Security problems and solutions in WLAN access zones

Karri Huhtanen karri.huhtanen@wnsonline.net

10th May 2001

Contents

1 Introduction **4**

2 WLAN Access Network **5**
2.1 General . . . 5
2.2 Threats . . . 5
2.2.1 Eavesdropping . . . 5
2.2.2 Denial of Service . . . 5
2.2.3 Integrity . . . 6
2.3 Solutions . . . 6
2.3.1 WEP encryption . . . 6
2.3.2 IPSEC / VPN . . . 7
2.3.3 Intelligent network elements . . . 7
2.3.4 Network management . . . 7
2.3.5 Legislation . . . 7
2.4 Problems . . . 8
2.4.1 WEP encryption algorithm . . . 8
2.4.2 Access control and MAC address filtering . . . 8

3 Regional Access Zone **9**
3.1 General . . . 9
3.2 Threats . . . 10
3.2.1 Unauthenticated and unaccounted use of network . . . 10
3.2.2 Faked services and networks . . . 10
3.2.3 Attacks against network management . . . 11
3.3 Solutions . . . 11
3.3.1 IPSEC/VPN . . . 11
3.3.2 Routers, router filters and rules . . . 11
3.3.3 Security education for users . . . 12
3.4 Problems . . . 12
3.4.1 Fake networks and services . . . 12
3.4.2 IPSEC/VPN interoperability . . . 12
3.4.3 IPSEC/VPN architecture design . . . 13
3.4.4 IPSEC/VPN certificate management and distribution . . . 13

4 Public Access Zone **14**
4.1 General . . . 14
4.2 Threats . . . 15
4.2.1 Unauthenticated and unaccounted use of network . . . 15
4.2.2 Eavesdropping . . . 15
4.3 Solutions . . . 15
4.3.1 Public Access Controller (PAC) . . . 15
4.3.2 The vendor specific solutions . . . 16
4.4 Problems . . . 17
4.4.1 PAC authentication security . . . 17

4.4.2 Network Address Translation (NAT) 17
4.4.3 The vendor specific solutions 17

5 Corporate Access Zone **19**
5.1 General 19
5.2 Threats 20
5.2.1 Unauthenticated and unaccounted use of network 20
5.2.2 Denial of Service 20
5.2.3 Social attacks against users 20
5.3 Solutions 20
5.3.1 Firewalls, Public Access Controllers 20
5.3.2 WEP encryption 21
5.3.3 Company policies and standards 21
5.3.4 Personnel security training 21
5.3.5 Hardware evaluation and redundancy 21
5.4 Problems 21
5.4.1 Users 21

6 Conclusion **23**

7 References **25**

1 Introduction

Wireless LAN (WLAN) networks discussed in this report are presumed to be based on IEEE 802.11b standard. In the real world there are also WLAN networks operating on 2.4GHz unlicensed radio band that may be based on the old IEEE 802.11 standard, HiperLAN or vendor proprietary technology. Unlicensed means that the access for this band is not regulated by authorities with the exception of transmitting power and possible sequental interference the devices operating on this band may cause. The network consists on access zone level of an WLAN access point(s) and terminals equipped with WLAN cards. Current off-the-shelf WLAN access points are basically intelligent bridges with some filtering capabilities for protocols, MAC addresses and IP traffic. This report focuses on problems and solutions on MAC / IP address level especially in WLAN environment leaving the general radio path for less attention.

The content is divided first to overall description of WLAN access network and general threats, problems and solutions that may be found in all access zone scenarios. Then three different access zone case with invidual threats, problems and solutions are presented. For each access zone case there is first a general introduction, then the threats unique or important to the case, found solutions and the remaining problems. The report ends in conclusion that summarizes the threats and their existence in the different access zone cases.

2 WLAN Access Network

2.1 General

Access network is a concept from the Internet Service Provider (ISP) world based on thought that WLAN is only yet another completing access method among others like GSM/GPRS data, fixed line, UMTS data etc. access. The WLAN access network is a network of access points, public access controllers, routers, firewalls and security gateways. Because treating the whole WLAN access network as a single entity would be very confusing, the access network may be divided to access zones to clarify different methods to use the network. For example corporate users may have quite different needs for features and network security compared to residential/regional users who may just want to surf the web non-encrypted. This means there is already a need for two differently configured WLAN networks, namely corporate and regional access zones. By providing different kind of access zones the needs of different users and groups may be served better. An access zone is generally a radio access area consisting of one or several WLAN access points. These access points usually are part of the same bridged network segment so inside access zones the users may eavesdrop each other very easily.

The complexity of the network and the users' needs as well as technology itself create security threats that may be unique for each service/access zone case and must be dealed with so that the trade-off solution between ease-of-use and security satisfies both the users and the operator.

