Security analysis of WLAN roaming solutions

Jacob Ferm
jacob.ferm@gmail.com

Lunds Tekniska Högskola

Advisor: Ben Smeets, ben.smeets@eit.lth.se
Johan Almbladh, johan.almbladh@anyfinetworks.com

August 19, 2013

Printed in Sweden
E-huset, Lund, 2013

Abstract

A ubiquitous Internet connection is becoming an important part of peoples professional and private lives. There exist several systems that aim to provide this by using WLAN infrastructures for roaming. To prevent misuse of such an infrastructure there is a need for access control and for protecting the users there is a need for confidentiality and integrity protection. Other topics of interest in such systems are key agreement, trust relations, privacy, and legal aspects.

This thesis develops an analysis framework for performing a security analysis of such systems. The analysis focuses on two scenarios. Firstly how the systems are used in the scenario where an Internet Service Provider deploys the system for its customers and, secondly, the scenario where a Mobile Network Operator uses the WLAN infrastructure for mobile offload.

The analysis framework is applied on five systems and compares them with each other. Systems that are based on tunnels to a trusted node are found to be superior in almost all security related aspects. They are also found to provide the most consistent level of security similar to what users receive from their home or mobile network. Systems not using tunnels are found to have different levels of security depending on which networks they utilize for Internet access.

Acknowledgements

I would like to thank my supervisor Ben Smeets for his support throughout the entire thesis. His knowledge in network- and telecommunications was an invaluable source of information and his guidance was a great aid in keeping the thesis on the right track.

I would also like to thank Johan Almbladh and Björn Smedman from Anyfi Networks who created the opportunity for this thesis. During the thesis they also provided valuable insights into WLAN roaming solutions.

Finally I would like to thank the employees of Anyfi Networks who provided a pleasant work environment for the past few months.

Glossary

3GPP - 3rd Generation Partnership Project
Organization defining standards for telecommunication systems such as 3G and 4G.

AAA - Authentication, Authorization and Accounting

AES - Advanced Encryption Standard
Encryption standard based on the Rijndael cipher.

AKA - Authentication and Key Agreement
Authentication protocol used with 3G and 4G networks.

ANQP - Access Network Query Protocol
Service discovery protocol used in Passpoint.

AP - Access Point

AuC - Authentication Centre
Authentication and authorization server on GSM networks.

CA - Certificate Authority
Entity managing a PKI and issuer of certificates.

CCMP - Counter Cipher Mode with Block Chaining Message Authentication Code Protocol
Encryption protocol used in WPA2.

CRL - Certificate Revocation List
List of certificates that are no longer valid.

DHCP - Dynamic Host Configuration Protocol
Configuration protocol for IP addresses on networks.

EAPOL - EAP over LAN
Handshake protocol used in wireless connections.

HSS - Home Subscriber Server
Authentication and authorization server on 3G and 4G networks.

IEEE - Institute of Electrical and Electronics Engineers
Organization defining standards for many industries including IT and telecommunications.

IPsec - Internet Protocol Security
Secure tunneling protocol for Internet traffic. Often run in the Authentication Header (AH) or Encapsulating Security Payload (ESP) modes.

ISP - Internet Service Provider
Company providing infrastructure to allow customers to reach the Internet.

LTE - Long-Term Evolution (4G)
Mobile network standard.

MAC address - Medium Access Control address
Address of a network interface used in IEEE 802 networks.

MCS - Mobility Control Server
Management service used in Anyfi.net.

MIC - Message Integrity Code
Short code calculated from a set of data to ensure the integrity of the data. Outside the WLAN context often referred to as a Message Authentication Code (MAC).

MNO - Mobile Network Operator
Company managing the infrastructure of a mobile network.

MS-CHAP - Microsoft Challenge-Handshake Authentication Protocol

DNS - Domain Name System
System for translating readable domain names into IP addresses.

PAP - Password Authentication Protocol
A simple authentication protocol without security features.

PEAP - Protected EAP
Secure encapsulation protocol for EAP. Based on TLS.

PKI - Public Key Infrastructure

PMK - Pairwise Master Key
Master key used in the EAPOL protocol.

PTK - Pairwise Transient Key
Session key generated by the EAPOL protocol.

RAKE - Roaming Authentication and Key Exchange
Authentication and key transfer protocol used in SWISH.

RC4
Stream cipher used in WEP.

RSNA - Robust Security Network Association
Authentication and key management protocol used in WLAN.

SIM - Subscriber Identity Module
Integrated circuit containing identity and key used in GSM and GRPS/EDGE networks.

SSID - Service Set Identifier
String containing the name of a wireless network.

SSL - Secure Socket Layer
Cryptographic tunneling protocol for Internet communications.

TKIP - Temporal Key Integrity Protocol
Encryption protocol used in WPA.

TLS - Transport Layer Security
Cryptographic tunneling protocol for Internet communications. Successor to SSL.

TTLS - Tunneled TLS
Protocol for performing server authentication and establishing a secure tunnel for user authentication. Based on TLS.

USIM - UMTS Subscriber Identity Module
Integrated circuit containing identity and key used in 3G and 4G networks.

WEP - Wired Equivalent Privacy
Encryption protocol for wireless networks.

WLAN - Wireless Local Area Network

WPA - Wireless Protected Access
Encryption protocol for wireless networks.

WPA2 - Wireless Protected Access 2
Encryption protocol for wireless works.

Table of Contents

List of Figures

List of Tables

Chapter 1
Introduction

A strong trend in today's society is that people are using the Internet more and more while being mobile. Laptops, tablets, and smartphones are all widely used mobile devices that are able to connect the user with the Internet. People are also becoming more reliant on services requiring Internet connectivity such as Cloud services, media streaming, social media etc. This change in people's life style has created a need for ubiquitous Internet connectivity.

Mobile networks solve this problem in part but not all devices are able to connect to such networks. Furthermore, the capacity of mobile networks is not always enough when data intensive services such as media streaming are used or too many users are connected to the same radio cell. This problem is expected to grow worse as traffic sent over mobile networks is increasing faster than the capacity of the networks [1].

One possible solution to this problem is to use existing WLAN infrastructures which are present in urban areas to provide high performance Internet connectivity. If such WLAN networks also can be used by mobile network roaming users, these WLAN networks can be a cheap way to provide a considerable capacity increase.

However, the deployment of WLAN networks for this purpose does not come without problems. Besides the financial and business considerations that come into play there are also issues concerning network security that must be addressed. In this thesis we will investigate some of these security issues while studying a number of systems whose purpose is to provide Internet access via WLAN to roaming users.

1.1 Setting the problem

Internet connectivity is something that has traditionally been supplied by trusted networks such as a home network or by a Mobile Network Operator. However, WLAN roaming systems give mobile devices access using unknown networks. Hence the mobile user cannot trust such network to handle the user data in the same way as in a home network.

In general, when a mobile device connects to unknown WLAN networks several security questions arise:

- How is authentication performed?
- How is authorization performed?
- How is the data protected?

These questions, along with several more, can be dealt with in different ways which results in different levels of security. The questions also contributes to the process by which users will decide if a network is trusted enough or not. The notion of a trusted network is however vague as trust combines not only technical security considerations but also judgements on the quality and honesty of the network and the ones that operate it. For example, users normally have to live with the potential risk that their Internet Service Provider is not following agreements or local regulations. Thus in most cases, although we speak of trusted networks such networks will be conditionally trusted in the sense that the network is trusted to perform a given task. Hence, the same network can at the same time be viewed as untrusted when being used for other tasks.

Thus the three previously listed questions are only a part of the much more complex question if a particular service or system can be trusted. Yet the technical analysis and answers to these three questions gives users good arguments when making judgements regarding the overall security of a service or system.

1.2 Goal of this thesis

The goal of this thesis was to analyse Anyfi.net and several similar systems that aim to provide WLAN roaming capabilities and evaluate their security. The systems were then compared to each other and the thesis explored how the differences have effect on the overall security of the systems. A secondary goal was to prepare the material for a paper on a study on the security of the systems.

1.3 Report outline

This thesis is structured in the following way:

Chapter 2 Gives an introduction to security elements relevant to WLAN roaming and authentication.

Chapter 3 Describes the way the analysis in the thesis was performed, presents the analysis framework and introduces the systems that were analysed.

Chapter 4 Presents the analysis of the WLAN roaming systems.

Chapter 5 Compares the results from the analysis.

Chapter 6 Presents the conclusions of the analysis and comparison.

Chapter 2
Background

This chapter provides a background to comprehend the contents of the thesis. We present a way to model networks and describe their different parts. Our choice of this model is driven by a security and functional perspective. Several elements in security that are vital for the reader to understand are explained briefly.

2.1 Network models

The most basic roaming scenario for an Internet connection can be seen in Figure 2.1. It consists of a mobile device, U, which is the roaming user that desires Internet connectivity and an access point (AP) which supplies the Internet access. In this thesis we often do not make a distinction between the user and the mobile device. The roaming user will often be referred to as a mobile user.

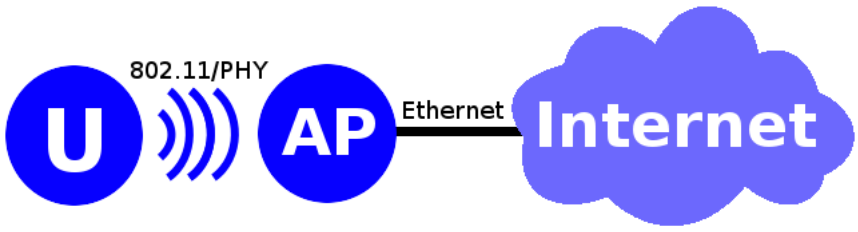

Figure 2.1: Basic system model containing a mobile user communicating using the WLAN standard with an access point which in turn is connected using Ethernet to the Internet.

In this setup the AP has several responsibilities. It supplies wireless radio access, it acts as the authenticator of the mobile device, it performs any encryption/decryption, and it supplies the mobile device with Internet access. A more detailed view of this model can be seen in Figure 2.2.

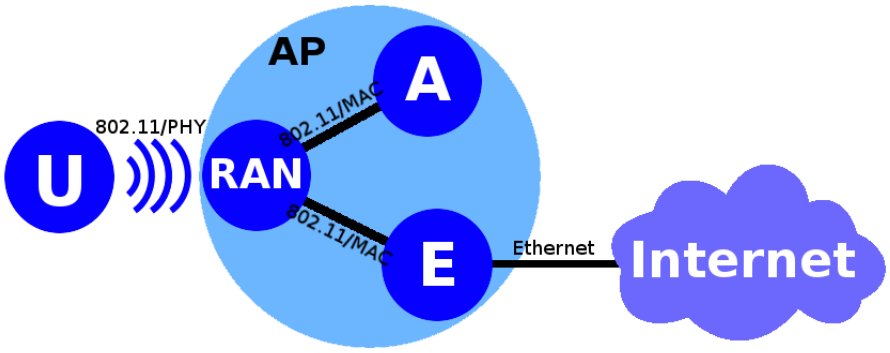

Figure 2.2: Detailed basic system model displaying the internal nodes of an access point.

The model in Figure 2.2 captures reality well when the authentication is performed locally such as with WPA or WPA2 but in many instances the authentication is performed in an external Authentication Authorization and Accounting (AAA) server which can be seen in Figure 2.3. The AAA server communicates with the authenticator in the access point using an AAA protocol such as RADIUS[2] or DIAMETER[3].

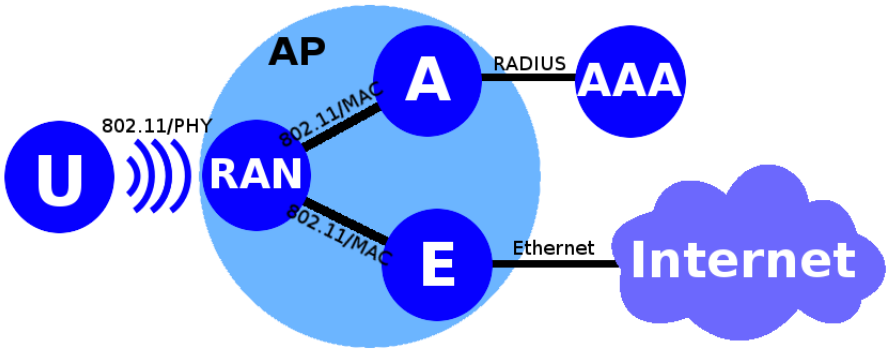

Figure 2.3: Basic model with external AAA server

This model can be enhanced even further with multiple AAA servers where some act as a proxy for the authentication requests and an external Authentication Centre (AuC), which supplies authentication information. This model is illustrated in Figure 2.4. As we will see later this model covers the setup where the authentication involves a Mobile Network Operator's (MNO) AuC (pre 3G mobile systems) or Home Subscriber Server (HSS) (for 3G and LTE (4G) systems).

When using these models it is appropriate to define several entities in the system:

- **U** - Mobile user/device roaming into other networks.

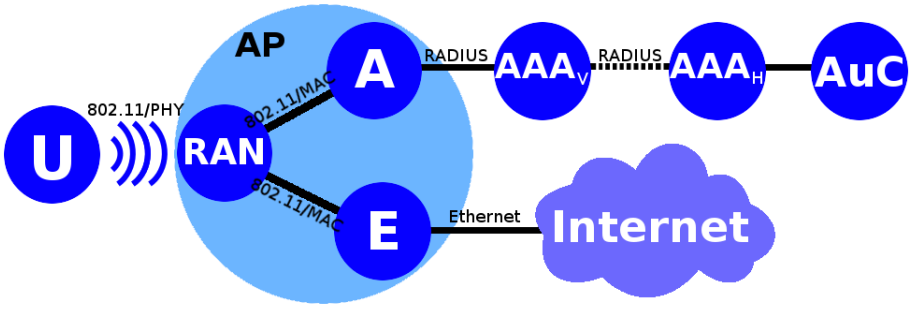

Figure 2.4: General system model with multiple AAA servers and an Authentication centre. A dotted line indicates a connection where an undefined amount of nodes may be placed.

- **RAN** - Radio Access Node in the visited network that translates the traffic between Media Access Control and Radio Frequency.
- **A** - Authenticator that either performs the authentication locally or uses external authentication infrastructure.
- **E** - Exit point for Internet destined traffic and designated termination point of encrypted traffic and location of translation between Medium Access Control and Ethernet.
- **AAA**$_V$ - AAA server on the visited network.
- **AAA**$_H$ - AAA server on the home network.
- **AuC** - Authentication centre on the home network which stores the credentials of the users and provides authentication data on request[1]

The location of these entities in the model does not need to strictly follow the designated positions in the general model. Different systems may place them somewhat differently in their architecture. Especially interesting are the systems that split the AP into different nodes which are then placed at different network locations. Such a division has, for example, effect on where encryption keys are available and used which in its turn effects the entire security model of the systems. Another interesting aspects that comes as a result of this division is when the exit node is not on the same network as the mobile device. This makes the origin network of the traffic different from where it enters the Internet which affects traceability and legal intercept properties of the system.

2.2 Cryptographic primitives

In this section we summarize give a brief overview of the security mechanisms that are relevant for our systems. For a general introduction in security we refer to *Computer Security* [4].

[1] In 3G/LTE system one uses the term HSS instead.

2.2.1 Wireless security

Wireless traffic uses the radio frequency spectrum which is a shared medium. This means that everyone that is able to receive the radio signals has access to the traffic being sent. There is no way to physically secure the traffic as is possible with wired transmissions maybe with the exemption of meteor scatter communication. This observation creates the need for protection of data sent over the wireless link. Typically encryption is used to confidentiality protect the traffic and Message Integrity Code (MIC)[2]or signature schemes are used for data integrity protection.

Another problem that arises is the need for access control to prevent unauthorized access or utilization of resources. Wired transmissions require a device to be physically connected to the router or modem which often provides enough protection. But with wireless transmissions anyone in the physical proximity is able to interact with the access point.

There are three different substandards defined in the 802.11 WLAN specification that all aim to solve these two issues. They are WEP, WPA, and WPA2 where WEP is the oldest one and WPA2 is the newest one [5].

Wired Equivalent Privacy (WEP)

Authentication in WEP is optional and uses the protocol called Shared key authentication which is based on a challenge-response exchange. The access point generates a challenge which it sends to the mobile device. The mobile device encrypts the challenge using WEP encryption.

The encryption in WEP uses an initialization vector combined with the secret key as seed into the RC4 stream cipher which produces a key stream that is XOR'ed with the plain text to produce the cipher text.

WEP is today deprecated as severe faults were discovered in it is construction and recovering the secret key was found to be a trivial process. As no new standards were ready when these faults were detected, WPA was rushed into completion as a quick fix.

Wi-Fi Protected Access (WPA)

WPA was designed to replace WEP without requiring hardware upgrades. This allowed for easy deployment to quickly combat the security flaws of WEP.

WPA uses an authentication protocol RSNA which uses EAPOL (EAP over LAN) from the 802.1X standard, a challenge-response exchange that results in a session key [6]. This session key is then used to perform encryption.

WPA uses the cipher mechanism called TKIP for securing the data. It is based on the same encryption that is used in WEP but adds a new function for generating and updating the keys and initialization vectors used.

[2]The WLAN specifications use MIC instead of the acronym for Message Authentication Code to avoid confusion with the already reserved term MAC in data communication.

Wi-Fi Protected Access 2 (WPA2)

WPA2 uses the same authentication protocol as WPA to achieve authentication and to generate the session keys.

WPA2 differs from WPA by replacing TKIP with a new cipher suite called CCMP. CCMP is based on the AES encryption algorithm, a US FIPS approved symmetric-key encryption algorithm which is stronger than RC4 (sometimes also referred to as ARCFOUR).

Older hardware that was designed for WEP is unable to implement WPA2 due to the new algorithms used.

2.2.2 Asymmetric Encryption

Asymmetric (or public-key) encryption schemes use public and private keys. That means that different keys are used for encryption and decryption. Data encrypted with the public key can only be decrypted with the private key. Most such schemes work the other way as well, data encrypted with the private key can be decrypted with the public key. The latter is utilized to create public-key based digital signature schemes where the public key can be used by outsiders to verify the signature that is created by using the private key. We refer the reader to any standard book on modern cryptography such as *Computer Security* [4, p. 264] for more details.

2.2.3 Public Key Infrastructure

In public-key cryptographic schemes the public key usually has to be associated with a specific entity or user. The most common way to achieve this is to setup an infrastructure in which these public keys are approved (as valid), say by a third party. A common tree like infrastructure to implement this is refereed to as a Public Key Infrastructure (PKI) and the third party that approves the public keys is called a Certificate Authority (CA). As an evidence of the CA's approval the CA issues so-called certificates which are signed data blobs that contain information on the public key and a signature by the CA. As a result PKIs are (key) infrastructures that facilitates several useful functions related to security. Using the keys in a PKI it is easy to implement procedures that can be used to authenticate parities without previous knowledge of each other, the keys in a PKI can facilitate secure communication and they can be used to create digital signatures, [4, p. 288].

Certificates

As explained in the previous section a PKI is designed as a tree structured hierarchy of certificates The authenticity of each certificate is guaranteed by its parent certificate. The only exception is the root certificate which guarantees its own authenticity. The root certificate is generally created by the CA which also manages the infrastructure by adding and removing certificates. The CA is also responsible for maintaining a Certificate Revocation List (CRL) which contains certificates

that are no longer valid. Alternatively the CA operates a service through which it is possible to verify that a given certificate is still in use and not has been revoked.

