FAKULTA MATEMATIKY, FYZIKY A INFORMATIKY

UNIVERZITY KOMENSKÉHO V BRATISLAVE

DIPLOMOVÁ PRÁCA

Apríl 2005

Martin Pernecký

Comenius University

Faculty of Mathematics, Physics and Informatics

Department of Computer Science

Martin Pernecký

Security of wireless networks based on ANSI/IEEE 802.11

Diploma thesis

Thesis supervisor: Mgr. Ivan Kopáčik

Bratislava

April 2005

I do declare that I elaborated this submitted thesis on my own using only literature listed.

Bratislava, April 2005

Martin Pernecký

I would like to express my gratitude to my family and friends for their support and also to my supervisor Mgr. Ivan Kopáčik, for his valuable comments.

Contents

List of figures

List of tables

Abstract

The aim of this document is to give a comprehensive overview about current status of security of wireless networks based on IEEE 802.11. It will analyze security mainly from authentication, confidentiality and availability standpoint. The goal is to describe all usable security protocols and analyze their strong and weak points. It will also describe possible attacks on wireless networks; analyze their impact and method of detection and mitigation. It will try to propose solution for some common wireless network applications – analyze their needs, risks, propose a solution and evaluate its suitability and validity.

1 Introduction

The scope of this work is to describe wireless network based on ANSI/IEEE 802.11 (commonly referred as Wi-Fi), analyze current security status of these networks and show how to make these networks as secure as possible.

The motivation for writing this thesis comes from the current security status of wireless networks. Because of easy accessibility of this technology, its affordability, ease of use and deployment, the wireless networks are used in many areas from homes to big corporations. Wireless service providers offering connectivity through wireless hotspots or long haul directional antennas started using this technology when it became widely accessible. But through this whole development the security aspect was overlooked and massively abused. Now with maturing of this technology and emerging of new security protocols we wanted to provide a complex and complete overview of this technology from security viewpoint and provide an objective analysis of achievable security.

Current surveys show that wireless security is not a number one concern neither for home users nor many large enterprises. A large percentage of wireless access points still work with default configuration, allowing anyone passing by to use the connection and read all communication, including personal data such as emails or IM conversations. But even if the wireless network is secured there are open still many routes though which the networks can be successfully attacked. A short survey in Bratislava using only a wireless network discovery tool and a PDA revealed that from about 100 wireless networks more then 80% were not using any confidentiality protocols at all. Judging by the ESSIDs of observed networks some of them belonged to large corporations. And in our opinion that is very alarming.

We will analyze wireless security from a complex standpoint, not only as means to ensure privacy of information, but to achieve other aspects of security, namely integrity, privacy, availability. To achieve this, we will look at authentication, authorization, auditing, privacy, integrity and availability.

We will look not only at protocols from the IEEE 802.11 suite (WEP, TKIP), but at the whole spectrum of security protocols, to achieve our goal. This includes protocols from IP suite (IPSec, SSL), tunneling protocols (IPSec, L2TP, and PPTP), and authentication and authorization mechanisms (IEEE 802.1x: EAP, RADIUS).

In second part we will propose security solutions for some common wireless network applications. This will include an analysis of their needs, weaknesses, risks and methods to eliminate them.

2 Security

2.1 Overview

In computer environment security can be defined as protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users or the provision of service to unauthorized users, including those measures necessary to detect, document, and counter such threats.

Security can be broken down into several aspects that can be solved separately to achieve security. Solving of these partial problems is easier then solving security from a complex point of view. When securing networks and information exchanges security can be divided into:

- authentication;
- authorization;
- privacy (or confidentiality);
- auditing;
- availability.

2.2 Authentication

The goal of authentication is to confirm identity of a person/user. In network environments, WWW internet or extranet applications it makes sense to distinguish one user from another.

This can be done in many different ways. The identity of the user can be determined by supplying security credentials. The most basic form of credentials is user name and password. Password is private information known only to the user that has to be authenticated. But it can be guessed by the attacker. The most common attacka to defeat password authentication are dictionary attacks, brute force attacks or a hybrid attacks. They all have a set of possible passwords and try it one by one. The dictionary attack has a finite set of password stored in a file that is called a dictionary, brute force attacks generate all passwords in lexicographic ordering and hybrid attacks combine the advantages of both by transforming an initial set of passwords using some rules that simulate the process that users use to memorize passwords (e.g. they transform the password dog to: dog, Dog, DoG, D0g etc.).

To reduce the impact of these attacks the system can impose a certain complexity rules for the passwords, such as length or combination of character classes. But when enforcing a very complex password there could be a danger that users can not remember the password and write it down, which lowers the security considerably.

Another authentication scheme is based on certificates and public key infrastructure. Each user that needs to be authenticated has a digital certificate describing his identity and private key that corresponds to the pubic key in the certificate. The private key can be stored on the computer or on an external token, such as smart card or USB key. In this case the user does not need to remember anything; he just needs to protect the private key.

2.3 Authorization

Authorization is a process of determining if a specified user has permission to use a specified service or resource. Authorization can rely on authentication to determine the identity of user or on authorization token. Familiar examples of authorization tokens are keys and tickets.

2.4 Privacy

Privacy is concerned with protecting information in a way, that only authorized users can read the information. It uses cryptography and encryption ciphers and protocols to achieve this.

Ciphers use a secret information (called a key) to encrypt information from cleartext to encrypted form called the ciphertext. This process is called encrypting. The opposite process is called decrypting and transforms the ciphertext using a key to the corresponding cleartext.

All current ciphers can be divided into two categories – symmetric ciphers and asymmetric ciphers. Symmetric ciphers use the same key for encoding and decoding of information. The advantage of these ciphers is that they can be quite fast. The disadvantage is that prior to first communication all communication parties have to know the key. When the parties do not know each other they have no means to exchange the encryption keys securely. The most prominent symmetric ciphers are DES, Triple-DES and AES.

The other category of ciphers is asymmetric ciphers. These use two keys in the encryption/decryption process. One key is used to encrypt the plaintext to ciphertext and another key is used to decrypt the ciphertext. Its advantages and disadvantages are the exactly opposite as in symmetric ciphers. They are very slow compared to symmetric ciphers. But the communication of parties that do not know each other is easy. Every party transfers its public key (the one used for encryption) to others. Then the other party encrypts the data using this private key and sends it to the owner of the private key. Then he and only he can decrypt the information using his private key (the key used for decrypting). Other application of asymmetric ciphers is digital signing of data to ensure integrity and non-repudiation of a document.

The combination of both cipher categories is called hybrid encryption. Asymmetric ciphers are used to transfer a key to a symmetric cipher, which is then used to transfer all data.

2.5 Auditing

Auditing is concerned with collecting and analysis of data in the environment. Devices of programs used to collect data send it to a system where it is evaluated using various methods such a fingerprinting or various heuristics to detect unusual activity that could mean a breach in security.

2.6 Availability

A commonly overlooked aspect of security is availability. While most people know that authentication and encryption are vital for security of a service or network, availability is an equally important one. Every service is useless when anyone can disrupt its operation.

In network scenarios availability is achieved mostly using redundancy. It is achieved by eliminating single points of failure from the network topology by introducing alternate paths to destination or backup network devices such as routers or switches.

But redundancy is not the only paradigm to provide availability. When protocols used on the network are not secure and give anyone the ability to perform actions that can affect availability, then redundancy would not be of much help.

3 Overview of IEEE 802.11

3.1 History

IEEE 802.11 was standardized in 1999 by IEEE. It introduced wireless networks using radio signals in 2.4 GHz or using light infrared band. The maximum transfer rate was 2 Mbit/s. In the same year an amendment to this standard called IEEE 802.11a was ratified. It defined a new physical layer using 5 GHz radio band. Because this band is wider that the 2.4 GHz band the maximum transfer rate is 54 Mbit/s. Also in the same year IEEE introduced a new high-speed physical layer using the 2.4 GHz band. This was the 802.11b. The maximum transfer rate rose to 11 Mbit/s.

In 2003 IEEE ratified a new amendment to 802.11 to raise the maximum speed to 54 Mbit/s in the 2.4 GHz band. This was amendment 802.11g. To this point the security protocols have been untouched. The only security protocol to this date was Wired Equivalent Privacy (WEP), which was starting to be insufficient, because of known attacks.

The remedy to this problem came from Wi-Fi Alliance in form of Wi-Fi Protected Access (WPA). Wi-Fi Alliance is non-profit organization dedicated to promoting Wireless LANs and enhancing user experience. It also runs a “Wi-Fi CERTIFIED” certification program to certificate wireless devices to ensure their interoperability. Wi-Fi Alliance took from unfinished draft of IEEE 802.11i Temporal Key Integrity Protocol (TKIP) and PSK protocol and introduced it as WPA.

The amendment IEEE 802.11i was ratified July 23rd, 2004. It introduced a score of new security improvements to the MAC sublayer such as the security protocols TKIP and CCMP; and interoperability with IEEE 802.1x.

The following table shows the chronology of wireless standards plus and outlook to the future of wireless local area networks.

Table 1 – Chronology

1999	IEEE 802.11	Initial wireless standard
	IEEE 802.11a	5 GHz band physical layer
	IEEE 802.11b	2.4GHz band high-speed physical layer
2003	WPA	Improved security protocol by Wi-Fi Alliance new
	IEEE 802.11g	Further 2.4 GHz band speed improvement
2004	IEEE 802.11i	Security enhancements for MAC
Future	IEEE 802.11n	High speed improvements (up to 200 Mbit/s) in 2.4 GHz and 5 GHz band
	IEEE 802.11s	Wireless mesh networks

3.2 Description

The ASNI/IEEE 802.11: 1999 covers the first two layers of ISO/OSI model – the physical layer (PHY) and data link layer. Data link layer in IEEE 802 networks is divided into two sublayers – Media Access Control (MAC) and Logical Link Access (LLC). ANSI/IEEE 802.11 covers PHY and MAC. LLC used in wireless networks is defined in ANSI/IEEE 802.2 and is common for all 802 network types. Therefore the PHY used is transparent to higher layers.

3.3 Physical layer (PHY)

Wireless networks use electromagnetic waves propagating through air. Contrary to wired network this transmission medium is not closed as in wired networks, where users have to plug a cable into the network to communicate, wireless networks are accessible to anyone who is within the area, where the signal is strong enough.

This means that the network boundaries are not absolute or readily observable. They can also change with time, depending on many outside influences.

Other than using radio waves in 2.4 GHz and 5 GHz frequency band, wireless networks can operate using near-visible infrared light. This physical layer was defined in IEEE 802.11: 1999, but failed to spread. Because of properties of light these networks are more secure, because direct visibility is required. But this is also a big disadvantage of these networks. Also the transfer speed can reach only theoretical 1 Mb/s. Now only devices using radio signals are used, so we will not cover networks using this PHY.

The signal is propagated into space using antennas. Each antenna can be characterized using a radiation pattern and gain.

Radiation pattern is a three dimensional representation of the energy distribution of an antenna in polar or rectangular coordinates. Commonly two projections of radiation pattern are used to display the radiation characteristic of the antenna: horizontal and vertical view.

Gain of an antenna is defined as ratio of the received or transmitted signal compared to an isotropic antenna. Isotropic antenna is a hypothetical antenna that radiates equally in all directions and is used only as reference for measuring antenna gain. It is usually measured in dBi. The higher the gain the fainter signals can the antenna pick up and amplify from certain direction. Gain can be also viewed as a measure of antenna directivity because gain in one direction can be increased at a cost of degrading it in other direction.

Antennas can be divided into several types based on their radiation patterns.

3.3.1 Omni-directional antennas

Omni-directional antennas radiate their signal in all directions. The radiation pattern is donut shaped (see Figure 2). That means that directly above the antenna there is no signal and the signal is the strongest at the horizontal level of the antenna.

Omni-directional antennas usually have gain from 2 dBi to around 15 dBi.

