Security in wireless networks:

Vulnerabilities and countermeasures

Department of Software Engineering
and Computer Science
Blekinge Institute of Technology

Spring 2003

Authors:
Josephine Larsson
Ida Waller

Supervisor:
Anders Carlsson
Miroslaw Staron

Examinator:
Guohua Bai

Abstract

The market for wireless networks has increased over the years, more and more organizations implement this technology. The need to work flexible, convenient and cost-effective are three reasons for the technology's raised popularity. The use of wireless networks has exposed new aspects of network security. The information is no longer dependent on wires because it can be transmitted trough radio waves instead. The exposure of information increases, therefore also the vulnerabilities. This leads to more security problems related to the exposure of the transmitted information.

It is difficult to understand the importance of network security and why to invest resources for it. Investing in security can lead to lower costs in the long run, because incidents can be perceived before it is too late.

This thesis will describe why it is important to perform a risk assessment before developing a security policy. One of the reasons for having a security policy is to clarify the responsibilities for the network security to raise understanding for security within the organization. Other motive is to define how the information should be protected when transmitted in the wireless network. For example, by using the IEEE standard protocol (WEP), which may not be the best encryption solution.
For organization that handles sensitive information it is important to be aware of the security problems that exist and to prevent the security risks. A case study was performed at several county councils in Sweden. The reason for this was that county councils handle sensitive information. The case study's main purpose was to evaluate the level of knowledge about wireless security at county councils.

Keywords:
Wireless networks, Security, Security policy, WEP

Index

1 Introduction

The market for wireless networks has increased during the last years because of reduced prices, which gives the opportunity to work more mobile. Installations of access points for wireless networks are quite expensive, but the time and cost savings for adding another node is very low. Wireless networks are less expensive than ordinary wired networks in maintenance of hardware, because there is no need for cables.

Since the market for wireless networks is continuously growing, various security problems and aspects have emerged [C]. The security aspects concern how to protect the information and how to guarantee authentic transmissions. The security problems are well known and many studies have been done in this area. The studies have been more focused on the technical aspects of security [15]. However, the studies, which examined wireless networks, found several networks that were insecure. Maybe these problems have emerged because of the company's priority. According to a study made by Meta Group [5], 41 per cent of the companies spend two per cent or less of their IT-budget on security. Lack of knowledge may be an important reason why companies do not spend more resources on security. To increase the awareness of the security problems, one should start analyzing the risks and try to find the threats against the organization's information. From the result of the risk analysis a security policy can be developed.

The thesis explains how aware the county councils in Sweden are about the security problems that exist in networks, especially wireless networks. Which methods the county councils used for developing their existing security policies and what kind of encryption technique that is used will be described in the thesis.

1.1 Problem domain

Wadlow [D] says, "A perfect state of security is never achievable". There is no hardware or software that can protect a network to 100 percent, but a certain level of protection could always be achieved. The process of improving the security in a network is a never-ending work. This thesis intends to attract attention to why it is important to improve the security, especially to organizations that handle sensitive information. A great help to improve the security can be a functional policy. This can guide all administrators and users to how to handle information and equipment. For example, to avoid critical incidents, like theft and virus-attacks. Encryption can be a good way to protect the information that is transmitted over the network.

1.1.1 Hypothesis

"The level of knowledge about security in wireless networks among county councils in Sweden is low."

According to Dawson knowledge can be divided in these terms [A]:

- Data – elements describing objects or events. Representation of gathered raw numbers and raw text.
- Information – processed data to provide insight. The data has been analyzed, summarized and processed to understandable and useful formats.
- Knowledge – higher level of understanding. Knowledge represents understanding of the "why" compared to the information's idea of the "what". The personal interpretation of gained information from rules, patterns, decisions, models, and ideas.
- Wisdom – the ability to put the knowledge into practice. Represents the ability to apply skills and experiences to create new knowledge and adapt to different situations.

The levels of knowledge that the authors of the thesis have defined are based on Dawson's terms of knowledge. To evaluate the stated hypothesis the following levels have been applied:

- Zero – no knowledge at all about security in wired and wireless networks.
- Low – have knowledge about security, wired and wireless networks, but have problems to realize how important security is.
- Medium – have knowledge about security, wired and wireless networks and understand the importance of security and can apply some parts of it.
- High – have good knowledge about security, wired and wireless networks and can apply all this knowledge into practice.

1.2 Delimitations

The delimitations in this thesis will be three county councils in Sweden and the security related problems in wireless networks. This involves problems with secure transmissions of information over the wireless network by using encryption techniques. The case study is based on interviews with IT-managers, since they are the most appropriate and knowledgeable personnel.
One of the main delimitation of this thesis is the time span (end of January to end of May).

1.3 Methods

The methods that are used in this thesis are data collection from literature, Internet and the performed case study to evaluate the hypothesis.

1.3.1 Methods for case study

The research methods that are used in the case study are a quantitative study and a qualitative study. A questionnaire will be used for the quantitative method and open questions for the qualitative method.

1.3.2 Data Collection

The data is collected from literature and Internet. The subjects of the literature are mainly network security and network communication. Most of the literature is published not later than 2000.The main part of the collected data consists of published articles and papers that were found on Internet. The authors of the thesis have been very careful with the sources on Internet, to be sure that this information is true and has been published.

1.4 Purpose

The purpose of the thesis is to discover how aware the county councils are about the security problems in wireless networks.
Reasons for the thesis is to show the threats and to inform about the problems concerning wireless networks and try to get the companies to spend more resources on security. Increasing security in wireless networks can in the long run lead to lower costs compared to the costs of repairing the damages after each incident.

1.5 Target group

The target group for the thesis is Network and Security Managers working at medium and large organizations in Sweden. The reason for choosing organizations in Sweden is that the organizations follow the same laws and regulations. Technical terms that are only mentioned, but not defined, in the thesis are explained in the glossary in appendix A.

2 Definitions of wireless network and security

2.1 Wireless Network

A wireless network, IEEE 802.11 [1] can be used where wired networks cannot be used, for example outside. Implementing a wired network can cause problems with cable installations. Wireless networks installations can be less complicated than wired networks when it comes to adding nodes, although installing access points can be problematic. These problems come from for instance building materials, furnishing and electronic equipment, which can interfere signals. In the long perspective wireless network equipment will be less expensive than equipment to wired networks. The access points and the network interface cards to wireless are still expensive, but there is no costs for cables and their maintenance. [C]
The advantages of wireless networks can be, for instance to facilitate the work to decrease the risk of typing wrong or forget information. [C] This can lead to increased productivity.
The disadvantages of wireless networks are the limited range and the security aspects. [C] The limited range can from the point of security be good, because the encryption standard (WEP) in wireless networks are not secure enough. If sensitive information is transmitted over the wireless network it is recommended to use more protection.

2.2 Security

According to the dictionary security means a state without fear [E]. Security in the area of computer science refers to techniques for ensuring that data stored in a computer cannot be read or compromised by unauthorized users. Another way of perceiving security is protection against interference leading to negative consequences.
Security consists of four parts [15]:

1. Physical security - how to prevent interference signals.
2. Data Security – what encryption techniques are used to protect the network against eavesdropping.
3. User authentication – how to protect the wireless network from unauthorized users.
4. User anonymity- what kind of protection is used against information gathering.

Wadlow [I] says that security is a process and the process can be applied again and again to the network and the organization that maintains it. If this is done the security of the network will be improved. Since, every time the process is applied, security gaps can be found, which means that countermeasures can be accomplished. If stop applying the process of security, the security becomes reduced, due to all threats and techniques that emerged from day to day.

3 Security policy

3.1 Description

A security policy is a document that describes the organizational rules of acceptable use for computing resources, security practice and operational procedures.
Wadlow [I, p.12] gives a few examples of why a security policy serves a number of purposes and those are:

- It describes what is being protected and why.
- It sets priorities about what must be protected first and at what cost.
- It allows an explicit agreement to be made with various parts of the organization regarding the value of security.
- It prevents the security department form acting frivolously.

3.2 Risk assessment

To develop a security policy it is recommended to start with a risk assessment, i.e. find out what weaknesses, threats and vulnerabilities a company has. According to the Security Policies & Standards Group [10] the process of performing a risk assessment before developing a policy has its advantages, for instances:

- *Cost justification* - Additional application of security more or less always involves additional expense. As this investment does not directly generate revenue, it should be justified in financial terms.
- *Targeting of security* - Security should be directly targeted and related to potential impacts, such as threats and existing vulnerabilities. If it fails to achieve this it could result in unnecessary expenditures. The process of the risk analysis should be applied across the entire business, to be able to establish the areas of greatest risk as quickly as possible.
- *Consistency* - A major advantage of the applying the process risk analysis is that it brings a consistent and objective approach to all security assessments of all the systems within the company.
- *'Baseline' Security and Policy* - Many companies are devoted to certain 'baseline' standards. This could be for many different reasons, such as legislation (e.g.: Data Protection Act, i.e. PUL in Sweden), company policy and culture and regulatory controls for example. The risk analysis method should support such requirements and enable identification of any problems.

- S*elf-Analysis* - The risk assessment should be as simple as possible to enable its use without any necessary IT and security knowledge. This approach enables security to be applied into a larger area of the company, because it enables security to become a part of the company culture, which leads to that business management will take more responsibilities for the security.

3.2.1 Risk analysis

There are two different approaches for risk analysis, quantitative [25] and qualitative, which is the most widely used. Usually a qualitative risk analysis consists of three elements, threats, vulnerabilities and controls.

Threats
To do a risk assessment start with a threat assessment. The reason for this is to realize the company's threats, weaknesses and vulnerabilities. An important thing to think about is that it exists three different types of threats [B].

