secrets & solutions* by Cache, Wright and Liu *(2010)*.

Even though I planned the routes thoroughly, it is evident that I could not register all access points in the areas and that there were several factors that had influence on my research. Firstly, as my research was conducted outside and included electronic equipment I was relying on good weather. Even though it was possible to gather data while it was mildly raining or snowing, I faced some difficulties when I needed to modify configurations or making sure everything was working properly. Another factor is that heavy rain and snow affects RF signals, and could in theory reduce the number of detected access points (Carpenter and Barrett 2008).

Secondly, access points have limited broadcast range and the signal strength can also be manually reduced to keep the wireless packets within the building. Thick walls and a poor placement of the access point can also make it difficult for outside war-walking. In addition, access points do not handle broadcasting to different floors very well. Influencing variables are chipsets used, bitrate, weather, wall material, objects in between and so on (Carpenter and Barrett 2008). Such variables make it impossible to do an estimation of what floors I was able to see access points on. While it could be possible to see an access point on the 10th floor because the signal is bouncing of a neighbouring house, an access point on 2nd floor, obstructed by concrete, could be unreachable.

Thirdly, while I used two network cards and different antennas, I still needed to cycle through the broadcasting channels to be able to find the networks. The optimal solution to avoid this would be to use one network card for each of the 13 channels. But having 13 different network cards and antennas in a small bag would not only be chaotic, but also create a large amount of heat. Packing such equipment close together also reduces its reception potential. It would be possible for that type of war-driving setup in a vehicle, but this prevents search for networks in narrow streets and alleys.

Fourthly and finally, because my research was based on gathering data in an unobtrusive manner, my results only show the encryption broadcasted by the access points. This means that even if the wireless network had encryption at layer 3 such as VPN, it would not show in my results. Connecting to a network in order to retrieve such information is illegal without the consent of the WLAN owner.

All these factors show that in this kind of research the technical equipment has great importance for the gained results. Therefore, if the research was to be repeated in order to ensure reliability, similar equipment and data collection method should be employed. If the control sampling is done within a short time span and follows my recommendations, I believe the results would be similar to mine and have high reliability as such.

3.5.2 Validity

Data validity refers to how well the gathered data is representing the researched phenomena. The term poses the question “are we measuring what we intend to measure?” (Johannessen, Tufte, and Kristoffersen 2004, 195). I will now present three commonly used categories of data validity.

3.5.2.1 Construct Validity

Construct validity concerns the relation between the research subject and the specific data measured (Johannessen, Tufte, and Kristoffersen 2004). Regarding my research and my first research question on encryption usage on WLANs, this refers to how well war-walking/war-driving is accurate in establishing WLAN security practice. It also refers to my approach to discovering information about the ISP's practices.

Prior to gathering access point data I contacted the Data Inspectorate[22] and the Norwegian Post and Telecommunications Authority[23], enquiring about WLAN security practice and similar research. This led to referrals to various persons such as university professors and Telenor employees. Trying to find statistics and usable data I also contacted other organizations such as the Norwegian Centre for Information Security[24] (NorSIS). None of these sources returned relevant data. The lack of existing data for my first research question led me into conducting the war-walk/war-drive in order to retrieve valuable information regarding WLAN security. I considered other approaches such as surveys and interviews, but the amount of unique user data would be insufficient. I would also have faced difficulties in that security questions about wireless access points are rather technical, and answers could consequently be lacking in detail.

In cases where the relation between research method and expected result appears convincing, the term *face validity* is used (Johannessen, Tufte, and Kristoffersen 2004). In this thesis, war-walking as a research method has face validity when it comes to establishing WLAN encryption usage.

3.5.2.2 Internal Validity

"A study has internal validity to the extent that the data support conclusions about the hypothesis in the specific instance studied" (Stern and Kalof 1996, 62). In other words, *internal validity* refers to the validity of the conclusions in general, regarding whether or not they are rightfully drawn from the data material. For instance, in my thesis I will draw conclusions from the data material I have gathered regarding security issues and user practices. I will carefully go through the process towards these conclusions in order to ensure the validity of them. In order to explore end-user reasoning in terms of WLAN security, the most appropriate research method would have been a qualitative research, including

[22] Datatilsynet.
[23] Post- og teletilsynet.
[24] Norsk senter for Informasjonssikring.

interviews. But as end-user reasoning is not the main focus of this thesis, I decided that the potential end product would not weigh up for the time and resources spent. I will, however, include a discussion concerning both assumptions and speculation on user practices regarding WLAN security.

Regarding my second research question on how ISPs are affecting the situation, some conclusions are drawn from personal correspondences and documentary data such as articles and statistics. However, the majority of the conclusions are based on the research data retrieved from war-walking. I also combined these approaches in order to enhance the validity of my findings through data triangulation. The validity increases by matching the data from the war-walk to the documentary data (Frankfort-Nachmias and Nachmias 2008).

Internal validity also refers to the extent to which the gained results show a causal relationship between the variables (Johannessen, Tufte, and Kristoffersen 2004). Even though my research is primarily a descriptive study, cause-effect relations are apparent in research questions 1b and 3a where location, population size and time are variables that affect my findings. For instance, there is a causal relation between preconfigured access points and encryption strength. Nonetheless, these occurrences can be affected by end-users and have therefore a lesser internal validity.

3.5.2.3 External Validity

External validity refers to the extent to which the data results can be held true to similar research with varying factors of location and time (Johannessen, Tufte, and Kristoffersen 2004). As my research subject is changing rapidly in relation to technology expansion and internet dependency, a later similar research will have variations depending on growth of WLAN usage and change in security practices. Another factor is that the security focus could be stronger in areas with higher population density. Additionally, findings from gathering data similarly in other locations will be affected by the propagation of the various broadband providers who deliver preconfigured wireless access points.

Even though my research shows certain patterns that might be valid for a greater area, my data sample is too small to generalize WLAN security on a national level. I did, however, attempt to cover a typical selection of the Norwegian cities and some of their most populated areas. By doing this I believe I got a representative selection for real life scenarios of WLAN attacks. Therefore, through choosing a sample that reflects the characteristics of the population of interest, I attempted to ensure the external validity of my findings (Frankfort-

Nachmias and Nachmias 2008). In this way, even though not generalizable, my findings should give a pointer on the current security situation. Furthermore, the problems and solutions discussed in this thesis are relevant in every society with wireless networks.

3.6 Ethical Concerns

As my research concerned sensitive and security-related data, it was important not to cross ethical or legal boundaries. Additionally, because this research was done without consent from the WLAN owners, issues of privacy, anonymity and confidentiality were essential (Frankfort-Nachmias and Nachmias 2008).

Prior to the war-walk I needed to make sure that my research method would not interfere with network data traffic. I therefore set my network cards into monitor mode and configured Kismet to log only the public information the access points were broadcasting. To ensure that I did not log any traffic I contacted Mike Kershaw, the developer of Kismet, and he was kind enough to add a setting that filtered away the data payload. By enabling this setting, Kismet ignored all the user traffic and only retrieved the header showing the access point information I needed. In reality, this made it have less interference on the networks than most Operating Systems do when they are searching for WLANs to connect to.

Subsequent to the war-walk I still possessed information that could be sensitive if treated improperly. The most obvious problem was the relation between location and SSID. This risk of identification, and consequent exposure of private home owners to criminal activity, was the reason why I refrained from including combinations of location and SSID together. In order to provide anonymity I needed to separate "the identity of individuals from the information they give" (Frankfort-Nachmias and Nachmias 2008, 78).

In certain parts of this thesis it may appear as undisclosed information regarding WLAN security practices is being revealed. However, all data was gathered through either publicly available information sources online or through e-mail conversations with Internet providers' spokespersons. No information was gathered through illegal or unethical channels.

4 RESEARCH FINDINGS: INSECURE WLANS AND VULNERABLE ISP ROUTERS

With regard to my first research question, *What is the current state of WLAN encryption in Norway?*, I will start in this chapter by presenting an overview of the areas and routes where I detected wireless networks. I will then present the encryption data and show comparisons and patterns that form the foundation for the discussion chapter. Lastly, and in order to investigate my second research question, *How are Internet service providers affecting the situation?*, I will present data of potentially problematic wireless routers distributed by Norwegian ISPs.

I am primarily focusing on unencrypted and WEP-encrypted networks because these pose the biggest threat. However, in the following results I will also include networks that for various reasons can be broken into, even if they use a stronger encryption. The data was gathered in the 4th quarter of 2010.

4.1 Routes of War-walking and War-driving

While the war-walking routes were planned ahead, detours were taken if I discovered other areas that presumably had a high density of wireless networks. As previously mentioned, to measure the distance of the routes, I used the distance measurement tool in Google Maps. I will now present the routes taken and the results focusing on encryption protocols. By doing so I intend to show the wireless network encryption distribution and whether city population or location is an influencing factor. Note that WLANs are so widespread that I detected new access points every few metres on every street in every city. My findings are presented city-by-city in order of population size.

4.1.1 Oslo

Figure 4.1 – War-walking/war-driving route in Oslo

The distance I covered in Oslo totalled to 47 kilometres. In average, for every 2.3 meters I detected a new WLAN. Due to the high number of business offices and retail stores in the city centre, I also used public transportation to reach areas further away. While I was walking in the areas around The Royal Palace, Majorstuen, Grønland, Torshov and St. Hanshaugen, I also took a bus that went up north to Nordberg that passed through several residential areas. Because a slower movement in theory detects more WLANs, it would be inaccurate to some extent to directly compare metres per network with other cities where I did not use vehicles.

From the 20 552 WLANs I detected in Oslo, I got the following results:

- 12.9 % or 2 649 WLANs were unencrypted.
- 21.2 % or 4 356 WLANs had WEP encryption.
- 65.9 % or 13 547 WLANs had stronger encryption.
    - 12 624 used PSK.
    - 923 used 802.1X.

4.1.2 Bergen

Figure 4.2 – War-walking route in Bergen

In Bergen I gathered WLAN information in the areas Møhlenpris, Nygårdshøyden, Grieghallen, Torgallmenningen and Nordnes. In these areas I found a total of 6 927 WLANs on a walked distance of 16 kilometres. That means that for every 2.3 metres I detected a new WLAN.

From the 6 927 WLANs I detected in Bergen, I got the following results:

- 14.8 % or 1 028 WLANs were unencrypted.
- 19.1 % or 1 322 WLANs had WEP encryption.
- 66.1 % or 4 577 WLANs had stronger encryption.
    - 4 253 used PSK.
    - 324 used 802.1X.

4.1.3 Kristiansand

Figure 4.3 – War-walking route in Kristiansand

As Figure 4.3 shows, the city blocks in the centre of Kristiansand are shaped in a rectangular form. This made it easy to plan an efficient path to register a high number of WLANs. Through 7.6 kilometres of war-walking I found 2 230 wireless networks, meaning one access point for every 3.4 metres.

From the 2 230 WLANs I detected in Kristiansand, I got the following results:

- 17.4 % or 387 WLANs were unencrypted.
- 23.7 % or 529 WLANs had WEP encryption.
- 58.9 % or 1 314 WLANs had stronger encryption.
    - 1 248 used PSK.
    - 66 used 802.1X.

4.1.4 Tromsø

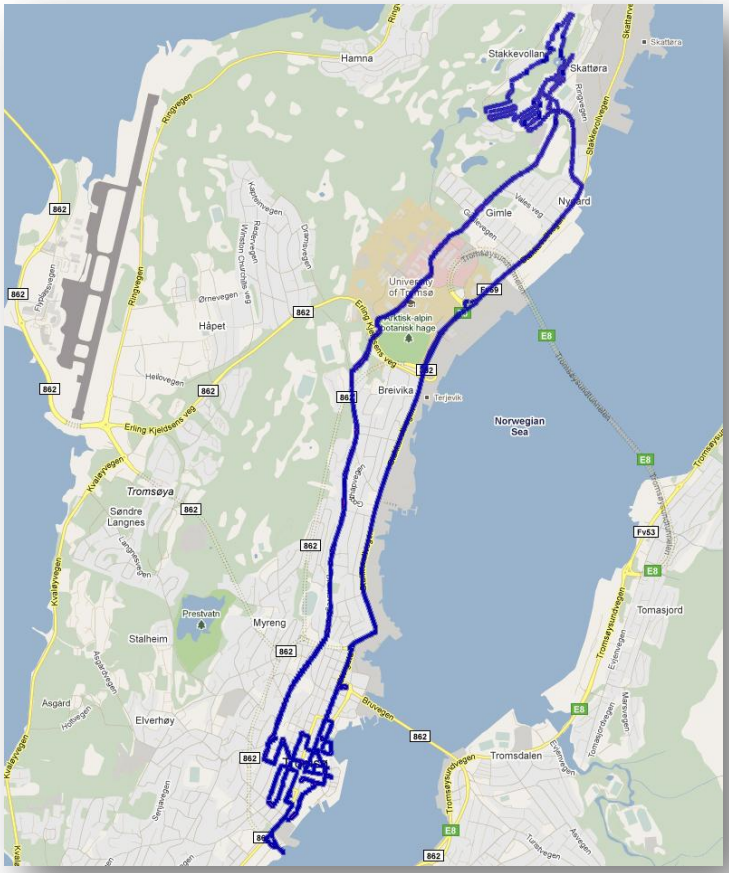

Figure 4.4 – War-walking/war-driving route in Tromsø

The total distance I travelled while gathering data in Tromsø was 35 kilometres. As I found 4 273 WLANs, I discovered a new one every 8.2 metres. However, I made two roundtrips of 12 kilometres each from a housing cooperative in the north to the city centre in the south. I chose to include these overlapping roads when calculating the distance because additional wireless networks are discovered when routes are repeated. Therefore, retracting 12 kilometres from the total 35 would not necessarily return a more accurate measurement of distance travelled per WLAN.

From the 4 273 WLANs I detected in Tromsø, I got the following results:

- 17.0 % or 728 WLANs were unencrypted.
- 23.3 % or 997 WLANs had WEP encryption.
- 59.6 % or 2 548 WLANs had stronger encryption.
    - 2 238 used PSK.
    - 310 used 802.1X.