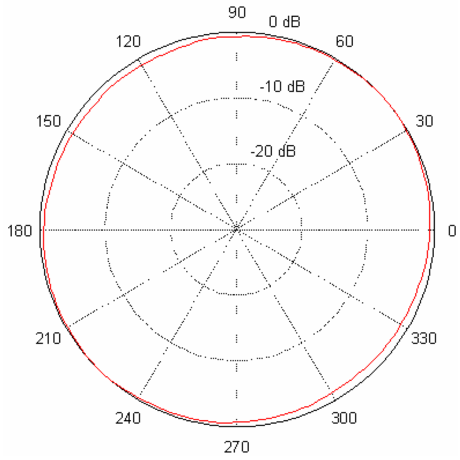

Figure 1 – Horizontal radiation pattern projection for omni-directional antenna

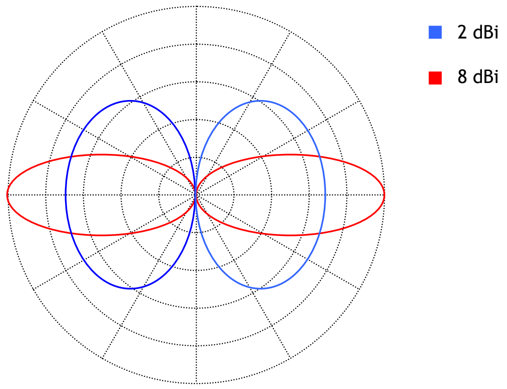

Figure 2 – Theoretical vertical radiation pattern projection of omni-directional antenna

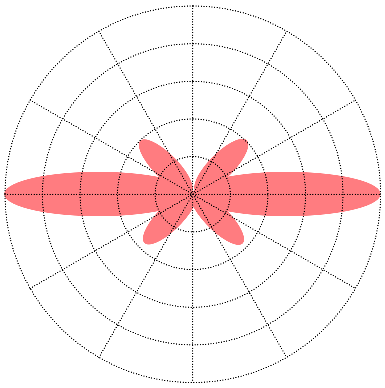

Figure 3 – Main and side lobes of omni-directional antenna

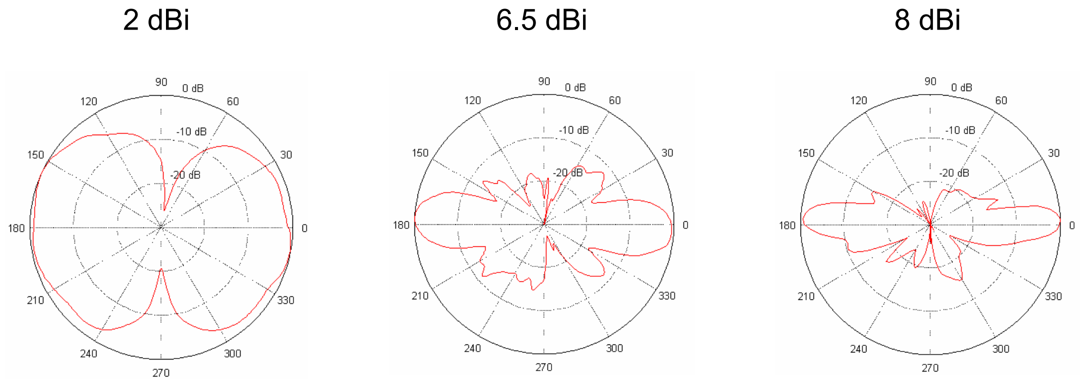

Figure 4 – Vertical radiation pattern projection for several omni-directional antennas

3.3.2 Sector antennas

Sector antennas can cover a specified sector. The most common are 60°, 90° or 180° antennas. These antennas cover only the specified section of the space, so they can be very useful to constrain the signal only to desired area.

3.3.3 Directional antennas

Directional antennas transmit and receive the signal only from a small section of space. They can come in form of parabolic grid or dish antennas, or yagi antennas. These antennas have highly directional radiation pattern.

Directional antennas are used to transmit the signal over long distances. The imperative when using a point to point link is direct visibility, therefore they can be built on building roofs or masts. But direct line of visibility is not enough. Line of sight for microwave includes an area around the direct path called the Fresnel zone. It is an elliptical area immediately surrounding the visual path. It varies depending on the wavelength of the signal. The Fresnel zone must be taken into account when designing a wireless link. Any object within the Fresnel zone attenuates the transmission between the endpoints.

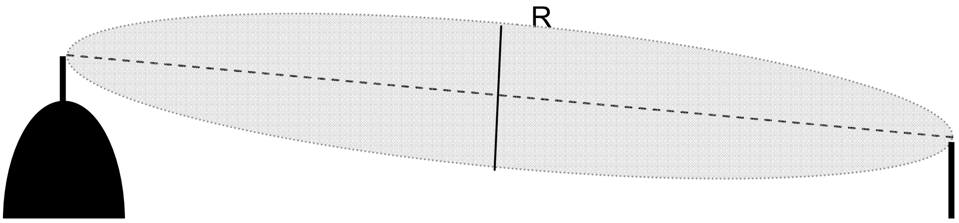

Figure 5 – Fresnel zone for directional antenna

The maximum radius for Fresnel zone *R* in meters is:

$$R = 17.32 \times \text{sqrt}\ (d/4f)$$

where d is distance in km;

f frequency in GHz.

3.4 Media Access Control sublayer (MAC)

MAC is a sublayer of data link layer. It provides service to LLC sublayer and uses PHY layer to deliver unicast, multicast or broadcast MAC service data units (MSDU) on best-effort connectionless basis. There is no guarantee that the MSDUs will be delivered successfully.

MAC uses services to deliver MSDUs (integration and distribution service) and has services to protect (confidentiality service) and authenticate (authentication service) user communication. These services run on stations and/or access points.

MAC layer uses same addressing scheme as Ethernet (IEEE 802.3), where each station has its own 48 bit MAC address.

3.4.1 Components of wireless networks

The basic building block of wireless network is Basic Service Set (BSS). BSS is an area, in which stations can communicate among each other. In Figure 6 there are two BSS with two stations each. Only stations 1 & 2 and 3 & 4 can communicate with each other.

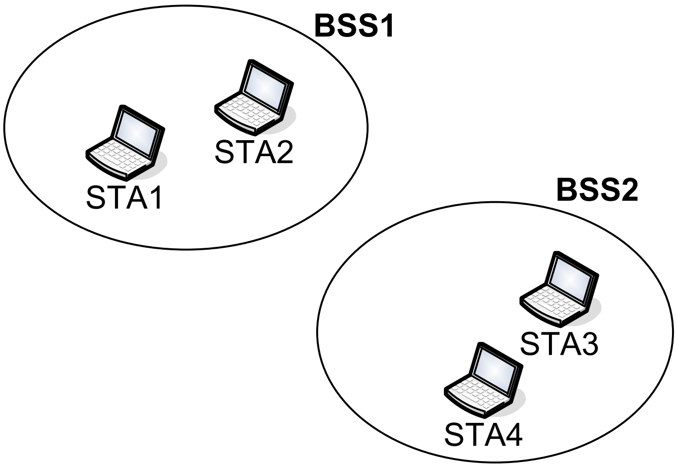

Figure 6 – Basic Service Set

To build a network with extended coverage or some topology a distribution system (DS) must be established. In DS we distinguish between the wireless medium that is used for communication with stations and distributed system medium which is used to maintain the distribution system.

3.4.2 Services

3.4.2.1 Distribution service

Distribution service is used to distribute frames across an infrastructure network. It only runs on access points. When a station wants to send a frame to another station, it sends this frame to access point. The access point then uses the distribution service to determine where the destination station is, if it is associated with it (in its BSS) or with a different access point. Based on the result the access point then forwards the frame to the destination station or to the access point with which the destination station is associated. The implementation of the service used for transfer to another access point is not defined in [1].

3.4.2.2 Integration service

Integration service is used to transport frames outside the bounds of the wireless network. Integration service runs on access points. Integration is also concerned with address translation if necessary. If the integration service determines that the destination of the frame lies outside the wireless network the frame is sent to portal, which than routes the frame to destination network.

3.4.3 Operation modes

3.4.3.1 Ad-hoc mode (IBSS – Independent basic service set)

This is the most basic type of IEEE 802.11 network. It consists of at least two stations within a specified BSS. In ad-hoc mode all stations must be able to communicate with each other. The association of stations is dynamic; there is no explicit association or deassociation. When a station leaves the BSS area or is turned off it leaves the ad-hoc network.

In IBSS when a station wants to communicate with other station it must be within range of the signal from the station. So when more then two stations want to communicate with each other, each station must be able to receive signal from all other stations.

3.4.3.2 Infrastructure mode (ESS – Extended service set)

A network in infrastructure consists of one or more basic service sets. These can be either overlapping or non-overlapping. The size of the network can be unlimited. The network looks like one local area network to upper layer protocols (LLC and above).

In ESS the center of each BSS is an access point. If a station wants to communicate with another station in ESS it send the frame to the access point, the access point then determines if the destination lies in its BSS. If the destination station is within its BSS it forwards the frame to that station. Distribution service running on the access point is responsible for this. When the destination lies outside the ESS then the access point invokes the integration service that transfers the frame to the correct destination.

3.4.4 Frame types

Table 2 – 802.11 frame types

Frame type	Subtype	Description
Management frames (type: 00)		
Association Request	0000	This frame is sent to an access point (in a BSS or ESS) or to any other peer (in an IBSS or ad hoc network). The sender must already be authenticated in order to gain a successful association.
Association Response	0001	This frame is sent from an access point (in ESS) or from any other peer (in an IBSS) in response to an association request frame. If the request is successful, the response will include the Association ID of the requester.

Frame type	Subtype	Description
Reassociation Request	0010	Like an association request, but it includes information about the current association at the same time as it requests a new association (either with the original Station after some lapse of time, or with a new station upon moving from one BSS to another). This frame is sent to an access point (in ESS) or to any other peer (in an IBSS). The sender must already be authenticated in order to gain a successful association.
Reassociation Response	0011	Like an association response, but in response to a reassociation request. This frame is sent from an access point (in ESS) or from any other peer (in an IBSS) in response to a reassociation request frame. If the request is successful, the response will include the Association ID of the requester.
Probe Request	0100	Probe request is used to actively seek any, or a particular, access point or BSS.
Probe Response	0101	Probe response replies with station parameters and supported data rates.
Beacon	1000	Beacon frames are sent by the access point in a BSS (or its equivalent in an IBSS) to announce the beginning of a Contention Free period (CF), during which the right to transmit is conferred by the access point by polling. Beacon management frames carry BSS timestamps to help synchronize member stations with the BSS, and other information to help them locate and choose the BSS with the best signal and availability.
ATIM	1001	Announcement Traffic Indication Message. This frame serves much the same function in an IBSS that the Beacon frame does in an infrastructure (ESS) topology. The frame sets the synchronization of the group and announces that messages are waiting to be delivered. Stations in Power Save mode wake up periodically to listen for ATIM frames in ad hoc (IBSS) networks, just as they do for Beacon frames in infrastructure (ESS) networks.

Frame type	Subtype	Description
Disassociation	1010	This frame is an announcement breaking an existing association. It is a one-way communication (meaning it does not require or accept a reply), and must be accepted. It can be sent by any associated station or BSS and it takes effect immediately.
Authentication	1011	Authentication frames are sent back and forth between the station requesting authentication and the station to which it is attempting to assert its authentic identity. The number of frames exchanged depends on the authentication method employed. Information relating to the particular scheme is carried in the body of the Authentication frame.
Deauthentication	1100	This frame is an announcement stating that the receiver is no longer authenticated. It is a one-way communication from the authenticating station (a BSS or functional equivalent), and must be accepted. It takes effect immediately.
Control frames (type: 01)		
PS-Poll	1010	Power Save polling frame. Stations in power save mode awaken periodically to listen to selected Beacons. If they hear that data is waiting for them, they will awake more fully and send a PS-Poll frame to the access point (BSS) to request the transmission of this waiting data. In Control frames of the Power Save-Poll type, the Duration/ID field contains the association ID (AID) for the station sending the frame.
RTS	1011	Request To Send. Coordinates access to airwaves.
CTS	1100	Clear To Send. Response to a RTS and coordinates access to airwaves.
ACK	1101	Acknowledges receipt of transmitted data.
CF End	1110	Signals the end of Contention Free period.

Frame type	Subtype	Description
CF End + CF ACK	1111	Signals the end of the Contention Free period and Acknowledges the receipt of some frame in a single message.
Data frames (type: 10)		
any	any	Multiple subtypes exist for Data type frames, but all have the same basic format, that is described in [1]. The different Data subtypes essentially just piggyback CF-Poll, CF-ACK, and CF-End messages onto the data message in a single transmission. This allows the BSS to gain higher throughputs possible using PCF (point coordinating function).

3.4.5 Allowed frames

Frames are divided into 3 classes based on their frame type. These classes are called Class 1, Class 2 and Class 3. The types of frames that can be sent depend on the state of the sending station. The states are:

- State 1: Initial state: unauthenticated, unassociated
- State 2: Authenticated, unassociated
- State 3: Authenticated, associated

The allowed frames in each of the states are:

- State 1:
  - Controls frames
  - Management frames: Probe request/response, Beacon, Authentication, Deauthentication,
  - Data frames: FC: “To DS” = false and “From DS” = false
- State 2: all frames from state 1 and:
  - Management frames: Association request/response, Reassociation request/response, Disassociation
- State 3: all frames from state 2 and:
  - Data frames
  - Management frames: deauthentication
  - Control frames: PS-Poll

4 Wireless security

The security according to [1] is provided by the authentication and privacy services. Authentication ensures that unidentified stations cannot use the wireless network, and privacy service ensures that the data transmitted remains private.