- Physical threats – for example fire, theft, destruction, problems with components.
- Logical threats – manipulation or unauthorized use of a system.
- Human/Organizational threats – these threats arise when users within the organization have bad routines, the responsibilities are unclear or that the users do not have enough knowledge.

Vulnerabilities
Make a system more open to attacks that are likely to have some success or impact. For example, for fire vulnerability would be the presence of inflammable materials.

Controls
The four types of countermeasures for vulnerabilities are [25]:

- Warning controls reduce the likelihood of a deliberate attack
- Preventative controls protect vulnerabilities and make an attack unsuccessful or reduce its impact
- Corrective controls reduce the effect of an attack
- Detective controls discover attacks and trigger preventative or corrective controls.

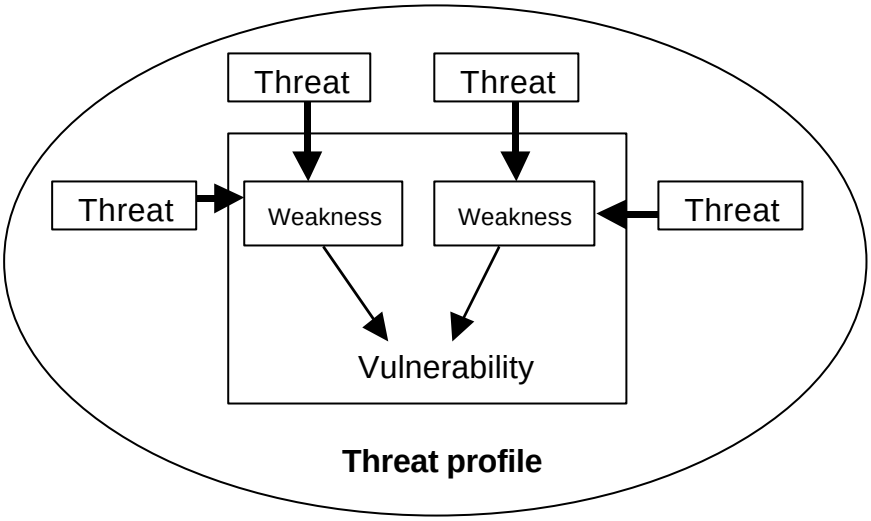


Figure 1: External threats and weaknesses create vulnerability [B].

3.3 Developing a security policy

3.3.1 Security policy concepts

In the beginning of the development of the policy, the different terms needs to be defined to avoid misunderstandings.
A sample policy defined by Mitrovic [B] describes the responsibilities for different positions within the organization. The board of the organization and/or the chief executive officer has the comprehensive responsibility for the IT security.
The IT manager and other managers are given specific areas to be responsible for.
Mitrovic [B, p.139-140] defines the terms threat, weakness and vulnerability. These terms will help the organization to achieve a clear threat profile.

3.3.2 Countermeasures

The countermeasures can be divided into the same groups as threats. [B]

- Physical countermeasures – Are used to decrease the damages of possible occurred threats.
- Logical countermeasures – To reach a higher level of protection one can have a single authorization administration and have common anti-virus protection and intrusion detection.
- Administrative countermeasures – It is good to have a clear organization that describes the company's culture and also have a clear regulation including the audit trails of things that occur in the information system.

Before start analyzing the different part of the organization's information system the organization should make a decision about what security levels should be applied. Mitrovic [B, p. 142] gives an example of five levels.

- No damage – In this level one can find resources that can easily be replaced at low cost. The company can survive without these resources for a week or even longer.
- Small damage – These IT resources are not important to the company, but they will not pass by without problems. The resources are not very complicated to restore, and this can be done to a low cost. The company can be without these IT resources up to a week.
- Damage – The IT-resources that are placed in this category are important to the company but not very critical for the company itself or the customers. The restoring of the damage is uncomplicated but expensive. Up to three days the company can survive without these resources.
- Serious damage – In this category the resources are very important for the company and they cannot be without it more than a day. The resources must be restored fast and are very expensive.
- Very serious damage – if there is damage on the resources placed in this level it will have very serious impact on the entire system. The resources must work every day and night at all time. If there will be a stop, it cannot last more than an hour. It is very critical and expensive to repair the damages therefore are the company trying to avoid incidents on these resources.

3.4 The IT security guide - FA22

FA22 is a security guide from the Swedish Emergency Management Agency former Swedish Agency for civil emergency planning. The security guidelines are written to the authorities in first hand, but it is a good guideline for all organizations.
The FA22 security guide describes a way of approve the IT operations, which can almost be compared with a certificating of the systems.

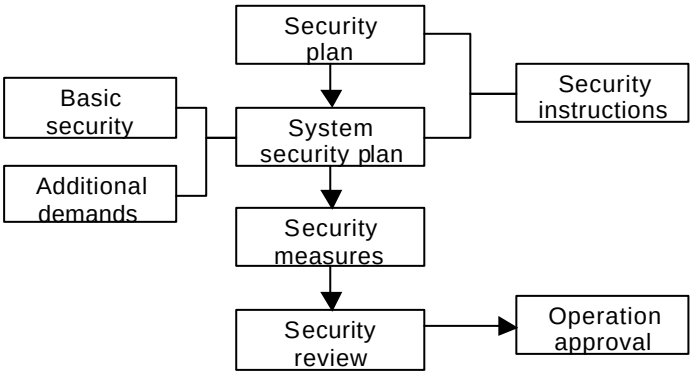


Figure 2: The process of security according to the FA22 standard. [16]

As seen in the figure above, the FA22 is about deciding specific goals for the IT security. The organization needs to identify the requirements and what countermeasures that may be needed. The FA22 guide will help the organization through this process step by step. By help from different documents the organizations can develop their security policy.

3.4.1 Security plan

The first part of the FA22 security guide is about developing a security plan, which is essential for the security policy. This document is a comprehensive document that should satisfy the organization's needs for IT security. The following things are recommended to be included in the security plan [16]:

- Goals
- Guidelines
- Responsibilities

The goals for the IT security work should be developed at the management level. The goals must be concrete and measurable to be accepted by the entire organization. The security plan must follow laws and regulations, for instance the personal data act. The goals can consist of who is responsible for following the security plan and its goals. Other issues are what type of security levels should exist, follow up and control of the IT security. How should the goals be achieved in reality is the question that should be answered in the guidelines section. The questions are, who is responsible for the information, which is responsible for the coordination of the IT security throughout the entire organization and to plan and perform education. The last point should specify the responsibilities and how these are divided among the different functions within the organization. See the following example of FA22 security guide:

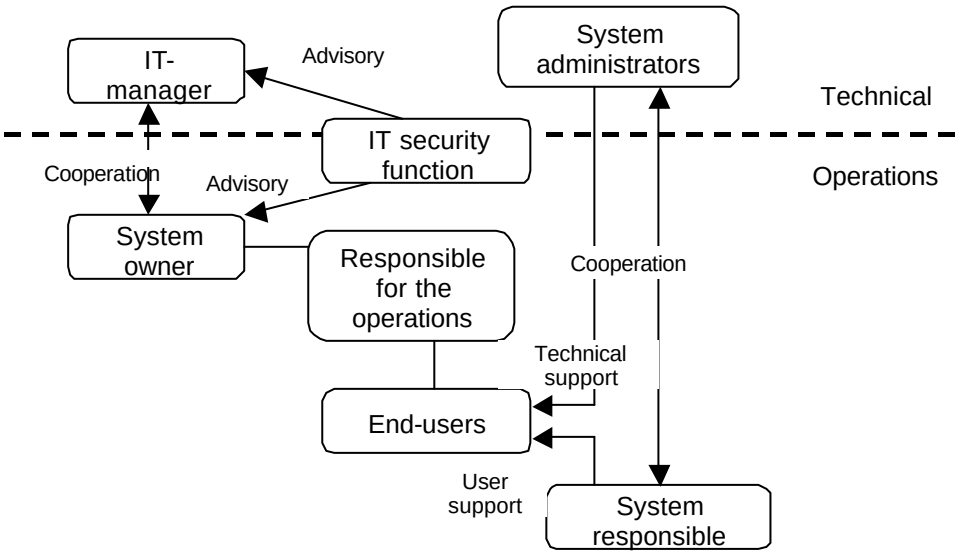


Figure 3: The IT security responsibilities always follow the organization's structure [16].

The IT security responsibilities more or less always follow the organization's structure, i.e. those that are head of a department, are also responsible for the IT security at that department. It is important that laws and regulations are followed, because of the personal integrity protection and different partners' demands for correct information, this includes the publics right to see official documents.

When developing a security policy it is important to decide the lowest level of security for a system and function, because of this FA22 IT security guide recommends organizations to develop a security plan for each system within the organization. From this a security document can be developed which states the regulations to follow. A document of security instructions can be developed and it can consist of different versions, depending on which system or systems are used and by whom. In a system security policy one should define what type of system and who are the owner, the responsible and the users of a particular system. Other things that one will find in the system security policy are information about each system and the connections between other systems. It should also include information about laws and regulations that the system must follow. The confidentiality, reliability and availability are important, because those will show how sensitive the system are for interruptions.

Other documents that the FA22 security guide recommends are interruption plan and catastrophe plan. The interruption plan contains countermeasures that will be used in certain situations to get the system work as it should as fast as possible after an interruption. The catastrophe plan will be used in situations that are called catastrophic by the management team and contain a backup plan with alternative ways to get the system work again.