4.1.5 Flekkefjord

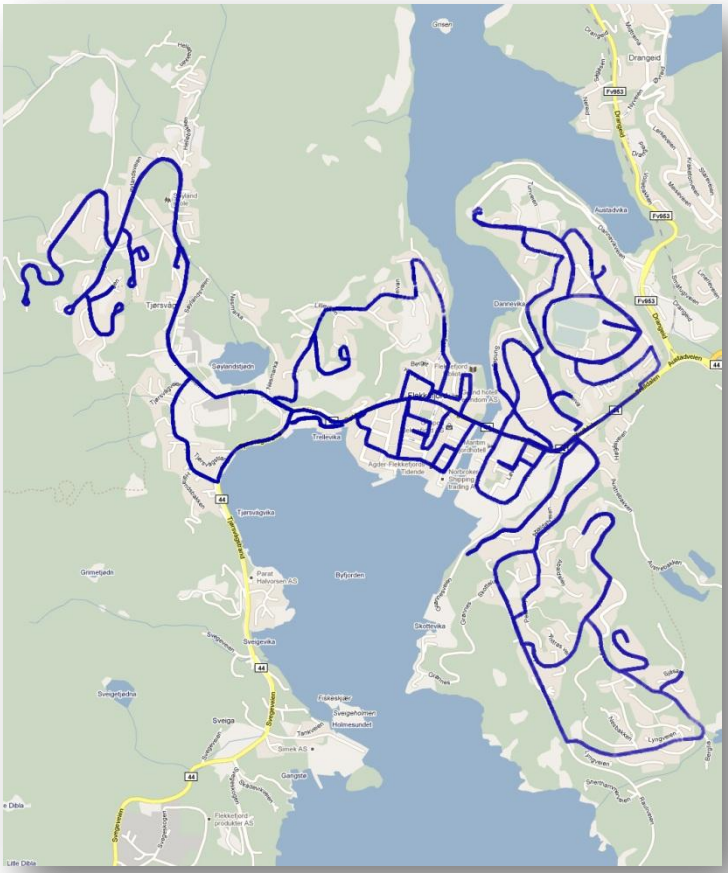

Figure 4.5 – War-driving route in Flekkefjord

Due to the lower density of private homes and WLANs in Flekkefjord I used a car for the entire distance of gathering data. After two hours of very slow driving I had gathered information about 1 212 wireless networks. As I calculated the total distance to be 31 kilometres, a WLAN was detected every 25.6 metres. While gathering access points in Oslo, Bergen and Kristiansand could be performed without much overlapping of roads, many dead ends in Flekkefjord had an effect on the WLANs per metre ratio. For the same reason as in Tromsø, I chose to include the overlapping roads when measuring the distance driven.

From the 1 212 WLANs I detected in Flekkefjord, I got the following results:

- 17.0 % or 206 WLANs were unencrypted.
- 33.2 % or 402 WLANs had WEP encryption.
- 49.8 % or 604 WLANs had stronger encryption.
    - 580 used PSK.
    - 24 used 802.1X.

4.2 Encryption Data

I will now present comparisons in encryption usage between the cities. Table 4.1 shows the specific number of WLANs using the various encryptions. Chart 4.1 displays this in percentage to easier show the similarities. Finally, Chart 4.2 combines the number of networks from all cities and shows a clear majority of PSK + 802.1X.

City	Unencrypted	WEP	PSK	802.1X	Total
Oslo	2 649	4 356	12 624	923	20 552
Bergen	1 028	1 322	4 253	324	6 927
Kristiansand	387	529	1 248	66	2 230
Tromsø	728	997	2 238	310	4 273
Flekkefjord	206	402	580	24	1 212
Total	4 998	7606	20943	1 647	35 194

Table 4.1 – Encryption distribution in the sampled cities

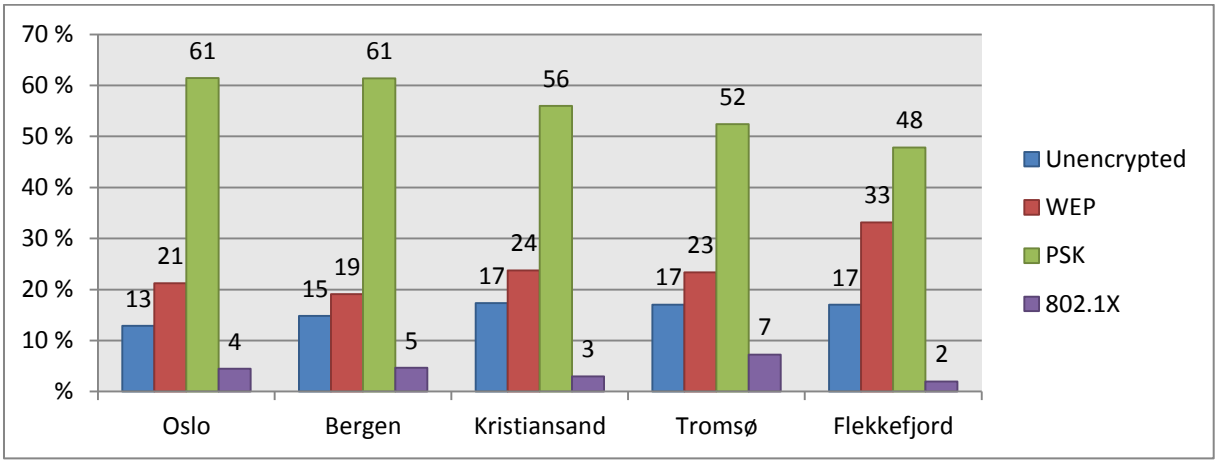

Chart 4.1 – Encryption distribution in the sampled cities, in percentage

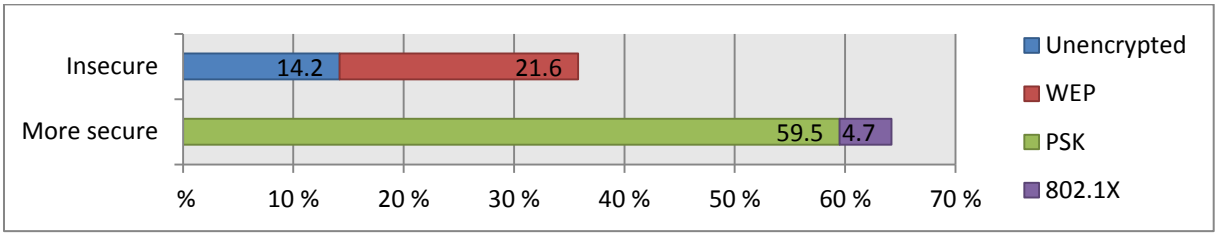

Chart 4.2 – Encryption distribution, insecure vs. more secure

In the following Table 4.2, I have placed unencrypted and WEP-encrypted networks in one category, and networks with PSK and 802.1X in another. My intention is to show that even though many wireless networks are relatively secure, an alarming amount is still insecure.

City	Unencrypted + WEP	PSK + 802.1X
Oslo	7 005	13 547
Bergen	2 350	4 577
Kristiansand	916	1 314
Tromsø	1 725	2 548
Flekkefjord	608	604

Table 4.2 – Encryption distribution, Unencrypted+WEP vs. PSK+802.1X

Chart 4.3 below does not only show that there is a very high percentage of insecure networks, but also a pattern of better encryption usage in larger cities.

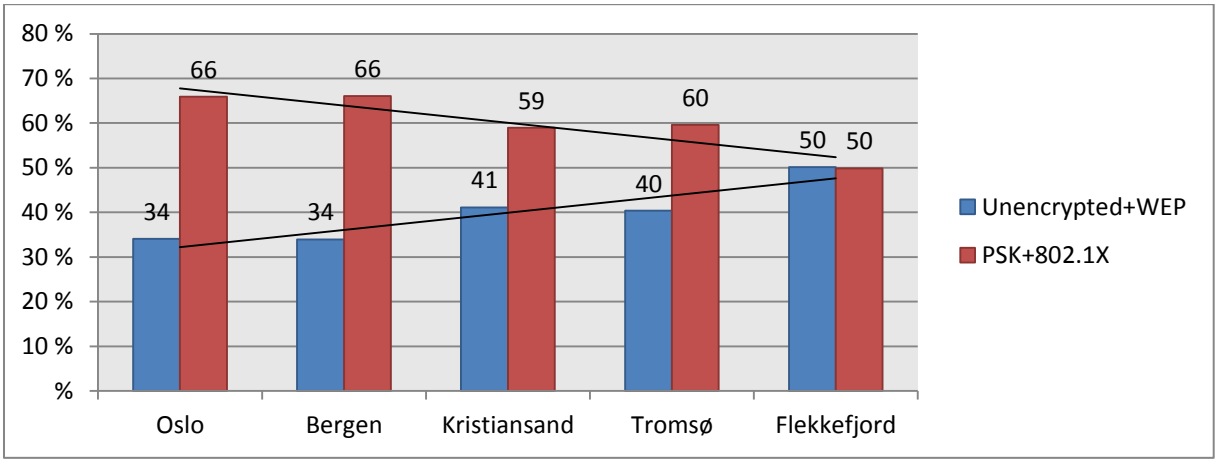

Chart 4.3 – Encryption distribution, Unencrypted+WEP vs. PSK+802.1X, in percentage

4.2.1 Cloaked SSIDs

Most wireless routers have the option to disable the broadcast of SSID. Disabling this setting requires the users to enter the SSID the first time they connect, instead of selecting it from a list. In this subchapter I will present encryption usage related to cloaked SSID, with the intention of establishing similarities or differences to visible networks. In the following tables I will show that the percentage of less secure networks tends to be higher if the network is cloaked. However, due to my relatively small data sample and the consequent low number of cloaked networks found in the cities (perhaps except for Oslo), my findings may not be completely representative. Nevertheless, I have chosen to include these results as there seems to be an interesting pattern.

In Oslo there were 844 routers out of 20 552 that had cloaked SSID. 84 of these were unencrypted and 246 used WEP.

Oslo	Visible	Cloaked
Unencrypted	13.0 %	10.0 %
WEP	20.9 %	29.1 %
WPA/WPA2	66.1 %	60.9 %

Table 4.3 – Visible and cloaked networks in Oslo

For Bergen the results were similar. I detected 272 cloaked WLANs out of 6 927, of which 60 were unencrypted and 75 used WEP.

Bergen	Visible	Cloaked
Unencrypted	14.5 %	22.1 %
WEP	18.7 %	27.6 %
WPA/WPA2	66.8 %	50.3 %

Table 4.4 – Visible and cloaked networks in Bergen

Out of 2 230 WLANs in Kristiansand, 59 were cloaked. Only 5 of these were unencrypted and 23 used WEP.

Kristiansand	Visible	Cloaked
Unencrypted	17.6 %	8.5 %
WEP	23.3 %	39.0 %
WPA/WPA2	59.1 %	52.5 %

Table 4.5 – Visible and cloaked networks in Kristiansand

In Tromsø I detected 138 networks that were cloaked out of 4 273. 20 of these were unencrypted and 56 had WEP encryption.

Tromsø	Visible	Cloaked
Unencrypted	17.1 %	14.5 %
WEP	22.8 %	40.6 %
WPA/WPA2	60.1 %	44.9 %

Table 4.6 – Visible and cloaked networks in Tromsø

Flekkefjord had only 16 cloaked WLANs out of a total 1 212. Out of these were 3 encrypted with WEP and 3 unencrypted. Note that the margin of error here is higher due to very few cloaked networks in Flekkefjord.

Flekkefjord	Visible	Cloaked
Unencrypted	17.0 %	18.8 %
WEP	33.4 %	18.8 %
WPA/WPA2	49.6 %	62.4 %

Table 4.7 – Visible and cloaked networks in Flekkefjord

In Chart 4.4 below it is apparent that in all the cities except for Flekkefjord, the use of WEP was more common if the network had cloaked SSID. For unencrypted networks the difference looks more variable.

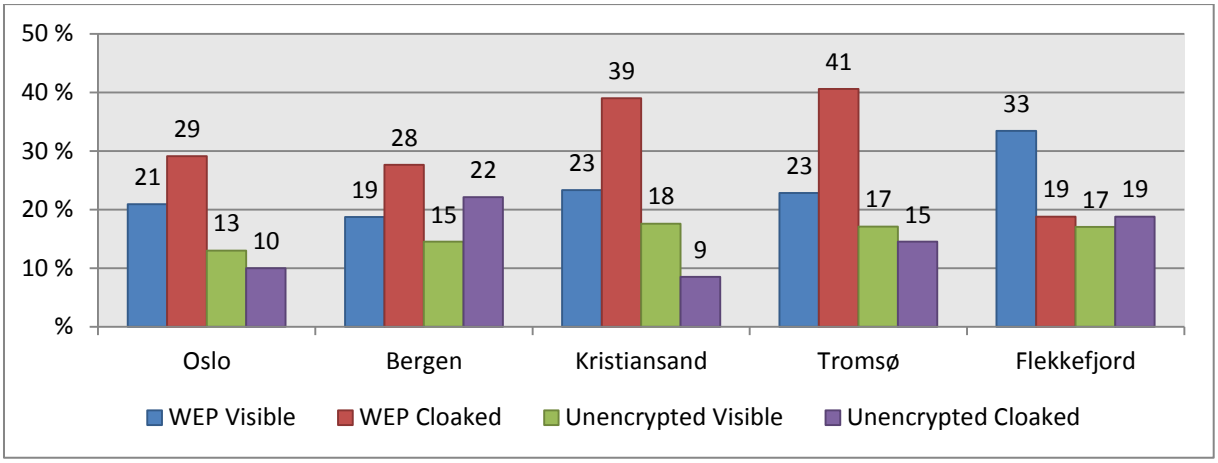

Chart 4.4 – Visible and cloaked networks in the sampled cities

However, when looking at WEP and unencrypted combined in Chart 4.5 below, the use of insecure WLANs is more frequent when cloaking is enabled:

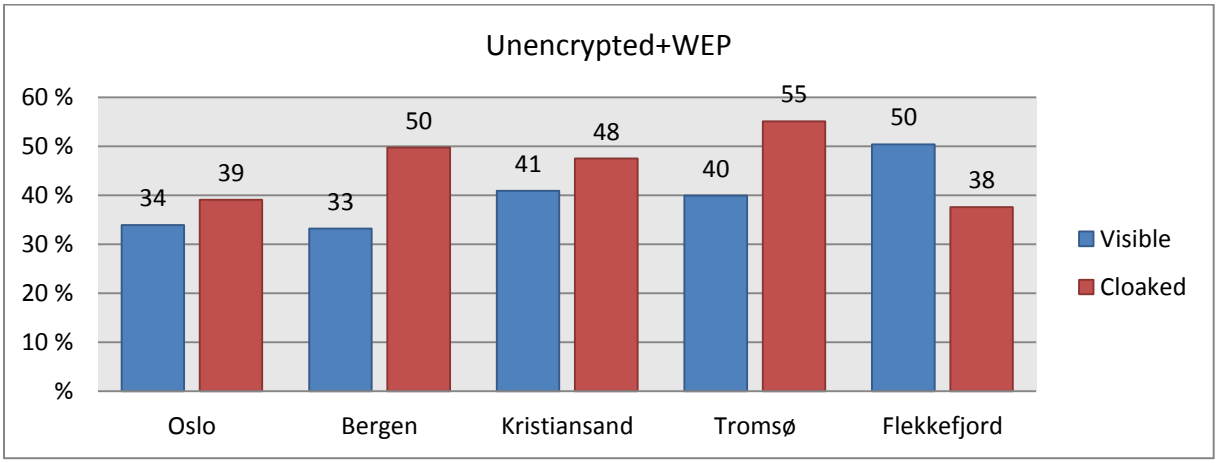

Chart 4.5 – Unencrypted+WEP, visible vs. cloaked

Naturally, and as presented in the following Chart 4.6, a more frequent use of insecure WLANs is still the case when looking at the networks gathered from all the cities combined. Out of the total 35 194 WLANs there were 1 329 with cloaked SSID.