IEEE 802.11 defines only one protocol used for authentication and encryption: WEP. Then IEEE introduced IEEE 802.11i (see [2]), an amendment improving security in wireless networks. This amendment introduced stronger protocols for encryption and authentication (AES, TKIP). Wi-Fi alliance introduced WPA protocol, comprised of WPA-PSK for home usage authentication and TKIP or CCMP for data encryption. WPA can function on hardware supporting WEP encryption, because it uses the same cipher (RC4) to encrypt data. Only a firmware upgrade is necessary. On the other side most existing devices do not support 802.11i because it requires AES encryption for CCMP which can not be realized on its hardware. So when moving to 802.11i or planning wireless networks it is advisable to look for devices prepared for 802.11i.

4.1 Privacy

4.1.1 Wired Equivalent Privacy (WEP)

WEP is a security protocol introduced in [1] to serve authentication and privacy purposes. It was not designed to be the most secure protocol on the market. As its name suggests (Wired Equivalent Privacy) it should provide the same level of security as a wired network does. In wired network you only need an entry point to connect to a network. Another goal when designing WEP was to make it as exportable as possible. This was done in the time, when there was a 40-bit key restriction for exporting cryptography from

United States in effect. So a 40-bit key length was chosen to comply with these export rules.

When using WEP every user in the network must know the same shared key to communicate. Time showed that the design of WEP was flawed and allowed many attacks against networks using it.

WEP supports setting of 4 independent keys, which can be rotated when encrypting frames. The indication of which key is used is part of the IV in the frame payload.

WEP uses stream cipher RC4 to encrypt and decrypt data portion of the frame. The secret in this protocol is a 40-bit key that is shared among all communicating parties. When a station wants to send a frame, it first generates an Initialization vector (IV), then concatenates the key with IV and uses this as input for the RC4. The RC4 function outputs an arbitrary long key stream, which is then XOR-ed with the data portion of the frame and the CRC checksum.

$$D = IV \,.\, RC4\,(key \,.\, IV) \oplus (P \,.\, c(P)),$$

where D is the resulting data field,

IV the Initialization Vector for the frame,

key the secret WEP key,

P plaintext data,

c(x) function to compute checksum.

The size of the key in WEP is 40 bits and the size of IV is 24 bits. This gives us 64 bits, for the input if the RC4 key generation function, of which 24 bits are public.

When using WEP only the data frames are encrypted and encrypted is only the Frame Body and FCS. Therefore all management and control frames are all sent in cleartext and are easily interceptable. Among these frames are deassociation and deauthentication frames.

Currently there exists an extension that allows having 104 bit key and 24 bit IV. This is called WEP2 of 128bit WEP.

4.1.1.1 Key management

Key management in WEP environment is not defined by [1]. So the key management was left up to vendors. The simplest scheme is to distribute the keys manually. In this case the administrator has to enter the keys into each station manually. Here only administrator knows the secret key, but the instance of key is located on all computers, so with some effort it can be extracted by the users and misused. They can be stored in registry, in configuration files and so on. Another possibility is to use some other secure channel (download from a secure website, sending by e-mail).

Also WEP uses one key for all participating stations, so a station that is located near the access point can decrypt all communication running through this access point using its key.

WEP key can be entered using a 40-bit binary key (hex encoded), or using a passphrase, which can be transformed into to key either by ASCII encoding or using a hash function. When using a passphrase the whole communication is susceptible to dictionary attacks.

4.1.1.2 Flaws and problems

WEP inherited all problems of RC4 cipher and included some of its own. The good practice when using RC4 is not to use weak keys and drop first 512 bytes of generates keystream. None of these are used by WEP, so the key can be derived when enough frames are collected using known techniques.

Also no IV management or expiration is defined, so for a device to comply with IEEE 802.11 it must accept any IV the station sends. This leads to possible replay and known plaintext attacks. Replay attacks mean that an attacker can sniff and resend any encrypted frame without being noticed. RC4 also suffers from known plaintext attacks. When we know cleartext value a frame and its encrypted representation, we can extract the keystream. And when knowing the keystream for specified IV, the attacker can forge a new frame and send over the network.

Since the generation of IVs is not standardized the IV generation is left up to vendor. The most common are:

- using static value
- using two values and switching between them
- using counter, which is reset on restart (the counter can be big-endian on little-endian)
- using a random value

Each of these implementations has its own problems. When using static value we only need to know the value of one frame and its ciphertext and we know the respective keystream for the session. Using this keystream we can decrypt all other frames. The same problem is with using two values. When using a random IV the IVs repeat after approximately after 5.000 frames (because to birthday paradox).

When using counter to increment the IV, we get many frames with small IV values, so we can produce a dictionary with keystreams and use it to encrypt other frames. Also when generating IVs sequentially, the device can produce so called weak IVs, which give away information about the secret key. When the hacker collects enough frames with weak IVs, he can compute the secret key, and then the whole communication can be compromised. It should be said, that this attack can be executed off-line, so that the attacker can collect the frames, then try co compute the key from them and then decrypt the whole past communication and any future communication that uses the same key. This type of attack has been implemented in program AirSnort.

It is shown that this attack needs to collect around one million to five million keys to compute the secret key. This corresponds to less that 1GB of data. On busy networks it can be achieved in few hours.

In a new version of this attack only about 100,000 frames suffice to compute the secret key. This speeds up the breaking of the key by a factor of ten, resulting in 100MB of data. In worst case when all frames hold ARP traffic the key can be broken with only approximately 5MB of data.

Many vendors, now that the attacks on WEP have gone public, implemented algorithms that do not use weak IVs but filter them out. But filtering the IVs does not result in WEP being unbreakable; it merely slows it down.

When the attacker has access to the network from inside (such as an employer, or someone using the company computer unauthorized) the frames can be generated very fast, thus satisfying the needed frame count in matter of seconds or minutes. The easiest way of generating packets is by pinging a station with zero timeout, or in Linux environment pinging the broadcast address of the network and thus flooding the whole network with ICMP packets.

Even when the attacker has no access to the network, he can generate new frames. He can pick some frame and resend it over and over. The best way is to pick an ARP request packet, which occurs normally on the network and is easily distinguishable even when encrypted, because is has a very specific length (42 bytes). When resending this frame the station which address needs to be resolved sends an ARP reply with new IV that can be used to compute the key. Another advantage of these packets is that they are very short thus the attacker gets many IVs per megabyte.

4.1.2 Temporal Key Integrity Protocol (TKIP)

The goal of TKIP is to strengthen the encryption strength on existing hardware. It uses RC4 cipher, the same cipher as WEP. Because of this it can run on the same hardware that can run WEP only with a software or firmware update.

The biggest improvement is that TKIP does not use a static key to encode the traffic but it generates a new key for every session. The key that is used to encrypt the traffic is called Pair-wise Transient Key. This key is computed using a 4-way handshake (see Figure 7) between the access point and station. PTK is a function of MAC addresses of the stations, a Pair-wise Master Key (PMK). Since these can be static the variables are two nonces generated by both stations. The only secret here is the PMK which is shared between the two parties.

Another countermeasure that is implemented in TKIP is a protection against replay attacks. TKIP uses a counter to sequentially number all outgoing frames. The receiving station drops all frames comes out of order. This provides a protection against replay attacks, because a replied frame sent by an attacker is dropped by the receiving station automatically. The sequence number is encoded into WEP IV end extended IV field.

TKIP also introduces a Message Integrity Code (MIC) called Michael to protect the integrity of the transferred data. It protects data, source and destination address and priority field. This protects the transmission from following attacks:

- bit flipping attacks;
- data modifications: truncation, concatenation;
- fragmentation attacks;
- iterative guessing attacks against the key;
- redirection attacks (by modifying Destination Address field);
- impersonation attacks (by modifying Source Address field).

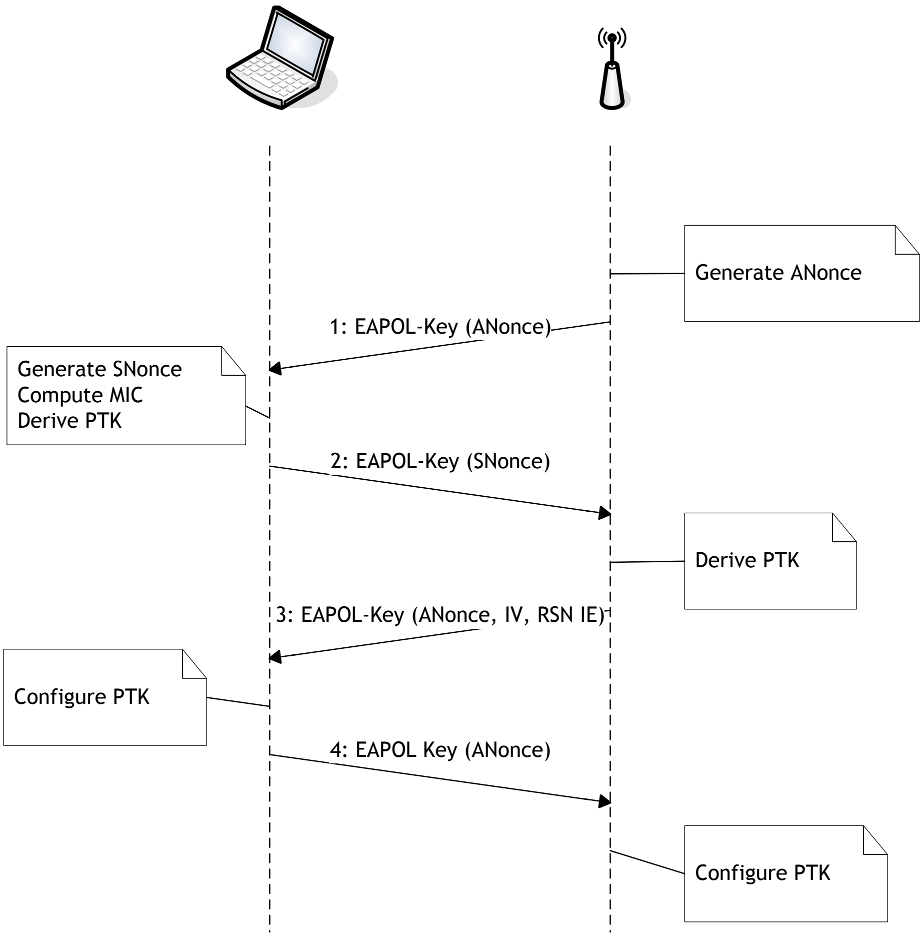

Figure 7 – 4-way handshake

TKIP uses a hierarchy of keys that are used for various purposes. All keys can be divided into keys that are used for unicast traffic (Pair-Wise Keys) (see Figure 8) and key used for multicast and broadcast traffic (see Figure 9). By using two different hierarchies of keys the unicast traffic can be protected from spoofing attacks, because when an attacker spoofs an address field the frame will be discarded upon decapsulation by the station.

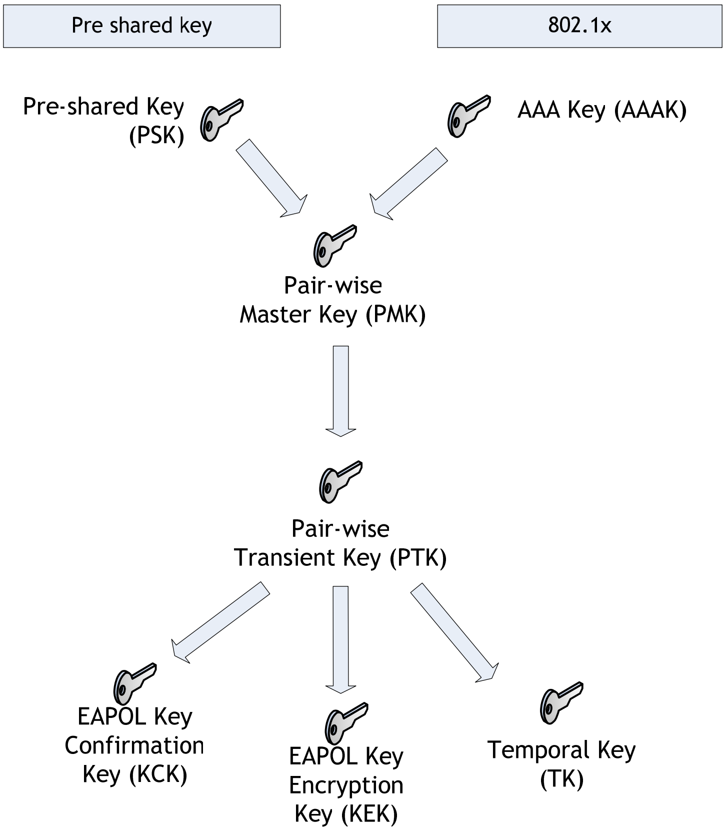
Pre shared key
802.1x
Pre-shared Key (PSK)
AAA Key (AAAK)
Pair-wise Master Key (PMK)
Pair-wise Transient Key (PTK)
EAPOL Key Confirmation Key (KCK)
EAPOL Key Encryption Key (KEK)
Temporal Key (TK)

Figure 8 – Pair-wise key hierarchy

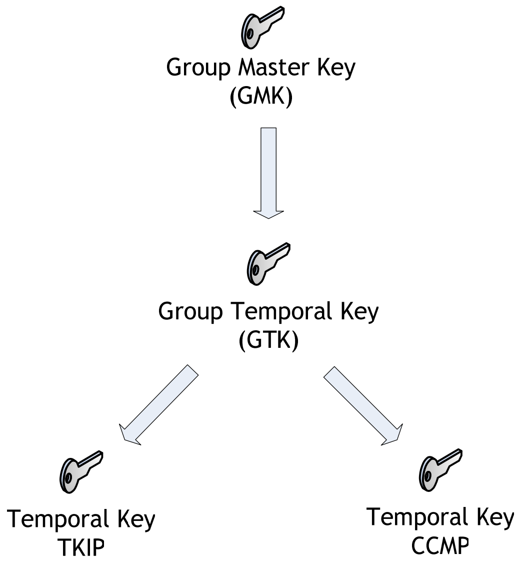

Figure 9 – Group key hierarchy

4.1.3 CTR [counter mode] with CBC-MAC [cipherblock chaining (CBC) with message authentication code (MAC)] Protocol (CCMP)

This security protocol was introduced into wireless world in the IEEE 802.11i standard. It is an authenticate-and-encrypt mode of operation for any block cipher. This means that every message sent is encrypted using the block cipher and an authentication field is present.