Besides the public key and the signature of the issuer a certificates also contains information about its owner and the intended use of the certificate. It can contain information such as names, addresses, emails etc. Connected to the certificate but not included in the certificate is the private key known only by the owner. Thus, a certificate does not contain any secret information and can be sent via untrusted channels. The receiver, assuming he/she has possession of the CA root certificate, can verify the authenticity of the received certificate using CA root certificate (plus possible a chain of parent certificates).

2.2.4 Authentication

In general, there are two entities involved in authentication. The WLAN standard uses the terms supplicant and authenticator. A supplicant is the entity that desires access to some resource and the authenticator is the one that grants or denies access. To authenticate means for an authenticator to verify that the identity claimed by the supplicant is correct. This is in general accomplished by proving the possession of a secret key. The key itself can be in the form of a network passphrase, a user password, or a (U)SIM card amongst others.

Simple authentication protocol

The simplest form of an authentication protocol would be for the supplicant to simply send the authentication credentials to the node wishing to verify the identity. However, this is generally a bad protocol unless the medium over which the credentials are transferred are secured through other means as the secret key becomes known to entities with access to the transfer medium.

Another problem with this type of protocol is that the authenticator must generally be known before a peer chooses to transfer its secret key which means that authentication of the authenticator must be performed prior to this. This is often accomplished through the use of certificates.

Challenge-response protocol

A more secure way of performing authentication is to have the authenticator generate a random number called a challenge which is sent to the supplicant. The supplicant creates a response to this challenge by performing a cryptographic function that uses both the challenge and the secret key as input. The specific cryptographic algorithm is often either a simple keyed hash or MIC function. If the result calculated by the authenticator is the same as the response received by the supplicant then the possession of the secret key can be verified without sending the actual credentials. This reduces the security requirements for the medium used to communicate.

A vulnerability in challenge-response protocols is that recording a single exchange allows an attacker to perform offline attacks to recover the secret key used to calculate the response. While protocols generally use a key size large enough to

make them resistant to brute-force attacks, they cannot protect against dictionary attacks when the secret key is chosen improperly by a security unaware user.

Authentication using certificates

As mentioned, the certificates can be used for authentication by proving the possession of the private key. This can be accomplished by encrypting a challenge with the private key. Since the certificate contains the public key, the authenticator can decrypt the challenge with the public key and verify that the response must have been created by one that possesses the private key.

Mutual authentication

A desired property in communication is that both entities involved are authenticated. This property is referred to as mutual authentication and is often required to establish the trust relations that user plane data security rely on.

For residential WLAN networks the authentication protocol RSNA is enough to achieve mutual authentication as the secret key is a group key shared by all member of the network. The protocol establishes that both the mobile user and the network possesses the passphrase which is sufficient to establish trust in each other.

For more advanced networks the authentication of the mobile user and the network itself is performed separately as each user possesses different keys. In general, the network authenticates to the mobile user using a certificate which may result in establishing a secure channel through which user authentication is performed. The mobile user authenticates using either a simple authentication protocol or a challenge-response protocol.

2.2.5 Extensible Authentication Protocol (EAP)

Described in the 802.1X standard is the framework EAP which contains a number of sub-protocols that facilitates mutual authentication using different credentials. Successful execution of the protocol also results in keying material that is intended to be used for deriving session keys which protects the following user plane data communication. This authentication protocol is often referred to as WPA-Enterprise and is standard among enterprise level networks, [7].

Some examples of common EAP protocols are:

- **EAP-TLS** - Both supplicant and authenticator use a certificate to authenticate, [8].
- **EAP-TTLS** - Authenticator uses a certificate to authenticate and establishes a secure tunnel for supplicant authentication, [9].
- **EAP-SIM** - Both supplicant and authenticator use a SIM-card to authenticate, [10].

- **EAP-AKA** - Both supplicant and authenticator use a USIM-card to authenticate, [11].

The ability to choose which credentials to use by picking a compatible protocol gives networks high flexibility and makes the protocol very compatible with any existing access control mechanisms. It is not even required that all users in a network use the same credentials, some may for example authenticate with a password while others use a certificate.

The protocols EAP-SIM and EAP-AKA are especially interesting as they function with authentication credentials normally used on mobile networks. This is an important aspect in mobile offload as cellular devices already possess the required credentials without needing further configuration and key distribution. It also means that the MNO are able to use the same authentication infrastructure as on the mobile network.

A simplified version of an EAP exchange can be seen in Figure 2.5. Note that during the execution of the sub-protocol external resources such as a AuC or a HSS may be used.

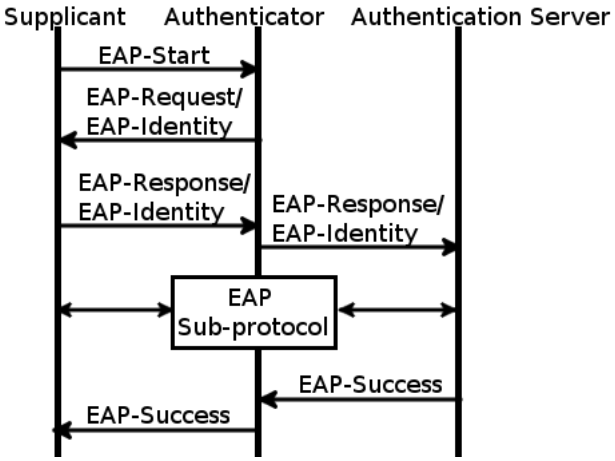

Figure 2.5: Simplified EAP exchange

2.2.6 Long term keys and session keys

A concern in many cryptographic protocols is that the more a key is used, the more likely it is to be compromised. To prevent this problem either large keys (keys with high entropy) that have a long life-time could be used or the keys could be changed on a regular basis. Neither of these solutions are without problems, large keys require more computational power to perform encryption and changing keys often puts more strain on the key distribution infrastructure.

A common solution to this is to use a long term key, which is in general large and use it to generate new, possibly smaller keys for each session. The long term key is thus less exposed and may be used with a longer life-time and the session

keys are only used for a short period of time and in some cases can be smaller. The latter can give performance benefit in the cryptographic computations. All this also introduces the functionality that a node can be given the responsibility of performing encryption/decryption without requiring access to the long term key.

2.2.7 Digital Signatures

Digital signatures are used for a similar purpose as paper signatures, to prove the genuineness of a digital document. As explained above public-key cryptosystems are used to create digital signature schemes. A particular useful property that digital signatures schemes provide is that of non-repudiation. Non-repudiation means that once data has been signed the signer cannot deny the signing of it.

In most digital signature schemes the signature contains an encrypted hash value of the data to be signed. By the cryptographic properties of hash functions one has a very high degree of certainty that outsiders with no access to the private key cannot modify the data and keep the signature value the same.

2.2.8 Data tunneling

By data tunneling we refer to a way of transferring data between two points such that (most) properties of the data are not visible or just relevant to the entities that are involved in the transportation. A common approach to realize such tunneling is to employ data encapsulation.

When a tunnel is established between two points the data will automatically be encapsulated at the sender and decapsulated at the receiver. In our setting data tunnels use encryption and data integrity mechanisms to protect the tunneled data against an active wire-tapper. Well-known tunneling solutions are IPSec and TLS. Encapsulation, encryption, addressing and such functions are typically performed at layers below the application and may be transparent to the application. To the application it will appear as if data enters and passes through a tunnel.

Data tunneling can thus be characterized in this thesis as an automatic end-to-end encryption and data transfer procedure.

2.3 Security concepts

2.3.1 Trust relations

As we already explained initially trust is a concept that is very difficult to define in a precise manner. Yet we need to do some reasoning related to trust and cannot only perform our analysis on technical observations and facts. To make the notion of trust a bit more tangible we have chosen to define trust as the expectation that an entity will perform some action or protect some asset the way one wants.

For example, allowing an entity access to ones private data builds on the use of trust that the entity will not misuse that privilege.

Trust can be established in several ways. An entity may be trusted a priori as with an MNO. A mobile user that becomes a subscriber of a mobile network automatically puts trusts in the MNO. Trust can also be established through a protocol. If a protocol makes it impossible for an entity to misbehave (undetected) then the network operated by this entity can be trusted. Another way to establish trust is through legal agreements and business relations. Two MNOs may chose to trust each other if the legal and business agreements are such that any breach of the agreements is is economically disadvantageous.

2.3.2 Anonymity

Anonymity is a concept that is often desired in communication. In general it means that the identities of the communicating peers are unknown to anyone outside the conversation. A way to measure how strong anonymity a user has is to calculate the anonymity set. An anonymity set is defined as the set which the identity of the user is contained in. An example of such a set is all the subscribers of a carrier which is a very large anonymity set that makes it difficult to identify a user in. An example of a small anonymity set is a residential network containing only a few users. Finding the identity of a user when there is only a few possible alternatives is rather easy.

Another concept closely linked to anonymity is unlinkability. It refers to the property that mobile users cannot be tracked between different sessions. For each session it is impossible to determine if that mobile device have visited the network before.

Both of these concepts can be broken in multiple ways by eavesdropping on the communication. An authentication exchange often include identities being transferred which will break both anonymity and unlinkability unless pseudonyms are used. It is also possible to identify a user by analysing the contents of the communication as it contains cookies, emails, visited web pages etc.

2.3.3 Rogue Access Points

A rogue access point refer to a wireless access point that is operated by someone with malicious intent. Such APs often impersonate valid APs to trick unsuspecting users or devices into connecting. By connecting to a rogue AP a user's security is compromised in several ways and we will give a short description of a few.

If the AP requires authentication it may allow the rogue AP to acquire the user's credentials. This affects APs that rely on simple authentication protocols or web based authentication.

Another point is that the rogue AP gains access to the traffic and can intercept all data that is not secured through other means. This data can contain sensitive information such as session cookies, emails, passwords, etc.

Finally the rogue AP can redirect the user's traffic and trick the user into visiting other web sites than what was intended. This may result in the user disclosing sensitive information or authentication credentials of other services.

A dangerous property of all these attacks is that they may not affect the service expected by the user and can thus be performed without the user noticing it.

Chapter 3
Approaches to analysis

This chapter presents how we setup our analysis in this thesis and explains how they were performed. As standardized frameworks for security analysis such as Common Criteria rely on the existence of protection profiles which do not exist for our setup and since the use of Common Criteria requires much experience a simpler more adequate analysis framework was developed instead [12]. Some inspiration was found in the approach used by Gustafsson and Thor in their analysis of Fon [13].

3.1 Methodology

This section describes how the thesis work was structured.

3.1.1 Literature study

As the goal of the thesis was to perform a comparison between Anyfi.net and similar systems the first part of the study was dedicated to researching different systems. The first iteration of this step focused on finding systems that were somewhat similar to Anyfi.net, either in design or in usage. After this some time was spent on deciding which of these systems to include in the analysis. This decision was made by identifying the two main use case scenarios Anyfi.net could be used in and then choosing systems that could be used in at least one of those scenarios.

Each of these systems were then studied closely, a step that continued in parallel with the development of the framework and the analysis.

To improve the understanding of the authentication in the systems, some time was also spent studying the authentication protocols used in the systems.

3.1.2 Analysis Framework

Before the analysis could be performed, a framework describing how the analysis was to be performed was needed. This framework was required to provide a structured way of analysing the systems so that the result could be used as the basis for a comparison.

The framework was developed iteratively in parallel with the analysis so that faults could be identified and fixed before too much time was invested in them.

3.1.3 Analysis

The analysis was performed for each system according to the framework. As with the framework, it was performed iteratively. Results found during the analysis required changes to be made in the framework which then affected the analysis of all systems.

Towards the end of the analysis it became apparent that the framework did not focus enough on the authentication in the systems. An extra study, focusing mainly on the authentication and data security, was thus performed.

3.1.4 Comparison

As comparing systems that are used in different scenarios would not give fair results the system were divided into two groups, one for each use case. The systems were then only compared with other systems in the same group.

The comparison explored most of the points examined in the analysis but focused especially on the authentication and data security as they were deemed the most important.

3.2 Analysis framework and use cases

This section presents a short description of the framework that was developed and the sections it contains. The full framework is available in Appendix A.

3.2.1 Introduction

As explained before, the framework was introduced to provide a structured way of analysing systems which serve to share or distribute WLAN access. Such systems solve this access problem in many different ways which makes it difficult to analyse them in a similar way. The framework tries to overcome this by focusing on a few aspects of the access provisioning which are very central in most systems.

3.2.2 Use cases

An important part of the framework was defining the different use cases. The use cases were developed according to what scenarios the systems were likely to be used in. This depended on both what requirements a potential end-user of the system would have as well as which scenarios were feasible for a company to deploy.

Two use cases were defined, one describing an Internet Service Provider (ISP) that enables its customers to share WLAN access with each other and one describing MNOs performing mobile offload using WLAN.

These use cases were then used to identify which parts of the system that were relevant to the analysis and which parts could be ignored. The use cases also were an important part of the comparison.

Use case A - ISP distributes Internet access

An ISP gives its customers Internet access by allowing users to connect to any modem or router managed by that ISP, regardless of which customer has physical control of the device. Customers that subscribe to this service either have the firmware on their modem or have their router updated or receive new hardware as part of the service. When the customers encounter the network of another customer with this service they are able to connect to that network. After they have been authenticated they are given Internet access.

The use case can be characterized now as follows:

1. ISP manages modems in participating networks
2. Mobile device associates with visited network
3. Mobile device is authenticated
4. Mobile device is given Internet access

Use case B - Mobile offload using WLAN

Through an agreement between a WLAN network operator and an MNO, subscribers of that carrier are given access to the WLAN network. When the mobile device of a subscriber comes within range of the visited network the device will automatically connect to it. After the mobile device is authenticated by the carrier it is given Internet access.

The use case can be characterized now as follows:

1. The MNO creates a roaming agreement with a WLAN network operator
2. The mobile device associates with visited network
3. The mobile device is authenticated by the MNO
4. The mobile device is given Internet access
5. The visited network operator charges MNO for the service

3.2.3 Framework structure

Our framework was organized into a number of steps. To begin with, the entities in the system were specified and their important assets were identified.

The next part specified how to analyse the design of the system by defining which trust relationships were present in the system, what they protected and identifying possible vulnerabilities.

The following parts specified how to analyse different areas in the system. The areas analysed were:

- Authentication
- Data security
- Anonymity
- Availability
- Legal aspects

Each of these items consisted of defining the area under analysis, specifying which threats were relevant in this area, how these threats were dealt with and which threats were not dealt with sufficiently.

Security and Trust

In the systems that we will analyse there are often trust relations in place by which involved entities can sidestep procedures or protocols that otherwise should guarantee that the counterpart entity indeed is operating as agreed/designed, or that express assumptions that cannot even be verified through a reasonable protocol. Since trust relations can be associated with different aspects of a security function or with the handling of different kind of sensitive assets it is often so that it is hard or sheer impossible to compare trust relations. Also we lack the details from an actual realization that would allow us to perform a meaningful risk assessment of the trust relations. As a consequence of these considerations we will be brief when addressing trust aspects.

3.3 Selection of systems

The literature study identified several systems that were of possible interest for the analysis. The following systems/protocols were considered for the analysis. The ones in bold were eventually selected for the analysis:

- **Anyfi.net** - A commercial system developed by Anyfi Networks that provides wireless roaming over unknown networks, [14].
- Control And Provisioning of Wireless Access Points (CAPWAP) - A specification for a protocol that allows a network to be distributed across multiple access points, [15].
- Citywide Ubiquitous Wi-Fi Access - An academic system designed for wireless roaming, [16].
- **Eduroam** - A cooperative system among educational institutions that facilitates roaming between institutions, [17].

- **Fon** - A commercial system developed by Fon Ltd. that supports sharing of Internet connectivity, [18].
- Mobile IP - A protocol that facilitates seamless roaming over known networks, [19].
- **Passpoint** - A specification by Wi-Fi Alliance for a system designed for commercial hotspots, [20].
- PISA - An academic system designed for wireless roaming over unknown networks, [21].
- **Secure Wi-Fi Sharing (SWISH)** - A academic system designed for wireless roaming over unknown networks, [22].
- Wifi.com - A commercial system designed to allow users to share security keys with each other, [23].

Anyfi.net was obviously selected for analysis as one of the defined goals of this thesis was to analyse it and compare it to similar systems.

While the CAPWAP protocol supports roaming it is designed for distributing a single network across multiple APs rather than facilitating roaming across many different networks. This is somewhat different from what is specified in the use cases which is why we chose not to analyse it.

Fon was chosen for the analysis since it can be used to realize Use case A. It is also of interest because of its large presence on the commercial market.

Mobile IP was never seriously considered for the analysis as it did not support either of the use cases but was interesting due to it being one of the first systems to tackle wireless roaming.

Eduroam was selected for the analysis despite not supporting either use case very well. Its role in facilitating roaming using WLAN networks across the entire world and a clearly defined design is why we chose to include the system anyway.

Passpoint was chosen for the analysis primarily due to its commercial position. Several large companies are pushing for Passpoint to become a commercial standard for hotspots in the same way Wi-Fi is a commercial standard for WLAN which makes an analysis of this system very interesting.

Both SWISH and PISA are based on the ideas developed by Sastry et al., author of the Citywide Ubiquitous Wi-Fi system, making them more advanced solutions with similar design. As analysing three similar systems would be unnecessary we chose to focus only the system that was deemed most mature, SWISH.

Wifi.com was not selected for the analysis due to that we found only very little information about the system. Hence analysing the system would be difficult. The little information that was available also indicated that the system would fulfil very few security requirements a user might have, making a deep analysis redundant.

3.3.1 Anyfi.net

Introduction

Anyfi.net is a system developed by the company Anyfi Networks. It is a system intended to link together the existing WLAN infrastructure with a user's home network or carrier network.

Anyfi.net is implemented through software modules that are run on both home networks and visited networks. No client-side software is required in the mobile devices.

Design

The concept of the system is to distribute the mobile user's home WLAN network through other access points in the system. These access points act as a radio access node which tunnels the data to the home network where it is processed. As the system does not prescribe how the data is processed it allows for high flexibility for different types of authentication and data security.

Anyfi.net also includes a Mobility Control Server that translates device addresses in to network addresses, authorizes connection attempts and performs accounting. Its main function of translating addresses can be seen as similar to a DNS.

3.3.2 SWISH

Introduction

SWISH, Secure Wi-Fi Sharing, is an academic system described in 2011 by Leroy et al. from universities in Belgium and Germany. It is based on the tunneling protocol designed by Manilus et al. [24]. It introduces new protocols for performing authentication and accounting which rely on a PKI.

SWISH is implemented through software modules that are run both networks and mobile devices in the system.

SWISH has been deployed in an experimental setup at two universities in Belgium.

Design

The concept of the system is to extend the home network of a mobile user to each access point in the system. These access points act as a radio access node which tunnels the data to the home network where it is processed.

The visited and home network perform an accounting protocol with each other that uses digital signatures to ensure validity.

3.3.3 Fon

Introduction

Fon is a commercial system by the company Fon Ltd. deployed in 2005. Its aim is to link together existing WLAN infrastructures by having the users of the system share Internet access with each other. As of June 2013, Fon claims to have over 8 million access points connected to the system.

Fon is implemented through software modules that are run on the visited network. No client-side software is required in the mobile devices.

Design

The concept of the system is that every user in the system agrees to share their Internet connection with others. In return they are able to use the connections of other users. An access point in the system is divided into two parts, one for private use by the network owner and one public for use by the Fon members.