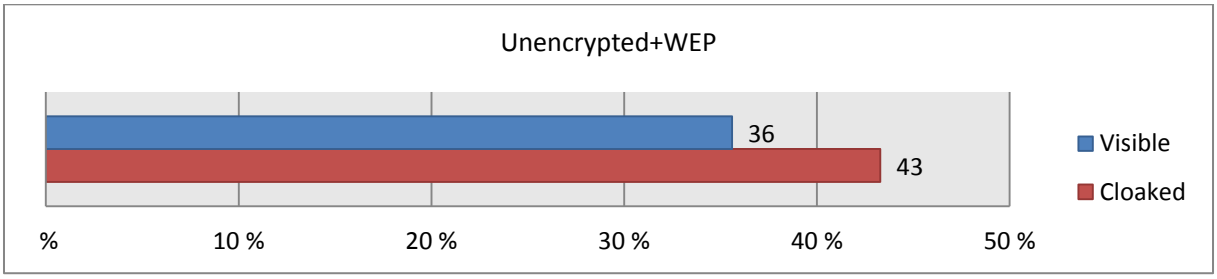

Chart 4.6 – Unencrypted+WEP for sampled cities combined, visible vs. cloaked

4.2.2 Popular SSIDs

Evidently, it is rather common to make use of wireless access points without changing the default network name. The following Table 4.8 shows the most common SSIDs I found and their distribution.

SSID	Oslo	Bergen	Kristiansand	Tromsø	Flekkefjord	Total
Dlink	401	96	65	94	57	713
Linksys	209	59	41	59	83	451
AirLink59300	239	68	31	66	11	415
AirLink89300	190	70	23	65	11	359
AirLink29150	200	46	19	25	7	297
GIGABYTE	106	68	25	10	1	210
NETGEAR	97	27	15	13	4	156
3com	75	10	7	24	17	133

Table 4.8 – Most common default SSIDs

It is also common for businesses and institutions to have a broad spread of access points with identical network names. This is shown in Table 4.9 below. SSIDs such as *telenor* and *wayport* are wireless network portals that require subscriptions and logon credentials to be used. The SSIDs *eduroam*, *UiB* and *skolenwpa2* belong to educational institutions.

SSID	Oslo	Bergen	Kristiansand	Tromsø	Flekkefjord	Total
eduroam	97	185	0	0	0	282
wayport	131	45	36	62	0	274
telenor	82	49	20	103	0	254
UiB	0	190	0	0	0	190
utsikt	101	0	0	0	0	101
insikt	93	0	0	0	0	93
skolenwpa2	81	0	0	0	0	81
netpoint	42	0	34	0	0	76

Table 4.9 – Most common SSIDs by businesses and institutions

4.2.3 Popular Manufacturers

According to my war-walk, the following 8 access point manufacturers hold 70 % of the total market. Table 4.10 below shows that Cisco is the most common when considering Cisco's subsidiary company, Linksys, which was acquired in 2003.

Manufacturer	Oslo	Bergen	Kristiansand	Tromsø	Flekkefjord	Total
D-Link Corp.	4 457	808	949	367	261	6 842
Cisco	2 424	1 212	801	256	9	4 702
Cisco-Linksys	1 845	430	322	242	214	3 053
ZyXEL Com.	1 050	583	336	225	166	2 360
Edimax Technology	1 090	449	243	135	54	1 971
Thomson Telecom	993	477	173	131	84	1 858
Inteno Broadband	579	855	86	101	41	1 662
Apple Inc	940	231	80	52	4	1 307

Table 4.10 – Most common manufacturers

4.2.4 TKIP and CCMP

Even though the TKIP encryption protocol, commonly used in WPA and WPA2, is not completely broken, flaws have been found that open for attacks. The following Chart 4.7 shows the percentage of TKIP and CCMP in WPA and WPA2. For all the access points using WPA/WPA2, TKIP was used in 83 % and CCMP in the remaining 17 %.

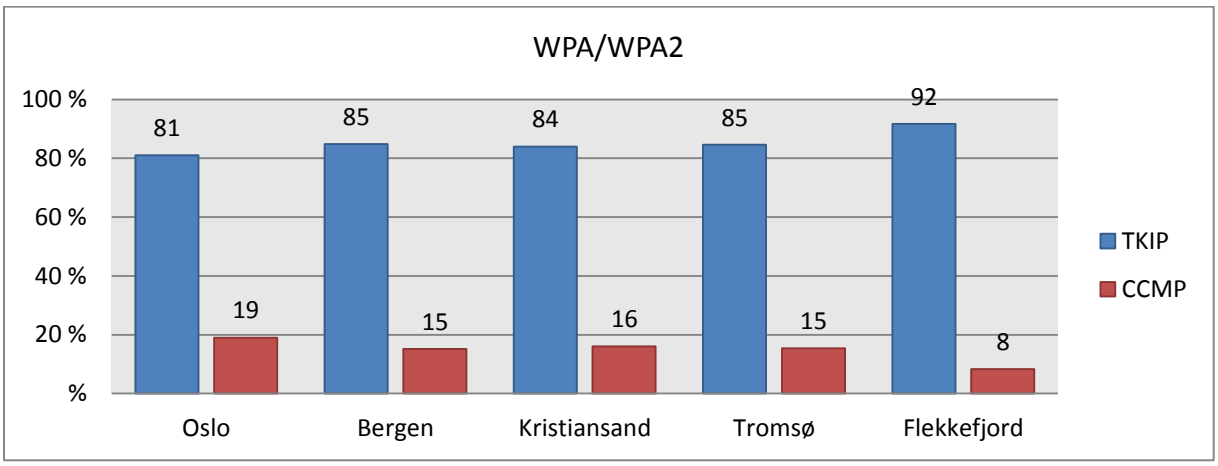

Chart 4.7 – TKIP and CCMP in WPA/WPA2

4.3 Internet Service Providers: Problematic Encryption Practices

In this subchapter I intend to give an overview of the various SSIDs used by broadband providers. The purpose is to show the extensive distribution of preconfigured routers, and whether or not the end-users are likely to change the default settings. For convenience, I will in the following chapters use the variables in Table 4.11 to substitute characters in SSIDs. For instance will the SSID *privat1234klm* be written *privatYYYYxxx*.

Variable	Substitute	Characters
X	uppercase alphabetic	A-Z
x	lowercase alphabetic	a-z
Y	digits	0-9
Z	uppercase hexadecimals	0-9 A-F
z	lowercase hexadecimals	0-9 a-f
Q	uppercase alphanumeric	0-9 A-Z
q	lowercase alphanumeric	0-9 a-z

Table 4.11 – Variables substituting characters in SSIDs

SSID	Oslo	Bergen	Kristiansand	Tromsø	Flekkefjord	Total
privatZZZZZZ	439	148	77	129	59	852
SpeedTouchZZZZZZ	63	56	9	6	7	141
ThomsonZZZZZZ	53	0	0	0	0	53
Total	555	204	86	135	66	1 046

Table 4.12 – Circulation of WEP encryption in privatZ*, SpeedTouchZ* and ThomsonZ*

Table 4.12 shows WEP-encrypted Thomson routers that use default SSID and are vulnerable to exploitation that does not require data packet monitoring. The following Chart 4.8 shows this comparison in percentage.

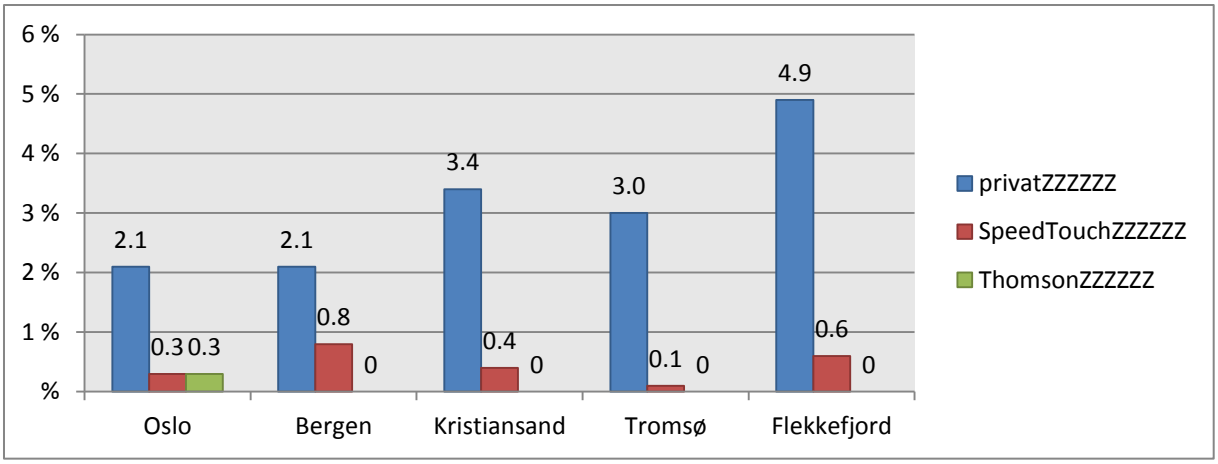

Chart 4.8 – Circulation of WEP-encrypted Thomson routers from ISPs in percentage

Table 4.13 below shows the ISPs' SSIDs I found that use WPA-PSK. Because of the certain possibility of cracking WEP, I have chosen not to include those networks below.

SSID	Oslo	Bergen	Kristiansand	Tromsø	Flekkefjord	Total
GETXXXX(X/XX)PRIVAT	1 090	7	34	0	0	1 131
NextGenTel_ZZ	438	707	84	60	33	1 322
privatYYYYxxx	841	462	180	283	145	1 911
privatZZZZZZ	14	2	1	2	2	21
SpeedTouchZZZZZZ	34	34	3	3	2	76
Telenor-6YYYYYYY	45	16	4	10	0	75
ThomsonZZZZZZ	55	4	1	0	0	60
VenteloZZZZZZ	18	158	13	2	0	191
Total	2 535	1 390	320	360	182	4 787

Table 4.13 – ISP preconfigured routers with WPA-PSK

Manufactured by Thomson[25] SA, the WLANs above with SSID *privatZ**[26], *SpeedTouchZ** and *ThomsonZ**, have passphrases that in theory can be calculated in the way Kevin Devine discovered in 2008. However, reports by users on the web site GNUCITIZEN[27], dating back to July 2010, claim that new routers are using a new algorithm.

[25] Thomson SA was re-branded Technicolor SA in 2010. In this thesis, however, I will use the Thomson name due to its wide recognition.
[26] To facilitate readability I have substituted ZZZZZZ with Z*.
[27] The GNUCITIZEN web page can be found at: http://www.gnucitizen.org/

4.3.1 ISP Routers: Altered or Unaltered Configuration

Wireless routers and access points are generally without preconfigured encryption when sold retail. That means that the purchaser actively has to enable encryption when the wireless network is being installed. The consequence of routers and access points requiring an installation process is that the end-user chooses encryption and a custom SSID. When it comes to the broadband providers in Norway, they have had a tendency of choosing rather uncommon wireless routers. If a router has solely been distributed by ISPs and not sold retail, it is possible to get an estimation of configuration change by comparing the SSIDs to the manufacturer. I will now compare the tendency to use custom SSIDs, which refers to cloaked networks or alterations to the default SSID set in the configuration by the ISP or manufacturer. For the three most common router brands used by ISPs, default SSID refers to *SpeedTouchZ**, *ThomsonZ** and *privatZ** for Thomson SpeedTouch, *privatYYYYxxx* for ZyXEL and *NextGenTel_ZZ* for Inteno.

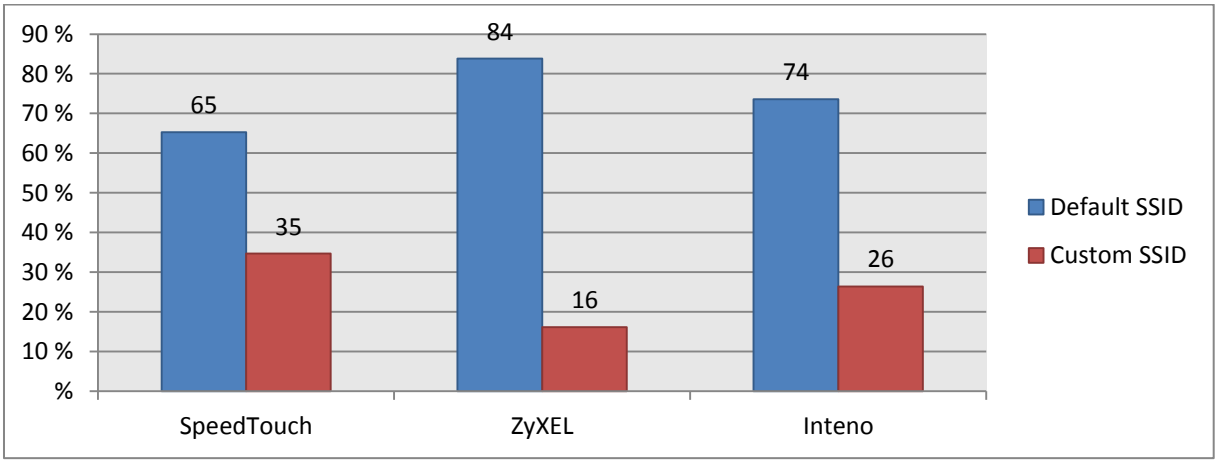

Chart 4.9 – Tendencies to alter SSID on SpeedTouch, ZyXEL and Inteno routers

Chart 4.9 shows that altering the SSID is more common on SpeedTouch and Inteno routers than on ZyXEL. It also makes it evident that the majority of end-users that receive routers from their broadband providers do not alter the SSID.

I will now present more detailed data that will assist in comprehending the alteration differences between the routers.

4.3.1.1 Thomson SpeedTouch

Generally, wireless routers from Thomson SpeedTouch have been delivered through broadband providers, and have rarely been sold retail. Subtracting the ISPs' common SSIDs from the total amount of Thomson routers, would therefore give an estimation of routers where the configuration has been modified by end-users.

Encryption	Oslo	Bergen	Kristiansand	Tromsø	Flekkefjord	Total
Unencrypted	50	44	11	4	7	116
WEP	512	203	86	135	65	1 001
WPA-PSK	102	40	5	5	4	156
Total	664	287	102	144	76	1 273

Table 4.14 – SpeedTouch routers with default SSID

Encryption	Oslo	Bergen	Kristiansand	Tromsø	Flekkefjord	Total
Unencrypted	10	4	1	1	0	16
WEP	165	90	15	11	5	286
WPA-PSK	197	131	17	24	5	374
Total	372	225	33	36	10	676

Table 4.15 – SpeedTouch routers with custom SSID

Table 4.14 shows that there are many SpeedTouch routers in use with default SSID, and that most of them use WEP encryption. In Table 4.15 it is apparent that the encryption on SpeedTouch routers is better when users have changed or cloaked the SSID.

