Secure Wireless Communication

ADMIR MUHOVIC

KTH Information and Communication Technology

Master of Science Thesis
Stockholm, Sweden 2007

COS/CCS 2007-09

Secure Wireless Communication

Admir Muhovic

Master of Science Thesis
1 March 2007

Royal Institute of Technology (KTH)
Department of Communication Systems
Stockholm, Sweden

Supervisor at KTH: Professor Gerald Q. Maguire Jr.
Supervisor at FMV: David Olgart, CISSP, Principal Information Assurance Officer

Abstract

The need for and requests for utilization of wireless equipment are growing rapidly. Advantages of using wireless communication are easy to realize. Having access to electronically stored information no matter where you are is a big advantage. Furthermore, wireless communication is increasingly utilized in everyday work and there is a constant development of new wireless equipment. Today, utilization of wireless communication is very practical as well as effective.

On the other hand, using wireless equipment and communication entails risk unless efforts are made to secure this communication. Some wireless protocols exist and are used, despite their being vulnerable to attacks. Additionally, the traffic can easily be eavesdropped. Incorrect installation of wireless equipment contributes to the vulnerabilities of wireless communication.

Some of the IT-equipment available on the market today offers wireless communication. This equipment is increasingly used within FMV. Such equipment includes: laptops, PDAs, cellular phones, etc. This wireless equipment, according to FMV's information security policy, must be approved from a security viewpoint before it can be used at FMV. Thus an analysis of risks associated with usage of wireless equipment must take place and the mechanisms necessary to ensure adequate security must be identified. The document "Requirements on Security Functions (Kraven på SäkerhetsFunktioner, KSF)" identifies the technical and/or administrative requirements for such equipment.

The aim of this thesis was to analyze if it is possible to utilize wireless equipment at FMV, specifically, if it can be connected to the internal LAN at FMV. In other words, the wireless equipment must be able to offer security protection corresponding to the information security class: HEMLIG/RESTRICTED.

The thesis contains an analysis of which security functions are available on the market today and evaluates whether these security functions meet the requirements given in KSF. The result is a proposal for the best security mechanism(s) within the constraints of KSF and the available equipment. The thesis proposes a technical solution along with suitable security mechanisms. The advantages and drawbacks of each has been analyzed. Additionally, the thesis presents a number of (administrative) security policies in order to be able to handle security aspects which are not covered by the KSF.

Sammanfattning

Behoven och efterfrågan av mobil och trådlös utrustning är i dagsläget allt större. Fördelarna med att använda sig av trådlös kommunikation är enkla att inse. Att kunna ha tillgång till elektroniskt lagrad information oavsett var man än befinner sig är en stor fördel. Vidare implementeras trådlös kommunikation allt mer i det vardagliga arbetet samtidigt som utrustning för denna sorts kommunikation är i ständig utveckling. I slutändan är användandet av trådlös kommunikation väldigt praktiskt samtidigt som det är effektivt.

Användandet av trådlös utrustning och kommunikation medför ett risktagande då denna typ av kommunikation allmänt är osäker. Detta eftersom teknologin fortfarande är i utvecklingsfasen. De i dagsläget aktuella trådlösa protokollen är sårbara för attacker och det är dessutom enkelt att avlyssna trafiken. Felaktig installation av utrustning bidrar dessutom också till att den trådlösa kommunikationen blir sårbar.

En del av den IT-utrustning som idag finns tillgänglig ute på marknaden och som alltmer används inom FMV har möjlighet att kommunicera trådlöst med omgivningen. Exempel på sådan utrustning är bärbara datorer, PDA:er, mobiltelefoner mm. Denna typ av utrustning, dvs. trådlös utrustning, skall enligt FMVs informationssäkerhetspolicy godkännas från säkerhetssynpunkt innan den får tas i bruk på FMV. Det innebär att man utför en analys av vilka risker som är förknippade med användandet av trådlös utrustning samt att man identifierar adekvata skyddsåtgärder. Till sin hjälp använder man sig av Kraven på SäkerhetsFunktioner (KSF) som består av tekniska och/eller administrativa krav.

Syftet med detta examensarbete var att undersöka om det finns möjlighet att använda trådlös utrustning på FMV, dvs. att denna används på interna LAN på FMV. Med andra ord skall den trådlösa utrustningen kunna erbjuda ett skydd motsvarande högst informationssäkerhetsklassen HEMLIG/RESTRICTED (H/R).

Examensarbetet innefattar en analys av vilka säkerhetsfunktioner idag finns tillgängliga ute på marknaden och utvärderar huruvida dessa säkerhetsfunktioner uppfyller kraven givna i Kraven på SäkerhetsFunktioner (KSF). Resultatet är ett förslag på de bästa säkerhetsmekanismerna inom restriktionerna av KSF och den tillgängliga utrustningen. Examensarbetet föreslår en teknisk lösning med lämpliga säkerhetsmekanismer. Dess för- och nackdelar har analyserats. Examensarbetet presenterar dessutom ett antal (administrativa) säkerhets policies som hanterar säkerhetsaspekter som inte omhändertas av KSF.

Acknowledgements

I would like to thank and express my most sincere gratitude to my supervisor at KTH, Professor Gerald Q. Maguire Jr., for his time, his advices, and his support during this thesis project.

I am very grateful to my supervisor at FMV, David Olgart, for his guidance, his encouragement throughout this thesis project and his support. Further, I would like to thank Jasmir Beciragic and Robert Wiksten for their advice, their ideas, and their support.

I would also like to thank FMV for giving me the opportunity to do this thesis project.

Special thanks go to my family for believing in me, for their unconditional support throughout this thesis project, and for their encouragement.

Finally, I would like to thank my girlfriend and my friends for supporting and encouraging me through the difficult moments.

Table of contents

1. Introduction

1.1 General overview

As networks expand beyond wires and fibers, developers and administrators are trying to control network usage and maintain data privacy. Users like use wireless LANs (WLANs) because this offers them the ability to access resources attached to their local area networks (LANs) and Internet without being restricted to a particular place. Because of the simplicity and low cost for installation and maintenance of a WLAN, administrators are also interested in deploying WLANs. WLAN is a rapidly growing technology, not only within academic and business settings, but increasingly for private users in their homes. Today's WLAN products are no longer simply implemented zx PC-cards to be used in mobile computers and personal digital assistants (PDAs), but due to decreased costs of WLAN interfaces they are being incorporated directly into such devices. Utilization of wireless communication brings benefits such as efficiency, increased accuracy, and lower business costs. This has resulted in a growing market for WLANs which in turn has resulted in a growing need for security for such WLANs.

In addition to the advantages of WLANs, as with every other technology - this too has its drawbacks. Enterprises will have to invest in purchasing and deploying wireless access points and equipping users with wireless network cards, even though they already have working network interface cards for the wired LAN, or replacing their equipment with equipment which has built in WLAN capability. Additionally, there are also concerns about the fact that radio waves are not constrained within a given physical space and that this may increase the risk of eavesdropping. However, in actuality use of radio simply makes the possibility of eavesdropping more apparent; as eavesdropping of signals on cables and fibers is also technically feasible.

Since the introduction of the wireless telephones, there have been security issues. For example, for analog cellular telephony it was relatively easy to listen to someone's telephone conversation. This was especially an issue for large companies where vital internal data concerning thousands of people and millions of dollars could be stolen or used against the company. Some of the protocols for wireless communication available today are not satisfactory from a security point of view, since they have been proven to be vulnerable to attacks. However, there do exist protocols which can be used to provide authentication, authorization, accounting, and privacy for wireless communications; these will be described later. Another important factor concerning securing wireless communication is the fact that the wireless equipment must be properly installed and maintained, otherwise it will contribute to vulnerabilities in the wireless communication; these issues will be addressed in chapter 3.

Since usage of WLANs is growing, the security issues must be clearly addressed otherwise there is a risk that the use of WLAN never reaches its full potential. Increasing use of WLANs for transmission and management of confidential information about companies and private citizens are reasons to emphasize the use of suitable security.

As all wireless equipment to be utilized at FMV, must first be approved from a security point of view according to FMVs information security policy and an analysis of the usage of wireless equipment has to be done. This analysis will consider the document "Requirements on Security Functions" [13], which states the technical and/or administrative requirements.

1.2 Problem statement

The aim of this thesis is to investigate if wireless equipment can be used in the internal LAN at FMV, where it must be able to offer security protection corresponding to the information security class HEMLIG/RESTRICTED.

This thesis project will consist of following steps:

- Market research – Analysis of which security functions exist in the market today. The goal is to find a number of security functions which met FMVs' KSF in order to be able to propose the best security mechanism(s).

- Information security classes – FMV has several different information security classes, but this thesis will only consider the information security class HEMLIG/RESTRICTED. There are several security functions required for HEMLIG/RESTRICTED information, these are:

    - Access control/User authorization control
    - Security logging
    - Protection against interception/unauthorized disclosure
    - Intrusion protection
    - Protection against malicious code

- Proposal of a technical solution, alternatively presentation of several available security mechanisms which completely or partly fulfill KSF. A presentation of their advantages and disadvantages will be included.

- Policy – In order to regulate wireless communication with, for example help of rules and procedures, KSF is an important tool. A complement to KSF could be to formulate policies to handle security aspects which are not covered by the KSF. This thesis presents a number of such administrative rules and procedures.

2. Security functions

The security functions are designed to work as an entirety in order to protect an IT-system against any identified threat. Security functions could be considered as “the characteristics of an IT-system”. In other words, the IT-system can not be secured by utilization of only one security function.

By means of different security mechanisms, the security functions of an IT-system can be realized. No one-to-one mapping between a security function and a security mechanism exists [13]. A security mechanism can be used by several security functions, while a security function can be realized by one or more security mechanisms. Furthermore, a combination of physical, administrative, organizational, and technical measures can be used in order to achieve the approved security functionality [13]. Another important issue is the fact that the security mechanisms which realize different security functions have to be integrated so together that they can protect the information handled in the IT-system.

2.1 Description of security functions

As mentioned earlier, FMV has defined several information security classes. The information security class HEMLIG/RESTRICTED (which is the only security class considered in this thesis) requires the following security functions [13]:

- Access control/User authorization control
- Security logging
- Protection against interception
- Intrusion protection
- Protection against malicious code

2.1.1 Access control/User authorization control

“Access control/User authorization control” is used to identify and authenticate a user as well as to enable access for authorized users only to specific parts of the IT-system. The security function itself can be implemented by the means of different policies or a combination of these.

In this case, a role-based authorization policy (other alternatives could be organizational or individual based) can be used. Role-based authorization policy means that an organizations different roles in the IT-system can be used to allot authorizations to specific users [13]. These roles, which are often hierarchical, can be based on different work related functions of the users activity or of the IT-system.

The advantage of role-based authorization policy is that it is relatively simple to administer and there is the possibility to allot authorization for roles instead of individuals. The role-based authorization policy can also be used to implement relatively advanced systems, including dynamic roles.

One of the drawbacks with role-based authorization policy is that the information in the system should belong to the same information security class. The problem is that this kind of

policy actually does not support multiple-level systems, such as for processes. Two different scenarios, read-up and write-down, can occur [13]:

- Read-up occurs when, since processes usually are not allotted any role, a process reads information from an object which has higher information classification than the authorization for the role that the users of this process has.
- Write-down occurs when a processes transmits information objects to a lower information classification.

Therefore, if role-based authorization policy is to be used for multiple-level systems, the subjects have to be defined in terms of roles and then the access rights that these subjects must have should be defined.

2.1.2 Security logging

The aim of security logging as a security function is that afterwards one can trace events which are important from a security point of view. Events which are critical can be placed on a level with security relevant or security critical events. It should also be noticed that the security function security logging handles all kind of events which are of importance for the security in IT-systems, thus it also handles events that can come up in other security functions in the IT-system.

A security log is useful when [13]:

- An analysis can be carried out based on the security log.
- It contains a certain amount of data which is of interest for the person that carries out the analysis.
- It is known what security measures the security log takes automatically if certain conditions are fulfilled.
- It is obvious how the security log shall be protected.

The difference between an analysis and a review is that an analysis is used to describe a repetitive deterministic method while a review depends upon individuals ability to read, study, and draw conclusions from what can be discerned from a security log.

2.1.3 Protection against interception

Protection against interception will actually not be included in this thesis since the Swedish Armed Forces have special requirements on this security function (included from information security class HEMLIG/CONFIDENTIAL). However, a brief presentation of this security function is given below.

The aim of communication is to transmit information in a secure manner from one physical or logical place to another. This can be realized, depending on the conditions, by means of [13]:

- Unencrypted connection, for instance the transmission of secret information from one IT-system to another, e.g. from a computer to a printer.
- Optical fiber cable, for instance could carry transmissions between buildings within an enclosed and guarded area, between such areas, or to a building outside such an

area. This can be realized when an optical fiber cable is used for transmission and the cable is provided with an approved alarm.