2.2 Threats

2.2.1 Eavesdropping

The most obvious threat for WLAN access network is eavesdropping. Eavesdropper may listen the traffic in real time or record it for future cryptoanalysis. This can be done on radio, link layer (MAC) or network (IP) level. The required mass storage space is nowadays quite easy and affordable to acquire (360GB disk space for 1400 euros, 25.4.2001 estimate). In Wall Street Journal's article [Gomes] Lee Gomes presents several examples of major software/network companies that haven't really paid attention to configuring / securing their WLAN networks. In the article two security specialists were able to just drive to the parking lot or past office buildings in Silicon Valley and gain access to WLAN networks just turning their laptop equipped with WLAN card. This way they were able to monitor email and web traffic even more easily than connecting to a fixed network.

2.2.2 Denial of Service

The WLAN access network is vulnerable to all denial of service attacks possible both in radio networks and TCP/IP networks. Also interference from other radio devices and access methods operating on same unlicensed 2.4GHz radio

band may be considered as a denial of service threat although not a malicious one. An example of non-malicious threat to performance of the 2.4GHz WLAN is Bluetooth. An active i.e. transmitting Bluetooth device may drop the WLAN performance so much the interference can be thought as denial of service threat.

2.2.3 Integrity

Integrity threats focus mainly on link and network level. Possible attacks are for example MAC address forging and IP hijacking. This can be done without serious effort with a normal WLAN card and Linux host. Looking from the user perspective the network authentication is inadequate or even non-existent. It is also possible to set up fake networks and access points and regular user may not notice anything wrong until he/she has already revealed sensitive data like user account and password giving the attacker this way means to infiltrate the user's home network.. Also all kinds of man-in-the-middle attacks like forging email, capturing SSH keys and feeding wrong keys are possible.

2.3 Solutions

2.3.1 WEP encryption

The WEP (Wired Equivalent Privacy) encryption algorithm is part of the IEEE 802.11 standard. Its primary function is to protect wireless communication from eavesdropping, but the secondary function is to prevent unauthorized access to wireless network although this was not thought as a goal when defining the standard.

If a user wants to connect with a WLAN device to the access point with WEP encryption enabled, the user must know the shared key and network name (called also ESSID) to do so. If the user doesn't know these, the user can't connect to an access point even on MAC level that would help eavesdrop the traffic.

> WEP relies on a secret key that is shared between a mobile station (eg. a laptop with a wireless ethernet card) and an access point (ie. a base station). The secret key is used to encrypt packets before they are transmitted, and an integrity check is used to ensure that packets are not modified in transit. The standard does not discuss how the shared key is established. In practice, most installations use a single key that is shared between all mobile stations and access points. More sophisticated key management techniques can be used to help defend from the attacks we describe; however, no commercial system we are aware of has mechanisms to support such techniques.
>
> *[BorGolWag2]*

There is a vendor specific solution from Cisco to change WEP keys between mobile nodes and access points without user intervention. This like all vendor specific solutions have the disadvantage of limiting the usable hardware to

one or few vendors, which is not acceptable in most Internet Service Provider environments.

2.3.2 IPSEC / VPN

Transferring the securing of traffic to IP level is probably currently the best choice to secure wireless traffic. Advantages are for example radio access independency. If one can run IP over radio path, one can run IPSEC. The encryption strength can be modified according to use by selecting the encryption algorithm and key length. Also now the access points do not need so much processing power as the encryption/decryption process has moved to IPSEC gateway/terminator.

Protecting the traffic from eavesdropping is not the only advantage of an using a IPSEC / VPN solution. IPSEC also brings certificates and secured key exchange where both parties, the user and the network, can ensure each other's identity. Of course this means they both have to trust to the Certificate Authority, who has signed the keys.

2.3.3 Intelligent network elements

Access to radio path, network elements and further to network may be controlled by network elements. For example WLAN access points from several vendors have the ability to filter the access to network based on client's MAC address. These rules may be entered in access point or the access point may retrieve them from authentication/settings database via RADIUS protocol. Here the built in security/encryption of RADIUS protocol secures the transfer. Some access points also have the capability to filter packets based on protocol, port number and destination address i.e. a limited firewall functionality.

2.3.4 Network management

Network management provides the means to detect and find some attacks. For example if the location of WLAN access points is known and the network management system alerts that certain three access points are overloaded. Then by using the location information, e.g. GPS coordinates, we may pinpoint the problem to the area that all of these three access points cover. Access points and other network elements may also send alarms when suspicious packets, traffic or load is found or the signal/noise ratio of radio connects approaches or reaches some threshold.

2.3.5 Legislation

In Finland and several other countries the legislation helps to prevent malicious denial of service attacks by the power of penalties. Deliberate interference of tele and data communications is forbidden by law and an operator may always report denial of service attacks to authorities. Legislation is also one of the few

methods to handle the possibility of fake networks and services unless additional means like IPSEC are used to further authenticate the user and the network.

2.4 Problems

2.4.1 WEP encryption algorithm

A recently published report about the security of WEP algorithm, "Intercepting Mobile Communications, The Insecurity of 802.11" [BorGolWag1], accurately pointed out that there were serious design flaws in WEP algorithm which created new threats for security in networks that relied on WEP encryption. The web page related to the report [BorGolWag2] describes in more detail the vulnerabilities of WEP protocol and the attacks these vulnerabilities would make possible.