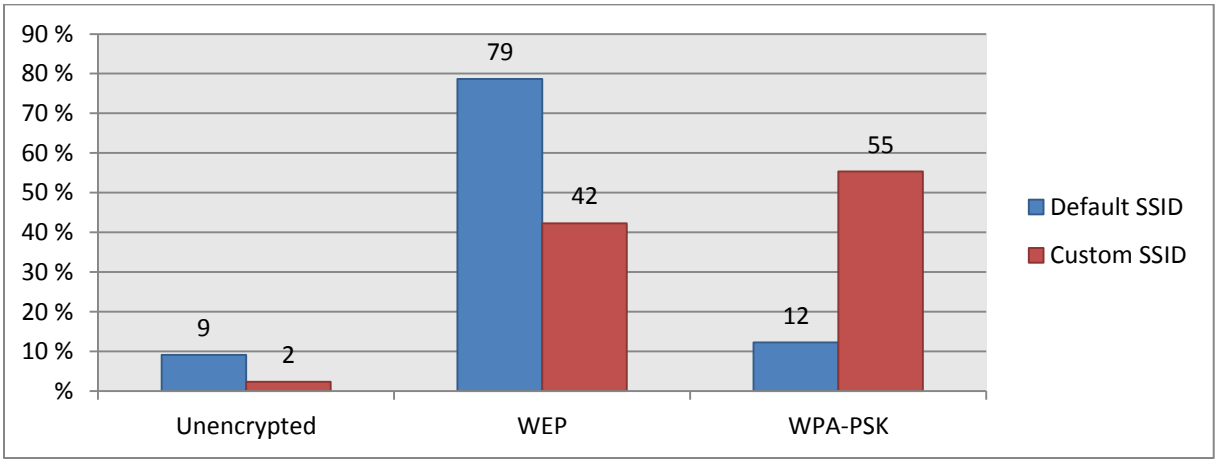

Chart 4.10 – SpeedTouch encryption, default SSID vs. custom SSID

Chart 4.10 shows a high majority of WEP encryption when the SpeedTouch router is using a default SSID. It also shows that when the SSID is custom, there is less use of WEP encryption and higher use of WPA-PSK.

4.3.1.2 ZyXEL

As Telenor has used several different router models from ZyXEL Communications Corporation, both WEP and WPA-PSK have been employed. While there is a multitude of ZyXEL routers available in retail stores, Chart 4.9 showed that 84 % used the SSID *privatYYYYxxx* which originates from Telenor.

Encryption	Oslo	Bergen	Kristiansand	Tromsø	Flekkefjord	Total
Unencrypted	4	0	0	1	0	5
WEP	186	69	35	58	36	384
WPA-PSK	838	461	180	283	145	1 907
Total	1 028	530	215	342	181	2 296

Table 4.16 – ZyXEL routers with default SSID

Encryption	Oslo	Bergen	Kristiansand	Tromsø	Flekkefjord	Total
Unencrypted	20	22	1	9	1	53
WEP	54	32	9	16	5	116
WPA-PSK	119	72	36	37	10	274
Total	193	126	46	62	16	443

Table 4.17 – ZyXEL routers with custom SSID

Table 4.16 shows there are very few ZyXEL routers with default SSID that use no encryption. It also shows that WPA-PSK is much more common than WEP. Table 4.17 shows that when the SSID has been changed on ZyXEL routers, there is a greater share of networks without encryption.

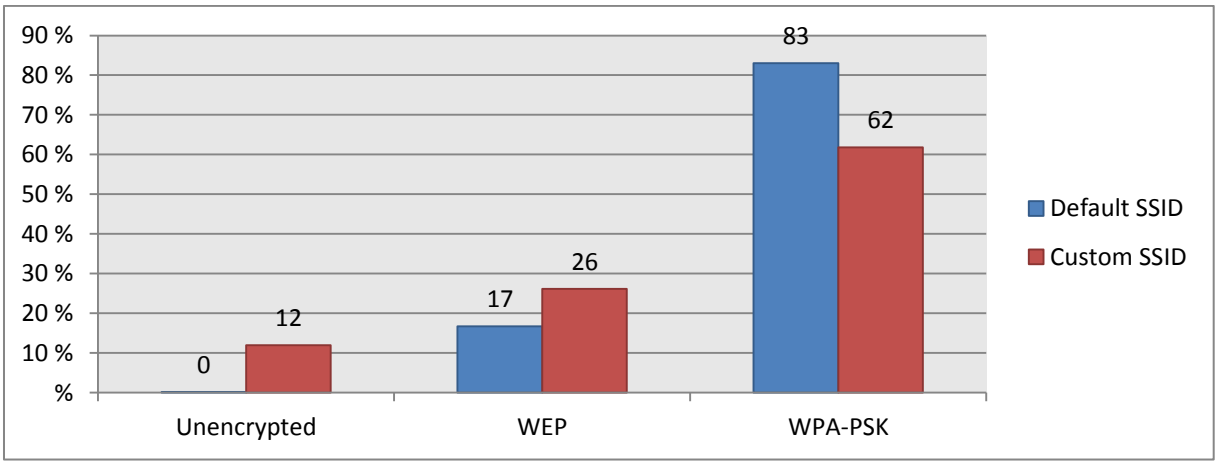

Chart 4.11 – ZyXEL encryption, default SSID vs. custom SSID

Contrary to the numbers from SpeedTouch routers, Chart 4.11 shows a higher percentage of unencrypted and WEP-encrypted routers with custom SSID, and a lower percentage of WPA-PSK.

4.3.1.3 Inteno

Inteno routers in Norway are distributed solely by NextGenTel and are not sold retail. Therefore, the wireless routers manufactured by Inteno that do not have SSID *NextGenTel_ZZ*, must have been altered by end-users. Additionally, because they are only delivered with WPA-PSK, Table 4.18 and Table 4.19 below give insight into end-user encryption practices when SSIDs have been changed.

Encryption	Oslo	Bergen	Kristiansand	Tromsø	Flekkefjord	Total
Unencrypted	3	1	0	0	0	4
WEP	6	2	0	1	0	9
WPA-PSK	438	706	83	60	33	1 320
Total	447	709	83	61	33	1 333

Table 4.18 – Inteno routers with default SSID

Encryption	Oslo	Bergen	Kristiansand	Tromsø	Flekkefjord	Total
Unencrypted	1	1	0	1	0	3
WEP	33	27	2	2	0	64
WPA-PSK	180	170	27	25	9	411
Total	214	198	29	28	9	478

Table 4.19 – Inteno routers with custom SSID

Table 4.18 shows that almost all Inteno routers with default SSID use WPA-PSK, and Table 4.19 shows a greater use of WEP encryption when SSID has been altered.

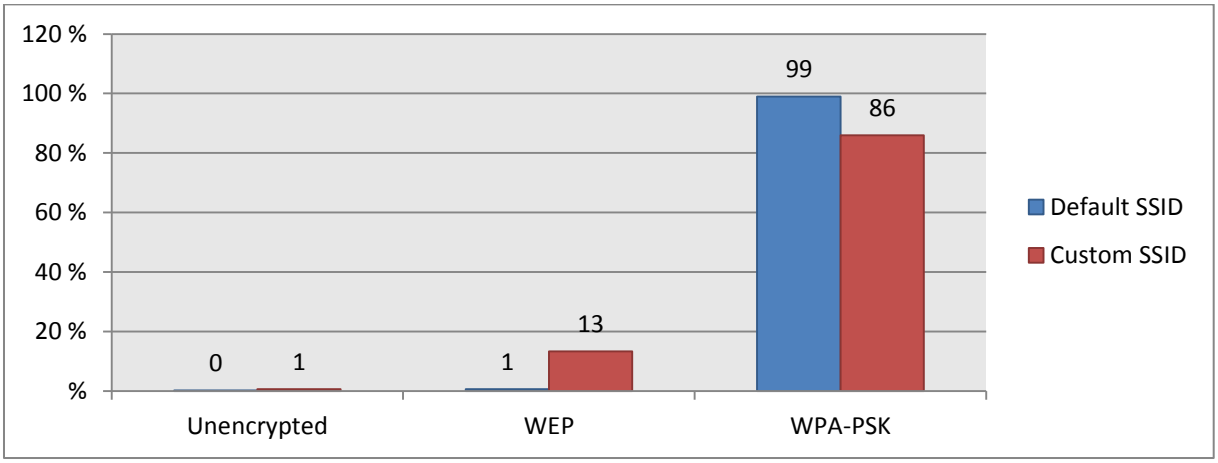

Chart 4.12 – Inteno encryption, default SSID vs. custom SSID

Chart 4.12 shows that Inteno routers in many cases are altered to use the less secure WEP encryption instead of WPA-PSK.

5 DISCUSSION

In this chapter I will discuss my findings based on my three research questions in consecutive order. I will start by discussing the encryption usage in Norway based on the data from my war-walk. I will then discuss the Internet broadband providers and their role in WLAN security, partially based on my war-walking data and partially based on the supplementary sources. Lastly, I will discuss societal challenges we face by ignoring the issues of WLAN security. I will also give my opinions on how we should approach these issues.

5.1 Encryption Usage in Norway

The number of insecure WLANs in Norway is alarmingly large. 14.2 % of all the WLANs I found did not use encryption at all. I was rather surprised to see that Oslo was the only city below the average, when considering all the hotels and hotspots a large city has. Out of the total 35 194 WLANs in all the cities, 7 606 used WEP. Combined with the unencrypted, it means that 36 % of the networks I detected can be broken into within few minutes. The 2.4 % SpeedTouch routers with WEP encryption can be broken into by only knowing the SSID. Additionally, there are wireless networks that use dictionary-based WPA-PSK. To be able to remember their passphrase, many people tend to use a simple and common word. And even if the WPA-PSK specification requires a minimum of 8 characters, words such as *baseball* and *superman* are subject to dictionary attacks and will be found within minutes. It is also popular to use phone numbers for passwords, but since Norwegian phone numbers are only 8 digits long, an attacker is able to run through every possible phone number in just 15 minutes.

In research question 1b I ask whether population size or location affect encryption practices. My results presented in Chart 4.1 and Chart 4.3, indicate that WLAN security is higher in larger cities. Is this because end-users in smaller cities are less aware of potential dangers or are simply too trusting of their neighbours? Or is there really less chance of WLAN break-ins in smaller cities?

In areas with lower density of private residences there is likely a lesser chance of perpetrators. A perpetrator would in most cases be interested in high density areas where attacks can be performed on several sources simultaneously, and where it is possible to stay hidden in a rented apartment or hotel room. An unknown car in front of a solitary house would look rather suspicious. However, in the areas where I collected the WLAN data, even in the small town Flekkefjord, there was always a neighbouring house that could hide a potential perpetrator.

Another theory is that end-users in larger cities are more Internet dependent and consequently more technology competent. Chart 5.1 below shows the percentage of private broadband subscriptions in the sampled cities.

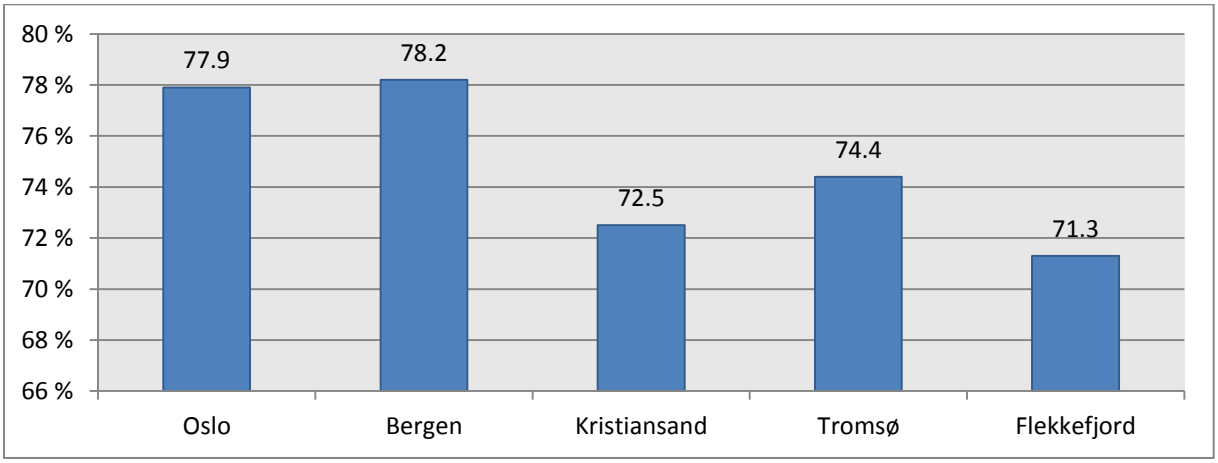

Chart 5.1 – Private broadband subscriptions in percentage (SSB 2011c)

These numbers could also mean that end-users in larger cities were early adopters of wireless networking. As a consequence, the early adopters have had more time to acquire knowledge about the technology and the corresponding security issues. At the same time, early adopters are more likely to have used WEP encryption if they received their wireless access point from an ISP.

Another reason for area-based variations might be the WLAN owners' different socioeconomic status. I therefore contacted municipalities and Statistics Norway in an attempt to find statistics for living conditions. Unfortunately, their data was not categorized in small enough geographical sections for me to compare with my sampling areas.

5.1.1 Comparison to Similar Research

Hole, Dyrnes and Thorsheim (2005) said that 244 of the 706 wireless access points they found were using WEP encryption. That gives 34.6 % using WEP and 65.4 % having no encryption at all. When considering that Hole, Dyrnes and Thorsheim did not specify exactly where in Bergen they conducted their research, and that WPA is now significantly more common, a direct comparison is not very relevant. However, some interesting developments can be seen. As the percentage of unencrypted wireless networks in my results is 14.8 %, it is apparent that using some sort of encryption is much more common today than in 2004. The use of WEP also appears to have dropped from 34.6 % to 19.1 %. Furthermore, assuming that they

covered an area similar to the area I covered, the number of WLANs in the centre of Bergen has increased from about 500 to almost 7 000 in seven years.

Since little similar research has been done in Norway I had to look abroad. While I hoped and expected to find war-driving performed by institutions in Scandinavia or at least in a European country, the only credible source I could find was from Hong Kong. This research from December 2010 showed 14 % unencrypted networks and 34 % WEP encryption (PISA and WTIA 2011). Compared to my results there were 12.9 % unencrypted networks in Oslo and 21.2 % with WEP encryption. However, due to the structural and cultural differences I find it unproductive to speculate on the reasons for the differences. Nevertheless, the study from Hong Kong showed an improvement in encryption practices over the last years. Unfortunately, except for the study by Hole, Dyrnes and Thorsheim, there are no available data I can compare my results with in Norway.