Membership of the service is verified by Fon itself or by one of its partnered ISPs. When the user is authenticated traffic is passed directly to the Internet by the visited network.

3.3.4 Eduroam

Introduction

Eduroam is a cooperative system between universities and research facilities located around the world. Its aim is to allow students and staff receive Internet connectivity when visiting other institutions.

Eduroam is implemented through software modules run on both the visited network and the home network. No client-side software is required in the mobile devices.

Design

Eduroam is structured as a hierarchy of AAA servers. Each educational institution has its own AAA server able to authenticate the members of that institution. Networks are grouped into federations, one for each country, that enable communication in between the different networks. All the different federations belong to a confederation which handles communication between federations.

When a user connects to an Eduroam network the authentication is routed through multiple AAA servers to the user's home institution. When the user is authenticated traffic is passed directly to the Internet by the visited network.

3.3.5 Passpoint

Introduction

Passpoint is a specification developed by the Wi-Fi Alliance. Its aim is to improve roaming between different networks by providing advanced network selection. It uses a new protocol introduced in the 802.11u standard that enables mobile devices to discover the capabilities of the visited network before a connection attempt is made.

Passpoint is implemented through software modules that are run on both networks and mobile devices in the system. The client-side software required may become standard in future mobile devices.

Design

The concept of the system is to create an easy way for mobile users to get Internet connectivity at various networks without requiring users to keep track of multiple accounts used to authenticate. Instead the system is intended to automatically discover if the visited network accepts any of the accounts known by the user.

When a user connects to a Passpoint network the authentication is routed through multiple AAA servers to the user's home network. When the user is authenticated traffic is passed directly to the Internet by the visited network.

Chapter 4
Analysis

In this chapter we present an analysis for each of the systems using the approach put forward by our framework.

Each analysis starts by defining the Use cases for the system and describing how they differ from the use case presented in the framework. Next it presents the entities present in the system and which assets are of importance to those entities. The different trust relationships between these entities are defined and examined.

The analysis presents and examines the authentication in the system and how data is protected. It also examines achieved properties and any vulnerabilities in regards to anonymity and availability of the system.

Finally we give a brief account on certain legal aspects from a management and law enforcement perspective.

4.1 Anyfi.net

Anyfi.net supports both Use case A and B as described in the framework.

Use case A

When realizing Use case A with Anyfi.net we include two additional entities. First is the home network of the mobile device. Second is the Mobility Control Server that is typically managed by the ISP or by Anyfi Networks.

Anyfi.net requires that entities in the system register with the MCS before connections can be established.

The use case now has the following steps:

1. ISP manages the firmware/configurations in the modems in the home and visited networks.
2. Home and visited networks register with the MCS.
3. The home network registers the mobile device with the MCS.
4. The mobile device sends a probe request when in range of the visited network.

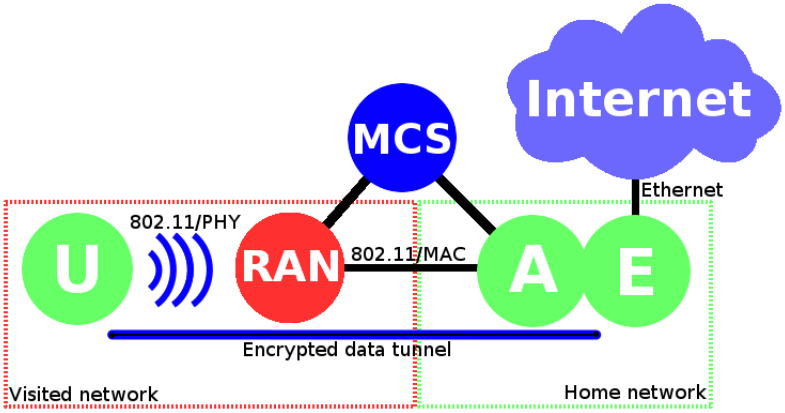

Figure 4.1: Anyfi.net Use case A design

5. The visited network performs an IP lookup with the MCS.
6. The MCS introduces the visited and home networks with each other.
7. The visited networks begins tunneling all traffic from the mobile device to the home network.
8. The home network and the mobile device authenticate each other.
9. The mobile device is given Internet access by the home network.

Use case B

When realizing Use case B with Anyfi.net we include an additional entity. Like before in Use case A we need the MCS that is typically managed by the MNO in the system and/or by Anyfi Networks.

Anyfi.net requires that entities in the system register with the MCS before connections can be established.

The use case is now as follows:

1. The MNO and the visited network register with the MCS.
2. The MNO and the visited network operator establish a roaming agreement.
3. The MNO registers the mobile device with the MCS.
4. The mobile device sends a probe request when in range of the visited network.
5. The visited network performs an IP lookup with the MCS.
6. The MCS introduces the visited network and the carrier network with each other.
7. The visited network begins tunneling all traffic from the visited network to the carrier network.

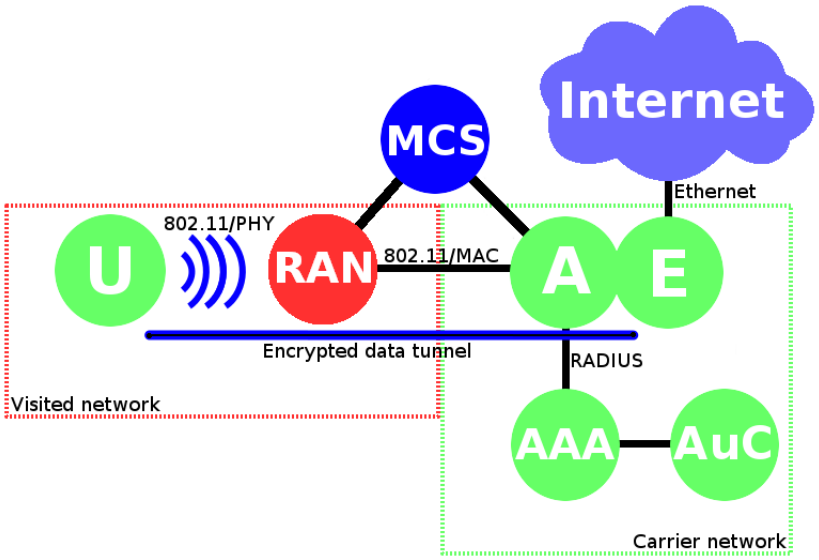

Figure 4.2: Anyfi.net Use case B design

8. The MNO and the mobile device authenticate each other.
9. The mobile device is given Internet access by the MNO.
10. Both the visited network and the MNO report accounting information to the MCS.
11. The MCS may assist in any charging operations between the visited network operator and the MNO.

Note that the last steps are only needed if the roaming agreement includes requirements for performing charging.

4.1.1 Entities

Which entities are involved in the system depends slightly on which Use case the system is configured for.

For Use case A, the following entities are involved:

- **Mobile device** belonging to a user in the system. This device is using the service to roam across networks in the system.
- **Home network** of the mobile device. This network contains a router or a modem running Anyfi.net software.
- **Visited network** that the mobile device is connecting to. This network contains a router or modem running Anyfi.net software.
- **ISP** that manages the networks in the system.

- **MCS** that performs authorization and routes connections in the system. This entity may be run by the ISP.

For Use case B, the following entities are involved:

- **Mobile device** belonging to a user in the system. This device is using the service to roam across networks in the system.
- **Carrier network** which the mobile user is a subscriber of. This networks contains a tunnel termination gateway running Anyfi.net software.
- **Visited network** that the mobile device is connecting to. This network contains a router or modem running Anyfi.net software.
- **MCS** that performs authorization and routes connections in the system. This entity also manages payments between networks in the system. This service is typically controlled by the MNO and/or Anyfi Networks.

4.1.2 Assets

The following assets are important to (at least) some entity in the system:

- **Authentication credentials** - The credentials used by the mobile device and home network to authenticate each other. This can be passwords, certificate private keys, SIM cards or other credentials.
- **User plane data** - The data sent to/from the mobile device.
- **Control plane data** - The data sent to/from the MCS.
- **Hardware** - All entities possess hardware which are used in the system.
- **Capacity** - The visited networks provides network capacity to the mobile device.
- **Authentication infrastructure** - In Use case B the carrier network opens up its infrastructure for performing the authentication.
- **Accountin? Control plane data - The data sent to/from the MCS.g Information** - In Use case B the networks may charge each other for the use of their infrastructure.
- **Mobility Control Server** - The ISP/MNO/Anyfi Networks operates an address translation service.
- **User information** - The MCS will store information tied to the networks and users in the system.
- **Brand image** - The company operating the system and Anyfi Networks have a brand image to protect.

Table 4.1: Assets in Anyfi.net as well as which entities they are important to.

Asset	Entity
Authentication credentials	Mobile device Home network
User plane data	Mobile device Visited network
Control plane data	Home network Visited network
Hardware	All
Capacity	Visited network
Authentication infrastructure	Carrier network
Accounting Information	Carrier network Visited network
MCS	ISP/MNO/Anyfi Networks
User information	ISP/MNO/Anyfi Networks
Brand image	ISP/MNO/Anyfi Networks

4.1.3 Trust relations

Use case A

As illustrated in Figure 4.3, there is a strong mutual trust relationship between the mobile device and the home network. These entities trust each other more or less by definition as they have access to and have to protect the credentials for the authentication. It can be assumed that the same owner is in control of both the mobile device and the home network. The authentication credentials, data security, network resources and Internet access rely on this relationship to remain secure. As illustrated by the bold arrows in the figure, these assets are critical to the system.

The visited and home networks also by definition trust the ISP that operates the system. This trust is a consequence of the fact that the ISP is assumed to be able to remotely manage the modems and routers of the networks. The ISP also needs access to device information required to run the MCS.

As seen in Figure 4.3, the ISP trusts the visited and home networks which implies that the ISP is exposed to threats originating from the visited network as well as from the home network. The visited and home networks send control data to the MCS but there is nothing that ensures that this data is authentic. Registration information is not directly protected either although such data can be exchanged through other interfaces than in use under operating conditions. However, as noted by the very thin arrow in the figure, the control data that is protected by this trust relationship is not critical to the system. It may affect availability but it cannot compromise a user's credentials or data.

One thing worth noting is the absence of trust relationships between the visited and home networks and between the mobile device and the visited networks. No trust is necessary here as these entities do not rely on the other party to protect something.

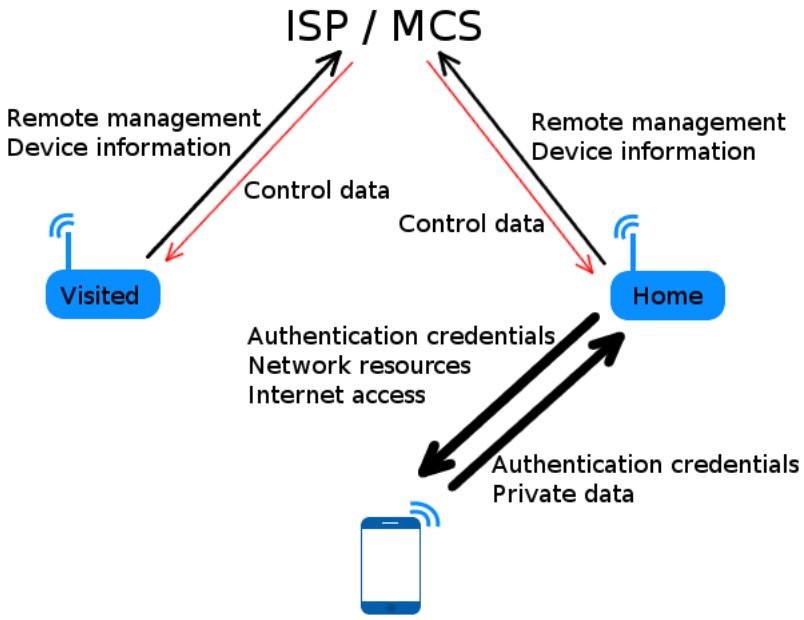

Figure 4.3: Trust relationships in Anyfi.net when configured according to Use case A. An arrow from node A to node B denotes that node B is trusted by node A to protect some asset or perform some action. A bold arrow means it protects important assets. A red arrow means a possible weakness.

Use case B

As seen in Figure 4.4, the trust relationships in Use case B do not differ much compared to the ones in Use case A.

Between the mobile device and the carrier network there is a strong mutual trust relationship. One difference compared to Use case A is that the mobile device is not trusted by the carrier network to protect the authentication credentials. As the authentication protocol EAP-AKA or EAP-SIM is used, each user in the system possesses their own secret key. If that key is compromised only traffic to and from that specific user is compromised, other users remain secure. In Use case A all traffic on the network is protected by the same passphrase which means that if that passphrase is compromised the entire network becomes compromised.

Another difference is that the trust allocated by the networks in the MCS is now more important. This is because with mobile offload the visited networks that facilitate the capacity may be expected to be paid for this service. This means

that the trust relationship now also protects the authenticity and integrity of the accounting reports. This could be a problem as the trust is established through external factors such as business deals which cannot be enforced by the system. A breach of this trust would however only affect the networks involved, the users would be unaffected.

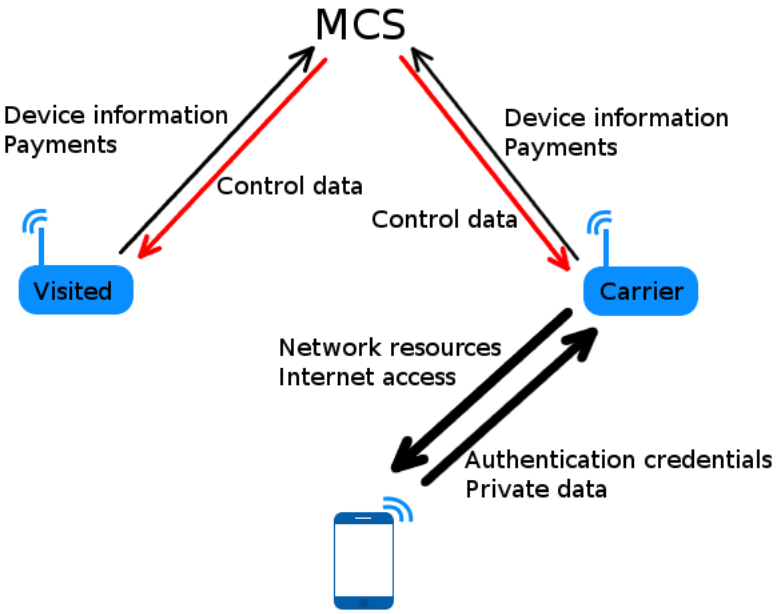

Figure 4.4: Trust relationships in Anyfi.net when configured according to Use case B. An arrow from node A to node B denotes that node B is trusted by node A to protect some asset or perform some action. A bold arrow means it protects important assets. A red arrow means a possible weakness.

4.1.4 Authentication

When the mobile device comes in range of the visited network, but before the authentication is performed, the visited network queries the MCS if the home network of the mobile device is known. The mobile device is recognized by its Media Access Control (MAC) address. If the device is known the visited network receives the information from the MCS that facilitates the visited network with the capability to advertise the SSID of the home network and to tunnel the traffic to the home network.

The authentication protocols used may differ depending on which use case the system is used in. The scenario in Use case A assumes the utilization of WPA/WPA2 authentication and Use case B assumes the utilization of EAP-AKA or EAP-SIM authentication. The Anyfi.net software enforces a minimum level of security by blocking WEP from being used.

Use case A

The authentication flow is illustrated in Figure 4.5.

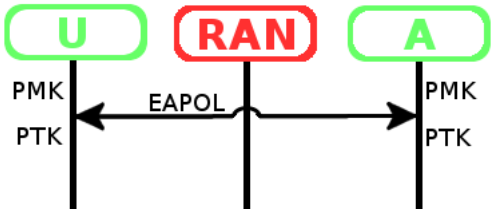

Figure 4.5: Authentication and key transfer in Anyfi.net Use case A. A double headed arrow denotes a negotiation. Text above arrows describes which protocol is used.

WPA/WPA2 authentication uses the EAPOL 4-way handshake to perform mutual authentication between the mobile device and the home network, see Figure 4.5. This handshake protocol transfers nonces and security settings. The actual authentication comes from verifying that the MIC values of these messages are calculated correctly using the secret key. At the end of the protocol both mobile device and the A node have verified that the other party knows the pre-shared secret key and they have created a session key based on the secret key, the identities of both parties and random numbers from both parties.

The properties achieved by the authentication are:

+ Mutual authentication between mobile device and home network
+ Session key agreement
+ Both entities contribute to key derivation
- Long term secret exposed as explained below

Vulnerabilities

As explained in Section 2.2.4 a weak point in the WPA/WPA2 authentication is that eavesdropping on the EAPOL exchanges enables an attacker to perform offline attacks such as dictionary attacks to recover the passphrase. Even a single exchange is in principle sufficient. Hence users should deploy methods through which the keys and passphrases in use are properly chosen.

Note that since the authentication exchange is routed through the Internet there is a higher risk for attacks as any existing vulnerability can now be exploited by a broader audience.

Use case B

The authentication flow in Use case B is shown in Figure 4.6.

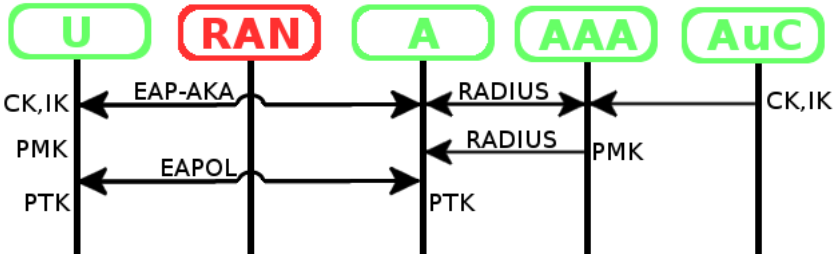

Figure 4.6: Authentication and key transfer in Anyfi.net Use case B. A double headed arrow denotes a negotiation. A single headed arrow denotes a key transfer. Text above arrows describes which protocol is used.

The EAP-AKA (we ignore the EAP-SIM case for the moment) protocol starts with the mobile device sending its identity in a EAP-Response/Identity message. This identity can be either a permanent identity, a temporary identity or a re-authentication identity. The AAA server may respond with an identity request if the received identity was not enough.

Subsequently the AAA server requests an authentication vector based on the received identity and a sequence number from the AuC which contains a nonce, an authentication token, a result value, an encryption key (CK) and an integrity check key (IK). The AAA server sends the nonce and authentication token to the mobile device together with a MIC value calculated from these.

The mobile mobile device runs AKA algorithms to check that the authentication token is correct and to compute the encryption key, integrity check key, result value, and MIC. It then verifies that the received MIC was correct by which it authenticates AuC and then it sends the calculated result to the AAA server.

The AAA server verifies that the received result value is correct by which it authenticates the mobile device. If correct, the server sends an EAP-Success message to the mobile device.

Finally the mobile device and the A node perform the EAPOL 4-way handshake to derive the encryption keys used for the session. The secret key used in the EAPOL exchange is based on the Pairwise Master Key (PMK) generated by the AKA algorithms.

The properties achieved by the authentication are:

+ Mutual authentication between mobile device and carrier network
+ Possible with identity protection
+ Session key agreement
+ Both parties contribute to key generation

4.1.5 Data security

The different kinds of communication can be categorized as follows:

- Internal communication on the visited network.
- Internal communication on the home network.
- Wireless user plane communication between the mobile device and the visited network.
- Wired user plane communication between the visited network and the home network.
- Control plane communication between the MCS and the visited network.
- Control plane communication between the MCS and the home network.