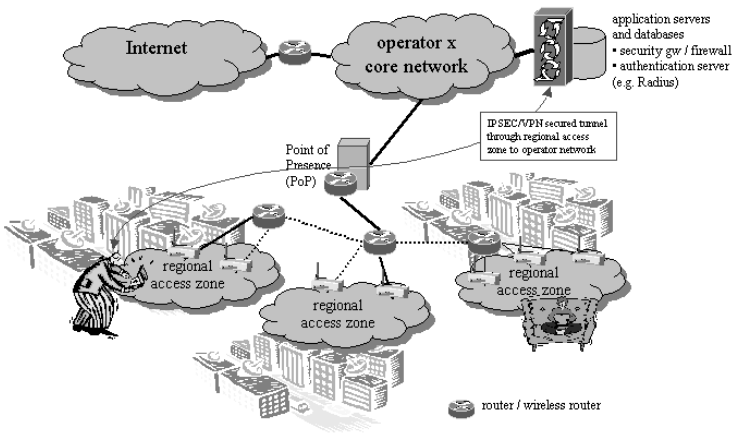
The problems why WEP was abandoned as a method to secure the radio traffic in the wireless networks the author has participated in designing, were however different. It was thought to be insecure even before the insecurity report on the basis of keylength, but there were more reasons to the decision too. One reason were the interoperability issues. WLAN cards might have different length shared keys and these were not interoperable. The presentation of the shared key was different, some cards wanted text key and some wanted it in hexadecimal format. Actually the only time when the WEP encryption actually worked was with same vendor's access point and card. And when the only advantage that the WEP encryption would provide was that random sniffer from street couldn't associate (unless he/she knew the shared secret known by hundreds of legitimate users) to access point, there was no point in trying to secure the radio path with WEP encryption. Keeping the radio path unencrypted however brought other problems.

2.4.2 Access control and MAC address filtering

Because in some or most cases WEP encryption can't be used, some other kind of access control must be found. This is where the limited firewall capability of firewalls may be used to deny access from the devices which don't have their MAC address in access list. This however can be circumvented very easily by faking the MAC address to some legitimate user's MAC address. The changing of MAC address is supported in several operating systems and also in Windows there were drivers and firmware combinations where this was possible. Because of this, additional authentication and security were required. One way to solve this was the architecture used in the regional access zone concept.

3 Regional Access Zone

3.1 General



Regional access network is a network that covers some specific area. The WLAN access points are installed outside and provide the both outdoor coverage and partly indoor coverage for users who live in their own houses or flats. The users may then use an outdoor or indoor antenna to connect the network. This way the wireless link is used to replace the cable otherwise required for fixed connection. As also presented in the picture the wireless links may be used to deliver the last mile from roof to roof. Then sharing of the fixed connection may be done by using regular Ethernet/HomePNA cabling in for example flat.

In this access network scenario the user has usually a fixed client – service provider relationship. This means that the service provider may to some extent determine the used VPN/IPSEC client, settings and even recommended vendor and antenna solution. The Service provider cannot however force certain hardware solution or configuration to users without seriously limiting the customer base. The regional access network consists of regional access zones. It is separated from core network with filters, access lists, routes and IP address selection (e.g. private / grey addresses in routers). The regional access zones consist of one or several bridged access points connected to a (wireless) router that may be located behind a wireless or fixed uplink.

The WLAN device connects first to the access point in one regional access zone. This is where the first authentication occurs. First the device's MAC address is checked against authentication database. If the MAC address doesn't

exist in database, the traffic to or from the device will not go through the access point. Next the WLAN device gets a dynamic grey IP address that allows the device to send and receive data in regional access network. The user can now initiate the final authentication by activating the VPN client in his terminal and creating the IPSEC tunnel to the VPN terminator. Through the tunnel the user receives a real dynamic/fixed Internet IP address and is able to connect to the Internet. Now the user has an encrypted tunnel through radio access network and there is always a possibility to create another tunnel from VPN terminator if additional security over Internet is needed. Using this kind of method also helps conserve IP addresses as only the users with an active VPN tunnel will have a fixed "real" Internet IP address.

3.2 Threats

3.2.1 Unauthenticated and unaccounted use of network

The first threat is the unauthenticated and unaccounted access to Internet. Crackers may use the network and other users' account information as a nice way to hide and then attack against the service provider's system or against the other hosts connected to Internet. If the cracker for example uses some user's MAC address and account to conduct attacks, the cracker can only be tracked to that certain user account and there is no real information who actually did use the account.

The legislation at least in Finland requires that the service provider is able to control and track these kinds of network abusers. Service provider that clearly lacks this kind of security control over network, very quickly loses for example peering agreements with other providers. This means that if the provider is seen as some kind of shadowy lair for crackers, it is disconnected from other operators and eventually even from the whole Internet.