5.1.2 Common SSIDs and Manufacturers

In Table 4.8 I presented the 8 most common network names. All the occurrences of these default SSIDs turned out to be 11 % of the total 35 194 WLANs. But this percentage is based on the network names set by the manufacturer and does not include access points set up by larger businesses, hotels and institutions. It also does not include the wireless routers provided by ISPs that only differs in SSID by the last characters. Subtracting all these network names that are not set manually by end-users, I found out that about 50 - 60 % use a custom SSID.

Obviously, the use of default network name does not have to mean that encryption has not been set. I compared the various encryptions on WLANs with custom SSID to WLANs with default SSID, and the difference was significant. There was more than twice the chance for a network to be unencrypted if it had default SSID from manufacturer. PSK was less used but surprisingly also WEP. Additionally, none of the WLANs used 802.1X.

It appears that wireless access points bought retail are commonly used without enabling encryption. Wireless networks with SSIDs such as *dlink* and *linksys*, for instance, were unencrypted for 50 % of the occurrences. However, the unencrypted percentage for *AirLink59300* and *AirLink89300* was less than 5 %. The reason for this is that access points from D-Link and Linksys are distributed with encryption disabled and do not require any user configuration to work, except for plugging them into a power socket. The Air:Link access points from Jensen Scandinavia (SSID *AirLink59300* and *AirLink89300*) are conversely sold preconfigured with WPA-PSK enabled and also support WPS (Wi-Fi Protected Setup). These

percentages show that many tend to disregard encryption when setting up wireless networks. Additionally, it shows how important it is that the manufacturers distribute the access points preconfigured with encryption.

In Table 4.10 I presented the 8 most common manufacturers of wireless networks that I found in my war-walk. This showed that D-Link has 19 % of the access point market and Cisco and Cisco-Linksys combined have 22 %. In general, access points by Cisco are intended for the business market whereas the access points by Cisco-Linksys are intended for the private market. The majority of D-Link access points are sold retail, but 16 % had a recognizable SSID that meant they were distributed by the broadband provider GET. As mentioned before, the access points from ZyXEL are distributed by Telenor and the ones from Inteno are distributed by NextGenTel. The access points from Edimax are sold under the brand name Air:Link by Jensen Scandinavia.

5.1.3 The IEEE 802.1X Standard

Even though I do not elaborate much on the use of 802.1X in this thesis, I will now present some of the parties that utilize WLANs with the mentioned authentication mechanism. The information is deduced from the SSIDs and locations of the relevant access points.

In Oslo, there were many university WLANs and quite a few owned by Ministry of Foreign Affairs[28] and the National Rail Administration[29] that were using 802.1X authentication. A few other examples of wireless network using 802.1X were the newspaper VG, Norwegian State Railways[30] and Oslo Courthouse. I also noticed that out of the 923 WLANs in Oslo that used 802.1X authentication, 22 % where using hidden SSID. This is in strong contrast to the other Norwegian cities where it was only 0 – 6 %.

Almost all wireless networks with 802.1X authentication in Bergen were connected to one of the faculties of University of Bergen, but a few were connected to other educational facilities. As in Oslo, the Norwegian National Rail Administration and some other businesses were also utilizing 802.1X.

In Tromsø, location and SSIDs such as *TFK-Elev*, *HN-IKT*, *UNN* and *eduroam* indicated that most of the 802.1X networks belonged to the university or another educational institution.

[28] Utenriksdepartementet.
[29] Jernbaneverket.
[30] Norges Statsbaner (NSB).

UNN stands for University Hospital of North Norway[31], HN-IKT belongs to Northern Norway Regional Health Authority[32] and eduroam stands for Education Roaming.

In Kristiansand there were many 802.1X WLANs belonging to an upper secondary school. Additionally, several others were spread around the city centre that did not have an SSID with a recognizable name.

In Flekkefjord, all 24 wireless networks using 802.1X authentication were made by the same manufacturer, ProcurveNet. The SSIDs used were *SOadmin*, *Sadmin*, *Tadmin* and *USAdmin*. Almost all of the networks were found in close vicinity of a school or a kindergarten.

The primary protection against WPA-PSK cracking "is to use enterprise class security instead of the PSK", and the name WPA-Enterprise for 802.1X usage seems well justified (Carpenter and Barrett 2008, 454). A combination of location data and SSID often makes it easy to identify the owner of a WLAN, and it showed that the majority of wireless networks using 802.1X appeared to be owned by an educational institution. In the cases where it did not, 802.1X was rarely in use in private residencies. A likely reason for this is a more troublesome configuration process compared to using WEP and PSK. While the other cities had few to none cloaked WLANs using 802.1X, Oslo had as many as 22 %. Even though I cannot be sure, I assume most of them are owned by a few big companies that require broad network coverage. The few hidden SSIDs I was able to see with Kismet also supported this assumption.

5.1.4 Temporal Key Integrity Protocol (TKIP)

In Section 4.2.4 I showed that TKIP was used in 83 % of access points employing WPA/WPA2 encryption. For the TKIP attack to succeed, however, certain conditions must be met. Firstly, the access point must support QoS (Quality of Service). Secondly, key renewal interval needs to be longer than the attack period of around 20 minutes (Halvorsen et al. 2009). However, it is common practice by access point manufacturers to set this interval to 60 minutes.

The practical attacks on TKIP are so far limited to Denial of Service, DNS spoofing and direct traffic between network clients and an attacker without network authorization. The latter can for instance be used to "exploit some un-patched vulnerability at the client" (Halvorsen et al.

[31] Universitetssykehuset Nord-Norge.
[32] Helse Nord RHF.

2009, 129). However, the current TKIP attack is not a key recovery attack and can therefore not be used to crack the passphrase of the WLAN. Halvorsen et al. expressed it neatly by saying "TKIP was developed to fix the insecurity of WEP, but now it is TKIP that needs to be fixed" (2009, 132). However, instead of altering the encryption protocol, they believe the best approach is to migrate to CCMP.

5.2 The Role of the Internet Service Providers

Several Internet service providers offer a wireless router when their customers order broadband. As previously mentioned, NextGenTel estimated to have delivered such routers to about 70 % of their broadband customers. While some of these wireless routers may not be in use, there are also additional access points bought retail. If assuming that 70 % of all broadband subscriptions have WLANs employed, there are 1.2 million access points in Norway. This number is based on the 1.7 million broadband subscriptions reported by the Post and Telecommunications Authority (PT 2011). Unfortunately, due to the nature of wireless technology, there is no way to measure the current circulation of wireless networks. Google, with its location-based services, is probably the party that has the largest database of wireless access points. I tried contacting them for statistical data regarding both distribution of WLANs and encryption use, but their press contacts were unable to help me.

Wireless routers distributed by ISPs are often preconfigured with SSID and WEP/WPA-PSK encryption so the client can get online without a difficult setup process. Depending on the method used to create the information, this preconfigured state poses a threat to security. This chapter will show how configuring the router information by using an algorithm can be problematic.

In Section 4.3.1 I showed that few tend to change the pre-set SSID from their ISP. I think the reason for the higher ratio of custom SSIDs on SpeedTouch routers is due to their early entrance to the broadband market. For one thing, that means that the owners of such routers have had more time to change configurations. More importantly, the SpeedTouch routers have been delivered with weaker encryption enabled than for instance ZyXEL and Inteno are now. When many of these SpeedTouch routers were installed, there was less awareness of WLAN encryption and WEP vulnerability.

The MAC addresses of the ZyXEL routers I found in my research show that there are certain MAC ranges that almost exclusively use WEP encryption, and other MAC ranges that only use WPA-PSK. These different MAC ranges indicate that various router models are delivered

with different encryption. Table 4.16 showed that there were just a few unencrypted ZyXEL routers with default SSID. That means that if end-users alter the encryption on the routers but keep the SSID, they either change from WEP to WPA-PSK or vice versa. And because the MAC ranges give away the original encryption, I can find out what is most common. Surprisingly, even though only 1 % of the ZyXEL routers with default SSID had gotten the encryption altered, in most cases the change was from WPA to WEP and not the other way around. I believe the reason for this is the use of obsolete hardware and certain devices such as the handheld game console Nintendo DS, which do not support WPA.

Table 4.17 showed an increased use of unencrypted ZyXEL routers with custom SSID compared to default SSID. Initially I believed this was due to small stores and cafés providing free internet for their customers. But while the relevant SSIDs showed several recognizable names of cafés, the majority used the SSID *homerun*, which are hotspots set up by Telenor.

There could also be a connection between choice of ISP and post-distributed configuration of the router. My results in Table 4.18 and Table 4.19 showed that users with Inteno routers often changed SSID but kept the WPA-PSK encryption. While I can only speculate, perhaps customers who choose NextGenTel over Telenor are more computer literate or security-conscious. Another reason could be that the installation process and configuration setup on Inteno routers are more user-friendly, and therefore easier to alter. There is also a third possibility in that Inteno routers are altered because they have a less secure passphrase than the ZyXEL routers, but I believe such cases to be rare.

5.2.1 Vulnerable ZyXEL Routers

July 19, 2010, a user under the pseudonym Ranvik (2010b) started a thread on the Norwegian Internet forum *Norsk Freakforum*[33]. He claimed that he had found out a way to calculate the default WPA password on ZyXEL P2602HWT routers used by Telenor, and asked forum members to post the MAC address of routers they wanted password to. This was, however, not done in the same way as Kevin Devine did in 2008, but rather by opening his router and using a JTAG and a TTL cable to isolate a program that ran when the router was booting up. Ranvik explained that the TTL cable gave him console access to the router and the JTAG cable gave access to everything stored on it (Groten 2010, #102). The program he isolated was creating the MAC address and WPA password on the router from its serial number, and

[33] The web page for *Norsk Freakforum* can be found at: http://www.freak.no/

Ranvik was able to retrieve the passwords he wanted by modifying this (Ranvik 2010b, #514) (Bie 2010).

The forum thread accelerated quickly and after a month he had posted nearly 100 WPA passwords to Telenor's routers. He then created a script that automated the process and answered to 500 more requests from the forum users until the 25th of October (Ranvik 2010b, #193). That is when another forum user called Groten (2010) published a list of 9 000 WLANs located in Norway. The list included access points' GPS coordinates, SSID, MAC addresses and the WPA passwords. All these access points were made by ZyXEL and sent out by Telenor to broadband customers. This meant that anyone could now log into any of these 9 000 networks and exploit them in numerous ways. The security breach quickly hit the news and gave Telenor a large amount of bad publicity. Communications Manager in Telenor, Per A. Meling, claimed they had known about the problem for four months but not taken counter-measures due to its "very small scope" (Nilsen 2010; Gilbrant 2010a). He also claimed that nobody had been *hacked* due to this problem, but later retracted it by saying that Telenor cannot know if anyone has been hacked or how many if so. A couple of days later Meling said they were now in the process of calling every owner of the access points on the published list and that they were going to report Groten to the police (Gilbrant 2010b).

A few days after Meling's statement, someone created a profile on Norsk Freakforum named Maclist and published a list of 165 000 Telenor routers made by ZyXEL. However, this list did not include SSID and passwords, but MAC addresses, GPS locations and the geographical addresses instead. An anonymous source revealed to me that the data was originally gathered by Google and were subsequently retrieved by sending multiple queries to Google's servers. While the thread was removed by forum moderators after just three hours, it was picked up in Google's cache and remained available for months. The thread is completely removed now, but I saved a copy for my research that shows that the link to the list of 165 000 WLANs is still functional. Since Ranvik only needed the MAC address to find both the SSID and WPA password, he could easily have run these MAC addresses through his automated script and thereby have known the location and WPA password for 165 000 WLANs provided by Telenor. At the time of this writing (May 2011), Ranvik has not been online since a post on Freakforum November 22th, which was around the same time his web page was taken down. Groten also stopped being online, but wrote a post the 3rd of January wishing Telenor a good year with users wanting safer networks (Groten 2010, #213).

5.2.2 Potentially Vulnerable Routers

Telenor is not the only ISP in Norway that uses software to automatically configure routers with WPA encryption. NextGenTel, GET and Ventelo are other examples. While Telenor has a market share of 48.8 % (Canal Digital included), these three other broadband providers have the combined market share of 25.4 % (PT 2011). In 2009 Ranvik actually published a guide on how to crack default WPA passwords on Inteno routers from NextGenTel. But due to the cracking progress taking over a week and the fact that most Inteno routers appeared to be using hexadecimals and not only digits as first assumed, the thread did not get much attention (Ranvik 2010a). However, during the period when ZyXEL passwords were published, Ranvik claimed he was able to calculate the first two of ten hexadecimals in default WPA passwords on Inteno routers (Ranvik 2010b). While there are 1 100 billion possibilities for 10 hexadecimals, the remaining 8 hexadecimals limit the number of possibilities to 4 billion. Assuming Ranvik's claim was legit, he would be able to break into NextGenTel WLANs within 7 hours on a desktop computer utilizing the AMD Radeon HD 6990 graphics card[34].

In the forum thread on the ZyXEL passwords Ranvik also mentioned that he was acquiring a router from GET as well to see if they had a similar vulnerability he could exploit (Ranvik 2010b). However, I was informed[35] by GET that they used a different practice than Telenor, but they did not elaborate on the details.

BKK is another ISP that used to deliver wireless routers pre-set with WEP encryption. But this ISP also prevented access to the router's configuration settings, which meant that the BKK customers were unable to change the encryption. The result was that every WLAN provided by BKK (SSID was *BKKYYYY*) could easily be cracked within minutes. Fortunately, when Ventelo bought BKK's broadband client portfolio in 2009, consisting of 11 500 broadband users, they also replaced the router encryption with WPA (Ventelo 2009). Additionally, Product Manager in Ventelo, Svein Asle Bjørheim, explained[36] that existing users were told to return their wireless routers. In theory, this meant that all routers from BKK with WEP encryption would seize to exist. The complete absence of BKK SSIDs in my war-walk in Bergen goes far in confirming this.

[34] Based on 170 000 keys per second using Pyrit.
[35] E-mail correspondence with Øyvind Husby, press contact in GET, 04.04.2011.
[36] E-mail correspondence, 23.05.2011.

5.2.3 Wired Equivalent Privacy (WEP)

Security Officer in Telenor, Rune Dyrlie, said[37] that Telenor started employing WPA encryption from September 2009 with the shipping of ZyXEL P2602HWT routers. He also said that they still distribute wireless routers from Thomson SpeedTouch preconfigured with WEP. This is done despite the fact that WEP was already in 2004 declared deprecated by IEEE with the ratification of the 802.11i standard (IEEE 2004). Telenor's late employment of WPA, however, can be excused due to compatibility issues with older hardware. Also various other ISPs have distributed Thomson SpeedTouch routers with WEP encryption, and through my research it became evident that there are still a large number of these routers with pre-set WEP encryption.

