TAMPERE UNIVERSITY OF TECHNOLOGY
Department of Information Technology

Karri Huhtanen

The Design and Deployment of the TUT Public Access Architecture

Master's Thesis

Subject approved by the department council on 10.4.2002
Supervisors: Prof. Tommi Mikkonen
Prof. Jarmo Harju

Foreword

This master's thesis was done as a part of the author's research work in the ICEFIN research project at the Institute of Communications Engineering at the Tampere University of Technology (TUT).

First the author wishes to express his gratitude to the supervisors of the thesis: Prof. Tommi Mikkonen and Prof. Jarmo Harju.

The author wishes also to extend his thanks to Jussi-Pekka Pispa and Martti Jokipii from TUT's Information Technology Management for the support they have given and also because of the given opportunity to turn the researched architecture into a real-life implementation.

The TUT Public Access architecture also would not be what it is now without the experience the author gathered working in the service of companies like Nokia Oyj and Saunalahti Group Oyj, and without the numerous discussions the author has had here and there with his former and current coworkers.

Last, but not least, the author wishes to thank Sami Keski-Kasari and Heikki Vatiainen, both coworkers and founders of Arch Red, for their cooperation, work effort and support in realising TUT Public Access, Funet WLAN Roaming and Arch Red.

On 25th of May 2005, in Tampere, Finland.

Karri Huhtanen
khuhtanen@iki.fi

Abstract

TAMPERE UNIVERSITY OF TECHNOLOGY
Department of Information Technology
Institute of Software Systems

HUHTANEN, KARRI: The Design and Deployment of TUT Public Access Architecture

Master of Science Thesis, 54 pages.
Examiners: Prof. Tommi Mikkonen and Prof. Jarmo Harju
June 2005

Keywords: wlan security, network architecture, access control

The development and widely spread usage of wireless networks, laptop computers, and other mobile technologies have increased both the number of mobile users and the need for secure, usable, and scalable methods to control the user access to the network. Especially in wireless networks, the security architecture is often designed as if wireless medium would just be a cable replacement. Considerable effort is invested in securing the radio access with encryption, but at the same time end-to-end security and user mobility requirements are neglected.

To develop a good network architecture a broader view is needed. The architecture must balance the requirements concerning usability, management and security, to get it widely accepted and used. By concentrating on a single issue like link-level security, this cannot be achieved. Instead, the architecture must be developed so that all requirements and existing infrastructures and services, are taken into account from the beginning of the design process. This thesis presents the TUT Public Access architecture, which was designed in this way, and deployed successfully at the campus of Tampere University of Technology.

Tiivistelmä

TAMPEREEN TEKNILLINEN YLIOPISTO
Tietotekniikan osasto
Ohjelmistotekniikka

HUHTANEN, KARRI: The Design and Deployment of TUT Public Access Architecture

Diplomityö, 54 sivua.
Tarkastajat: prof. Tommi Mikkonen, prof. Jarmo Harju
Kesäkuu 2005

Avainsanat: wlan-turvallisuus, verkkoarkkitehtuuri, pääsynvalvonta

Langattomien verkkojen, kannettavien tietokoneiden ja muiden mobiilitekniikoiden kehittyminen ja lisääntynyt käyttö on kasvattanut sekä liikkuvien käyttäjien määrää että tarvetta turvallisille, käytettäville ja skaalautuville tavoille hallita käyttäjien verkkoonpääsyä. Erityisesti langattomissa verkoissa turva-arkkitehtuuri on usein suunniteltu niin kuin langaton media olisi vain kaapelin korvike. Huomattavaa vaivaa nähdään radioverkon suojaamiseen salauksella, mutta samaan aikaan jätetään huomioimatta päästä-päähän-turvallisuus ja käyttäjien liikkuvuusvaatimukset.

Hyvän arkkitehtuurin kehittämiseen tarvitaan yllä esitettyä laajempi näkökulma. Saadakseen käyttäjien hyväksynnän arkkitehtuurin on tasapainotettava käyttäjien, käytettävyyden, hallinnan ja turvallisuuden vaatimukset. Keskittymällä yksittäiseen asiaan, kuten linkkitason turvallisuuteen, näin ei pystytä tekemään. Arkkitehtuuria kehitettäessä täytyy sen sijaan ottaa huomioon kaikki vaatimukset ja olemassaolevat infrastruktuurit ja palvelut jo suunnitteluprosessin alusta lähtien. Tämä diplomityö esittelee TUT Public Access -arkkitehtuurin, joka suunniteltiin edellämainitulla tavalla ja otettiin onnistuneesti käyttöön Tampereen teknillisellä yliopistolla.

Table of Contents

List of Acronyms

AAA	Authentication, Accounting, Authorisation
AC	Access Controller
ADSL	Asymmetric Digital Subscriber Line
AES	Advanced Encryption Standard (cryptography)
AP	Access Point, e.g. WLAN Access Point
ARP	Address Resolution Protocol (Internet, RFC 826)
CBC-MAC	Cipher-Block Chaining Medium Access Control (IEEE standard 802.11i)
CCMP	Counter mode with CBC-MAC Protocol (IEEE standard 802.11i)
CSC	Center for Scientific Computing (org.)
DHCP	Dynamic Host Configuration Protocol (RFC 2131)
DoS	Denial of Service (security)
EAP	Extensible Authentication Protocol (RFC 3748)
ICE	Institute of Communications Engineering
IEEE	Institute of Electrical and Electronic Engineers (org., USA)
IETF	Internet Engineering Task Force (org.)
IMAP	Internet Message Access Protocol (RFC 2060)
IP	Internet Protocol [version 4] (RFC 791)
IPSEC	Internet Protocol SECurity
IPv6	Internet Protocol Version 6 (IP, RFC 1883/1884)
IT	Information Technology
MAC	Media Access Control
RADIUS	Remote Authentication Dial-In User Service (RFC 2865)
RC4	Rivest Cipher / Ron's Code 4 (cryptography)

SIP	Session Initiation Protocol (IETF, VOIP)
SMTP	Simple Mail Transfer Protocol (RFC 821, TCP/IP)
SSH	Secure SHell (Unix, Shell)
SSL	Secure Sockets Layer
TERENA	Trans-European Research and Education Networking Association (org., Netherlands, Europe)
TKIP	Temporary Key Integrity Protocol (IEEE standard 802.11i)
TLS	Transport Layer Security [protocol] (SSL)
TUT	Tampere University of Technology
VLAN	Virtual Local Area Network (LAN, IEEE 802.1q)
VPN	Virtual Private Network
WECA	Wireless Ethernet Compatibility Alliance (org., WLAN, LAN), also known as WiFi Alliance
WiFi	Wireless Fidelity, the popular acronym for 802.11b wireless networking
WLAN	Wireless Local Area Network (IEEE standard 802.11, 802.11a, 802.11b, 802.11g and 802.11h)
WPA	Wireless Protected Access (industry standard)
WPA2	Wireless Protected Access version 2 (industry standard)
WWW	World Wide Web

1 Introduction

The rapid development of wireless networks, the decreased costs of their deployment, and the increased usability and support in terminals and operating systems have led to a situation where practically anyone can buy a cheap wireless access point and create a network without any deeper understanding or knowledge of network planning or used technologies. While this has been favorable development from the viewpoint of end customers and network equipment vendors, the wild growth and deployment of wireless networks has at the same time become a problem for organisations and their IT management, who would like a more organised approach to develop and deploy wireless network services.

This thesis was written as a part of the co-operation project between Institute of Communications Engineering and Information Technology Management at Tampere University of Technology. The goal of the project was to design, implement and deploy unified public access network architecture for Tampere University of Technology. The public access network was named TUT Public Access. During the project the developed architecture was also presented in the national and international network conferences that led to contributing and combining it to TERENA Mobility Taskforce's Eduroam WLAN roaming architecture. The developed architecture was also adopted by Wireless Mobile Vaasa project in Finland and commercialised by Arch Red Oy, a company founded by the author and his two colleagues during the project.

The author's role and contribution in the TUT Public Access project can be char-

acterised as working as a system architect responsible for the evaluation, selection and combination of the network technologies to be used, and the design and development of the architecture. In the project the author was able to combine his practical experience from working in the WLAN industry to the new ideas and solutions researched and matured during the author's work at the Institute of Communications Engineering. The result is the TUT Public Access architecture presented in detail in this thesis.

This thesis is structured as follows. After the introduction, the second chapter describes the situation and environment in the beginning of the TUT Public Access project. The second chapter is followed by third and fourth chapters describing the feasible options for access control and network architecture. The fifth chapter introduces the developed architecture and analyses its strengths and weaknesses in detail. The sixth chapter describes the deployment of the architecture, found problems and solutions, current situation and the possible directions for the future development. The thesis and the experiences collected during the development of TUT Public Access architecture are summarised in the final seventh chapter.

2 Problem Scoping

This chapter introduces the environment in the beginning of the TUT Public Access project as well as the general needs and problems related to the public area network access control. The chapter also describes one of the most important design principles behind the design decisions of the architecture to be presented, called *sufficient security* — the balance between usability and security.

2.1 Initial Environment

The initial wireless network environment at Tampere University of Technology is an excellent example of a wireless network grown gradually without defined guidelines or a common architecture. The situation is similar in almost all organisations that have had different departments gradually adopting wireless networks in their own pace and from their own, possibly very early iniative. This has created a situation where there exists several different WLAN networks with different kind of access control, security measures, procedures and settings. The results of an extempore WLAN network scanning walk around TUT campus in Table 2.1 demonstrate the situation in the end of June 2003 with about 61 different access points in 13 different wireless networks. In the table, WANO, WIWA, freedom and Hermia were wireless networks outside TUT campus.

Table 2.1: Results of a WLAN network scanning walk

Network (ESSID)	*APs found*	*WEP Encryption*
ACI	3	yes
AIBONET	2	yes
BIO	1	yes
CS_WLAN	10	yes
Digital Systems WLAN	8	yes
ELE WLAN	6	yes
freedom	2	no
Hermia	1	no
IT	1	no
KAU	2	yes
MIT WLAN	2	no
MODEEMI	1	no
ttek	1	yes
TUT	13	no
TUTVRC	1	no
WANO	6	no
WIWA	1	yes

2.2 Initial Problems

This section introduces the initial problems and restrictions identified in the beginning of the TUT Public Access architecture development.

2.2.1 Management

The first problem of having multiple wireless networks controlled by different parties in a large organisation is that there is no clear centralised view of deployment, settings, or security level of these networks. The situation could be compared to a large building, where every occupant is able easily without earlier building experience to install doors and decide if and how they secure and use them. This kind of anarchy

is a nightmare for organisation's information technology department, whose mission usually is to provide clearly defined, controlled, managed and supported services to the users. Rogue wireless networks hinder this goal by interfering with the existing production systems and by introducing a lot of unknown variables in the organisation's information technology infrastructure. This can make solving of user problems more challenging and providing the support likewise harder.

2.2.2 Access Control

The lack of access control in some of the TUT campus wireless networks could have provided an attacker an easy access to the owner department's core network. Although there were no known cases of malicious attackers, one could have acquired confidential information like user names, passwords and documents from some departments' network and servers, or used the network services and resources like file and email servers without authorisation or approval.

In the beginning of the project some of the more security aware TUT departments used MAC address access lists and WEP encryption to secure their WLAN networks, which provided quite reasonable security to deter most attackers. However the network architecture was not designed from the mobility's viewpoint, and was more like wireless intranet presented in detail in Section 4.2 with its advantages and disadvantages.

2.2.3 Usability

Different wireless network architectures and their settings made it impossible to offer securely a general access through departments' wireless networks. In fact, even the TUT employees had at least to change their settings when accessing the network on the different department's coverage area. Often, an access through a more secured department network required that the department's system administration had to add the MAC address of the terminal to the access lists of all department's access points and also provide the user the shared encryption key. This was time and resource consuming, and because the encryption key had to be shared with several users, the

security provided by it is somewhat questionable.

The used encryption also provided more usability problems when some of the WLAN cards required either shorter or longer keys than the ones used in the accessed network. Because almost every network had different settings and different procedures to get the network access, the users were constantly confused how to access the network in each place and the utilisation of the network was usually limited to the employees of the department providing the coverage. For these users the usability was good as long as they stayed under their own deparment's coverage. However, convenient and usable organisation-wide utilisation of the wireless network was not possible.

2.3 Initial Solutions

Already in the beginning of the TUT Public Access project several partial and some complete solutions to the initial problems described in the previous section existed. There were several methods for controlling the terminal and user access to the network as well as network architecture models to combine and choose from.

The problem with these initial solutions was that none of them were specifically designed for the kind of environment the TUT network is. Because of this, a new architecture combining the best practices and the best solutions available, was needed. To develop the architecture, first the available initial solutions had to be identified and analysed. The results of the evaluation of initial solutions are collected in the next two chapters titled Access Control Methods and Network Architecture Models.

It was clear from the beginning of the project that just combining solutions blindly would not lead to a secure, stable and and the same time scalable and usable architecture, which was required. Because of this to control the combining of different solutions and to prevent the unwarranted decrease in the usability a basic design guideline, described in the next section, was devised.

2.4 Sufficient Security

Based on section Initial Problems, it is easy to make the assumption that by choosing the most secure and management-friendly access control methods and architecture for wireless networks, and by deploying and forcing users to use them, would solve the whole situation. This assumption is false, however, if the usability of the introduced architecture is not good enough to be accepted by the users.