The crackers are not the only users that may abuse the network. If it is not controlled, the users may be able to use the network bandwidth unaccounted by using the grey IP network for data transfers and leaving out the second authentication. This is a threat to availability as these kind of users may be able to fill the network bandwidth for example with FTP traffic.

3.2.2 Faked services and networks

The third threat presented here are the faked services and networks. Inside one regional access zone it is possible to setup a fake DHCP service and in this way trick the user to connect to fake service or re-route user's traffic to a hostile network. Using this kind of method it is possible to capture the user authentication information the unsuspecting user uses. Many users for example do not care to check if the certificate for their online Internet bank is a valid one. They may not even notice if the connection is SSL encrypted or not.

3.2.3 Attacks against network management

An attack may also be directed against network management traffic. If the attacker is able to associate to an access point and connect to the network, he/she may be able to send fake dynamic routing annoucements thus disrupting the normal router management. This can be a denial of service threat or also integrity threat if done similarly as the fake DHCP server example in Section 3.2.2.

3.3 Solutions

3.3.1 IPSEC/VPN

IPSEC/VPN can be once again used both to secure the radio path and to authenticate the user to the network and network to the user. To make this useful, some security education for users is needed. If wireless links between routers are used, IPSEC can also be used to protect the network management traffic / traffic between routers. WEP encryption may also be used in this case, but then the WEP encryption key must be securely changed very frequently. Methods for doing this between routers do not exist in vendors' current solutions.

3.3.2 Routers, router filters and rules

When there is not enough intelligence in the WLAN access points to do the filtering or routing changes, the features of upper level network elements may be used to add security and filtering for access network and access zones.

In most routers it is possible to create access control lists and firewall rules for limiting the traffic to certain hosts and even forcing the users to use the VPN/IPSEC by denying most or all non-encrypted traffic. The latter choice is quite a good one in regional access network as the VPN/IPSEC client solution is provided by operator to clients and there are no ad-hoc visitors or tourists in the network. It also solves the availability issue of users using the regional access network as a private transport network. When all traffic has to flow through single or few points, it is easier to track the users that may waste unreasonably other users' bandwidth.

The filtering rules may also be extended to filter out routing/management protocols with suspicious source and destination addresses or what could potentially interfere with the normal network routing protocols. This however is not always needed, as the dynamic routing is not always required in the network. Static routes may also be enough and sometimes even more secure than using dynamic routing protocols. If dynamic routing is used, the selection of dynamic routing protocol becomes more important (e.g. RIP vs OSPF). If the routing protocol does not provide security features that help protect the network against attacks, then there is no point in using it.

3.3.3 Security education for users

The security of the regional access network may be improved with technological means, but most of the methods are not really effective, unless the users know how to distinguish between fake networks and services and real ones. The users must be informed to check for signs for suspicious networks, unencrypted bank web sites, missing certificates, even to check the certificates the web browser accepts. And what comes to IPSEC security, few users understand when it is secure and when someone is faking the connection.

3.4 Problems

3.4.1 Fake networks and services

On the regional access zone level the fake networks and services type attacks can be prevented with those router settings presented above. However inside one regional access zone it may be a bit harder depending on the network elements used. If the network elements support routing and routing/firewall filters, this helps, but at least with regular vendor access points faking a DHCP server within one access point coverage area may be an easy task and it can not be currently solved with anything else but user education.

3.4.2 IPSEC/VPN interoperability

IPSEC/VPN interoperability between vendors has improved but there are still products in use or market that are not interoperable with each other. The author has witnesssed for example a case where a Cisco router and Checkpoint Firewall-1 couldn't agree on encryption method and key length. This was due to the fact that the Firewall-1 VPN/IPSEC product was weakened because of the US export restrictions. In another case the VPN terminator / security gateway had an old, non-updated operating system in use and it supported only Diffie-Hellman Group 1 key echange when the other side required at least Diffie-Hellman Group 2. This was corrected by upgrading the security gateway to a newer version, but this isn't sometimes possible because of the interoperability issues with old systems / clients, regulatory reasons (encryption strength may be limited in some countries), company policies etc.

The IPSEC/VPN interoperability may be partially blamed for a problem called double tunneling. This means running an IPSEC tunnel inside an IPSEC tunnel. For example when the corporate user wants to connect to corporate intranet with company client, must the user first establish the service provider's VPN connection and then his own VPN connection inside the first one. This problem can be circumvented by re-tunneling certain users/groups from the operator's VPN/security gateway to that corporate network, but sometimes users or companies do not want the operator to have any access to non-encrypted data. In the re-tunneling scenario the first tunnel ends in a VPN/security gateway and a new one starts from there ending to the corporate network security gateway.