The input into this block cipher mode is:

- Key
- Nonce
- Message
- Authentication data

The length of nonce is variable; there is a trade off between the maximum message size and nonce size. For protocol with short messages a small maximum message size is required, so the nonce can be longer. On the other hand nonce should not be smaller, because then the protocol is susceptible to replay attacks.

The main requirement is that, within the scope of a single key, the nonce values are unique for each message. A common technique is to number messages sequentially, and to use this number as the nonce. Sequential message numbers are also used to detect replay attacks and to detect message reordering.

In IEEE 802.11i the Advances Encryption System (AES) block cipher is used. CCMP uses the same key hierarchy as TKIP and they are also derived by the same means.

4.1.4 IPSec

IPSec is a framework of network standards designed to secure communications on network layer. It was developed and is maintained by Internet Engineering Task Force (IETF). IPSec is used to authenticate, encrypt and ensure integrity of communication between computers, firewalls routers or gateways. It also provides some anti-replay protection. IPSec can employ various encryption and hashing algorithms, such as MD5 and DES. The usage of specific algorithms can be easily configured by administrator.

IPSec transports data using one of two modes: transport and tunnel mode. Both modes can be used to secure traffic between two hosts, but tunnel mode is designed to secure communication between end-user host and a gateway. Transport mode leaves the original IP header in place and inserts an authentication header and/or replaces the data part of the packet with encrypted payload. Tunnel mode encapsulates the existing packet into a new packet with a new header. Then upon reaching the gateway the packet is stripped from the encapsulation and is forwarded.

Currently many implementation of IPSec from many vendors exist. Some of them are supplied with operating systems, others are proprietary and some of them are open source implementations. Some of these implementations may have security flaws (e.g. they do not require certificates with verifiable chain of trust, which can lead to man-in-the-middle attacks, thus compromising the privacy of communication), so a careful selection and configuration process is required.

Because of the encapsulation and appending authentication header IPSec lowers the effective bandwidth of the existing network. Also all IPSec packets require decryption that can consume valuable CPU time on devices with lower performance. Combined with the broadcast nature of the wireless media this can lead to Denial of Service attacks, by flooding the stations with replayed frames.

4.1.5 PPTP and L2TP tunneling protocols

Point-to-Point Tunneling Protocol (PPTP) and Layer 2 Tunneling Protocol (L2TP) are used mostly create Virtual Private Networks (VPN) for secure remote access to networks. The securing of the data is done on transport layer, where whole IP packets that should go to the remote network are encapsulated and encrypted into another IP packet that carries additional control information used by the tunneling protocol.

In insecure wireless environment these protocol could be used to protect traffic traveling from station to a point behind to access point, so that all traffic transferred over the wireless link would be encrypted.

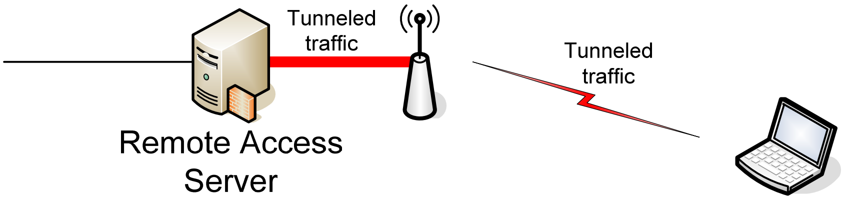

Figure 10 – Tunneling topology

The advantage of this approach is support of these protocols, because they have been around and widely used for a long time. Their security properties are known and are regarded as quite secure. The disadvantage is that are working on transport layer of the network and thus having a big overhead, because of doubling IP headers and because of the need of their own control fields. The other problem lies in the complicated procedure for setting up a tunnel. The opening of a tunnel required about 10 packets to be exchanged between the host and the remote access server and can take more that 0.5 seconds. When a wireless link fails, which in not uncommon in a wireless environment, the tunnel may need to be reestablished. In an environment with some interference this renders the wireless connection unusable or severely degrades its performance.

4.2 Authentication

4.2.1 Open System authentication

Open System authentication is the simplest authentication scheme available. This scheme needs no credentials. This does not mean that the authentication needs to be successful at all times.

First the station sends a management frame to authenticating station with request for Open System authentication. Then the authenticating station sends a reply with indication whether the authentication was successful.

4.2.2 Shared Key authentication

This authentication scheme is defined in [1]. It requires the support for WEP for all participating stations, since it uses WEP (RC4) for encrypting the authentication frames. The secret key should be already present on all stations participating in Shared Key authentication. The process of distributing secret is not covered in IEEE 802.11 standard nor any other standards.

During the authentication process the authenticator sends the authenticating station a challenge text in cleartext and the authenticating station responds with the challenge text encrypted with its secret key. The authenticator decrypts the encrypted challenge text and if the result is the same as the sent challenge text (meaning both station know the same secret) then sends the authenticating station notification about successful authentication.

Shared key authentication is not suitable, because it allows known plaintext attacks. An attacker can see the challenge the authenticator sends, and then he can see the encrypted challenge, which yields the keystream.

4.2.3 Service Set Identifier authentication

When connecting to wireless network the user has to know the ESSID of the network. The ESSID is public and broadcasted in the Beacon frames. But the broadcasting of this Beacon frames can be disabled, so the infrastructure network would not appear in the list of available networks. Another possibility is to remove the ESSID from the Beacon frame. This is called cloaking of the ESSID. The user has to know the exact ESSID of the network to connect.

This authentication method is not very powerful, because passive sniffing of the frames can reveal the ESSID, because it is part of the Management frames (Association, AP Probe).

4.2.4 MAC Filtering

This authentication scheme is completely implemented in the access point. It utilizes a MAC access list to determine which stations can be authenticated. It can be combined with another authentication scheme to constrain the set of station that are authorized to use the network.

The level of security of this authentication scheme it not very high, because all MAC addresses are transferred in clear and can be easily spoofed by intruder. Also the MAC access list is not easily managed. Therefore is this scheme not suitable for bigger infrastructure networks. If the MAC access lists should span through more access points a proprietary exchange protocol must be utilized, since not standard for such protocol has been proposed or adopted. This limits the utilization of devices from different vendors.

4.2.5 Universal Access Method (UAM) (Captive server)

This solution is used by Internet Service Providers who provide hotspots to authenticate and authorize users using their wireless network. This solution should be easier to implement from provider as well from client side. It was introduced before 802.1x was used for securing wireless networks, when the only possibility to secure wireless networks was WEP and shared authentication.

The principle here is simple and has nothing to do with wireless networks. When a new user enters a local network (wired or wireless) his MAC address is unknown. So the captive server blocks all traffic except ARP, DHCP and DNS traffic and SSL to a specified website, where the provider can authenticate the user. Unauthenticated user is redirected to the authentication website from every page he wants to access. This is achieved using DNS hijacking, where for every DNS request the address of the authentication website is returned. The authentication is done using a web form where user enters his credentials. When the authentication is correct and user is authorized to use the network the captive server unlocks all traffic from the client’s MAC address and IP address.

This method uses TLS/SSL tunnel to secure the authentication (when the authentication server uses HTTPS), so no sensitive data is revealed during the course of authentication.

The problem is that the authentication can be only triggered from a browser window. When a client wants to download his mail first it will fail, because the client is not authenticated yet, so the port to mail server is blocked. The same happens for VPN connections and other applications. Other disadvantage is that UAM does not enforce any encryption of the data transferred over the wireless network. The access point can be set up to use WEP, but since the WEP key is common to all hotspot users it provides no real security.

4.2.6 Wi-Fi Protected Access – Pre Shared Key (WPA-PSK)

WPA-PSK authentication uses TKIP to authenticate users and to generate an encryption for a session between a station and an access point. The stations share a pre-shared secret in form of a passphrase. WPA-PSK has a single passphrase per ESSID. So every station shares a common secret. From this passphrase the PMK is derived in the following manner:

$$PMK = PBKDF2\ (passphrase,\ ESSID,\ len\ (ESSID),\ 4096,\ 256)$$

This means that passphrase, ESSID and ESSID length are concatenated and hashed 4096 times into a 256 bit digest that is used as the PMK. Since the ESSID is public the passphrase is the only secret.

WPA-PSK is supported in all recent versions of widely used operating systems. In Windows environment WPA-PSK support is built in from XP, in older versions where wireless networking is not supported out of the box and WPA support is driver dependent. In UNIX systems WPA-PSK support is provided by wpa_supplicant utility. MacOS X has also support for WPA-PSK.

Since passphrase contains only alphanumeric characters is usually contains only 2.5 bits of security per character. The mapping form passphrase to key thus converts it to a key with approximately $2.5n + 12$ bits of security.

WPA-PSK provides a very good security for small deployments, since it does have the same key management as WEP and does not support per user passphrases. Because the passphrase can be determined using a dictionary attack a long passphrase should be used (20 characters or more, or a random passphrase).

4.2.7 EAP

EAP protocol is used in 802.1x authentication. It is specified in RFC 2284 and was initially developed for Point-to-Point Protocol (PPP). In PPP it uses a single protocol number but supports a variety of encryption schemes and authentication protocols. Because of its extensibility it has survived for over 7 years, and was the protocol of choice in IEEE 802.1x.

EAP encapsulates data link frames (PPP, 802.3 (Ethernet) or 802.11)

This is an enterprise authentication scheme, that can be used for authentication, authorization and accounting (AAA) services. It employs an external authentication server (such as Remote Authentication Dial-In User Server (RADIUS)) to issue a per-session, per-user secret key used for communication in the wireless and/or wired network. A common topology can be seen on Figure 11.

The EAP authentication occurs after successful association between station and access point. The station first passes Open System authentication (IEEE 802.11) then associates with access point and then initiates EAP authentication. On successful authentication both the station and access point have a set of keys to encrypt the traffic between them. The whole process is displayed in Figure 12.

Here can be seen that the initial IEEE 802.11 discovery/authentication/association is not protected, either by authentication of encryption. This can lead to denial-of-service attacks.

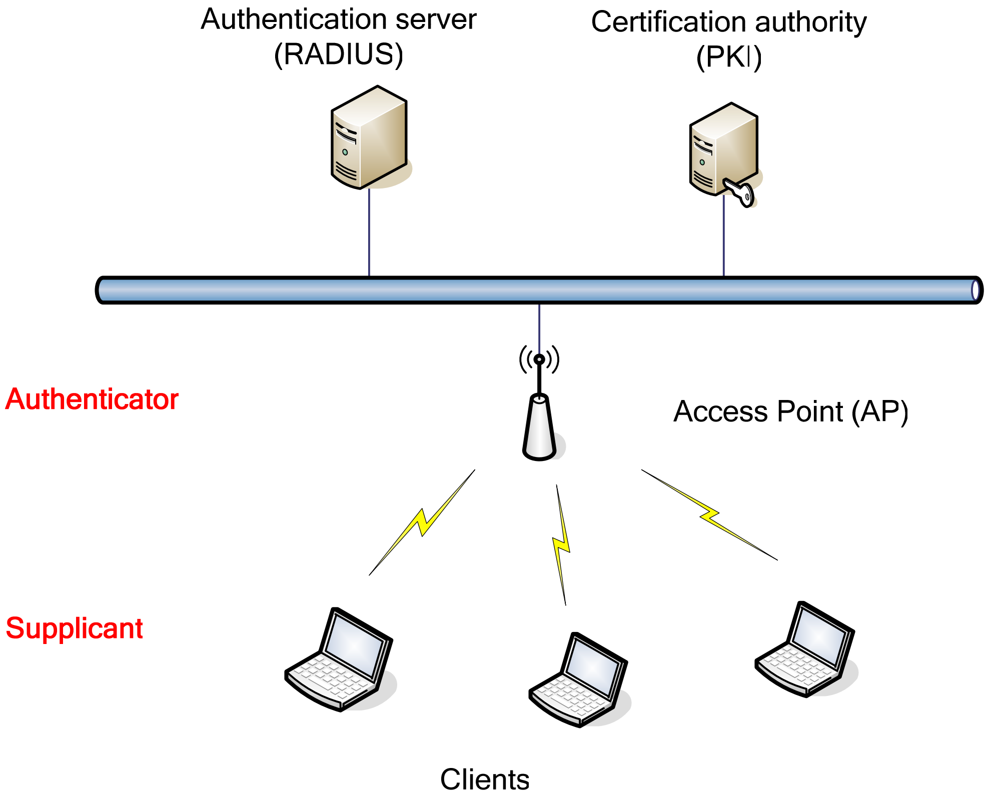

Figure 11 – EAP architecture

A number of protocols can be used to authenticate the users. The list of protocols with some details can be found in Table 3.