The accelerated adoption of the wireless networks began when the users noticed that wireless networks were better and more usable alternative to long ethernet cables and fixed sockets. When designing and deploying a new architecture and security solutions, it is important that also the usability of these is evaluated in the combination of all of them. If the usability of a new common wireless architecture is not acceptable for users, they will most likely try to find ways to circumvent the security or the architecture to retain the usability of the old solution. This may lead to new security and management problems when users and in the worst case whole departments start to rebel by introducing their own rogue architectures and access points instead of doing the networks according to the common architecture.

A balance between usability and security in the new architecture must be found for the architecture to be succesfully deployed. The new architecture must provide enough benefits to compensate the possible increased weaknesses in the user usability and at the same time be able to secure the network and its users sufficiently well from attackers. From here on this balance and design principle is called sufficient security in this thesis.

3 Access Control Methods

This chapter introduces a few commonly used and possible methods for access control in the public access networks. The introduction is intentionally focused on three major access control methods used in this kind of networks, leaving out more marginal solutions like Mobile-IP authentication and proprietary vendor solutions preceeding WPA and WPA2 standards.

3.1 IEEE 802.11 based Access Control

The IEEE standard 802.11 defines a shared key authentication service and the Wired Equivalent Privacy (WEP) algorithm [1, pages 59–65], which both can be used in combination to provide access control for WLAN public area networks. Because the standard concentrates on wireless networks, it is obvious that this access control method cannot be applied in a fixed network environment.

The functionality of 802.11 based access control is based on the shared secret authentication and encryption of the data between mobile terminals and the WLAN access points with the help of WEP algorithm. The shared secret acts as a credential that allows a terminal to join to the WLAN network.

The advantages of this access control method are that it is very easy to use and reasonably secure at least for networks where the network traffic, and that the amount

of users is relatively small. As the amount of network traffic increases, the possibilities to break the WEP encryption via traffic analysis increase. Another disadvantage is that the shared secret is only as strong and as secret as the users and network administrators have decided to keep it. If the network has a lot of temporary users or guests, the effectiveness of this access control method is nearly nonexistent as all users knowing the shared secret are able to connect and even eavesdrop the network traffic of the other users.

3.2 WPA, WPA2 and IEEE 802.11i

To address the vulnerabilities [2] and disadvantages of the basic IEEE 802.11 authentication and WEP encryption, IEEE formed a working group with a goal to create a new standard for wireless security, 802.11i [3]. This new standard consisted of three parts. First, a Temporal Key Integrity Protocol (TKIP) provides a session and user specific encryption keys instead of a single shared key like in the original implementation. The second major part of the standard was to use the 802.1X standard [4] for port based network access control to control the authentication done between the WLAN access point and terminal. The third major part was to replace the WEP encryption with the CBC-MAC Protocol (CCMP) in the future thus providing AES encryption instead of the RC4 used in the WEP.

The 802.11i working group's progress was not fast enough for the WLAN industry and on-going WLAN deployments. Therefore the WiFi Alliance decided to create Wireless Protected Access (WPA) industry standard which incorporated the TKIP and 802.1X related parts of the coming IEEE 802.11i standard. In the WPA, the encryption is still based on WEP and TKIP provides only dynamically changing, session specific, WEP keys. The encryption enhancement, CCMP, was however then under development, but because it required hardware changes to access points and terminal products, the WiFi Alliance decided to postpone the requirement to the next WPA standard called WPA2.

In proportion to TUT Public Access project timeline, these new standards came too late to be implemented in the first version of the network, but not too late to

be considered in the architecture design. The WPA came first with first compliant products in April 2003, but the WPA2, which is the industry standard for devices supporting IEEE 802.11i, was not released until the September 2004. Currently, in November 2004, WPA standard compliant new devices are available, and the full driver and network support is included in the major operating systems like Microsoft Windows XP and MacOS X as well as in the PDA operating systems like PocketPC 2003 and Symbian Series 80. Partial support is also available for the open source operating systems, like Linux and different flavours of BSD.

In the heterogenous networks like TUT Public Access, the adoption of the new access control methods is slower as the user devices and access points vary. Because of this even when WPA and WPA2 would provide a more secure access control method, they cannot be chosen as the only possible authentication method. Instead, additional attention must be given in defining a flexible architecture that supports gradual adoption and cooperation of the different access control methods.

3.3 WWW-based Authentication

WWW-based authentication was first introduced in the operator controlled WLAN access areas called hotspots or access zones to control the access of the users and make the billing of network access possible. Because of the diversity of the user terminals, a common authentication method that did not require specific software to be installed on the terminal was needed. WWW-browser based authentication was the one available in almost any terminal capable of using the network. Figure 3.1 presents an example how the authentication process can work in practice. The sequence diagram is done on the basis of the TUT Public Access Network's access controller device. In addition to the presented polling method, there are several other methods for determining if the user terminal is still active in the network, but the basic idea of the separate access control device called access controller or WWW authentication gateway doing the polling and controlling access remains the same.

The modest terminal requirement for only a WWW browser is the biggest advantage of WWW-based authentication. Still there are also other advantages to be consid-

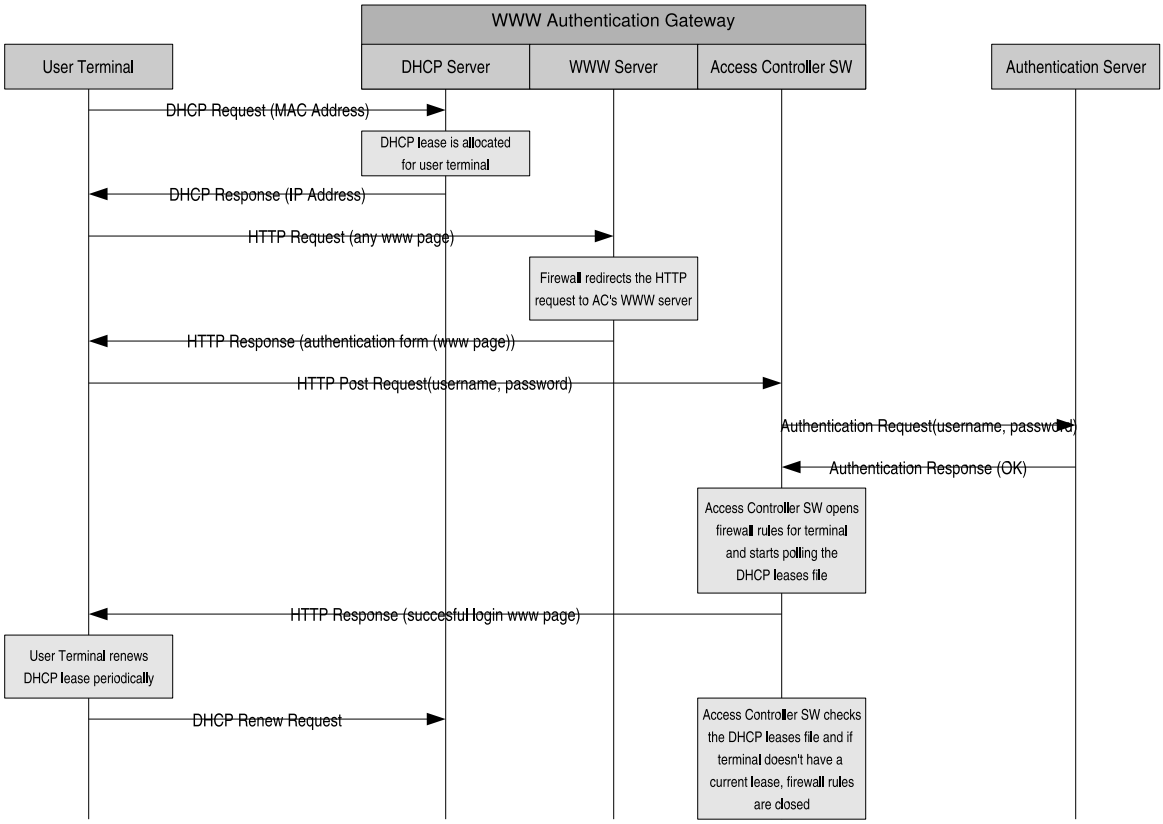

Figure 3.1: An example of the successful WWW-based authentication process

ered. Authentication WWW-page can also be used for other purposes like informing the user about changes in the network or instructing in the possible problem or mal-configuration situations. Moreover WWW-based authentication method is medium independent, and thus the authentication gateway can control the access from Ethernet network as well as from WLAN network. This medium independency ensures that access controller can also be used in the future for both authentication and instruction purposes if needed.

Unfortunately the disadvantages of this access control method are related to its security. Faking an access controller is relatively easy, if certificate management is not carried out properly or if the users are used to just accept self-signed certificates and enter their authentication information on the WWW pages without questioning the authenticity of the access controller. Another disadvantage is that WLAN networks are often configured to not to use any encryption. By finding out an authenticated terminal's IP and MAC address, it is possible to hijack and abuse some other user's connection by faking the IP and MAC address of the attacker's terminal in some implementations. It is also possible to eavesdrop unencrypted protocols and WWW traffic, which raises additional privacy issues.

3.4 VPN Authentication

While the WWW authentication was developed for operators, the VPN authentication was developed for corporate environment. In this kind of environment, one could assume that the terminals have VPN and other extra software installed. Because the VPN termination point already handles authentication before letting the user access the network resources, VPN can handle authentication and encryption requirements for securing both access and traffic to the corporate network. The network architecture usually used with VPN authentication is the one later described as access network model and is very near to the hotspot architecture displayed in the figure 4.1. The difference is that in the pure VPN authentication model the authentication gateway either terminates the user VPN connections or passes them through to strictly defined endpoints. All other traffic is filtered or rejected.

The greatest advantages of the VPN authentication approach are that the network connection to the home network is secured all the way from terminal to home network, strong authentication can be used in authenticating the user and VPN endpoint and the traffic is secured with strong encryption. All this can be achieved securely from any network in the Internet as the VPN authentication is media and network independent. The obvious disadvantage is that the model makes supporting visiting users harder because usually they cannot connect to the same VPN termination point and configuring firewall rules for each visitor with own VPN termination points consumes too much system administration resources.

4 Network Architecture Models

This chapter introduces three basic network architecture models, which are used in designing and implementing mostly wireless public area networks in organisational and operator environment. In addition to the architecture description of these models, this chapter also discusses the advantages and disadvantages of each model.

4.1 Operator Access Zone Model

The operator access zone model is a commonly used architecture model in the operator provided public WLAN access zones, often also called WLAN hotspots. It is based on the idea that every user is a visitor, or more precisely, a paying customer. Because of this, the access from the public access zone to the Internet and also inside the zone must be controlled so that unpaid, unauthorised use or hijacking other user's connection is not possible. The diversity of the customer terminals also creates the requirement to support as many different kind of terminals as possible. Often these requirements are solved by using WWW-based authentication presented earlier in Section 3.3.

The architecture of the typical operator access zone is presented in Figure 4.1. In addition to using WWW-based authentication and access controllers also other access control methods can and have been used for access control. One existing one has been SIM-card based authentication first introduced as a part of the Nokia Operator WLAN

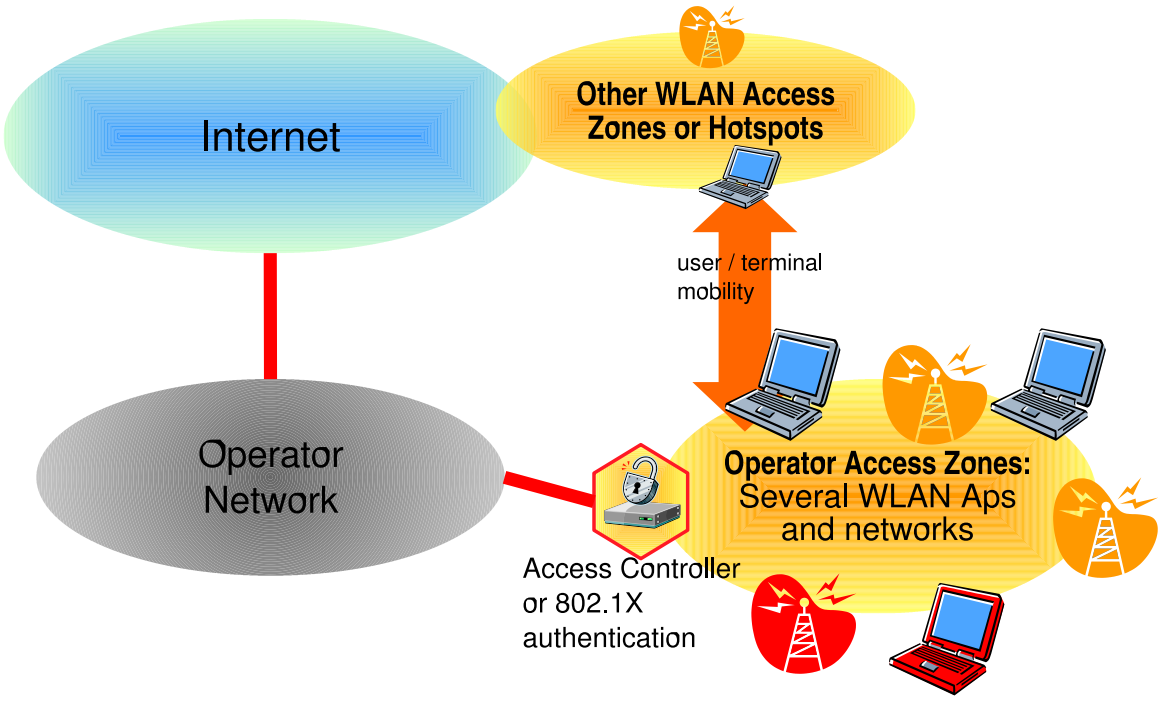

Figure 4.1: operator access zone model

solution [5] and later developed as an IETF standard extension to EAP protocol [6] called EAP-SIM [7]. So far both the SIM-based authentication as well as 802.1X authentication have not yet been widely spread because of the lack of support in the user terminals.