A mobile guest is separated from the internal communication on the visited network by letting the mobile device connect to a virtual network instead of the private network. The wireless traffic with the private network is protected using 802.11i secrity with keys not available to any visiting mobile devices.

Control communication between the MCS and the networks are not secured at all and thus available to anyone (in principle).

Traffic between the mobile device and the home network are encrypted using 802.11i security using the session key derived in the authentication. 802.11i security is considered secure by today's standards. This protection applies for both the wireless transmissions between the mobile device and the visited network as well as the wired transmissions between the host and home networks. It is never decrypted and available outside the mobile device and the trusted home network.

How the keys are generated differ between which use case the system is used in.

Key management

As can be seen in Figure 4.5 and 4.6, the session keys used for encryption are generated in the mobile device and in a device on the trusted network. They are never transferred from the trusted network which ensures confidentiality for the traffic.

Weaknesses

As there is no data protection for control messages to and from the MCS this data is at risk of being manipulated. Eavesdropping on the control data will allow a malicious entity to learn the identity of a router and impersonate it in communication with the MCS. This could potentially allow an attacker to modify network specific settings in the MCS which may affect the service received by the network. Securing this data with confidentiality and integrity protection will prevent such issues.

4.1.6 Anonymity

When a user connects through the Anyfi.net system the home network will become known to the visited network. This may allow the identity of the mobile user to be found. For a home network in Use case A the anonymity set is assumed to be very small and anonymity cannot be ensured. For Use case B the home network is assumed to be a Mobile Network Operator with a large amount of subscribers. Identifying a specific user among those subscribers is assumed to be impossible and thus anonymity can be ensured.

When a mobile user connects using WLAN the Medium Access Control (MAC) address of the device is used and this address can be used to track the user. In Anyfi.net the MAC address is used in the connection procedure which prevents a user from changing it. It is therefore impossible to achieve unlinkability in Anyfi.net.

4.1.7 Availability

There are two obvious points which could be targeted by a malicious entity aiming to disrupt the service for users.

The first and foremost point is the availability of the MCS. As this service is required to introduce networks with each other when setting up the connection, now new connections are possible if the MCS becomes unavailable. The MCS is controlled by an ISP, MNO or Anyfi Networks which are assumed to be able to ensure robustness of this service. It is thus considered unlikely that this weak point can be exploited.

The second weak point is the home network of the mobile device. As all traffic is tunneled to this network it must be available during the entire connection. For Use case A the home network is a residential gateway with low capacity which could easily be overloaded. This would prevent the system from being used by the devices associated with that network. The effect of such an attack would be very limited, likely only effecting a few users. For Use case B the home network is part of a carrier network. Such a network is assumed to be very robust. It is thus considered unlikely that this weak point can be exploited in Use case B.

The visited network may be concerned that the system will disrupt normal traffic by using too much capacity. To avoid this the Anyfi.net software limits the amount of capacity that can be used by visiting devices to only a portion of the available capacity.

4.1.8 Legal aspects

As all traffic in Anyfi.net is tunneled in a protected form from the mobile device to the home network, the home network will appear as the origin and destination of the roaming user's traffic. This transfers all legal responsibilities of the traffic from the visited network to the home network.

Law enforcement performing legal interception of traffic is able to intercept all traffic by monitoring the home network when a mobile user is using the system.

A network operator may have regulatory, moral or financial reasons for restricting certain types of traffic in the system. Only the home network has the possibility to put restrictions on the traffic. The visited network cannot effect the traffic, not on a protocol level nor on a content level.

4.2 SWISH

SWISH supports by some modifications both Use case A and B as described in the framework.

Use case A

To realize Use case A SWISH includes an additional entity. This is the home network of the mobile device. It also requires a secure channel for distribution of certificates.

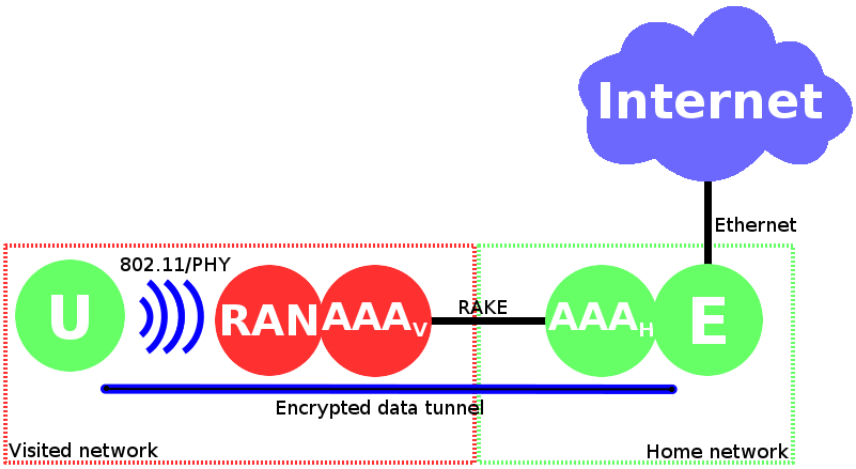

Figure 4.7: SWISH Use case A design

The use case is now as follows:

1. ISP manages firmware/configurations in the modems on the home and visited network and in the mobile device.
2. Home and visited networks register with the CA and receive certificates.
3. The mobile device associates with the visited network.
4. The mobile device, home and visited networks authenticate each other through the RAKE protocol.
5. The visiting network begins tunneling all traffic to the home network.
6. The accounting protocol between home and visited network starts.
7. The mobile device is given Internet access by the home network.

Use case B

While SWISH can be modified to support Use case B, it is not optimal as it does not support SIM-based authentication. However, the accounting protocol included in SWISH is very suitable for this use case.

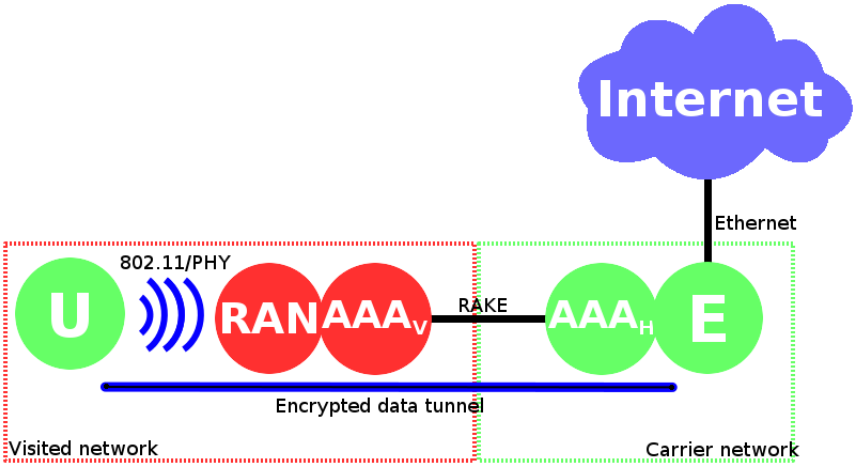

Figure 4.8: SWISH Use case B design

The use case looks now as follows:

1. The MNO and the visited network register with the CA and receive certificates.
2. The mobile device associates with the visited network.
3. The mobile device, visited network and MNO authenticate each other through the RAKE protocol.
4. The visited network begins tunneling all traffic to the carrier network.
5. The accounting protocol between the carrier and visited network starts.
6. The mobile device is given Internet access by the carrier network.
7. The visited network charges the MNO for the service.

4.2.1 Entities

The entities involved in SWISH differ slightly depending on if the system is configured for Use case A or B.

For Use case A, the following entities are involved:

- **Mobile device** running SWISH software and belonging to a user in the system. This device is using the service to roam across networks in the system.

- **Home network** of the mobile device. This network contains a router or a modem running SWISH software.
- **Visited network** that the mobile device is connecting to. This network contains a router or modem running SWISH software.
- **ISP** that manages the networks in the system. The ISP is also assumed to act as a CA and perform location discovery services for the visited networks.

For Use case B, the following entities are involved:

- **Mobile device** running SWISH software and belonging to a user in the system. This device is using the service to roam across networks in the system.
- **Carrier network** which the mobile user is a subscriber of. This networks contains a server running SWISH software.
- **Visited network** that the mobile device is connecting to. This network contains a router or modem running SWISH software.
- **CA** that distributes certificates to the networks in the system. This CA will also likely perform location discovery services for the visited networks.

4.2.2 Assets

The following assets are important to some entity in the system:

- **Authentication credentials** - The credentials used by an entity in the system to authenticate itself. This includes passphrases for networks and certificate private keys.
- **User plane data** - The data sent to/from the mobile device.
- **Control plane data** - The control data sent between the visited and home network.
- **Hardware** - All entities possess hardware which are used in the system.
- **Capacity** - The visited networks provides network capacity to the mobile device.
- **Accounting information** - In use case B the networks may charge each other for the use of their capacity.
- **CA service** - The ISP or CA issues certificates and manages a CRL.
- **User information** - The ISP or CA will store information tied to the networks and users in the system.
- **Brand image** - The ISP and company running the CA service have a brand image to protect.

Table 4.2: Assets in SWISH as well as which entities they are important to.

Asset	Entity
Authentication credentials	Mobile device Home network Visited network
User plane data	Mobile device Visited network
Control plane data	Home network Visited network
Hardware	All
Capacity	Visited network
Accounting information	Carrier network Visited network
CA service	ISP / CA
User information	ISP / CA
Brand image	ISP / CA

4.2.3 Trust relations

Use case A

As illustrated in Figure 4.9, there is in SWISH, similar to the Anyfi.net system, a strong mutual trust relationship between the mobile device and the home network. These entities trust each other by definition as they share keys and it is normally assumed that the same owner is in control of both the mobile device and the home network. The security of authentication credentials, data security, network resources and Internet access rely on this relationship. These assets are critical to the operation of the system which is illustrated in the figure with a bold arrow.

The visited and home networks also by definition trust the ISP that operates the system. This trust is established by allowing the ISP to remotely manage the modems and routes of the networks. It is also trusted to act as a CA in the system. As illustrated by the thinner arrow in the figure, the assets protected by this trust relationship are not critical to the operation of the system.

One thing worth noting is the absence of trust relationships between the networks and between the mobile device and the visited network. No trust is necessary between them as they do not rely on the other party.

Use case B

As can be seen in Figure 4.10, the trust relationships does not differ much compared to Use case A.

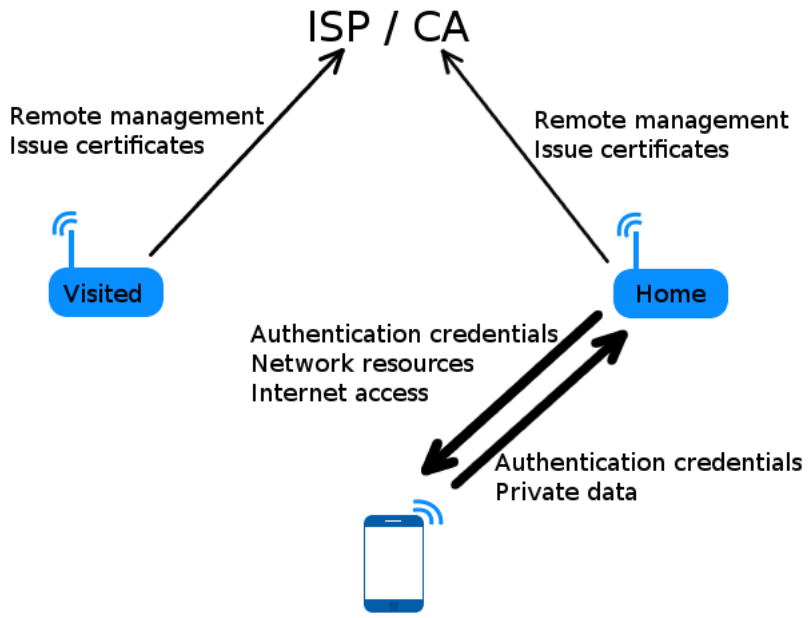

Figure 4.9: Trust relationships in SWISH when configured according to Use case A. An arrow from node A to node B denotes that node B is trusted by node A to protect some asset or perform some action. A bold arrow means it protects important assets. A red arrow means a possible weakness.

One difference is that the networks no longer trust an ISP to remotely manage the network. However, the trust in the CA becomes more important as the usage of certificates is more important in Use case B because of their role in the accounting protocol.

Another difference is that there is a trust relationship between the networks which protects the accounting. This trust is backed by authentication of the networks and an accounting protocol that provides non-repudiation.

4.2.4 Authentication

To perform the authentication SWISH uses a new protocol called RAKE (Roaming Authentication and Key Exchange) which is an extension of EAP and designed especially for SWISH.

All three entities have an active part in the execution of the RAKE protocol by supplying identities and nonces as well as performing authentication.

RAKE

The authentication flow in the RAKE protocol is depicted in Figure 4.11.

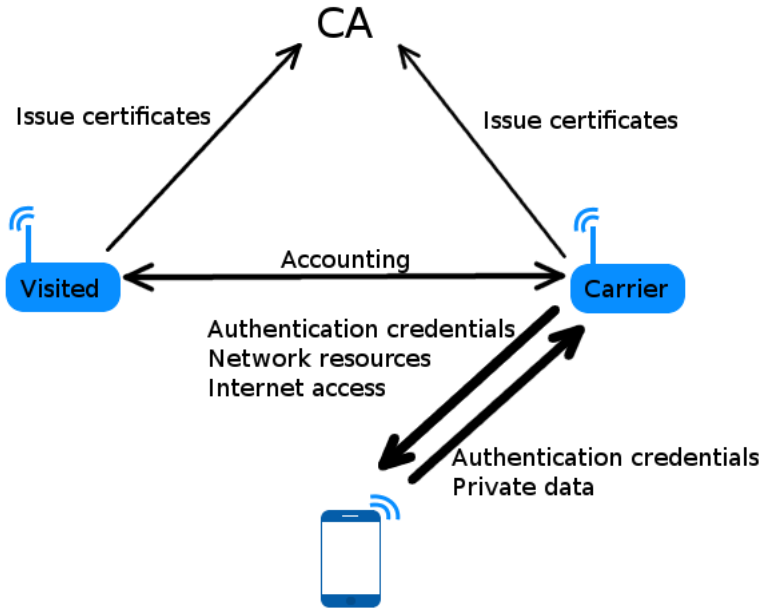

Figure 4.10: Trust relationships in SWISH when configured according to Use case B. An arrow from node A to node B denotes that node B is trusted by node A to protect some asset or perform some action. A bold arrow means it protects important assets. A red arrow means a possible weakness.

The protocol starts with standard EAP messages to decide on a specific authentication protocol after which the AAA_V sends a message with its identity and a nonce to the mobile device.

The mobile device answers with its own nonce, its temporary identity that provides identity protection, and the identity of the home network.

AAA_V sends the two nonces and the identities of U and AAA_V to the AAA_H server.

The AAA_H server generates its own nonce and can then, using the three nonces, the three identities and a secret key shared with U, compute two session keys. It sends the message to AAA_V containing its nonce and identity, a MIC of the session value, one of the session keys encrypted using the public key of AAA_V and finally its signature.

AAA_V verifies the signature to authenticate AAA_H and decrypts the session key. The other data is passed on to U.

U uses the identities and the nonces to calculate the session keys and verifies that the MIC is correct, thereby authenticating AAA_H. It then calculates its own MIC which it sends to AAA_V.

AAA_V signs this message with its private key and passes it on to AAA_H. Using the MIC and the signature, AAA_H can authenticate both U and AAA_V.

The properties achieved by the RAKE protocol are:

+ Mutual authentication between U and AAA_H
+ Mutual authentication between AAA_H and AAA_V
+ Possible with identity protection
+ Session key agreement
+ All entities contribute to key derivation
- Long term secret exposed as explained below

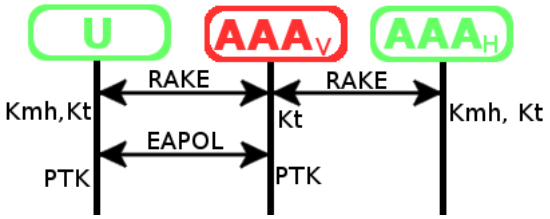

Figure 4.11: Authentication and key transfer in SWISH. A double headed arrow denotes a negotiation. Text above arrows describes which protocol is used.

Weaknesses

A weak point in the authentication is that eavesdropping on a single authentication exchange allows an attacker to perform offline attacks such as dictionary attacks to recover the secret key, see Section 2.2.4. This vulnerability assumed only to be relevant for Use case A where the user can pick their own, potentially weak, passphrase for the home network. In Use case B the user is more likely to be assigned one by the MNO which can avoid poor choices by having proper management procedures in place.

The authentication exchange is routed through the Internet which results in that any existing vulnerabilities are exposed to a broader audience.

Another weakness which in the SWISH authentication solution is the use of certificates. As we discuss in our final Chapter 6 the use of certificates, albeit technically sound, has practical disadvantaged in certain setups.

4.2.5 Data security

Data communication in SWISH can be divided into the following categories:

- Internal communication on the visited network.
- Internal communication on the home network.
- Wireless user plane communication between the mobile device and the visited network.

- Wired user plane communication between the visited network and the home network.
- Control plane communication between the visited network and the home network.

Exactly how these communications channels are secured is not specified by the SWISH system as such things are regarded implementation details.

The end-to-end encryption is an optional setting in the SWISH system which can be disabled if the visiting network operator can be trusted. The tunnel between the two networks still protects the data transferred over the Internet.

In an implementation proposal of the system the SWISH designers use 802.11i security for the wireless transmissions. For the tunneled communication IPsec is used in AH mode for the network to network communication and IPsec in EPS mode for the mobile device to home network communication. The private part of the visited network are separated from the end-user by having the router broadcast two different SSID for the connections.

Key management

As a result of the authentication protocol two keys are generated and distributed, one key, K_t, that is shared among the networks and the mobile device and one key, K_{mh}, shared only by the home network and the mobile device. The key known by all is intended to be used for a secure tunnel between the network and for creating the PTK for securing the wireless transmissions between the mobile device and the visited network. The key shared only by the home network and the mobile device is intended to be used for secure end-to-end encryption.

As illustrated by Figure 4.11 the session keys appearing in the system are generated in the mobile device and in a device on the home network. The end-to-end encryption key K_{mh} is never transferred from these devices which ensures confidentiality for the traffic.

The session key K_t that is used for wireless protection and to secure the accounting protocol is encrypted using the public key of the visited network and transferred to the visited network. It is thus only known by the three parties involved in the connection.

4.2.6 Anonymity

During the authentication, SWISH uses anonymous identities for the mobile user but this is not always enough. When a user connects to the home network through the SWISH system, the home network becomes known to the visited network. This may allow the identity of the mobile user to be found despite using an anonymous identity. For a home network in Use case A the anonymity set is assumed to be very small and anonymity cannot be ensured. For Use case B the home network is assumed to be an MNO with a large amount of subscribers. Identifying a specific user among those subscribers is assumed to be impossible and thus anonymity can be ensured.

When a mobile user connects using WLAN the MAC address of the device is used and this address can be used to track the user. While this MAC address can be changed the system does not specify a way to do it. It would also require the network interface to be restarted which could interrupt other services. It is therefore too impractical to achieve full unlinkability in SWISH.

4.2.7 Availability

There are two points which could be targeted by a malicious entity aiming to disrupt the service for users.