- Pair shielded terminal cable, can for example be used for connections within the building, within an enclosed and guarded area. However, the terminal cable has to be approved and used in such a way that it can be inspected through its whole length within a sectioned area. A sectioned area refers to an area within a building which is marked off by a specific entry-pass system and where only authorized staff has access.
- Shielded terminal cable, for example within a sectioned area, where all staff members have same authorization to secret information.

2.1.4 Intrusion protection

Intrusion protection is aimed to, in a controllable way, grant access to different services in the IT-system. This should be realized both from the inside and the outside of the protected IT-system. Control is accomplished by allowing, denying, and/or conducting the information flow through the intrusion protection.

Intrusion protection can in principle be implemented in two different ways. However, there is a difference in principle between their implementations [13]:

1. Incoming and outgoing information flow passes through some kind of a filter which, based on the rules, decides if the information shall pass through the filter or not. The intrusion protection can vary in strength depending on how the filter is implemented.
2. Using encryption which, through the decryption of the incoming information flow, can decide whether the decryption is correct or not and thus allow the correct information to pass into the IT-system. The outgoing information flow is encrypted in a similar way such that in order to be able to study the information, the receiving party has to have access to the correct key.

It should be noted that both of these methods can be used in cooperation in order to strengthen the intrusion protection.

2.1.5 Protection against malicious code

The aim of protection against malicious code as a security function is to protect the IT-system against executable code which could be harmful to the IT-systems' resources. In other words, this security function should protect against code which can expose, change, or destroy the information, files, and programs within the IT-system.

Protection against malicious code can be implemented in different ways. The most common protection is to use software for detecting malicious code by means of so-called antivirus software [13]. However, that is not the only solution. Another type of protection which can be implemented in IT-systems is to use integrity checks for subjects and objects as well as to use configuration control of the software. An alternative to utilization of antivirus software is to only allow software that is trustworthy, i.e. the software where the source is well-known and evaluated, or to only allow digitally signed software ("white listing"). The later solution generates additional demands, since it has to know what subjects and objects the activity needs and thus what access shall be allowed. Another demand is that the signing party has to be trusted.

3. Wireless communication standards

The first WLAN standard, often referred to as 802.11, was created by the Institute of Electrical and Electronics Engineers (IEEE) in 1997. The aim was to create a standardized approach for wireless communication in businesses, homes, and public areas [3]. Another important issue was the need to address the interoperability between wireless products in order to ensure that the growth of WLAN will be supported by consumers and vendors. The 802.11 standard addresses performance and security concerns, as well as outlines available technologies to be used for transmission of wireless communication. Technologies used for transmission are for instance Direct Sequence Spread Spectrum (DSSS) and Frequency Hopping Spread Spectrum (FHSS).

Because of the growing popularity of wireless communication, the IEEE has developed a series of substandards of 802.11 with different specification for bandwidth, frequency, and transmission technologies in order to improve the performance of WLANs [3]. The most common 802.11 standards will be discussed in following subsections. A summary of these standards is given in table 1.

3.1 802.11b standard

The most common standard within the family of 802.11 standards is 802.11b [3]. It is commonly referred to as Wireless Fidelity or Wi-Fi. The 802.11b standard specifies a data rate of up to 11 Mbps in the 2.4-GHz ISM (Industrial, Scientific, and Medical) frequency band. It applies DSSS as the technology for transmission. 802.11b-based networking products are tested by the Wi-Fi Alliance which is a non-profit organization. The products are tested for proper interoperability and functionality, then a Wi-Fi certification is awarded to products that pass those tests.

3.2 802.11a standard

802.11a standard specifies a data rate of up to 54 Mbps in the 5-GHz UNII (Unlicensed National Information Infrastructure) frequency band. Furthermore, the transmission technology applied, unlike 802.11b standard, is Orthogonal Frequency Division Multiplexing (OFDM). The reason behind the choice of OFDM as transmission technology is primarily because it uses spectrum more efficiently [3]. The substantial increase in bandwidth has contributed to a growing interest, especially over the last several years, in the 802.11a standard. However, there is an incompatibility between 802.11a and 802.11b standards due to their use of different frequency bands, which forces customers to further invest in order to take advantage of 802.11a products, even though they already have invested in 802.11b WLANs.

3.3 802.11g standard

In June 2003, the IEEE approved a new WLAN standard – 802.11g. It runs in the 2.4-GHz ISM frequency band, specifies a data rate of up to 54 Mbps, and applies OFDM as the transmission technology. 802.11g is backward-compatible with 802.11b which facilitates the growth of WLAN by enabling 802.11b users to speedup their WLANs [3].

Table 1. IEEE 802.11 WLAN standards [4].

Standard	Spectrum	Maximum physical rate	Layer 3 data rate	Transmission	Compatible with	Major disadvantage	Major advantage(s)
802.11	2.4 GHz	2 Mbps	1.2 Mbps	FHSS/DSSS	None	Limited bit rate	Higher range
802.11a	5.0 GHz	54 Mbps	32 Mbps	OFDM	None	Smallest range of all 802.11 standards	Higher bit rate in less-crowded spectrum
802.11b	2.4 GHz	11 Mbps	6-7 Mbps	DSSS	802.11	Bit rate too low for many emerging application	Widely deployed: higher range
802.11g	2.4 GHz	54 Mbps	32 Mbps	OFDM	802.11/ 802.11b Due to narrow spectrum	Limited number of colocated WLANs Higher range than 802.11a	Higher bit rate in 2.4-GHz spectrum

3.4 802.1x standard

IEEE developed and approved a new standard for network access security – 802.1x. This new standard provides port-based network access control. 802.1x was initially designed for wired communications, however, it was later adopted for wireless communication. Mutual authentication, between a network controller and its client, is provided by the 802.1x standard. Rogue access points, which are an issue for organizations and their WLANs, are well addressed by this standard. In other words, users will not authenticate to simply any wireless access point (AP), but will only authenticate to the actual LAN which they wish to access. This authentication occurs through an authentication database, such as RADIUS (Remote Authentication Dial-In User Service). This RADIUS server is placed behind the AP [3].

3.5 802.11i standard

IEEE 802.11i, released in June 2004, is considered to be of great importance for all future WLAN standards. The security of 802.11 WLANs is enhanced via the 802.11i standard by addressing issues pertaining to both Media Access Control (MAC) and physical layers of wireless networks [3]. The Extensible Authentication Protocol (EAP) and 802.1x are the foundation authentication mechanisms within 802.11i. This will allow vendors to design different types of the authentication credentials for WLANs. Furthermore, for data confidentiality, Counter-Mode/CBC-MAC Protocol (CCMP) is applied. 802.11i uses Wired Equivalent Privacy (WEP) protocol for its encryption services, but another encryption mechanism can be applied, i.e., Advanced Encryption Standards (AESs). The main benefit is that AES is compatible with the WEP protocol's RC4 algorithm. In order to improve the security of the keys used in WEP, a Temporal Key Integrity Protocol (TKIP) is used.

3.6 Proprietary standards

Beside the IEEE, many vendors are trying to develop and implement proprietary WLAN security standards in order to force their way into the market. For instance, the Wi-Fi Alliance in cooperation with the IEEE developed a new industry security standard – Wi-Fi Protected Access (WPA), which was presented in the beginning of 2003. WPA was created in order to replace the WEP protocol, enabling more secure and interoperable services – which would be able to use the existing hardware in the field.

3.6.1 Wi-Fi Protected Access (WPA)

Wi-Fi's Protected Access (WPA) [17] is a specification of standards-based, interoperable security mechanisms that provides better data protection and access control for current and future WLANs [15]. WPA was developed by the Wi-Fi Alliance [16] in cooperation with IEEE. It is derived from IEEE's 802.11i standard, and the two standards are forward-compatible. Since WEP proved to be vulnerable to attacks, WPA was developed using a strong encryption technology – TKIP with Message Integrity Check (MIC). Technologies such as EAP, IEEE 802.1x, or Pre-Shared Key (PSK) are used in order to provide **mutual** authentication.

There are two modes of certificates provided by WPA, where each offers encryption and authentication. These are [15]:

- WPA Personal mode
- WPA Enterprise mode

However, this thesis will focus on the WPA Enterprise mode. It should also be noted that the Wi-Fi Alliance introduced a second generation of WPA: Wi-Fi Protected Access 2 (WPA2) [17]. It is based on the IEEE 802.11i standard (and as with WPA), it provides both personal and enterprise modes. For data encryption the AES standard is used.

Table 2 presents details of both WPA and WPA2 with respect to personal and enterprise modes:

Table 2. WPA and WPA2 modes [17]. Here PSK means Private Shared Key.

	WPA	**WPA2**
Enterprise Mode (Business and Government)	Authentication: IEEE 802.1x/EAP Encryption: TKIP/MIC	Authentication: IEEE 802.1x/EAP Encryption: AES-CCMP
Personal Mode (SOHO/personal)	Authentication: PSK Encryption: TKIP/MIC	Authentication: PSK Encryption: AES-CCMP

WPA Enterprise mode

The WPA enterprise mode, as well as the WPA2 enterprise mode, consists of six mandatory components. They are [15]:

- Client supplicant
- Authenticator
- Authentication server

- EAP types
- Wi-Fi Protected Area Information Element (WPA IE)
- Operational framework

Client supplicant

An IEEE 802.1x supplicant executes on the client. A supplicant is actually a piece of software that is installed on the client to implement the IEEE 802.1x protocol framework and one or more EAP methods. Supplicants may be included in the client operating system, integrated into drivers, or installed as third-party standalone software.

Authenticator

The authenticator authenticates the supplicant to the authentication server. Authentication is enforced by the authenticator within IEEE 802.1x protocol. The authenticator can either authenticate the supplicant and the authentication server itself; or just forward the authentication traffic between the supplicant and the authentication server. In the later case, an Access Point (AP) usually acts as the authenticator.

Authentication server

In order to provide mutual authentication in Wi-Fi networks, IEEE 802.1x authentication with EAP types is used within the WPA enterprise mode. In this way, only authorized users are granted access to the network and they can only access authorized subnets of the network. The authentication server is actually a database where the list of names and credentials of authorized users against which the authentication server verifies user authenticity is stored; usually RADIUS servers are used. Furthermore, user credentials may be stored in an external database, such as SQL or LDAP, and can be accessed by the authentication server. However, the standards do not determine the configuration; which implies that it can be implementation specific.

EAP types

The Extensible Authentication Protocol (EAP) types offer several options which can be used with different authentication mechanisms, operating systems, and back-end databases. Different types of user logins, credentials, and databases used in the authentication are provided by these EAP types. Possible EAP types are: EAP-MD5, EAP-Cisco Wireless (LEAP), EAP-TLS, EAP-TTLS, and PEAP. Each will be described in this thesis.

Wi-Fi Protected Area Information Element (WPA IE)

Using beacon, probe response, and (re)association frames, the parameters between an AP and station (STA) are negotiated within a WPA enabled WLAN. WPA Information Element, containing information about security features and cipher suites provided by the AP, is sent in the beacon and probe response frames by WPA enabled APs. By selecting the security features and cipher suites from this AP's WPA IE, the STA constructs its own WPA IE which is then sent in a (re)association frames. Thus, the negotiation of security parameters occurs during a 4-way handshake.

Operational framework

Within the WPA enterprise mode, mutual authentication is initiated by the user, i.e. when the user associates with an AP. The user is not granted access to the network and is blocked by the AP until the user gets authenticated. Credentials provided by the user are forwarded to the authentication server within the IEEE 802.1x/EAP framework. IEEE 802.1x/EAP creates a framework where a client workstations and the authentication server mutually authenticate each other via an AP. By means of mutual authentication, only authorized users are granted access to the network and this confirms that the client is authenticated only to an authorized server [15].

The client can join the network once the user's credentials are accepted by the authentication server. In this case, a Pairwise Master Key (PMK) is simultaneously generated by both the authentication server and the client. Afterwards, a 4-way handshake completes the authentication process between the AP and the client, and establishes and installs the TKIP encryption keys. The data exchanged between the client and the AP is now protected by the agreed encryption [15].

Key hierarchies

WPA enterprise mode applies a EAPoL-key exchange that uses several keys, as well as key hierarchy to split the initial key material into useful keys [15]. The key hierarchies applied are:

- Pairwise key hierarchy
- Group key hierarchy

The IEEE 802.1x has defined an RC4 EAPoL-key frame, but WPA has defined its own EAPoL-key exchanges that are based on the IEEE 802.11i standard. However, these EAPoL-key exchanges are specified as a 4-way handshake and the group key handshake within the IEEE 802.11i standard. The pairwise and group key hierarchies are shown in following figure.