4.1.1 Advantages

The advantages of the presented architecture model are the support for the wide variety of terminals and the ease of use. Although the access zone architecture was not first standardised anywhere, most of the operator deployments converged into this kind of architecture, which was then chosen as a guideline [8] to implement WLAN access zones compatible for WLAN roaming between operators. For users the benefit of this kind of deployment was that the operator provided WLAN access zones around the world are at least similar, if not identical, to use. This improves the overall usability and user satisfaction, because the users do not have to learn multiple ways to use the access zones.

4.1.2 Disadvantages

The operator focused architecture also has its disadvantages. While paying for the Internet access seems reasonable to most users, the operator usually wants to bill also for using the WLAN network infrastructure itself even without an access to the Internet. To enable this, the operator may introduce filters in the access points to prevent user terminals to communicate directly between each other. Then, all traffic must go through access control device and sometimes through Internet to make peer to peer connections possible. While this kind of an approach is understandable from operator business and user terminal security viewpoints, applying filters usually breaks other useful functionality like IPv6 duplicate address detection for example. Without these filters, however creating rogue access points and attacking or infecting other user terminals in the access zone is a clear and present threat.

The EAP-SIM or WPA authentication in access points partially solves the filter problem, but unfortunately creates a few additional ones. One is naturally the terminal support, but the second problem is that the terminal using 802.1X does not have network connectivity before authentication and is therefore unable to receive for example the WWW-page from the access control device describing how to access the Internet. This problem can be circumvented by providing multiple parallel ways to authenticate — An architecture solution, which will be described in detail in the Chapter 5. The problem, which the EAP-SIM and WPA authentication do not solve, is the malicious or infected terminal. After authentication the terminal is again a part of the access zone and capable of infecting or attacking other terminals if terminal-to-terminal filtering in access points is omitted.

When considering organisational networks one important problem, which the operator access zone architecture fails to address, is the need for secure intranet access in addition to the Internet access. The regular operator access zone architecture does not address this problem, but on the other hand, does not limit the possibility to use for example VPN clients as long as the network authentication is satisfied via operator provided methods. The use of WWW-based authentication in the daily business may however become an annoyance when the use of the wireless network is regular and not random.

4.2 Wireless Intranet Model

While the operators have converged into the access zone model, in the world of organisations and enterprises the most common architecture is a model, which could be described as the wireless intranet model. The architecture is common in organisations, which have just adopted WLAN networks or which have increased their use gradually from the early adopters to other parts of the organisation. This has created a mixed network, where wireless and wired network are mixed together without real distinction or segmentation besides for example departmental ones like in Figure 4.2.

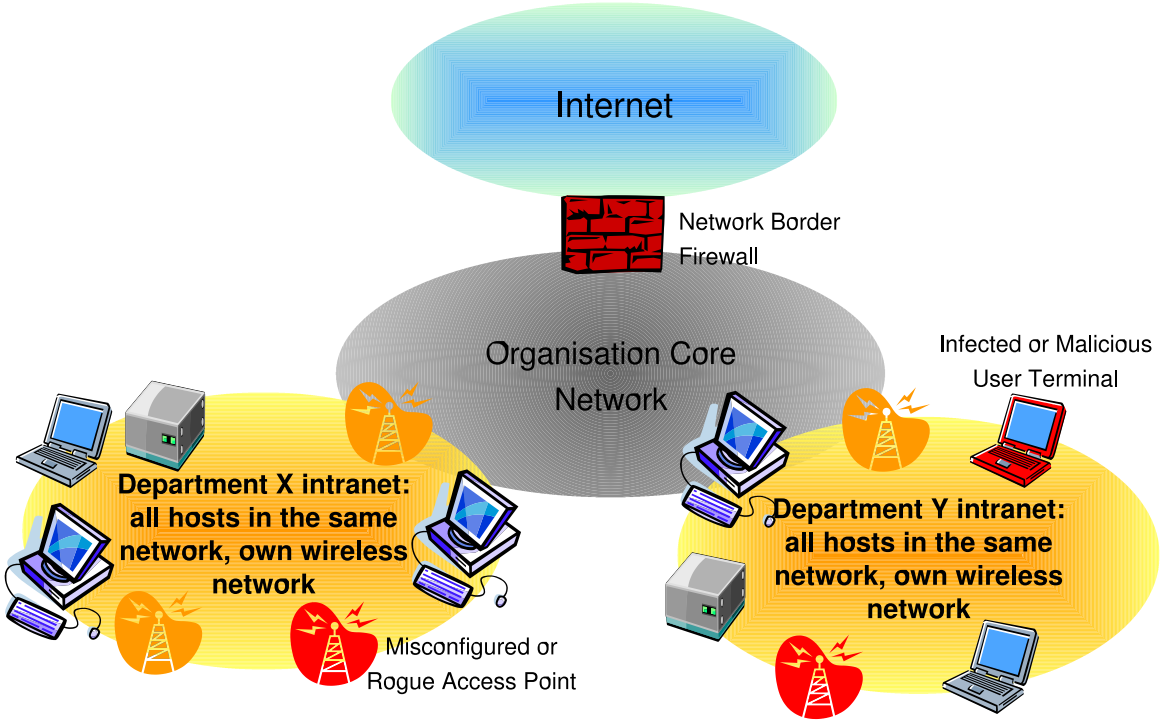

Figure 4.2: wireless intranet model

Often in this kind of networks, the network access control, if it is done in the first place, is based on WEP encryption and MAC address lists i.e. IEEE 802.11-based access control described in Section 3.1. In the more modern deployments these methods have been replaced by the WPA/WPA2 based approach (Section 3.2) securing this way the radio access, but at the same time failing to address the network security as a whole.

4.2.1 Advantages

The major advantage and also a major disadvantage of this model is that it is easy and simple. It is easy to deploy and easy to use at least within one network, for example one department of the organisation. There are no extra requirements for designing and modifying the services and the wireless and wired, mobile and fixed terminals are treated equal in a combined mixed network. This creates an illusion of simplicity and functionality when wireless or mobility requirements and threats are not being considered.

4.2.2 Disadvantages

In this model, fixed and wireless networks are mixed and the wireless network is considered just as cable-replacement. Network services like e-mail and Windows file sharing and domain services are used without additional encryption. The Network is protected from threats coming from Internet, but internal security is neglected. A single misconfigured or rogue access point may provide an attacker way straight to the heart of the network. Infected mobile terminal easily infects the whole company network or at least one network segment i.e. department in Figure 4.2. Malicious user (terminal) can eavesdrop network traffic without detection as the services generally are not protected with TLS/SSL as long as the user terminal has passed the access control. The mobility is often not considered, for example how does the user read her emails from or via a foreign network.

4.3 Access Network Model

The access network model (Figure 4.3) is an architecture model, where the operator access zone model is applied to the organisational network environment to provide an architecture that combines the ease of use of the wireless intranet model and the user terminal indifference and visitor features of the operator access zone model.

In this model the wireless network is separated from the intranet to a separate network

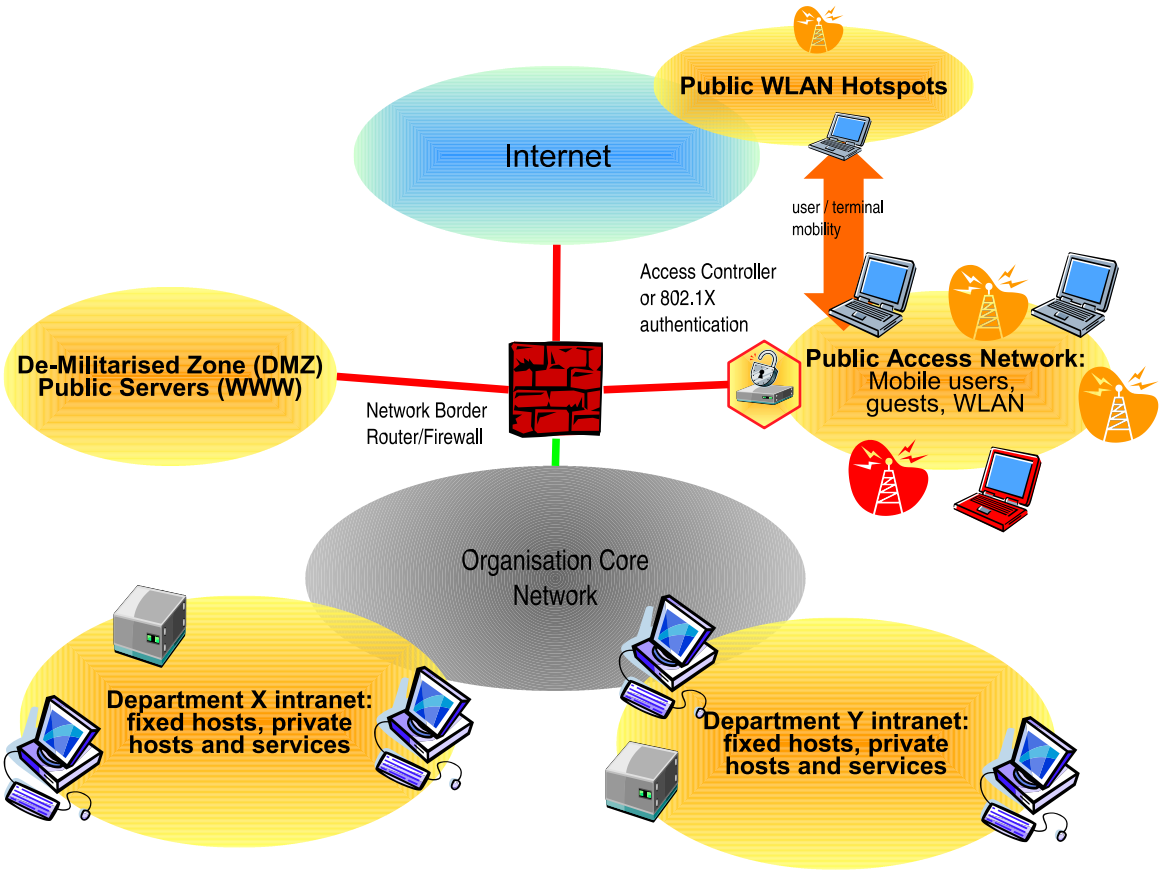

Figure 4.3: access network model

called the public access network. From the security perspective, the public access network is as untrustworthy network as any other in the Intenet. Because of this, the public access network is positioned outside the organisation's intranet and firewall as a separate access network much like the demilitarised zone often used in organisational networks. This way breaking the access control system in the border of the access network grants the attacker only the access to the Internet instead of direct route to organisation's intranet.

The public access network is common to all the employees of any department as well as to the possible visitors. The separation of user groups is done via different access control and traffic securing solutions. Several different ones may be used from access controllers to WPA, from TLS/SSL secured traffic to the full VPN deployments.

4.3.1 Advantages

The first and most important advantage of this model is that the wireless or mobile network is now a separate network. The special qualities and requirements of the mobile terminals can now be handled better than in the mixed model. For example the security and usability are now considered also from mobility's viewpoint instead of relying wireless network to be just a cable replacement. This means that the organisation's communication services must now be designed so that they are secure even if they are used by mobile terminal in a hostile network. More attention is, and must be focused in the mobile terminal security because there are not any place for terminals that could be considered safe.

The above together with the model's other requirements from organisation, clarify and add security also to the organisation's other infrastructure by creating processes and practices needed to support mobile users and overall mobility. For example VPN or secure email services that were originally created and deployed for public access network can be re-utilised in providing secured access to organisation resources and intranet also from employees' home ADSL connections. The user experience still stays the same wherever the user is. The WWW authentication is the one operator hotspots use and the VPN can be used to access the intranet resources in the public access network in home coverage area or in the operator hotspot in the same way.

The separation of the mobile network from the organisation's internal network also enhances the security by making the area open for infection or infiltration smaller. The malicious or infected terminal can attack hosts and services inside public access network, but the hosts and services in the internal network are not in immediate danger as is the case in the wireless intranet model. The misconfigured or rogue access points and found weaknesses also do not immediately invalidate the security of the organisation's whole network. In fact as long as the rogue access points are connected to the public access network and relay traffic they work like the valid access points.

Because the access control methods and traffic securing solutions are not forced, both old and new access points can be used in the same network and be gradually upgraded

when the requirements increase. This encourages to the cost-effective network evolution instead of the upgrade revolution everytime a new access control technology is discovered.