One of them is the availability of the CRL and location discovery service. The CRL and location discovery service may be required for networks to connect to each other, if this service is unavailable then no (new) connections are possible. The CRL and location discovery service is assumed to be controlled by a corporation able to ensure the robustness of the service. It is thus considered unlikely that this weak point can be exploited.

The second point is the home network of the mobile device. As all traffic is tunneled to this network it must be available during the entire connection. For Use case A the home network is a residential gateway with low capacity which could easily be overloaded. This would prevent the system from being used by the devices associated with that network. The effect of such an attack would be very limited, likely only effecting a few users. For Use case B the home network is part of a carrier network. Such a network is assumed to be able to handle large amounts of traffic and be very robust. It is thus considered unlikely that this weak point can be exploited in Use case B.

The visited network in Use case A may be concerned that the system will disrupt normal traffic by using too much capacity. To avoid this the mobile device and the visited network perform an continuous negotiation of how much capacity is available and how much is desired.

4.2.8 Accounting

The SWISH system contains a protocol for performing accounting and adding the ability to charge users for the capacity provided. This comes with a couple of concerns that are relevant in Use case B:

- A malicious visited network operator may attempt to charge too much for the service.
- A malicious home network may attempt to avoid paying for the service.

The SWISH system attempts to solve this by introducing a protocol that provides non-repudiation.

The mobile device negotiates with the visited network how much data it wants to send and how much the visited network allows to send. The mobile device provides a cryptographic commitment of this. After the data has been transferred the visited network requests and proof of this from the mobile device and then requests a non-reputable receipt from the home network. This protocol is then repeated multiple times during the connection.

This protocol ensures that any fraud attempt will be extremely minor. At most only two iterations of the protocol will be at risk which will correspond to a very small amount of data.

4.2.9 Legal aspects

As all traffic in SWISH is tunneled in an encrypted form from the mobile device to the home network the home network will appear as the origin and destination of the traffic. This transfers all legal responsibilities of the traffic from the visited network to the home network.

Law enforcement performing legal interception of traffic is able to intercept all traffic by monitoring the home network when a user is using the system.

A network operator may have moral or financial reasons for restricting certain types of traffic in the system. Only the home network have the possibility to put restrictions on the traffic. The visited network cannot effect the traffic, not on a protocol level or on a content level.

4.3 Fon

Fon supports Use case A as described in the framework. It works best with what can be described as a nomadic user, not a mobile (network) user as in Use case B.

Use case A

The entity deploying the system does not have to be an ISP, it could be Fon itself or another company. However, the system fits the use case best when it is deployed by an ISP that can manage the networks in the system remotely.

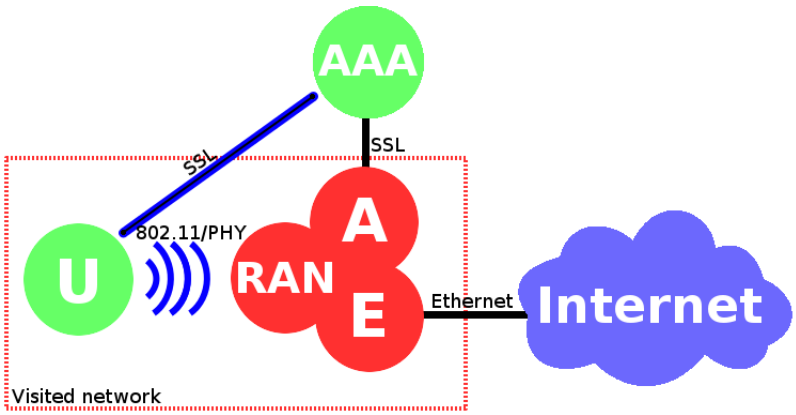

Figure 4.12: Fon Use case A design

Use case A looks now as follows:

1. The ISP manages the firmware/configurations of the modems in network.

2. The mobile user creates an account with the ISP authentication service.
3. The mobile device connects to a visited network.
4. The visited network redirects the mobile device to the authentication service.
5. The authentication service authenticates the mobile device.
6. The mobile device is given Internet access by the visited network.

4.3.1 Entities

The following entities are involved in Fon:

- **Mobile device** belonging to a user in the system. This device is using the service to roam across networks in the system.
- **Visited network** that the mobile device is connecting to. This network contains a router or a modem running Fon software.
- **Authentication server** that performs the authentication of users in the system. This server may be operated by Fon itself or by one of its partnered ISPs.

4.3.2 Assets

The following assets are important to some entity in the system:

- **Authentication credentials** - The credentials used by the mobile device and authentication server to authenticate each other. This is a combination of an email address and a password and a certificate private key.
- **User plane data** - The data sent to/from the mobile device.
- **Control plane data** - The control data sent between the visited network and the authentication server.
- **Hardware** - All entities possess hardware which are used in the system.
- **Capacity** - The visited networks provides network capacity to the mobile device.
- **Accounting information** - The mobile device may purchase a temporary pass for a given amount to use the service. This amount is split between the visited network used to make the purchase and the company running the authentication server.
- **User information** - The authentication server will store information tied to the networks and users in the system.
- **Brand image** - The company running the authentication server have a brand image to protect.

Table 4.3: Assets in Fon as well as which entities they are important to.

Asset	Entity
Authentication credentials	Mobile device Authentication server
User plane data	Mobile device Visited network
Control plane data	Authentication server Visited network
Hardware	All
Capacity	Visited network
Accounting Information	All
User information	Authentication server
Brand image	Authentication server

4.3.3 Trust relationships

As seen in Figure 4.13, the mobile device by definition trusts the ISP that operates the system. This trust relationship protects the authentication credentials of the mobile user.

Also the visited network, by definition, trusts the ISP. This trust is a result of the fact that the ISP is assumed to be able to remotely manage the modems and routers of the network.

The visited network also trusts the mobile device. This trust relationship is a result of allowing the nomadic user to use the Internet connection of the visited network. As depicted in the figure, this relationship reveals that the visited network is exposed to threats from a malicious mobile device since being able to authenticate to the ISP is the only required step to becoming trusted. The visited network is not able to decide who is to be trusted but may face consequences if the connection is misused.

Finally the mobile device trusts both the visited network as well as every device capable of receiving WLAN data in the physical proximity. This trust is a consequence of not encrypting data which allows anyone to view it. As seen in the figure, this relationship is easily compromised since trusting everyone in the physical proximity is not feasible. Hence we have a strange situation where the mobile device has to trust its environment but there are no means in place to instrument such a trust. Hence only data that requires no security can be sent under such a regime or the user must instrument protection means above the connection level.

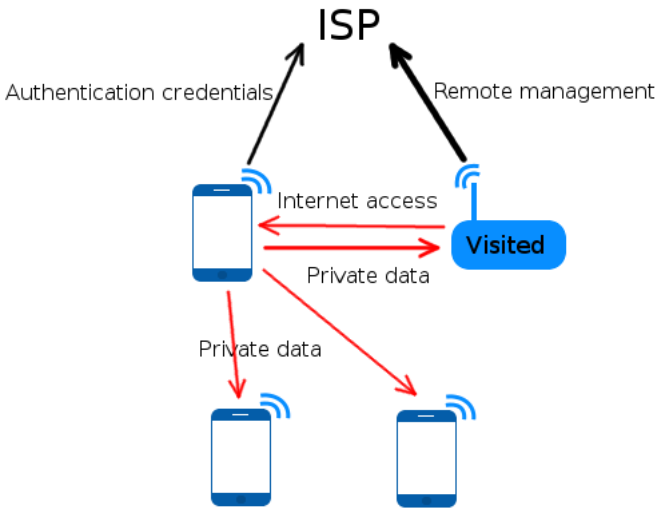

Figure 4.13: Trust relationships in Fon when configured according to Use case A. An arrow from node A to node B denotes that node B is trusted by node A to protect some asset or perform some action. A bold arrow means it protects important assets. A red arrow means a possible weakness.

4.3.4 Authentication

No authentication is required for the initial connection to the visited network but the user is only given restricted Internet access.

When the user attempts to use the connection to visit a web page the user is redirected to the authentication server. This connection is secured using SSL which ensures confidentiality of the data sent.

In SSL the authentication server authenticates to the mobile device using its certificate after which they negotiate security parameters and derive sessions keys use for encrypting the traffic.

The mobile user then submits its authentication credentials over this connection though a web form. The authentication server can then verify that the credentials are correct after which it notifies the visited network to lift the restrictions for the mobile device.

The properties achieved by the authentication are:

+ Mutual authentication between U and AAA

- Security based on user awareness as explained below

- No authentication of visited network

Weaknesses

Browsers typically warn the user if the certificate received in an SSL connection attempt is invalid. However, browsers do not warn if the SSL connection is missing all together as with a normal HTTP connection. The user must himself verify that the authentication is actually performed over a secure connection with the correct server. This makes it easy to trick a user into connecting to a rogue access point which routes the traffic to a fake authentication server.

When this is combined with the fact that the user sends the credentials directly to the authentication server instead of using an authentication protocol it becomes trivial for an attacker to acquire the credentials.

4.3.5 Data Security

The different kinds of communication can be divided into the following categories:

- Internal communication on the visited network.
- Wireless user plane communication between the mobile device and the visited network.
- Control plane communication between the visited network and the authentication server.

The private and public networks are separated using virtual networks. The Fonera router broadcasts two different SSIDs for the networks.

The internal traffic on the visited network is secured using 802.11i wireless security.

There is no security at all for the public part of the visited network. This means that anyone in physical proximity of the visited network are able to view the traffic.

Weaknesses

The lack of data security on the public part of the network may lead to sensitive data getting disclosed by security unaware users and it will limit the use of the system for security aware users.

It also makes it possible to hi-jack connections by changing to the same MAC address as an authenticated user. This allows a mobile device to bypass the authentication.

If a Fon router is incorrectly configured to connect to the Internet through another router running DHCP instead of connecting to the Internet directly, guests connected to the public Fon network will be considered as members of the private network. They will have access to all the resources and traffic on the private network.

4.3.6 Anonymity

As the authentication is performed over an encrypted SSL tunnel, a user has the possibility of staying anonymous when using the system. However, since the traffic sent by the mobile device is not confidentiality protected there is a risk that a user can be identified by studying the data. The mobile user could be identified using cookies, email, web sites visited among other things.

When a mobile user connects using WLAN the MAC address of the device is used and this address can be used to track the user. While this MAC address can be changed the system does not specify a way to do it. It would also require the network interface to be restarted which could interrupt other services. It is therefore too impractical to achieve unlinkability in Fon.

4.3.7 Availability

There is one main point which could be targeted by a malicious entity aiming to disrupt the service for users. This is the authentication server that is used to authenticate users. If this server is unavailable then no new connections are possible.

The visited network may be concerned that the system will disrupt normal traffic by using too much capacity. Fon prevents this by allowing the visited network to specify how much capacity should be available to guests.

4.3.8 Legal aspects

As guest traffic is seen as originating from the visited network, the visited network operator is the first suspect if the Internet connection is used for something illegal. The authentication server keeps logs of every guest connection which may help to prove the operator innocent but additional logs are required by the visited network to identify which traffic was from the private part of the network and which was from guests. The correctness of the logs may also be disputed due to the problem with rogue access points and connection hi-jacking mentioned previously.

Sharing or reselling of Internet access is against the Terms of service of many ISPs. Unless a visited network's ISP is explicitly partnered with Fon he may risk losing Internet access if using the Fon service.

4.4 Eduroam

Eduroam supports Use case B as described in the framework. It does not support Use case A as it requires an infrastructure too advanced for residential networks.

Use case B

Eduroam is not designed for mobile offload but could be used in a similar way. It realizes the use case by replacing the MNO with an educational institution

without means for SIM-based authentication. It also introduces a new entity, federations, that aid in routing authentication exchanges.

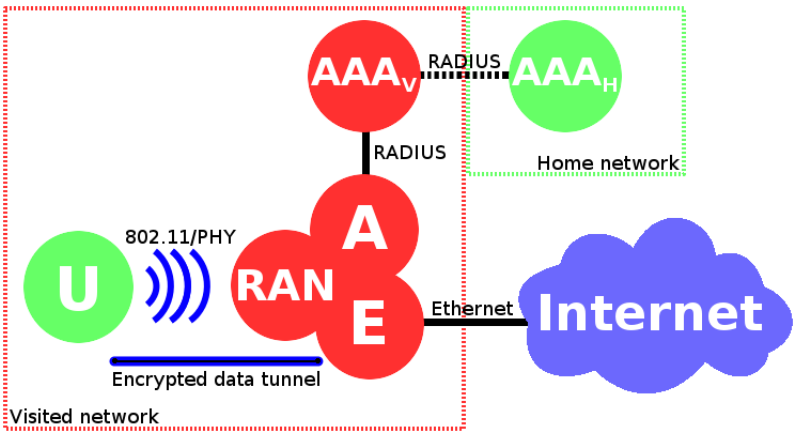

Figure 4.14: Eduroam Use case B design

Use case B looks now as follows:

1. An institution becomes part of the Eduroam system.
2. A user registers at the institution and receives authentication credentials.
3. The user associates with an eduroam network of another institution.
4. The visited network forwards the authentication request to the federation servers.
5. The federation routes the authentication request to the home institute.
6. The mobile device and the home institute authenticate each other.
7. The user is given Internet access by the visited network.

4.4.1 Entities

The following entities are involved in Eduroam:

- **Mobile device** belonging to a user in the system. This device is using the service to roam across networks in the system.
- **Home institute** of the mobile device. This network contains an AAA server able to authenticate the user.
- **Visited network** that the mobile device is connecting to. This network contains an AAA server.
- **Federation servers** that are used to route authentication requests between networks.

4.4.2 Assets

The following assets are important to some entity in the system:

- **Authentication credentials** - The credentials used by the mobile device and home institute to authenticate each other.
- **User plane data** - The data sent to/from the mobile device.
- **Hardware** - All entities possess hardware which are used in the system.
- **Capacity** - The visited networks provides the mobile device with capacity.
- **Authentication infrastructure** - The home network contains infrastructure for performing the authentication.
- **Brand image** - The organisation/institutes running the authentication servers have a brand image to protect.

Table 4.4: Assets in Eduroam as well as which entities they are important to.

Asset	Entity
Authentication credentials	Mobile device Home institute
User plane data	Mobile device Visited network
Hardware	All
Capacity	Visited network
Authentication infrastructure	Home institute
Brand image	Home organisations/institutes

4.4.3 Trust relations

As depicted in Figure 4.15, the mobile device by definition trusts its home network. This trust protects the authentication credentials used by the mobile user.

The mobile device also trusts the visited network. This trust comes as a result of allowing the visited network access to the data sent by the mobile device. As can be seen in the figure, this trust relationship exposes the mobile device to threats from a malicious visited network. This is a result of not authenticating the visited network which means the mobile device does not know who it is placing trust in.

The visited network trusts the mobile device. This trust is a result of allowing the mobile device Internet access and the use of network resources. As seen in the figure, this trust relationship exposes the visited network to malicious mobile devices as the visited network cannot choose which mobile devices to place this trust in.

Finally the home network trusts the visited network. This is a result of the home network exposing its authentication infrastructure to the visited network. As they may communicate through proxy servers they may not know exactly who they are placing the trust in. This may be feasible for the current use of Eduroam but it could cause problems if the system is more widely used.

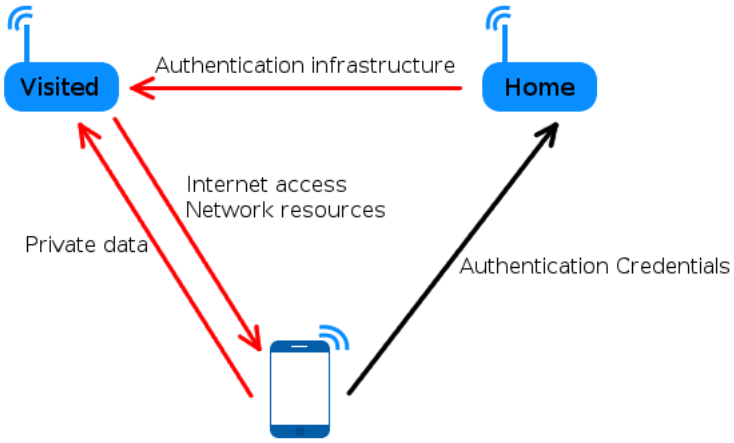

Figure 4.15: Trust relationships in Eduroam when configured according to Use case B. An arrow from node A to node B denotes that node B is trusted by node A to protect some asset or perform some action. A bold arrow means it protects important assets. A red arrow means a possible weakness.

4.4.4 Authentication

The authentication infrastructure in Eduroam is structured as a hierarchy of AAA servers using the RADIUS protocol. When a mobile device connects to the visited network the authentication request is routed using RADIUS/TSL to the AAA server on the user's home institute. The AAA servers use a shared secret when communicating which means that they must have knowledge of each other in advance.

The type of credentials used to authenticate mobile users is decided by the home institute and may be different for different institutes. For university students and staff it is however assumed that they will use a username and password combination.

Eduroam requires that there is some form of confidentiality protection for the authentication exchange. Combined with username and password credentials the most likely protocols for the authentication would be EAP-TTLS + PAP or EAP-PEAP + MS-CHAPv2.

The authentication flow can be seen in Figure 4.16.

Both authentication protocols work in a similar way. They create a TLS connection from the mobile device to the AAA_H server through which the user authentication is performed. The AAA_H server authenticates to the user during the setup of the TLS connection with its certificate.

If PAP is used for authentication the user sends its username and password directly to the AAA_H server through the secure tunnel. The server authenticates the user by comparing the credentials received with values stored in its database.

If MS-CHAPv2 is used for authentication the server sends a challenge containing a nonce to the user. The users sends a response containing its own nonce, and a hash of the username, password and the two nonces to the server. The server verifies that the response was correct and replies with a Success message containing a response to the user-challenge.

The properties achieved by the authentication are:

+ Mutual authentication between mobile device and home institute
+ Possible with identity protection
+ Session key agreement
+ Both parties contribute to key generation
+ Verification of roaming agreement with visited network
- No authentication of visited network

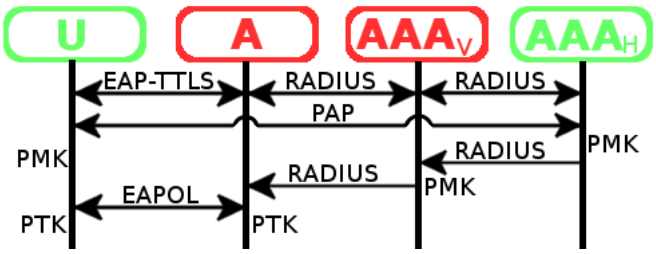

Figure 4.16: Authentication and key transfer in Eduroam. A double headed arrow denotes a negotiation. A single headed arrow denotes a key transfer. Text above arrows describes which protocol is used.

Weaknesses

The visited network is never explicitly authenticated by the mobile device, it is only verified through the RADIUS protocol that a roaming agreement exists with the home institute. This means that the mobile device does not know which network it connects to. This exposes the mobile device to the threat of rogue access points which can be created if the attacker acquires the RADIUS credentials of any eduroam access point.

4.4.5 Data security

The different kinds of communication can be divided into the following parts:

- Internal communication on the visited network.
- Wireless user plane communication between the mobile device and the visited network.
- Control plane communication between the visited network and the home network.

The two parts of the network are separated using virtual networks.

The communication on the network is protected using 802.11i security. The encryption keys used are derived during the authentication.