The Thomson SpeedTouch routers distributed through broadband providers in Norway that are vulnerable to Devine's exploit, use either the SSID *privatZZZZZZ*, *SpeedTouchZZZZZZ* or *ThomsonZZZZZZ*. Based on Telenor's list of wireless routers on their web page, networks with the SSID *privatZ** and *SpeedTouchZ** have been delivered by Telenor. But as NextGenTel and Telenor both have distributed SpeedTouch 585 routers with SSID *SpeedTouchZ**, it is impossible to know which broadband provider these WLANs are connected to. I tried to look at Thomson user manuals and user guides on the ISP web pages to match examples of MAC addresses to my data material, but I could still not differentiate *SpeedTouchZ** between Telenor and NextGenTel. The last preconfigured SpeedTouch SSID I found was *ThomsonZ**, but I have been unable to find out which ISP distributes it. It is certain, however, that *privatZ** is only distributed by Telenor.

As previously mentioned, WEP has become very easy to crack by exploiting the RC4 stream cipher as discovered by Fluhrer, Mantin and Shamir (FMS) (2001). But this FMS attack requires packet monitoring in close range to the access point. However, if details from the ISPs' setup process of routers are discovered, WLANs can be broken into as shown in Section 2.2.1 and Section 5.2.1. Contrary to the FMS attack, cracking the passphrases for these access points will only require the MAC address or SSID, and can be performed without packet monitoring. The simplicity of breaking into these WLANs means that just about anyone can gain unauthorised access.

Furthermore, since Telenor and other ISPs over the years have shipped several routers with WEP encryption, a large number of WLANs have been exposed. My results in Table 4.12,

[37] E-mail correspondence, 08.04.2011.

which show that there were 1 046 WEP-encrypted Thomson SpeedTouch routers, indicate that ISPs tend to ignore older routers that are not up to date on security. The customers pay the same subscription fee, but the early adopters of ISP's WLAN routers get less security if they do not know how to change it.

Chart 4.8 shows that SpeedTouch routers delivered by Telenor (SSID *privatZ*)* have a higher market share in smaller cities. These numbers are of course highly affected by how common Telenor is as an Internet provider in the different areas. While I was unable to find information showing differences between ISPs in regional broadband subscriptions, Telenor had 870 000 broadband customers nationwide at the end of the first quarter of 2011 (Telenor 2011). This number includes customers from their wholly-owned subsidiary, Canal Digital, which currently provides broadband access for 266 000[38] customers through cable television. From the total 35 194 WLANs I detected, there were 852 WEP-encrypted with the SSID *privatZ**. This gives the percentage of 2.4 %. Even though the calculation tool made by Kevin Devine reportedly worked on routers that were delivered with WPA as well, my findings showed that use of this encryption was a rarity on the SpeedTouch routers distributed by Telenor. Out of 873 WLANs named *privatZ**, only 21 used WPA and the rest used WEP.

Someone with illicit intent is most likely indifferent whether or not the wireless router is an unaltered Thomson SpeedTouch with a pre-set encryption, as long as the network is using WEP. This is because this adversary knows how to break in either way. But for the average person looking for free access to Internet, Devine's easy method of retrieving the password to SpeedTouch routers becomes an option.

5.2.4 Wi-Fi Protected Access Pre-shared Key (WPA-PSK)

WLANs that are unencrypted, use WEP or a dictionary passphrase with WPA-PSK, offer limited security. A fourth aspect, that in practice could reduce security, is preconfigured routers. Due to the nature of my research I am unable to establish with 100 % certainty whether the router configuration has been modified after the ISP sent it out. But if a wireless network uses an SSID identical to the ones from an ISP and has the same type of encryption and MAC range (has the same manufacturer), I believe it is fair to presume that this WLAN is still using preconfigured settings. If an end-user was to change encryption on his access point, I think he in most cases would change the SSID as well. The opposite scenario where end-

[38] E-mail correspondence with Roald Orheim, press contact in Canal Digital, 03.05.2011. Number is accurate as of the end of 1st quarter 2011.

users who change SSID are also likely to change password, is the reason why I primarily sorted the results in Table 4.13 from SSID and not MAC range. Even though the method Ranvik used on Telenor's routers only required the MAC address, it would presumably not work on networks where the SSID has been changed.

Despite the fact that the number of preconfigured SpeedTouch routers with WPA was only 157, they are presumably all possible to crack with Devine's method. The exception is when the router is newer than the summer of 2010, when Internet users claimed that Thomson had changed their encryption process. In Table 4.13 I showed that 4 787 (13.6 %) of all the wireless routers I detected had SSID from an ISP and used WPA-PSK encryption. This preconfigured state introduces a potential vulnerability in which the password can be calculated if the algorithm is found, or if someone finds a way to create passwords through the wireless router as Ranvik did. I have, however, not been able to obtain in-depth details on the encryption process from the ISPs, as many were reluctant to reveal such information. Director of Marketing and Information in NextGenTel, Morten Ågnes, explained[39] that divulging security practices to the public could attract unwanted attention and be a security risk in itself. He did, however, confirm that their routers by default used 10 hexadecimals as passphrase. While NextGenTel considers this as sufficient, it is considerably less secure than the 10 alphabetic characters Telenor uses and the 11 alphabetic and hexadecimals GET uses. Table 5.1 below shows the passphrase strength of the four largest ISPs in Norway that distribute wireless routers.

ISP	Length	Characters	Possibilities	In billions
NextGenTel	10	0-9 a-f	16^{10}	1 100
Telenor	10	a-z	26^{10}	141 000
Ventelo	8	0-9 a-z A-Z	62^{8}	218 000
GET	11	0-9 a-z	36^{11}	131 600 000

Table 5.1 – WPA passphrase strength of the largest ISPs that distribute wireless routers

These numbers indicate that GET is better prepared for a potential major breakthrough in brute-force attack speed. With the encryption scheme above, a brute-force attack on a GET router would take 900 and 120 000 times longer than on Telenor and NextGenTel routers respectively. The routers from Ventelo, which are manufactured by Jensen Scandinavia AS, use shorter passphrases than the routers from NextGenTel and Telenor, but are still more

[39] E-mail correspondence with Morten Ågnes, Director of Marketing and Information in NextGenTel, 26.04.2011.

secure due to the variation of characters. Additionally, a computer technician from Jensen said[40] that their routers generate the WPA passphrase in a "completely different way" than Telenor, and is subsequently not vulnerable to that type of breach.

The method Ranvik used on ZyXEL routers shows us, however, that a relatively strong password can be insufficient if the configuration process is not secure. As Ranvik was able to do this, it is plausible that there are also others. A perpetrator, who knows about such vulnerabilities and exploits them for illicit purposes, is often better served by keeping them to himself.

Even though preconfigured routers delivered by ISPs have proved to be vulnerable, the logic behind the practice is understandable. A preconfigured router using strong encryption and a solid password often provides better security than the end-user who often use short and simple passwords found in dictionaries. But as the WPA-PSK cracking speed is reaching 200 000 keys per second on a single graphics card, and GPU clusters are increasing this tenfold, the ISPs need to assess their practices and be able to update security on existing routers. Given a cluster with 100 computers where every node is able to process 200 000 passphrases per second, it would take up to 15 hours to crack WLANs from NextGenTel (10 hexadecimals), 82 days for Telenor (10 alphabetic) and 126 days for Ventelo (8 mixed). While access to such computer power is limited and expensive today, it is hard to predict the situation a few years from now. As many of the broadband providers are able to modify their customers' router setups remotely, the challenge is to find a way to upgrade security that does not cause problems for the customers.

In my opinion, the most secure password administration for ISPs is using completely randomized passphrases. In that way, the only option of retrieving the passphrases is by brute-force attack or breaking into the computer system of the vendor or ISP. If the vendor and ISP do not keep logs of the generated passphrases, the method of attack is limited to brute-force only.

However, using preconfigured routers might mislead end-users into thinking their WLAN is secure forever, and they remain unaware of the dangers linked to wireless networks. Having ISPs deliver pre-setup routers is not necessarily a bad idea, but it still requires awareness of ICT security. There also has to be a plan of counter-measure ready when flaws are found in the security protocols.

[40] E-mail correspondence with Tor Torkveen, computer technician at Jensen Scandinavia AS, 16.05.2011.

5.3 Societal Challenges and Countermeasures

Most people do not realize how insecure wireless networks are. Due to the increasing distribution of access points, the associated risks need to be taken seriously. In my opinion, insecure WLANs are not only limited to cause problems for end-users, but can also affect our society on a national level. An important contributing factor in order to improve security is to share the responsibility between the appropriate parties.

Senior vice president in the GPU manufacturing company Nvidia, Tony Tamasi, presented his view on the future of graphics card power at the 2011 East Coast Game Conference (ECGC) (Parrish 2011). He claimed that GPU performance would increase 1 000 % by 2015, based on annual growth rate between 2007 and 2011. Such an increase is also consistent with Moore's law, commonly implying a performance doubling every 18 months, even though opinions differ on whether this theory applies to GPUs. The GPU company AMD, which currently outperforms Nvidia on WPA cracking performance, has shown that their GPU power between 2005 and 2009 actually outpaced Moore's law (Chu 2010).

The prediction of 10 times faster brute-forcing of PSK in 2015 is a potential problem to passphrase strength that currently is sufficient. For one thing, the problem applies to WLANs that are still using the same password 5 years from now, which by then could be possible to crack. That scenario is only problematic if the WLAN encryption is not being updated according to advances in cracking technology. A more serious problem arises when information is still sensitive after many years. Even without the key, a determined perpetrator can capture the encrypted data being transferred wirelessly, and then store everything on his hard drives. When the cracking performance reaches a level high enough and the perpetrator is able to crack the passphrase, he can decrypt the information he captured from years back.

From an adversary's point of view, I believe there are two different factors of interest when selecting wireless networks to break into. The first one is that a high density of insecure WLANs increases the odds of finding a suitable target to monitor. A high density also most likely means a more crowded area and therefore less exposure of the adversary. The second factor is that a high percentage of insecure WLANs also means a larger chance that a pre-chosen target is insecure. Instead of breaking into random networks, an attacker in Norway can use the publicly available lists of people's income to find potential targets that can provide economic winnings. Telephone directories can then be used to find the addresses and subsequently lead to attacks on the selected victims.

An article published in 2009 challenges another perspective where insecure WLANs are causing societal threats. In this report, Hu, Myers, Colizza and Vespignani (2009) problematized the risk of malware on WLANs, and created an epidemiological model to estimate its propagation. The authors state that wireless routers are valuable targets because they "are the perfect platform to launch a number of attacks that previous security technologies have reasonably assumed were unlikely" (Hu et al. 2009, 1318). Hu et al. explain this by the fact that wireless routers tend to always be on and connected to the Internet, and that there currently is no software specifically aiming to detect or prevent their infection. It is required, however, that the routers are in close proximity to each other, much like in any urban area. The article points out that such malware would take advantage of unencrypted and WEP-encrypted networks, but also of the common usage of default passwords for router administration. In a simulated model of Manhattan, New York, the authors expect 18 000 wireless routers to be infected within 2 weeks (Hu et al. 2009). They also point out that a worm made for wireless networks would not even need to infect any personal computers, but could instead be made to monitor data traffic on the router and relay it back to the creators of the worm. The creators would then be able to search the traffic for valuable data such as credit card information.

In a short documentary presented by VG in December 2011, member of the Norwegian Parliament, Lise Christoffersen, says that they have been instructed by the Parliament to use wireless networks when travelling, in order to save money (Gulliksen 2011). Christoffersen says that she has asked specifically whether they should use unencrypted networks, to which the reply was yes. An anonymous source in the documentary provides the following imagined scenario of how such practices can be problematic, even on a national level: A Member of Parliament travels to China to negotiate about fishery policy. He sits in a meeting all day and goes back to his hotel to write a report. He then uses the hotel's wireless network and sends the report back to Norway via e-mail. But at the same time, and without his knowledge, the report is being printed out and brought to the Chinese who will face him the next day around the negotiating table.

The example above is just one of many scenarios that could happen if key personnel are incautious with sensitive information. It can also be transferred to other sections where employees take their work home and handle it on insecure WLANs. In extreme situations I believe it can affect critical functions in society such as power, transport and economy – perhaps in collaboration with social engineering methods explained in the paragraph below.

Social engineering is a popular method by scammers to retrieve sensitive information from unsuspecting victims, and I believe insecure WLANs are contributing to this. Carpenter and Barrett explain social engineering as "a technique used for persuading people to give you something that they should not give you" (2008, 460). If a person gets a phone call from a scammer pretending to be working in a bank, the person will most likely refuse to give up sensitive data such as credit card details. But if the scammer had personal information about the victim and his recent online purchases, the case might be different. Such information could have been retrieved by the scammer through a WLAN break-in, where e-mail login details were monitored. Scammers who are skilled at social engineering can make persons divulge almost anything (Joshi, Das, and Saha 2009). For such reasons it is not sufficient to have a secure computer system if the user practices are insecure.

5.3.1 WLAN Breaches in Norway

There have been few incidents of big scale WLAN breaches in Norway. If there has been any, it has rarely gotten media coverage. The reason for this could be that there simply are no breaches in Norway caused by attacks on wireless networks. Does that mean that insecure WLANs in practice pose no threat and that there is no need to secure your network? A more probable reason is that such attacks are rarely being noticed. Breaking into a WLAN and then monitoring it for sensitive information, leaves very little footprint. Say the attacker logs onto the victim's e-mail account. If this is done on the victim's wireless network, all logs will show that the e-mail is being accessed from the normal address. The only footprint an attacker leaves on the router is the MAC address – an address that can be spoofed with the click of a button.

The previously mentioned report by The National Institute for Consumer Research on identity theft says that about 240 000 persons in Norway have experienced some sort of identity theft (Brusdal and Lavik 2011). These acts were executed by exploiting the identity to either take up loans or credit, purchase products or services, or to damage reputation through name abuse. The report states that 10 % of the survey participants say that their identity theft have not been resolved (Brusdal and Lavik 2011). At the same time, Head of Communications at Telenor, Kristin V. Tønnessen, claims that about 50 % of the identity thefts Telenor reports are being dismissed (Dvergedal and Melby 2012). Assistant Chief of Police at the National Police Directorate[41], Torgeir Magnussen, explains that the percentage of dismissed cases is

[41] Politidirektoratet.

difficult to estimate because there are no penalty provisions for identity thefts specifically (Dvergedal and Melby 2012).

While the case scenarios in the report do not directly point out wireless networks as a gateway, they do mention online purchases as a source of credit card theft as well as misuse of national identity number to take up loans. Both of these methods can originate from network monitoring, and many have no clue how they have been victimized. A common scenario is that a perpetrator uses the national identity number to order several credit cards, steal the credit ratings from the post box and then the credit cards themselves when they arrive. When these credit cards are abused, the victims are left with a huge hassle of clearing payment remarks. Chief Executive Officer in the insurance company HELP Forsikring, Johan Dolven, says that this often requires assistance from lawyers due to its magnitude (Furuseth 2012).

5.3.2 Common Security Myths

The official study guide for CWNA (Certified Wireless Network Administrator) lists four common recommendations that "either provide no added security or minimal added security" (Carpenter and Barrett 2008, 518). These are all indications of erroneous assumptions caused by insufficient information.