3.4.3 IPSEC/VPN architecture design

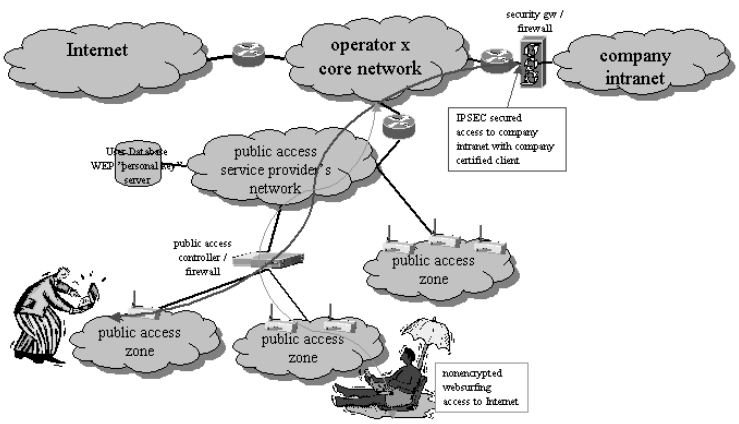
Most IPSEC/VPN products and devices and their architecture is designed to protect some limited number of networks (e.g. corporate home network) from the rest of the world. In the regional access network this is reversed. The rest of the world is protected from limited number of networks. The users use VPN clients to connect to internet instead of using VPN clients over the Internet to connect the corporate network. The author has participated in evaluation of many vendors' products where the software or configuration is designed or fixed to the corporate network scenario so that configuring and implementing this kind of reverse solution is not possible. Some have even fixed the inside, outside and de-militarized zones into certain network interfaces. Fortunately today few implementations and products are not limited in this sense and provide the freedom to define the interfaces according to user's needs..

3.4.4 IPSEC/VPN certificate management and distribution

IPSEC/VPN certificate based authentication would solve many issues, for example the network – user authentication and would make faking the network and its services harder. When the amount of users is small, the author sees this as a feasible solution to enhance security especially in corporate networks. These kinds of certificates can then reside on smart cards or similar kind of storage devices and can be used like equivalent of SIM cards in several devices. The problem that the author sees is the management and distribution of these certificates to clients. It is not for example very feasible and reasonable to enter one certificate per user using a graphical user interface, instead the operator/service provider needs a method to make and distribute large number of certificates very easily for example based on a user database. Currently the author is not aware of any vendor solution that would do this and still interoperate with the VPN termination or security gateway devices. Some software product may for example do this, but cannot transfer the certificates to a security gateway that does the encryption work etc.

4 Public Access Zone

4.1 General



Public access zones are the user scenario the current WLAN technology vendors try to market to services providers and operators. The public access zones differ from regional access zones in that public access zone users may not have any fixed client – service provider relationship to public access zone operator. Instead many temporal relationships may be created and removed during for example credit card payments. The public access zones are usually located in hotels, net cafes, airports and similar hotspots, where mobile users want to use the Internet.

This makes difficult to do the radio path security and the user authentication via VPN/IPSEC solution in the way it may be done in the regional access zone scenario. The public access zone users may not have a VPN client software at all or they may have a VPN solution that terminates to the corporate network's security gateway. The user cannot be forced to use one vendor's solution or otherwise the amount of users will most certainly drop reducing the possible income from public access zone and hotspot services too much. Also fixed lists of MAC addresses in access points are troublesome to set up and clean when the users come and go.

To handle the problem technology vendors have created a network element / concept called public access controller (PAC). The public access controller controls the access to network. A public access zone may consist of one or several access points and a public access controller. It may also consist of only

WLAN access points if a single institution can be determined to be responsible of the connecting users' actions. In the latter case the access control is then somewhat limited but it may be enough, because this institution may be held responsible.

The public access zone may have real Internet IP addresses or grey/private IP addresses which are NATed to real Internet IP address(es). These are distributed to all clients that connect to public access zone usually with DHCP.

4.2 Threats

4.2.1 Unauthenticated and unaccounted use of network

Unauthenticated and unaccounted use of network must in this case be emphasized as temporary client – provider relationships make tracking of users difficult. The question in public access zones is: who has the responsibility of the users' actions? Is it for example the users, the net cafe owner or the operator whose network they use? The size of public access zones help the operator to track abusers and denial of service attacks but then again if many-to-one NAT (i.e. many grey IP addresses are masqueraded to fewer Internet IP addresses) is used it is almost impossible to distinguish which user did what and when. If all these kinds of connections on the other hand were logged, the amount of log data would make tracking still unfeasible.

4.2.2 Eavesdropping

In the public access zones WEP encryption cannot be usually used because of the interoperability issues and also because of the fact it wouldn't be very useful because all zone users would know it. Invidual users may use VPN/IPSEC clients to secure traffic, but by default most of the traffic is unencrypted. Now if the user or service authentication is done in clear text, the eavesdropper gains easily user authentication information. Of course the SSH and SSL encrypted connections are as safe as they are in the wired network. The non-encrypted traffic however is available on region access zone level to anyone inside the coverage. By default the eavesdropper has access to IP-level without authentication which makes it also easy to record all encrypted traffic for later analysis.