4.3.2 Disadvantages

Most disadvantages of the access network model are dependent of the chosen access control methods and access point capabilities in case wireless network is used. If the only access control method is WWW-based authentication and the access points are used just as wireless bridges without encryption, the model is as vulnerable to the man-in-the-middle attacks and faked access controllers as the operator access zone model. If access point traffic filteration is not used, the user terminals may still attack, infect or listen to each other's traffic as well as use the public access network area for peer to peer traffic between terminals. What is different, however, is that if more security is required, more secure access control methods can be used in parallel with the old ones to provide all capable terminals a more secure access without abandoning support for the legacy systems and terminals.

5 Architecture

This chapter describes the TUT Public Access architecture, its goals and design principles, functionality and network architecture as well as presents a SWOT (Strengths, Weaknesses, Opportunities, Threats) analysis of it.

5.1 Goals and Design Principles

In the beginning of the project the author defined, identified and collected a set of goals and principles to guide the design work of the architecture. The following set was then presented to, and approved by the TUT IT Management.

5.1.1 Sufficient Security

Defining the security requirements was one of the most important guidelines as it controlled the selection of the access control methods, and affected also the selection of network architecture model.

For TUT Public Access sufficient security meant that all users had to be authenticated before they gained access to the network. It also meant that the user access to the network, or the access from network to user terminals, could be limited to secure the network from users, and the users from the network. Gaining unauthorised access to network had to be difficult enough to encourage most of the potential attackers

to give up. To secure the privacy and confidentiality of the users' traffic, the users had to be able to use encryption solutions to secure their traffic, without architecture limiting this possibility.

5.1.2 Flexibility, Upgradeability, Scalability

The architecture had to make it possible to introduce new services and network elements without having to redesign or reorganise the entire network. Also the technology and network element upgrades had to be possible without having to prepare for long downtimes. The architecture had to be designed so that it would not limit the scalability, and the natural growth of the network.

5.1.3 Interoperability, Openness, Standards

The architecture had to support both the commercial and the noncommercial network elements via standardised interfaces. Open standards and interfaces were to be preferred and closed vendor specific solutions avoided.

5.1.4 Usability

The architecture was not to require any additional hardware, software or operating systems from the user terminal. This means that the user should be able to gain basic access to the network having just a compatible network adapter in the terminal.

5.2 Functionality

The key in defining a network architecture for a heterogeneous organisation like Tampere University of Technology is realising that there really does not exist a single solution for access control that would satisfy all the users. Because of this, the author decided to utilise standard software engineering practices in designing the architecture, namely identifying roles, use cases and collecting the different requirements of

each one of these. Four user roles i.e. different ways to access the network were found during the process.

5.2.1 Basic User Access

Basic user access was originally called student access, because students were the first users to be identified having this role. A basic user is a kind of user that uses the network access for email, WWW browsing and handles file transfer mostly using these methods, but may also in some cases use different file transfer methods, like the ones SSH client offers. All of the services the basic user uses can be secured with encryption without using additional software like VPN clients. This means that the only thing required from the access control and network is just to provide and control the access to the Internet.

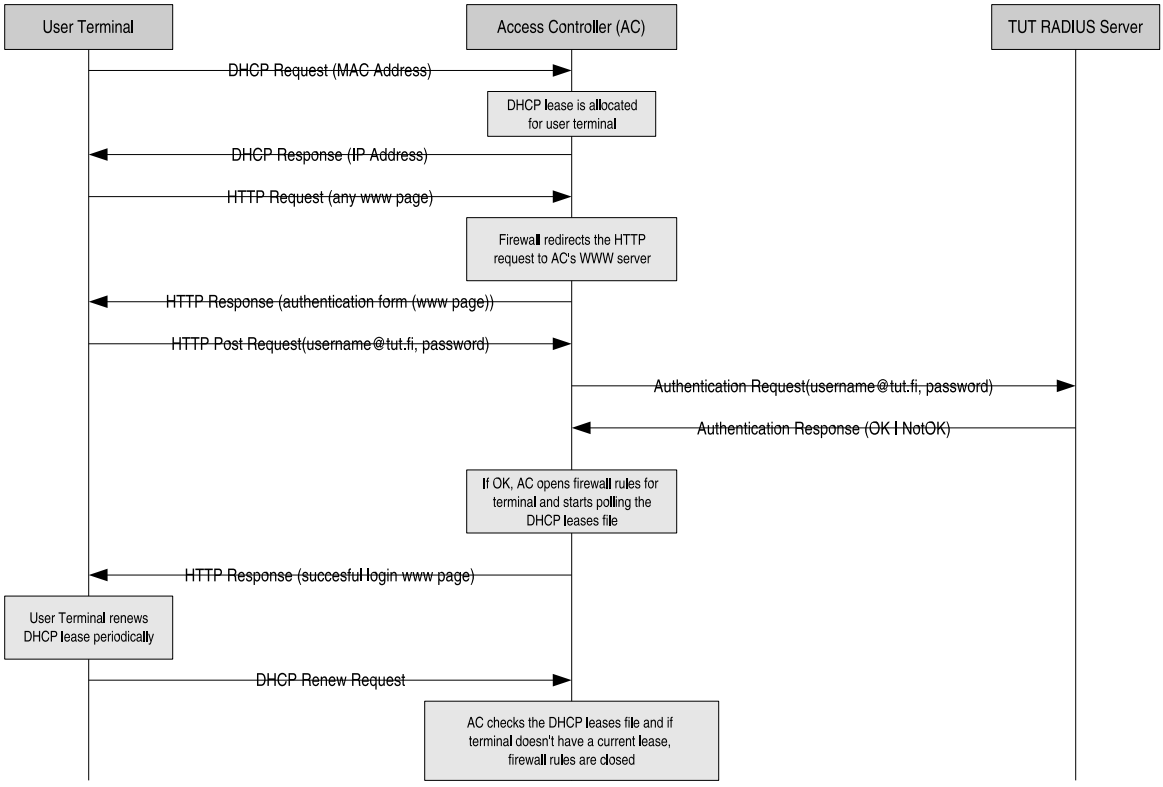

Figure 5.1: basic user access

The simplicity of the user requirements made it possible to select WWW-based authentication (Figure 5.1) for an access control method. Because WWW-based authentication did not require any extra software in the user terminal, this was the easiest

and also the most interoperable method for controlling the access for a very diverse set of user terminals.

5.2.2 Secure User Access

The basic user access fails to satisfy the security needs of the users using Windows file sharing, printing, and other applications that do not include application-level encryption. An IP transport-level encryption is needed to secure this kind of user traffic and so the secure user access method was designed.

Because the user requiring secure user access could now be assumed to have a fixed connection to the organisation and possibly a organisation owned terminal, the requirement for no extra software in the user terminal could be interpreted more loosely. On a IP-transport level, VPN software is the common solution to secure traffic over hostile networks, and as the VPN can also function as a authentication solution, the VPN-based access control method was selected for securing both the user access and the traffic.

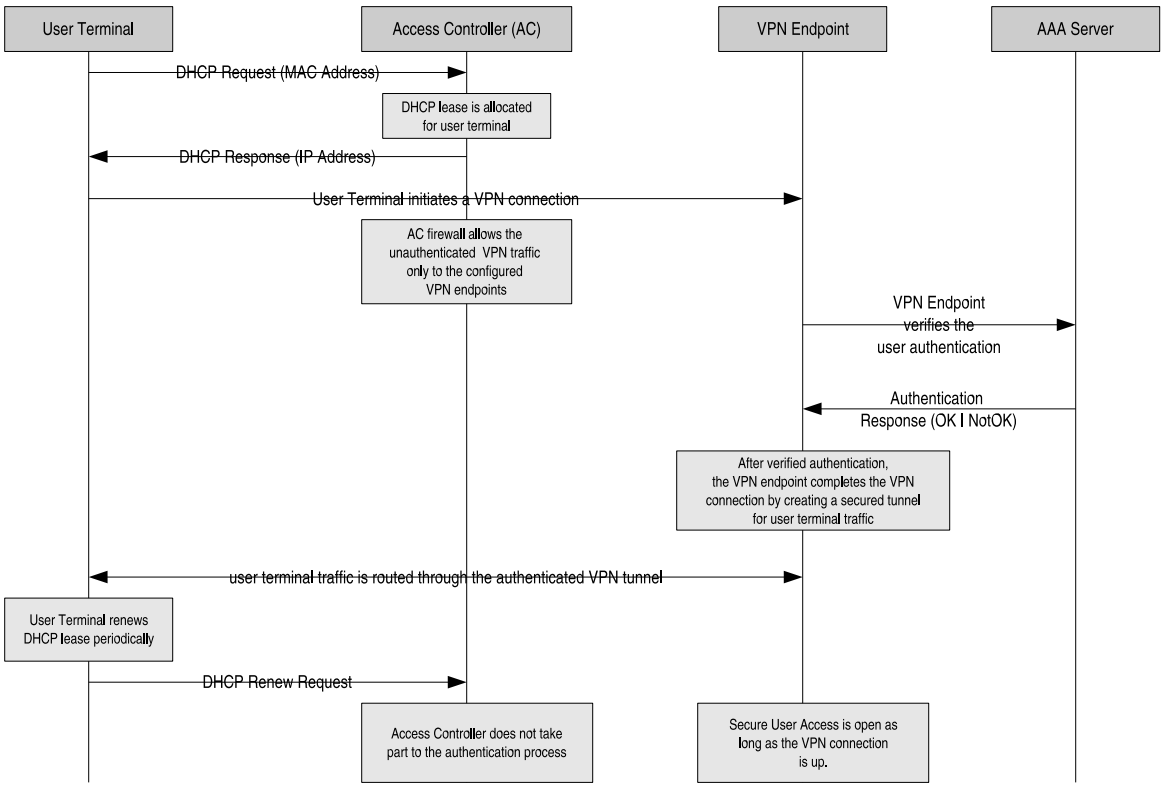

Figure 5.2: secure user access

To make the authentication easier for users, and also to remove the need for double authentication, the WWW authentication was removed. It was replaced by the assumption that if the VPN client succesfully connects to some known VPN termination point and manages to route traffic through the VPN termination point, the user already has a legitimate access. This way the secure user access could be designed to function like presented in Figure 5.2. Now the users didn't have to enter their access credentials twice, the authentication for VPN connection was enough.

5.2.3 Guest User Access

In a networked organisation with several cooperating organisations and partners, there is bound to be a lot of visitors. Most of these visitors do not have any formal connection to the organisation and cannot this way authenticate against the organisation's authentication database. These kind of users required a guest user access to be developed for the TUT Public Access network.

Because having the users constantly added and removed from the TUT authentication database would have been both resource consuming and would possibly compromised the user database integrity, a separate authentication database and software for handling temporary users was developed.

The idea of the guest server access becomes apparent in Figure 5.3. The network access control method is identical to the one for basic user access, but the authentication system and the management of the users is handled differently.

In the guest user case, the power and responsibility to create user accounts is designed to be given to the host or some other organisation employee, who in the practical sense is also responsible for his or her visitors and their conduct. By storing the information who authorised and created the temporary user accounts used to access network, an organisation employee is connected to the guests. This way a temporary user utilising guest access may in abuse cases be traced at least back to the person who authorised his or her access.

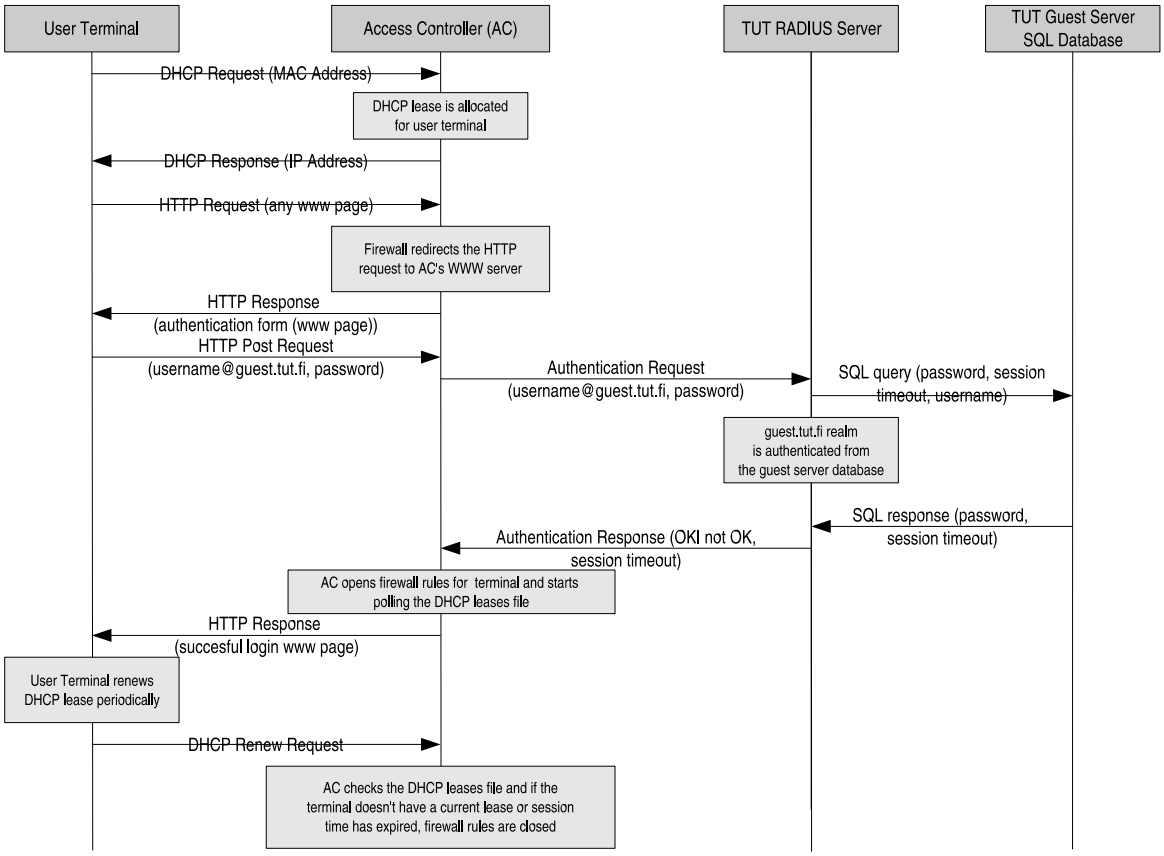

Figure 5.3: guest user access

5.2.4 Roaming User Access

The roaming user access (Figure 5.4) is based on the idea of RADIUS-based WLAN Roaming. The idea was first presented by the WirLab [9] for the operators and other interested parties. The presentation inspired Sami Keski-Kasari and the author to develop the idea further and adapt it to fit into the requirements of Funet network [10] and organisations. A RADIUS hierarchy was created to enable roaming between Funet organisations. The parallel RADIUS-based roaming projects in Europe made it possible to connect the RADIUS hierarchies to what now is called EduRoam [11] roaming infrastructure.