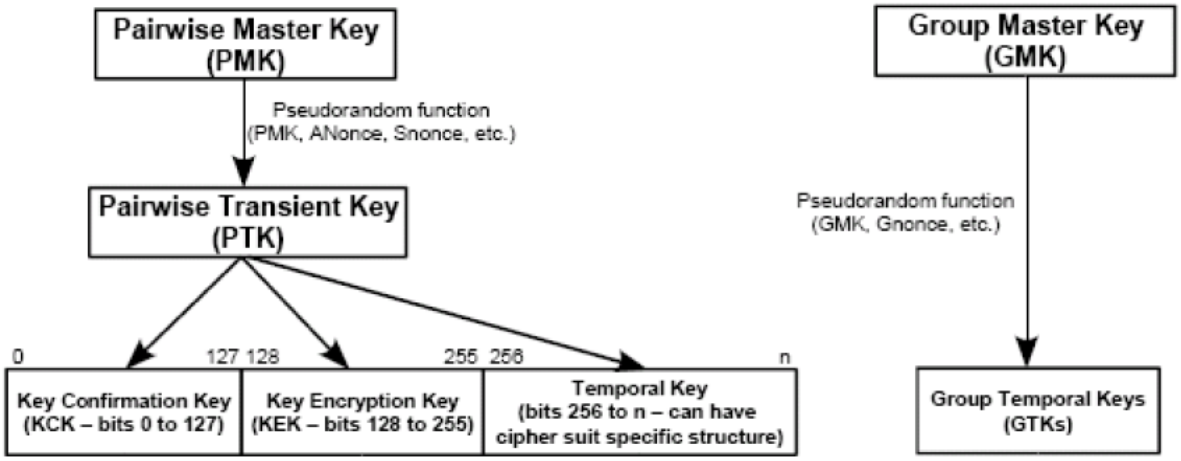

Figure 1. Pairwise Master Key (PMK) and Group Key hierarchy [15].

4. Virtual Private Network – VPN

Today, there is an increasing demand in widely distributed internetworking for connecting distant networks and users. One way to protect the information which is transmitted over unprotected networks, i.e. the Internet is by applying a technology called Virtual Private Network (VPN) [5]. A VPN allows users to establish a virtual private tunnel via the internal network and to access the internal resources through the Internet from home, hotels, and other external networks.

This section provides a general overview of VPNs as a basic technology. A discussion about the potential security risks that may be encountered and the security considerations that should be taken into account when implementing a virtual private network are also addressed.

4.1 What is a VPN?

A Virtual Private Network (VPN) is a private network which uses a public network to connect remote sites and users together [1]. Instead of using a dedicated connection, such as a leased line, a “virtual” connection is made between geographically separated users and networks over a shared or public network such as the Internet. The data is first encrypted and then transmitted just as if it was going through private connections.

The transmission of data in a VPN is done with help of so called “tunneling” [1]. This implies that a packet is encapsulated into a new packet, with a new header before the packet is transmitted. The new header “carries” routing information for it to traverse the shared or public network to reach its tunnel endpoint. The so called “tunnel” is the way the encapsulated packets travel through the shared or public network. The packet is decapsulated and forwarded to its final destination once it reaches the tunnel endpoint.

4.1.1 Usages of VPN

A Virtual Private Network (VPN) is usually used in the following scenarios:

Remote access VPN — It is a user-to-network connection for mobile users connecting to corporate private network from various dispersed locations. Such a VPN provides secure, encrypted connections between a corporate private network and remote users.

Intranet VPN — In this scenario a VPN is used to connect fixed locations, like for example branch offices. Such a LAN-to-LAN VPN connection unites multiple remote locations into a single private network.

Extranet VPN — This kind of VPN is used to connect business partners, such as suppliers or customers, it allows various parties to work on a shared environment.

WAN replacement — A VPN can be utilized as an alternative to a Wide Area Network (WAN). It offers greater scalability than traditional private network using leased lines and it generally requires less money and administration than a simple WAN.

4.1.2 Typical elements of a VPN connection

A VPN typically consists of following elements:

VPN server — VPN connections from VPN clients are accepted by a server. A VPN server provides either secure remote access or a gateway-to-gateway VPN connection.

VPN client — A VPN connection is initiated from a computer to a VPN server. A VPN client can either be a remote computer accessing a remote access VPN connection or a router obtaining a gateway-to-gateway VPN connection.

VPN tunnel — A VPN tunnel is a connection where data is encapsulated and encrypted.

Tunneling protocols — These protocols are used to manage tunnels and encapsulate data.

Tunneled data — It is the data that is encapsulated and encrypted, then sent across a link.

Transit networks — The transit network is a shared or public network, such as a private intranet or the Internet, where the encapsulated data passes through.

4.1.3 Types of VPN products

Different types of VPN products are:

Firewall-based VPNs — Such a VPN is equipped with both a firewall and VPN capabilities. In order to restrict the access to the internal network, it utilizes the security mechanism in the firewall. The features this type of VPN provides include address translation, user authentication, real-time alarms, and extensive logging.

Hardware-based VPNs — This type of VPN offers the highest network throughput, better performance, and reliability since there is no processor overhead.

Software-based VPNs — Such a VPN is used when VPN endpoints are not controlled by the same party and when different firewalls and routers are used. Additionally, hardware encryption accelerators can be used in order to enhance the performance.

4.1.4 Advantages of using VPN

Advantages provided by a VPN are:

- It extends the geographic connectivity.
- It improves the security for a remote user and their network connection.
- It reduces operational costs, compared with a traditional leased line WAN connection.
- It reduces installation time and transportation costs for remote users.

- It improves productivity since resources can be accessed from remote networks by users.

4.2 Secure Sockets Layer (SSL) VPN

A VPN based on so called Secure Sockets Layer (SSL), is becoming increasingly popular for remote access [14]. Secure Sockets Layer (SSL) is a protocol which is commonly used to enable encrypted and authenticated communication over the Internet. In order to enable remote users to have secure authorized access to legacy applications, web-based applications and client/server applications, an SSL VPN uses SSL and proxies. Thus, only authorized users are allowed access to corporate specific resources according to the corporate security policy.

Since SSL VPNs offers clientless access when SSL is supported by standard web browsers, its popularity for remote access and extranet VPN is growing. This implies that this kind of VPN can reduce the cost of implementation and operation. Of course, this may be limited by how well the application(s) function and how good the support is.

A Secure Sockets Layer (SSL) VPN is designed to give access to the applications themselves, but not to the network [1]. A SSL VPN application gateway is a single application layer gateway device that can support one or more of the following functions:

1. Allow clientless, browser-based access to a legacy application where the remote user is allowed to use their web browser to operate the legacy application as if the application was installed and running on the user's local machine.
2. Allow secure access to intranet web-based applications and portals using http reverse-proxy technology; where the remote user can access the back-end web server(s) securely.
3. Allow desktop access to local client/server applications such as email systems using SSL tunneling technology, where a SSL VPN adapter (which is a small program) is first downloaded and installed on a user's computer the first time the user logs into the client/server application, then the adapter negotiates with the client/server application to create a secure SSL tunnel via the user's web browser.

It should be mentioned that SSL VPNs are not designed to replace the conventional IPsec-based site-to-site VPNs. However, they are becoming popular because of the ease of deployment, clientless access, flexibility, and lower initial and ongoing administrative and operating costs. On the other hand, an SSL VPN may limit the user's remote access needs to only those applications that the corporation is currently using.

4.3 Common VPN tunneling technologies

Tunneling protocols are operated at either data-link layer (layer two) or network layer (layer three) of the Open System Interconnection (OSI) model. The most common tunneling protocols, each of which will be presented in next subsections, are:

- Internet Protocol Security (IPsec) [6]
- Point-to-Point Tunneling Protocol (PPTP) [12]
- Layer Two Tunneling Protocol (L2TP) [11]

4.3.1 Internet Protocol Security (IPsec)

The Internet Engineering Task Force (IETF) [7] developed Internet Protocol Security (IPsec) for secure transfer of information at the network layer across a public IP network, such as the Internet. Unlike the other two tunneling protocols, that are able to transmit non-IP traffic, IPsec is limited to sending only IP packets. However, it should be noted that most protocols can be tunneled in IP packets, these in turn can be protected using IPsec.

Using IPsec, a system can select and negotiate the required security protocols, algorithms, and secret keys to be used for the requested services. Basic authentication is provided by IPsec, as well as data integrity and encryption services. Two different security protocols are utilized in IPsec, the Authentication Header (AH) [9] and the Encapsulated Security Payload (ESP) [10].

Security protocols

As previously mentioned, IPsec utilizes two different security protocols, AH and ESP.

- Authentication Header (AH) protocol: The AH protocol provides integrity and source authentication, but not encryption. The Authentication Header (AH) is used to verify the sender, ensure data integrity, and prevent replay attack and is added to the packet by the sender.
- Encapsulated Security Payload (ESP) protocol: In addition to source authentication and integrity, ESP protocol also provides data confidentiality. It makes use of a symmetric encryption algorithm, such as 3DES, to provide data privacy.

Mode of operation

There are two modes of operation, supported by each security protocol [1]: tunnel mode and transport mode. In the first case the header and the data of each packet are encrypted, while in the second, only the data is encrypted.

1. Tunnel mode

An original IP packet, with original destination address, is inserted into a new IP packet, and AH and ESP are then applied to the new packet. The new IP header points to the end point of the tunnel. Finally, upon receipt of the packet, the tunnel end point decrypts the contents and the original packet is forwarded to the original destination in the target network.

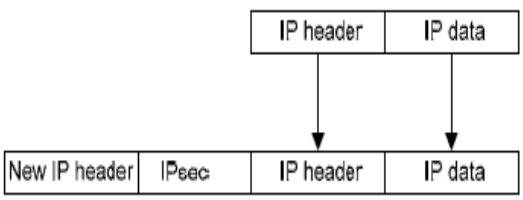

Figure 2. Tunnel mode [1].

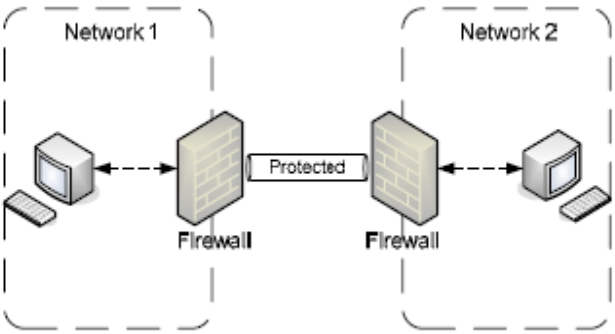

Figure 3. Tunnel mode communication [1].

2. Transport mode

In this scenario the Authentication Header (AH) and Encapsulated Security Payload (ESP) are applied to the data of the original IP packet. The data is authenticated, but the IP header is not. The overhead added in the case of transport mode is less than that in tunnel mode.

Transport mode is usually used in the case of end-to-end communication, while tunnel mode is used when the data is protected along only a part of the path.

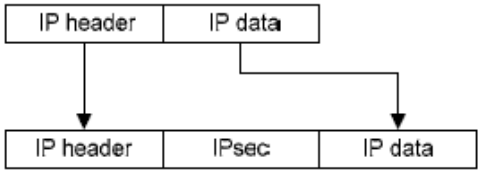

Figure 4. Transport mode [1].

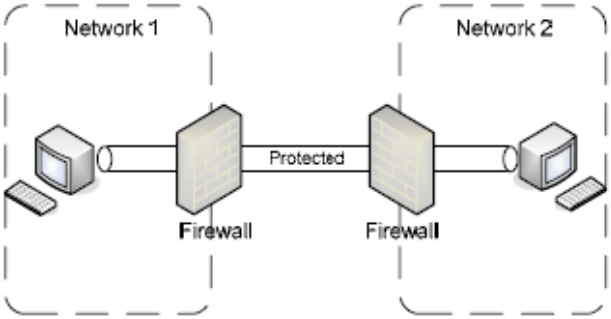

Figure 5. Transport mode communication [1].

Key exchange and management

The following sections will present two types of key management supported by IPsec: manual and automated key management.

1. Automated key management

Internet Protocol Security (IPsec) uses Internet Key Exchange (IKE) [8] as its default protocol in order to determine and negotiate protocols, algorithms, and keys, and to authenticate the two communicating parties. IKE is useful for scalable and widespread deployment of VPN implementations.

IKE supports the use of digital certificates. The user authenticates with their digital signature key and the other end point verifies this signature. By means of IKE, an authenticated, secure tunnel between two parties is created. IKE then negotiates the Security Association (SA) between them and exchanges the keys.