An important note is that the data protection only applies for the wireless transmission, the visited network has access to the unencrypted traffic.

The control plane traffic is secured using the RADIUS protocol.

Key management

During the authentication keying material is derived from the TLS connection in the mobile device and in the AAA_H on the home institute. This keying material is used to create the session key. As seen in Figure 4.16, the session key is then transferred using the RADIUS protocol to the access point on the visited network where the encryption keys are derived.

Weaknesses

The fact that the visited network has access to the data combined with the fact that the visited network is never explicitly authenticated means that the mobile user does not have any control of who is given access to the data. This may be acceptable when it is known that the visited network is another university which may earn it some degree of trust but it may prevent the system from being used in other situations on a larger scale.

4.4.6 Anonymity

As mentioned earlier it is possible to use anonymous identities during the authentication which gives users the possibility or staying anonymous when using the system. However, since the traffic is available to the visited network there is a risk that the user can be identified by studying the data. The mobile user could be identified using cookies, email, web sites visited among other things.

When a mobile user connects using WLAN the MAC address of the device is used and this address can be used to track the user. While this MAC address can be changed the system does not specify a way to do it. It would also require the network interface to be restarted which could interrupt other services. It is therefore too impractical to achieve unlinkability in Eduroam.

4.4.7 Availability

There are two obvious points which could be targeted by a malicious entity aiming to disrupt the service for users.

First is the AAA server of the home institute. If this server is unavailable it is not possible for users belonging to that network to authenticate themselves which prevents them from using the service.

The other point is the federation servers used to route authentication requests. If these become unavailable then authentication requests to or from institutions within that federation will fail and the user will not be able to use the service.

Both the AAA servers of institutions and those of federations are assumed to be managed by large organizations able to ensure that they are robust. It is thus considered unlikely that these weak points can be exploited.

4.4.8 Legal aspects

As guest traffic is seen as originating from the visited network, the visited network is the first suspect if the Internet connection is used for something illegal. Due to this both the visited network and the home institute are required to keep logs of the connections to be able to identify misbehaving users.

It also means that law enforcement performing legal interception of a user's traffic must monitor all networks that the user connects to.

4.5 Passpoint

Passpoint supports Use case B as described in the framework. While it could support Use case A as well it is designed for commercial use and would require an authentication infrastructure more advanced than what is typically available in a residential network.

Use case B

When realizing the use case Passpoint introduces a new protocol, Access Network Query Protocol (ANQP), that lets the mobile device discover the capabilities of the visited network before it actually attempts to connect.

For Passpoint Use case B looks now as follows:

1. The MNO creates a roaming agreement with the visited network operator.
2. The mobile device determines the capabilities of the visited network.
3. The mobile device associates with the visited network.
4. The visited network routes the authentication request to the carrier network.
5. The mobile device and the MNO authenticate each other.
6. The mobile device is given Internet access by the visited network.
7. The visited network operator charges the MNO for the service.

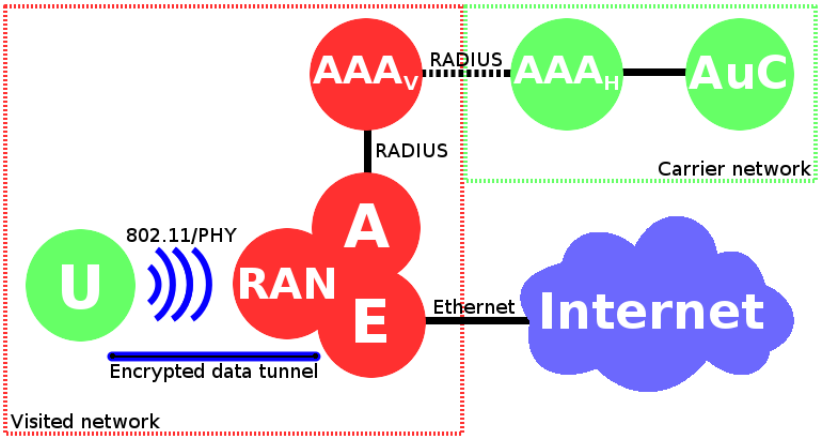

Figure 4.17: Passpoint Use case B design

4.5.1 Entities

The following entities are involved in Passpoint:

- **Mobile device** belonging to a user in the system. This device is using the service to roam across networks in the system.
- **Carrier network** of the mobile device. This network contains an AAA server able to authenticate the user.
- **Visited network** that the mobile device is connecting to. This network contains an AAA server.

4.5.2 Assets

The following assets are important to some entity in the system:

- **Authentication credentials** - The credentials used by the mobile device and carrier network to authenticate each other.
- **Use plane data** - The data sent to/from the mobile device.
- **Hardware** - All entities possess hardware which are used in the system.
- **Capacity** - The visited networks provides the mobile device with capacity.
- **Authentication infrastructure** - The carrier network contains infrastructure for performing the authentication.
- **Accounting information** - The carrier network may pay the visited network for the use of the network.
- **Brand image** - Both the visited network and the carrier network have an brand image to protect.

Table 4.5: Assets in Passpoint as well as which entities they are important to.

Asset	Entity
Authentication credentials	Mobile device Carrier network
User plane data	Mobile device Visited network
Hardware	All
Capacity	Visited network
Authentication infrastructure	Carrier network
Brand image	Carrier network Visited network

4.5.3 Trust relations

As can be seen in Figure 4.18, the mobile device by definition trusts its carrier network. This trust protects the authentication credentials used by the mobile user and the carrier network.

The mobile device also trusts the visited network. This trust comes as a result of allowing the visited network access to the data sent by the mobile device. This trust relationship exposes the mobile device to threats from the visited network since the visited network is not authenticated which means the mobile device does not know who it is placing trust in.

The visited network trusts the mobile device. This trust is a result of allowing the mobile device Internet access. As seen in the figure, this trust relationship exposes the visited network to misuse by the mobile devices as the visited network cannot choose which mobile devices to place this trust in.

Finally the carrier network trusts the visited network. This is a result of the carrier network exposing its authentication infrastructure to the visited network and allowing the visited network to perform the accounting. The carrier network may not directly authenticate the visited network and has no guarantee that the visited network is honest when performing the accounting which exposes it to possible fraud.

4.5.4 Authentication

The authentication flow can be seen in Figure 4.19.

The authentication procedure starts when the mobile device comes within range of the access point and starts the Passpoint exchange. The mobile device requests information about which services the access point can provide and which MNOs or other service providers it has roaming agreements with. If the mobile device finds the access point sufficient for its needs it will attempt to connect. The access point forwards the authentication data to its local AAA_V server on the

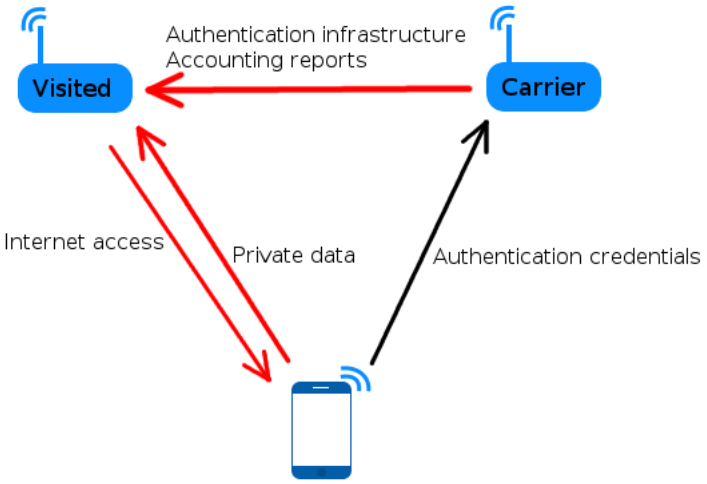

Figure 4.18: Trust relationships in Passpoint when configured according to Use case B. An arrow from node A to node B denotes that node B is trusted by node A to protect some asset or perform some action. A bold arrow means it protects important assets. A red arrow means a possible weakness.

visited network. From there the authentication request is routed using RADIUS through multiple AAA servers to one on the carrier network.

Between the mobile device and the AAA_H server the EAP-AKA protocol is performed.

The EAP-AKA protocol starts with the mobile device sending its identity in a EAP-Response/Identity message. This identity can be either a permanent identity, a temporary identity or a re-authentication identity. The AAA server may respond with an identity request if the received identity was not enough.

The AAA_H server then requests an authentication vector based on the received identity and a sequence number from the AuC which contains a nonce, an authentication token, a result value, an encryption key (CK), and an integrity check key (IK). The AAA_H server sends the nonce and authentication token to the mobile device together with a MIC value calculated from these.

The mobile mobile device runs its AKA algorithm(s) to check that the authentication token is correct and to compute the encryption key, integrity check key, result value, and MIC. It then verifies that the received MIC was correct by which it authenticates AuC and then it sends the calculated result to the AAA_H server.

The AAA_H server verifies that the received result value is correct by which it authenticates the mobile device. If correct, the server sends an EAP-Success message to the mobile device.

The properties achieved by the authentication are:

+ Mutual authentication between mobile device and carrier network
+ Possible with identity protection
+ Session key agreement
+ Both parties contribute to key
+ Verification of roaming agreement with visited network
- No authentication of visited network

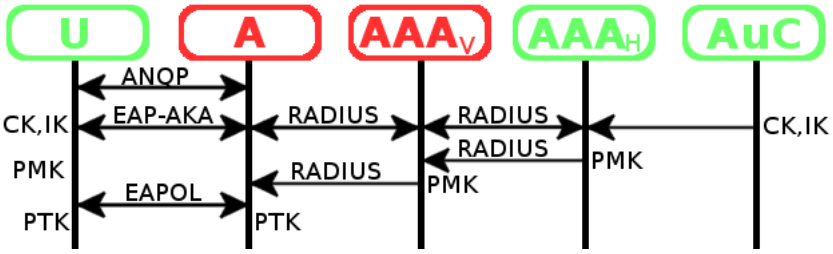

Figure 4.19: Authentication and key transfer in Passpoint. A double headed arrow denotes a negotiation. A single headed arrow denotes a key transfer. Text above arrows describes which protocol is used.

Weaknesses

The visited network is never explicitly authenticated by the mobile device, it is only verified through the RADIUS protocol that a roaming agreement exists with the carrier network. This means that the mobile device does not know which network it connects to and can thus not protect against rogue access points. Possessing the shared secret used with RADIUS of a single access point in the system is enough to setup a rogue access point.

4.5.5 Data security

The different kinds of communication can be divided into the following parts:

- Wireless user plane communication between the mobile device and the visited network.
- Control plane communication between the visited network and the home network.

The user plane traffic is protected using 802.11i security with the encryption keys derived during the authentication. An important note is that the data protection only applies for the wireless transmission, the visited network have access to the unencrypted traffic.

The control plane traffic is secured with the RADIUS or DIAMETER protocol.

Key management

During the authentication keying material is derived through the EAP-AKA protocol in the mobile device and in the AuC server on the carrier network. This keying material is used to create the session key. As seen in Figure 4.19 the session key is then transferred using the RADIUS protocol to the access point on the visited network where the encryption keys are derived.

Weaknesses

The fact that the visited network has access to the data combined with the fact that the visited network is never explicitly authenticated means that the mobile user does not have any control of who is given access to the data.

4.5.6 Anonymity

During the authentication, EAP-AKA uses anonymous identities for the mobile user which gives users the possibility of staying anonymous when using the system. However, since the traffic is available to the visited network there is a risk that the user can be identified by studying the data. The mobile user could be identified using cookies, email, web sites visited among other things.

When a mobile user connects using WLAN the MAC address of the device is used and this address can be used to track the user. While this MAC address can be changed the system does not specify a way to do it. It would also require the network interface to be restarted which could interrupt other services. It is therefore too impractical to achieve unlinkability in Passpoint.

4.5.7 Availability

There is one point which could be targeted by a malicious entity aiming to disrupt the service for users.

The AAA_H server on the carrier network must be available for a user to authenticate himself. If it is unavailable then none of that carrier's subscribers will be able to use the service. The carrier network is assumed to be robust hence it is considered unlikely that this weak point can be exploited.

4.5.8 Legal aspects

As guest traffic is seen as originating from the visited network, the visited network is the first suspect if the Internet connection is used for something illegal. Due to this both the visited network and the carrier network are required to keep logs of the connections to be able to identify misbehaving users.

It also means that law enforcement performing legal interception of a user's traffic must monitor all networks that the user connects to.

Chapter 5
Comparison

This chapter contains a comparison of the five analysed systems. They are divided into two groups based on the use cases presented in the framework. In each group the systems are compared against each other according to the subjects treated in the analysis.

Table 5.1: Table of systems that will be compared. Comparison will be column-wise.

Use case A	Use case B
Anyfi.net	Anyfi.net
SWISH	SWISH
Fon	Eduroam
	Passpoint

5.1 Use case A

5.1.1 System design

As can be seen in the Figures 4.3 and 4.9, the design of Anyfi.net and SWISH are similar. Both systems split the traditional AP across different networks. In SWISH, the visited network is more complex than in Anyfi.net. This is because in SWISH the visited network is involved with the authentication and contains functions such as encryption/decryption and accounting. In Anyfi.net the visited network acts only as a radio head. Something similar to the MCS entity in Anyfi.net will likely be present also in SWISH but it is not clearly defined in the system.

Fon differs a lot from the other two in that it does not contain a user controlled home network. The authentication server is instead a centralized server outside of the mobile user's control. It also means that all of the normal AP functionality is contained on the visited network.

5.1.2 Trust model

As can be seen in Figures 4.3, 4.9, 4.13 and summarized in Table 5.2, the trust relationships in Anyfi.net and SWISH are very similar. An important common point is that the mobile devices are not required to trust the visited networks, they only trust their home networks. This relationship is identical in both systems, it covers authentication, Internet access, network resources and data.

Table 5.2: Trust relations in Use case A. The table displays if a trust relation exists or not or if it is not applicable to the system.

Property	Anyfi.net	SWISH	Fon
Mobile user trust home network	Yes	Yes	-
Mobile user trust visited network	No	No	Yes
Mobile user trust ISP	-	-	Yes
Home network trust mobile user	Yes	Yes	-
Home network trust visited network	No	No	-
Home network trust ISP	Yes	Yes	-
Visited network trusts mobile user	No	No	Yes
Visited network trusts home network	No	No	-
Visited network trusts ISP	Yes	Yes	Yes
ISP trust mobile user	No	No	No
ISP trust home network	Yes	No	-
ISP trust visited network	Yes	No	No

The main difference between them is that in Anyfi.net the ISP trust the networks. This relationship is not found in SWISH. Since this relationship in Anyfi.net exposes the ISP it gives SWISH an advantage but it is very small as the relationship does not affect the security of the end users.

Fon is very different from the other two systems as there is no connection to the home network when a mobile device is roaming, there is not even a need for a home network to exist. Instead the mobile device must trust both the visited network as well as other mobile devices in the physical proximity. This limits the environments where the system is suitable in and which type of traffic that should be sent on it. The visited network must also trust the mobile device as it is giving it direct Internet access. This can be a problem since the visited network relies on the ISP to authorize mobile devices instead of choosing which devices to trust on its own.

Anyfi.net and Fon are similar in that there is not a big requirement for networks to become a part of the system. The only thing that is required is that the access point run software specific to the system. This makes the trust relationships that depend on these entities susceptible to abuse.

All three systems are similar in that the networks by definition trust the ISP that runs the systems. In Fon the mobile device also trusts the ISP.

5.1.3 Authentication

Authenticated entities

The interesting functions for the authentication are the following:

- **F1** - Authenticate the authentication server on the trusted network
- **F2** - Authenticate the visited network
- **F3** - Authenticate the mobile device
- **F4** - Route authentication exchanges

Table 5.3: Overview of the location of authentication functions. Green backgrounds denote that the entity is by definition trusted by the mobile device and red backgrounds denotes that the entity is untrusted by the mobile device.

Anyfi.net	U	RAN	A		E	
F1	X					
F2	-	-	-		-	
F3			X			
F4	-	-	-		-	
Fon	U	RAN	A		E	AAA_H
F1	X					
F2	-	-	-		-	-
F3						X
F4	-	-	-		-	-
SWISH	U	RAN		AAA_V	E	AAA_H
F1	X			X		
F2						X
F3						X
F4				X		

All systems attempt to achieve similar goals with authentication. As seen in the Table 5.3, they all achieve mutual authentication between the mobile device and the authenticator.

Fon is slightly different in this as the authenticator is a central server which is the same for all users, rather then a server in the home network as with Anyfi.net and SWISH.

SWISH is the only system that performs the authentication through a proxy server. In both Anyfi.net and Fon the mobile device connects directly to the authentication server. This increases the ways the authentication protocol in SWISH could be attacked but presently no vulnerabilities that could exploit this attack vector are known.

SWISH differs from the other two systems in that it also performs mutual authentication between the visited and home network. This enables the networks to perform better control of who is allowed to use the networks. However, this control is not so relevant for Use case A as both networks are assumed to be managed by the same ISP which removes the need for security in the accounting protocol as no charging will be required.

SWISH does, however, make it more expensive to recover from security incidents. While the secret key of a network can be changed rather easily if the number of users of the network are few, revoking a certificate, requesting a new one, issuing it and finally installing it is a expensive process. While a compromised certificate does not compromise the data which relies on the secret key, it allows a malicious entity to impersonate the network towards other networks and the managing ISP. Again, this is not a big issue in Use case A where accounting is less relevant.

Authentication implementation

Table 5.4: Authentication credentials used in the different systems.

	Anyfi.net	**Fon**	**SWISH**
Mobile device	Secret key	Email+password	Secret key
Authenticator	Secret key	Certificate	Secret key/Certificate
Visited network	-	-	Certificate

As can be seen in Table 5.4 the most similar authentication is in the systems Anyfi.net and SWISH. Anyfi.net uses the standard EAPOL handshake from the 802.11 standard and SWISH uses the RAKE 3-way handshake. Both protocols are based on a challenge-response exchange using a secret key to perform the authentication of the mobile device and the home network.

Both systems suffer from the vulnerability that offline attacks can be mounted to recover the secret key after eavesdropping on the authentication exchange. This vulnerability is present in normal WPA/WPA2 authentication as well but becomes more serious in the considered systems as the authentication exchange is exposed to a broader "audience". This affects users who use a weak secret key that is vulnerable to dictionary attacks.

Compared to Anyfi.net the protocol in SWISH is a little different in that it includes digital signatures that allow the networks to authenticate each other even if they had no prior knowledge of each other (but recall the there the CA and its root key forms the a priori knowledge). The authentication also results in two different keys, one for data end-to-end encryption and one for securing the accounting protocol used between the networks.

Fon on the other hand is very different as it does not use an authentication protocol. The fact that the authentication relies on a SSL connection means that users must manually detect a rogue access point rather then a automatic detection through a protocol as in Anyfi.net and SWISH. This makes is far more likely that

authentication credentials are compromised in Fon compared to Anyfi.net and SWISH. As the authentication credentials are the email and password of the user there is a risk that the user is using the same password or a similar one with other accounts such as email, banking or social web sites which could also become compromised.

The authentication in both Anyfi.net and SWISH can be performed without any user interaction if they have connected to the network before. Users of Fon must manually perform the authentication each time.

Data security and key management

The interesting functions for the data security and key management are the following:

- **F5** - Perform encryption/decryption of data
- **F6** - Derive session key
- **F7** - Access to session key

Table 5.5: Overview of the location of data security functions. Green backgrounds denote that the entity is by definition trusted by the mobile device and red backgrounds denotes that the entity is untrusted by the mobile device.