With the help of the roaming infrastructure the users of the participating organisations are able to use their home organisation user credentials to get a network access in any compliant organisation without having to find out how to get guest access to the network. This also reduces the load of the visited organisation's administrative staff

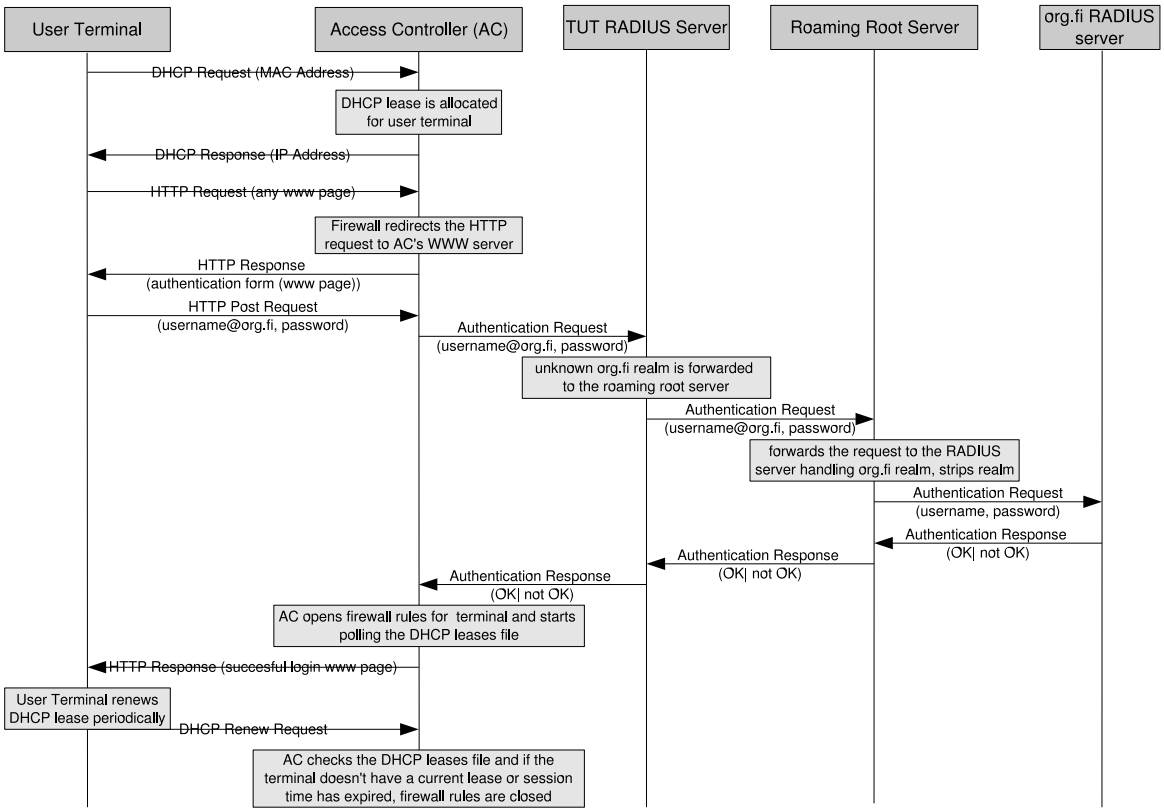

Figure 5.4: roaming user access

as guest accounts do not have to be assigned and distributed to those users, who utilise roaming user access.

The roaming user access was actually invented and designed before the guest user access, which now utilises the same idea to create the required functionality. The similarities can be found by comparing Figures 5.4 and 5.3.

5.3 Network Architecture

While the selection of access control methods was mainly guided by the roles and use cases of the users, the design of the network architecture was based on the well-known practices, security and management requirements.

5.3.1 Internal and Public Networks, Access Controllers

From the beginning of the project the selection of network architecture was quite clear. The development should lead from separate and incoherent wireless intranets to a common unified access network model. The access network model, presented in Figure 5.5, was the only one that was flexible and secure enough to handle TUT's heterogenous user and terminal base.

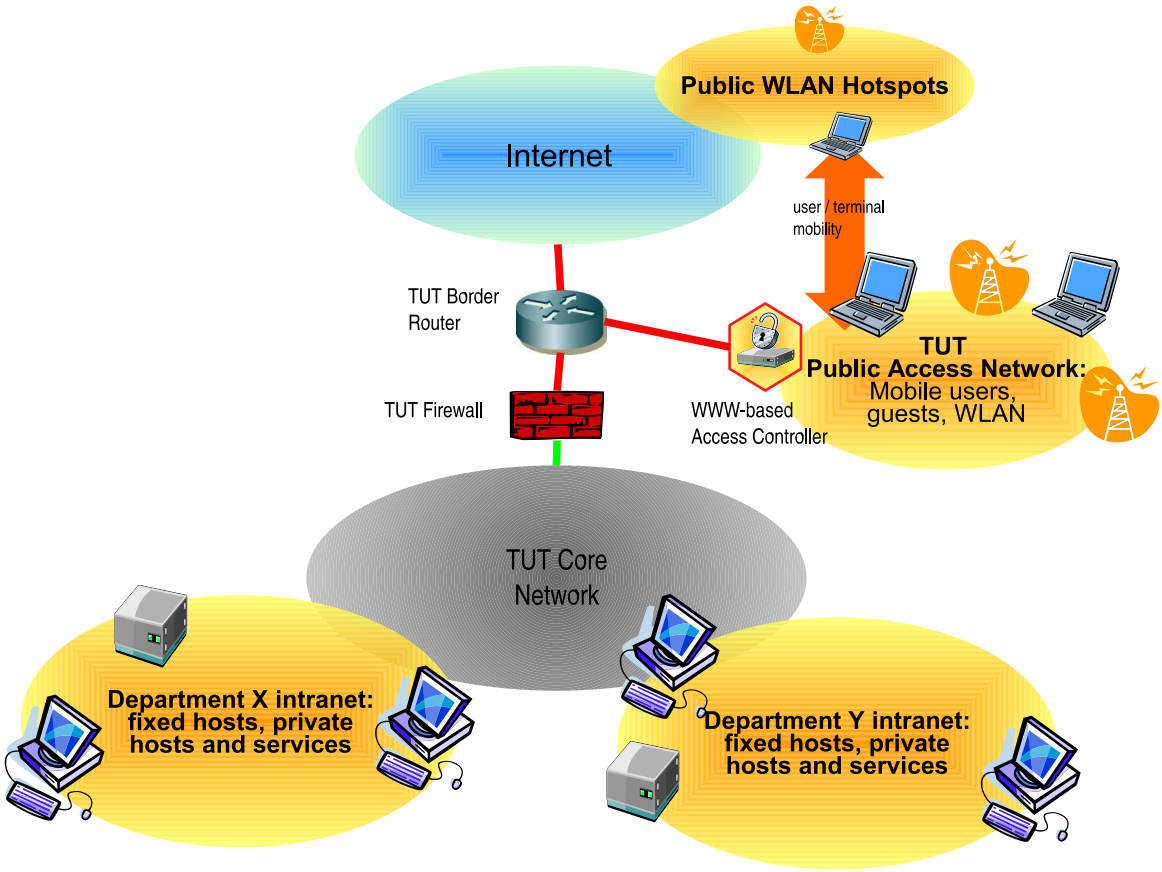

Figure 5.5: TUT Public Access Network

The WWW-based access controller provides the means to authenticate the user terminals without the need for users to install additional software. The separation of mobile network and internal networks protects the possibly vulnerable hosts and services in the department intranets as well as in the rest of the TUT core network.

The clarified network architecture also provides clear control points — the access controller and the TUT firewall — for controlling wireless mobile terminal access to TUT network services. This makes it possible to implement multilevel security for

wireless access. Even if the WWW-based access controller would fail to function, the TUT internal network would not be completely open for attack.

5.3.2 Securing Network Traffic

The sections describing basic user access (Subsection 5.2.1) and secure user access (Subsection 5.2.2) already mentioned the lack of linklevel encryption and the necessity of encrypted protocols in securing the network traffic. Because of this need, additional infrastructure like secure email services and VPN service architecture (Figure 5.6), were developed in cooperation with TUT's IT Management.

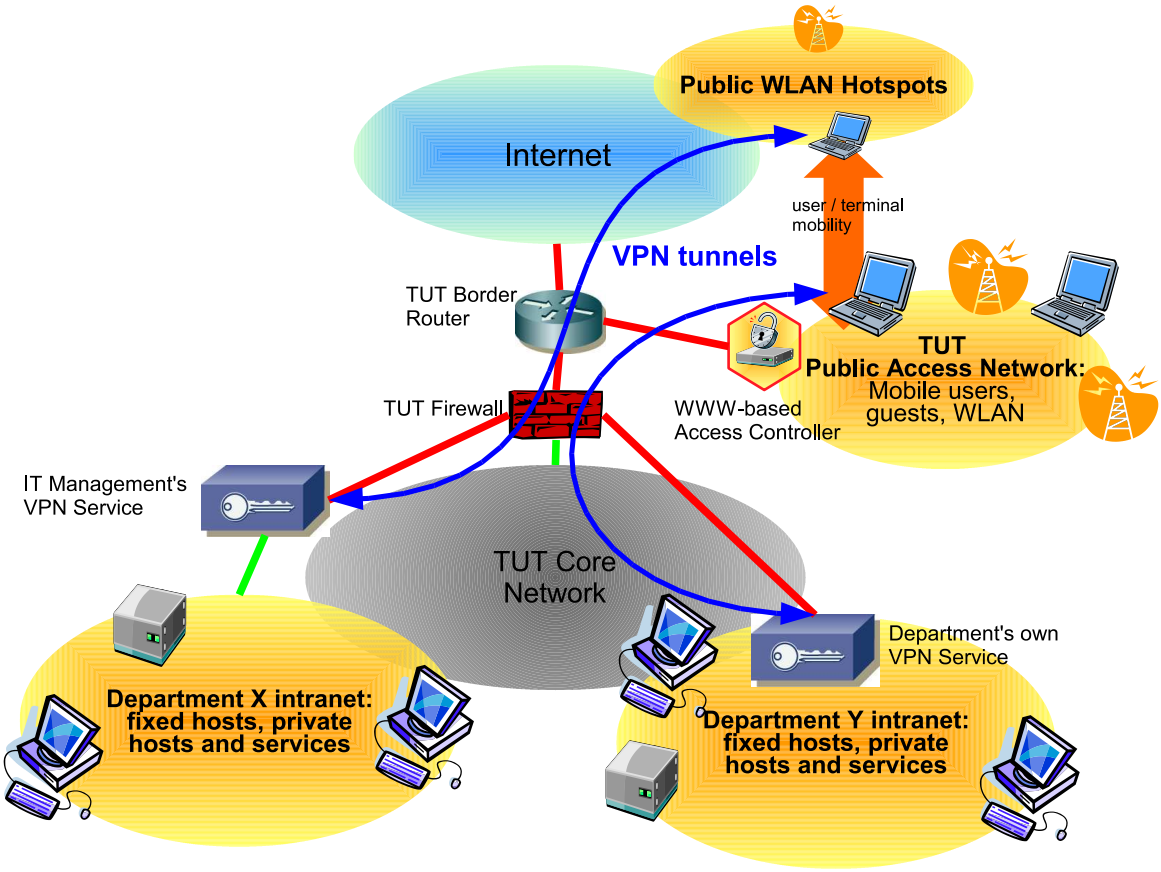

Figure 5.6: VPN architecture

The VPN architecture was developed based on the principle that also the VPN client should be used same way whether the user was in the home network or not. This way the same VPN architecture could be utilised in securing network traffic from everywhere to home network.

Because of the different requirements for management of the internal network services, and varying system administration competencies in different departments, the VPN service was designed to be implemented as a IT management's service or the department may also implement its own solution. The IT management's service is a centralised solution for departments with common requirements for securing network traffic or who already are utilising other IT management's administration services. The Department VPN service, on the other hand, is for departments requiring more flexibility, control or some special settings and software.