The negotiating parties use the Security Association (SA), which is a set of parameters, to define the services and mechanisms for protecting the (one-way) traffic. These parameters include location policy, algorithm identifiers, modes, secret keys, etc.

2. Manual key management

In manual key management, secret keys and SAs are manually configured at both communicating parties before a connection starts. Furthermore, the sender and the recipient are the only ones to know the secret key for the security services. Hence, the recipient will know that the communication came from the sender and that it was not modified if the authentication data is valid. This type of key management is easy to use in small and static environments. The keys should be distributed to the communicating entities securely

beforehand. If the keys are compromised, then others could act as the user and create a connection.

4.3.2 Point-to-Point Tunneling Protocol (PPTP)

Point-to-Point Tunneling Protocol (PPTP) [12] is an OSI layer two protocol developed by the PPTP forum which is a collaboration between Microsoft and some Internet Service Provider (ISP) equipment manufacturers.

This tunneling protocol is built upon the Point-to-Point Protocol (PPP), where PPP is a dial-up, multi-protocol used to connect to the Internet. By first dialing into the local ISP, remote users could access a private network via PPTP. PPTP connects to the target network by creating a virtual network for each remote client. A PPP session, with non-TCP/IP protocols (e.g. IP, IPX, or NetBEUI), is tunneled through an IP network using PPTP.

A PPTP-based VPN utilizes the same authentication mechanisms as PPP, such as Challenge-Handshake Authentication Protocol (CHAP) and Password Authentication Protocol (PAP).

In the Point-to-Point Tunneling Protocol (PPTP) data tunneling is performed through multiple levels of encapsulation. PPP frames are encapsulated, using a modified Generic Routing Encapsulation (GRE), then tunneled over an IP network, such as the Internet or a private intranet.

Generic Routing Encapsulation (GRE) provides a flow and congestion controlled encapsulated service for carrying PPP packets. Data of the encapsulated PPP frames can be encrypted and/or compressed. It results in, GRE and PPP-encapsulated source and destination IP addresses for the PPTP client and server. Upon receipt of the PPTP tunneled data, the PPTP server removes the IP, GRE, and PPP headers, decrypts and/or decompress the PPP data.

4.3.3 Layer Two Tunneling Protocol (L2TP)

The combination of the Point-to-Point Tunneling Protocol (PPTP) and the Cisco Layer Two Forwarding Protocol (L2F) resulted in the Layer Two Tunneling Protocol (L2TP) [11]. It is the product of a partnership between the members of the PPTP forum, Cisco, and the IETF.

The Layer Two Tunneling Protocol (L2TP) can be used as a tunneling protocol in order to encapsulate PPP frames to be sent over IP, X.25, Frame Relay, or ATM networks. It also allows multiple connections to be transmitted through one tunnel.

L2TP is an OSI layer two protocol. The data in PPP frames is encapsulated by layer two VPN protocols. These layer two protocols are capable of transmitting non-IP protocols over an IP network. The major difference from PPTP is that L2TP is IPsec compliant. As with PPTP, L2TP also uses Challenge-Handshake Authentication Protocol (CHAP) and Password Authentication Protocol (PAP) as authentication mechanisms. The security services are provided by IPsec's AH and ESP when L2TP is running over IPsec. All L2TP control and data appear as homogeneous IP data packets to the IPsec system.

L2TP tunneling is performed through multiple levels of encapsulation. The PPP data is encapsulated with a PPP header and a L2TP header. The encapsulated packet is further encapsulated with UDP header with the source and destination ports set to 1701. The packet is then again encapsulated with a final IP header containing the source and destination IP addresses of the VPN client and server.

4.4 VPN security

The underlying security mechanism of a VPN is encryption. The main goal of a VPN is to assure that the data which is transmitted over the network is protected and unauthorized access and modification prevented. A Virtual Private Network (VPN) utilizes tunneling to encapsulate the encrypted data into a secure tunnel, to cross over a public network. This ensures that the data can not be disclosed or changed during the transmission.

A data integrity check is also provided by the VPN. It is usually done by utilization of a message digest to ensure that the data was not manipulated during the transmission and thus the data received is identical to the data sent.

By default a VPN neither provides nor enforces strong user authentication. In some, the user can enter a simple username and password to enter into internal private network from home computer or other insecure networks. On the other hand, some VPN support add-on authentication mechanisms such as smart cards and tokens.

4.5 Security risks and limitations

The following subsections will concisely present different security risks and limitations when using VPN. These risks and limitations are:

- Hacker attack
- User authentication
- Client side risk
- Virus infection
- Incorrect network access rights
- Insecure network connection
- Interoperability

4.5.1 Hacker attack

The client machine may be the target of an attack or a staging point of an attack upon the network. Using hacker tools, viruses, and exploits, the hacker may discover vulnerabilities in the client machine and then launch attacks on this machine. Virus infections, man-in-the-middle attacks, and VPN hijackings are some of different types of attacks. Briefly the later two are [2]:

- Man-in-the-middle attacks affects the traffic sent between the communicating parties. They include interception, insertion, deletion, and modification of messages; reflecting messages back at the sender; replaying old messages; and redirecting messages.

- VPN hijacking is the unauthorized take over of an established VPN connection from the remote client, thus impersonating the client to the connecting network.

4.5.2 User authentication

As mentioned earlier, by default does VPN not provide or enforce strong user authentication, even though a VPN connection should only be created by authenticated parties. An unauthorized party may access the connected network and its resources if the authentication is not strong enough to restrict unauthorized access. Furthermore, there are some implementations that provide only limited methods of authentication. For instance, Password Authentication Protocol (PAP) that is used in PPTP transports the user name and password in clear text, thus a third party could capture this information and use it to subsequently get access.

4.5.3 Client side risk

Home users VPN client machines may be connected to the Internet via a broadband connection together with other traffic. The client machine may also be shared with other parties who have poor security awareness. Furthermore, the laptop of a mobile user may be connected to the Internet, wireless LAN, hotel, airport, or other foreign networks. However, the security protection at most of these places is insufficient. If the VPN client machine is compromised, either before or during the connection, it will pose a risk to the network.

4.5.4 Virus infection

The network will be affected if the other party is infected with a virus. For instance, there is a risk that if a client machine is infected with a virus that it could send the password for a VPN connection to the attacker [2]. While for an intranet or extranet VPN connection, if one network is infected with a virus, the virus may spread widely to other networks (if their anti-virus protection is ineffective).

4.5.5 Incorrect network access right

In this scenario, some clients may be granted greater access rights than needed.

4.5.6 Insecure network connection

There is a possibility by using a split tunneling that users could have a VPN connection to the private network while at the same time they could connect to the Internet or other insecure networks. This may constitute a risk to the private network.

4.5.7 Interoperability

Interoperability can also be a security concern. For example, IPsec compliant software from two different vendors may not always be able to work together, resulting in a denial of service.

4.6 Security considerations

A number of different security considerations when applying VPN technology will be addressed in this subsection, specifically [5]:

- VPN security considerations in general
- Extranet VPN security considerations
- Client side VPN security considerations
- Common security features of VPN products

4.6.1 VPN security considerations in general

- Using a firewall together with a VPN can strengthen security.
- In order to monitor attacks more effectively, an Intrusion Detection System (IDS) [18] may be used.
- Unsecured and unmanaged systems with simple or no authentication should not be allowed to make a VPN connection to an internal network.
- To prevent the spread of virus, anti-virus software should be installed in the connected networks and remote clients.
- Logging and auditing functions should be provided to record network connections, especially for unauthorized access attempts, and the log should be reviewed regularly.
- The network/security administrator and supporting staff as well as remote users should receive training in order to ensure that they follow the best security practices and follow the security policies during implementation and use of a VPN.
- Security policies and guidelines on the appropriate use of a VPN and network support should be distributed to responsible parties to govern their use of a VPN.
- The VPN entry point should be placed in a demilitarized zone (DMZ) in order to protect the internal network.

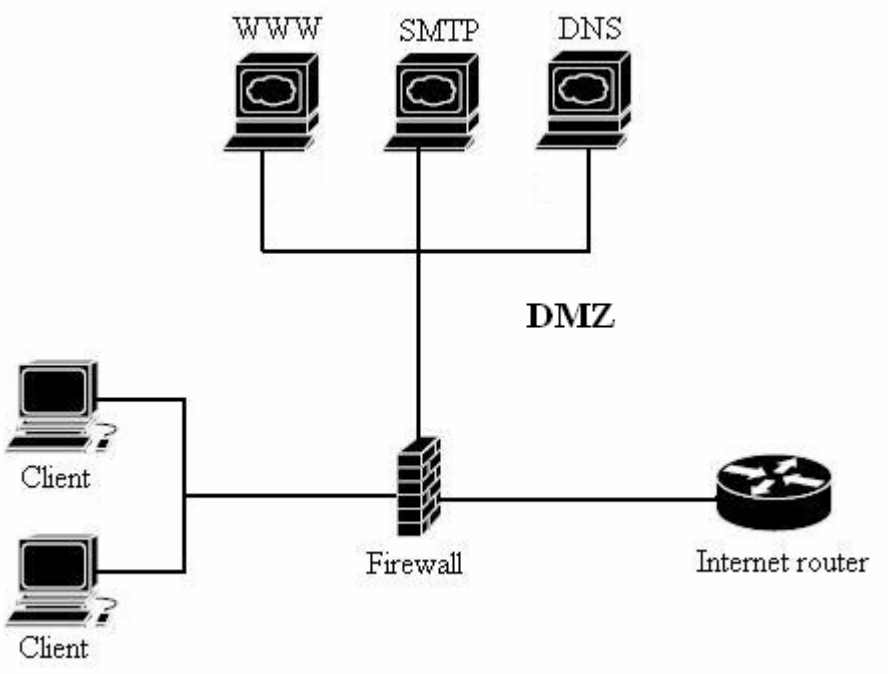

Figure 6. Demilitarized zone (DMZ) [19].

- It is preferable not to access the Internet or other insecure networks simultaneously during a VPN connection by the use of split tunneling. However, if split tunneling is to be used, a firewall and IDS should be used to detect and prevent attacks from other insecure networks.

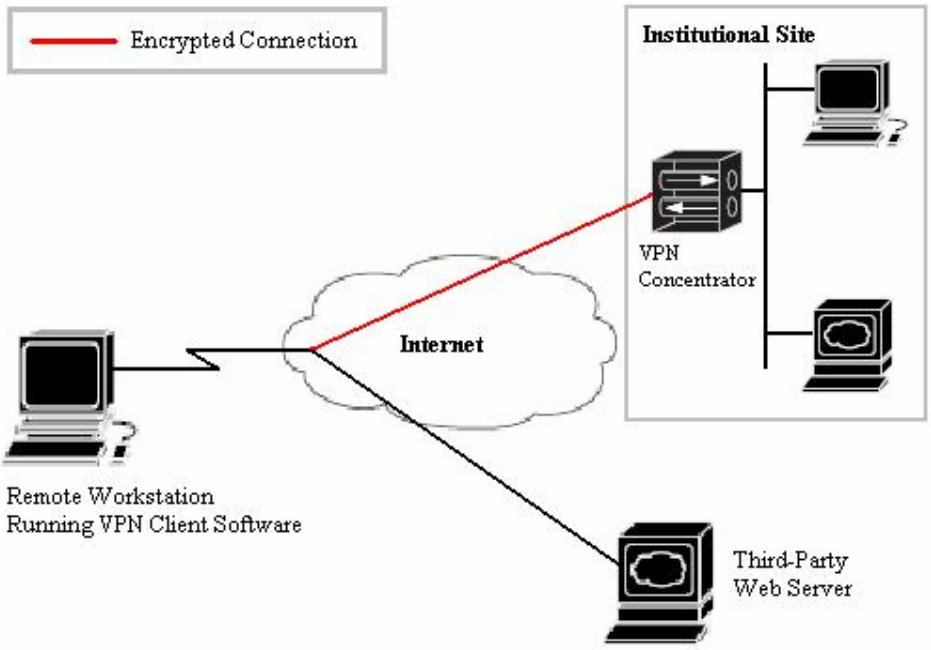

Figure 7. Split tunneling [20].

- There should be a restriction on unnecessary access to the internal network.

4.6.2 Extranet VPN security considerations

- Strong user authentication should be enforced.
- The VPN entry point should be placed inside a DMZ to prevent partners from accessing the internal network.
- Only the access rights necessary should be granted.

4.6.3 Client side VPN security considerations

- Strong authentication is a requirement when users connect dynamically from different untrusted networks, e.g. by means of certificates, smart cards, or tokens and add-on authentication systems such as RADIUS and TACACS+ [25].
- A personal firewall should be properly configured and installed on the client VPN machines in order to block unauthorized access to the client and to ensure that it is safe from attack. Personal firewall functions are included in many recent remote access VPN clients. Other configuration checks, e.g. the client cannot connect to the network if anti-virus software is not running or the signature is outdated, may also be included.
- The anti-virus protection software, with up-to-date signature, should be installed on the client machine to detect and prevent virus infections.
- The user should be aware of the physical security of the machine.
- Access from home should be taken equally seriously as access at work, and the users should be educated on safe Internet practices.