3.5 The standard ISO 17799

ISO 17799 is the most widely recognized security standard and it is based on BS7799, which was published in May 1999 for the last time. The first version of ISO 17799 was published in the end of 2000. ISO17799 is a complete standard in coverage for security issues, not only developing security policy, but also how to maintain the entire network. It contains a large number of control requirements, some very extremely complicated. It is therefore recommended that the ISO 17799 standard be approached step by step. The best starting point is often a risk assessment of the current position to identify the risks. The step follows by identification of what changes that are needed to be able to follow ISO17799 standard. Then it is time for planning and implementing the standard. [9]

3.5.1 The content of ISO 17799

ISO 17799 is an extremely detailed security standard, organized into ten different parts. The parts are as follows [11]:

- ***Business Continuity Planning***
  To work against interruptions and if they do occur how to handle the critical situation.
- ***System Access Control***
  This part is about how to control access, to prevent unauthorized users to gain computer access and access to the information systems. It is important to ensure the protection of network services and to detect unauthorized activities. Another issue under system access control is to ensure that information is secured transmitted over mobile networks.
- ***System Development & Maintenance***
  The section handles system development and maintenance. First of all to ensure that security is built into the systems and to maintain the security of software applications. To ensure that support activities behave in a secure way and to protect the confidentiality, authentication and integrity of information. Maintenance means to prevent loss, modification or misuse of user data in application systems.
- ***Physical and Environmental Security***
  The four part is about how to prevent unauthorized access, damage and interference to the company's buildings, but also to prevent compromise or theft of information and information processing services. To prevent loss, damage or compromise of assets and interruption of business activities.
- ***Compliance***
  To avoid that any criminal or civil law and legal, regulatory or contractual responsibilities of security requirements are violated.
  Guarantee compliance of systems with organizational security policies and standards are essential. Maximizing the effectiveness of the system audit process and to minimize the interference.
- ***Personnel Security***
  When it comes to personnel security ISO 17799 says that reducing risks of human errors, fraud, theft or misuse of facilities are necessary to ensure that users are aware of information security threats. The personnel should be concerned about their security and support the security policy in their daily work, to minimize the damages of security incidents.
- ***Security Organization***
  The security of information processing should be managed within the company, even when information has been outscored to other organizations or used by third parties.
- ***Computer & Operations Management***
  This section handles how to ensure that correct and secure operations of information are used. The supporting infrastructure must secure the information in the networks and to minimize the risk of system failures. Information needs to be protected and to maintain the integrity of software and information during transmission in the network. Another important aspect in this section is to prevent damage to assets and interruptions to the activities of the business. The

last issue is to prevent loss, modification or misuse of information exchanged between organizations.

- ***Asset Classification and Control***
  The ISO standard believe that it is important to maintain appropriate protection of company's assets to ensure that information assets receive an appropriate level of security.
- ***Security Policy***
  To implement a document provided with management direction and support for information security. Within each of these ten sections there are detailed statements that should be stated in the policy document. If following these, a functional security policy and security standard will be set at the organization.

3.6 Personal data act

The data act from 1973 had been out of date for a long time, and needed to be substituted with a new law, when the personal data act was established in 1998. According to section one in the personal data act the purpose of the law is to protect people against violation of their personal integrity by processing of personal data [7]. Before describing the personal data act further, a few definitions will be made [8]:

- Personal data – all kinds of information that is directly or indirectly referable to a natural person who is alive constitute personal data. The personal data act applies to such processing of personal data as is entirely or partly performed with the support of computers.
- Processing – refers to everything one does with personal data, whether performed through computer system or not. The following may be mentioned as examples of processing personal data: collection, registration, storage, processing, and disclosure by transfer, dissemination or other provision of data and compilations or joint processing.
- The Controller – A person who alone or together with others decides why and how personal data shall be processed is called the controller of personal data. This is usually a legal person, for example, a company, an association, a public authority or a local authority. Even a natural person as a businessman may be a controller.
- Assistant – Personal data assistant refers to a person who processes personal data on behalf of the controller. The assistant may be an employee or an independent service provider.
- Representative – A personal data representative is a physical person who, on the assignment of the controller, shall ensure that personal data is processed in a lawful and proper manner.

The personal data act consists of requirements regarding the processing of personal data. These demands include that personal data may only be processed for specific, explicitly stated and justified purposes. Personal data may, if these fundamental requirements are fulfilled, in principle only be processed if the person registered gives his/her permission. The exemptions are in the exercise of official powers, when a work task of public importance is to be performed and in order that the controller of personal

data should be able to fulfill a legal obligation. Organization, like county councils that have personal data in computer systems needs to have a controller and a representative that are permitted by the Data inspection board to fulfill these demands. Section 18 in the personal data act state that health and hospital organizations are allowed to process sensitive personal data if necessary [7].

The controller is obligated to implement appropriate technical and organizational measures to protect the personal data that is processed. The measure that needs to be fulfilled is that the most appropriate technical possibilities available are used. The same applies to what it can cost to implement these technical possibilities, the special risks that exist with the processing of personal data and how sensitive the data in fact are that is processed. [7, Section 31]

According to section 36 [7] the controller of personal data chooses a representative. The controller shall inform the Data inspection board when choosing a representative and when changing the representative at the organization. The representative should supervise the controller and report to the Data inspection board if the controller does not manage the personal data in an appropriate way.
Another task that a representative have, is to ensure that the controller processes personal data in a lawful and correct manner. If unsure, the representative should consult with the supervisory authority, i.e. the Data inspection board, in case of doubt about how the rules of processing personal are data applied.
If the controller causes a registered person injure and in this way violate the personal integrity according to the personal data act [7, section 48], the person has the right to compensation.

4 WEP and VPN

4.1 Wired Equivalent Privacy

Wired Equivalent Privacy (WEP) is a security protocol, designed to provide a wireless network with a level of privacy and security, which is comparable to a protocol used for a wired local area network. A wired network is protected by physical devices that are efficient for a controlled environment but not for a wireless network, since the wireless uses radio waves. The WEP protocol seeks to establish an equivalent environment as for the wired network by encrypting the data that is transmitted over the wireless network. The encryption protects the exposed wireless link between access points and clients. The protocol's security goals are proposed to enforce these three specific requirements [13]:

- Confidentiality: to prevent casual eavesdropping is a fundamental requirement.
- Access control: to protect access to a wireless infrastructure.
- Data Integrity: to prevent interference for transmission of messages.

WEP is based on the Ron's Code 4 Pseudo Random Number Generator (RC4 PRNG) algorithm, a symmetric key encryption algorithm from RSA Security, Inc [20].
This algorithm generates a number sequence, a key that is entered and controlled by the user. The access points and clients use the same key to encrypt and decrypt transmissions. The key that WEP uses consists of either 64 or 128-bits in length. 24-bits of the key length is an initialization vector (IV). The protocol also uses an integrity check vector (ICV) to ensure the integrity of each packet. WEP is used at the data link and physical layer of the Open Systems Interconnect (OSI) reference model [H].
WEP process the ICV by performing a 32-bit cyclical redundancy check (CRC-32) of the frame and attach the ICV to the original frame, resulting in the plaintext. Then, the message plus ICV is encrypted via the RC4 PRNG algorithm using a long sequence key stream of pseudorandom bits. The sequence key stream consists of the 40-bit secret key and the 24-bit initialization vector (IV). All authorized users in the wireless network share this secret key. To produce the cipher text an operation is performed between the plaintext and key stream. The operation is called an exclusive-or (XOR) operation. The produced cipher text is then sent over the access point. Data integrity is supplied by the cipher text and due to encryption, confidentiality is provided. The receiver, of the cipher text, has to go trough the same procedure, but in reverse to retrieve the original message frame. This means that to retrieve the plaintext the cipher text must be decrypted with a duplicated key stream. The receiver must validate the checksum on the plaintext by comparing the computed ICV with the last 32 bits of the plain text. This is done to ensure that the receiver only accepts the frames with the valid checksum.

The WEP protocol can either be implemented with a 40-bit key and a 24-bit IV or an extended version that use a larger key. Thus, the shorter key can easily be compromised via a so-called brute-force attack [D]. However, the larger key can also be compromised, but the 104-bit key makes it more difficult to perform the attack.
There are of course other alternative attacks that are useful because they do not require a brute-force strategy. Which means that the strength of the key does not matter.

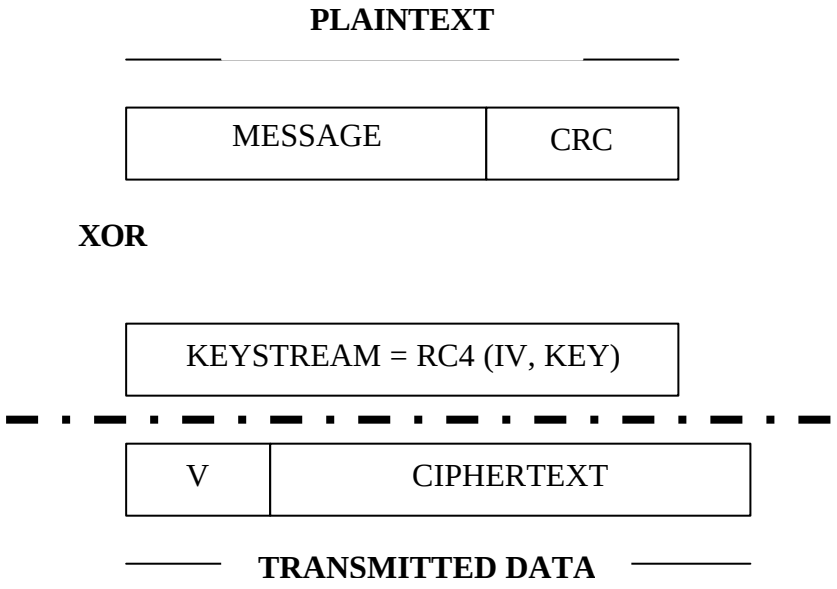


Figure 4: Encrypted WEP frame [13]

4.1.1 WEP´S Weaknesses

There are unfortunately a few problems connected with WEP [13]. A paper [26] written by three of the world's foremost cryptographers demonstrated the vulnerability of the RC4 cipher. The paper's authors discovered several ways to uncover patterns in packets of information passing over wireless networks. These patterns can be used to figure out the WEP encryption "key" and the number used to scramble the data being transmitted. Once the key is recovered, it can be used to decrypt the messages.
The authors say using a longer key, one of 104 bits compared to the current WEP standard of 40 bits, does not make it significantly harder for attackers to uncover the process. This shows that anyone with a wireless laptop, plus software that is available from the Internet, can now gain access to a wireless network within less than 15 minutes. RC4 is based on a cipher stream sequence, and this stream sequence contains the inherent weaknesses that proved to be devastating in the attack performed by the authors of the paper.