4.3 Solutions

4.3.1 Public Access Controller (PAC)

Public access controller is a network element for access control. The vendors have various ways to approach the problem, but they may be divided to client-based and clientless solutions. Client-based solutions require specific client to be installed or run from user's terminal. Clientless public access control solutions do not need separate client installed on user terminal, instead for example web browser may be used.

The author sees clientless solutions more useful than the client-based ones as they provide access control for all kinds of devices and do not require separate client installation. If a separate client were to be installed, why not install a full VPN client instead?

The clientless public access controller like Nokia's P020 by default denies all traffic through it unless the user has gained an access to some certain IP address through authentication. The authentication usually works so that the PAC captures the unauthenticated user's request for web page and instead of the web page returns an authentication page or a redirect order to user's web browser. Then the user may enter his user id and password on an authentication web form to gain access to network. Then the PAC checks the authentication information from a local mirrored authentication database or via for example RADIUS from the authentication database. If the authentication information is correct then the public access controller opens the access through PAC for the IP address the user is using. This can be done by modifying simple firewall rules inside PAC.

Now the user has gained access to Internet. The access can be limited to certain addresses or ports with firewall filters in the PAC. This way the threat of using the public access for wrong purposes can be minimized. Now the user may use whatever VPN/IPSEC client that goes through the PAC to secure his connection to for example a corporate intranet. In regional access zone this would usually require double tunneling but in the public access zone case the user is able to use his/her own VPN client straight through the Internet.

4.3.2 The vendor specific solutions

In addition to Cisco's solution to exchange invidual WEP keys, Nokia has also developed an authentication method based on WLAN cards, GSM SIM cards, public access controller and GSM operator's AAA (authentication, authorization, accounting) services. In Nokia's WLAN card there is a smart card reader where the operator's SIM card is inserted. Then the user gives the PIN code to the client software and the client software sends an authentication request to the GSM operator's VLR (Visitor Location Register). The authentication request goes through a GSM billing gateway so that the user can be billed. The VLR then sends a random number to the public access controller that forwards the number to the client software. Using the SIM card for calculation the client software gets the response and sends it to the public access controller. The public access controller verifies the response and if it is a correct one, lets the user pass similarly as in the normal public access controller case.

Unfortunately the author is unable to provide more detailed information about the SIM card usage as the source of information, the presentation "Public Access Zone and Operator WLAN" [Viljakainen] does not go into technical details.

4.4 Problems

4.4.1 PAC authentication security

Because it is easy to join to public access zone and eavesdrop traffic, extra care should be focused in securing the authentication done with public access controller. If the authentication information is transmitted via web forms without SSL encryption, it is easy for eavesdropper to catch the user accounts and passwords needed to gain access through the public access controller. This can however be prevented or made more difficult by using SSL encryption, one-time-passwords and, if the public access controller supports them, MAC address filtering and limitations for one user account to have only one IP address in use at the same time.

4.4.2 Network Address Translation (NAT)

Often when using the public access controller it may be appealing to use Network Address Translation (NAT) in the public access controller or perhaps even in the WLAN access points to conserve IP addresses. Using NAT has however until recently been a problem for IPSEC connections. At least if they are not terminated in the network element doing the NAT and then continued. In a nutshell the problem is:

> Any attempt to perform NAT operations on IPSEC packets between the IPSEC gateways creates a conflict.
>
> IPSEC wants to authenticate packets and ensure they are unaltered on a gateway-to-gateway basis.
>
> NAT rewrites packet headers as they go by.
>
> IPSEC authentication fails if packets are rewritten anywhere between the IPSEC gateways.
>
> *[FreeswanNAT]*

Recently the IPSEC stack / VPN vendors like SSH Communications Security and SecGO have released client and server software capable of NAT traversal. It will however take time for the NAT traversal feature to get implemented in the dedicated VPN server appliances. This makes using real Internet IP addresses nowadays the most attractive approach to the problem of getting the IPSEC clients work in public access zones.

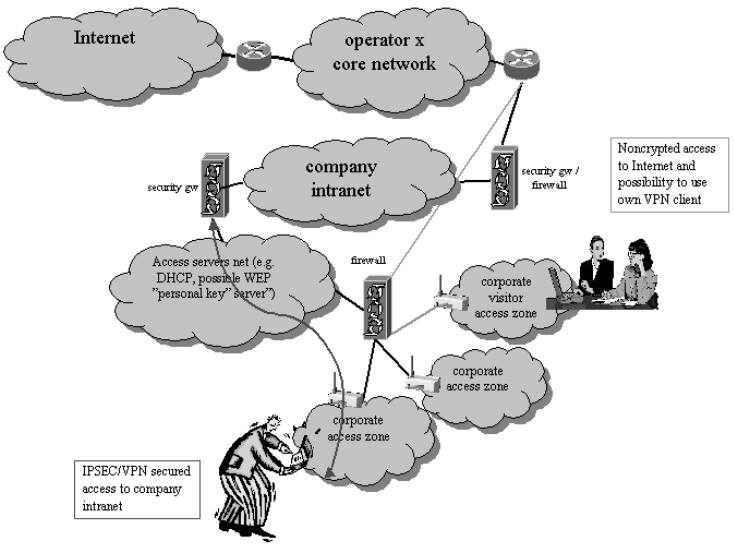
4.4.3 The vendor specific solutions

Actually the name says it all, vendor specific solutions are vendor specific meaning that if they are used, the users are either forced to use some vendor's cards or clients or the service provider has to do different kind of authentication method

configurations for each different WLAN card type. This is a no-win scenario for service provider as forcng users to use only certain type of WLAN vendor would get less users and then again, doing everything for everybody would take too much resources. So at least in author's opinion, a vendor specific solution bad, a vendor independent solution good.