4.6.4 Common security features of VPN products

- Strong authentication support, e.g. smart card/token.
- Encryption algorithm with strong key strength support to protect the data during transmission. This algorithm should be industrially proven.
- Anti-virus support.
- Personal firewall support for each end user.
- Strong security default for maintenance ports.
- Intrusion Detection System (IDS).
- The use of digital certificates, e.g., using certificates for site-to-site authentication.
- Address management: assigning a client address on the private network and ensure that the private addresses are kept private.

4.7 Comparison of IPsec vs. SSL/TLS

The IPsec and SSL/TLS VPNs differ significantly in the following four areas [2]:

- Authentication and access control
- Defence against attack
- Remote computer security
- Cost of ownership

4.7.1 Authentication and access control

Concerning user identification, IPsec and SSL utilize different methods. As said earlier, IPsec uses Internet Key Exchange (IKE), where either digital certificates or pre-shared secrets for two-way authentication are used. However, if SSL technology is employed, the users are authenticated by means of digital certificates, irrespective of what method is used to authenticate the corresponding client.

Certificate-based user authentication is supported by both IPsec and SSL; where both technologies provide options through individual vendor extensions [2]. Despite these similarities, the two technologies differ mainly in how they implement these extensions. IPsec vendors offer options, such as eXtended Authentication (XAUTH). Before the tunnel set-up starts, eXtended Authentication (XAUTH) enables the gateway to prompt a client for further authentication, such as a SecurID code [2]. Most SSL vendors, support password and token-based authentication, such as via SMS messages. Finally, SSL is regarded as the more secure solution for organizations that decide to implement **certificate** user authentication [2].

IPsec and SSL differ in their access control and implementation. When per-application access control is required, SSL is considered the best option, whereas IPsec is preferable to give trusted user groups access to entire private servers and subnets. Selectors, i.e. packet filters that are used to permit, encrypt, or block traffic to individual destinations or applications, are supported by IPsec. For practical reasons, it is easier to grant hosts access to entire subnets instead of having to create or modify selectors for every IP address. On the other hand, SSL can utilize a filter, since the selectors operates at the session layer. SSL can use filters to decide if a user or group should have access to individual applications, embedded objects, selected URLs, application commands, or content in order to deliver more detailed and practical levels of control [2].

4.7.2 Defence against attack

Another important issue when protecting VPNs is their resistance to message replay and other attacks. Block encryption algorithms are supported by both IPsec and SSL. The utilization of IPsec offers greater flexibility even though SSL supports stream encryption which is often used for web browsing. The problem with SSL is that it only supports algorithms which are implemented in the standard web browsers while IPsec is designed such that new algorithms can easily be implemented afterwards.

Man-in-the-middle attacks pose one of the biggest security threats to VPNs [2]. By applying IPsec technology, this problem is easily overcome because packet modification is not allowed in IPsec. Another issue however comes up, since packet modification generates operational problems, mainly if Network Address Translation (NAT) is used [1]. Network Address Translation (NAT) is used to substitute public IP addresses for private addresses included in data packets, so IPsec and NAT do not work problem-free with each other. SSL, however, carries sequence numbers inside encrypted packets and in that way prevents packet injection, so the NAT problem is avoided if SSL technology is applied. Changes of IP addresses which may occur when a packet transits a firewall does not affect SSL because it creates session bindings above the IP layer. If HTTP/HTTPS is permitted, no changes of a firewall's rule-set are required by SSL since port 443 is already used there is no need for further ports to be opened [2].

By means of sequencing, message replay attacks are detected and these packets can be dropped. Both technologies, IPsec and SSL, utilize sequencing. However, in terms of effectiveness, IPsec should be used rather than SSL. Out-of-order packets are rejected lower in the stack when IPsec is used, whereas in the case of SSL, the TCP session engine or the SSL proxy engine first need to detect out-of-order packets before they can be rejected. This means that SSL consumes more resources.

4.7.3 Remote computer security

Irrespective of what VPN technology is applied, a VPN is only as secure as the remote computers connected to it [2]. Thus further security measures should be taken into consideration for organizations which utilize VPNs. These further security measures could be personal firewalls, malware scanning, intrusion prevention, OS authentication, and file encryption.

In order to utilize IPsec, a client has to be loaded onto the remote computer. This means that the number of remote computers which are able to connect to the network of that particular organization is limited. Furthermore, complementary security measures should be installed and managed by the organization since they usually own these computers. Pre-configuration of clients before they are installed is also possible, thus IPsec vendors can add extra security measures into the client software, which makes IPsec the safer solution when securing remote computers [2].

On the other hand, if an SSL VPN is used, organizations run a greater risk. That is because any computer potentially can get access to the network. However, to prevent this kind of scenario, sessions should start by downloading a Java Applet or ActiveX control [1]. By means of this Java Applet or ActiveX control, the remote computers are searched for

complementary security measures which makes it possible for corporations to make a decision about whether to allow this access. If loading of applets or ActiveX is not permitted by the browser, then a decision has to be taken by the corporation of whether to allow or deny access from that particular computer [2].

4.7.4 Cost of ownership

Another important factor, when considering VPN technologies, is the question of cost of ownership. Therefore, since there is no need to purchase and support a client, SSL technology is regarded as a cheaper alternative for implementation and management [2]. On the other hand, SSL technology usually requires that applications are web-enabled so they can be accessed from a SSL VPN. However, there is a possibility to build applications that are not web based, for example with OpenSSL. Thus the number of users and the applications supported will determine the cost of ownership.

5. Access control/User authorization control

Since WLAN provides physical access to a corporate network from outside of the building, there is also an ability to snoop on others' traffic. In order to prevent this becoming a security issue, access to intruders has to be denied. There are currently a number of different authentication techniques in use for identification and authentication of users; these are [24]:

- Open System Authentication
- SSID as Authentication
- Shared Key Authentication
- MAC Address Authentication
- 802.1x and Extensible Authentication Protocol (EAP)

5.1 Open system authentication

By applying Open System Authentication, which is a common default, one should be aware of the risks since it actually does not provide any security at all. This means that everyone can associate with the AP and access the network. This method is not recommended except in some cases where a second authentication system is used, for instance in public hot spots.

5.2 SSID as authentication

However, if SSID is used as the authentication technique, another issue comes up. The problem is that each WLAN Access Point's SSID is broadcasted in clear text by both the access point and the client, which means that it easily to obtain (by just snooping the traffic). The problem remains even if SSID beaconing by the AP is turned off.

5.3 Shared key authentication

When it comes to shared key authentication, shared keys are feeble due to possibility that the laptop can be stolen, the employee leaves his device after becoming logged in, etc. Furthermore, the transmission of the shared key is not properly secured by the IEEE 802.11 protocol. This implies that an attacker is able to determine the shared authentication key as well as the key used in the authentication process. The key that is used in the authentication process is also re-used as the WEP key, which compromises the authentication and also the subsequent encryption.

5.4 MAC address authentication

In order to prevent unauthorized access to the network, many developers have, in addition to WEP, used Access Control Lists (ACLs), which are based on the Medium Access Control (MAC) address of a WLAN interface. However, these MAC addresses can easily be obtained by snooping the traffic because they are sent in the clear. Once, the MAC address is obtained, the attacker is able to change his wireless interface's MAC address to match. Another drawback with MAC address authentication is that a network administrator has to manage hundreds of MAC addresses which cannot be considered as effective.

5.5 802.1x and Extensible Authentication Protocol (EAP)

The IEEE 802.1x is one of the latest approaches for authentication. As mentioned earlier, a RADIUS server is used for authentication with some form of credentials that are transferred using the EAP protocol. In this case, credentials could either be username/password or a security certificate.

EAP is an authentication framework mostly used in wireless networks and Point-to-Point connections. However, the EAP protocol is not limited to wireless LAN networks, as it can be used for wired LAN authentication as well.

As mentioned, EAP is an authentication framework and not a specific authentication mechanism. A number of common functions and a negotiation of desired authentication mechanism are provided by EAP. These mechanisms are referred to as EAP methods and the most common in use today are [24]:

- EAP-MD5
- EAP-Cisco Wireless (LEAP)
- EAP-Transport Layer Security (TLS)
- EAP-Tunnelled TLS (TTLS)
- EAP-Protected EAP (PEAP)

By invoking EAP via an IEEE 802.1x enabled Network Access Server (NAS) device, such as an IEEE 802.11 a/b/g Wireless Access Point (WAP), EAP methods can provide a secure authentication mechanism and negotiate a secure Pair-wise Master Key (PMK) between the client and NAS. Further, the PMK is then used for the wireless encryption session which applies TKIP or AES encryption.

5.5.1 EAP-MD5

To begin with, EAP-MD5 [29] is an open standard that supports username/password authentication, but does not provide key management or dynamic key generation which means that attackers can easily learn the WEP key. Furthermore, WAP authentication is not provided, allowing attackers to use rogue WAP in order to fool clients. Finally, one-way authentication is not secure enough.

5.5.2 EAP-Cisco Wireless (LEAP)

The Lightweight Extensible Authentication Protocol (LEAP) [30] is an EAP method developed by Cisco Systems. LEAP is actually not supported by any Windows operating system, however, it is supported by third party supplicants. Like EAP-MD5, vulnerabilities to dictionary attacks within LEAP have been known from the beginning. Cisco, however, maintains that LEAP can be secure if sufficiently complex passwords are used. The problem is that complex passwords are rarely used because of the difficulty they pose for average users. This problem is avoided if, for instance EAP-TTLS or PEAP are applied, because they create a secure TLS tunnel for user authentication session and they can operate on Cisco and non-Cisco Access Points (APs).

Session keys are dynamically generated by the LEAP. There is also a possibility to dynamically change keys every few minutes. In addition, two-way as well as username/password authentication are provided by the LEAP. However, LEAP uses MS-CHAPv1 authentication, which has potential weaknesses meaning that it can be compromised.

5.5.3 EAP-Transport Layer Security (TLS)

EAP-TLS [31] was developed by Microsoft as an open standard. It is also well-supported among wireless vendors. EAP-TLS provides good security because TLS is considered as the successor of the SSL standard. The credentials used by EAP-TLS are security certificates instead of username and password. It also applies two-way authentication as well as dynamic key generation. However, one of the drawbacks with EAP-TLS is that it requires a Public Key Infrastructure (PKI) for certificates. Thus, the easiest way to deploy EAP-TLS is MS clients using and logging into Active Directory.

EAP-TLS is the original standard WLAN EAP authentication protocol and is considered to be one of the most secure EAP standards available. The requirement for a client-side certificate gives EAP-TLS its authentication strength and illustrates the classic convenience vs. security tradeoff. Even though a password is compromised, that is not enough to break into EAP-TLS enabled systems, since the hacker still needs to have the client-side certificate. By situating the client-side certificates in smartcards, significant security is offered because there is no easy way to steal a certificate's private key from a smartcard without stealing the smartcard itself. There is also greater probability that physical theft of a smartcard would be immediately noticed, then the smartcard and certificate could be revoked, and a new card issued; this is compared to noticing that a password has been stolen, followed by changing the password or disabling the account.

5.5.4 EAP-Tunnelled TLS (TTLS)

EAP-TTLS [32] was developed by Funk Software in cooperation with Certicom. It supports mutual as well as username/password authentication where the AP uses certificates in order to authenticate to the client. Security provided by EAP-TTLS is considered as very good, when using PKI certificates only on the authentication server.

5.5.5 EAP-Protected EAP (PEAP)

PEAP [33] was proposed jointly by Cisco Systems, Microsoft, and RSA Security as an open standard. PEAP is a method to securely transmit authentication information, such as passwords, over wired or wireless networks. It uses only server-side public key certificates in order to authenticate clients by means of an encrypted SSL/TLS tunnel between the client and the authentication server. The encrypted tunnel protects the ensuing exchange of authentication information from casual inspection.

The following table summarizes the various EAP approaches.

Table 3. Variants of EAP and their details.