The known weaknesses that the WEP protocol has are [13]:

- Key management and key size
- The Initialization Vector is too small
- WEP's use of RC4 is weak
- The Integrity Check Vector algorithm is not appropriate
- Authentication messages can be easily forged

The first weakness
The first weakness that WEP has depends on that the key management is not specified for the WEP standard. Without having the interoperable key management, the used keys will be long-lived with reduced quality. It is known that wireless networks use one single key between the nodes of the network. This results in that the access points and clients are programmed with the same key. The process of changing keys is quite difficult and uninteresting, that is why the keys are rarely changed for the network. The size of the key that consists of 40-bits can also be defined as a weakness. There are larger keys that can be used to be more interoperable, and these keys size are 104-bits. Unfortunately the 104-bit key is sometimes called the 128-bit key, but this comparison is totally not fair. When setting up the larger key the users have to enter 13 characters, but it should be 16 characters to be called a 128-bit key. Whether the encryption key consist of 40-bits or 104-bits the IV remain the same with 24-bits. The use of a larger key will be more resistant to a brute-force attack compared to attacks on 40-bits keys that can be discovered in a relatively short time.

The second weakness
The second weakness that the protocol has is the problem with the IV, because it is too small. The size of the IV is 24-bits and can provide approximately 16,7771216 different cipher streams for a given key [17]. The cipher stream is exclusive-or operated with the original packet to give the encrypted packet, and the IV is sent in clear text with every transmitted packet. The main problem is that the IV can be reused. If an attacker finds the given IV in a cipher stream, the attacker is able to decrypt packets that have been encrypted with the same IV or worse even forge packets. It makes a large difference depending on how the IV is chosen, because there are only 16 million IV values available. How the IV is chosen or how often it is changed is not specified by the WEP protocol. The IV can start at zero and increases for each packet and goes back to zero after 16 million packets have been sent. The IV can be chosen randomly, which seems to be an excellent idea, but unfortunately this is not true. If the IV is chosen randomly, the chance of reuse is over 50% after less than 5000 packets. To discover cipher streams for particular IV's, there are several methods to use. If two encrypted packets have the same IV, an attacker can find the original exclusive-or operation by exclusive-or operating the encrypted packets. The attacker can send e-mails or just ping the victim if the victim is on the Internet. By observing and analyzing the encrypted packets, the attacker is able to deduce the cipher streams.

The third weakness
The third weakness is that the ICV algorithm is not appropriate. The ICV is based on the cyclic redundancy check algorithm, and this is developed for detecting common errors and noise in transmission. So basically the CRC-32 is really excellent for

detecting errors, but for cryptographic hash it is useless. There are other algorithms that can be used for the ICV, for example MD-5 or SHA-1 [G]. The message consists of the CRC-32 ICV, which is a linear function. Because of this the attackers are able to modify encrypted messages and fix ICVs to make the message authentic. The possibility to modify encrypted messages gives opportunities for number of simply attacks to be performed. The attacker can capture encrypted packet streams, modify the destination addresses of each packet to be the attacker's IP address, fix the CRC-32, and retransmit the packets. The victim's access point will then decrypt the packets and forward them to the attacker. This is an example of how a simply attack can be performed. The problem with IV- and ICV-based attacks is that they are independent of the key sizes. Large or small keys do not matter; they all appear to be the same.

The fourth weakness

The fourth weakness concerning WEP is the protocol's weak use of the RC4 algorithm. It has been found that the implementation of this algorithm in WEP has weak keys. Having a weak key means that correlation between the output and the key is more than it ought to be. An attacker can easily take advantage of this weakness, because the first three bytes are taken from the IV and these are sent unencrypted in each packet. This makes it easy for the attacker to determine the weak key of the encrypted packets. All the attacker needs to do is to be within 30 meters of the access point.
There are about 9000 IV values out of 16 million that are valuable for this kind of attack, which means that these values indicates the presence of weak keys. By filtering for IVs that indicates weak keys, the attacker can capture packets that seem interesting. After gathering the interesting packets, the attacker analyzes them and only need to try a few keys to be able to gain access to the wireless network. It is not difficult for the attacker to know when the right key has been determined, since all IP packets start with known values. The attacker has to capture between 2,000 and 4,000 packets to be able to determine a 104-bit WEP key. To protect the network from these kinds of attacks, it is a benefit not to use weak IV values. However, if one of the nodes in the network uses a weak key, the attack can be performed.

The fifth weakness

The fifth weakness that the protocol deals with is the problem with authentication messages; they can easily be forged. There are two different kinds used for authentication [2]: Open System (no authentication) and Shared Key authentication, which are used to authenticate the client to the access point. The reason for developing Shared Key authentication was that it would be better to use than not to use any authentication at all, because the user has to prove knowledge of the shared WEP key, to be able to authenticate him. Unfortunately, this is not true: the use of authentication reduces the total security of the network and makes it easier for attackers to determine WEP keys. This means when using Shared Key authentication a user has to prove the knowledge of the shared WEP key. However, an attacker can observe the user when proving the knowledge of the shared key and take advantage of this. The attacker can determine the RC4 stream used to encrypt messages from the observations of the user and use this stream to decrypt messages in the future. By monitoring a successful authentication, the attacker can forge an authentication. The use of Shared Key authentication has one advantage; it reduces the ability to perform a denial-of-service attack [G] against the network. The other authentication method that can be used provides better network security.

Network managers should turn off Shared Key authentication and depend on other authentication protocols instead.

4.2 Virtual Private Network

Virtual private network (VPN) [3] is a network that uses a public telecommunication infrastructure, to provide remote offices or individual users with secure access to their organization's network. The VPN follows a client and server approach.
The VPN clients and VPN servers are used in three different scenarios [4]:

1. Support remote access to an intranet.
2. Support connections between multiple intranets within the same organization.
3. Join networks between two organizations, forming an extranet.

The VPN supply connectivity over a long physical distance, and can be seen as a form of Wide Area Network (WAN). A VPN server can connect directly to another VPN server. The connection between the two servers extend the intranet or extranet to span multiple networks. The creation of tunnels, the setting of configuration parameters, and the connection and disconnection from the server are supported by VPN. VPN solutions use a number of different network protocols, for example PPTP (Point-to-Point Tunnelling Protocol), L2TP (Layer Two Tunnelling Protocol), IPsec, and SOCKS.
The encrypted data at the sending end and the decrypted data at the receiving end must be sent trough a tunnel. The data must be properly encrypted, otherwise it cannot be sent. To provide a better level of security the originating and receiving network addresses are encrypted as well. Without sacrificing features or basic security the VPN technology implements restricted-access in networks that use the same cabling and routers as a public network. The main benefit is that VPN have same capabilities that other networks have, but it can be provided at a lower cost.

A virtual private network solution is the most suitable alternative for wireless networks compared to the use of WEP and MAC address filtering. The VPN network support security mechanisms to defend data and ensure that only authorized users can access the network. The most used network protocol for securing VPN traffic is IPSec (Internet Protocol Security). IPSec uses DES, 3DES or other bulk algorithms to encrypt the data and keyed hash algorithms (HMAC, MD5, SHA) for authentication of packets. Digital certificates can be used to validate public keys. A VPN also support other authentication methods like RADIUS [E] and SecureID. The mentioned methods facilitate the integration into existing network infrastructures.
IPSec includes three primary security elements [12]:

- **Authentication Header (AH)** – provides authentication and integrity by adding authentication information to the IP datagram. This ensures that data will not be available to an unauthorized station.
- **Encapsulation Security Payload (ESP)** – provides confidentiality. Integrity and authentication can be provided, depending on which algorithm that is used. When using ESP, part of the header and the contained data in the datagram is

encrypted. Available modes are transport and tunnel; the last is the choice for remote access.

- **Internet Key Exchange (IKE)** –key management protocol used for negotiating the cryptographic algorithm choices to be employed by the AH and ESP. The mechanisms used in IKE provide for an extremely scalable solution. The Diffie-Hellman algorithm [G] ensures that the keys are exchanged securely.