Anyfi.net	U	RAN	A		E	
F5	X				X	
F6	X		X			
F7	X		X		X	
Fon	U	RAN	A		E	AAA_H
F5	-	-	-		-	-
F6	-	-	-		-	-
F7	-	-	-		-	-
SWISH	U	RAN		AAA_V	E	AAA_H
F5	X				X	
F6	X					X
F7	X				X	X

As can be seen in Table 5.5, Fon differs significantly from the other systems by not having any data security for the public part of the network. This is obviously a big issue if the users of the system wish to transmit sensitive data. As a result, Fon users are limited in where they can use the system and what they can use it for.

The resulting security for user plane data traffic is the same in both Anyfi.net and SWISH. Data is encrypted end-to-end from the mobile device to the exit point on the home network. The key used for end-to-end encryption is derived in the

mobile device and at the home network and never transferred to any untrusted device. This means that users of the system can expect the same level of user plane data security as when they are connected to their home networks directly.

SWISH has the option to use additional encryption for the wireless transmission but it is unnecessary when end-to-end encryption is being used. A compromised K_{mh}, see section 4.2.5, will likely be caused by a compromised secret key which would allow the attacker to also derive the PTK.

5.1.4 Availability

All three systems share a similar weak point when it comes to availability. Particularly it is the Mobility Control Server in Anyfi.net and SWISH and the AAA server in Fon that could cause concern. However, these are enterprise owned and controlled servers and can thus be considered robust. Therefore it is considered unlikely that these servers become unavailable.

Anyfi.net and SWISH share another weak point which is availability of the home network. Since if the home network which is now made accessible from the outside to provide the Internet access service, becomes unavailable through an attack likewise the roaming Internet service will be not available. However, the effect of such an event is rather limited, effecting only the user (or users) from the targeted home network. The home network becoming unavailable may thus be considered to be a minor vulnerability.

5.1.5 Anonymity

Table 5.6: How the systems perform in regards to anonymity.

	Anyfi.net	**Fon**	**SWISH**
Anonymity	No	Depends on user	No
Unlinkability	No	No	No

As can be seen in Table 5.6, none of the systems achieves complete anonymity. With Anyfi.net and SWISH the address of the home network will be known. As a residential network is assumed to have a very small anonymity set, this may allow an attacker to find the identity of the mobile user. With Fon and attacker could use information from the traffic such as cookies, web sites visited and the information sent to learn the identity of the mobile user.

The systems also all fail to achieve unlinkability as they rely on the WLAN standard which uses the MAC address of devices. This MAC address can be tracked between different sessions even if the data sent is encrypted.

5.1.6 Legal aspects

Because of the use of a tunneling solutions in Anyfi.net and SWISH but not in Fon the former two have similar characteristics when looking as the legal implications

of the solutions. Fon on the other hand gives a setup where the user data flow is connected to the Internet via the different visited networks. We come back to the implications of these differences in the last chapter.

It should be noted that identity theft is rather simple to stage in the Fon system. This makes also that the logging in the Fon system may not be accurate which could be worse than no logs at all.

5.2 Use case B

5.2.1 System design

As with Use case A, Anyfi.net and SWISH have a similar design, they both split the traditional AP across different networks. The difference is that the visited network is slightly more complex in the SWISH case and Anyfi.net supports a more advanced authentication infrastructure.

The design of Eduroam and Passpoint are very similar as well. In many cases they would be identical but in connection with Use case B Passpoint is assumed to also contain a AuC. Compared to Anyfi.net and SWISH they keep the traditional AP in the visited network. Rather then connecting directly to the home network Eduroam and Passpoint use multiple proxy AAA servers.

5.2.2 Trust model

The trust relations for the systems are illustrated in Figures 4.4, 4.10, 4.15 and 4.18 and summarized in Table 5.7.

Table 5.7: Trust relations in Use case B. The table displays if a trust relation exists or not or if it is not applicable to the system.

Property	Anyfi.net	SWISH	Eduroam	Passpoint
Mobile user trust carrier network	Yes	Yes	Yes	Yes
Mobile user trust visited network	No	No	Yes	Yes
Mobile user trust third party	No	No	-	-
Carrier network trust mobile user	Yes	Yes	No	No
Carrier network trust visited network	No	Yes	Yes	Yes
Carrier network trust third party	Yes	Yes	-	-
Visited network trusts mobile user	No	No	Yes	Yes
Visited network trusts carrier network	No	Yes	No	No
Visited network trust third party	Yes	Yes	-	-
Third party trust mobile user	No	No	-	-
Third party trust carrier network	Yes	No	-	-
Third party trust visited network	Yes	No	-	-

Similar to the grouping in the design, we see that the trust models for Anyfi.net and SWISH are very similar and that the models for Eduroam and Passpoint are very similar.

The largest difference between the two groups is that with Eduroam and Passpoint the mobile device must trust the visited network and the visited network must trust the mobile device. This is not needed in Anyfi.net and SWISH. This assumed trust relationship is a problem as the visited network and mobile device are unknown to each other. Holding trust in an unknown entity is not feasible.

Another difference is that the networks in Eduroam and Passpoint do not require any trust in a third part like with Anyfi.net and SWISH which utilizes a MCS or location discovery service.

Within the two groups there are only small differences. In Anyfi.net the third party trusts the networks which is not present in SWISH. This is a potential cause of problems as the networks are trusted to provide accounting reports but there are insufficient means to ensure that these are accurate.

In SWISH the networks trust each other to perform the accounting. This trust is ensured by mutual authentication between the networks and non-repudiation in the accounting protocol.

For Eduroam and Passpoint, the trust relationship between the visited network and the home network is more important in Passpoint as it also protects any accounting. In the real Eduroam system the accounting is in fact mostly irrelevant as no charging from individuals is in place. In both systems this is deemed to be a possible vulnerability as the networks do no authenticate each other.

5.2.3 Authentication

Authenticated entities

The interesting functions for the authentication are the following:

- **F1** - Authenticate the authentication server on the trusted network
- **F2** - Authenticate the visited network
- **F3** - Authenticate the mobile device
- **F4** - Route authentication exchanges

As seen in the Table 5.8, all systems achieve mutual authentication between the mobile device and a server on the home network as functions F1 and F3 are performed in the system.

SWISH differs from the rest by also performing function F2 which achieves mutual authentication between the visited network and the home network. This enables the networks to perform better control of who is allowed to use the network and which networks are allowed to be used.

Anyfi.net does not achieve authentication between the networks but that is not a negative point. As all authorization and accounting is handled through a trusted third party, such authentication would be unnecessary.

Table 5.8: Overview of the location of authentication functions. Green backgrounds denote that the entity is by definition trusted by the mobile device and red backgrounds denotes that the entity is untrusted by the mobile device.

Anyfi.net	U	RAN	A		E	AAA_H	AuC
F1	X						
F2	-	-	-		-	-	-
F3						X	
F4			X				
SWISH	U	RAN		AAA_V	E	AAA_H	
F1	X			X			
F2						X	
F3						X	
F4				X			
Eduroam	U	RAN	A	AAA_V	E	AAA_H	
F1	X						
F2	-	-	-	-	-	-	
F3						X	
F4			X	X			
Passpoint	U	RAN	A	AAA_V	E	AAA_H	AuC
F1	X						
F2	-	-	-	-	-	-	-
F3						X	
F4			X	X			

While the routing system used in Passpoint and Eduroam usually requires shared secrets between the servers involved in the routing it does not fulfil authentication. This is because the authentication may be routed through multiple servers and thus the carrier network and the visited network may not communicate directly. It does however verify that there exist some form of roaming agreement between them.

Authentication implementation

As can be seen in Table 5.9, while the credentials used are different, the systems all achieve similar results through the protocols used. All systems uses some form of confidentiality protection for the authentication. EAP-AKA in Anyfi.net and Passpoint and RAKE in SWISH uses a challenge-response handshake to perform the authentication. In Eduroam the credentials are transferred through an encrypted TLS tunnel.

The protocol in SWISH is a little different in that it also includes digital signatures and results in two different keys, one for the end-to-end encryption and one for the accounting protocol.

Table 5.9: Authentication credentials used in the different systems

	Anyfi.net	**SWISH**	**Eduroam**	**Passpoint**
Mobile device	USIM key	Secret key	Username+ Password	USIM key
Authenticator	USIM key	Secret key/ Certificate	Certificate	USIM key
Visited network	-	Certificate	-	-

The protocol in SWISH suffers from the vulnerability that offline attacks to recover secret key can be performed after eavesdropping on the authentication exchange. However if the system is deployed by an MNO for mobile offload it would seem unlikely that subscribes could pick their own, potentially weak, secret keys. Instead they are assumed to be assigned strong keys by the MNO that are not easily broken.

All systems can connect to a network and authenticate without user intervention. However in Anyfi.net, SWISH, and Eduroam, devices must be configured to connect to a specific network, either through a previous connection or through settings pushed by an MNO. In Passpoint, devices may connect to unknown networks if the capabilities of the network match the requirements of the device. Such requirements are typically configured by an MNO.

Data security and key management

The interesting functions for the data security and key management are the following:

- **F5** - Perform encryption/decryption of data
- **F6** - Derive session key
- **F7** - Access to session key

As can be seen in Table 5.10, all four systems perform encryption to provide confidentiality protection for the data. However they differ on which network this confidentiality protection is terminated.

In all systems the session key is derived by the mobile device and an authentication server on the trusted network.

In both Anyfi.net and SWISH the data protection session key is transferred to another point on the trusted network where the encryption/decryption is then performed. An important point with this is that the session key is never transferred outside the trusted network.

In both Eduroam and Passpoint the data protection session key is transferred to the visited network where the encryption/decryption is then performed. This means that the data confidentiality only applies for the wireless part and the protection is terminated on a network not trusted by the mobile device. This means

Table 5.10: Overview of the location of data security functions. Green backgrounds denote that the entity is by definition trusted by the mobile device and red backgrounds denotes that the entity is untrusted by the mobile device.

Anyfi.net	U	RAN	A		E	AAA_H	AuC
F5	X				X		
F6	X						X
F7	X		X		X	X	X
SWISH	U	RAN		AAA_V	E	AAA_H	
F5	X				X		
F6	X					X	
F7	X				X	X	
Eduroam	U	RAN	A	AAA_V	E	AAA_H	
F5	X				X		
F6	X					X	
F7	X		X	X	X	X	
Passpoint	U	RAN	A	AAA_V	E	AAA_H	AuC
F5	X				X		
F6	X						X
F7	X		X	X	X	X	X

that users are limited in which environments that they can use the systems as they must trust the visited networks with their data.

SWISH has the option to use additional encryption for the wireless transmission but it is unnecessary when end-to-end encryption is being used. A compromised K_{mh} will likely be caused by a compromised secret key which would allow the attacker to also derive the PTK.

5.2.4 Availability

All systems share a similar weak point when it comes to availability. The authentication of the mobile device is always performed by a server on the trusted network. If this authentication server is unavailable the mobile user will be unable to connect. In Use case B this server is assumed to be owned and managed by an MNO and is thus considered to be robust. This server becoming unavailable is considered unlikely for all systems.

Another weak point present in Anyfi.net and SWISH is the end-point to where traffic is tunneled. This point must also be available for the systems to work. For Use case B this point is assumed to be located on the core network of an MNO and is thus considered to be robust. This point becoming unavailable is considered unlikely for both systems.

5.2.5 Anonymity

Table 5.11: How the systems perform in regards to anonymity

	Anyfi.net	SWISH	Eduroam	Passpoint
Anonymity	Yes	Yes	Depends on user	Depends on user
Unlinkability	No	No	No	No

As can be seen in Table 5.11, all systems support some form of anonymous identities during the authentication which prevents identifying the mobile user when using the assumed authentication protocols. While the home network can be identified in all systems it is not considered a vulnerability. Since the home networks in this use case will be MNOs which serves a large number of mobile devices it is assumed to be unlikely that a mobile user can be identifies based on which carrier they use.

Eduroam and Passpoint are somewhat weaker than Anyfi.net and SWISH as the traffic of the mobile user is available to the visited network. The traffic may contain information which could identify the mobile user.

All the systems fail to achieve unlinkability as they reveal their MAC address when communicating with the visited network.

5.2.6 Legal aspects

When it comes to tracking malicious users there is not that much difference compared to a mobile users using the normal mobile data connection among the systems.

For Anyfi.net and SWISH there is no difference at all since the traffic is tunneled to the carrier. From the outside it will appear the same as normal mobile data traffic and a carrier is assumed to have sufficient logs for that.

For Eduroam and Passpoint additional logs on the visited network combined with the ones from the carrier are required to identify a misbehaving user.

Similar to tracking, the difficulty of legal interception of traffic does not change when using Anyfi.net or SWISH.

The same is not true for Eduroam and Passpoint. A mobile user that roams to many different WLAN networks instead of staying on their mobile connection makes it much more difficult to intercept the traffic. Law enforcement would be required to monitor traffic from each network used which may not be feasible.

The possibilities for content filtering and restrictions are different between the systems. For Anyfi.net and SWISH the mobile user are subjected to the same restrictions as on the carrier network. For Eduroam and Passpoint the mobile user is subjected to the restrictions of the visited network. This means that a carrier that for example wishes to block VoIP traffic is able to do so with Anyfi.net and SWISH but not with Eduroam and Passpoint. This is obviously in the interest of carrier. It may also be in the best interest of the mobile user as it ensures a constant experience.

Chapter 6
Conclusions

In this chapter we summarize the conclusions of the analysis and comparison of the systems. Thus far we tried to avoid to make conclusions on how the observed differences affect the overall security. To arrive at such an overall judgement on the security of the systems is not an easy task and, as a matter of fact, such an endeavour is best done when also the trust relations in the system are fully characterized. The latter requires either a real life system or a detailed application model. In our analysis we can only judge the systems security from a generalized model perspective and we have chosen to do this on the basis of the two use cases that were introduced in Section 3.2. As such we largely ignore to explore different setups and security implications that are the result of business originating trust relations. On the other hand we believe that through our approach that led to the selection of the systems and use cases that we in fact cover other solutions and usage scenarios as well.

The chapter is organized as follows. First we discuss some general security considerations that are more or less independent with respect to the two use cases. Then follow two sections that relate to the specific use cases.

6.1 General aspects

The analysed systems can be divided into two main groups, which we designated as *tunnel based* solutions and *non-tunnel based* solutions, 6.1. The word tunnel refers here to a cryptographically protected communication (one-hop) channel between the connecting mobile device and a trusted node (AP) in the user's home network. It is also via this trusted node that the user will be accessing the Internet. Systems belonging to the same group realize a protection that has much in common but systems belonging to different groups realize a protection that differs in many ways. The reader should be aware that Passpoint actually does not refer to a specific system but to a set of standardized mechanisms from which a system can be implemented. Yet through its nature we regard systems that will utilize Passpoint as non-tunneling. Note that there are system implementations that use a tunnel between the visited network and the home network. We do not refer to these as tunneling solutions because they are multi-hop solutions.

Table 6.1: Tunnel and Non-Tunnel solutions

Tunnel	Non-Tunnel
Anyfi.net	Fon
SWISH	Eduroam
	Passpoint

6.1.1 User data plane protection

From the mobile user perspective, the tunnel based solutions Anyfi.net and SWISH provide Internet access with a security level that is similar to what the home network or carrier network provides. For example, any firewall protection for Internet access that is deployed in the home network is easily made available to the mobile user. If the mobile user trusts the device and the home network, the mobile user also can trust the secure tunnel. Users that cannot trust the device will have to rely on protection mechanisms that are realized closer tight to the application and that provide pure end-to-end security.

The security of the tunnels rely on well established protection mechanisms in both systems. Anyfi.net extends the WLAN protection which use AES for encryption and MIC schemes for data integrity protection and SWISH uses IPsec to protect the tunnel.

The non-tunnel based solutions provide a reduction in security compared to the home network as the break-out to the Internet occurs on the visited network. This gives the AP access to clear text user plane data which adds the requirement for trust in the visited network. This trust can be difficult to establish as the visited network is never authenticated in any of the non-tunnel based solutions. To reach the same level of security as with tunneled solutions the mobile user needs to employ additional protection measures such as a VPN tunnel.

6.1.2 Key management

The main difference between the tunneling and the non-tunneling solutions is that for Anyfi.net and SWISH the session keys never leave the home network or carrier network. For Eduroam and Passpoint the visited networks are given access to the session key which creates many weaknesses in the trust relations of the systems.

Except for SWISH the systems basically use the existing procedures for authentication and key establishment. SWISH uses its own protocol that relies on a PKI infrastructure. In SWISH the certificates are used to implement more protection features than the other systems which can be viewed as an advantage over the other systems. However the use of PKI based solutions to support setups like our Use case B is problematic. For small networks setting up a PKI is unnecessary complex and for large networks the interoperability problems between PKIs rooted in different CAs creates locking barriers from technical perspective and from trust perspective. Hence the key management in SWISH is more suited for operation in a single organisation.

It should be noted that in the tunneling solutions the WLAN protection mechanism originally designed primarily for local air interface protection is now operated over other networks. Like said before, this is not causing any concern for the user data protection itself. But, as noted before, the challenge response mechanisms are now operated over unknown channels which increases the risk of becoming exposed to attacks on the underlying keys through off-line dictionary attacks. Hence compared to WLAN access only in the home network the mobile user should shorten the life-time of shared WLAN keys.

6.1.3 Privacy

None of the systems manages to provide full anonymity. Either the anonymity set is too small or there may be control data transmitted that can disclose the identity of the user. It should be noted that this is hardly surprising as requirements on access control forces the use of identities or pseudonyms which give inroads to methods that correlate to the user's identity. The fact that part of the data for access control is transmitted by radio waves or open interfaces makes it even more difficult to hide the identities of the users. As we will see the situation is somewhat better in Use Case B.

6.1.4 Control plane protection

Since all the solutions provide a way to get Internet access there is interest from outsiders to use networks for Internet access. Hence it is obvious that protection mechanisms must be in place that protect the interfaces over which the control data is transmitted. It is the visited network that has most interest in such protection. We return to this subject when we consider the specific use cases. We conclude here with the observation that although the motives for protection may differ between use cases a lack of access control increases the risk of denial of service attacks getting deeper into the network, that network interfaces are becoming more exposed, and that capacity is wasted on unauthorized users.

6.1.5 Legal aspects

The solutions that rely on tunnels bring a clear advantage over the non-tunnel based solutions when it comes to tracking down malicious users. The fact that the break-out to the Internet always occurs via the home network or carrier network means that legal interception is simple to carry out and that Internet misuse can more easily be traced in the tunnel mode solutions than in the non-tunnel mode ones where the mobile users get access to the Internet via different internet access routes. The non-tunnel approach requires additional logs from the visited network to be able to identify users.

Content filtering and restrictions have an interesting effect in Anyfi.net and SWISH due to their tunneling. Mobile users are subjected to the same restrictions as on their home network which can be both good and bad for the user. It means that users will get around any local restrictions that would otherwise disrupt the connection. They can however not use the system to get around any restrictions

on their home network, nor can they gain access to extra services available for the visited network.

In Fon, Eduroam, and Passpoint the mobile user is always subjected to the filtering and restrictions of the visited network which may result in a less consistent user experience.

6.2 Use case A

In the comparison of Chapter 6 it becomes apparent that there is a large gap in the security between the two tunnel based solutions Anyfi.net and SWISH and the non-tunnel based solution Fon.