For this authentication scheme to work the access point must support the 802.1x authentication. The support of the authentication protocols is a matter of client and server capabilities.

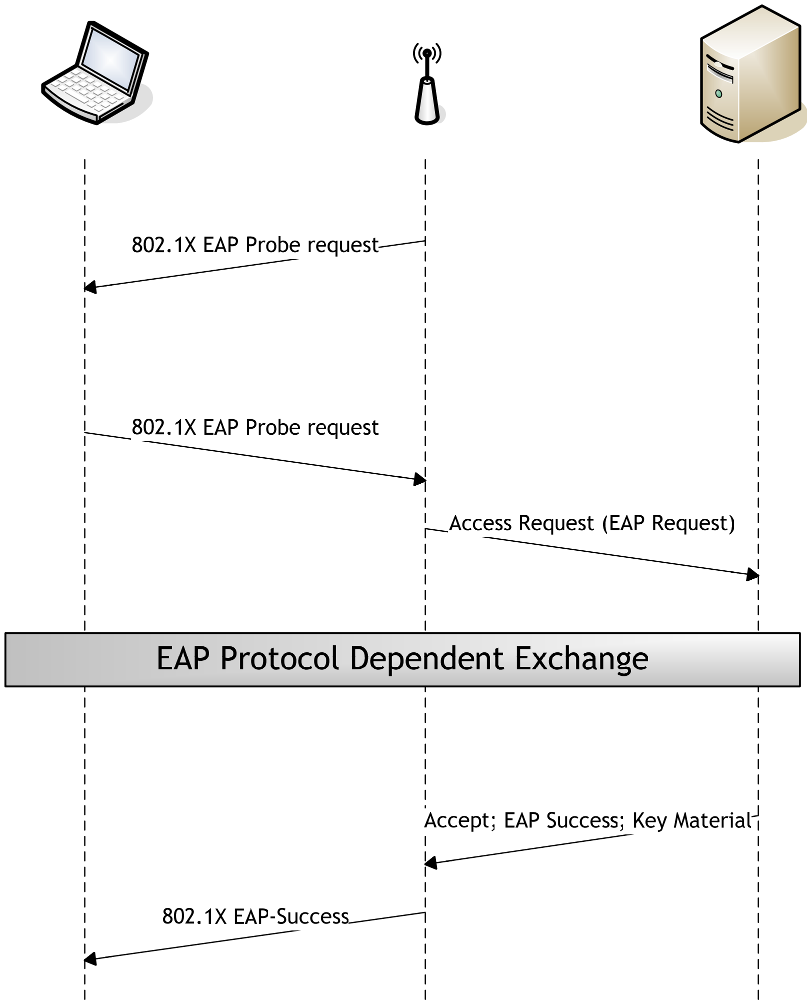
802.1X EAP Probe request
802.1X EAP Probe request
Access Request (EAP Request)
EAP Protocol Dependent Exchange
Accept; EAP Success; Key Material
802.1X EAP-Success

Figure 12 – EAP authentication sequence

Table 3 – EAP protocols overview

	Authentication method	Client authentication	Server authentication
LEAP	MS-CHAPv2		
EAP-FAST	MS-CHAPv2	PAC	
PEAP	MS-CHAPv2		Certificate
EAP-TLS	X.509	Certificate	Certificate
EAP-TTLS	CHAP, PAP, MS-CHAP, MS-CHAPv2		Certificate

4.2.7.1 Lightweight EAP (LEAP)

LEAP is a proprietary EAP protocol developed by Cisco Systems, Inc. in 2000. It should enhance the security of their access points when compared with WEP. It now has a quite big market share. In 2003 Cisco began licensing the technology to other manufacturers.

LEAP relies on MS-CHAPv2 for authentication purposes. The MS-CHAPv2 exchange is not protected in any way from eavesdropping. The problem of MS-CHAPv2 is that it does not use salt, and uses a weak 2 byte DES key, and username is sent in cleartext. This makes MS-CHAPv2 fundamentally weak and susceptible to offline dictionary attacks. But MS-CHAPv2 was not designed to be used over a public medium like wireless.

With pre-calculated databases of common passwords hashes the password can be cracked within seconds, since it only requires a dictionary lookup.

Pros: mature and established, good client side support

Cons: low security, proprietary, Cisco dependent

Conclusion: Unsuitable for new deployments

4.2.7.2 EAP-TLS

Currently the most secure EAP implementation is EAP-TLS which utilizes full client-to-server and server-to-client certificate authentication, to ensure the identity of server and client. Only after checking the identity (authenticating) the user the authorization service can enable the communication of the station and issues a key for usage.

First the authentication server presents its certificate to station, then when the user trusts the certificate the user sends his client certificate to the server. The usage of client certificate can be protected by a passphrase or can be stored on an authentication token for added security.

The downside of this approach is that the identity of user is not protected. The client certificate can be extracted from the authentication communication. And since user certificate contains data such as name of user, his login name or both, it can be used to track information such as user habits and work time plan.

Another disadvantage of EAP-TLS is need for a complex PKI. Secure issuing of server and user certificates must be created. Also client certificates must be revoked when users have their access to wireless network revoked.

Pros: very secure, does not rely on remembering password

Cons: hard to deploy, does not protect user identity

Conclusion: A very secure solution suitable for companies that already have a PKI/Smart card infrastructure deployed, or plan to deploy.

4.2.7.3 EAP-TTLS and PEAP

EAP-TTLS and PEAP were developed in response to PKI barrier in EAP-TLS, where deploying a PKI for user authentication can be quite complex task. So the goal with EAP-TTLS and PEAP was to design a protocol with comparable security but that is easier to deploy by using older authentication mechanisms.

Both EAP-TTLS and PEAP are two-stage protocols. In first stage they establish a secure connection. The secure connection is provided through a TLS tunnel that is opened between the supplicant and authentication server. Then the authentication server is authenticated using its server certificate. In second stage the client authentication credentials are exchanged.

EAP-TTLS uses the TLS channel to exchange attribute-value pairs. This encoding allows EAP-TTLS to authenticate users using all methods defined in EAP as well as several older methods such as PAP, CHAP, MS-CHAP, MS-CHAPv2. EAP-TTLS can be easily extended to implement new authentication protocols by defining new attributes to support them.

PEAP also uses the TLS tunnel to secure a second EAP exchange. So authentication is performed using a protocol that is defined for use with EAP. This includes all major authentication protocols such as MS-CHAPv2. The main difference between PEAP and EAP-TTLS is that EAP-TTLS has wider implementation base. PEAP is pushed mainly by Microsoft. But that changed now and PEAP clients are also available for Linux and Mac OS X.

Pros: secure, quite easy to deploy, protects user identity

Cons: requires PKI for server authentication

Conclusion: A very good solution also for environment that require user identity protection.

4.2.7.4 EAP-FAST

EAP-FAST was created as a successor to LEAP by Cisco to strengthen the security. Cisco claims that EAP-FAST is as easy to deploy as LEAP and as secure as PEAP. It uses a TLS protected tunnel, the same as PEAP, to protect the authentication credentials. The reason EAP-FAST should be easier to deploy is that there is no need for a PKI to authenticate the authentication server.

EAP-FAST is a two stage protocol. First it establishes a secure tunnel using TLS. The second stage uses MS-CHAPv2 to authenticate the client to the authentication server. The difference between PEAP and EAP-FAST is that PEAP uses a server certificate and EAP-FAST uses Protected Access Credentials (PAC) shared secret to setup the tunnel. A unique user specific PAC is generated from EAP-FAST Master Key on the authentication server for each user.

The problem is distributing the PAC to users. The distribution of PAC is called Phase 0 and can be done automatically using Automatic Provisioning or using other out-of-band methods such as file share. For EAP-FAST to be as secure as PEAP the Phase 0 would require a server-side authentication which requires server certificate. In this case the requirements are the same as for PEAP. One the other side the PAC provisioning can be done using anonymous Diffie-Hellman mode. In this case there is no way of detecting who is on the other side. So a man-in-the-middle attack is possible. But even this is much improvement over LEAP, because the Phase 0 occurs only once, and if it completes successfully then the future authentication is secure as PEAP.

The problem is that all the PACs have to be distributed to stations that need the network access. For big networks this is very cumbersome and much harder and time consuming then PEAP or EAP-TTLS deployment.

Pros: more secure then LEAP

Cons: Cisco proprietary protocol, harder to deploy on large scale, confusing provisioning options

Conclusion: It is definitely a better protocol then LEAP but without a server certificate it is not as secure as PEAP and is very hard do deploy on large scale. When a server certificate is available it is as secure as PEAP or EAP-TTLS but has not got the operating system support as those two protocols, because it uses Cisco proprietary software for authentication.

4.2.7.5 Conclusion

From all analyzed EAP protocols the best is EAP-TTLS – it is easy to deploy, has good support throughout the operating system spectrum and provides sufficient security for most deployments. The only more secure protocol is EAP-TLS but because the complexity of deployment it is only justified when a company has already a full-fledged PKI for authentication deployed or it requires very high security. The level of security can be increased even more if the certificates and privates key are stored on secure tokens.

5 Attacks

5.1 Overview

Attacks against wireless networks can target any part of the whole infrastructure and target any layer. On physical layer the attacks can employ interference generators to disrupt the communication. On data link layer the attacker can mount attacks to eavesdrop, deny service, spoof identity and many more. A hacker can also target the authentication process, EAP authentication and so on. The more complex the infrastructure is, the more weak points can the whole network have.

5.2 Attack types

There are many types of attacks known today. They can be categorized by their properties such as by their target (ISO/OSI Layer, specific protocol), or whether they need to actively participate in exchange (active or passive attacks) or what aspect of security they try to defy (privacy, authentication, availability).

Passive attacks are virtually undetectable, the attacker just collects data from the network and then analyze it and gain access to the network for example. On the other hand active attacks require active participation of the attacker. Therefore they are harder to perform and can be detected by certain fingerprints. The example of this attack is setting up a rogue access point. The fingerprint of this attack is the beacon frames sent by the rogue access point.

5.3 Layer 1 attacks

5.3.1 Interference

Because 802.11 wireless networks operate in public frequencies, there are many other devices that use the same frequency band as these networks. Among these are cordless phones, Bluetooth® devices or garage gate openers. Other devices do not operate in the same frequencies as wireless networks but spread a wideband EM interference covering the 2.4 GHz or 5 GHz band thus disrupting the operation of networks, such as microwave ovens, which can reliably disrupt all wireless communication in area.

There can be also devices constructed specifically to disrupt communication in certain frequencies. These can be very compact, battery powered and easily concealable.

When planning a wireless network, all types of interferences must be accounted for – both the intentional and unintentional ones. The initial map of interferences is produced during site survey. It contains signal and noise strength in an area and a list of wireless devices that operate there.

5.4 MAC sublayer attacks

Here are some attacks that abuse weaknesses of the IEEE 802.11 network design. These attacks can use the design flaw that management and control frames are not encrypted or authenticated and they can be easily spoofed. They lead to various Denial of Service attacks and can easily render the whole network unusable. Also these attacks are hard to trace, because many auditing tools do not log (or cannot log) the 802.11 control and management frames. Therefore these attacks can pass unnoticed.

An example of such attack was implemented in program AirJack or WLANJack. It continuously broadcasts deauthentication frames with the spoofed MAC address of the access point. That results in station being deauthenticated from network. This renders the network unavailable, because users cannot reassociate with the access point.

With proper tools these attacks are easy to detect, because they produce large number of mentioned frames at a high rate. When a network operates normally the number of these frames is very low, so any sustained increase in that kind of traffic signals and attack in progress.

5.5 WEP attacks

These attacks target the WEP security protocol. The ultimate goal of the attacker is determining the secret WEP key to gain access to the network and ability to read all traffic.

Over the time many tools were developed to crack the key. They work by collecting frames from wireless network and then analyze them to determine the key. First tools needed millions of captured frames but the most recent tools need only few hundred thousands to crack any WEP key.