The right solution

The combination of VPN (IPSec) and 802.11 is an excellent solution for the security needs of wireless networking. The wireless access points are configured for open access with no WEP encryption, the VPN handles the security. VPN provide encapsulation, authentication and encryption over the wireless network. The result is that the organizations have fully protected, transparent access to network resources. The VPN servers can be centrally managed, which decreases the administrative overhead. VPN solutions are scalable to a very large number of users, unlike the use of the wired equivalent privacy protocol. The VPN approach is flexible enough to be used in a variety of different scenarios, all with the same user login interface and procedure (See Figure 5 below):

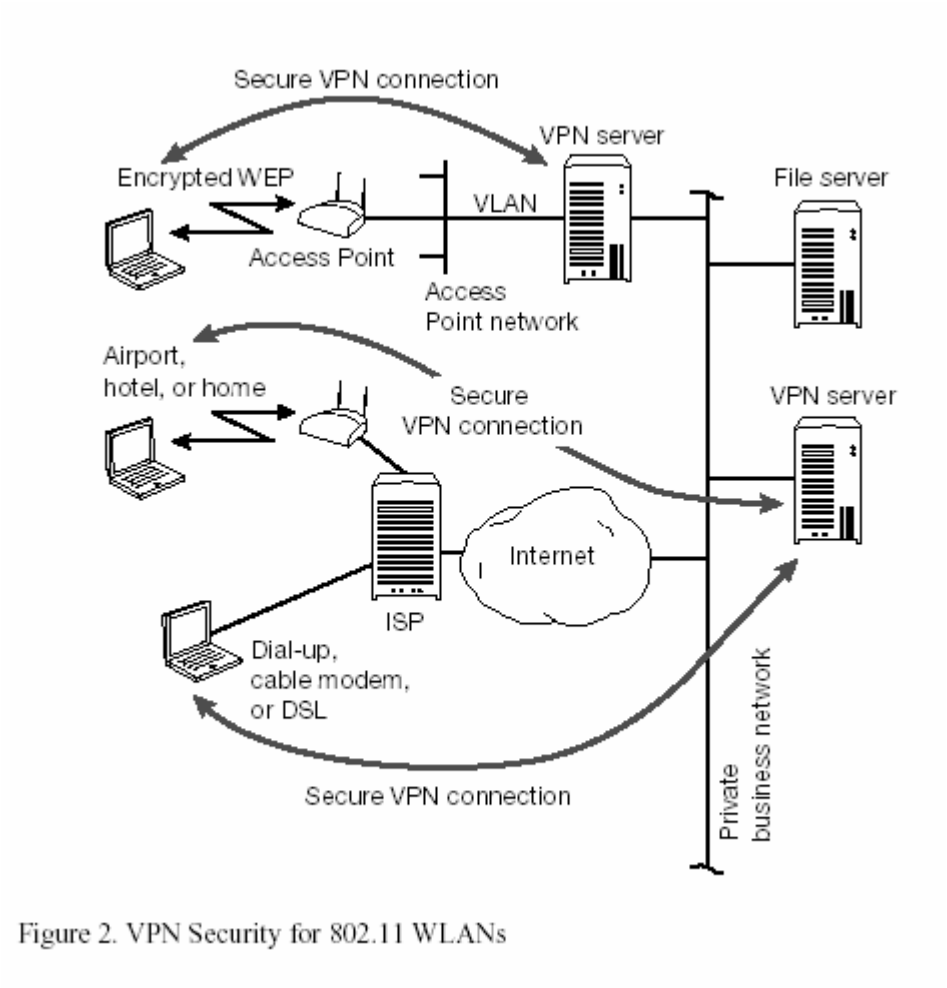


Figure 2. VPN Security for 802.11 WLANs

Figure 5: VPN Security for 802.11 WLANs [12].

Using dial-up, cable modems or Digital Subscriber Line (DSL) connections to the Internet, remote users can establish a connection to the VPN server and wireless network. Public wireless access areas, like airports, can be used to establish a VPN connection back to the wireless network. On-campus 802.11 wireless accesses can be implemented by means of a VPN connection.

Cipher block sequences are used in VPN solutions and are more difficult to crack. This is why virtual private networks offer the best solution for security aspects in wireless networks.

4.3 War drive

War driving is the act of locating and possibly exploiting connections to wireless networks. To do war driving, the attacker needs a vehicle, a laptop, a wireless network card, software and an antenna. Because a wireless network may have a range that extends beyond the office building, an attacker can gain access to the wireless network, to obtain free Internet connection, the possibility to view the company's records and other resources. Some people have made a sport out of war driving, to demonstrate how easy it is to compromise a wireless network. The war driver can systemically map the locations of wireless access points with an antenna and a GPS system.
Companies that have a wireless network are recommended to add security utilities ensuring that only intended users have access.[23]

4.4 WEPCrack

WEPCrack is an open source tool for breaking the WEP protocol's secret keys, developed by Anton Rager. The tool is an implementation from the attack that was described by Fluhrer, Mantin, and Shamir in their paper [26].
WEPCrack was the first available code that demonstrated the attack; the code was first released two years ago [24]. The tools capabilities are Perl based, and are composed of certain scripts. The first script, WeakIVGen.pl, generates different Initialization Vector (IV) combinations that can weaken the secret key used to encrypt the packets.
The next script, prism-getIV.pl, searches for IVs that match the pattern known to weakened secret keys. The script captures the first byte of the encrypted output and places the weak IVs and the captured byte in a log file. The third script, WEPCrack.pl, uses data collected or generated by the first script, WeakIVGen to attempt to determine the secret key. The script works with either 40bit or 104bit WEP. The last script, Prism-Decode.pl can decode most frame types for wireless networks. The script can be used for capturing SSIDs, Access Points MAC addresses, or authentication data.

5 Case study

5.1 Design of the case study

To evaluate the hypothesis a case study was performed on three county councils in Sweden, because of confidentiality, the county councils will be mentioned as A, B and C. The case study consists of three interviews with the responsible managers for network communication and security. The chosen managers were the most suitable for the interviews, because they are responsible for the security issues.
Before the interviews, the county councils received e-mail with the questionnaire, to give the councils time to read through the questions and prepare answers. The interviews were divided into two parts; the first part is a questionnaire and the second, a few open questions.

The questionnaire has a rating scale from 1 (disagree) to 5 (totally agree), this scale is known as the Likert scale [19]. The questions in the questionnaire were for example about security policy and standards for this, education for security, encryption, and wireless networks utilities. The questions can be categorized in general and specified questions. An example of a general question is: “Have you followed any guidelines or standards when developing your security policy” and a specified question is: “Did you follow the standard FA22, when developing your security policy?”(See appendix B). For the open questions the county councils had to motivate their ratings for each question in the questionnaire. The personal data representatives at each county council were e-mailed open questions about the personal data act.

5.1.1 Operation

During a period of 9 days in March 2003, the interviews were performed at the county councils´ IT-departments. The interviews last for about an hour each and both authors of this thesis took notes. Question about Personal data act were emailed to the personal data representatives at each county council. The answers were received within three weeks from the questions were sent.

5.2 Result from interviews

5.2.1 County Council A

Based on the interview with county council A, the authors of the thesis have distinguished certain characteristics:

- Have a manager that is responsible for the security.
- Aware of the security problems that are connected with the use of wireless networks.
- The IT-department are interested in solving these problems by testing their wireless network.
- Apply the same level of security throughout the entire network.
- Guidelines and standards, i.e. FA22 and ISO17799, have been followed when developing the security policy.
- The policy is updated when changes occur.
- The staff at the IT-department does mostly learn from each other.
- Performs tests on their networks in safe environments

5.2.2 County Council B

Based on the interview with county council B, the authors of the thesis have distinguished certain characteristics:

- Does not have a manager that is responsible for the security, and they are aware that this is a problem.
- The person we interviewed had difficulties with answering the questions related to the security policy because he had not been involved with the development of the security policy.
- The policy has not been updated since it was developed a couple of years ago.
- The county council's wireless network is only tested when incidents occur.
- The staff at the IT-department has the opportunity to take courses and visit conferences at least one to two weeks per year.

5.2.3 County Council C

Based on the interview with county council C, the authors of the thesis have distinguished certain characteristics:

- Does not have a security policy, but the IT-department is developing a security policy based on available standards, for example the standard FA22.
- Does not have a manager responsible for the security.
- Does not test the networks themselves, but instead external consultants provide help with the testing of the networks twice a year.

- The personnel are able to take courses up to two weeks per year; they generally prefer to take courses in the security area.
- The end-users at the county council, who use the networks, are forced to change their passwords after 90 days.

5.2.4 General characteristics for A, B and C

The following characteristics are the same for all the county councils:

- The information that is transmitted over the wired and wireless network are completely the same for A, B and C.
- There are no limits for what kind of information that can be transmitted over the networks. Thus, the wireless networks are only used for specific systems.
- No protection is used against interference signals.
- Are familiar with WEPCrack and war driving.
- Neither one of the county councils are dependent on their suppliers for assistance with installations and maintenance of the equipment for wireless networks.
- The firewalls and anti-virus protection is frequently updated at the three county councils.
- No specific programs for audit trails are used among the three county councils.
- The end-users for the networks are responsible for changing and choosing their own passwords.

5.2.5 Result of open questions

The results of the open questions for the three county councils were almost the same. Neither of the county councils had different security policies for wired and wireless networks. There were no reasons for not transmitting the same information over the wired and wireless networks.
The passwords can consist of either lower case and upper case letters and special signs and numbers. There are no regulations for how the password should be chosen.
The three county councils have not had any problems with interference signals.
There is no specific percentage of the IT-budget that is assigned for security.
It varies from year to year.
The encryption technique that is used by the three county councils is the standard for IEEE 802.11 networks, the Wired Equivalent Privacy protocol (WEP).
All three county councils are going to implement a virtual private network solution in the near future, because no one uses VPN today.

5.2.5.1 Result of Personal data act questions

County council A:

- The county council is a part of an authority that is the personal data controller.
- That personal data are handle in an accurate and legal manner is the task of the representative.
- The data inspection board had done it possible to control personal data under responsibility.
- At each administration there is a personal data representative.
- The tasks for a personal data representative both at administration and authority level are:
    - To be informed about all use of personal data and to get this information to the representative.
    - To be responsible for that other laws and rules are followed.
    - To be responsible for that information's obligation are fulfilled according to the law.
    - To be responsible for that errors are corrected.
    - To follow up the use of personal data and security aspects.
    - To inform the board if problems occurs and those not are taken care of.
    - Follow the policy for information security
    - The personal data are protected enough if section 31 in the personal data act is followed.