- MAC filtering
- SSID cloaking
- Current equipment uses "better WEP"
- Wireless networks cannot be secured

A common myth is that enabling MAC filtering is sufficient to deny intruders access to a network (Carpenter and Barrett 2008). Finding out whether a network has this function enabled, however, requires an attempt to connect to the access point. Hence, my research cannot be used to show if there is a widespread use of MAC filtering. Nevertheless, I believe it is important to point out that such filtering is no substitution for a solid encryption. MAC filtering can be easily defeated using MAC address spoofing (Gast 2005; Carpenter and Barrett 2008).

SSID cloaking is an attempt of providing security through secrecy, an approach commonly referred to as *security through obscurity*. In terms of wireless networks, however, an SSID is not a secret (Cache, Wright, and Liu 2010). Passive sniffers, such as Kismet, will show the

SSID when a client associates with the network. It is even possible for a perpetrator to perform a deauthentication attack to force a client to reconnect instead of waiting for it to happen (Cache, Wright, and Liu 2010). Cloaked SSID is consequently only stopping the occasional bandwidth stealer and the persons who generally do not pose a threat.

In Section 4.2.1 I showed that 3.8 % of the WLANs I found had cloaked SSID. As shown in Chart 4.6, it was apparent that the percentage of insecure WLANs was higher when the networks were cloaked (43 % versus 36 %). While it is difficult to know for certain, I believe that end-users assume that hiding the SSID makes the network secure from intruders. It is also possible that some manufacturers have deactivated the SSID broadcast by default, and thus bringing in a new potential factor of error to my results – in addition to the relatively low number of cloaked networks. Consequently, I studied the data from cloaked networks in detail, but did not find any protruding irregularities. Because the network name is hidden on cloaked networks, it is more difficult to point out variations that could help with identification and comparisons. As such, there is no denying that the network name on visible networks often reveals a large amount of information. The remaining factors with value when the SSID is hidden are the MAC address, manufacturer, location and encryption.

When the initial scare of WEP's vulnerability hit, many vendors started implementing altered versions of the encryption protocol. Carpenter and Barrett (2008) say that, as a result, people started to think that new hardware fixed the WEP problems. The authors further argue that vendors should not be trusted to have implemented algorithms that protect against WEP weaknesses just because they use newer hardware (Carpenter and Barrett 2008).

There is also a notion that WLANs simply cannot be properly secured. In the official study guide for CWNA, Carpenter and Barrett state that wireless networks can be employed in a secure fashion by "using IEEE 802.11i (Clause 9 of IEEE 802.11-2007) and strong EAP types" (2008, 520). They further point out that WLANs can be far more secure than most wired LANs that do not use any real authentication mechanisms at the node level. Additionally and in a business perspective, to refrain from employing a WLAN increases the odds of employees installing rogue access points in the workplace (Carpenter and Barrett 2008).

When it comes to security myths, my impression is that if a wireless network is unencrypted, its users believe they have nothing to hide or do not consider the risks they expose themselves to. If the network is WEP-encrypted or cloaked, the users most likely think that their

connection is secure. These WLAN security myths are an obstacle in the process of securing wireless networking.

5.3.3 Security Measures by State Institutions

Following the Mumbai terror attacks in 2008 where related terror e-mails had been sent anonymously over WLAN connections, the Mumbai police created a task force to get rid of all insecure WLANs (Gadgil and D'Monte 2009). In the city believed to have over 30 000 unencrypted or anonymous WLANs, around 80 police personnel and 100 volunteers were trained for this task. The approach taken was to drive through Mumbai and directing owners of unencrypted networks to secure it. The Mumbai police told Business Standard that "If the Wi-Fi connection in a particular place is not password protected or secured then the policemen accompanying the squad will have the authority to issue a notice to the owner of the connection directing him to secure it " (Gadgil and D'Monte 2009).

Also Queensland Police in Australia planned in 2009 to conduct war-driving around selected towns in Queensland (Winterford 2009). In this case the police would pay a friendly visit to the households or small businesses that had open networks, and inform them of the risks they were exposed to. Queensland Police also stated they were going to promote it through media in order to highlight the significance of the problem. They were also hoping to return to the surveyed areas within a month to see if there had been any improvement. But even though I contacted Queensland Police and Mumbai Police on several occasions, they were unable to provide me with information on the current state of WLAN security in the respective areas.

On a similar note, the top criminal court in Germany ruled in May 2010 that private users were obligated to adequately secure their WLANs in order to prevent "third parties abusing it to commit copyright violation" (Grieshaber 2010). While owners of insecure networks now risk fines up to 100 euros, the court ruled that they would not be held responsible for the unauthorized criminal activity itself. The court did not expect users to constantly be updating security, but rather required setting up a password during WLAN installation.

5.3.4 Countermeasures and Recommendations

From an end-user perspective, the general approach to protect WLANs is to employ a strong encryption protocol in combination with a strong password. This means using WPA2-PSK, CCMP and preferably a long, complex and random passphrase. If TKIP is required, key renewal interval should be set to a low value. The Wi-Fi Alliance recommends that the passphrase should be at least 8 characters long and a mixture of symbols and upper and lower

case letters (Wi-Fi Alliance 2012). They give *FJ45od$#* and *%GkdR#$43* as examples of effective passphrases and *JohnDoe123* and *543Main* as ineffective. The first two examples would take up to 1 900 years and 182 000 years respectively to brute-force at 100 000 PSKs per second. While the latter two examples would take 266 000 years and 400 days to brute-force, dictionary attacks make them far less secure than the first two examples. The Wi-Fi Alliance (2012) states that passphrases should not contain personal information or words found in dictionaries. Additionally, the off-the-shelf SSID should be changed into something uncommon to avoid rainbow table attacks. Periodically changing the passphrase is also recommended. From a business perspective it is often better to employ the enterprise version (802.1X) of WPA2 than PSK. While it requires a more difficult installation process, the added security it offers should weigh up.

It is also important to prepare for and predict encryption vulnerabilities and breakthroughs in decryption methods. As clever use of graphical processing units significantly accelerated brute-forcing, quantum computing has the potential to ridicule many of today's encryption protocols. I am not saying that all encryption algorithms must be able to withstand a future threat of quantum computing, but there must be a plan ready for when security mechanisms become obsolete.

In May 2010, the Wi-Fi Alliance presented a roadmap that showed their plans for the certification with regard to encryption protocols (Fleishman 2010). This roadmap said that TKIP were to be prohibited from 2011 on access points and from 2012 on all devices, except as a component in mixed mode. In 2013, WEP will be disallowed for access points and in 2014 for all devices. This late deprecation of WEP is due to certain legacy devices that cannot be upgraded (Fleishman 2010). Also mixed mode of TKIP/AES will be prohibited from 2014. The slow-going process of certification amendment is a problem when considering how quickly encryption algorithms may be exploited when vulnerabilities are found. The Wi-Fi certification is also not solving the problem of old routers employing deprecated encryption. As such, even though the Wi-Fi Alliance's constantly evolving certification is a step in the right direction, it is not sufficient in providing general WLAN security.

There are, however, signs of improvement. For instance, the new user interface for ZyXEL routers show an indication of password strength when the user is configuring the WLAN security settings. There is little point for the Wi-Fi Alliance to enforce strong encryption protocols if ISPs and end-users are using too simple passwords. Furthermore, as access point

manufacturers use different user interfaces for their router configurations, the simplicity of enabling encryption can be an important factor in improving WLAN security.

The previously mentioned security measures by state institutions show initiative from authorities in different parts of the world. Whether these approaches have had beneficial effect is difficult to say without further research. While there is no doubt that the technology to secure wireless networks exists and can be easily applied, the challenge is to enlighten and convince everyone to use it. An important part of this challenge is to find out what sectors are to be appointed this responsibility, whether it is the router manufacturers, ISPs, state institutions or other establishments.

In my opinion, router manufacturers, ISPs and state institutions have a shared responsibility in securing wireless networks. Even though router manufacturers do not necessarily benefit from distributing routers with a preconfigured passphrase, a reputation of strong security is generally desirable. As several manufacturers make wireless routers for the ISPs, it is important that the manufacturers do not follow ill-advised specifications suggested by the ISPs, but instead counter with amendment proposals.

From the Internet service providers' point of view, secure routers would prevent bad publicity if the encryption mechanisms get exploited – which happened in the Telenor ZyXEL case. While I do not believe that a statutory requirement to secure private WLANs is the right approach, I do think it is crucial that organizations such as ICT Norway, Norwegian Centre for Information Security and Norwegian Post and Telecommunications Authority work together and put pressure on the sectors distributing wireless access points and routers.

A report on identity thefts by The National Institute for Consumer Research[42] from December 2011 investigated security practices in relation to education and age (Brusdal and Lavik 2011). The report showed that people with a higher education exposed themselves to the risks of identity thefts to a greater degree than people with a lower education. More people with lower education said that they would hide their pin code entry at ATMs, tear apart sensitive papers and log out of computers after sessions. The report also showed that older people was better at this than younger people.

These results, showing that security aspects are taken more lightly by younger persons and those with higher education, came as a surprise to me. While the report was not investigating

[42] Statens institutt for forbruksforskning (SIFO).

WLAN security, I believe it proves a need for similar research that focuses on wireless networks. Revealing insight of user practices will make it easier to approach the security issues from the right angle – both from a manufacturing and educational point of view.

As the report shows that higher education is not enough, it is essential to educate our society specifically about the dangers related to ICT security. Mixed recommendations on the ISP web pages on whether to use WEP or WPA makes it difficult to choose the right protocol. Secure WLANs will not only benefit the end-user, but it will also make for a more resilient society in general. Some enlightenment is spread through media where articles expose the risks of using open networks, especially when you are travelling. One example is the previously mentioned documentary on NRK that demonstrated how vulnerable wireless networks can be. Another example is from May 2011, when researchers from NorSIS demonstrated in the newspaper VG the simplicity of creating a fake access point in hotels and cafés (Engan 2011). They set up a strong network card as a router and named the SSID as the original WLAN. As the network card they used was ten times more powerful than regular routers, end-users would connect to the fake access point rather than the original. Because the traffic was now going through the researchers' PC they could monitor every action and steal sensitive information when e-mail accounts were logged on. VG published the article as a warning for travelling persons that use random WLANs to check their e-mail. The typical advice is to only log onto networks that you know belong to the facility you are in and to always use *https* in front of web addresses. There are, however, methods to beat the SSL/TLS protocols when *https* are being used. Nevertheless, the use of this encrypted communication is significantly more secure than transferring information unencrypted over regular *http.*

In my opinion, a key factor to improve our encryption practices lies within usability. The end-user needs a simple way of securing his network that does not require an understanding of the encryption protocols. At the same time, having a strong encryption on wireless networks does not matter if people connect to fake access points deployed by criminals, or share sensitive information on unencrypted public WLANs. That means that not only must there be awareness on securing home networks, but also on the risks of using wireless networks in general.

6 SUMMARY

A central goal of this study was to investigate the degree of insufficiently encrypted wireless networks in Norway. I also wanted to find out the reasons for the current status and how to improve it. In doing so, I hope to promote WLAN security awareness to the ICT industry and the general public. As I have investigated and developed on my initial concerns, I will in this chapter summarize my main findings.

In my **first research question** I ask about the current state of WLAN encryption in Norway. I have shown that there are a large amount of unencrypted and poorly encrypted WLANs in Oslo, Bergen, Kristiansand, Tromsø and Flekkefjord. While there were minor fluctuations between the cities, my main finding is that at least 36 % of the 35 194 wireless networks in my research were insufficiently encrypted. Including WPA-encrypted networks with weak passphrases would raise the percentage further.

I also ask whether city population or location affect encryption usage. While there was a higher percentage of insecure WLANs in the smaller cities, I was unable to answer whether this was caused by the geographical area or other factors. This would have been easier to establish if the cities' geographical sub-areas were smaller, or if my research had spanned a larger area. Had that been the case, it would have been possible to make a comparison with existing research on living standards such as education, income and unemployment.

My **second research question** is about how the Internet service providers affect the situation. It is obvious that they have an important role due to their distribution of wireless access points. Their preconfigured routers must use solid encryption, strong passphrases and be prepared for breakthroughs in decryption. I have shown that this is not the case for every ISP and that they tend to leave the responsibility for securing routers in the hands of their customers.

My **third research question** concerns the consequences poor WLAN encryption has for our society. I have presented a multitude of methods in which wireless networks can be abused, and exemplified it with actual events that have occurred. I believe that the broad circulation of insecure WLANs contributes to identity thefts, loss of accessibility and business secrets being stolen. Additionally, penetrated insecure WLANs could endanger critical functions in our society.

In research question 3a I ask whether encryption practices have changed over the last few years. Even though research on the subject is lacking, I have argued that encryption usage seems to be improving. Better ISP practices and increased knowledge is contributing to this. The Wi-Fi certification is adapting and routers are more likely to be distributed with WPA now. The Wi-Fi Alliance has also presented a roadmap that disallows WEP completely in 2014.

In order to answer research question 3b, I have presented my recommendations to improve today's situation by arguing that the responsibility is shared between end-users, broadband providers, access point manufacturers as well as the government. End-users must learn to secure their WLANs properly and broadband providers need to use solid encryption and strong passphrases. The manufacturers must implement logical user interfaces and write comprehensible instructions.

All the different actors involved need to take wireless network security seriously, and governmental organizations must find a way to make this happen. By continuing the indifference and allowing the problems concerning WLAN security to exist, both the individual and the society remain at risk.

6.1 Future Research

For future research it would be very interesting to cover the same areas of wireless networks and find out if encryption practices are really changing. It would also be interesting to dig deeper into causes for the encryption variations between cities, and to compare more specific areas within the cities. For instance, comparing business areas versus residential areas could be beneficial if considering various approaches to improve the general WLAN security. When it comes to user practices, a qualitative study would probably give a better picture of end-user reasoning.

As raising the awareness of the issues of wireless networking was motivating me to write this thesis, I want to publish my findings through the media. I have been in dialog with the Norwegian Post and Telecommunications Authority who wanted to create an article of my findings. I hope this will lead to further and in-depth research on WLAN security in Norway.

7 REFERENCES

Aardal, J. V. *Arealplankart - Utsnitt bydeler*. Kristiansand kommune, 25.02.2011 [cited 04.03.2011]. Available from http://www.kristiansand.kommune.no/no/planer-prosjekter/Kommuneplan/Kommuneplankart/.

AirSnort. *AirSnort Homepage*. AirSnort 2011 [cited 29.03.2011]. Available from http://airsnort.shmoo.com/.

Altius IT. *Top 10 Wireless Network Risks*. Altius IT, 2010 [cited 29.04.2011]. Available from http://www.altiusit.com/files/blog/Top10WirelessNetworkRisks.htm.

Bie, T. *Så lett får de tilgang til tusenvis av private nettverk*. ITavisen, 2010 [cited 18.02.2011]. Available from http://www.itavisen.no/854879/saa-lett-faar-de-tilgang-til-tusenvis-av-private-nettverk.