All of these attacks can be passive so they are unable to detect. The attacker only collects the frames and then he can analyze them offline. Because of this WEP is regarded as insecure for all new installations.

For more about WEP attacks see 4.1.1.2.

5.6 WPA-PSK attacks

As TKIP became available it instantly became the target for attacks. Time showed that TKIP is much more robust then WEP. But there are some problems also with the personal version of TKIP with PSK authentication. When WPA-PSK came out it was presented as very secure protocol that does not use the passphrase to encrypt traffic, so that there is no traffic to be captured that could reveal the secret passphrase. So the impression was that the passphrase could be anything, event a simple word. After all that as what word passphrase evokes in most peoples' minds.

But this made WPA-PSK susceptible to dictionary attack. When intercepting one authentication exchange, the attacker can then run a offline dictionary attack to guess the secret key.

So this attack is passive but it can be prevented by using very long passphrase (more than 20 characters).

5.7 EAP attacks

The compromise of data when using EAP is harder then using other protocols. It can be aimed at stealing user credentials to gain access to the network or at reading the data transferred over network. The advantage of EAP is that each user has a separate key so a compromise of security credentials of one user only allows the attacker to gain access to the network but not to read all traffic.

Currently only LEAP is susceptible to a dictionary attack. Using a tool called ASLEAP and an attached dictionary the tool can discover passwords within seconds. Other more advanced protocols that protect the authentication process using a secure tunnel are not susceptible.

Other type of attack uses rogue authentication server or man-in-the-middle attack to get to the authentication data transferred inside the tunnel. This attack is only possible if the authentication server does not authenticate itself using a server certificate.

6 Wireless security devices and tools

6.1 Firewall

When the security of network is not sufficient, the wireless network should be treated as outside network. By explicitly specifying only protocols that can pass into trusted part of the network, the security can be partially enforced.

For example by allowing only:

- HTTPS intranet access,
- HTTP for outside internet
- IMAPS for access to company mailbox.

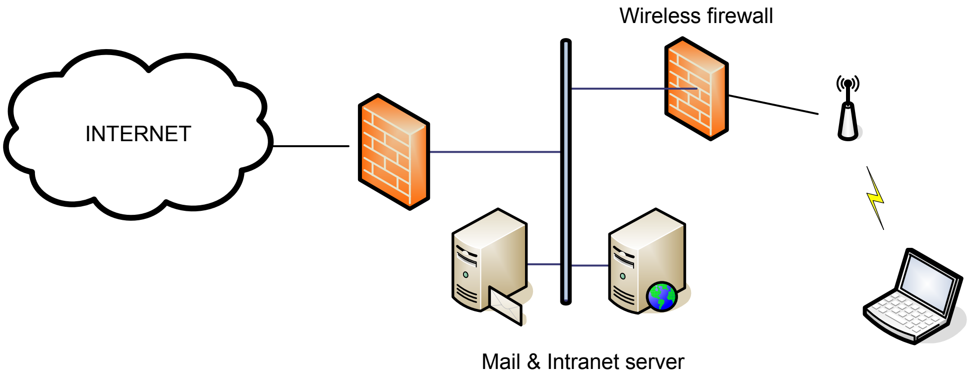

Figure 13 – Limiting wireless communication with firewall

6.2 Probes and loggers

Probes are used to collect wireless traffic from environment. The data is sent to central repository where it can be evaluated. This part of infrastructure is essential for detecting attacks and monitor network operation. From the consolidated traffic an attack can be localized and triangulated.

Probes are proprietary hardware devices that are connected to a central logging server, where they forward all traffic. Loggers are programs that can store and forward wireless traffic in promiscuous mode. The most prominent member is open source program Kismet.

6.3 Intrusion detection systems (IDS)

Intrusion detection systems or especially wireless intrusion detection systems analyze incoming to detect attacks in progress. To achieve this they can have a database of attack fingerprints or use heuristics to detect inappropriate content for specified protocol that could possibly be a new kind of attack. IDS do not prevent attacks they just detect them and alert the operator.

Wireless IDS should be able to detect all attacks mentioned here, such as replay attacks, rogue AP detection (when supplied with a list of valid AP MAC addresses), DoS attacks etc.

6.4 Authentication servers

Authentication servers are used in 802.1x scenarios. They authenticate users against an existing directory service (Active Directory, LDAP, relational database of users). In network topology the authentication server and directory service server should be located on the same local networks, because any additional delay when authenticating a wireless user is not desirable and communication between authentication server and directory service server can consume many resources. The alternative is that the authentication server should be able to cache user credentials to save bandwidth and speed up reauthentication process.

Authentication servers should also support a variety of EAP protocols, to suit for various scenarios and security requirements.

7 Case studies

7.1 Home network

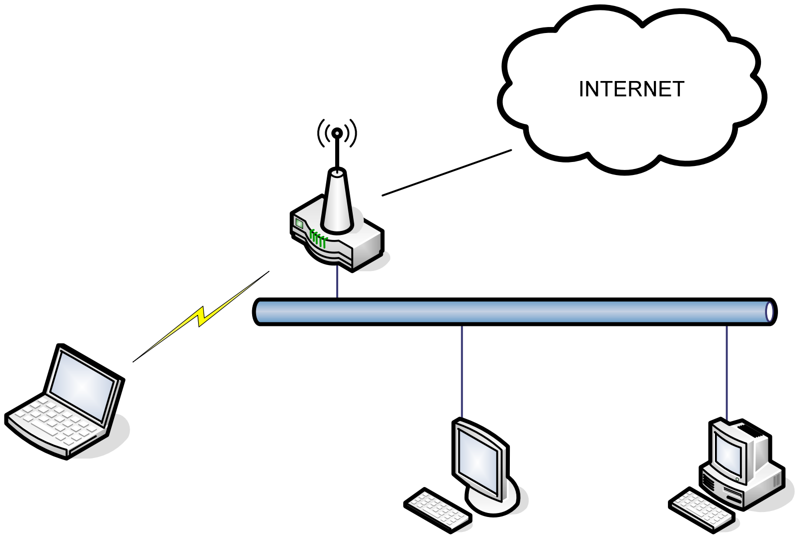

Figure 14 – Home network topology

7.1.1 Analysis

Home networks are build in homes or home offices. They are used to share broadband internet connection or data among computers located in homes or home offices. The motivation for building these networks using wireless technology is the ease of deployment, mobility and cost. The centre of the network is usually a wireless router which serves here as a gateway to Internet, wireless access point and provides services such as Dynamic Host Configuration Protocol (DHCP) and Network Address

Translation (NAT). The computers then connect to this wireless router using a wired or wireless connection.

Number of computers in home networks rarely exceeds 10. And all of the computers can be managed by the same person. Because of this key management is not a major issue, because keys can be easily distributed and updated manually. This can be cumbersome, but if employed with an encryption scheme does not need updating the keys frequently, it is acceptable.

The other requirement is that the network should not be easily found. When occasional passing by wardriver does not detect the network, the probability of an intrusion or eavesdropping drops dramatically.

7.1.2 Solution

For encryption WPA with long passphrase should be used. The best would be if the passphrase is random. It should be at least 20 characters long, since each letter hold only 2.5 bits of information (see 4.2.6). So a 20 character passphrase will provide 64 bits of security. This should be enough for most home use wireless networks. For more paranoid users or deployments in dense urban areas with high concentration of wireless networks and possible attackers a longer passphrase can be used or it can be changed periodically.

To other effective countermeasures count limiting the output power of the access point's and stations' transmitters. When signal does not reach outside the premises it is hard to detect the network or eavesdrop on the signal. But it must be kept in mind that control frames are transferred at lower bit rates and can be detected from greater distance then data frames. Also disabling ESSID broadcasting and other ESSID masking/cloaking techniques can be useful, since networks using these do not show up in NetStumbler listings. This decreases the possibility of detecting the network by passing wardriver.

To detect attacks and misuses of the network there is not much to be done with this infrastructure. Most wireless access points can log DHCP requests; some feature a firewall or simple intrusion detection system. These features should be employed to detect and prevent intrusions.

7.1.3 Conclusion

Since home networks cannot provide strong authentication and encryption based on 802.1x, without significant investment into infrastructure (dedicated RADIUS server), it cannot withstand a sustained effort to break in by an experienced intruder. But such sustained attack is not very probable, since the value if the data is not very high.

If the network contains sensitive data it should be protected by other means, that are not specific to wireless network, such as using secure protocols to transfer data, protect computers by firewalls etc.

7.2 Corporate network

7.2.1 Analysis

Corporate networks contain many computers, some of which use wireless network as a connection medium. Among users who usually use wireless network are managers and IT department employees. These users work with sensitive valuable data, so securing wireless access is a must in this scenario.

Also availability is very prominent, because wireless access may be the only network connection for some employees.

7.2.2 Risks and possible attacks

A large network can be attacked from many vectors and using various techniques. It can be also attacked from inside by employees, either intentionally or unintentionally, by clients or subcontractors that have access to premises or by external attackers.

Setting up an unauthorized access point by an employee is an example of unintentional breach in security. This can happen because the employee does not have full bandwidth or for other reasons. Then it can happen that the access point is left with default configuration and open for attack without any authentication or encryption. Other problem can occur when a device is left to associate with other devices in ad-hoc mode. This connection bypasses the security policy and so the device poses a security risk.

An attacker can employ the whole range of attacks as described in chapter 5. The methods for attacking these networks can be more sophisticated, because the cost of the data that is transferred can be significant. These networks can be target of variety of attacks aimed to compromise the data, gain access to the network or render it unavailable. Some of these attacks can be performed from great distance others can be executed using small specialized devices, used to monitor and collect data or disrupt network traffic.

When a device to disrupt the operation of the network is planted in the network, it can be easily detected, but it can be very hard to locate. It can possibly very small and easily concealable. To locate such devices enterprise solutions exist, where each access point logs suspicious frames and the logs can be evaluated in a central point.

The rogue device can be localized using two methods. The first simple one is determining which access point or agent sees the traffic and that means that the device is near it. The more sophisticated method is triangulation. It can be used when more then one device sees the traffic. Using a site map can be then determined the most probable location of the rogue device. It should be said that the device does not need to be on the same floor.

7.2.3 Solution

Large corporate networks can employ complex infrastructure to ensure the required level of security. But that does not mean that they should forget about the simplest security means such as monitoring signal range. This is because the wireless networks are as of now vulnerable to Denial of Service attacks using spoofed management frames.

7.2.3.1 Planning

So the first step in deploying a wireless network is a site survey and mapping where we want signal and where to place access points and what types of antennas to use. The access point can be places in the edge of the building/site but then a sector antenna facing into the building should be used, so that the signal does not reach outside of the building and that the antennas do not pickup signal from unprotected areas (e.g. nearby park, lobby, publicly accessible cafeteria). So area covered by wireless network needs to be physically protected to allow access of only authorized persons. But this can only minimize the risk of network compromise not entirely mitigate it, because own employees can sabotage the network, they can carry devices planted by attackers on them or staff (cleaning, maintenance or guarding service) can smuggle these devices inside. Because of this no IEEE 802.11 compliant wireless network can be protected. This is the inherent flaw of the protocol.

7.2.3.2 Site Survey

The first step when creating a bigger wireless network is a site survey. Its purpose is to determine the coverage of the signal and the signal to noise ratio and packet loss ratio. It can also produce a list of unauthorized access points in range; identify sources of interference and leakage of signal into outside area.

The result of site survey is a plan of coverage drawn on the flood plan, with signal strengths and/or packet loss ratios. Site survey can also produce list and positions of interfering devices (microwave ovens, cordless phones etc.) and list of external wireless devices. This includes first and foremost access points that the employees should not associate with.

7.2.3.3 Infrastructure

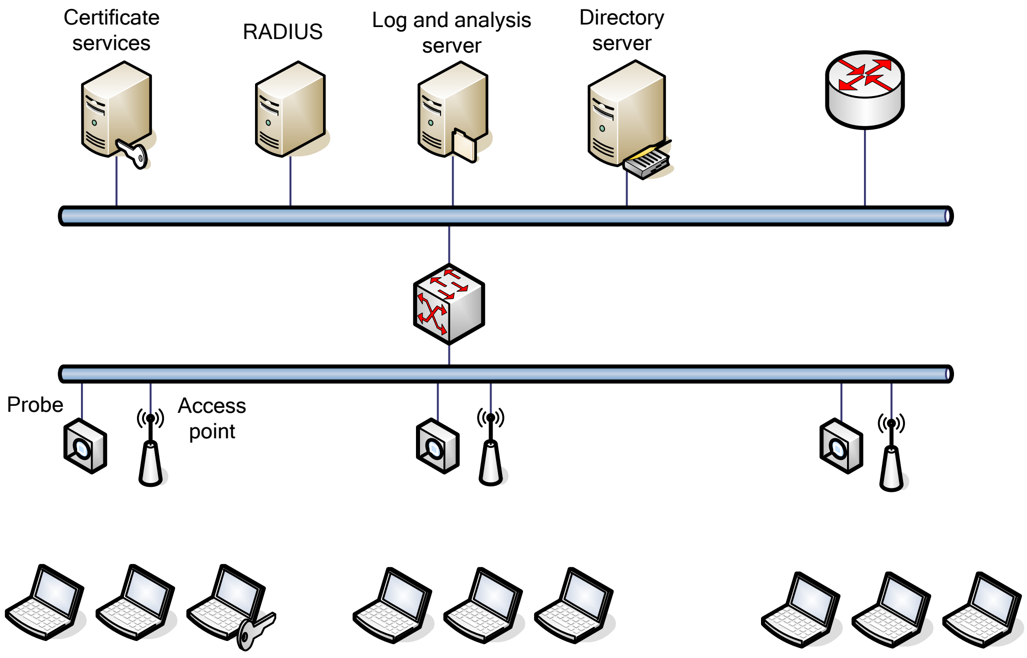

Figure 15 – Corporate network topology

Enterprise networks require complex infrastructure to achieve desired level of security. For authentication purposes a directory service is required to hold authentication data for all users that are able to logging on to network. RADIUS server serves as point of authentication for wireless access clients.