County council B

Has not received answers from county council B regarding the open questions about personal data act.

County council C

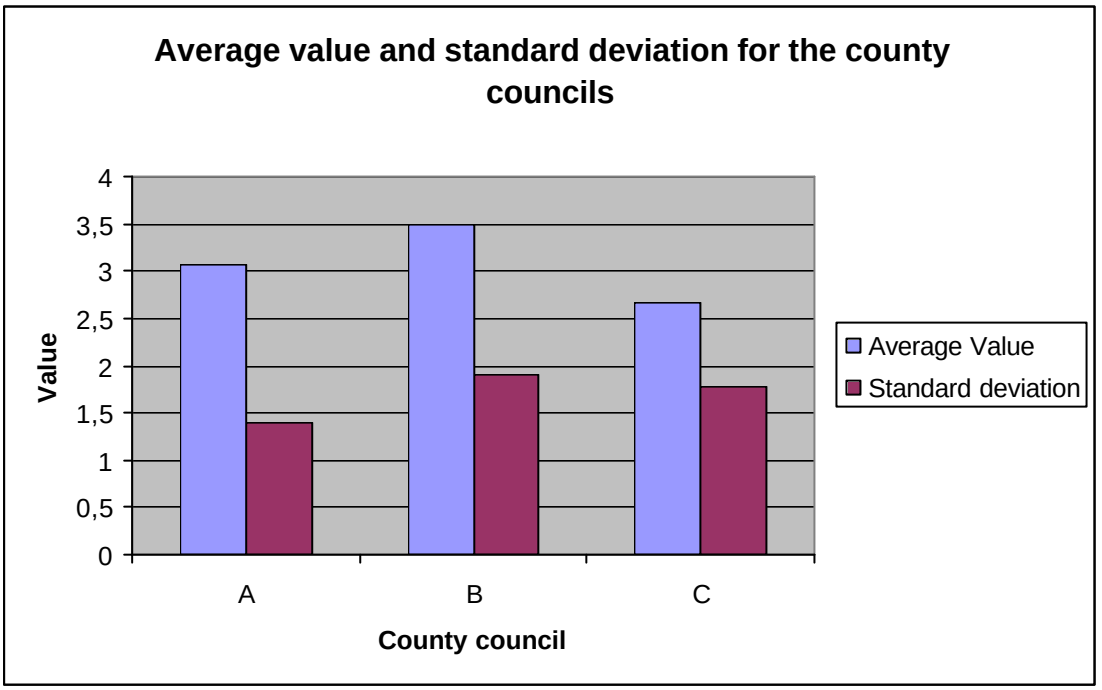
- The county council has a personal data representative.
- Have responsibility to process personal data in a secure and accurate way.
- Transmitting personal data in a wireless network is not secure
- Personal data controllers are the county council board and the county council director
- If understanding, knowledge and interest for these questions exist at the county council board, it is possible to protect personal data in a legal, proper and ethical manner.
- The old law, i.e. the data act, was not better at protecting the personal data.

5.2.6 Summary of the results

The results of the questionnaires are summarized to give an easier overview of the three county councils´ answers [See appendix D].

The table below presents the average value and standard deviation that is calculated for each county council.

County Council	**A**	**B**	**C**
Average Value	3,06	3,5	2,67
Standard deviation	1,39	1,9	1,78
Number of questions	18	16	18
Number of N/A	0	2	0



5.3 Discussion

Before the interview with county council B, the board had to see the questionnaire to decide whether we were allowed to perform the interview with the IT-manager or not. This may be a confounding factor[1], because it may have influenced the answers of the interview and the answers could be different, if the confidentiality did not exist. The reason for the board to take this decision, can be something positive, since this is a sign that the board at the county council are concerned about the information that exists in the organization.

During the interviews we recognized that county council B and C did not have a functioning and updated security policy. We believe that it is a risk not to have a functioning security policy, because it can cause problems within the organization. For example, for who is responsible for what and the authentication levels should be clear. The administrators and the end-users ought to have different levels that they are authorized for. When developing a security policy a risk analysis is performed, this can be a good help when it comes to realizing the treats that exists against the networks. How to handle an incident should also be stated in the security policy. This will lead to that when an incident occurs, the policy has direction for how to handle the situation.

A conclusion that could be drawn from the case study is that the IT-departments at the county councils were very nonchalant against the information they have in their systems. No one seems to be interested in the information, since the county councils transmit the same information over the wired and wireless networks.
A county council handles very sensitive information about the patients at for example a hospital and the information should be confidential.
According to the Personal Data Act, section 31 the organization has to "implement appropriate technical and organizational measures to protect the personal data that is processed" [7]. This is why an organization like a county council needs to be careful with the information that is transmitted over the wireless network.

The county councils are using the standard encryption technique for protecting the wireless networks, but as mentioned in the theory part (see 5.1), the wired equivalent privacy protocol has several weaknesses. The weaknesses are difficult to attend to since the key stream is reused and the initialization vector is static. The attacker has no problems with decrypting the encrypted messages, if the attacker is patient.
To use the wired equivalent privacy protocol is better than not using any encryption at all, cause it provides a certain amount of protection.
We strongly believe that when handling sensitive information like the patients´ journals, the best way is to apply the virtual private network solution to protect the transmitted information over the wireless network.

[1] A confounding factor is something that is incorrect, but cannot be explained, which leads to that it influences the result.

When using the WEP protocol the keys are static and must be changed frequently to prevent access from the outside. Unfortunately the county councils do not change their keys or change them very seldom, which gives attackers excellent opportunities to take advantage of the county councils network and information.
The county councils are planning to implement VPN in the near future, but for now it is under construction. This shows that the county councils are aware that their existing protection should be improved.
However, the county councils are not testing their networks as frequently as they should. County council A performs test on the wireless network in safe environments before implementing. External consultants performs tests on the entire network at county council C. Unfortunately county council B only test their network after an incident has occurred.
There are several reasons for testing the network; the first reason is to discover the existing security gaps. The second reason is to diminish the risks for intrusion and the third is to find traces from attackers intrusion attempts. The main reason is to secure the network to prevent future attacks.

The firewalls and anti-virus protection for the wired is frequently updated at the three county councils, which is very good. The county councils may prioritize the wired network more than they prioritize the wireless. Reasons for this can be that it is easier to protect wired networks, because of more knowledge and more tools to help secure the network. Wireless networks are known to be difficult to protect because the use of radio waves, which can be easily intercepted. It is also difficult to find hardware and software that can be used to improve the security in wireless networks. The security products used for wireless networks are more expensive than products used for wired networks.

Two county councils do not use specific program to help them analyze the audit trails and the third have developed their own program for this. The county councils may divide their audit trails even more since it is uninteresting and time demanding to go through a very large file. If the audit trails are divided, it is easier to discover anomalies and deal with them before incidents occurs in the network. Checking audit trails are a part of testing networks to gain knowledge about the traffic the network generates.

The IT-departments at the county councils have difficulties with the end-users, because the end-users do not understand the importance of security. It should be the IT-department's responsibility to inform the end-users about the security aspects that are of importance. This should be specified in the security policy that the end-users must have access to. The persons who are responsible for the different systems within the network are supposed to be stated in the security policy. If end-users have problems they should know whom to contact for assistance.
It is positive that the responsible managers at each county council are able to receive education in the security field. It may be good if the end-users also could receive some kind of education in the same field.

The end-users are free to choose which password they want and are recommended to change the passwords frequently, except at county council C. There are the end-users forced to change passwords after every 90 days. Since the end-users are not forced to choose passwords that consist of upper cases, lower cases, numbers and special signs, it is more likely that the end-users chooses a password like the dog's name or child's name. The passwords should be randomly generated and consist of different characters, which makes it more difficult to crack. Thus, the end-users have several passwords for different systems and the use of a randomly generated password for each system may be a problem for the end-users. They can easily forget the passwords and keep notes to remember them. If an unauthorized user gain access to an end-user's workstation, it is possible to find a note with the passwords around the workstation, i.e. on the computer screen or under the keyboard.

The county councils seemed to be aware of tools that can be used for attacking a wireless network. Though the county councils have not attempted to use these by themselves, but seem to have a clear view of how for example WEPCrack and war drive work. It may be good to test attack tools like WEPCrack and Netstumbler[2] to gain more knowledge about how these works. The reason for this is that it is important to be aware of the tools that are used by attackers to prevent incidents from occurring.

No protection is used against interference by the county councils. At the moment, the county councils only use the wireless network at certain places within the organization. When one of the county councils has problems with interference signals, they install new access points to solve the problem with interference. However, it is not for sure that a new access point will solve the problem, since building material and furnishing can cause the problems. To prevent from interference the organization can plan and test the surrounding area before implementing new access points.

From the summary of the result of the questionnaire we could see that the average value for the county councils differed. County council B had the highest average value, but they did not answer to all the 18 questions and they answered with either a 1 or a 5 for the questions. This increased their average value compared to county council A that had more scattered answers. The reason for the low average value for county council C is that they did not have a security policy, which meant that they had to answer the questions about security policies with ones.
The reason for the high standard deviation value for county council B is the same as mentioned for the average value.
County council C has a higher standard deviation value than county council A, because county council A's answer was more scattered than county council C.

We believe that the county councils do their best with the resources they possess, but of course one can always try harder.