5 Corporate Access Zone

5.1 General



The corporate access zones are access zones designed to provide WLAN access to the corporate users inside office. They are probably the easiest access zone case for network designer as this was the use case the WLAN was first thought to be used.

Under the corporate access zone coverage there is a limited amount of users so that there is also a limited number of people who need to know the shared secrets. Software/hardware configurations for firewalls, security gateways, VPN solutions and user terminals are often fixed or at least they can be fixed with company policies and standards for the information systems.

This helps in focusing the extra effort needed to ensure the interoperability between devices in other access zone cases instead to keeping the network as secure as possible and minimizing the external threats as well as threats against the availability.

The picture above presents a network architecture that may be used when building corporate access zones where critical information is transferred. In the environment where less security is needed the first firewall counted from the corporate user to intranet could be combined with the second one. This way the network access servers like DHCP servers would reside in company's intranet. In case the reader is interested in learning what other kind of network architectures may be used, the author would like to suggest to look into Mikko Jarvinen's presentation "Nokia Wireless LAN" [Jarvinen].

The author would however like to recommend the use of additional VPN/IPSEC encryption in any case some privacy/security is needed as the WEP encryption very clearly is not the solution for securing the radio path.

5.2 Threats

5.2.1 Unauthenticated and unaccounted use of network

In the corporate access zone unauthenticated and unaccounted use of network could mean two things. It could be an attacker doing industrial espionage or a user that connects to the unsecured corporate network and uses it as an Internet access provider deliberately or non-deliberately. The latter one may happen very easily accidentally as a user surfs with WLAN equipped PDA device and suddenly the system pickups the stronger unsecured corporate network and associates to it. The author has experienced situation himself when the PDA has roamed into some corporate network, got an IP address from DHCP and been able to surf the Internet through that corporation's Internet connection unaccounted.

5.2.2 Denial of Service

Denial of service attacks against companies are common nowadays. Depending on the criticality of the network access to the company, denial of service attacks against firewalls, routers and mail systems may cause financial losses, when the systems are not available when they are needed. The author has noticed few times when the mail delivery system has been down (not because of the attack though), that he couldn't do really anything useful for half a day because of the problem. In designing the corporate networks also these kinds of threat possibilites should be considered.

5.2.3 Social attacks against users

Even if the network elements were secured and configurations were flawless, the attack that most likely succeeds is based on the lack of security education and gullibility of the users. The attacker may for example pose as a support person asking for the WEP shared key and user account details for testing the account or some new system. In alarmingly many cases the regular users give this information without any questions why someone would need it.

5.3 Solutions

5.3.1 Firewalls, Public Access Controllers

Firewalls and public access controllers may, as presented in the network architecture picture, be used to control the access as strictly as needed. They may be configured so that no other than IPSEC protected traffic goes through. This

way the users are forced to use an IPSEC client to access the work / network resources and the traffic over radio path is secured.

Depending on the firewall solution also the special intrusion detection software may be used to alert the IT support when a denial of service or other attack is launched against the systems.

5.3.2 WEP encryption

The WEP encryption is still not feasible in author's opinion to use as the radio path encryption, but it may be used as a basic access control mechanism. The shared key may be told only to personnel and then no one who doesn't know the key can connect to network accidentally.

5.3.3 Company policies and standards

The company policies and standards may be used as a tool to minimize hardware/software conflicts that would result down-time in network access as the users would wait for IT support to configure their systems correctly. Policies and standards may also be used in defining company wide security policies and protocols that will help against social attacks. The users may for example be told not to give in any circumstances their user id, password or shared WEP key and network name.

5.3.4 Personnel security training

Personnel security training is perhaps the most efficient way to protect the company against social attacks from outside and also from inside. If the people are aware of the possibility of attacks and the ways the social attacks are done, they can be used as a living intrusion detection system giving alerts when an attacker has contacted someone.

5.3.5 Hardware evaluation and redundancy

By using several firewalls and other redundant hosts it is possible to minimize the effects of denial of service attacks. Also the normal load may be balanced on several hosts enhancing this way the availability. Careful selection and evaluation of software and hardware solutions is also very useful as in this way the number of interoperability and availability problems can be diminished.