Brusdal, R., and R. Lavik. *Identitetstyveri - Omfang, tillit og beskyttelse mot risiko*. SIFO, 28.12.2011 [cited 17.03.2012]. Available from http://sifo.no/files/file78016_oppdragsrapport_nr_6-2011_id_tyveri_rev.pdf.

Cache, J., J. Wright, and V. Liu. 2010. *Hacking exposed wireless: wireless security secrets & solutions* 2nd ed. New York, NY: McGraw-Hill.

Carpenter, T., and J. Barrett. 2008. *CWNA: Certified Wireless Network Administrator Official Study Guide (Exam PW0-100)*. New York: McGraw-Hill.

Chu, M. M. *GPU Computing: Past, Present and Future with ATI Stream Technology*. AMD, 09.03.2010 [cited 25.05.2011]. Available from http://developer.amd.com/gpu_assets/GPU%20Computing%20-%20Past%20Present%20and%20Future%20with%20ATI%20Stream%20Technology.pdf.

Cisco Systems, I. *Omni Antenna vs. Directional Antenna*. Cisco, 27.02.2007 [cited 13.03.2011]. Available from http://www.cisco.com/application/pdf/paws/82068/omni-vs-direct.pdf.

Devine, C. *aircrack documentation*. Wirelessdefence.org, 2011 [cited 30.03.2011]. Available from http://wirelessdefence.org/Contents/AircrackORIGINAL.html.

Devine, K. *Default WEP/WPA key algorithm for Thomson routers* 2008 [cited 31.01.2011]. Available from http://hakim.ws/st585/KevinDevine/.

Dvergedal, P. V., and A. Melby. – *Altfor mange ID-tyverisaker henlegges*. NRK.no, 21.02.2012 [cited 17.03.2012]. Available from http://www.nrk.no/nyheter/distrikt/ostlandssendingen/1.8005610.

Engan, Ø. *Slik blir du lurt i en trådløs felle*. VG, 26.05.2011 [cited 29.01.2012]. Available from http://www.vg.no/teknologi/artikkel.php?artid=10091881.

Finkle, J. *Amazon cloud can help hack WiFi networks: expert*. Reuters, 07.01.2011 [cited 03.04.2011]. Available from http://www.reuters.com/article/2011/01/07/us-amazon-hacking-idUSTRE70641M20110107.

Finkle, J., and P. Wahba. *Target Co was victim of hacker Albert Gonzalez*. Reuters, 30.12.2009 [cited 23.03.2011]. Available from http://www.reuters.com/article/2009/12/30/us-hacker-idUSTRE5BS3LU20091230?type=technologyNews.

Fleishman, G. *Say Goodbye to WEP and TKIP*. Wi-Fi Net News, 18.06.2010 [cited 12.01.2012]. Available from http://wifinetnews.com/archives/2010/06/say_goodbye_to_wep_and_tkip.html.

Fluhrer, S., I. Mantin, and A. Shamir. 2001. Weaknesses in the Key Scheduling Algorithm of RC4. In *Selected Areas in Cryptography*, edited by S. Vaudenay and A. Youssef: Springer Berlin / Heidelberg.

Frankfort-Nachmias, C., and D. Nachmias. 2008. *Research methods in the social sciences*. New York: Worth Publishers.

Furuseth, F. *Tone Damli Aaberge risikerer identitetstyveri etter bloggtabbe*. TV2.no, 12.01.2012 [cited 20.03.2012]. Available from http://www.tv2.no/underholdning/gkn/tone-damli-aaberge-risikerer-identitetstyveri-etter-bloggtabbe-3681709.html.

Gadgil, M., and L. D'Monte. *Mumbai police plug Wi-Fi security holes*. Business Standard, 13.01.2009 [cited 30.04.2011]. Available from http://www.business-standard.com/india/news/mumbai-police-plug-wi-fi-security-holes/00/56/346002/.

Gast, M. 2005. *802.11 Wireless Networks: The Definitive Guide*. Beijing: O'Reilly.

Gaudin, S. *Estimates Put T.J. Maxx Security Fiasco At $4.5 Billion*. InformationWeek, 02.05.2007 [cited 22.03.2011]. Available from http://www.informationweek.com/news/security/showArticle.jhtml?articleID=199203277.

Gilbrant, J. M. *Telenor har visst om alvorlig sikkerhetshull siden juli*. Dagbladet, 31.10.2010a [cited 21.02.2011]. Available from http://www.dagbladet.no/2010/10/30/nyheter/telenor/innenriks/14064713/.

Repeated Author. *Telenor politianmelder «hacker»*. Dagbladet, 02.11.2010b [cited 21.02.2011]. Available from http://www.dagbladet.no/2010/11/02/nyheter/telenor/innenriks/14106128/.

Grieshaber, K. *German court orders wireless passwords for all*. Msnbc Digital Network, 12.05.2010 [cited 30.04.2011]. Available from http://www.msnbc.msn.com/id/37107291/ns/technology_and_science-security/.

Groten. *gps + ssid + wpa key = internett der du trenger.* Norsk Freakforum, 2010 [cited 27.01.2011]. Available from http://freak.no/forum/showthread.php?t=169211.

Gulliksen, T. *300 sekunder: Trådløs*. VGTV, 2011. Available from http://www.vgtv.no/#!id=47312.

Halvorsen, F., O. Haugen, M. Eian, and S. Mjølsnes. 2009. An Improved Attack on TKIP Identity and Privacy in the Internet Age, edited by A. Jøsang, T. Maseng and S. Knapskog: Springer Berlin / Heidelberg. Available from http://dx.doi.org/10.1007/978-3-642-04766-4_9.

Hole, K. J., E. Dyrnes, and P. Thorsheim. 2005. Securing Wi-Fi Networks. *Computer* 38 (7):28-34.

Hu, H., S. Myers, V. Colizza, and A. Vespignani. 2009. WiFi networks and malware epidemiology. *Proceedings of the National Academy of Sciences of the United States of America* 106 (5):1318-23.

IEEE. 2004. IEEE Standard for Information Technology- Telecommunications and Information Exchange Between Systems- Local and Metropolitan Area Networks- Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Medium Access Control (MAC) Security Enhancements. *IEEE Std 802.11i-2004*:0_1-175.

Iversen, M. *Kommuneplanens arealdel*. Bergen kommune, 05.01.2011 [cited 04.03.2011]. Available from https://www.bergen.kommune.no/aktuell/tema/arealplan/5643.

Jewell, M. *Encryption faulted in TJX hacking*. USA Today, 26.09.2007 [cited 22.03.2011]. Available from http://www.usatoday.com/tech/news/computersecurity/infotheft/2007-09-26-tjx-encryption-breach_N.htm.

Johannessen, A., P. A. Tufte, and L. Kristoffersen. 2004. *Introduksjon til samfunnsvitenskapelig metode*. Oslo: Abstrakt forl.

Joshi, Y., D. Das, and S. Saha. 2009. Mitigating man in the middle attack over secure sockets layer. Paper read at Internet Multimedia Services Architecture and Applications (IMSAA), 2009 IEEE International Conference on, 9-11 Dec. 2009.

Jupp, V. 2006. *The Sage dictionary of social research methods*. London: Sage.

Kerber, R. *Cost of data breach at TJX soars to $256m*. Boston Globe, 15.07.2007 [cited 23.03.2011]. Available from http://www.boston.com/business/globe/articles/2007/08/15/cost_of_data_breach_at_tjx_soars_to_256m/.

Kershaw, M. *Documentation*. Kismet, 2011 [cited 08.03.2011]. Available from http://www.kismetwireless.net/documentation.shtml.

Ledingham, M. *Sentrumsplanen 2008 (kommunedelplan for sentrum)*. Tromsø kommune, 19.03.2010 [cited 07.03.2011]. Available from http://www.tromso.kommune.no/sentrumsplanen-2008-kommunedelplan-for-sentrum.4546088-121597.html.

Marczyk, G., D. DeMatteo, and D. Festinger. 2005. *Essentials of research design and methodology*. Hoboken: Wiley.

Ministry of Justice and the Police. *St.meld. nr. 17 (2001-2002)*. Regjeringen.no, 05.04.2002.2002 [cited 21.11.2011]. Available from http://www.regjeringen.no/Rpub/STM/20012002/017/PDFA/STM200120020017000DDDPDFA.pdf.

NETGEAR. *What's New in Security: WPA (Wi-Fi Protected Access)*. NETGEAR, 15.02.2011 [cited 10.02.2011]. Available from http://kb.netgear.com/app/answers/detail/a_id/1105/~/what's-new-in-security%3A-wpa-(wi-fi-protected-access).

Nilsen, J. E. *10 000 rutere må byttes ut*. Hardware.no, 29.10.2010 [cited 21.02.2011]. Available from http://www.hardware.no/artikler/10_000_rutere_maa_byttes_ut/79157.

Parrish, K. *Nvidia: The Future of Graphics Processingw*. Tom's Hardware, 06.05.2011 [cited 25.05.2011]. Available from http://www.tomshardware.co.uk/Tony-Tamasi-ECGC-2011-Tegra-ray-tracing-DirectX-11,news-35544.html.

Pereira, J. *How Credit-Card Data Went Out Wireless Door: Biggest Known Theft Came from Retailer With Old, Weak Security*. The Wall Street Journal, 04.05.2007 [cited 22.03.2011]. Available from http://online.wsj.com/article/SB117824446226991797.html.

PISA, and WTIA. *Wireless LAN War Driving Survey 2010 Hong Kong*. Safewifi.hk, 04.03.2011 [cited 26.10.2011]. Available from http://www.safewifi.hk/files/War-driving%20Report%202010%20(v0.6).pdf.

PST. *Annual threat assessment 2011*. Norwegian Police Security Service, 01.03.2011 [cited 21.05.2011]. Available from http://www.pst.politiet.no/Filer/utgivelser/trusselvurderinger%20engelsk/Unclassified_threat_assessment_2011.pdf.

PT. *Det norske markedet for elektroniske kommunikasjonstjenester - 1. halvår 2011*. Norwegian Post and Telecommunications Authority (PT), 14.11.2011 [cited 12.12.2011]. Available from http://www.npt.no/ikbViewer/Content/132865/Det%20norske%20markedet%20for%20elektroniske%20kommunikasjonstjenester%20foerste%20halvaar%202011.pdf.

Punch, K. F. 2005. *Introduction to social research: quantitative and qualitative approaches*. London: Sage Publ.

Rager, A. T. *WEPCrack*. WEPCrack, 2011 [cited 29.03.2011]. Available from http://wepcrack.sourceforge.net/.

Ranvik. *Hvordan cracke WPA-nøkkel hos rutere med SSID NextGenTel_XX.* Norsk Freakforum, 2010a [cited 20.02.2011]. Available from http://freak.no/forum/showthread.php?t=143236.

Repeated Author. *Hvordan finne standard WPA på zyxel-routere fra Telenor(privatXXXXXYYY)*. Norsk Freakforum, 2010b [cited 18.02.2011]. Available from http://freak.no/forum/showthread.php?t=161543.

Sinha, A. *Preventing Wireless Data Breaches in Retail*. The ICOR, 2007 [cited 05.04.2011]. Available from http://www.theicor.org/art/present/art/ARCI00029.pdf.

SSB. *Andel som har brukt Internett og minutter brukt til Internett en gjennomsnittsdag, etter kjønn, alder og utdanning*. Statistics Norway, 31.03.2011a [cited 27.04.2011]. Available from http://www.ssb.no/tabell/04519.

Repeated Author. *Brukere av Internett, hyppighet og sted siste 3 måneder. Andel av befolkningen, etter kjønn, alder, utdanning og arbeidssituasjon.* Statistics Norway, 21.07.2011.2011b [cited 27.11.2011]. Available from http://www.ssb.no/ikthus/tab-2011-07-01-04.html.

Repeated Author. *Jamn utvikling mot raskare breiband*. Statistics Norway, 07.03.2011c [cited 27.04.2011]. Available from http://www.ssb.no/emner/10/03/inet/.

Repeated Author. *Utviklingstrekk. Breibandsabonnement fordelt etter marknad. Berre aktive abonnement. Heile landet utan Svalbard*. Statistics Norway, 08.03.2011d [cited 27.04.2011]. Available from http://www.ssb.no/emner/10/03/inet/tab-2011-03-08-03.html.

Staveland, L. I. - *Offentlig datasikkerhet er en stor bløff*. Aftenposten.no, 17.11.2011 [cited 01.04.2012]. Available from http://www.aftenposten.no/nyheter/iriks/--Offentlig-datasikkerhet-er-en-stor-blff-6699134.html.

Stern, P. C., and L. Kalof. 1996. *Evaluating social science research*. New York: Oxford University Press.

Telenor. *Hjelp til bredbånd*. Telenor, 2010 [cited 01.02.2011]. Available from http://www.telenor.no/privat/kundeservice/bredbandshjelp/.

Repeated Author. *Q1 2011 Interim report - January–March 2011*. Telenor, 04.05.2011 [cited 04.05.2011]. Available from http://www.telenor.com/en/resources/images/2011-q1-telenor-report_tcm28-58478.pdf.

Tews, E., and M. Beck. 2009. Practical attacks against WEP and WPA. In *Proceedings of the second ACM conference on Wireless network security*. Zurich, Switzerland: ACM.

Tews, E., R.-P. Weinmann, and A. Pyshkin. 2007. Breaking 104 Bit WEP in Less Than 60 Seconds. In *Information Security Applications*, edited by S. Kim, M. Yung and H.-W. Lee: Springer Berlin / Heidelberg.

Thompson, C. *NY case underscores Wi-Fi privacy dangers*. Associated Press, 25.04.2011 [cited 29.04.2011]. Available from http://www.usatoday.com/tech/news/2011-04-25-wifi-warning.htm.

Ventelo. *Ventelo kjøper ADSL-porteføljen fra BKK*. Ventelo, 13.11.2009 [cited 22.02.2011]. Available from http://www.ventelo.no/om-ventelo/aktuelt-og-media/nyhetsarkiv/pressemeldinger/13.11.2009-ventelo-kjøper-adsl-porteføljen-fra-bkk.html.

Weil, N. *Hacker Gonzalez gets 20 years for Heartland breach*. Reuters, 26.03.2010 [cited 23.03.2011]. Available from http://www.reuters.com/article/2010/03/27/urnidgns002570f3005978d8002576ef004839d-idUS387115075320100327.

Wi-Fi Alliance. *Make Security a Priority in 2011: Protect Your Personal Data on Wi-Fi® Networks*. Wi-Fi Alliance, 02.02.2011 [cited 29.04.2011]. Available from http://www.wi-fi.org/media/press-releases/make-security-priority-2011-protect-your-personal-data-wi-fi®-networks.

Repeated Author. *Security*. Wi-Fi Alliance, 2012 [cited 19.01.2012]. Available from http://www.wi-fi.org/discover-and-learn/security.

Winterford, B. *Queensland Police plans wardriving mission*. iTnews, 17.07.2009 [cited 01.05.2011]. Available from http://www.itnews.com.au/News/150387,queensland-police-plans-wardriving-mission.aspx.