	MD5	Cisco (LEAP)	EAP-TLS	TTLS	PEAP
Mutual authentication?	No: user only	Yes	Yes	Yes	Yes
Overall security	Weak	Better than MD5, weaker than other EAP methods	Strongest	Strong	Strong
Client software	Windows XP	Cisco. Funk and Meetinghouse provide drivers for other NIC's.	Windows XP, 2000	?	Windows XP, 2000
Client-side PKI?	No	No	Yes	No	Yes

For implementation of 802.1x in an wireless deployment, mixing and matching of vendors' offerings, dependently on what EAP protocol is planed to be used, is necessary. A RADIUS server has to be picked in order to handle the credential verification. I present details of how two different RADIUS servers can handle some or all of the EAP methods. The two products which I have selected (as representative of similar products) are:

- Access Control Server (ACS) [25] from Cisco Systems was developed for UNIX as well as for Windows platforms. It is a full fledged TACACS+ and RADIUS server and for wireless authentication it supports both LEAP and EAP-TLS [26].
- Funk Software has developed a product called Steel Belted RADIUS (SBR) [27]. It handles wireless authentication exclusively. SBR supports almost all of the commonly used EAP protocols: EAP-MD5, EAP-TLS, LEAP, and EAP-TTLS [26].

It should be noted that following decisions regarding the two selected products and how they met the KSF requirements are not based on actual testing because of financial and time issues but rather on a publication of others and information [25] and [27] from respective vendor.

5.6 KSF – Access control/User authorization control

5.6.1 Evaluation in terms of the common KSF requirements

Protection of the security function

Table 4. KSF requirements.

Requirement description	ACS	SBR
	Fulfils KSF	
	Completely/Partly/Not at all	Completely/Partly/Not at all
Security function must together with other security functions in the IT-system enforce own security domain that protects against manipulation or interference both from subjects and users that belong respectively not belong to that domain.	Completely	Completely
Security function must together with other security functions in the IT-system have possibility to provide reliable time.	Completely	Completely
Security function must guarantee that only authorized administrator is able to administrate the security function and to manage its security settings.	Completely	Completely

Assurance requirements

Table 5. KSF requirements.

Requirement description	ACS	SBR
	Fulfils KSF	
	Completely/Partly/Not at all	Completely/Partly/Not at all
Security function must be tested in a structural approach.	Not at all	Not at all
All documentation regarding the security function must be marked with a unique reference.	Not at all	Not at all
There must be documentation that describes the results of the review carried out by an independent authority.	Not at all	Not at all
There must be documentation that in an informational way and a comprehensive level describes how the security function is edified. The documentation must contain a description of all hardware and software that is used to reach necessary security functionality.	Completely	Completely
There must be documentation that in an informational way describes how the functional security requirements are implemented in a security function.	Completely	Completely
There must be documentation that describes how the delivery and installation of a security function should be applied.	Partly, information about the delivery is missing	Not at all

Requirement description	ACS	SBR
	Fulfils KSF	
	Completely/Partly/Not at all	Completely/Partly/Not at all
There must be documentation that describes how an authorized administrator configures, administrates and manages the security function in a proper way in order to receive and retain a necessary security level.	Completely	Not at all
There must be documentation describing what tests with belonging results are carried out.	Not at all	Not at all

5.6.2 Evaluation in terms of the specific KSF requirements

Functional security requirements

Table 6. KSF requirements.

Requirement description	ACS	SBR
	Fulfils KSF	
	Completely/Partly/Not at all	Completely/Partly/Not at all
Security function must prevent access to the IT-systems subjects and objects from users and subjects that do not have authorization and access rights to the IT-system.	Completely	Completely
Security function must uniquely identify and authenticate a user before accessing some functionality or allotting access rights takes place in the IT-system that is protected by the security function.	Completely	Completely
Security function must authenticate a user at: • In signing. • Annulling of temporal access protection. • Change of security attribute for authentication. • When time for time limited usage of the IT-systems resources have passed.	Completely	Completely
Security function must guarantee certain quality for the security attribute, if it is a password, that is used for authentication by controlling that the security attribute is given: • A least validation time. • A least number of allowed symbols for creation of the security attribute. • A longest validation time used for the security attributes.	Completely	Completely
Security function must guarantee that all users can be individually responsible for their taken actions in the IT-system.	Completely	Completely
Security function must use user's, subject's and object's security attribute as control mechanism when steering the access.	Completely	Completely

Requirement description	ACS	SBR
	Fulfils KSF	
	Completely/Partly/Not at all	Completely/Partly/Not at all
Security function must use password or corresponding as control mechanism and security attribute for authentication.	Completely	Completely
Security function must be able to take automatic measures at authentication faults. Such measures must comprise denying of access to the IT-system as well as locking of the concerned users account for some period.	Partly, ability of locking an account is missing	Partly, ability of locking an account is missing
Security function must make use of different defined roles possible.	Completely	Completely
Security function must guarantee locking of such security attributes that could be revealed to users or subjects that does not have authorization and access rights to the IT-system. Locking can occur directly or at next in signing.	Not at all	Not at all

Administration of the security function

Table 7. KSF requirements.

Requirement description	ACS	SBR
	Fulfils KSF	
	Completely/Partly/Not at all	Completely/Partly/Not at all
There must be possibility of adding, removing or in another way changing what checks are performed in order to guarantee the quality of the security attribute.	Completely	Completely
There must be possibility of adding, removing or in another way changing what access rights authorized users have to the IT-systems subjects and objects. Such access rights must comprise: • Create • Read • Write • Execute • Remove	Completely	Partly, there is a possibility of adding, removing or changing what access rights authorized users have but there is no information whether mentioned attributes are supported
There must be possibility of adding, removing or in another way changing what actions must be taken at authentication faults.	Completely	Completely
There must be possibility of adding, removing or in another way changing at what occasions locking of such security attributes that are considered as revealed must take place.	Completely	Not at all

Assurance requirements

Table 8. KSF requirements.

Requirement description	ACS	SBR
	Fulfils KSF	
	Completely/Partly/Not at all	**Completely/Partly/Not at all**
There must be documentation that from a user's point of view describes how the security function works and that contains instructions and guidelines about how the security function is used in a secure manner.	Completely	Not at all
There must be documentation presenting test cases with belonging results that proves the functionality of the security function. The test cases must include both tests that checks the functionality of the security function and tests that checks absence of undesired behavior within the security function.	Not at all	Not at all

6. Security logging

As previously mentioned, having the possibility to afterwards trace events that are important for the security within an IT-system is useful. In order to do so, security logging is utilized. With security logging, processing, storing, and displaying of the security event data collected within the network(s) is possible and might be monitored in near real-time.

I selected two different management platforms that are commonly used to trace security event data, they are:

- Network Security Manager (NSM) v4.1 [21] from Intellitactics Incorporated. NSM stores and displays event data collected from third-party security devices, such as firewalls, routers, and Intrusion Detection System (IDS) sensors that are deployed within the monitored network(s).
- NetDetector/NetVCR [21] from NIKSUN Incorporated. NetDetector/NetVCR appliance provides the capability to record and analyze traffic streams to detect and report on anomalous activities. Furthermore, data captured by the appliance is analyzed to inspect traffic flows for improper activities, detect intruders, and send alerts.

It should be noted that following decisions regarding the two selected management platforms and how they met the KSF requirements are not based on actual testing because of financial and time issues but rather on a publication of others and information [21] presented by an independent party that performed tests on these products.

6.1 KSF – Security logging

6.1.1 Evaluation in terms of the common KSF requirements

Protection of the security function

Table 9. KSF requirements.

Requirement description	NSM	NetDetector/NetVCR
	Fulfils KSF	
	Completely/Partly/Not at all	Completely/Partly/Not at all
Security function must together with other security functions in the IT-system enforce own security domain that protects against manipulation or interference both from subjects and users that belong respectively not belong to that domain.	Completely	Completely
Security function must together with other security functions in the IT-system have possibility to provide reliable time.	Completely	Completely
Security function must guarantee that only authorized administrator is able to administrate the security function and to manage its security settings.	Completely	Completely

Assurance requirements

Table 10. KSF requirements.

Requirement description	NSM	NetDetector/NetVCR
	Fulfils KSF	
	Completely/Partly/Not at all	Completely/Partly/Not at all
Security function must be tested in a structural approach.	Completely	Completely
All documentation regarding the security function must be marked with a unique reference.	Completely	Completely
There must be documentation that describes the results of the review carried out by an independent authority.	Completely	Completely
There must be documentation that in an informational way and a comprehensive level describes how the security function is edified. The documentation must contain a description of all hardware and software that is used to reach necessary security functionality.	Completely	Completely
There must be documentation that in an informational way describes how the functional security requirements are implemented in a security function.	Completely	Completely
There must be documentation that describes how the delivery and installation of a security function should be applied.	Completely	Completely
There must be documentation that describes how an authorized administrator configures, administrates and manages the security function in a proper way in order to receive and retain a necessary security level.	Completely	Completely
There must be documentation describing what tests with belonging results are carried out.	Completely	Completely

6.1.2 Evaluation in terms of the specific KSF requirements

Functional security requirements

Table 11. KSF requirements.

Requirement description	NSM	NetDetector/NetVCR
	Fulfils KSF	
	Completely/Partly/Not at all	Completely/Partly/Not at all
Security function must in a security log register such events that are important for the security in the IT-system.	Completely	Completely
Security function must together with every individually registered event, also register date and time for the event as well as the users or the subjects' identity.	Completely	Completely
Security function must guarantee that tracing of abuse and attempts of abuse of the IT-system can be carried out.	Completely	Completely
Security function must guarantee that all registered events in the security log can be presented in a readable form.	Completely	Completely
Security function must make use of tool-based check of registered events in the security log possible.	Completely	Completely
Security function must make secure copying of the security log possible.	Not at all	Not at all
Security function must guarantee that registered events are not erased, over-writed or in another way destroyed as a result of an error in the security function or because the security log is full.	Completely	Completely

Administration of the security function

Table 12. KSF requirements.

Requirement description	NSM	NetDetector/NetVCR
	Fulfils KSF	
	Completely/Partly/Not at all	Completely/Partly/Not at all
There must be possibility of adding, removing or in another way changing which security relevant events will be registered in the security log.	Completely	Completely

7. Intrusion protection

Intrusion protection can be implemented in two different ways: by the use of a filter (firewall) or by the use of encryption. Further, both of these methods can be used together in order to provide even stronger protection. However, the KSF only specifies intrusion protection by the use of a filter.

Therefore, a presentation of two different (representative) filters (firewalls) follows next:

- Cisco Secure PIX Firewall V6.2(2) [21] from Cisco Systems. Cisco Secure PIX Firewall V6.2(2) is a packet filtering firewall that controls the flow of the IP traffic by matching the information contained in the headers of connection-oriented or connectionless IP packets against a set of rules specified by the firewall's authorized user.
- Check Point VPN-1/FireWall-1 NGX [21] from Check Point Software Technologies. The Check Point VPN-1/FireWall-1 is a network boundary protection device that provides controlled connectivity between two or more network environments. It provides information flow controls, including traffic filtering, application-level proxies, and intrusion detection and prevention capabilities.

It should be noted that following decisions regarding the two selected filters (firewalls) and how they met the KSF requirements are not based on actual testing because of financial and time issues but rather on a publication of others and information [21] presented by an independent party that performed tests on these products.

7.1 KSF – Intrusion protection

7.1.1 Evaluation in terms of the common KSF requirements

Protection of the security function

Table 13. KSF requirements.

Requirement description	PIX Firewall	NGX Firewall
	Fulfils KSF	
	Completely/Partly/Not at all	Completely/Partly/Not at all
Security function must together with other security functions in the IT-system enforce own security domain that protects against manipulation or interference both from subjects and users that belong respectively not belong to that domain.	Completely	Completely
Security function must together with other security functions in the IT-system have possibility to provide reliable time.	Completely	Completely
Security function must guarantee that only authorized administrator is able to administrate the security function and to manage its security settings.	Completely	Completely

Assurance requirements

Table 14. KSF requirements.

Requirement description	PIX Firewall	NGX Firewall
	Fulfils KSF	
	Completely/Partly/Not at all	Completely/Partly/Not at all
Security function must be tested in a structural approach.	Completely	Completely
All documentation regarding the security function must be marked with a unique reference.	Completely	Completely
There must be documentation that describes the results of the review carried out by an independent authority.	Completely	Completely
There must be documentation that in an informational way and a comprehensive level describes how the security function is edified. The documentation must contain a description of all hardware and software that is used to reach necessary security functionality.	Completely	Completely
There must be documentation that in an informational way describes how the functional security requirements are implemented in a security function.	Completely	Completely
There must be documentation that describes how the delivery and installation of a security function should be applied.	Completely	Completely
There must be documentation that describes how an authorized administrator configures, administrates and manages the security function in a proper way in order to receive and retain a necessary security level.	Completely	Completely
There must be documentation describing what tests with belonging results are carried out.	Completely	Completely

7.1.2 Evaluation in terms of the specific KSF requirements

Functional security requirements

Table 15. KSF requirements.