To ensure the authenticity of RADIUS servers and/or to provide certificates for users when using EAP-TLS a certificate service is needed. It issues certificates trusted throughout the enterprise to identify clients and servers.

For monitoring purposes the network should be able to collect data transferred over network for analysis. This can be done using a specialized agents/probes or if the access points provide this functionality then using them. The data is then stored, consolidated and analyzed on the log and analysis servers. These can then provide a list of unauthorized devices, access points, associations to rogue devices, active attacks (DoS attacks). It can also help in locating rogue devices by locating a nearest probe or triangulating its signal.

7.2.3.4 Protocols

Encryption and authentication scheme such as WEP or WPA-PSK are unsuitable because their lack of key management. When using these, the administrator would have to manually distribute the keys or use other out-of-band channel. There exist proprietary key distribution applications for WEP, but this implies additional cost and security of the key distribution mechanism cannot be proven most of the time becasue the solutions are proprietary closed source applications. There could also be problems with heterogeneous environments. Also the large number of WEP attacks makes WEP unsuitable for any usage. WPA-PSK is not as vulnerable as WEP but suffers from same key management issues and is susceptible to dictionary attacks. WPA-PSK was never meant to be an enterprise solution.

So the natural solution is using EAP for authentication and key management. When using EAP the encryption protocol and authentication protocol must be selected. Encryption protocol can be one of TKIP or CCMP. Authentication protocols should be selected from PEAP, EAP-TLS, and EAP-TTLS. The details of encryption methods and EAP protocols are covered in chapter 4.

The most secure from IEEE 802.1x protocol suite is EAP-TLS (for more information about EAP protocols see 4.2.7). The access points must support 802.1x to be usable with EAP. EAP-TLS uses strong server-to-client and client-to-server certificate authentication. The downside is that the deployment of a PKI suitable for this scenario can be quite difficult and prone to errors. Another one is that EAP-TLS does not hide the identity of the client, because the certificates are sent unencrypted. But the only information this reveals is only information contained in the certificate: user name, department. If this is not acceptable another protocol must be used (EAP-TTLS, PEAP).

In EAP-TLS every user connecting through wireless network must have its own client certificate. These must be issued by a trusted certification authority. It does and should not be a globally trusted CA. It can be a corporate CA used only to issue certificates to employees solely for EAP authentication purposes. This lowers the cost as compared to using public CA and gives control to issue certificates to the corporation.

The company should already have enterprise authentication established using Active Directory in Windows environment or some other LDAP or directory solution on other platforms. That way, users can be globally authenticated and identified throughout the enterprise.

The hardest part is to issue the certificates to the end users. One difficulty is to authenticate the users when they place the certificate request the other is to secure the communication between the client and RADIUS server prior to the deployment of certificate. One possibility is to deploy the certificate not using wireless connection but require the users to use wired connection. Other possibility is to use time restricted connection to network to acquire the client certificate. This requires that the RADIUS server can send a time restricted key to access point/client without prior authentication.

RADIUS server can act a single point of failure and can affect availability severely. It also performs complex cryptographic operations, so it can process only limited number of authentication requests per second. The average number of authentication can be computed by dividing the length of session in seconds by the number of users. For example when a session duration is set to 10 minutes and there are 50 wireless users on network the RADIUS server should handle 0,08 transactions per second. Table 4 displays required transactions per second for specified number of users and session duration.

Table 4 – Average RADIUS server load

Users	Session duration minutes	Session duration seconds	Session duration/ connection	Transaction/s
10	5	300	30.00	0.03
10	10	600	60.00	0.02
10	30	1800	180.00	0.01
10	60	3600	360.00	~ 0.00
100	5	300	3.00	0.33
100	10	600	6.00	0.17
100	30	1800	18.00	0.06
100	60	3600	36.00	0.03
1000	5	300	0.30	3.33
1000	10	600	0.60	1.67
1000	30	1800	1.80	0.56
1000	60	3600	3.60	0.28
10000	5	300	0.03	33.33
10000	10	600	0.06	16.67
10000	30	1800	0.18	5.56
10000	60	3600	0.36	2.78

So if a server can handle 40 request per second then it can support 10 000 users with 5 minute session timeout. So a single RADIUS server can handle a big corporate network. For bigger networks a more powerful server can be used or the performance can be achieved using multiple computers. The multiple computer approach also increases availability since the servers are redundant. The performance of a RADIUS server is highly dependent from the CPU performance, because it performs mainly cryptographic operations. According to Microsoft a Pentium II server can perform 200 CHAP authentication sessions per second and a 4-way Xeon III server up to 1000 authentication sessions per second. The creating of TLS tunnel can offloaded by external cards designed for this purpose. An EAP-TLS authentication requires approximately 20-30%

more processing time as compared to EAP-TTLS, so the number of transaction per second should be appropriately lowered.

Each access point has to have a list RADIUS servers specified. Some access points offer only one IP address of RADIUS server, while access points aimed at enterprise usage offer the configuration of multiple RADIUS servers for better scalability and availability. Several topologies can be used when having multiple RADIUS server based on their count and the capabilities of access points. Each access point used in enterprise networks should be able to be configured with two or more RADIUS servers. If this is not the case then IP load balancing should be used to forward the traffic to multiple servers. If the number of servers is lower then the maximum number of configured RADIUS servers in the access point, then all server addresses can be configured in the access point. Without using a management software that allows changing the setting for all access points this can be cumbersome to configure and lower the maintainability. The other possibility is to have a few RADIUS servers that are configured in the access points and have this server offload the authentication to next layer of RADIUS servers on demand.

7.2.4 Conclusion

From the identified risks some of them were fully addressed others were at least mitigated. Using probes, logging and analysis tools the use of rogue devices can be easily identified and deterred. Strong authentication and encryption can be provided by RADIUS server and EAP protocol. This addresses the key management issue and also provides method to limit access on user level. It also limits the compromise of the whole network when a security key for a user is stolen. Limiting session length using RADIUS server to a short period can make attacks on encryption methods impotent.

Protection against unauthorized devices and denial of service attacks is provided by monitoring the traffic. The source can be located in real-time and disabled, so availability should not be affected much. Combined with secured access to premises this danger can be lowered even further.

7.3 Public hotspot

7.3.1 Analysis

Public hotspots are a great way to provide internet connectivity in various public places such as airports, cafes or libraries. A user who is a client of an wireless internet provider can go into internet wherever the coverage is present. These users can be frequent users that use the hotspot network of a provider regularly or they can be one-time users that only pass through an airport and need an internet connection.

Current hotspot network use Universal Access Method (UAM) solutions to provide authentication and provide no traffic encryption. The only advantage of this approach is compatibility with all devices; the disadvantage is virtually no security at all. The user can only rely on higher layer security protocols such as HTTPS, TLS or IPSec to protect the communication. Without using an 802.1x authentication the users can either all have the same key or no key at all.

The highest priority when building wireless hotspots is security and privacy. The networks must be protected against external and internal attacks. After all, a user does not know anything about a neighbor sitting next to him on the airport. He may be very well someone whose only intention is to break into his or hers communication.

Also accounting is very important, since the provider needs to charge the users for using the connection. This can range from restricting user account validity to collecting the authentication and deauthentication events to provide detailed billing based on time spent on the network.

A hotspot network can serve potentially huge amount of clients. Because RADIUS server performs complex cryptographic computations it can become a bottleneck.

7.3.2 Risks and potential attacks

The most valuable asset on these networks is the data transferred by the clients. This includes their user data as well as their identities.

Next problem pose users who want to use the hotspot network without paying or registration. This leads to direct financial losses for the provider and should be avoided if possible.

And the problem common to all 802.11 wireless networks is the problem of availability. Low availability of network is undesirable and leads to unsatisfied customers.

In many countries providing a public hotspot network falls under the same legislation that covers public telecommunication networks. It is the same legislation that protects telephone networks or postal services. According to this law eavesdropping or helping someone to gain advantage by using information gained from messages that were not addressed to him can be fined with a very high monetary penalty or imprisonment. This is the difference between a privately owned network used for own purposes and a public network providing a telecommunication service.

7.3.3 Solution

7.3.3.1 Infrastructure

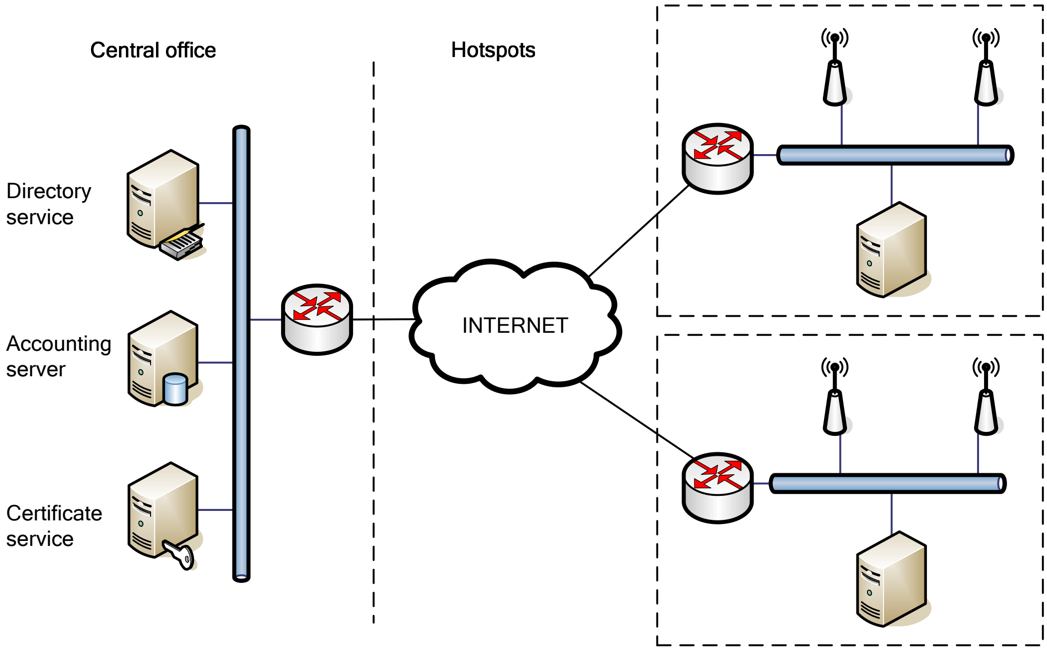

Figure 16 – Public hotspot topology

The architecture of the network should be decentralized, to avoid any single points of failure. Each hotspot should feature an own RADIUS server, to minimize traffic overhead and delay in authentication. Because the RADIUS session can be as short as few minutes and the number of users for a hotspot can reach several hundred for big hotspots the bandwidth consumed by the authentication process quite be quite significant. This also ensures scalability of the whole hotspot network.

The network core provides dictionary service for authenticating users, accounting services for billing purposes. It should also issue certificates for RADIUS servers used on hotspot locations.

Each hotspot location should have access points to provide wireless connectivity to clients. These access points are configured to authenticate against RADIUS server that is on the same local network as the access points. So the authentication runs over local network which saves bandwidth to the internet and speeds up the authentication process. The RADIUS server authenticates against the central directory service of the provider. The credentials should be cached to ease on the directory infrastructure the network.

7.3.3.2 Authentication

Other protocols then EAP are unsuitable for authenticating the potentially huge number of users. WEP or WPA-PSK protocols with a single shared secret do not provide the desired level of security. Therefore only an EAP protocol is suitable in this scenario.