In addition to the VPN solution, also TLS/SSL secured authenticated SMTP and IMAP mail services were introduced by IT management to offer lightweight secure email access for mobile devices and users. This way having a VPN client is not an obligatory requirement as emails can already be read and sent securely and file transfers can still be made with SSH secured solutions.

5.3.3 Radio Network, WLAN Access Points and VLANs

The initial TUT WLAN environment consisted of several separate WLAN islands, which usually were not designed to provide mutual WLAN coverage. Only channel settings were sometimes discussed, when there was trouble with overlapping channels. The 802.11b and 802.11g networks have only three channels that won't overlap and cause interference with each other [12]. Because of this, multiple separate WLAN networks in the same space could cause so much interference that the performance of the network would be severely degraded. In a unified radio network model, like TUT Public Access, it is possible to prevent this because there's only one official network service provider providing and controlling the WLAN network.

The TUT Public Access architecture was designed to embrace all access points, both new and old ones, so that they all could be used to provide WLAN coverage. This was realised by using VLANs to separate TUT Public Access traffic from network management traffic wherever it was possible (Figure 5.7). With the old access points not capable of VLAN traffic separation, the management traffic was designed to be routed through the access controller.

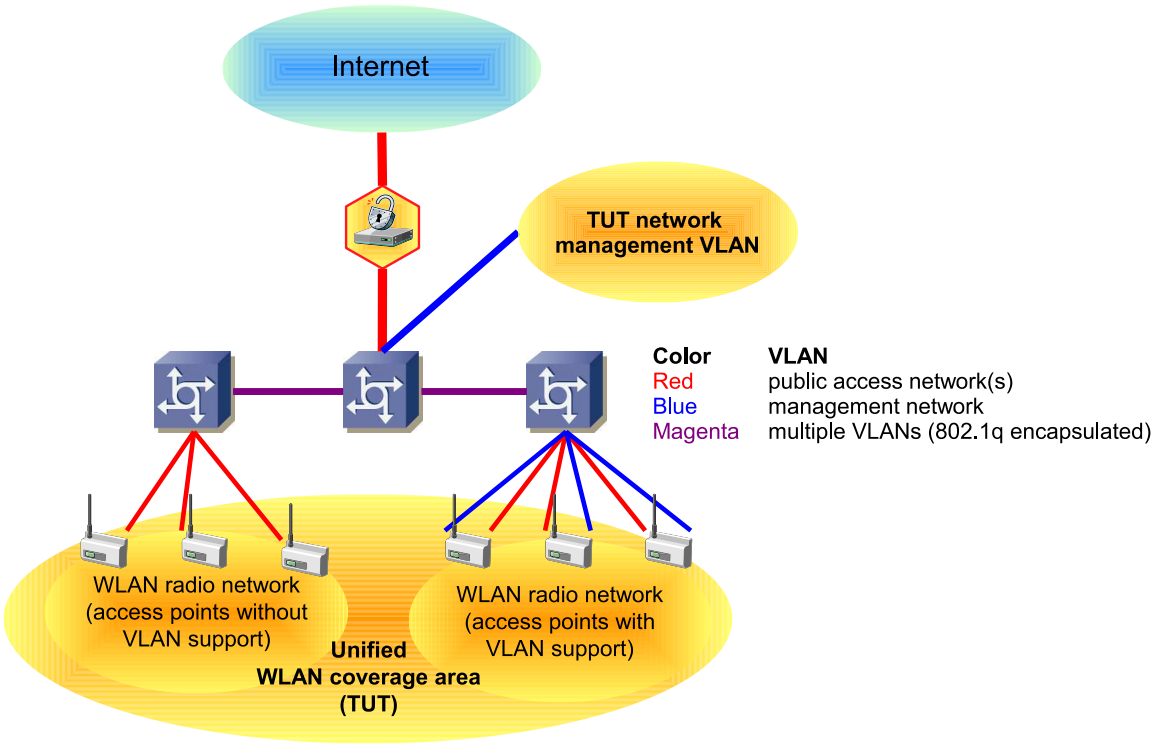

Figure 5.7: Radio network, WLAN access points and VLANs

In addition to improving security by separating the traffic, the utilisation of VLANs and VLAN capable WLAN access points also provides a way to add flexibly new WLAN networks and authentication methods. This functionality is a key feature in enabling the future development of the TUT Public Access network, presented later in Section 6.3.

5.4 Strengths

This section summarises the identified strengths and advantages of the TUT Public Access architecture. It is also the first part of the SWOT analysis promised in the introduction of the chapter.

5.4.1 Architecture Advantages

The most important architectural advantage, is the logical and physical separation of the mobile network from the rest of the organisation's network. This mobile network

could then be designed with the mobility and mobile security requirements in mind. The separation from the department intranets made it also possible to use the same network for students and guests, which was not possible with the old model.

The access controller provides single clear control point for network access from the WLAN networks, when earlier there were as many control points as there were separate WLAN network installations. Most of the old control points also were more like uncontrolled points as the competencies of the system administrator staff varies between departments.

The new architecture provides also additional security compared to the old access control by placing the access controller to control the access to the Internet instead of trying to control the access to department intranets. The difference is that, if TUT Public Access access control is compromised or bypassed, the access gained, is only the access to Internet and very limited access to the TUT core network. In the old model breaking the access control would have provided a direct attact route to the TUT's inner networks.

5.4.2 Usability Advantages

The design of the TUT Public Access user interface was based on the common practices in the WLAN networks making it possible to create same kind of user experience the user would have also in other external WLAN networks.

The selection of WWW authentication for access control method made this possible. The user needs only to learn to start and use WWW browser to gain access to the network — an authentication method, which is used in most WLAN service networks and hotspots all around the world. This also works on a local level. The wireless network can be used same way throughout the campus. The VPN services extend even this, and could be used same way wherever in the world and whenever the user had some kind of network connectivity.

By selecting this kind of a common way to authenticate, also security training and education of the users could now be concentrated on this authentication method, mak-

ing it easier for users to remember the related important security issues like verifying of the SSL/TLS certificates.

5.4.3 Synergy Advantages

The first synergy advantage was already mentioned in the Section 5.3.3. With unified and common WLAN network architecture different departments can consolidate their radio network coverage and network administration, decreasing the possibility for overlapping networks, interference and administration efforts. The departments do not have even to invest to new WLAN access points to be able to join to the common architecture, because of the architectural support for also the older access points.

Securing the existing services and deploying new ones, like the VPN access, drives the organisation information and service infrastructure evolution. Most of these new and secured services can also be used in other use cases. In TUT's case this was proven, when the access controller and VPN infrastructure were used to control and secure network access from fixed ethernet sockets around the campus and also from employees' home ADSLs. The VPN of course was even more useful as it could be used from everywhere just like the TLS/SSL secured and authenticated email services.

5.5 Weaknesses

This section describes identified weaknesses in the TUT Public Access architecture. All of the weaknesses were already found and considered in the design phase of the project, but found acceptable when the overall security was considered.

5.5.1 Denial of Service Attacks

The denial of service attacks can be differentiated at least to intentional and non-intentional attacks. For intentional attacks against wireless networks, there are not really other feasible defense methods than the legislation and the organisation's information system usage rules. Anybody can start a denial of service attack against the

network, but it is usually the fear of consequences, which discourages attackers to try.

A more likely denial service attack is an unintentional one. It might be badly configured rogue access point, which is not able to pass traffic through it, or even radio interference from the too closely or badly installed access points. Also a terminal configured to be an access point or in ad-hoc network with the same network name, may cause local denial of service situation. At the IP level, a terminal distributing IP addresses with DHCP in the public access network can also cause problems within one public access segment.

The best defenses for these kind of attacks are the working network monitoring system and of course educating the users so that there will not be so many rogue access point installations or configuration errors in the terminals.

5.5.2 Man-in-the-Middle Attacks

The worst weakness of the WWW-based access control system is the man-in-the-middle attack in one form or another. The unsuspecting terminal may be lured to impersonating host with DHCP or ARP based attack like in all networks utilising TCP/IP [13] protocol. Once the victim's traffic is routed through the attacker's system, attacker can try to confuse the user to accept self-signed, or in a worst case completely verifiable certificates, as authentic ones and give the authentication information this way to the attacker instead of the real authentication system.

In the most sophisticated implementations [14] of the man-in-the-middle attack, this all can be done transparently to user. The user just has to be uneducated enough to accept self-signed certificates without checking them. The man-in-the-middle attack is valid for all protocols using some kind of certificates or public/private key authentication ranging from email transfer protocols to VPN services like PPTP, SSH and IPSEC. However, most of these protocols and their implementations can be configured to accept only the certificates verified by one specific certificate authority, or at least warn about not verifiable ones. So the technical methods to warn the users exist, but the user education is still the key method in defending the architecture against the attacks based on this weakness.

Partly because of this weakness, partly because of the privacy weaknesses related to the TUT Public Access, a WPA/WPA2 based access control is being gradually introduced to the TUT Public Access architecture. When the technology has matured and been tested enough, it can be introduced as a primary method for secure authentication, while the WWW-based access control can still be used for guest and temporary easy access solution.

5.5.3 User Privacy

As the Basic User Access (Section 5.2.1) does not provide any means to encrypt the network traffic on a link level, it is possible to listen the unencrypted radio traffic of the terminals within listener's reach. Encrypted protocols are of course still secure, but it is possible to follow for example unencrypted WWW surfing of some other user. For a long time there has already been implementations of these kind of tools for Mac OS and UNIX operating systems like EtherPEG [15] and Driftnet [16].

Using VPN corrects also this problem, but the VPN is not available for all users. The already mentioned WPA/WPA2 brings a more elegant solution for this by providing terminal specific dynamically changing encryption keys for securing link-level traffic.

5.6 Opportunities

Few of the opportunites of this architecture have already been utilised. Namely, the opportunity to use the WWW-based access control and VPN architecture to secure also other traffic than the one in the wireless networks.

The key opportunity with the TUT Public Access architecture is however its flexibility and scalability. The architecture makes it possible to introduce new campus-wide services and solutions instead of heavy adaptation work required with separate department wireless networks. In the same way, research and service piloting is possible to be conducted in a campus-wide network without the need to build an another separate research network.

The roaming functionality of the TUT Public Access architecture makes it also possible for users to gain access to the network with their own user credentials in several other universities around Finland [17], around Europe and even in Australia [11].

5.7 Threats

Although the architecture has its known weaknesses, many of them have already been dealed with or improbable enough not to be accounted as threats. However, there still are several issues the author considers as some kind of threats to the functionality of TUT Public Access architecture, if they are not considered when developing the infrastructure.

One important threat is the growing number of access points, their management and security. The current method of one-by-one access point configuration or SSH-based scripts are not scalable enough to handle the large amount of access points, their software upgrades and configurations. The number of access points is also growing because of the access points in employee homes creating new challenges for the configuration management of both the access points and the user terminals. WPA/WPA2 configuration in terminals is not as easy to set up [18] as using the WWW authentication for network access, which demands also more from the user support and system administration staff.

With the increased number of access points, the need for radio planning and radio network management becomes also an important issue as it is possible to cause unintentional denial of service situations with radio interference.

Both of these threats can be handled with a network management and control system, which fortunately is already being considered by the TUT IT management and some options are already being evaluated during summer 2005.

6 Deployment

This chapter summarises the TUT Public Access architecture development and deployment project experiences, found problems and solutions as well as future development plans.

6.1 The TUT Public Access Project

The beginning of the TUT Public Access Project can be clearly fixed, but the end of the project is a matter of definition of the project's end. The TUT Public Access architecture was designed to be an evolving architecture and the service is still constantly being developed in cooperation between TUT IT Management and Arch Red. To make the project timeline easier to follow, the author decided to identify important dates in the project's history and define them as markers in Table 6.1. The phases of the project can now be defined in relation to the markers. Defining the project phases any other way would be pointless, because there were not any other clear milestones or deadlines in the development of the TUT Public Access architecture.

6.1.1 M1 — M3: Technology Evaluations

The time between markers M1 and M3 was mostly spent evaluating and comparing different WLAN access points, access controller software and network architecture

Table 6.1: Important markers in TUT Public Access Project

Date	*Marker*	*Description*
2002-03-01	M1	Author starts working with the TUT Public Access project.
2002-04-10	M2	The subject of author's thesis was approved.
2002-09-26	M3	WirLab presents Inter WISP WLAN Roaming idea.
2002-11-25	M4	TUT Public Access architecture and Funet WLAN Roaming idea presented at the Funet Technical Days
2003-01-10	M5	TUT Public Access architecture description (in Finnish) completed.
2003-01-28	M6	Arch Red Oy founded by author and two colleagues.
2003-05-22	M7	TUT Public Access architecture and Funet WLAN Roaming are presented in the TERENA conference in Zagreb, Croatia.
2003-05-22	M8	WLAN pilot network in the TUT library announced.
2003-06-27	M9	ICE WLAN network reconfigured according to TUT Public Access Architecture
2003-10-31	M10	Wireless Mobile Vaasa announces Palosaari Campus Wireless Network, Tino access controller software, and joins unofficial Funet WLAN roaming root at TUT.
2003-01-19	M11	Arch Red delivers an access controller product to TUT's Pori unit.
2004-02-18	M12	TUT access controller is replaced by Arch Red's access controller product.
2004-04-21	M13	CSC announces the official Funet WLAN roaming pilot.
2004-05-26	M14	CSC and Arch Red announce Funet WLAN Roaming Root Service agreement.
2004-06-03	M15	TUT and Arch Red make official announcement of the TUT Public Access network.
2004-12-07	M16	Guest account functionality announced by IT Management.

options for TUT Public Access. Preliminary plans for architecture were drafted and presented to the IT management and some of the requirements and design principles were already collected.