Requirement description	PIX Firewall	NGX Firewall
	Fulfils KSF	
	Completely/Partly/Not at all	Completely/Partly/Not at all
Security function must deny all access to the IT-systems subjects and objects from subjects that do not have access rights to the IT-system.	Completely	Completely
Security function must restrict what kind of information can be transmitted through the security function by controlling both incoming and outgoing information flow.	Completely	Completely
Security function must guarantee that information is not transmitted without usage of the security functions configurated filter.	Completely	Completely
Security function must make use of configuration possible so information only can flow in one direction through the security function.	Completely	Completely
Security function must guarantee that information belonging to the information security class RESTRICTED is not transmitted to other IT-systems than to such that can handle information according to information security class RESTRICTED or higher.	Completely	Completely
Security function must prevent that unidentified subjects can use, affect or in another way manipulate the security function.	Completely	Completely
Security function must guarantee that network traffic which is not allowed to be transmitted through the security function is not transmitted.	Completely	Completely
Security function must restrict the information that a user or a subject receives as a response at the denial of access to the security function.	Completely	Completely

Protection of the security function

Table 16. KSF requirements.

Requirement description	PIX Firewall	NGX Firewall
	Fulfils KSF	
	Completely/Partly/Not at all	**Completely/Partly/Not at all**
Security function must through self tests carry out correctness controls: • At start. • When an authorized administrator requires it. • At return to its ordinary operation from a secure state in order to demonstrate a correct functionality of the underlying solution.	Not at all	Completely
Security function must be able to maintain a defined secure state when whole or parts of the functionality that restricts what information that can be transmitted through the security function, is corrupt or inaccessible.	Not at all	Completely

Administration of the security function

Table 17. KSF requirements.

Requirement description	PIX Firewall	NGX Firewall
	Fulfils KSF	
	Completely/Partly/Not at all	**Completely/Partly/Not at all**
There must be possibility of adding, removing or in another way changing which configurated filters that the security function is using.	Completely	Completely
There must be possibility of adding, removing or in another way changing a filters configuration so a security function only allows the information to flow in one direction.	Completely	Completely
There must be possibility of adding, removing or in another way changing what type of network traffic is allowed to be transmitted through the security function as well as what type of network traffic is to be prevented.	Completely	Completely

8. Protection against malicious code

In order to protect the IT-systems resources against malicious code, several security measures can be taken. The most common way to protect an IT-system against code that can expose, change, or destroy the information within the IT-system is to use antivirus software.

Here we examine two (representative) antivirus programs from different vendors, which will later be matched against the KSF, these are:

- Symantec AntiVirus Corporate Edition [22] that combines industry-leading, real-time malware protection for enterprise workstations as well as network servers with graphical web-based reporting and centralized management and administration capabilities.
- McAfee Active Virus Defense [23] that protects against today's constantly evolving security threats, covering desktop, Internet gateway, e-mail servers, and file servers with antivirus protection.

It should be noted that following decisions regarding the two selected antivirus programs and how they met the KSF requirements are not based on actual testing because of financial and time issues but rather on a publication of others and information [22] and [23] from respective vendor.

8.1 KSF – Protection against malicious code

8.1.1 Evaluation in terms of the common KSF requirements

Protection of the security function

Table 18. KSF requirements.

Requirement description	Symantec	McAfee
	Fulfils KSF	
	Completely/Partly/Not at all	Completely/Partly/Not at all
Security function must together with other security functions in the IT-system enforce own security domain that protects against manipulation or interference both from subjects and users that belong respectively not belong to that domain.	Completely	Completely
Security function must together with other security functions in the IT-system have possibility to provide reliable time.	Completely	Completely
Security function must guarantee that only authorized administrator is able to administrate the security function and to manage its security settings.	Completely	Completely

Assurance requirements

Table 19. KSF requirements.

Requirement description	Symantec	McAfee
	Fulfils KSF	
	Completely/Partly/Not at all	Completely/Partly/Not at all
Security function must be tested in a structural approach.	Not at all	Not at all
All documentation regarding the security function must be marked with a unique reference.	Not at all	Not at all
There must be documentation that describes the results of the review carried out by an independent authority.	Not at all	Not at all
There must be documentation that in an informational way and a comprehensive level describes how the security function is edified. The documentation must contain a description of all hardware and software that is used to reach necessary security functionality.	Completely	Completely
There must be documentation that in an informational way describes how the functional security requirements are implemented in a security function.	Completely	Completely
There must be documentation that describes how the delivery and installation of a security function should be applied.	Partly, information about the delivery is missing	Not at all
There must be documentation that describes how an authorized administrator configures, administrates and manages the security function in a proper way in order to receive and retain a necessary security level.	Completely	Not at all
There must be documentation describing what tests with belonging results are carried out.	Not at all	Not at all

8.1.2 Evaluation in terms of the specific KSF requirements

Functional security requirements

Table 20. KSF requirements.

Requirement description	Symantec	McAfee
	Fulfils KSF	
	Completely/Partly/Not at all	Completely/Partly/Not at all
Security function must prevent all access to the IT-systems resources by objects containing malicious code.	Completely	Completely
Security function must, with means of control mechanism, guarantee that no malicious code can: • Change, • Destroy, • In another way manipulate objects in the IT-system that is protected by the security function.	Completely	Completely
Security function must guarantee detection of malicious code by controlling both the incoming and outgoing information flow.	Completely	Completely
Security function must guarantee that information is not transmitted to or from the IT-system without usage of the security functions control mechanism.	Completely	Completely
Security function must, if detection of malicious code occurs, be able to automatically take measures. Such measures must include placement of infected subject or object in the quarantine and warn an authorized administrator and the concerned user.	Completely	Completely
Security function must use definition file as control mechanism for objects in the IT-system that are protected by the security function.	Completely	Completely
Security function must carry out inspections of subjects and objects: • During operation. • At start. • When an authorized administrator requires it.	Completely	Completely
Security function must be able to update the protection against malicious code automatically under secure circumstances.	Completely	Completely

Protection of the security function

Table 21. KSF requirements.

Requirement description	Symantec	McAfee
	Fulfils KSF	
	Completely/Partly/Not at all	Completely/Partly/Not at all
Security function must through self tests carry out correctness controls at start as well as when an authorized administrator requires it in order to demonstrate a correct functionality of the underlying solution.	Completely	Completely

Administration of the security function

Table 22. KSF requirements.

Requirement description	Symantec	McAfee
	Fulfils KSF	
	Completely/Partly/Not at all	Completely/Partly/Not at all
There must be possibility of adding, removing or in another way changing what types of malicious code that the security function must protect against.	Completely	Completely
There must be possibility of updating the definition file that is used as the control mechanism.	Completely	Completely
There must be possibility of adding, removing or in another way changing what measures are taken when malicious code is detected.	Completely	Completely
There must be possibility of adding, removing or in another way changing in what way inspections of the IT-system occurs: • During operation. • At start. • When an authorized administrator requires it. Inspections can either be complete or incremental.	Completely	Completely

9. Cellular phone security

Cellular phone security is another important issue that is addressed in this thesis. Cellular phones are considered to be more vulnerable than regular wired phones. Primarily, the use of cellular phones entails risks of being eavesdropped. Another concern is that thieves can bill their own calls to ones account [34].

9.1 Eavesdropping

As previously mentioned, eavesdropping of a conversation is a main security concern when using cellular phones. If an analog cellular phone is used, a conversation can be overheard by someone with only using a scanner. Even though digital cellular phone transmissions are scrambled for better protection, unscrambling these transmissions is possible if the right equipment is used.

The best way to protect a connection is to be careful with what is discussed on the cellular phone since it actually acts as a handheld broadcast station. This implies that sensitive or confidential information should not be discussed on the cellular phone.

9.2 Fraudulent billing

Intercepting a cellular phone signal and cloning the phone's ID numbers, i.e., the phones Electronic Serial Number and Mobile Identification Number (ESN/MIN), is possible [34]. The result is the same as getting a calling card stolen.

Two of countermeasures against fraudulent billing that can be taken are:

Limit roaming All cellular phones that are enabled to roam should be reviewed and these should be limited as much as possible. The use of Personal Identification Numbers (PINs) is usually defeated by roaming and this is the reason why cloners prefer roaming phones [34]. Furthermore, when roaming is enabled, it is more difficult to use fraud-detection programs in order to monitor an account and to shut it down if fraud is detected.

Turn the phone off Cellular base stations are polled by cellular phones with the strongest signal every few seconds in order to let the system know which base station calls should be routed through. However, this procedure entails the risk that the phone will be intercepted or cloned.

10. Policies

Beside the use of KSF, which is an important tool, wireless communication can be regulated by means of rules and procedures. These rules and procedures are aimed to handle security aspects, so there is a need to formulate policies. The formulation of policies is important, because they can regulate wireless communication on all levels.

Following are a number of such administrative rules and procedures [28]:

- Antivirus process
- Password protection policy
- Personal communication device
- Remote access policy
- Virtual Private Network (VPN) policy
- Wireless communication policy

10.1 Antivirus process

- The corporate standard should always be used, where supported antivirus software is available from the corporate site. Antivirus software updates should be downloaded and installed as soon as they become available.
- Incoming email from unknown, suspicious, or untrustworthy sources where files or macros are attached should never be opened. Instead, these attachments should immediately be deleted (also from Trash).
- Files from unknown or suspicious sources should never be downloaded.
- Direct disk sharing with read/write access should be avoided, unless there is a business requirement to do so.
- Before using storage media, such as floppy diskette, flash drivers, DVDs, CDs, etc., from an unknown or suspicious source, it should always be scanned.
- Back-up critical data and system configurations regularly and store the data safety.
- Spam, chain, and junk email should be deleted without forwarding them.

10.2 Password protection policy

The purpose of a password protection policy is to establish a standard for creation of strong passwords, protection of them, and the frequency of change.

10.2.1 Policy

- System-level passwords, e.g., root, enable, NT admin, etc., must be changed on at least a quarterly basis.
- Production system-level passwords must be part of the Information Security administered global password management database.
- User-level passwords, e.g., email, web, etc., must be changed at least every six months.
- User accounts possessing system-level privileges, granted through for instance group memberships, must have a unique password from all other accounts held by that user.

- Passwords should not be inserted into email messages or any other form of electronic communication.
- Strong passwords should be used, containing for instance both upper and lower case characters, digits, and punctuations. They should be at least eight alphanumeric characters long and they should not be a word in any language, slang, dialect, jargon, etc.
- Do not reveal a password over the phone to anyone, in an email message, to the boss, on questionnaires or security forms, to co-workers, etc.

10.3 Personal communication and personal communication devices

Personal Communication Devices (PCDs) are handheld wireless devices, such as cellular telephones, laptop wireless cards, pagers, etc.

10.3.1 Policy

- PCDs will only be assigned to FMV's personnel with duties that require them to be in immediate and frequent contact.
- Bluetooth and other hands-free enabling devices should only be issued to authorized FMV personnel who have received approval. In order to avoid being recorded when peering Bluetooth adapters, care must be taken.
- FMV's personnel may be issued voicemail boxes. However, they must be protected by a PIN, which should be different from the last four digits of the telephone number of the voicemail box.
- Files containing confidential data should not be stored in PCDs, unless it is protected by approved encryption.
- Lost or stolen PCD must immediately be reported.
- PCDs and voicemail are issued for FMV's business. Personal utilization should be limited to minimal and incidental use.

10.4 Remote access policy

The remote access policy defines standards for connecting to FMV's network from any host in order to minimize the potential exposure to FMV from damages resulting from unauthorized use of FMV's resources. These damages include the loss of sensitive and/or confidential data, intellectual property, damage to public image, damage to critical FMV internal systems, etc.

10.4.1 Policy

- Remote access must be strictly controlled. Control should be enforced via one-time password authentication or public/private keys with strong pass-phrases.
- An employee at FMV should never provide their login or email password to anyone.
- Reconfiguration of equipment aimed for home use, for the purpose of split tunnelling or dual homing is never permitted.

- Hosts connected to FMV's internal networks via remote access technologies must apply the most up-to-date antivirus software (personal computers included).
- Personal equipment, used to connect to FMV's networks, must meet the requirements of FMV-owned equipment for remote access.

10.5 Virtual Private Network (VPN) policy

The purpose of VPN policy is to provide guidelines for Remote Access IPSec or L2TP VPN connections to FMV's corporate network.