[2] Netstumbler.com, http://www.netstumbler.com/, May 20, 2003

5.3.1 What else could we have done?

We contacted five different county councils in Sweden, but only three agreed to take part in our thesis. Out of the two county councils that did not agree, one county council was not using the wireless networks and the other one did not even reply to our request. The persons who were responsible for the security aspect were elected by us to be interviewed. The reason for e-mailing the questionnaire before the interviews were that the county councils wanted to prepare their answers. This may be a confounding factor, but in this case it is not. The county councils did receive the questionnaire before the interviews, but did hardly look at the questions, since they had to think about what to say during the interviews. We could have done interviews with other staff at the IT-departments, but also with the end-users of the systems. If we had done it with the end-users, our hypothesis may have been verified. We decided to interview the ones that were responsible, because they possessed information we required for this thesis.
The IT-departments at the county councils felt that they had problems with the end-users, because the end-users do not understand the importance of security.
The persons at the IT-departments told us that the end-users have several passwords for different systems and are unwilling to change their passwords frequently, if they are not forced to do that.
The used methods for the case study were chosen, because they were the most suitable. We wanted to perform the interviews in person, to be able to give an impression that we were honest and interested in their work. Other methods that we could have used would be a survey that was e-mailed or mailed out to all the county councils in Sweden, but since we decided to perform the interviews in person, we had to consider the geographic position of each county council.

6 Conclusion

The stated hypothesis that was evaluated in this thesis has been found falsified.
The county councils had a higher level of knowledge than presumed before the case study was performed. Since they had a higher level of understanding about security, wired and wireless networks. The county councils are aware of the problems involved with the use of wireless networks, which indicates that the county councils possess medium level of knowledge.
It is possible to generalize this to other county councils in Sweden, because they manage more or less the same sensitive information and the use of wireless networks are quite new to the county councils. This may also be applied to other authorities, but the information may not be the same as for the county councils.
The level of knowledge about security is probably the same for other county councils as it were for the three county councils that were examined in the case study. The ability to apply the knowledge about security in wireless networks may differ.

The risks that come with the use of wireless networks are at the moment very large. Major security threats related to wireless networks are [6]:

- Someone can explore access points within reach of the network's radio signal, to perform intrusion, virus and other types of attacks.
- When access points are deployed behind the organizations firewalls inside the networks, this makes the access points more attractive for attacks.
- Wireless networks are tremendously vulnerable to denial-of-service attacks and interruption attempts.
- Employees working at organizations can easily set up a wireless network to be able to communicate with people outside the organization.

For example, hackers and criminals can take advantage of the wireless network if no encryption is used, to find information about customers, patients, celebrities, et cetera. The information for beneficial use is gathering to perform attacks on computer systems, burglary and black mailing.
Wireless network technologies, bring new ways to break into networks, even Pentagon in the United States of America has decided to forbid the connections of wireless devices within classified networks. The Defense Department has released an established policy with definitions and responsibilities. The reason for this is to eliminate the vulnerabilities connected to wireless networks. The policy states that wireless network technologies may enable remote eavesdropping and unauthorized access into Pentagon's systems.[18]
Charles Hudson said about wireless network access; "It´s like having LAN jacks for your intranet on the sidewalk"[22].

6.1 Future research

Security in wireless networks is a large area; this thesis only examines a minor part. It concentrates on the level of knowledge that the interviewed county councils in Sweden possess. The stated hypothesis in this thesis could be changed and result in a completely new thesis. The new hypothesis will concentrate on the application level of security instead of the level of knowledge; "The application level of security in wireless networks among county councils in Sweden is low."

6.2 Recommendations

The board of the organization needs to understand why security is important. The board has the main responsible to facilitate the information security within the organization.

The organizations should form a security team that is responsible for the information security. The security team should be separated from the operation team and the budgets for each team as well. Managers working with operations should not be a part of the security team, because their main priority is to maintain the network and not the security issues. The use of wireless networks is at the moment full of risks. Organizations using this kind of networks believe that their networks are more secure than they actually are. Organizations that use the IEEE 802.11 standard encryption technique WEP should reconsider their decisions. The security increases particularly when implementing a VPN-solution.

7 Bibliography

Literature

A. Dawson, C.W, "The essence of computing projects, a students guide", Prentice Hall, 2000, Great Britain.
B. Mitrovic, P, "Handbok i IT-säkerhet" Pagina Förlags AB, Göteborg, Sweden, 2001
C. Olsson, F, "Trådlösa nätverk – WLAN i praktiken", Pagina Förlags AB 2002
D. Pfleeger, C P, "Security in computing", 2nd ed, Prentice Hall, New Jersey, USA, 2000
E. SIG Security 2001, "Säkerhet vid trådlös datakommunikation", Studentlitteratur, Lund, Sweden, 2001
F. Stallings, W, "Network and internetwork security principles and practice", Prentice Hall, New Jersey, USA, 1995
G. Stallings, W, "Network security essentials – applications and standards" Prentice Hall, New Jersey, USA, 2000
H. Stallings, W, "Local and Metropolitan Networks", 6th ed, Prentice Hall, New Jersey, USA, 2000
I. Wadlow, T A, "The process of network security – Designing and managing a safe network", Addison-Wesley, Reading, Massachusetts, USA, 2000

Internet

1. 802.11 Planet, 802.11 WEP: Concepts and Vulnerability, http://www.80211-planet.com/tutorials/article.php/1368661, May 6, 2003
2. Arbaugh, W.A, University of Maryland, Your 802.11 Wireless Network has no Clothes, http://www.cs.umd.edu/~waa/wireless.pdf , May 7, 2003
3. Computer Networking, VPN Tutorial, An introduction to VPN software, hardware and protocol solutions, http://compnetworking.about.com/library/weekly/aa010701a.htm, May 7, 2003
4. Computer Networking, VPN, http://compnetworking.about.com/library/glossary/bldef-vpn.htm, May 6, 2003
5. Computer Sweden, Säkerhet äter upp IT-budgeten, http://computersweden.idg.se/ArticlePages/200212/17/20021217165438_CS258/20021217165438_CS258.dbp.asp, May 8, 2003
6. Computerworld, How to build a secure WLAN, http://www.computerworld.com/mobiletopics/mobile/story/0,10801,78275,00.html, May 30, 2003
7. Datainspektionen, Personal Data Act, http://www.datainspektionen.se/PDF-filer/ovrigt/pul-eng.pdf, May 7, 2003
8. Datainspektionen, Personal Data Protection – Information on the personal data act, http://www.datainspektionen.se/PDF-filer/smaskrifter/ju-puleng.pdf, May 7, 2003
9. Information security policy world, ISO 17799 Description, http://www.information-security-policies-and-standards.com/iso17799desc.htm, May 7, 2003
10. Information security policy world, The benefits of: Security Risk Analysis http://www.information-security-policies-and-standards.com/benefits.htm, May 6, 2003

11. Information security policy world, The contents of ISO 17799, http://www.information-security-policies-and-standards.com/iso17799what.htm, May 7, 2003
12. Intel White Paper, Wireless Security and VPN: Why VPN is Essential for Protecting Today´s 802.11 Networks, http://www.intel.com/ebusiness/pdf/prod/related_mobile/wp0230011.pdf, May 6, 2003
13. Internet Security, Applications, Authentication and Cryptography (ISAAC), Intercepting Mobile Communications: The insecurity of 802.11, http://www.isaac.cs.berkeley.edu/isaac/wep-draft.pdf, May 6, 2003
14. Internet Security, Applications, Authentication and Cryptography (ISAAC), Security of the WEP algorithm, http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html, May 7, 2003
15. Johnson, H, Nilsson, A, Fiedler, M, Wireless network security http://www.bth.se/fou/Forskinfo.nsf/Sok/5405E61B05AB3566C1256C6F00408F59!OpenDocument, May 8, 2003
16. Krigsberedskapsmyndigheten, Välkommen till IT-säkerhetsguide FA22, http://www.krisberedskapsmyndigheten.se/verksamhet/information/fa22/intro.html, May 6, 2003
17. Network World Fusion, What's wrong with WEP?, http://www.nwfusion.com/research/2002/0909wepprimer.html, May 7, 2003
18. NetworkWorldFusion, Pentagon prohibits wireless, citing security reasons, http://www.nwfusion.com/news/2002/0927pgon.html, May 30, 2003
19. Research Methods Knowledge Based, Likert Scaling, http://trochim.human.cornell.edu/kb/scallik.htm, May 8, 2003
20. RSA Security, What is RC4, http://www.rsasecurity.com/rsalabs/faq/3-6-3.html, May 7, 2003
21. SANS Institute, Wired Equivalent Privacy Vulnerability, http://www.sans.org/rr/wireless/equiv.php, May 7, 2003
22. SearchSecurity.com, Company tackles wireless network security risks http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci863699,00.html, May 30, 2003
23. SearchSecurity.com, Wardriving, http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci812927,00.html, May 6, 2003
24. SourceForge Net, WEPCrack, an 802.11 key breaker, http://wepcrack.sourceforge.net/, May 7, 2003
25. The security risk analysis directory, Introduction to Risk Analysis, http://www.security-risk-analysis.com/introduction.htm, May 7, 2003
26. The Unofficial 802.11 Security Web Page, Weaknesses in the Key Scheduling Algorithm of RC4, http://www.drizzle.com/~aboba/IEEE/rc4_ksaproc.pdf, May 7, 2003

Other references

i. Andersson, Kenneth, IT-avdelningen, Centralsjukhuset i Kristianstad, interview, March 19, 2003
ii. Dorch, Stephen, Kommunikationsansvarig, IT-strategiska enheten, Kalmar, interview, March 27, 2003
iii. Jakobsson, Mats, Dataingenjör, Landstinget i Blekinge, interview, March 20, 2003
iv. Dicksson, Gunilla, Personuppgiftsombud, Landstinget i Kalmar, E-mail, April 24, 2003
v. Isacchi, Gianfranco, kanslichef/förvaltningsjurist, Centralsjukhuset i Kristianstad, E-mail, May 6, 2003

8 Appendix A – Glossary

The definitions, which are not defined in the thesis, are collected from the web page, http://whatis.techtarget.com/.