The access points in the existing WLAN network of the Institute of Communications Engineering (ICE) were replaced with up-to-date access points, but the network architecture was not changed in this phase. The introduction of the new access points in the ICE network however helped in getting deployment experiences from the real production environment as well as some conception of the current functionality of modern WLAN access points. This helped in confirming the architecture design decisions and hardware recommendations for example when the different access control methods and access points were considered.

6.1.2 M3 — M6: Architecture Design

Wirlab's presentation [19] in Autumn 2002 marked a significant point in the architecture design phase of the TUT Public Access project. The idea of applying the RADIUS-based WLAN roaming in the Funet network was invented in this meeting and it developed into an action plan during the author's and Sami Keski-Kasari's train trip back to Tampere.

The WWW based access control method was already chosen in this phase to be part of the TUT Public Access architecture, but also 802.1X access control was already added as part of the future development. The RADIUS WLAN roaming architecture supported both technologies, so the RADIUS-based roaming was integrated directly as a part of the TUT Public Access architecture.

During the period between M3 and M6, the TUT Public Access architecture [20] clarified and matured so that it could be presented with the Funet WLAN Roaming initiative [21] at the CSC's annual Technical Days conference in Helsinki. The developed architecture was also presented to the IT management and after approval it was also documented to a more formal architecture specification [22].

6.1.3 M6 — M10: Piloting and Promotion

M6 marked the time to start turning the designed architecture from research to reality. The first version of the access controller was already ready, but it had not been tested in the production environment with real load due to the lack of testing resources in the project. The TUT's library was on the verge of deploying a new larger WLAN network for student use and had already negotiated with Nokia, which was willing to donate WLAN equipment for the purpose. This was seen as a perfect opportunity to test the designed architecture in real use and utilise the gathered feedback and test information in refining and verifying the design decisions.

The TUT library pilot was started and published at the same time the developed public access and roaming architecture [23] was also promoted in the European research and education network conference in Zagreb, Croatia. In the same session also the 802.1X-based roaming architecture [24] was presented. Both of these architectures were later combined to the European roaming architecture now known as Eduroam.

Locally at TUT, it was decided that the Institute of Communications Engineering would be the first to reconfigure its network as part of the TUT Public Access as an example and proof that the pilot really worked also for employee access as it was designed. The possibility to join to the new architecture was also promoted to other departments, but most of them still seemed to wait the results of pilot and only the new WLAN deployments were made part of the TUT Public Access network.

Meanwhile, the published pilot, combined to the promotion work already done for the rest of the architecture and Funet WLAN Roaming, started to gather interest also from other Funet organisations, which were interested in deploying WLAN networks for common use. The Wireless Mobile Vaasa project was one of the first to make contact and utilise the lessons learned in developing TUT Public Access architecture. This made the Palosaari Campus Wireless Network [25] also one of the first ones to join with TUT and Wirlab to the Funet WLAN Roaming initiative. The Wireless Mobile Vaasa also made a valuable contribution back to TUT's Public Access network by developing the first version of the open source access controller software called Tino [26].

6.1.4 M10 — M13: Making Products

During the TUT library pilot several errors were found in the access controller software, which was originally chosen to handle the WWW-based authentication. Some of these errors were corrected or bypassed but the software did not seem to be live up to the expectations of a ready product. Especially, when one error in the software left the firewall rules open for certain IP address, it actually blocked the user from reauthenticating. This, of course, created a security problem, but the architecture compensated here offering a possible abuser just a free Internet access instead of the access to the intranet or worse. Piloting also revealed a lot of terminal side issues that were not visible when using the network with just a few mostly correctly configured terminals. The diversity of the terminals used to access the TUT Public Access pilot network however helped to develop and refine the architecture to consider a greater variety of terminals and settings.

The trouble with the original access controller was also where the Wireless Mobile Vaasa's contribution was found valuable. Because of the trouble with the same access controller software, they had decided to implement their own and while the new software was not directly applicable to the TUT Public Access, it could and was adapted to replace the original access controller software. The same open source software was actually developed further and integrated to an access controller product by the author's company, Arch Red. According to open source ideals, the modifications were published on the company WWW pages and the development of the product continued with the help of Heikki Vatianen and Sami Keski-Kasari, the other two founders of Arch Red.

The development of the packaged product was encouraged by the TUT IT management so that there would be continuity for the access control solution. So the support and cooperation agreements were formed between TUT and Arch Red to ensure the commercial support and development of the solution also in the future.

6.1.5 M13 — M16: Developing and Deploying Services

Promoting RADIUS-based roaming solutions and the compatible WLAN network architecture had already encouraged several other Finnish organisations to join to the FUNET WLAN Roaming. This and the work done in the TERENA Mobility Taskforce encouraged CSC to announce public WLAN roaming pilot [27] based on the RADIUS hierarchy. This official announcements led to negotiations and finally to an agreement [28] between CSC and Arch Red to start an official WLAN Roaming Root Service [28] with Arch Red as a technical service provider and CSC as the coordinator of the pilot.

At the same time TUT Public Access had proven to be stable and scalable mobile network architecture, and a decision was made by the IT management and Arch Red to announce the TUT Public Access as an official part of the TUT's production network. This announcement [29] encouraged also the departments still waiting to join to the growing area in addition to the new network deployments, which the IT management had already decided to be based on the TUT Public Access architecture. The announcement also marked the start of the official promotion and the fullscale deployment of the WLAN coverage to public areas. The effect of this promotion can be clearly seen in the statistics analysis in Section 6.2.

The final marker, which completed the work started in 2002, was the TUT's IT management's announcement of the campus-wide availability of guest accounts for TUT visitors. This feature was already piloted during the summer and autumn 2004, but it was the last of the defined use cases still pending.

6.2 Impact

The success of an product, service or even an architecture can be measured by the impact it makes and what is its popularity in the preferred user base. To give an impression, what was the impact of the TUT Public Access architecture once announced, author collected the monthly development of successful logins (Figure 6.1) and amount of unique users (Figure 6.2) in two graphs.

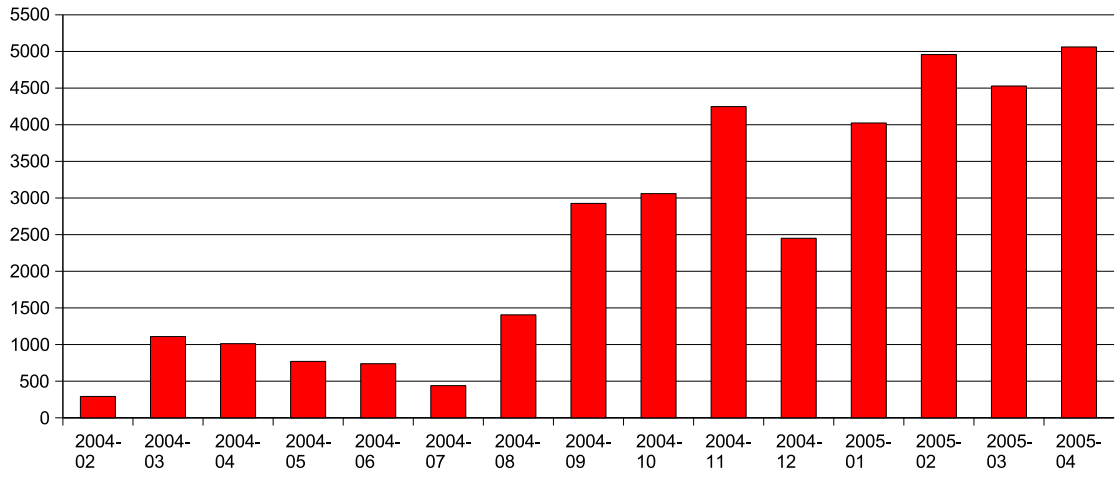

Figure 6.1: monthly successful logins

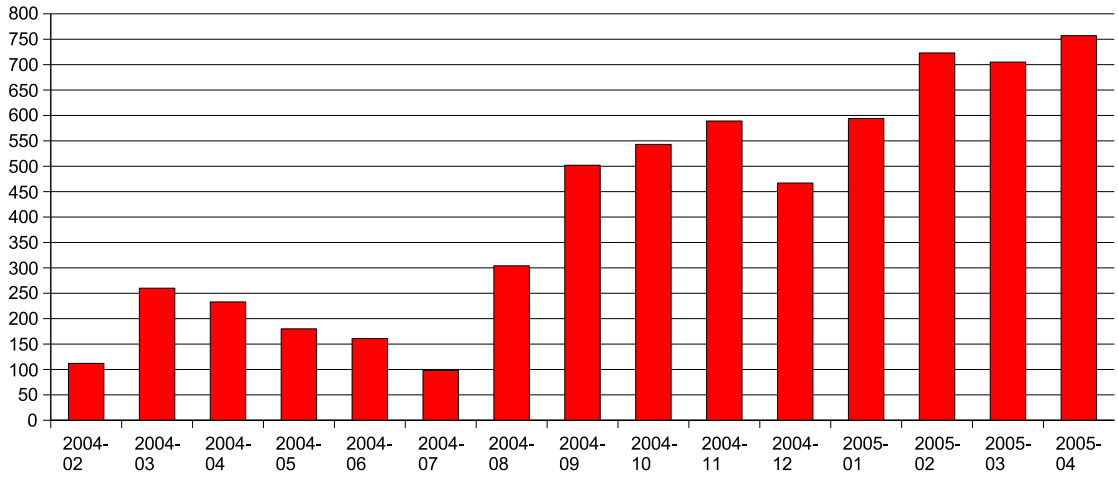

Figure 6.2: monthly unique users

As we can see, the amount of use and number of users has grown through out the period and still continues to grow as even more users and departments gradually adopt the wireless network as a part of their working environment. Also, the coverage of the TUT network has increased with at least 55 access points according to another WLAN network scanning walk the author decided to take in the end of May 2005. The results of this second walk were compared against the results of the 2003 walk in Table 6.2. The table compares only networks available both in 2003 and 2005 although there were a lot of other networks and access points detected especially at the Hermia area.

Table 6.2: Comparison of WLAN network scanning walks

Network (ESSID)	*2003-06*	*2005-05*
ACI	3	3
AIBONET/AIBONETAP	2	1
BIO	1	0
CS_WLAN	10	1
Digital Systems WLAN	8	6
ELE WLAN	6	5
freedom	2	0
Hermia	1	6
IT	1	0
KAU	2	1
MIT WLAN	2	0
MODEEMI/modeemiG	1	2
ttek/TTEK_WLAN	1	1
TUT/TUT-WPA	13	68
TUTVRC	1	0
WANO	6	52
WIWA	1	0

One interesting additional result of the network scanning walk was that although there were more networks on the Hermia area (177 APs in 38 networks), the TUT networks seemed to have already somewhat converged to the TUT Public Access architecture.

6.3 Future Development

Although the TUT Public Access has shown its scalability and interoperability during the pilots and in active use, the remaining challenge is how will the architecture support the evolution of the network also in the future.

The future will probably bring more and different kind of terminals. Especially the amount of smart phones and PDAs will probably increase, when new devices emerge. These new devices also change the use cases and possibly also the roles of the users and certainly how the network will be used. Instant messaging, internet telephone calls, video conferencing or location dependent services may be the driving factors for the TUT mobile network development in the future.

The vertical handover, seamless roaming, (Mobile-)IPv6, Skype, SIP, WPA/WPA2, zero and auto configuration may be the technical methods to realise the needed additional functionality.

6.3.1 Usability Development

The larger the number of users, terminals and especially the growing diversity of them, demands also that the access control system and architecture will be developed accordingly. Some of the work has already been done by adapting the WWW authentication page for mobile terminals, but a bigger challenge is how to develop the authentication system in the future so that new authentication methods can be added, but the gained usability level is not lost.

One of these kind of challenges is also the subject of the next section. Deploying WPA/WPA2 based authentication to the network may be easy, but on the terminal or user side, it requires education and information how it can be configured securely to different terminals. The WWW access controller may be used here as an instructional portal and of course as a backup system to balance the transition between authentication methods.

6.3.2 Deployment of WPA/WPA2 based authentication

The deployment of WPA/WPA2 is one of the most likely developments in the TUT Public Access architecture. Actually this development has already started as TUT IT management announced that the new WLAN capable ADSL modems for employees will use WPA for authentication. During the year 2005, the TUT IT management is also going to deploy the WPA/WPA2 also to the TUT Public Access network to ensure that the similarity of the user experience principle of the TUT Public Access can be followed.

The deployment of the WPA/WPA2 authentication also enables the easier use of terminals like Nokia Communicator 9500, because with this kind of authentication method, there is no need to authenticate via WWW page. The stronger terminal specific encryption also removes the privacy and some of the security concerns, even if the need of separate wireless network or VPNs does not completely go away.

Architecturally the change to network is not very big. The TUT Public Access access points will be just configured to have one WLAN network name more — this time just with WPA/WPA2 authentication enabled. The switches of course need one extra VLAN to be delivered to the access points but otherwise deploying this new access control method does not require anything else from the TUT Public Access Architecture. This makes adding the WPA/WPA2 a good example of architecture's capabilities for future extendability.