10.5.1 Policy

- Employees with VPN privileges have the responsibility to ensure that unauthorized users are not granted access to FMV's internal networks.
- Control by either a one-time password authentication such as token device or a public/private key system with strong pass-phrases is required for VPN use.
- When there is a connection to the corporate network, all traffic to and from the PC will be forced through the VPN tunnel, while all other traffic will be dropped.
- Split tunnelling is not permitted, because only one network connection is allowed.
- FMV's network operations groups must set up and manage VPN gateways.
- Up-to-date antivirus software that is the corporate standard must be used on all computers (including personal computers) that are connected to FMV's internal networks via VPN or any other technology.
- After 30 minutes of inactivity, VPN users must automatically be disconnected from FMV's network. This forces the user to logon again in order to reconnect to the network. Additionally, artificial network processes such as pings are not to be used to keep the connection open.
- VPN concentrators are limited to a maximum connection time of 24 hours.
- Users of computers that are not FMV-owned equipment must configure that equipment in order to comply with FMV's VPN and network policies – if this equipment is to be used with a VPN.
- Only Information Security approved VPN clients are allowed to be used.

10.6 Wireless communication policy

The purpose of the wireless communication policy is to prohibit access to FMV's networks via unsecured wireless communication mechanisms. Thus, wireless systems that meet the criteria of this policy or have been granted an exclusive waiver by Information Security can be approved for connection to FMV's networks.

10.6.1 Policy

- Wireless Access Points/Base Stations (APs/BSs) connected to FMV's networks must be registered and approved by Information Security. These APs/BSs are subjects to periodical penetration tests and audits. Wireless Network Interface Cards (NICs), which are used in corporate laptop or desktop computers, must be registered with Information Security.

- All WLAN access must use corporate approved vendor products and security configurations.
- Computers with WLAN devices must use a corporate approved VPN configured to drop all unauthenticated and unencrypted traffic. In order to comply with this policy, wireless implementations should maintain point-to-point hardware encryption of at least 56 bits. Implementations must support a hardware address which can be registered and tracked, i.e., a MAC address. They must also support and employ strong user authentication that checks against an external database such as RADIUS, TACACS+, etc.

11. Conclusions and future work

11.1 Conclusion

The aim of this thesis is to investigate if wireless equipment can be used in the internal LAN at FMV, where it must be able to offer security protection corresponding to the information security class HEMLIG/RESTRICTED.

The overall conclusion of this thesis project is that available security mechanisms analyzed throughout the project makes it feasible to deploy the security protection that is required by the FMV in order for the use of WLAN links.

Specific conclusions for this deployment are:

Access control/User authorization control

The comparison showed that Access Control Server (ACS) from Cisco Systems fulfilled more of the KSF requirements than Steel Belted RADIUS (SBR) from Funk Software. This implies that ACS is more suitable as a RADIUS and/or TACACS+ server to be used for access control/user authorization control. However, ACS does not fulfill all of the KSF requirements which is a prerequisite in order to be used at FMV.

Advantages

Ease of use	A web-based user interface facilitates and distributes configuration for user profiles, group profiles, and ACS configuration.
Scalability	ACS is built to support large networked environments, where it supports redundant servers, remote databases, database replication, and backup services.
Extensibility	LDAP authentication forwarding supports the authentication of user profiles stored in directories from leading directory vendors such as Sun and Microsoft.
Administration	ACS supports a number of access levels for each ACS administrator and the ability to group network devices. It also enables easier control and maximum flexibility to simplify enforcement and changes of security policy administration over all devices in a network.
Product flexibility	Support for AAA is embedded in Cisco IOS Software which means that ACS can be used across virtually any network access server that Cisco sells.
Integration	Because ACS is tight coupled with Cisco IOS routers and VPN solutions, it provides features such as Multichassis Multilink Point-to-Point Protocol (PPP) and Cisco IOS Software command authorization.
Control	ACS provides dynamic quotas for time-of-day, network use, number of logged sessions, and day-of-week access restrictions

Disadvantages

- Tests: ACS has not been tested by an independent party.
- KSF: Some of the KSF requirements are either partly fulfilled or are not fulfilled at all by ACS.

Security logging

In the case of security logging, both Network Security Manager (NSM) v4.1 from Intellitactics Incorporated and NetDetector/NetVCR from NIKSUN Incorporated equally fulfilled the various KSF requirements. However, NetDetector/NetVCR was chosen because more and detailed tests were performed.

Advantages

- NetDetector/NetVCR fulfills almost all KSF completely.
- It has been tested by an independent party.
- It captures network events the first time and stores them for a long time.
- It provides superior drill-down forensic analysis, down to the packet level.
- It includes a powerful event viewer.
- It provides secure and easy-to-use web interface with role-based access control.
- It provides advanced reporting, both scheduled and on-demand.
- Signature and statistical anomaly detection is included.

Disadvantages

- Access to some user data such as reports and FTP packet data through the management Graphical User Interface (GUI) without being identified and authenticated to the NetDetector/NetVCR is possible.

Intrusion protection

Check Point VPN-1/FireWall-1 NGX from Check Point Software Technologies fulfilled more KSF requirements than the Cisco Secure PIX Firewall V6.2(2) which implies that it is more suitable to use for intrusion protection. Furthermore, Check Point VPN-1/FireWall-1 NGX is also integrated with VPN functionality.

Advantages

- Check Point VPN-1/FireWall-1 NGX fulfills all KSF completely.
- It has been tested by an independent party.
- It defeats attacks against business applications.
- It prevents unauthorized network access.
- It forms flexible security infrastructure with best-of-breed solutions.
- It enables multi-gigabit firewall performance.
- It multicasts traffic control.
- It provides stronger authentication.
- It provides more granular policy control.

Disadvantages

- There are no clear vulnerabilities that are applicable to the Check Point VPN-1/FireWall-1 NGX or its direct predecessors and no other reporting mechanisms have identified any critical security flaws.

Protection against malicious code

Symantec AntiVirus Corporate Edition fulfilled more KSF requirements than McAfee Active Virus Defence, which suggests that it is more suitable to use as protection against malicious code.

Advantages

- It supports Microsoft Windows Vista.
- It guards against unauthorized virus access and attacks. Additionally, it protects users from viruses attempting to disable security measures.
- Integrated web-based graphical reporting is provided by the Symantec AntiVirus Corporate Edition.

Disadvantages

- Symantec AntiVirus Corporate Edition has not been tested by an independent party.
- Some of the KSF requirements are either partly fulfilled or are not fulfilled at all by Symantec AntiVirus Corporate Edition.

As mentioned earlier, protection against malicious code can be implemented in different ways. Beside the suggested antivirus software, another type of protection which can be implemented in IT-systems is to use integrity checks for subjects and objects as well as to use signed code. However, there is a demand that the signing party has to be trusted.

Virtual Private Network (VPN)

A Virtual Private Network (VPN) technology, such as IPsec, which protects the entire communication path from the source to the destination irrespective of what links and what networks it passes over, is a type of technology that should be used in order to achieve security protection. Furthermore, for example IPsec uses Internet Key Exchange (IKE) that supports the use of digital certificates. Digital certificates are to recommend for authentication process rather than passwords. This is due to the fact that passwords do not sufficiently protect access to a network and the data. However, the use of digital certificates allows one to more tightly control access to a network and to sensitive data as well as to control the privacy of the data.

Another option when using a VPN technology is to let FMV's WLAN be open. This means that there is no need for authentication for FMV's WLAN access itself, but in order to get access to applications a VPN technology has to be used. In fact, this means that there is only a need for authentication for application access by the use of VPNs. However, there is a risk by allowing a free access to FMV's WLAN meaning that one can misuse it, for hacking for example.

11.2 Future work

Some aspects that are interesting to investigate and should be done next are:

- To perform actual testing of devices/programs that was selected for deployment of the security protection that is required by the FMV.
- To investigate if there are other devices/programs existing in the market today that completely met all of the FMV's KSF requirements.
- To analyze how the security protection is affected if encryption (which is not specified by the KSF requirements) and protection against interception are used.
- To make a Request for Proposal (RFP), containing KSF requirements, to different vendors in order to investigate if there are other devices/programs that fulfills more or all KSF requirements.

References

[1] Raul Garcia Hijes, “Corporate Wireless IP Telephony”, M.Sc. Thesis, Royal Institute of Technology (KTH), Stockholm, Sweden, July 2005.

[2] R. Stanton, “Securing VPNs: Comparing SSL and IPsec”, Computer Fraud and Security, v 2005, n 9, September, 2005, p 17-19.

[3] J. S. Park and D. Dicoi, “WLAN security: current and future”, Internet Computing, Volume 7, Issue 5, September-October 2003, p 60-65.

[4] U. Varshney, “The status and future of 802.11-based WLANs”, Volume 36, Issue: 6, June 2003, p 102-105.

[5] Virtual Private Network Consortium, Feb. 2005, www.vpnc.org.

[6] S. Kent and K.Seo “Security Architecture for the Internet Protocol”, IETF, RFC 2401, Dec. 2004.

[7] Internet Engineering Task Force (IETF), Feb. 2005, www.ietf.org.

[8] D. Harkins and D. Carrel, “The Internet Key Exchange (IKE)”, IETF, RFC 2409, Nov. 1998.

[9] S. Kent and R. Atkinson, “IP Authentication Header”, IETF, RFC 2402, Nov. 1998.

[10] S. Kent and R. Atkinson, “IP Encapsulating Security Payload (ESP)”, IETF, RFC 2406, Nov. 1998.

[11] W. Townsley, A. Valencia, A. Rubens, G. Pall, G. Zorn, and B. Palter, “Layer Two Tunneling Protocol (L2TP)”, IETF, RFC 2661, Aug. 1999.

[12] K. Hamzeh, G. Pall, W. Verthein, J. Taarud, W. Little, and G. Zorn, “Point-to-Point Tunneling Protocol (PPTP)”, IETF, RFC 2637, July 1999.

[13] An FMV White Paper, “Requirements on Security Functions - Basics (Kraven på SäkerhetsFunktioner (KSF) – Grunder)”, Swedish Defence Materiel Administration (FMV), December 20, 2004.

[14] Alan O. Freier, Philip Karlton, and Paul C. Kocher “The SSL Protocol Version 3.0”, November 1996, http://wp.netscape.com/eng/ssl3/draft302.txt.

[15] Syed Muhammad Ali, “VoWiFi Roaming”, M.Sc. Thesis, Royal Institute of Technology (KTH), Stockholm, Sweden, January 2006.

[16] Wi-Fi Alliance, http://www.wi-fi.org, Last access on 10 November 2006.

[17] WPA and WPA2 Implementation White Paper "Deploying Wi-Fi Protected Access (WPA™) and WPA2™ in the Enterprise", http://www.wi-fi.org/OpenSection/protected_access.asp, Last access on 10 November 2006.

[18] Laing, Brian. *Intrusion Detection System, How-To-Guide*. Internet Security Systems, ISS. 2000

[19] Wikipedia, http://en.wikipedia.org/wiki/Demilitarized_zone_%28computing%29, Last access on 29 December 2006.

[20] University of Wyoming, http://uwadmnweb.uwyo.edu/InfoTech/vpn/split_tunnel.htm, Last access on 29 December 2006.

[21] Common Criteria, http://www.commoncriteriaportal.org, Last access on 29 December 2006.

[22] Symantec, http://www.symantec.com, Last access on 29 December 2006

[23] McAfee, http://www.mcafee.com, Last access on 29 December 2006.

[24] P J. Welcher and M Adkins, "Wireless LAN Security", http://www.netcraftsmen.net/welcher/papers/wireless02.html, Last access on 29 December 2006.

[25] Cisco Systems, http://www.cisco.com, Last access on 29 December 2006.

[26] Ars Technica, http://arstechnica.com/articles/paedia/security.ars/5, Last access on 29 December 2006.

[27] Juniper Networks, http://www.juniper.net, Last access on 29 December 2006.

[28] SANS Institute, http://www.sans.org, Last access on 29 December 2006.

[29] R. Rivest, "The MD5 Message-Digest Algorithm", IETF, RFC 1321, Apr. 1992.

[30] K. Sankar, A. Balinsky, D. Miller, and S. Sundaralingam, "EAP Authentication Protocols for WLANs", http://www.ciscopress.com/articles/article.asp?p=369223&seqNum=4&rl=1, Last access on 10 January 2007.

[31] B. Aboba and D. Simon, "PPP EAP TLS Authentication Protocol", http://tools.ietf.org/html/draft-ietf-pppext-eaptls-06, Last access on 10 January 2007.

[32] P. Funk and S. Blake-Wilson, "EAP Tunneled TLS Authentication Protocol (EAP-TTLS)", http://tools.ietf.org/html/draft-ietf-pppext-eap-ttls-05, Last access on 10 January 2007.

[33] A. Palekar, D. Simon, G. Zorn, and S. Josefsson, “Protected EAP Protocol (PEAP)”, http://tools.ietf.org/html/draft-josefsson-pppext-eap-tls-eap-06, Last access on 10 January 2007.

[34] Cornell University, http://www.cit.cornell.edu/cellphone/security.html, Last access on 24 February 2007.

COS/CCS 2007-09

www.kth.se