The most commonly supported protocols from IEEE 802.1x are EAP-TLS, EAP-TTLS and PEAP. EAP-TLS is the most secure of all because it uses a client certificate for authentication, while the other two rely on username/passwords credentials. But this does not come without disadvantages. The deployment of PKI that is used for issuing and distribution for all clients can be quite demanding. The other disadvantage is that the client certificate if transferred in cleartext over the wireless network during the authentication. The revealing of client information is highly undesirable. Therefore the other protocols are better suited for this scenario. The usernames and passwords can be easily generated and transferred to clients. When setting reasonable password complexity requirements this solution can be quite resistant to dictionary attacks. This hold true even more when the usernames are also random and never transferred in cleartext. For details about EAP-TTLS and PEAP see 4.2.7.3.

Also high fluctuation of client would require large certificate revocation lists or issueing of many certificates for a limited time.

For one-time users or new users who do not have credentials to access the network a time limited session with limited access can be established. During this session user can establish either a one-time account or buy a subscription from the provider. After the expiration of the session the user can authenticate with the server using the new credentials.

7.3.3.3 Encryption

The encryption of frames can be provided by any of the standard protocols (WEP, TKIP, CCMP).

When using WEP the session length should be adjusted accordingly to limit the session length, so the key cannot be determined from eavesdropping of the traffic. Since WEP can be broken by collecting about 100,000 to 500,000 frames the session length should be limited to few minutes. When an average frame size would be 100 bytes, the limit would be reached in by transferring 10 to 50 MB of data. When providing a 1Mbps bandwidth to user the limit is reached in 1 to 6 minutes. This is the worst case scenario but it shows that the session length should not exceed 5 minutes.

By supporting the newer encryption protocols the session length does not need to be limited. This can relieve the RADIUS server from the frequent rekeyings when using WEP.

Since the TKIP support in operating system is growing it should be the protocol of choice for most hotspot networks.

7.3.3.4 Scalability and availability

The availability of hotspot networks is crucial as client will not use a network that experiences downtimes and is unreliable. With the wireless networks open to DoS attacks and without qualified support personnel on-site the monitoring a reporting of incidents should be fully automated.

Traffic which is relevant from security standpoint should be logged and analyzed for attack fingerprints. These include deauthentication storms, beacon frames from access points trying to spoof the hotspot network etc.

7.3.4 Conclusion

From all identified need and risks all were addressed fully, except the availability issue. The protection of user identity can be achieved using PEAP or EAP-TTLS protocol that hides the authentication credentials in a TLS tunnel. The spoofing of authentication server or establishing a rogue access point could be mitigated using server certificate to authenticate the RADIUS server and logging service to look for rogue access points.

The ability of the users to access the network without prior payment can be achieved using time or access restricted session to allow the user to purchase credit or subscription.

The availability issue can be partially solved by logging and IDS. But disabling a device that affects the availability, either by interference or DoS attack, must by done manually by an operator, since the network infrastructure can only detect the attack and raise an alert.

8 Conclusion

The goal of this work was to provide a comprehensive guide into wireless network security. We wanted to analyze current status of security protocols that can be used in wireless environment, look at types of attacks that can target these networks and propose solutions for some common wireless network applications.

In chapter 4 we have described authentication and confidentiality protocols. We found out that although there are protocols unsuitable for any deployment such as WEP the introduction of new security protocols can raise the security level considerably. We also evaluated all authentication protocols, including WPA-PSK and EAP protocols. We found out that WPA-PSK is suitable for small deployments, while EAP protocols such as EAP-TLS and EAP-TTLS are right for big deployments in large enterprises or public networks.

In chapter 6 we provided a brief description of attacks against wireless networks and identified an inherent flaw in the protocol that allows easy denial of service attacks against any wireless network. We proposed solution to alleviate the availability implication of this problem. We also described attacks against confidentiality and authentication protocols that can be used in wireless networks.

In the last chapter (7) for the proposed network applications (home network, corporate network, public hotspot network) we analyzed the needs, risks and possible attacks. Then we proposed a solution and analyzed whether it solved all identified problems (either completely or partially). We found out that all proposed usages can be sufficiently secured.

9 Záver

Cieľom tejto diplomovej práce bolo poskytnúť prehľad bezpečnosti bezdrôtových sietí IEEE 802.11, pozrieť sa na bezpečnosť s komplexného hľadiska, čiže zaoberať sa nielen dôvernosťou prenášaných dát, ale aj autentifikáciou, autorizáciou a dostupnosťou týchto sietí.

Motiváciou na vznik tejto práce bolo, že bezdrôtové siete zaznamenali v posledných rokoch veľké rozšírenie, keď sa zariadenia na nasadenie týchto sietí stali veľmi dostupnými. Žiaľ, bezpečnosť týchto sietí zostáva na veľmi nízkej úrovni. Pri krátkom prieskume v Bratislave sme zistili, že z asi 100 nájdených bezdrôtových sietí bolo viac ako 80 % absolútne nezabezpečených. Medzi týmito nezabezpečenými sieťami sa objavovali aj podnikové siete veľkých spoločností. Preto sme chceli zistiť, či je problém zavinený technológiou, alebo či sú prostriedky na zabezpečenie týchto sietí dostupné a vina je v ľudskom faktore – neznalosťou technických pracovníkov, nedostatkom peňazí alebo podcenením tohto problému.

Preto sme chceli popísať bezpečnostné protokoly, ktoré môžu byť použité na zabezpečenie týchto sietí, a to nie len z portfólia protokolov definovaných v IEEE 802.11, ale aj iných protokolov (napríklad IPSec, PPTP, L2TP), analyzovať ich slabé a silné stránky a posúdiť ich vhodnosť pri nasadzovaní. Ďalej sme chceli poskytnúť prehľad o možných typoch útokov a spôsoboch ako ich odhaľovať.

Naším cieľom bolo navrhnúť riešenia, ako zabezpečiť určité modelové situácie pri nasadzovaní bezdrôtových sietí, analyzovať ich požiadavky a riziká, ktoré sa môžu vyskytnúť, a nakoniec vyhodnotiť naše navrhované riešenia z pohľadu, ako splnili zadefinované požiadavky.

V kapitole 1 sme poskytli pohľad na bezpečnosť a jej jednotlivé aspekty. V kapitole 3 sme sa pozreli na prehľad architektúry bezdrôtových sietí, noriem, ktoré tieto siete definujú, princípy fungovania, typy a použitia rámcov.

Kapitola 4 popisovala protokoly na zabezpečenie dôvernosti prenášaných dát a na autentifikáciu používateľov. Ukázali sme, že pri vzniku existujúci protokol na zabezpečenie dôvernosti WEP je nedostatočný a napadnuteľný množstvom spôsobov. Toto zmenil dodatok IEEE 802.11i, ktorý IEEE ratifikovala v roku 2004, ktorý priniesol nové protokoly na zabezpečenie dôvernosti (TKIP a CCMP), vhodné na ochranu prenášaných dát. Taktiež sme ukázali, že protokoly IPSec, PPTP a L2TP nie sú vhodnejšie na zabezpečenie aj z dôvodu, že pracujú na vyššej vrstve ISO/OSI modelu a toto pri povahe bezdrôtového spojenia, ktoré môže byť často prerušené kvôli interferenciám, môže vyžadovať opakované vytvorenie bezpečného kanálu, ktoré tieto protokoly používajú. Tieto protokoly navyše majú vyššie režijné náklady.

Na poli autentifikačných protokolov priniesol dodatok IEEE 802.11i zlepšenie v podobe protokolu WPA-PSK, ktorý je vhodný na použitie v malých sieťach a použití protokolov EAP definovaných v IEEE 802.1X. Tieto sú vhodné na použitie vo veľkých sieťach. Umožňujú pridelenie rozdielnych prihlasovacích údajov pre každého používateľa a rovnako aj použitie rôznych kľúčov na šifrovanie prenosu. Najvhodnejšími protokolmi sú EAP-TTLS a EAP-TLS. EAP-TLS je najbezpečnejší protokol, ale vzhľadom na zložitosť nasadenia je vhodný najmä pre firmy, ktoré túto bezpečnosť vyžadujú alebo už majú nasadenú autentifikáciu na existujúcich systémoch pomocou PKI alebo čipových kariet. Pre iné použitie je potom vhodnejší EAP-TTLS.

V kapitole 5 sme urobili prehľad útokov, ktoré môžu smerovať na bezdrôtové siete. Analyzovali sme útoky podľa cieľa ich útoku (vrstva ISO/OSI modelu alebo protokol), podľa toho či sú aktívne alebo pasívne, a ktorý aspekt bezpečnosti napádajú (autentifikáciu, dôvernosť, dostupnosť). Zistili sme, že bezdrôtové siete obsahujú chybu, ktorá vyplýva z ich návrhu v IEEE 802.11. Táto chyba sa nedá odstrániť a umožňuje útočníkovi prerušiť chod siete posielaním falošných deautentifikačných rámcov. Predstavili sme riešenie, ako tieto útoky odhaľovať a minimalizovať tak ich dopad.

V kapitole 7 sme sa pozreli na prípadové štúdie bezdrôtových sietí. Rozanalyzovali sme domácu sieť, veľkú podnikovú sieť a sieť bezdrôtových hotspotov. Určili sme bezpečnostné požiadavky, ktoré treba splniť a navrhli ich riešenia. Všetky prípadové štúdie sa nám podarilo navrhnúť tak, aby splnili vytýčené nároky. Jediný problém, ktorý sa nám nepodarilo úplne spoľahlivo vyriešiť boli problémy a dostupnosťou, ktorý vyplýva z návrhu bezdrôtových sietí.

Abbreviations and acronyms

AAA	Authentication, Authorization, Accounting
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
ARP	Address Resolution Protocol
BSS	Basic Service Set
CCMP	Counter-Mode Cipher Block Chaining Message Authentication Code Protocol
CHAP	Challenge-Handshake Authentication Protocol
DES	Data Encryption Standard
DoS	Denial of Service
EAP	Extensible Authentication Protocol
EAPOL	EAP over LAN
ESS	Extended Service Set (see 3.4.3.2)
ESSID	Extended Service Set Identifier
FCS	Frame Check Sequence
IBSS	Independent Basic Service Set (see 3.4.3.1)
IDS	Intrusion detection System
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IPSec	IP Security, see [7] for complete specification
IV	Initialization Vector
L2TP	Layer 2 Tunneling Protocol
LEAP	Lightweight Extensible Authentication Protocol
LLC	Logical Link Control
MAC	Message Authentication Code or Media Access Control
MD5	Message Digest 5, a standard hash algorithm
MSDU	MAC service data units
PAP	Password Authentication Protocol
PHY	Physical Layer in ISO/OSI model
PHY	Physical layer
PKI	Public Key Infrastructure

PMK	Pair-wise Master Key (see 4.1.2)
PPTP	Point-to-Point Tunneling Protocol
PTK	Pair-wise Transient Key (see 4.1.2)
RADIUS	Remote Authentication Dial-in User Service
RC4	Symmetric stream cipher designed at RSA Laboratories
RSA	An asymmetric cipher developed by Rivest, Shamir, and Adelman
SSL	Secure Sockets Layer
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
UAM	Universal Access Method (see 4.2.5)
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy (see 4.1.1)
WPA	Wi-Fi Protected Access

Bibliography

[1] ANSI/IEEE Std 802.11, 1999 Edition, Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications

[2] IEEE Std 802.11i™-2004 IEEE Standard for Information Technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications – Amendment 6: Medium Access Control (MAC) Security Enhancements

[3] Townsley, W., Valencia, A., Rubens, A., Pall, G., Zorn, G. and B. Palter. RFC 2661: Layer Two Tunneling Protocol 'L2TP', August 1999.

[4] Assigning Certificates to Domain Members via Autoenrollment in a Windows Server 2003 Active Directory Domain

http://www.tacteam.net/isaserverorg/exchangekit/2003autoenroll/2003autoenroll.htm

[5] D. Whiting, R. Housley, N. Ferguson. RFC 3610: Counter with CBC-MAC (CCM), September 2003

[6] EAP-TLS Deployment Guide for Wireless LAN Networks, Cisco http://www.cisco.com/en/US/tech/tk722/tk809/technologies_white_paper09186a008009256b.shtml

[7] R. Thayer, N. Doraswamy and R. Glenn. RFC 2411: IP Security – Document Roadmap, November 1998

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

[9] TakehiroTakahashi . WPA Passive Dictionary Attack Overview

[10] Matthew Gast. 802.11 Wireless Networks: The Definitive Guide. O'Reilly, 0-596-00183-5, April 2002

[11] Christian Barnes, Tony Bautts, Donald Lloyd, Eric Ouellet, Jeffrey Posluns, David M. Zendzian, Neal O'Farrell. Hack Proofing Your Wireless Network, Syngress, 1-928994-59-8

[12] Frank Ohrtman Konrad Roeder. Wi-Fi Handbook: Building 802.11b Wireless Networks, McGraw-Hill, 0071412514

[13] George Ou. PPTP VPN authentication protocol proven very susceptible to attack

[14] IEEE Std 802.1X-2001, IEEE Standard for Local and metropolitan area networks – Port-Based Network Access Control

[15] Mikael Högquist, Manus Bondesson. Wired Equivalent Privacy or Why WEP Is Insufficient, April 2003