6.3.3 Eduroam WLAN Roaming

The Eduroam WLAN Roaming initiative was already mentioned earlier in this thesis, when WLAN roaming in general was discussed. The success of the Funet WLAN Roaming Pilot and Eduroam architecture propagation around Europe, Australia and even United States strongly suggests that this infrastructure will be the dominant WLAN roaming architecture design.

Eduroam supports authentication methods from WWW-authentication to WPA/WPA2 and even VPN-based authentication all based on the RADIUS

roaming hierarchy. The 802.1X/WPA/WPA2 authentication is the recommended one and as the policies concerning network names and settings develop, the Funet WLAN Roaming Pilot and TUT Public Access will probably be first adopters because of the flexible and modern architecture already deployed.

Through Eduroam, the users of the participating organisations will be able to roam securely everywhere in each participating organisations' networks without the fear of someone capturing or hijacking their identity. This mainly because WPA/WPA2 makes this possible. It provides EAP extensions, which secure the authentication information through the RADIUS roaming hierarchy by encapsulating the authentication request in a TLS secured tunnel between the terminal and home organisation's authentication server. Visited organisation's access control point may only get the name of the user's realm and an OK or not OK response to the authentication request.

Integrating Eduroam functionality in the TUT Public Access network does not require anything else than the work needed to add WPA/WPA2 authentication. In fact, both of these technologies can be easily combined utilising the same WLAN network infrastructure like in Figure 6.3.

6.3.4 TUT Research Access Network

The TUT Research Access Network is an idea in development to do the same to the departments' separate research networks that was done to the WLAN networks. The idea is to collect all existing research networks together under common organisation control to save funding and resources, and to be able to do cooperative and more extensive research in a more free environment, as well as to have more leverage in negotiations regarding the research network's internal funding or organisation.

A common research network, administered by research-oriented administration staff, would this way provide a kind of production grade secure playground for researchers of different departments. In this kind of environment, projects could be developed in a realistic environment, and the results tested for things like interoperability or applicability into different kind of network environments.

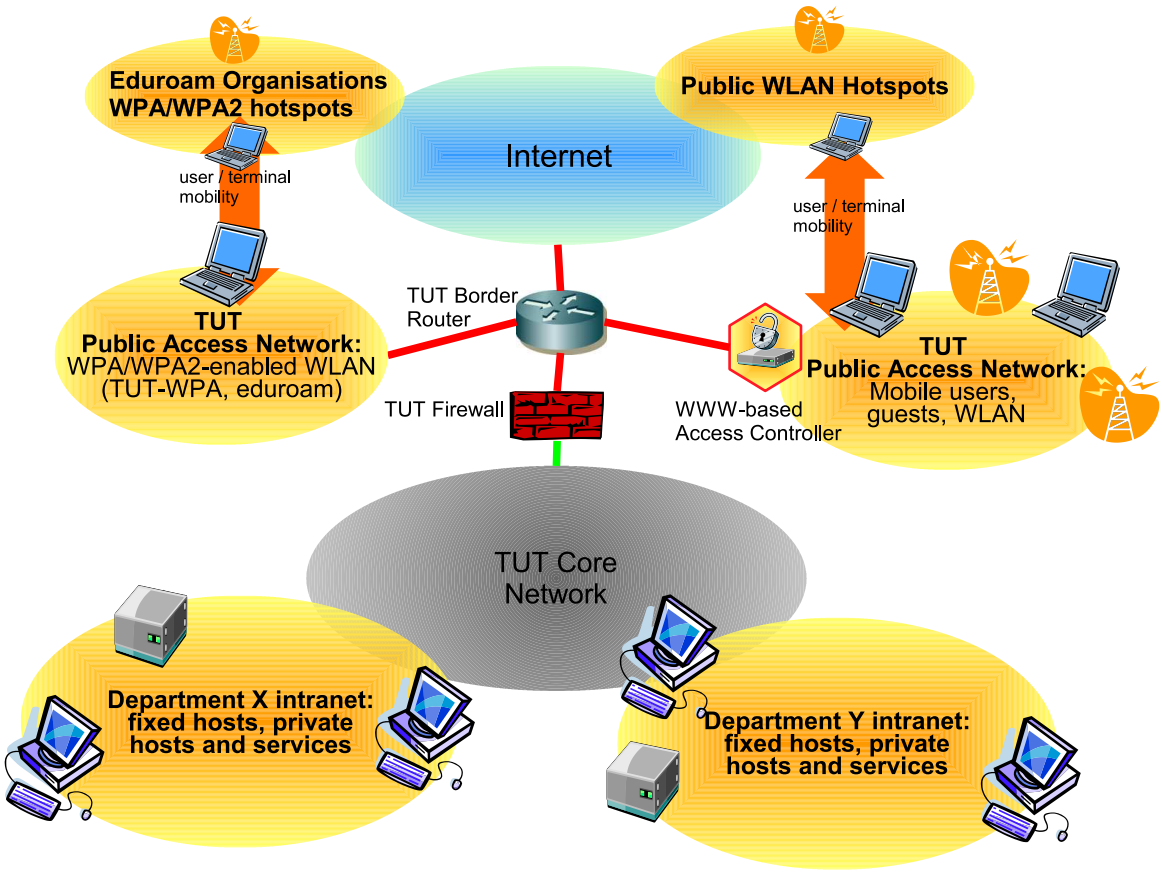

Figure 6.3: TUT Public Access network with Eduroam and WPA/WPA2

The TUT Public Access architecture could be partly integrated to this TUT Research Access Network by utilising the possibility to add one or more research oriented VLANs and WLAN networks. To ensure the functionality and decent service level of the production networks, these research VLANs could then be prioritised lower and controlled more carefully to avoid conflicts.

The cooperation of these two networks could result a large TUT campus-wide research network for wireless applications and services while the roaming functionality might extend this even further.

7 Conclusions

When the author started studying at the Tampere University of Technology, it was his clear intention to graduate as strictly technical software engineer and just develop good software. The first real position in the industry taught the importance and beauty of good design and architecture. The second position educated author about the importance interoperability, scalability, manageability and every day reality of the business world. The following positions confirmed the vision that none of these things matter, if nobody knows about the developed solutions, or if there is no will to make things happen.

The same lessons apply in designing and deploying the kind of network service architecture the TUT Public Access is an example of. Creating a successful architecture requires selecting well developed components and employing standard software engineering practices if new components are needed to be developed. The architecture design requires solid theoretical background and the ability to separate the working, efficient solutions from the solutions, which are not able to evolve or scale in the future. The theoretical knowledge, however, cannot cover the practical experience and the kind of knowledge, which is gathered from the imperfect world called reality. The practical knowledge, when utilised properly, brings the architecture closer to the applications and refines it to handle the imperfections so common in the real world. It also guides to select the technologies that work sufficiently well today instead of the technologies that might work better in the future.

This may be enough to make a technically solid architecture, but it is not enough to make this architecture a good and successful one. A good architecture is not worth anything, if nobody utilises or knows about it. If an architect wants to turn the designed architecture to reality, one must be able to present, promote and sell the architecture to its users and decision makers. Politics, people and sales skills are as important to the system architect as are the technical competencies. The journey to make an architecture a good and successful one does not end to the architectural specification. Instead, it is just a halfway stop on a road to get the architecture accepted and delivered to the ones that are to benefit from it.

TUT Public Access architecture was designed and deployed in the way described above. First the possible technologies and components were evaluated. Then the user and organisation requirements were gathered and the selection of feasible technology and architecture design solutions was refined. Through piloting, the architecture was tested in practice and adjusted to fit to the requirements of everyday production environment. Reaching even this point required sales and negotiation skills. Promoting the architecture and convincing the departments to migrate required still more work on this area, even if the network elements and support already were commercialised. The result of this design and deployment process was a sufficiently secure, scalable, usable and interoperable mobile network and services architecture, which already has proven its capabilities to expand and evolve without the need for additional large scale upgrades or installations.

References

[1] IEEE 802.11 Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. IEEE, 12 June 2003. 512p.

[2] Borisov N., Goldberg I., Wagner D., Intercepting Mobile Communications: The Insecurity of 802.11. Proceedings of the ACM SIGMOBILE, The 7th Annual International Conference on Mobile Computing and Networking, Rome, Italy, July 16-21, 2001, pp 1-9.

[3] IEEE 802.11i MAC Enhancements for Enhanced Security, IEEE, April 2004.

[4] IEEE 802.1X Port Based Network Access Control, IEEE, 14 June 2001, 142p.

[5] Ala-Laurila, J., Mikkonen, J., Rinnemaa, J.. Wireless LAN access network architecture for mobile operators. IEEE Communications Magazine, vol. 39, no. 11, November 2001. pp. 82-89.

[6] IETF Standard RFC3748 Extensible Authentication Protocol (EAP). IETF, June 2004. 67p.

[7] IETF Draft Extensible Authentication Protocol Method for GSM Subscriber Identity Modules (EAP-SIM). Haverinen, H., Salowey J., December 21 2004. http://www.ietf.org/internet-drafts/draft-haverinen-pppext-eap-sim-16.txt

[8] IR.61 WLAN Roaming Guidelines (also known as Inter-Operator Handbook). GSM Association, August 2004. 45p.

[9] Wirlab Network Research Center WWW Site. http://www.wirlab.net/

[10] Keski-Kasari S., Huhtanen K., Harju J., Applying Radius-based Public Access Roaming in the Finnish University Network (FUNET). Proceedings of the TERENA Networking Conference 2003, Zagreb, Croatia, May 19-22, 2003, pp 1-11.

[11] EduRoam WWW Site. Last modified: May 17, 2005. http://www.eduroam.org/

[12] Pravin Bhagwat and Bhaskaran Raman and Dheeraj Sanghi. Turning 802.11 inside-out. ACM SIGCOMM Computer Communications Review, Volume 34, Number 1 (January 2004). pp 33-38.

[13] Bellovin S. M., Security Problems in the TCP/IP Protocol Suite. Computer Communications Review, Volume 19, Number 2 (April 1989). pp 32-48

[14] Dsniff. Network auditing and penetration tool collection's WWW site. Last visited May 24, 2005. http://www.monkey.org/~dugsong/dsniff/

[15] EtherPEG. JPEG, GIF eavesdropping tool's WWW site. Last visited May 24, 2005. http://www.etherpeg.org/

[16] Driftnet. JPEG, GIF, MPEG audio eavesdropping tool's WWW site. Last visited May 24, 2005. http://www.ex-parrot.com/c̄hris/driftnet/

[17] Funet WLAN Roaming Pilot WWW Page. Last modified May 19, 2005 21:09:05. http://www.csc.fi/suomi/funet/roaming/index.html.en

[18] Simons, T., Snyder, J. 802.1X: Deployment Experiences and Obstacles to Widespread Adoption. October 2004 NANOG Meeting, Reston, Virginia, United States, October 17-19, 2004. http://www.nanog.org/mtg-0410/simons.html

[19] Mustikkamäki, M., Inter WISP WLAN roaming, A service concept by Wirlab. Wirlab Research Center, Seinäjoki, 26th September 2002. http://www.wirlab.net/wirlab_wlan_roaming.ppt

[20] Huhtanen, K., TUT Public Access Architecture. Funet Technical Days, Helsinki, Finland, 25th November 2002. http://www.csc.fi/suomi/funet/tekninenpaiva/2002/esitykset/

[21] Keski-Kasari, S., Huhtanen, K., Julkisten pääsyalueiden välinen verkkovierailu. Funet Technical Days, Helsinki, Finland, 25th November 2002. http://www.csc.fi/suomi/funet/tekninenpaiva/2002/esitykset/funet_pac-roaming.ppt

[22] Huhtanen, K., Tampereen teknillisen yliopiston julkinen pääsyverkko. 10th January 2003. http://www.atm.tut.fi/tut-public-access/documents/ttyn-julkinen-paasyverkko.pdf

[23] Keski-Kasari, S., Huhtanen, K., Applying Radius-based Public Access Roaming in the Finnish University Network (FUNET). Terena Networking Conference 2003, Zagreb, Croatia, 22th May 2003. http://www.terena.nl/conferences/tnc2003/programme/slides/s8d1.ppt

[24] Wierenga, K., Cross-organisational Roaming on Wireless LANs Based on the 802.1X Framework. Terena Networking Conference 2003, Zagreb, Croatia, 22th May 2003. http://www.terena.nl/conferences/tnc2003/programme/slides/s8d2.ppt

[25] Wireless Mobile Vaasa WWW site. Last modified 15th November 2003. http://www.wlan.puv.fi/

[26] Tino, access controller software WWW page. Last visited 24th May 2005. http://www.cc.puv.fi/ teu/tino/

[27] CSC: WLAN visiting pilot project starts in the Funet network. 21th January 2004. Press Release.

http://www.csc.fi/suomi/ajankohtaista/uutisarkisto.phtml.en?id=58

[28] CSC: Agreement reached on a root server for wireless network roaming. 25th May 2004 (english version). http://www.csc.fi/suomi/ajankohtaista/uutisarkisto.phtml.en?id=75

[29] Arch Red: TTY:lle yli 13 000 käyttäjän langaton verkko. Press Release (in Finnish). 3th June 2004. http://www.archred.com/pressreleases/tty-langaton-verkko-2004-06-03.txt