6.2.1 Mobile user perspective

Albeit a bit speculative, one can argue that in Use case A setups the mobile user is faced with APs of networks that he/she has little reason to trust. Hence tunneling solutions where the keys that protect the user data plane are only present at the home network node and the mobile user's device have a clear security advantage over the non-tunneling solutions[1].

Anyfi.net and SWISH achieve each a security similar to what a user receives when connected to their home network. Fon however falls short on both authentication and data security. In the Fon system, anybody is able to set up a rogue access point as the only requirement is to own a router or modem with Fon software on it. A mobile user has no way of protecting themselves against this. Hence users must manually verify the security each time they authenticate. Although technically possible it is likely that such a demand on the user leads to attacks exploiting human errors or using social engineering. Combined with the fact that the actual credentials are transferred, identity theft is thus a trivial task in Fon. The latter can be considered a serious drawback of Fon.

The lack of security in Fon's approach on the control as well as the user data plane is a major problem for the users that have some security requirements at all. These shortcomings result in a very high risk of being exposed to attacks as also can be seen from Figure 4.13. There are very few situations where such an approach is suitable. Users that have any form of requirement on protection are forced to use protection mechanisms at the application level. Such an approach is not acceptable for average users.

All systems require some form of pre-setup in form of registrations and/or keys that have to be arranged. Although the burden of such a setup and the subsequent maintenance are very implementation dependant we believe that the SWISH approach is more problematic as explained in the previous section.

As mentioned in the previous section, none of the system can claim to achieve anonymity when configured for Use case A.

[1] We ignore here the case of mobile users that desire to hide their internet access since for those users tunneling is a disadvantage.

6.2.2 Visited network perspective

In Use case A it is likely that we have a setup where AP owners share all or part of the AP capacity with mobile users. The access control that needs to be exercised to limit the capacity use only to registered user (customers) can be realized in all systems. In Anyfi.net and Fon the visited network delegates the decision to authorize or deny users access to the ISP that manages the system. SWISH may also rely on the ISP for this function but as the home networks are authenticated to the visited networks, each visited network may also perform access control.

6.3 Use case B

In Use case B the authentication centre that also authenticates cellular devices is used to authenticate registered WLAN users. As explained before network operators are very careful with exposing interfaces towards the authentication functionality of these authentication centres. Primarily because misuse of such interfaces leads to easy deployment of rogue APs and thus security breaches but also capacity concerns motivates great care when making the authentication interfaces available towards others.

The current 3GPP standards, e.g. [25], are very vague on how to effectively protect against misuse of an exported authentication interface and therefore we consider this type of approach as highly problematic when a network operator wants to use/cooperate with many independent WLAN infrastructure operators.

6.3.1 Mobile user perspective

For a mobile user, the tunnel based solutions Anyfi.net and SWISH achieve a security level similar to when the user is connected to a mobile network, both in terms of authentication and user plane data security. The mobile device and the carrier network are mutually authenticated and the user plane data is confidentiality protected from the mobile device to the carrier network.[2]

The non-tunnel based solutions Eduroam and Passpoint have very different characteristics. While these systems do achieve mutual authentication between the mobile device and the carrier network, such authentication is of little use to the mobile user. The only relevant property achieved by authenticating the carrier is the generation of the session key that provides confidentiality for the wireless transmissions and that the visiting network somehow has a connection to the network operator's authentication interfaces.

Another aspect is that the visited network, which is essentially unknown to the mobile user, is given access to the session key that is established in parallel with the authentication. Thus a visiting network has access to the user plane data. This is a major problem as the mobile device lacks ways of establishing the necessary trust in the visited network. The mobile device user has no way of protecting against rogue access points which misuse an authentication interface and then are able to intercept and modify the clear text user plane data. Since the

[2]The mobile networks do not provide data integrity protection in the use data plane.

only thing required to create a rogue access point is the secret key from one of the visited networks in the system this is not a secure design.

The tunnel based solutions provide anonymity in a satisfactory way as temporary identities can be used and the user plane data is not available outside the trusted network. This creates a large anonymity set that the mobile user will not be identifiable within.

The non-tunnel based solutions also allow temporary identities to be used but a mobile user might be identifiable by studying the user plane data traffic. Mobile users thus receive less anonymity than if they were to stay connected to a mobile network.

6.3.2 Visited network perspective

Provided the network operator opens up an interface to its AuC the visited network has a simple way to authenticate the legitimate users. Although the visited network cannot be sure if the (U)SIM card is actually present in the mobile user's device it can be sure with very high degree of certainty that the mobile user's device must somehow have a connection to the subscribers (U)SIM card[3] In the Anyfi.net solutions part of the problem of misuse of the AuC by rogue APs is avoided as now the use of the AuC results in a tunnel from the user into the MNOs network.

If the systems are used between different MNOs networks, SWISH provides the best solution for charging and accounting of data volumes by exploiting non-repudiation in the protocol. Passpoint and, to a certain degree, Anyfi.net, require the carrier networks to trust each other as dishonest accounting can be difficult to resolve. In Anyfi.net it is possible to detect such problems using the MCS node but in Passpoint the carrier networks lack means to address cheating in the accounting.

6.4 Wrap up

We see that in both use cases the tunneling solutions give the mobile user the best protection. Because the use of PKI schemes between different organisations is problematic we conclude that the Anyfi.net can be regarded as the preferred solution for the users. For the mobile user the better security experience offered by tunneling solutions can already be reason to use Anyfi.net. But Anyfi.net also has some advantages to the visited network operators and in Use case B to the mobile network operator by providing simple setup and protection of the use of the authentication interface for setting up rogue AP.

Yet in situations with lower security ambitions systems like Eduroam and Passpoint may be preferable as the lack of tunnels lead to an increase in performance. User with high security ambitions can still use these systems by using end-to-end security solutions like IPsec or TLS based VPNs.

[3] A setup comparable to the Remote SIM Access Profile in the Bluetooth standard.

References

[1] *Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2012-2017*, http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-520862.pdf

[2] C. Rigney, S. Willens, A. Rubens, W. Simpson, *Remote Authentication Dial In User Service (RADIUS)*, 2000, http://tools.ietf.org/html/rfc2865

[3] V. Fajardo, Ed., J. Arkko, J. Loughney, G. Zorn, Ed., *Diameter Base Protocol*, 2012, http://tools.ietf.org/html/rfc6733

[4] Dieter Gollman, *Computer Security 3rd ed.*, John Wiley and Sons, Ltd, 2011

[5] IEEE Computer Society, *Part 11: Wireless LAN Medium Access Control(MAC) and Physical Layer (PHY) Specifications*, 2012, http://standards.ieee.org/findstds/standard/802.11-2012.html

[6] IEEE Computer Society, *Port-Based Network Access Control*, 2010, http://standards.ieee.org/findstds/standard/802.1X-2010.html

[7] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, H. Levkowetz, Ed., *Extensible Authentication Protocol (EAP)*, 2004, http://tools.ietf.org/html/rfc3748

[8] D. Simon, B. Aboba, R. Hurst, *The EAP-TLS Authentication Protocol*, 2008, http://tools.ietf.org/html/rfc5216

[9] P. Funk, S. Blake-Wilson, *Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0 (EAP-TTLSv0)*, 2008, http://tools.ietf.org/html/rfc5281

[10] H. Haverinen, Ed., J. Salowey, Ed., *Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM)*, 2006, http://tools.ietf.org/html/rfc4186

[11] J. Arkko, H. Haverinen, *Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)*, 2006, http://tools.ietf.org/html/rfc4187

[12] *Common Criteria*, http://www.commoncriteriaportal.org/

[13] Johan Gustafsson, Daniel Thor, *Security Risk Evaluation of the FON Network*, Master of Science Thesis, KTH Informations- och kommunikationsteknik, 2007, Stockholm, Sweden

[14] Anyfi.net `http://anyfi.net/`

[15] Gabe Conradi, *Current Status and Overview of the CAPWAP Protocol*, 2010, `http://www.cs.wustl.edu/~jain/cse574-10/ftp/capwap/index.html`

[16] Nishanth Sastry, Jon Crowcroft, Karen Sollins, *Architecting Citywide Ubiquitous Wi-Fi Access*, in HotNets 07: Proceedings of the 6th Workshop on Hot Topics in Networks, 2007

[17] Eduroam, `https://www.eduroam.org/`

[18] Fon, `http://corp.fon.com/`

[19] Charles E. Perkins, *Mobile IP*, IEEE Communications Magazine, Volume 35, Number 5, 1997

[20] Wi-Fi CERTIFIED Passpoint, `http://www.wi-fi.org/discover-and-learn/wi-fi-certified-passpoint%E2%84%A2`

[21] Tobias Heer, Stefan Götz, Elias Weingärtner, Klaus Wehrle, *Secure Wi-Fi Sharing at Global Scales*, 2008, Aachen, Germany

[22] Damien Leroy, Gregory Detal, Julien Cathalo, Mark Manulis, François Koeune, Olivier Bonaventure *SWISH: Secure WiFi sharing*, Computer Networks 55 (2011) 1614-1630

[23] Wifi.com `http://wifi.com/`

[24] Mark Manulis, Damien Leroy, Francois Koeune, Olivier Bonaventure, and Jean-Jacques Quisquater, *Authenticated Wireless Roaming via Tunnels: Making Mobile Guests Feel at Home*, ASIACCS 09, March 10-12, 2009, Sydney, Australia

[25] *3GPP system to Wireless Local Area Network (WLAN) interworking; System description*, `http://www.3gpp.org/ftp/Specs/html-info/23234.htm`

Appendix A

Framework for a security analysis of WLAN sharing and distribution systems

A.1 Introduction

Presently there is no framework that we can use to compare the security of different WLAN access solutions for roaming users. Therefore, as part of this thesis work, we have developed such a framework ourselves. This framework is intended to provide a structured way towards analysing systems which serve to share or distribute WLAN access. Such systems solve this problem in many different ways which makes it difficult to analyse them in a way that enables comparison. This framework tries to overcome this problem by focusing on a few subjects which are very central in most systems.

The framework is organized into multiple steps. In these steps the entities acting in the system are specified and their important assets are identified. The system is then analysed by specifying which threats exists and how a malicious entity could exploit them, what countermeasures are employed and which threats remain in the system.

A.2 Entities

In this step we identify all the entities in the system and explain what their role is and their relations which each other.

A.2.1 End-user

Define the role of the end-user, the one acquiring capacity from a network under another entity's control. Explain what they are purchasing, from whom and through whom. Explain what hardware, software or accounts are required by an end-user. An end-user may also operate a visited network (to other end-users).

A.2.2 Visited network operator

Define the role of the visited network operator, the one providing an end-user with capacity from their own network. Explain what they are selling, to whom and through whom. Explain what hardware, software or accounts are required by a visited network. A visited network operator may also be an end-user.

A.2.3 Third party

Define the role of any third party. This entity could be a Mobile Network Operator (MNO), an ISP, a CA, a payment manager etc. Explain what its responsibilities are and how it interacts with the end-users and visited networks.

A.3 Use Cases

While not all systems solve the same problem, they solve similar problems. Most systems can be described using one or both of the following use cases with some modifications. In this step the systems are explained with these use cases as the base. Describe which use cases are fulfilled, to what degree and what modifications there are. Also explain which use case is the main use case that the system is intended for.

A.3.1 A - ISP distributes Internet access

An ISP gives its customers Internet access by allowing users to connect to any modem managed by that ISP, regardless of which customer has physical control of the device. Customers that subscribe to this service either has the firmware on their modem/router activated/updated or receive new hardware as part of the service. When they encounter the network of another customer with this service they are able to connect to that network. After they have been authenticated they are given Internet access.

The use case can be characterized as now follows:

1. ISP manages modems in participating networks
2. Mobile device associates with visited network
3. Mobile device is authenticated
4. Mobile device is given Internet access

An important point in this use case is how guests are separated from the visited networks. The visited networks are intended to be the private networks of end-users who expect their network to be secure against intrusion.

Other key points are how authentication and data security are handled. Depending on where the mobile guest is authenticated there will be different levels

of security for the data. If the authentication happens somewhere under the control of the mobile guest (i.e. the home network) then the mobile guest can achieve a high level of security. If the authentication happens somewhere under the control of the ISP then the mobile guest needs a strong trust relationship towards that ISP to achieve high security. If the authentication happens somewhere outside the control of the mobile guest or the ISP (i.e. the visited network) then high security cannot be achieved.

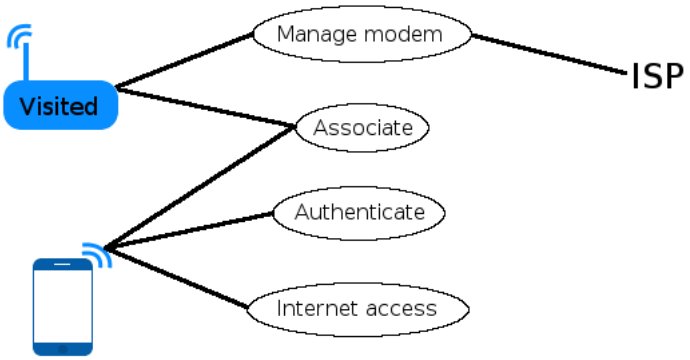

Figure A.1: Definition of Use Case A

A.3.2 B - Mobile offload using WLAN

Through an agreement between a WLAN network operator and an MNO, subscribers of that carrier are given access to the network. When a mobile device of a subscriber comes within range of the visited network the device will automatically connect to it. After the mobile user is authenticated by the carrier it is given Internet access.

The use case can be characterized as now follows:

1. The MNO creates a roaming agreement with a WLAN network operator
2. The mobile device associates with visited network
3. The mobile device is authenticated by the MNO
4. The mobile device is given Internet access
5. The visited network operator charges MNO for the service

Similar to use case A, an important aspect of this use case is where a user is authenticated and who is in control of that area. If the authentication is performed in the network of the MNO then a high level of security can be achieved. If instead the visited network is allowed to authenticate a user it will also gain access to the private data. This may not be apparent to the mobile guest as they may believe to have a secure connection to their MNO after authenticating to it.

Another important aspect of this use case is who is allowed access to the authentication framework. The authentication servers are often a very sensitive point, both from a security and a availability point of view. Who is allowed access to these affect the security of the system as that entity is allowed to accept connections in the name of the MNO.

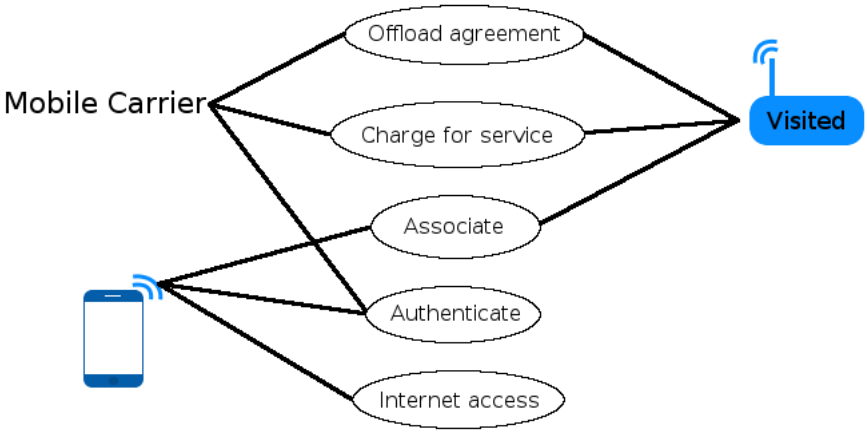

Figure A.2: Definition of Use Case B

A.4 Assets

This step aims to identify the important assets belonging to the different entities. It also estimates how critical these assets are to the entity.

A.4.1 End-user

Identify which assets are important to an end-user and estimate their importance. This could be authentication credentials, private data, payment credentials etc.

A.4.2 Visited network operator

Identify which assets are important to a visited network operator and estimate their importance. This could be authentication credentials, private data, payment credentials, capacity etc.

A.4.3 Third party

Identify which assets are important to any third party and estimate their importance. This could be authentication credentials, company credibility, payment

details, membership databases etc.

A.5 Trust relations

This step aims to clarify which trust relationships exist in the system and identify possible problems with them.

A.5.1 Trust details

Specify the trust relationships in the system and explain in which use case they are relevant. Provide figures that shows this. Try to provide an answer to the following questions:

- Who trusts whom?
- What does the trust protect?
- How important is the trust?

A.5.2 Possible weaknesses

Explain any weak points there are with this trust model.

A.6 Authentication

Most systems have some form of restrictions on who is allowed to use it and how they are authenticated. This section aims to clarify how this authentication work, identify potential threats, how they are countered and which threats are missed.

A.6.1 Authentication details

Specify how the authentication works and what the key points in the implementation are. Focus especially on the architecture of the authentication and how it relates to the trust model. Examine the authentication both from the perspective of the end user and from the system that performs the authentication. Try to provide an answer to the following questions:

- Who is authenticated and to whom?
- Where is the point of authentication and who controls it?
- Is the authentication distributed? If so, explain how.
- Who is allowed access to the authentication framework?
- Why is there need of authentication?
- What methods are used to authenticate?
- What type of credentials are used?

- Who has access to those credentials?
- Is the authentication user or group specific?

A.6.2 Threats

Identify which assets that could be a risk as a during the authentication process. This includes the actual authentication as well as storage of credentials.

Explore in what ways a malicious entity could try to take advantage of weaknesses to compromise the assets.

A.6.3 Countermeasures

Identify which countermeasures exists to prevent these weaknesses from being exploited and to protect the assets.

A.6.4 Remaining threats

Document which threats are not sufficiently dealt with and how it affects the security of the system.

A.7 Data security

Depending on the security model of a system, different measures are taken to protect the confidentiality and integrity of the communication. This sections aims to identify which type of communication there is in the system and clarify how they are protected. It also tries to identify potential threats, how they are countered and which threats are missed.

A.7.1 Security details

Specify what communication occurs between different entities in the system, how the data is transferred and who has access to the data. Specify how separation, if any, between end-user and visited network data is handled. Focus especially on the architecture of the security, rather then implementation details. Try to provide an answer to the following questions:

- What different types of communication are there?
- How is user data plane data protected?
- How is control plane data protected?
- How is wireless data protected?
- How is wired data protected?
- Who can view the data?
- Who can modify the data?

- How are visited networks protected from guests?
- How are guests protected from visited networks?

A.7.2 Threats

Identify possible weaknesses in this security model and specify which assets could be at risk.

Explore in what ways a malicious entity could try to take advantage of these weaknesses.

A.7.3 Countermeasures

Identify which countermeasures exists to prevent these weaknesses from being exploited and to protect the assets.

A.7.4 Remaining threats

Document which threats are not sufficiently dealt with and how it affects the security of the system.

A.8 Anonymity

For some end-users, remaining anonymous while using other networks is a important aspect of a system. This section aims to specify how anonymity is handled in the system and how it effects accountability.

Examine which measures are taken in the system to ensure users stay anonymous and how well they succeed. Also identify if different sessions from the same end-user can be linked together.

A.9 Availability

This section aims to determine if the systems introduces any weak points that affects the availability of the system.

Identify any possible threats to the availability of the system and examine what countermeasures there are to make the system more robust. Focus on weak points that are introduced by the system rather then existing weak points common to all WLAN networks.

A.10 Legal Aspects

Sharing Internet access comes with several legal implications such as accountability for the traffic or terms of service from the ISP. Identify any possible legal problems with the system and examine how they affect it.