- **3DES -** triple DES, the sane function as DES, but applies three keys in succession.
- **Brute force attack -** is a trial and error method used by application programs to decode encrypted data, through exhaustive effort (using brute force) rather than employing intellectual strategies.
- **DES -** Data Encryption Standard is a widely used method of data encryption using a private (secret) key. The sender and the receiver must know and use the same private key.
- **HMAC -** MAC that uses a hash function to reduce the size of the data it processes
- **IPSec -** Internet Protocol Security is a framework for a set of protocols for security at the network or packet- processing layer of network communication.
- **L2TP -** Layer Two Tunneling Protocol uses an Internet service provider (ISP) to enable the operation of a virtual private network (VPN) over the Internet.
- **MD-5 -** is an algorithm that is used to verify data integrity through the creation of a 128-bit message digest from data input (which may be a message of any length).
- **Perl –** is a script programming language that is similar in syntax to the C language.
- **PPTP -** Point-to-Point Tunneling Protocol is a protocol (set of communication rules) that allows corporations to extend their own corporate network through private "tunnels" over the public Internet.
- **RADIUS -** Remote Authentication Dial-In User Service is a client/server protocol and software that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service.
- **RC4 -** a stream cipher designed by Rivest for RSA Data Security (now RSA Security). It is a variable key-size stream cipher with byte-oriented operations.

- **SHA-1**- is an algorithm for computing a 'condensed representation' of a message or a data file. The 'condensed representation' is of fixed length and is known as a 'message digest' or 'fingerprint'.

- **SOCKS** - is a protocol that a proxy server server can use to accept requests from client users in a company's network so that it can forward them across the Internet.

- **VPN** - a virtual private network is a way to use a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network.

- **War Drive** - is the act of locating and possibly exploiting connections to wireless networks.

- **WEP** - Wired Equivalent Privacy is a security protocol, specified in the IEEE Wireless Fidelity standard, 802.11b, that is designed to provide a wireless local area network with a level of security and privacy comparable to what is usually expected of a wired local area network.

- **WEPCrack** - is an open source tool for breaking the WEP protocol's secret keys. The tools capabilities are Perl based, and are composed of certain scripts

- **XOR** - a binary bitwise operator yielding the result one if the two values are different and zero otherwise. XOR is an abbreviation for exclusive-or.

9 Appendix B – Questionnaire

Questionnaire – Security in wireless networks

1 = Do not agree
2 = Do agree to some part
3 = Do almost agree
4 = Agree
5 = Agree completely

1. Have you followed any guidelines or standards when developing your security policy?

1 **2** **3** **4** **5**

2. Did you follow the standard FA22 when you developed your security policy?

1 **2** **3** **4** **5**

3. Did you follow the standard ISO7799 when you developed your security policy?

1 **2** **3** **4** **5**

4. Do you apply your security policy?

1 **2** **3** **4** **5**

5. Is the security policy updated when changes occur in the network?

1 **2** **3** **4** **5**

6. Is it the same information that is being exchanged in both the wireless and the wired network?

1 **2** **3** **4** **5**

7. Are you dependent on your supplier for maintenance and installations?

1 **2** **3** **4** **5**

8. Does the responsible managers for IT-security have any kind of education in that area?

1 2 3 4 5

9. Are the audit trails checked frequently?

1 2 3 4 5

10. Do you use any kind of programs, for example “Log checker” for checking the audit trails?

1 2 3 4 5

11. Are the wireless network frequently tested to discover the security gaps by yourself?

1 2 3 4 5

12. Are firewalls and anti-virus protection being updated frequently?

1 2 3 4 5

13. Are the passwords being changed frequently?

1 2 3 4 5

14. Do the end users choose passwords by themselves?

1 2 3 4 5

15. Do you use any kind of protection to prevent interference in the wireless network?

1 2 3 4 5

16. Are you using any type of encryption technique?

1 2 3 4 5

17. Are you aware of what you can use the program “Wepcrack” to?

1 2 3 4 5

18. Are you aware of what “war drive” is?

1 2 3 4 5

Frågeformulär om säkerhet i trådlösa nätverk

1 = Instämmer inte alls
2 = Instämmer till en viss del
3 = Instämmer ganska väl
4 = Instämmer
5 = Instämmer helt och hållet

1. Har ni följt några riktlinjer eller standarder, då ni utvecklat er säkerhets policy?

1 **2** **3** **4** **5**

2. Följde ni standarden FA22 då ni utvecklade er säkerhetspolicy?

1 **2** **3** **4** **5**

3. Följde ni standarden ISO7799 då ni utvecklade er säkerhetspolicy?

1 **2** **3** **4** **5**

4. Tillämpar ni er policy?

1 **2** **3** **4** **5**

5. Uppdateras policyn då förändringar sker i nätverket?

1 **2** **3** **4** **5**

6. Är det samma information som skickas i både det trådlösa och det vanliga nätverket?

1 **2** **3** **4** **5**

7. Är ni beroende av er leverantör för underhåll och installationer?

1 **2** **3** **4** **5**

8. Har de som är ansvariga för säkerheten fått någon sorts utbildning inom området?

1 **2** **3** **4** **5**

9. Kontrolleras loggarna regelbundets?

1 2 3 4 5

10. Använder ni av något program för att kontrollera loggarna, till exempel Logchecker?

1 2 3 4 5

11. Testas det trådlösa nätet regelbundet för att ni själva ska kunna upptäcka säkerhetshålen?

1 2 3 4 5

12. Uppdateras brandväggar och anti-virus skydd regelbundet?

1 2 3 4 5

13. Byts lösenorden ut regelbundet?

1 2 3 4 5

14. Väljer användarna själva lösenord?

1 2 3 4 5

15. Använder ni något skydd för att förhindra störningar?

1 2 3 4 5

16. Använder ni någon typ av krypteringsteknik?

1 2 3 4 5

17. Är ni medvetna om vad man använder programmet ”Wepcrack” till?

1 2 3 4 5

18. Är ni medvetna om vad ”war drive” är?

1 2 3 4 5

10 Appendix C – Open Questions

Open questions

- Do you have different policies for the wired and the wireless network, if yes, what are the differences?
- Why is the same information transmitted over both the wired and the wireless networks?
- How do you perform the tests of the wireless network?
- What do the passwords consist of? Upper case and lower case capitals, special signs and or numbers?
- Have you had any problem with interference of the wireless network?
- How many percent of the IT budget are allocated to security?
- Are you using any kind of VPN solution?

Questions about Personal data act

- Have the county council permission to transmit personal data in the wireless network from the Data inspection board?
- What for tasks do a personal data representative have?
- What for tasks do a personal data controller have?
- Is the personal data protected enough according to the Personal data act, section 31?

Övriga frågor

- Har ni olika policys för trådlösa nätverk och andra nätverk, i så fall vad skiljer dem åt?

- Varför skickas samma information i både det trådlösa och det fasta nätverken?
- Varför/varför inte, motivera svaret?

- Hur utförs tester på det trådlösa nätverket?

- Vad består lösenord av? Gemener, versaler, siffror och eller special tecken?

- Har ni haft problem med störningar i det trådlösa nätverket?

- Hur många procent av IT-budgeten går till säkerhet?

- Har ni någon sorts VPN lösning?

Frågor om Personuppgiftslagen

- Har landstinget tillstånd från Datainspektionen att skicka personuppgifter i det trådlösa nätverket?

- Vad för arbetsuppgifter har en personuppgiftsansvarig?

- Vad för arbetsuppgifter har ett personombud?

- Anser ni att personuppgifterna skyddas tillräckligt med hänvisning till PUL §31?

11 Appendix D – Result of Questionnaire

The result of the questionnaire with county council A, B and C

1. Have you followed any guidelines or standards when developing your security policy?

A	**B**	**C**
5	2	1

2. Did you follow the standard FA22 when you developed your security policy?

A	**B**	**C**
2	?	1

3. Did you follow the standard ISO7799 when you developed your security policy?

A	**B**	**C**
2	?	1

4. Do you apply your security policy?

A	**B**	**C**
4	4	2

5. Is the security policy updated when changes occur in the network?

A	**B**	**C**
3	1	4

6. Is it the same information that is being exchanged in both the wireless and the wired network?

A	**B**	**C**
3	5	5

7. Are you dependent on your supplier for maintenance and installations?

A	**B**	**C**
1	1	1

8. Does the responsible managers for IT-security have any kind of education in that area?

A	**B**	**C**
2	5	4

9. Are the audit trails checked frequently?

A	**B**	**C**
4	5	1

10. Do you use any kind of programs, for example “Log checker” for checking the audit trails?

A	**B**	**C**
1	1	1

11. Are the wireless network frequently tested to discover the security gaps by yourself?

A	**B**	**C**
4	1	2

12. Are firewalls and anti-virus protection being updated frequently?

A	**B**	**C**
5	5	5

13. Are the passwords being changed frequently?

A	**B**	**C**
3	5	5

14. Do the end users choose passwords by themselves?

A	**B**	**C**
5	5	5

15. Do you use any kind of protection to prevent interference in the wireless network?

A	**B**	**C**
1	1	1

16. Are you using any type of encryption technique?

A	**B**	**C**
2	5	5

17. Are you aware of what you can use the program “WEPCrack” to?

A	**B**	**C**
4	5	3

18. Are you aware of what “war drive” is?

A	**B**	**C**
4	5	1