5.4 Problems

5.4.1 Users

Many systems would be just perfect without users and their requirements. Even inside one company there usually are groups and departments that need completely different kinds of systems and configuration than the rest. For example

research department requires more flexibility, but it also requires more security when the production may very happily settle for standard solution.

Sometimes security policies and rules are also seen as unnecessary bureaucracy and people rise to resistance even against reasonable solutions. It is very important that the security solution found satisfies users and administrators because if it doesn't it is very likely that people try to get around it or just disregard it damaging this way security.

6 Conclusion

The threats presented earlier in the different access zone cases are somewhat common to all access zones. The following table summarizes the existence and probability (x = likely, o = possible, but not likely) of different threats in each case (RAZ = Regional Access Zone, PAZ = Public Access Zone and CAZ = Corporate Access Zone).

Threat	**RAZ**	**PAZ**	**CAZ**
Eavesdropping	x	x	x
Denial of Service	x	x	x
Integrity	x	x	x
Unauthenticated and unaccounted use of network	x	x	x
Faked services and networks	x	x	o
Attacks against network management	x	o	o
Social attack against users	o	o	x

Because most of the threats are overlapping so are the countermeasures. However like in the case of IPSEC/VPN, different parts of the technology may be used differently in each type of access zone. For example in the public access zone there is no need to use IPSEC/VPN for casual surfing, but the users may use it to connect from public access zone to corporate network. The IPSEC in the public access zone is not used to secure only the radio path like in regional access zone. So not every applicable solution is used same way in every type of access zone.

In the following table solutions applicable for a certain access zone are marked with 'y', possibly applicable with 'p' and not applicable with 'n'. The table contents are mostly according to author's opinion and views for example about the usefulness of the WEP encryption may vary.

Solutions	**RAZ**	**PAZ**	**CAZ**
WEP encryption	n	n	y
IPSEC/VPN	y	p	y
Intelligent network elements	y	y	y
Network management	y	y	y
Legislation	y	y	y
Routers, router filters and rules	y	p	p
Public access controller	p	y	p
Firewalls	y	y	y
Company policies and standards	n	n	y
Personnel security training	p	n	y
Hardware evaluation and redundancy	y	y	y

The remaining problems in the access zone cases after applying the solutions vary even more than the applicable solutions or threats. The third table summarizes the existing (y), possible (p) and non-existing (n) problems in all three access zone cases.

Problems	**RAZ**	**PAZ**	**CAZ**
WEP encryption	y	y	n
Access control and MAC address filtering	p	p	n
Fake networks and services	y	p	p
IPSEC/VPN interoperability	y	n	n
IPSEC architecture design	y	p	n
IPSEC/VPN certificate management	y	p	n
PAC authentication security	n	y	p
Network Address Translation (NAT)	y	y	n
The vendor specific solutions	y	y	n
Users	p	p	y

What can be seen from these tables and from the descriptions of problems in each access zone, is that once again there is no silver bullet to use to remove all problems. There are solutions that fit to all access zone cases, but those solutions do not remove all problems and may even cause more if used alone. It is also clear that problems cannot be solved by just buying different WLAN vendor products and solutions. The solutions on market are usually very focused to handle certain problems, problem areas or access zone cases. There exists a need for customizable network elements and solutions that may be freely modified and improved as the new technologies mature and emerge to markets. Everything cannot be solved with off-the-shelf products and network elements but if there exist customizable, open elements, there is a possibility to do things better. The final question is where to draw the line between ease-of-use, required work and security. When is there enough security?

7 References

[**BorGolWag1**]
Nikita Borisov, Ian Goldberg, and David Wagner:
Intercepting Mobile Communications, The Insecurity of 802.11
http://www.isaac.cs.berkeley.edu/isaac/wep-draft.pdf
Mon May 7 06:43:19 EEST 2001

[**BorGolWag2**]
Nikita Borisov, Ian Goldberg, and David Wagner:
(In)Security of the WEP algorithm WWW page
http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html
Thu Apr 26 01:28:16 EEST 2001

[**FreeswanNAT**]
FreeS/WAN v1.9 IPSEC stack documentation
http://www.freeswan.org/freeswan_trees/freeswan-1.9/doc/firewall.html#NAT
Mon May 7 06:57:46 EEST 2001

[**Gomes**]
Lee Gomes:
"Often unguarded wireless networks can be eavesdroppers' gold mine"
article in Wall Street Journal
http://www.msnbc.com/news/565275.asp?cp1=1
Sun Apr 29 14:02:09 EEST 2001

[**Jarvinen**]
Mikko Jarvinen:
"Nokia Wireless LAN"
presentation from Tampere University of Technology course
Wireless Lans (http://www.cs.tut.fi/kurssit/83180/)
Mon May 7 06:43:19 EEST 2001

[**Viljakainen**]
Ari Viljakainen:
"Public Access Zone and Operator WLAN"
presentation from Tampere University of Technology course
Wireless Lans (http://www.cs.tut.fi/kurssit/83180/)
Mon May 7 06:43:19 EEST 2001